FortiSwitch-548B

Version 5.2.0.2

User Guide

FORTINET

FortiSwitch-548B User Guide

Version 5.2.0.2

Revision 2

15 December 2010

Trademarks

Regulatory compliance

FCC Class A Part 15 CSA/CUS

Table of Contents

1. Introduction

1.1 Scope

This document describes:

- how to install the FortiSwitch-548B switch (the Switch)
- how to use the CLI console to manage the Switch
- how to use the web-based management interface to configure the Switch

1.2 Documentation

The Fortinet Technical Documentation web site, http://docs.fortinet.com, provides the most up-to-date versions of Fortinet publications, as well as additional technical documentation such as technical notes.

1.2.1 Fortinet Knowledge Base

The Fortinet Knowledge Base provides additional Fortinet technical documentation, such as troubleshooting and how-to-articles, examples, FAQs, technical notes, a glossary, and more. Visit the Fortinet Knowledge Base at http://kb.fortinet.com.

1.2.2 Comments on Fortinet Technical Documentation

Please send information about any errors or omissions in this or any Fortinet technical document to techdoc@fortinet.com.

1.3 Customer Service and Technical Support

Fortinet Technical Support provides services designed to make sure that your Fortinet products install quickly, configure easily, and operate reliably in your network.

To learn about the technical support services that Fortinet provides, visit the Fortinet Technical Support web site at https://support.fortinet.com.

You can dramatically improve the time that it takes to resolve your technical support ticket by providing your configuration file, a network diagram, and other specific information. For a list of required information, see the Fortinet Knowledge Center article What does Fortinet Technical Support require in order to best assist the customer?T

1.4 Training

Fortinet Training Services provides classes that orient you quickly to your new equipment, and certifications to verify your knowledge level. Fortinet provides a variety of training programs to serve the needs of our customers and partners world-wide.

To learn about the training services that Fortinet provides, visit the Fortinet Training Services web site at http://campus.training.fortinet.com, or email them at training@fortinet.com.

2. Product Overview

2.1 Switch Description

FortiSwitch-548B is a SFP+ 10-Gigabit Ethernet backbone switch designed for adaptability and scalability. The Switch provides a management platform and uplink to backbone. Alternatively, the Switch can utilize up to 48 10-Gigabit Ethernet ports to function as a central distribution hub for other switches, switch groups, or routers. The built-in 1000/100/10 Ethernet port is for out of service. The FortiSwitch-548B power system provides two power supplies. The FortiSwitch-548B SFP+ port also provides 1-Gigabit speed by manual settings.

2.2 Features

- Supports 48 SFP+ 10-Gigabit Ethernet ports
- 1 built-in 1000/100/10 Ethernet port for out of band switch mangement.
- Support two power supplies

  Software will detect power failure and read information(what power install on your system)
- IEEE 802.3z and IEEE 802.3x compliant Flow Control for all 10-Gigabit ports
- Supports 802.1D STP, 802.1S MSTP, and 802.1w Rapid Spanning Tree for redundant back up bridge paths
- Supports 802.1Q VLAN, Protocol-based VLAN, Subnet-based VLAN, MAC-based VLAN, Protected Port, Double VLAN, Voice VLAN, GVRP, GMRP, IGMP snooping, 802.1p Priority Queues, Port Channel, port mirroring
- Supports VTP (VLAN Trunking Protocol)
- Supports CDP
- Supports LLDP with potential communication problems detection
- Supports Port Security
- Multi-layer Access Control (based on MAC address, IP address, VLAN, Protocol, 802.1p, DSCP)
- Quality of Service (QoS) customized control
- 802.1x (port-based) access control and RADIUS Client support
- TACACS+ support
- Administrator-definable port security
- Supports DHCP Snooping, Dynamic ARP Inspection and IP Source Guard (IPSG)
- ARP support
- IP Routing support
- OSPF v2 and v3 support
- RIP v1/v2 and RIPng support
- Router Discovery Protocol support
- Virtual Router Redundancy Protocol (VRRP) support

- VLAN routing support
- IP Multicast support
- IGMP v1, v2, and v3 support
- DVMRP support
- Protocol Independent Multicast - Dense Mode (PIM-DM) support for IPv4 and IPv6
- Protocol Independent Multicast - Sparse Mode (PIM-SM) support for IPv4 and IPv6
- IPV6 function
  - Supports DHCPv6 protocol, OSPFv3 protocol, Tunneling, loopback
  - Provides to configure IPv6 rotuing interface, routing preference
- DHCP Client and Relay support
- DNS Client and Relay support
- Per-port bandwidth control
- SNMP v.1, v.2, v.3 network management, RMON support
- Supports Web-based management
- CLI management support
- Fully configurable either in-band or out-of-band control via RS-232 console serial connection
- Telnet remote control console
- TraceRoute support
- Traffic Segmentation
- TFTP/FTP upgrade
- SysLog support
- Simple Network Time Protocol support
- Web GUI Traffic Monitoring
- SSH Secure Shell version 1 and 2 support
- SSL Secure HTTP TLS Version 1 and SSL version 3 support
- Fibre Channel Over Ethernet(FCoE)
  - FIP Snooping
- Data Center Bridge(DCB)
  - Enhanced Transmission Selection(ETS, IEEE 802.1Qaz)
  - Priority Flow Control(PFC, IEEE 802.1Qbb)
  - Congestion Notification(CN, IEEE 802.1Qau)

2.3 Front-Panel Components

The front panel of the Switch consists of 48 10-Gigabit interfaces, 2 LED indicators, 1 built-in 1000/100/10 RJ-45 Ethernet service ports, an RS-232 communication port, and 48 port LEDs.

The upper LED indicators display power status. The lower LED indicators displays the status of the switch. An RS-232 DCE console port is for setting up and managing the Switch via a connection to a console terminal or PC using a terminal emulation program. Each port LED has two colors: Color green represents port link status; Color Orange represents port activity status and it will be blinking if the port has an activity.

2.4 LED Indicators

The Status LED indicator represnts status of the switch. The Power LED indicator represent power ON or OFF.

2.5 Rear Panel Description

The rear panel of the Switch contains Dual Redundant AC power connector and Four Fans. The four fans can be built in back-to-front and front-to-back(depend on customer requirement).

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

2.6 Management Options

The system may be managed by using one Service Ports through a Web Browswer,Telent, SNMP function and using the console port on the front panel through CLI command.

2.7 Web-based Management Interface

After you have successfully installed the Switch, you can configure the Switch, monitor the LED panel, and display statistics graphically using a Web browser, such as Mozilla FireFox (version 3.6 or higher) or Microsoft® Internet Explorer (version 5.0 or above).

To access the Switch through a Web browser, the computer running the Web browser must have IP-based network access to the Switch.

2.8 Command Line Console Interface Through the Serial Port or Telnet

You can also connect a computer or terminal to the serial console port or use Telnet to access the Switch. The command-line-driven interface provides complete access to all switch management features.

2.9 SNMP-Based Management

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

- RFC1643 Ether-like MIB
- RFC1493 Bridge
- RFC 2819 RMON
- RFC 2233 Interface MIB
- RFC 2571 (SNMP Frameworks)
- RFC 2572 (Message Processing for SNMP)
- RFC 2573 (SNMP Applications)
- RFC 2576 (Coexistence between SNMPs)
- RFC 2618 (Radius-Auth-Client-MIB)
- RFC 2620 (Radius-Acc-Client-MIB)
- RFC 1724 (RIPv2-MIB)
- RFC 1850 (OSPF-MIB)
- RFC 1850 (OSPF-TRAP-MIB)
- RFC 2787 (VRRP-MIB)

- RFC 3289 - DIFFSERV-DSCP-TC
- RFC 3289 - DIFFSERV-MIB
- QOS-DIFFSERV-EXTENSIONS-MIB
- QOS-DIFFSERV-PRIVATE-MIB
- RFC 2674 802.1p
- RFC 2932 (IPMROUTE-MIB)
- Fortinet Enterprise MIB
- ROUTING-MIB
- MGMD-MIB
- RFC 2934 PIM-MIB
- DVMRP-STD-MIB
- IANA-RTPROTO-MIB
- MULTICAST-MIB
- FASTPATH-ROUTING6-MIB
- IEEE8021-PAE-MIB
- INVENTORY-MIB
- MGMT-SECURITY-MIB
- QOS-ACL-MIB
- QOS-COS-MIB
- RFC 1907 - SNMPv2-MIB
- RFC 2465 - IPV6-MIB
- RFC 2466 - IPV6-ICMP-MIB
- TACACS-MIB
- USM-TARGET-TAG-MIB
- IGMP/MLD Snooping
- IGMP/MLD Layer2 Multicast
- QoS – IPv6 ACL
- Voice VLAN
- Guest VLAN
- LLDP MED
- RFC 2925 (DISMAN-TRACEROUTE-MIB)
- RFC 2080 (RIPng)
- OSPFV3-MIB

3. Installation and Quick Startup

3.1 Package Contents

Before you begin installing the Switch, confirm that your package contains the following items:

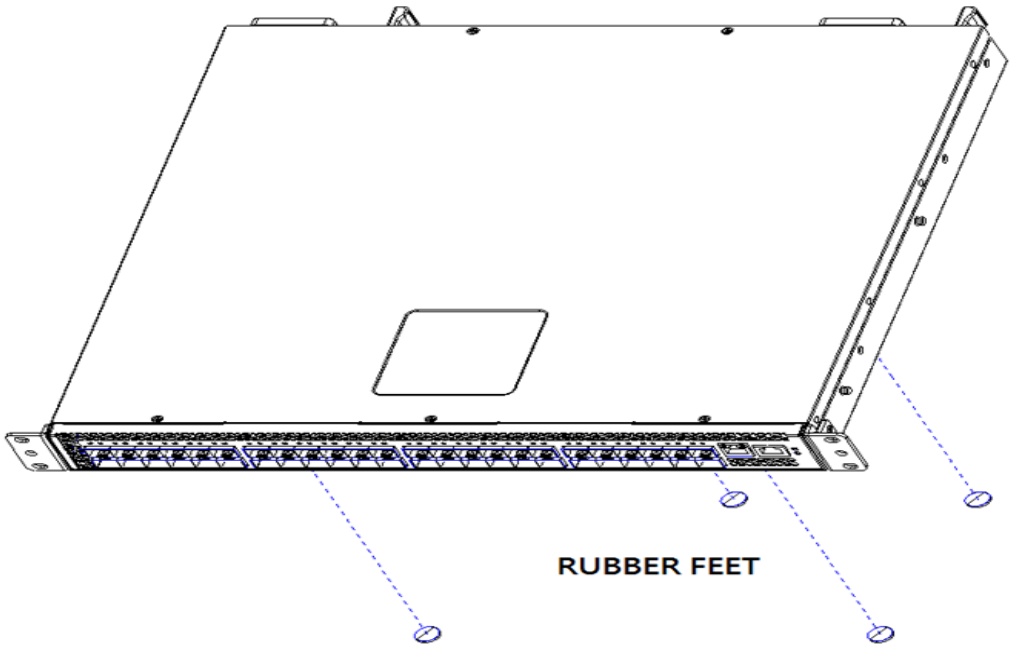
- One FortiSwitch-548B Layer III 10-Gigabit Managed Switch
- Mounting kit: 2 mounting brackets and screws
- Four rubber feet with adhesive backing
- One AC power cord
- This User’s Guide with Registration Card
- CLI Reference
- CD-ROM with User’s Guide and CLI Reference

3.2 Switch Installation

Installing the Switch Without the Rack

1. Install the Switch on a level surface that can safely support the weight of the Switch and its attached cables. The Switch must have adequate space for ventilation and for accessing cable connectors.
2. Set the Switch on a flat surface and check for proper ventilation. Allow at least 5 cm (2 inches) on each side of the Switch and 15 cm (6 inches) at the back for the power cable.
3. Attach the rubber feet on the marked locations on the bottom of the chassis.

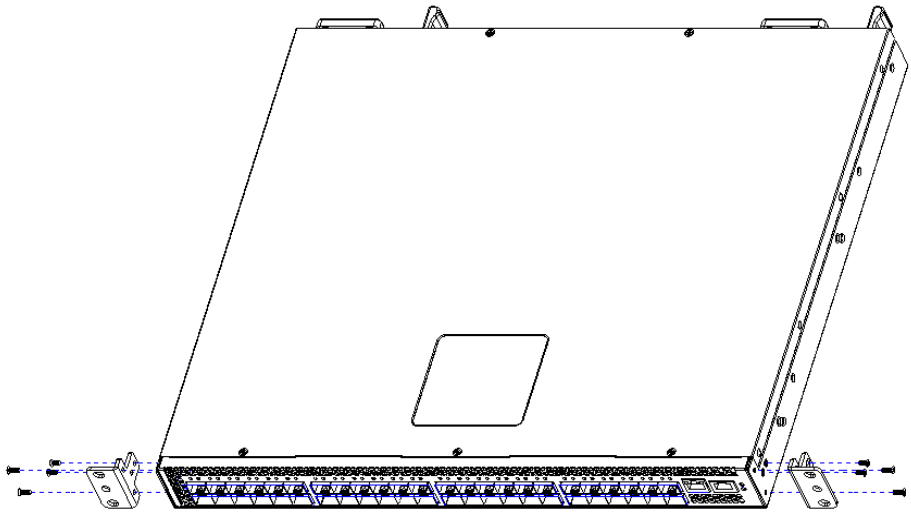
The rubber feet are recommended to keep the unit from slipping.



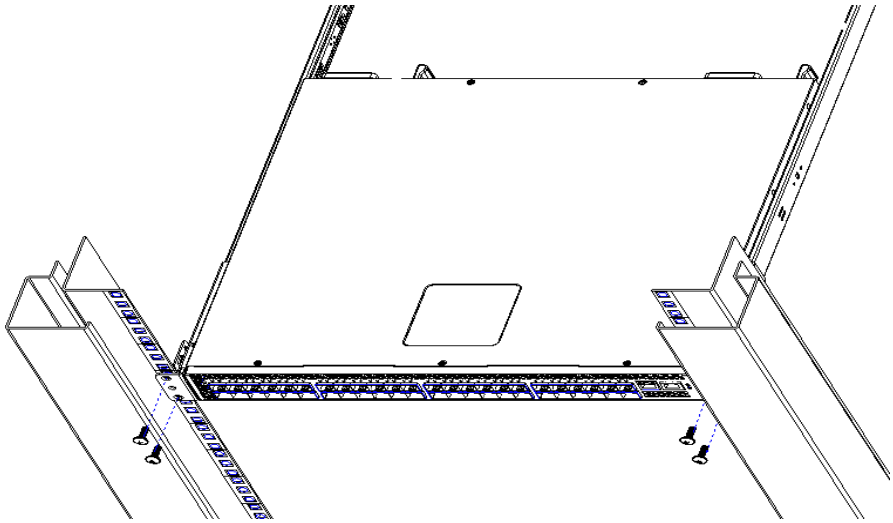
3.3 Installing the Switch in a Rack

You can install the Switch in most standard 19-inch (48.3-cm) racks. Refer to the illustrations below.

1. Use the supplied screws to attach a mounting bracket to each side of the Switch.
2. Align the holes in the mounting bracket with the holes in the rack.
3. Insert and tighten two screws through each of the mounting brackets.



MOUNTING EAR & SCREWS



3.4 Quick Starting the Switch

1. Read the device Installation Guide for the connectivity procedure. In-band connectivity allows access to the FortiSwitch-548B Series Switch locally. 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, do the following:
    - Type the word **admin** in the login area. Since a number of the Quick Setup commands require administrator account rights, FORTINET suggests logging into an administrator account.
    - Do not enter a password because there is no password in the default mode.
    - Press the <Enter> key
    - The CLI Privileged EXEC mode prompt will be displayed.
    - Use “configure” to switch to the Global Config mode from Privileged EXEC.
    - Use “exit” to return to the previous mode.

3.5 System Information Setup

3.5.1 Quick Start up Software Version Information

Table 2-1. Quick Start up Software Version Information

Command	Details
show hardware	Allows the user to see the HW & SW version the device contains System Description - switch's model name
show version	Allows the user to see Serial Number, Part Number, and Model name See SW loader, bootrom and operation version See HW version

3.5.2 Quick Start up Physical Port Data

Table 2-2. Quick Start up Physical Port

Command	Details
show Interface status { <slot/port> | all}	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 Flow Mode - Indicates the status of flow control on this port Cap. Status - Indicates the port capabilities during auto-negotiation

3.5.3 Quick Start up User Account Management

Table 2-3. Quick Start up User Account Management

Command	Details
show users	Displays all users that are allowed to access the switch User Access Mode - Shows whether the user is able to change parameters on the switch

	(Read/Write) or is only able to view (Read Only). As a factory default, admin has Read/Write access and guest has Read Only access. There can only be one Read/Write user and up to 5 Read Only users.
show loginsession	Displays all login session information
username <username> {passwd | nopasswd}	Allows the user to set passwords or change passwords needed to login A prompt will appear after the command is entered requesting the 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. The user password should not be more than eight characters in length.
copy running-config startup-config [filename]	This will save passwords and all other changes to the device. If you do not save config, all configurations will be lost when a power cycle is performed on the switch or when the switch is reset.

3.5.4 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

Table 2-4. Quick Start up IP Address

Command	Details
show ip interface	Displays the Network Configurations IP Address - IP Address of the interface Default IP is 192.168.2.1 Subnet Mask - IP Subnet Mask for the interface. Default is 255.255.255.0 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 inband 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.
ip address	(Config)#*interface vlan 1* (if-vlan 1)#*ip address <ipaddr> <netmask>* (if-vlan 1)#*exit* (Config)#*ip default-gateway <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 Displays all of the login session information

3.5.5 Quick Start up Uploading from Switch to Out-of-Band PC

Table 2-5. Quick Start up Uploading from Switch to Out-of-Band PC (XMODEM)

Command	Details
copy startup-config xmodem <filename>	This starts the upload and 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.

3.5.6 Quick Start up Downloading from Out-of-Band PC to Switch

Table 2-6 Quick Start up Downloading from Out-of-Band PC to Switch

Command	Details
copy xmodem startup-config <filename>	Sets the download datatype to be an image or config file. 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.

3.5.7 Quick Start up Downloading from TFTP Server

Before starting a TFTP server download, the operator must complete the Quick Start up for the IPAddress.

Table 2-7 Quick Start up Downloading from TFTP Server

Command	Details

copy <url> startup-config <filename>	Sets the download datatype to be an image or config file. The URL must be specified as: tftp://ipAddr/filepath/fileName. The startup-config option downloads the config file using tftp and image option downloads the code file.

3.5.8 Quick Start up Factory Defaults

Table 2-8 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 running-config startup-config [filename]	Enter yes when the prompt pops up that asks if you want to save the configurations made to the switch.
reload	Enter yes when the prompt pops up that asks if you want to reset the system. You can reset the switch or cold boot the switch; both work effectively.

4. Console and Telnet Administration Interface

This chapter discusses many of the features used to manage the Switch, and explains many concepts and important points regarding these features. Configuring the Switch to implement these concepts is discussed in detail in chapter 6.

4.1 Local Console Management

Local console management involves the administration of the Switch via a direct connection to the RS-232 DCE console port. This is an Out-of-band connection, meaning that it is on a different circuit than normal network communications, and thus works even when the network is down.

The local console management connection involves a terminal or PC running terminal emulation software to operate the Switch's built-in console program (see Chapter 6). Using the console program, a network administrator can manage, control, and monitor many functions of the Switch. Hardware components in the Switch allow it to be an active part of a manageable network. These components include a CPU, memory for data storage, other related hardware, and SNMP agent firmware. Activities on the Switch can be monitored with these components, while the Switch can be manipulated to carry out specific tasks.

4.2 Set Up your Switch Using Console Access

Out-of-band management requires connecting a terminal, such as a VT-100 or a PC running a terminal-emulation program (such as HyperTerminal, which is automatically installed with Microsoft Windows) to the RS-232 DCE console port of the Switch. Switch management using the RS-232 DCE console port is called *Local Console Management* to differentiate it from management done via management platforms, such as DView or HP OpenView.

Make sure the terminal or PC you are using to make this connection is configured to match these settings. If you are having problems making this connection on a PC, make sure the emulation is set to VT-100 or ANSI. If you still don't see anything, try pressing <Ctrl> + r to refresh the screen.

First-time configuration must be carried out through a console, that is, either (a) a VT100-type serial data terminal, or (b) a computer running communications software set to emulate a VT100. The console must be connected to the Diagnostics port. This is an RS-232 port with a 9-socket D-shell connector and DCE-type wiring. Make the connection as follows:

1. Obtain suitable cabling for the connection.You can use a null-modem RS-232 cable or an ordinary RS-232 cable and a null-modem adapter. One end of the cable (or cable/adapter combination) must have a 9-pin D-shell connector suitable for the Diagnostics port; the other end must have a connector suitable for the console's serial communications port.
2. Power down the devices, attach the cable (or cable/adapter combination) to the correct ports, and restore power.
3. Set the console to use the following communication parameters for your terminal:

- The console port is set for the following configuration:
- Baud rate: 11,520
- Data width: 8 bits
- Parity: none
- Stop bits: 1
- Flow Control: none

A typical console connection is illustrated below:

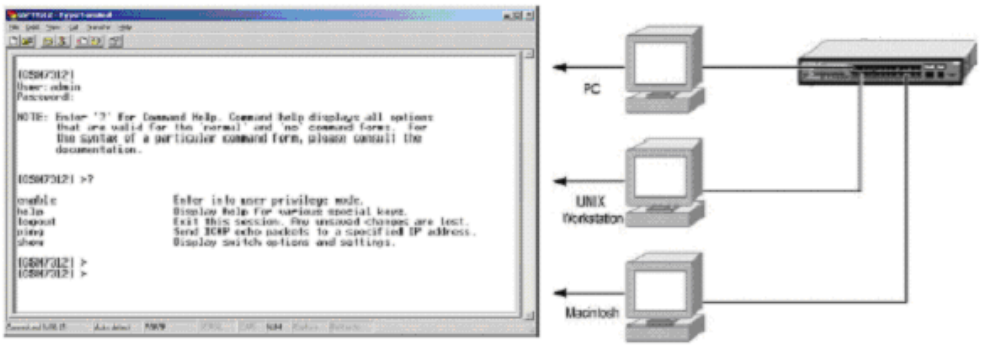


Figure 3-1: Console Setting Environment

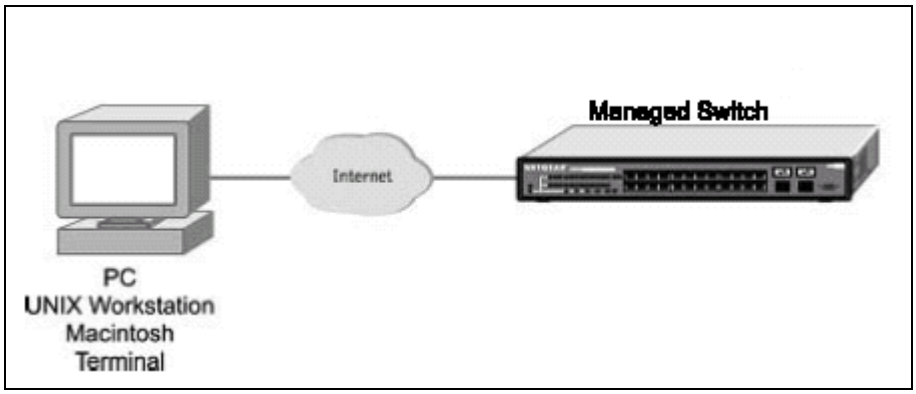
4.3 Set Up your Switch Using Telnet Access

Once you have set an IP address for your Switch, you can use a Telnet program (in a VT-100 compatible terminal mode) to access and control the Switch. Most of the screens are identical, whether accessed from the console port or from a Telnet interface.

5. Web-Based Management Interface

5.1 Overview

The Fortinet FortiSwitch-548B Series Layer III plus QoS Managed Switch provides a built-in browser interface that lets you configure and manage it remotely using a standard Web browser such as Microsoft Internet Explorer 5.0 or later or Netscape Navigator 6.0 or later. This interface also allows for system monitoring and management of the switch. The 'help' page covers many of the basic functions and features of the switch and its Web interface. When you configure the switch for the first time from the console, you can assign an IP address and subnet mask to the switch. Thereafter, you can access the switch's Web interface directly using your Web browser by entering the switch's IP address into the address bar. In this way, you can use your Web browser to manage the switch from a central location, just as if you were directly connected to the switch's console port. Below figure shows this management method.



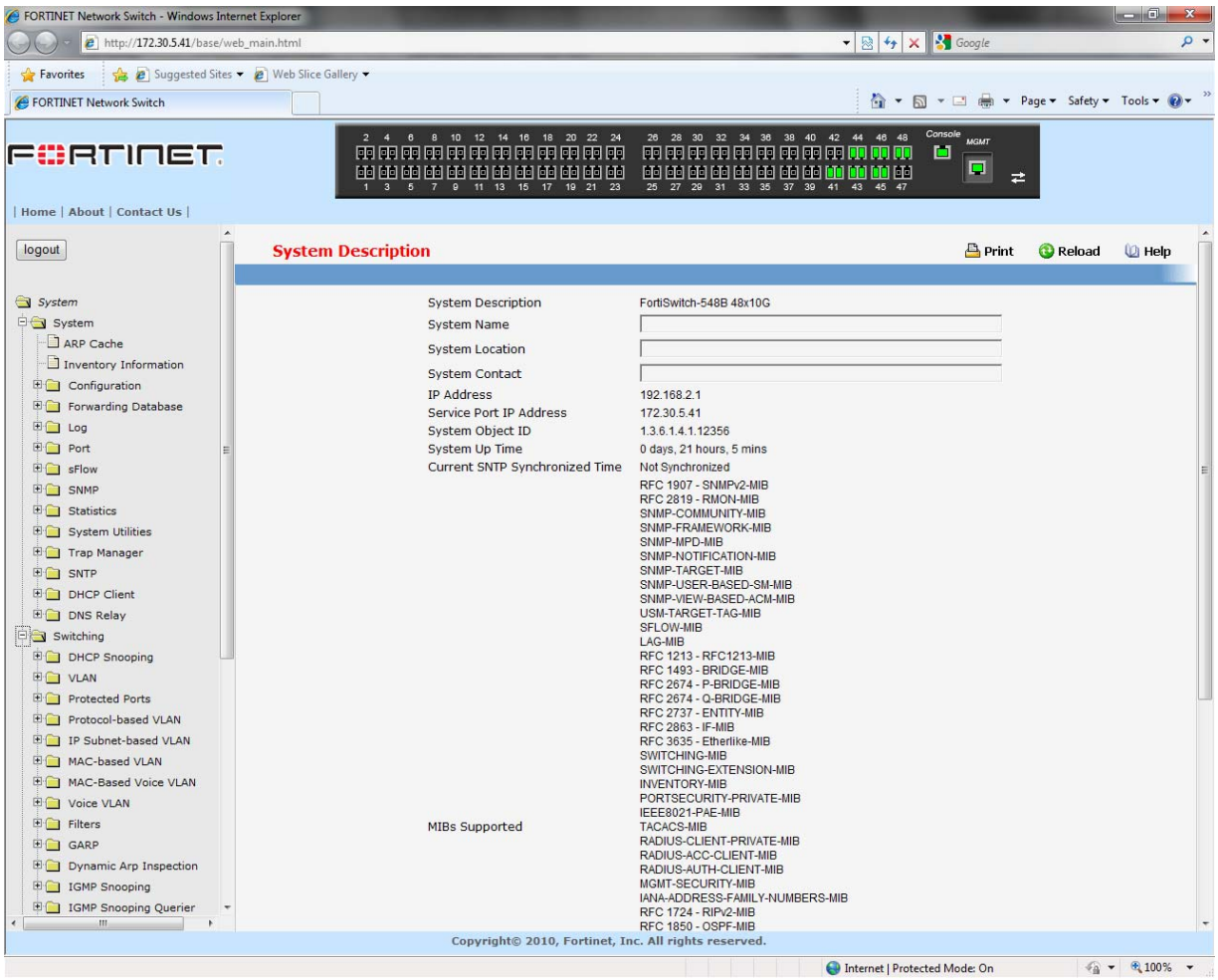
5.2 How to log in

The Fortinet FortiSwitch-548B Series Layer III plus QoS Managed Switch can be configured remotely from Microsoft Internet Explorer (version 5.0 or above), or Mozilla FireFox (version 3.6 or above).

1. Determine the IP address of your managed switch.
2. Open your Web browser.
3. Log in to the managed switch using the IP address the unit is currently configured with.
4. Type the default user name of **admin** and default of no password, or whatever password you have set up.

Once you have entered your access point name, your Web browser automatically finds the FortiSwitch-548B Series Layer III Managed Switch and display the home page, as shown below.

5.3 Web-Based Management Menu

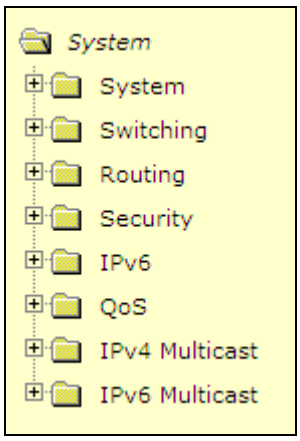


Menus

The Web-based interface enables navigation through several menus. The main navigation menu is on the left of every page and contains the screens that let you access all the commands and statistics the switch provides.

Main Menus

- System
- Switching
- Routing
- Security
- IPv6
- QoS
- IPv4 Multicast
- IPv6 Multicast



Secondary Menus

The Secondary Menus under the Main Menu contain a host of options that you can use to configure your switch. The online help contains a detailed description of the features on each screen. You can click the 'help' or the question mark at the top right of each screen to view the help menu topics.

The Secondary Menus are detailed below, with cross-references to the sections in this manual that contain the corresponding command descriptions.

System

- ARP Cache — see "show arp"
- Inventory — see "show hardware"
- Configuration — see "Management Commands and Device Configuration Commands"
- Forwarding Database — see "Device Configuration Commands' L2MAC Address"
- Logs — see "System Information and Statistics Commands"
- Port — see "Device Configuration Commands' Interface"
- sFlow — see "sFlow Commands"
- SNMP — see "SNMP Server Commands and SNMP Trap Commands"
- Statistics — see "show interface counters"
- System Utilities — see "System Utilities"
- Trap Manager — see "show traplog and SNMP Trap Commands"
- SNTP — see "SNTP Commands"
- DHCP Client — see "DHCP Client Commands"
- DNS Relay — see "Domain Name Server Relay Commands"

Switching

- DHCP Snooping — see "DHCP snooping Commands"
- VLAN — see "VLAN Management Commands"
- Portected Port — see "Portected Port Commands"
- Protocol-based VLAN — see "Protocol-based VLAN Commands"
- IP Subnet-based VLAN — see "IP Subnet-based VLAN Commands"

- MAC-based VLAN — see “MAC-based Commands”
- MAC-based Vocie VLAN — see “MAC-based Vocie VLAN Commands”
- Voice VLAN — see “Voice VLAN Commands”
- Filters — see “MAC Filters Commands”
- GARP — see “GVRP and Bridge Extension Commands”
- Dynamic Arp Inspection — see “DAI Commands”
- IGMP Snooping — see “IGMP Snooping Commands”
- IGMP Snooping Querier — see “IGMP Snooping Querier Commands”
- MLD Snooping — see “MLD Snooping Commands”
- MLD Snooping Querier — see “MLD Snooping Querier Commands”
- Port Channel — see “Port Channel Commands”
- Multicast Forwarding DataBase — see “L2 MAC Address and Multicast Forwarding Database Tables Commands”
- Spanning Tree — see “Spanning Tree Commands”
- Class of Service — see “L2 Priority Commands”
- Port Security — see “Port Security Configuration Commands”
- LLDP — see “LLDP Commands”
- VTP — see “VTP Commands”
- Link State — see “Link state Commands”
- Port Backup — see “Port backup Commands”
- FIP Snooping — see “FIP Snooping Commands”

Routing

- ARP — see “Address Resolution Protocol (ARP) Commands”
- IP — see “IP Routing Commands”
- OSPF — see “Open Shortest Path First (OSPF) Commands”
- BOOTP/DHCP Relay Agent — see “BOOTP/DHCP Relay Commands”
- RIP — see “Routing Information Protocol (RIP) Commands”
- Router Discovery — see “Router Discovery Protocol Commands”
- Router — see “IP Routing Commands”
- VLAN Routing — see “VLAN Routing Commands”
- VRRP — see “Virtual Router Redundancy Protocol (VRRP) Commands”
- Tunnels — see “Tunnels Commands”
- Loopbacks — see “Loopbacks Commands”

Security

- Port Access Control — see “Dot1x Configuration Commands”
- RADIUS — see “Radius Configuration Commands”
- TACACS+ — see “TACACS+ Configuration Commands”
- IP Filter — see “Network Commands”

- Secure HTTP — see “HTTP Commands”
- Secure Shell — see “Secure Shell (SSH) Commands”

IPv6

- OSPFv3 — see “OSPFv3 Configuration Commands”
- IPv6 Routes — see “IPv6 Routes Configuration Commands”
- RIPv6 — see “RIPv6 Configuration Commands”

QoS

- ACL — see “ACL Commands”
- Diffserv — see “Differentiated Services Commands”
- Class of Service see "Class of Service Commands"

IPv4 Multicast

- DVMRP — see “DVMRP Commands”
- IGMP — see “IGMP Commands”
- PIM-DM — see “PIM-DM Commands”
- PIM-SM — see “PIM-SM Commands”

IPv6 Multicast

- MLD — see “MLD Commands”
- PIM-DM — see “PIM-DM Commands”
- PIM-SM — see “PIM-SM Commands”

6. Command Line Interface Structure and Mode-based CLI

The Command Line Interface (CLI) syntax, conventions, and terminology are described in this section. Each CLI command is illustrated using the structure outlined below.

6.1 CLI Command Format

Commands are followed by values, parameters, or both.

Example 1

ip address <ipaddr> <netmask> [<gateway>]

- **ip address** 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.

Command

The text in bold, non-italic font must be typed exactly as shown.

6.2 CLI Mode-based Topology

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.

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, 0.0.0.0). The interface IP address of 0.0.0.0 is invalid.

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.

routerid The value of <router id> must be entered in 4-digit dotted-decimal notation (for example, 0.0.0.1). A router ID of 0.0.0.0 is invalid.

slot/port This parameter denotes a valid slot number, and a valid port number. For example, 0/1 represents unit number 1, 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.

Conventions

Network addresses are used to define a link to a remote host, workstation, or network. Network addresses are shown using the following syntax:

Table 5-1. Network Address Syntax

Address Type	Format	Range
IPAddr	A.B.C.D	0.0.0.0 to 255.255.255.255
MacAddr	YY:YY:YY:YY:YY:YY	hexidecimal digit pairs

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.

Empty strings (““) are not valid user defined strings. 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).

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.

The value of '-----' designates that the value is unknown.

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

7. Switching Commands

7.1 System Information and Statistics commands

7.1.1 show arp

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.

Syntax

show arp

Default Setting

None

Command Mode

Privileged Exec

Display Message

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: 00:23:45:67:89:AB

IP Address: The IP address assigned to each interface.

Interface: Valid slot number and a valid port number.

7.1.2 show calendar

This command displays the system time.

Syntax

show calendar

Default Setting

None

Command Mode

Privileged Exec

Display Message

Current Time displays system time

7.1.3 show process cpu

This command provides the percentage utilization of the CPU by different tasks.

Syntax

show process cpu

i It is not necessarily the traffic to the CPU, but different tasks that keep the CPU busy

Default Setting

None

Command Mode

Privileged Exec

Display Message

The following shows example CLI display output for the command.

Memory Utilization Report

status	bytes
free	192980480
alloc	53409968

Task Utilization Report

Task	Utilization
bcmL2X.0	0.75%
bcmCNTR.0	0.20%
bcmLINK.0	0.35%
DHCP snoop	0.10%
Dynamic ARP Inspection	0.10%
dot1s_timer_task	0.10%
dhcpsPingTask	0.20%

7.1.4 show eventlog

This command displays the event log, which contains error messages from the system, in the Primary Management System or in the specified unit. The event log is not cleared on a system reset.

Syntax

show eventlog [unit]

unit - The unit number of the remote system. The range is 1 to 8.

Default Setting

None

Command Mode

Privileged Exec

Display Message

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.

7.1.5 show running-config

This command is used to display/capture the current setting of different protocol packages supported on switch. This command displays/captures only commands with settings/configurations with values that differ from the default value. The output is displayed in script format, which can be used to configure another switch with the same configuration.

When a script name is provided, the output is redirected to a configuration script. The option [all] will also enable the display/capture of all commands with settings/configurations that include values that are same as the default values. If the optional <scriptname> is provided with a file name extension of ".scr", the output will be redirected to a script file.

Syntax

show running-config [all | <scriptname>]

all - enable the display/capture of all commands with settings/configurations that include values that are same as the default values.

<scriptname> - redirect the output to the file <scriptname>.

Default Setting

None

Command Mode

Privileged Exec

7.1.6 show sysinfo

This command displays switch brief information and MIBs supported.

Syntax
show sysinfo

Default Setting

None

Command Mode

Privileged Exec

Display Message

System Description: The text used to identify this switch.

System Name: The name used to identify the switch.

System Location: The text used to identify the location of the switch. May be up to 31 alpha-numeric characters. The factory default is blank.

System Contact: The text used to identify a contact person for this switch. May be up to 31 alphanumeric characters. The factory default is blank.

System Object ID: The manufacturing ID.

System Up Time: The time in days, hours and minutes since the last switch reboot.

Current SNTP Syncronized Time: The time which is synchronized from SNTP server.

MIBs Supported: A list of MIBs supported by this agent.

7.1.7 show system

This command displays switch system information.

Syntax
show system

Default Setting

None

Command Mode

Privileged Exec

Display Message

System Description: Text used to identify this switch.

System Object ID: The manufacturing ID

System Information

System Up Time: The time in days, hours and minutes since the last switch reboot.

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.

MAC Address: The burned in MAC address used for in-band connectivity.

Web Server: Displays to enable/disable web server function

Web Server Port: Displays the web server http port

Web Server 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.

Protocol Current: Indicates which network protocol is being used. The options are bootp | dhcp | none.

DHCP Client Identifier TEXT: DCHP client identifier for this switch.

7.1.8 show tech-support

This command displays system and configuration information when you contact technical support. The output of the show tech-support command combines the output of the following commands: **show version, show sysinfo, show port all, show logging, show event log, • show logging buffered, show trap log, show running config.**

Syntax
show tech-support

Default Setting

None

Command Mode

Privileged Exec

7.1.9 show hardware

This command displays inventory information for the switch.

Syntax
show hardware

Default Setting

None

Command Mode

Privileged Exec

Display Message

System 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.

Label Revision Number: The label revision serial number of this switch is used for manufacturing purposes.

Part Number: Manufacturing part number.

Hardware Version: The hardware version of this switch. It is divided into four parts. The first byte is the major version and the second byte represents the minor version.

Loader Version: The release version maintenance number of the loader 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'.

Boot Rom Version: The release version maintenance number of the boot ROM 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 Code 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'.

ADT7460_1: Now Temperature: The temperature of sensor of ADT7460 1.

ADT7460_2: Now Temperature: The temperature of sensor of ADT7460 2.

Depend on air flow FAN 1 – 4 connected ADT7460-1 or ADT7460-2:

Front-To-Back: (Connected ADT7460-1)

ADT7460_1: Fan 1 Status: Status of Fan1. It could be active or inactive.

ADT7460_1: Fan 2 Status: Status of Fan2. It could be active or inactive.

ADT7460_1: Fan 3 Status: Status of Fan3. It could be active or inactive.

ADT7460_1: Fan 4 Status: Status of Fan3. It could be active or inactive.

Back-To-Front: (Connected ADT7460-2)

ADT7460_2: Fan 1 Status: Status of Fan1. It could be active or inactive.

ADT7460_2: Fan 2 Status: Status of Fan2. It could be active or inactive.

ADT7460_2: Fan 3 Status: Status of Fan3. It could be active or inactive.

ADT7460_2: Fan 4 Status: Status of Fan3. It could be active or inactive.

Switch Power+ y…… Power Supply (The yth power supply information of switch 1).

Name: Name provided by Power Supply vendor.

Model: Model Number provided by Power Supply vendor.

Revision Number: Revision Number provided by Power Supply vendor.

Manufacturer Location: Location provided by Power Supply vendor.

Date of Manufacturing: Date of Manufacturing provided by Power Supply vendor.

Serial Numbe: Serial Number provided by Power Supply vendor.

Temperature 1:. Inner temperature 1 of Power Supply now

Temperature 2: Inner temperature 2 of Power Supply now

Fan Speed: Inner fan speed(rpm) of Power Supply now

Fan Duty: Inner fan duty(%) of Power Supply now

Below 10-Giga Interface information depend on plugging SFP+ Transceiver

Interface = y..... SFP+(The yth 10-Giga information of switch 1).

10 Gigabit Ethernet Compliance Codes: Transceiver's compliance codes.

Vendor Name: The SFP transceiver vendor name shall be the full name of the corporation, a commonly accepted abbreviation of the name of the corporation, the SCSI company code for the corporation, or the stock exchange code for the corporation.

Vendor Part Number: Part number provided by SFP transceiver vendor.

Vendor Serial Number: Serial number provided by vendor.

Vendor Revision Number: Revision level for part number provided by vendor.

Vendor Manufacturing Date: The vendor's manufacturing date.

Additional Packages: This displays the additional packages that are incorporated into this system.

7.1.10 show version

This command displays inventory information for the switch.

Syntax
show version

Default Setting

None

Command Mode

Privileged Exec

Display Message

Serial Number: The unique box serial number for this switch.

Hardware Version: The hardware version of this switch. It is divided into four parts. The first byte is the major version and the second byte represents the minor version.

Number of ports: Total number of port for this swirch system.

Label Revision Number: The label revision serial number of this switch is used for manufacturing purposes.

Part Number: Manufacturing part number.

Machine Model: Specifies the machine model as defined by the Vital Product Data.

Loader Version: The release version maintenance number of the loader 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 Code 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'.

Boot Rom Version: The release version maintenance number of the boot ROM 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'.

7.1.11 show loginsession

This command displays current telnet and serial port connections to the switch.

Syntax
show loginsession

Default Setting

None

Command Mode

Privileged Exec

Display Message

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.

Session Type: Shows the type of session: telnet, serial or SSH.

7.1.12 show command filter

This command displays the information that begin/include/exclude the regular expression.

Syntax
show command [| begin/include/exclude <LINE>]

Default Setting

None

Command Mode

Privileged Exec

Display Message

command: Any show command of the CLI

begin: Begin with the line that matches

include: Include lines that match

exclude: Exclude lines that match

<LINE>: Regular Expression

7.2 Device Configuration Commands

7.2.1 Interface

7.2.1.1 show interface status

This command displays the Port monitoring information for the system.

Syntax
show interface status {<slot/port> | all}

<slot/port> - is the desired interface number.

all - This parameter displays information for all interfaces.

Default Setting

None

Command Mode

Privileged Exec

Display Message

Intf: 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:

Source: This port is a monitoring port.

PC Mbr: This port is a member of a port-channel (LAG).

Dest: 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. It 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 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.

Flow Control Mode: Displays flow control mode. The possible values are:

None: This port is disabled flow control.

802.3X: This port is enabled flow control.

PFC: This port is enable Priority Flow control.

Capabilities Status: Displays interface capabilities.

7.2.1.2 show interface counters

This command displays a summary of statistics for a specific interface or all interfaces.

Syntax
show interface counters {<slot/port> | all}

<slot/port> - is the desired interface number.

all - This command displays statistics information for all interfaces.

Default Setting

None

Command Mode

Privileged Exec

Display Message

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 'all' are as follows:

Interface: The physical slot and physical port or the logical slot and logical port.

Summary: The summation of the statistics of all ports.

Packets Received Without Error: The total number of packets (including broadcast packets and multicast packets) received.

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.

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.

This command displays detailed statistics for a specific port or for all CPU traffic based upon the argument.

Syntax

show interface counters detailed {<slot/port> | switchport}

<slot/port> - is the desired interface number.

switchport - This parameter specifies whole switch or all interfaces.

Default Setting

None

Command Mode

Privileged Exec

Display Message

The display parameters when the argument is ' <slot/port>' are as follows:

Total Packets Received (Octets): 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 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 > 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 RX and TX 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 RX and TX 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 RX and TX 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 RX and TX 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 RX and TX 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 RX and TX 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 RX and TX 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 RX and TX 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 RX and TX 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 RX and TX 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).

Total Packets Received 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

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 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.

Undersize Received: The total number of packets received that were less than 64 octets in length with GOOD CRC(excluding framing bits but including FCS octets).

Fragments Received: The total number of packets received that were less than 64 octets in length with ERROR CRC(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 FCS with a non-integral number of octets.

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 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 Packets Transmitted (Octets)

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.

Total Packets Transmitted Successfully

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

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 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 Transmited Packets Discards

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.

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 and Registrations: The number of times attempted GVRP registrations could not be completed.

GMRP PDUs received: The count of GMRP PDUs received in the GARP layer.

GMRP PDUs Transmitted: The count of GMRP PDUs 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.

RSTP 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.

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:

Total Packets Received (Octets): The total number of octets of data received by the processor (excluding framing bits but including FCS octets).

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 Currently 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.

7.2.1.3 show interface switch

This command displays a summary of statistics for all CPU traffic.

Syntax
show interface switch

Default Setting

None

Command Mode

Privileged Exec

Display Message

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.

7.2.1.4 interface

This command is used to enter Interface configuration mode.

Syntax

```
interface <slot/port>
```

<slot/port> - is the desired interface number.

Default Setting

None

Command Mode

Global Config

7.2.1.5 speed-duplex

This command is used to set the speed and duplex mode for the interface.

The 10-Giga interfaces will not provide the following command. Instead, it provides a command to set the speed of 10-Giga port to 1Gbps. Use ‘speed-duplex 1000’ to change the speed of 10-Giga port to 1G speed.

Syntax

```
speed-duplex 1000
no speed-duplex 1000
```

1000 – 1000 Mbps, only valid for 10G ports.

no - This command will be back to 10G speed from 1G speed on a port.

Default Setting

None

Command Mode

Interface Config

This command is used to set the speed and duplex mode for all interfaces.

Syntax

```
speed-duplex all 1000
no speed-duplex all 1000
```

1000 – 1000 Mbps, only valid for 10G ports.

all - This command represents all interfaces.

no - This command will be back to 10G speed from 1G speed for all ports.

Default Setting

None

Command Mode

Global Config

7.2.1.6 negotiate

This command enables automatic negotiation on a port. The default value is enabled.

The 10-Giga interfaces will not provide the following command.

Syntax

```
negotiate
no negotiate
```

no - This command disables automatic negotiation on a port.

Default Setting

Enable

Command Mode

Interface Config

This command enables automatic negotiation on all interfaces. The default value is enabled.

Syntax

```
negotiate all
no negotiate all
```

all - This command represents all interfaces.

no - This command disables automatic negotiation on all interfaces.

Default Setting

Enable

Command Mode

Global Config

7.2.1.7 capabilities

This command is used to set the capabilities on specific interface.

The 10-Giga interfaces will not provide the following command.

Syntax

```
capabilities {{10 | 100 } {full-duplex | half-duplex}} | {1000 full-duplex }
no capabilities {{10 | 100 } {full-duplex | half-duplex}} | {1000 full-duplex }
```

10 - 10BASE-T

100 - 100BASE-T

1000 - 1000BASE-T

full-duplex - Full duplex

half-duplex - Half duplex

no - This command removes the advertised capability with using parameter.

Default Setting

10 half-duplex, 10 full-duplex, 100 half-duplex, 100 full-duplex, and 1000 full-duplex

Command Mode

Interface Config

This command is used to set the capabilities on all interfaces.

Syntax

```
capabilities all {{10 | 100} {full-duplex | half-duplex}} | {1000 full-duplex }
no capabilities all {{10 | 100} {full-duplex | half-duplex}} | {1000 full-duplex }
```

10 - 10BASE-T

100 - 100BASE-T

1000 - 1000BASE-T

full-duplex - Full duplex

half-duplex - Half duplex

all - This command represents all interfaces.

no - This command removes the advertised capability with using parameter

Default Setting

10 half-duplex, 10 full-duplex, 100 half-duplex, 100 full-duplex, and 1000 full-duplex

Command Mode

Global Config

7.2.1.8 storm-control flowcontrol

This command enables 802.3x flow control for the switch.

802.3x flow control only applies to full-duplex mode ports.

Syntax

storm-control flowcontrol
no storm-control flowcontrol

no - This command disables 802.3x flow control for the switch.

Default Setting

Disabled

Command Mode

Global Config

This command enables 802.3x flow control for the specific interface.

802.3x flow control only applies to full-duplex mode ports.

Syntax

storm-control flowcontrol
no storm-control flowcontrol

no - This command disables 802.3x flow control for the specific interface.

Default Setting

Disabled

Command Mode

Interface Config

7.2.1.9 storm-control flowcontrol pfc

The PFC function is disabled by default. Only after enabling it, the PFC process also starts. Once the feature is enabled, the original basic IEEE 802.3x PAUSE control cannot be enabled. It means these two features cannot be enabled at the same time.

i 802.3x flow control only applies to full-duplex mode ports.

Syntax

storm-control flowcontrol pfc
no storm-control flowcontrol pfc

no - This command disables Priority Flow Control for the specific interface.

Default Setting

Disabled

Command Mode

Interface Config

7.2.1.10 shutdown

This command is used to disable a port.

Syntax

shutdown
no shutdown

no - This command enables a port.

Default Setting

Enabled

Command Mode

Interface Config

This command is used to disable all ports.

Syntax

shutdown all
no shutdown all

all - This command represents all ports.

no - This command enables all ports.

Default Setting

Enabled

Command Mode

Global Config

7.2.1.11 description

This command is used to create an alpha-numeric description of the port.

Syntax

```
description <description>
no description
```

no - This command removes the description of the port.

Default Setting

None

Command Mode

Interface Config

7.2.1.12 mdi

i The 10-Giga interface will not provide the following command.

This command is used to configure the physical port MDI/MDIX state.

Syntax

```
mdi {auto|across|normal}
no mdi
```

auto - This type is auto selecting cable type.

across - This type is only allowed the Across-over cable.

normal - This type is only allowed the Normal cable.

no - This command restore the port mode to Auto.

Default Setting

Auto

Command Mode

Interface Config

7.2.2 L2 MAC Address and Multicast Forwarding Database Tables

7.2.2.1 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.

Syntax
show mac-addr-table [{<macaddr> <vlanid> |all}]

<macaddr> - enter a MAC Address to display the table entry for the requested MAC address.

<vlanid> - VLAN ID (Range: 1 – 3965)

all – this command displays the entire table.

Default Setting

None

Command Mode

Privileged Exec

Display Message

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. In an SVL system, the MAC address will be displayed as 6 bytes. **Note: This software version only supports IVL systems.**

Interface: The port on which this L2 MAC address was learned.

if Index: This object indicates the if Index 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 3/1 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 instance was learned via GMRP and applies to Multicast.

Other: The value of the corresponding instance does not fall into one of the other categories.

7.2.2.2 show mac-addr-table count

This command displays the total forwarding database entries, the number of static and learnning mac address, and the max address available on the switch.

Syntax

show mac-addr-table count

Default Setting

None

Command Mode

Privileged Exec

Display Message

Dynamic Address count: The total learning mac addresses on the L2 MAC address Table.

Static Address (User-defined) count: The total user-defined addresses on the L2 MAC address Table.

Total MAC Addresses in use: This number of addresses are used on the L2 MAC address table.

Total MAC Addresses available: The switch supports max value on the L2 MAC address table.

7.2.2.3 show mac-addr-table interface

This command displays the forwarding database entries. The user can search FDB table by using interface number <slot/port>.

Syntax

show mac-addr-table interface <slot/port>

<slot/port> - Interface number.

Default Setting

None

Command Mode

Privileged Exec

Display Message

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. In an SVL system, the MAC address will be displayed as 6 bytes. **Note: This software version only supports IVL systems.**

VLAN ID: The vlan id of that mac address.

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 3/1 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 instance was learned via GMRP and applies to Multicast.

Other: The value of the corresponding instance does not fall into one of the other categories.

7.2.2.4 show mac-addr-table vlan

This command displays the forwarding database entries. The user can search FDB table by using vlan id.

Syntax

show mac-addr-table vlan <vlanid>

<vlanid> - VLAN ID (Range: 1 – 3965)

Default Setting

None

Command Mode

Privileged Exec

Display Message

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. In an SVL system, the MAC address will be displayed as 6 bytes. **Note: This software version only supports IVL systems.**

Interface: The port on which this L2 MAC address was learned.

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 3/1 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 instance was learned via GMRP and applies to Multicast.

Other: The value of the corresponding instance does not fall into one of the other categories.

7.2.2.5 show mac-address-table gmrp

This command displays the GARP Multicast Registration Protocol (GMRP) entries in the Multicast Forwarding Database (MFDB) table.

Syntax

show mac-address-table gmrp

Default Setting

None

Command Mode

Privileged Exec

Display Message

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 is 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:).

7.2.2.6 show mac-address-table igmpsnooping

This command displays the IGMP Snooping entries in the Multicast Forwarding Database (MFDB) table.

Syntax

show mac-address-table igmpsnooping

Default Setting

None

Command Mode

Privileged Exec

Display Message

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. In an SVL system, the MAC address will be displayed as 6 bytes. **Note: This software version only supports IVL systems.**

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:).

7.2.2.7 show mac-address-table multicast

This command displays the MFDB information. If the command is entered with no parameter, the entire table is displayed. This is the same as entering the *all* parameter. The user can display the table entry for one MAC Address by specifying the MAC address as an optional parameter.

Syntax
show mac-address-table multicast {<macaddr> <vlanid> | all }

<macaddr> - enter a MAC Address to display the table entry for the requested MAC address

<vlanid> - VLAN ID (Range: 1 – 3965)

all – This command displays the entire table.

Default Setting

None

Command Mode

Privileged Exec

Display Message

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. In an SVL system, the MAC address will be displayed as 6 bytes. **Note: This software version only supports IVL systems.**

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.

Source: 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.

7.2.2.8 show mac-address-table stats

This command displays the MFDB statistics.

Syntax

```
show mac-address-table stats
```

Default Setting

None

Command Mode

Privileged Exec

Display Message

Max MFDB Table Entries: This displays the total number of entries that can possibly be in the MFDB.

Most MFDB Entries Since Last Reset: 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.

7.2.2.9 show mac-addr-table agetime

This command displays the forwarding database address aging timeout.

Syntax

```
show mac-addr-table agetime
```

Default Setting

None

Command Mode

Privileged Exec

Display Message

Address Aging Timout: This displays the total number of seconds for Forwarding Database table.

7.2.2.10 mac-address-table aging-time

This command configures the forwarding database address aging timeout in seconds.

Syntax

```
mac-addr-table aging-time <10-1000000>
no mac-addr-table aging-time
```

<10-1000000> - aging-time (Range: 10-1000000) in seconds

no - This command sets the forwarding database address aging timeout to 300 seconds.

Default Setting

300

Command Mode

Global Config

7.2.3 VLAN Management

7.2.3.1 show vlan

This command displays brief information on a list of all configured VLANs.

Syntax

```
show vlan
```

Default Setting

None

Command Mode

Privileged Exec

Display Message

VLAN ID: There is a VLAN Identifier (vlanid) associated with each VLAN. The range of the VLAN ID is 1 to 3965.

VLAN Name: A string associated with this VLAN as a convenience. It can be up to 16 alphanumeric characters, including blanks. The default is blank. VLAN ID 1 is always named `Default`. This field is optional.

VLAN Type: Type of VLAN, which can be Default, (VLAN ID = 1), can be static (one that is configured and permanently defined), or Dynamic (one that is created by GVRP registration).

Interface(s): Indicates by slot id and port number which port belongs to this VLAN.

7.2.3.2 show vlan id

This command displays detailed information, including interface information, for a specific VLAN.

Syntax

```
show vlan {id <vlanid> | name <vlanname>}
```

<vlanid> - VLAN ID (Range: 1 – 3965)

<vlanname> - vlan name (up to 16 alphanumeric characters)

Default Setting

None

Command Mode

Privileged Exec

Display Message

VLAN ID: There is a VLAN Identifier (VID) associated with each VLAN. The range of the VLAN ID is 1 to 3965.

VLAN Name: A string associated with this VLAN as a convenience. It can be up to 16 alphanumeric characters, including blanks. The default is blank. VLAN ID 1 is always named `Default`. This field is optional.

VLAN Type: Type of VLAN, which can be Default, (VLAN ID = 1), can be static (one that is configured and permanently defined), or Dynamic (one that is created by GVRP registration).

Interface: 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.

7.2.3.3 show vlan association mac

This command displays the VLAN associated with a specific configured MAC address. If no MAC address is specified, the VLAN associations of all the configured MAC addresses are displayed.

Syntax

show vlan association mac [<macaddr>]

<macaddr> - enter a MAC Address to display the table entry for the requested MAC address.

Default Setting

None

Command Mode

Privileged Exec

Display Message

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. In an SVL system, the MAC address will be displayed as 6 bytes. **Note: This software version only supports IVL systems.**

VLAN ID: There is a VLAN Identifier (VID) associated with each VLAN. The range of the VLAN ID is 1 to 3965.

7.2.3.4 show vlan association subnet

This command displays the VLAN associated with a specific configured IP-Address and net mask. If no IP Address and net mask are specified, the VLAN associations of all the configured IP-subnets are displayed.

Syntax

```
show vlan association subnet [<ipaddr> <netmask>]
```

<ipaddr> - The IP address.

<netmask> - The subnet mask.

Default Setting

None

Command Mode

Privileged Exec

Display Message

IP Subnet: The IP address assigned to each interface

IP Mask: The subnet mask.

VLAN ID: There is a VLAN Identifier (VID) associated with each VLAN. The range of the VLAN ID is 1 to 3965.

7.2.3.5 show protocol group

This command displays the Protocol-Based VLAN information for either the entire system, or for the indicated Group.

Syntax

```
show protocol group {<group-name> | all}
```

<group-name> - The group name of an entry in the Protocol-based VLAN table.

all – Displays the entire table.

Default Setting

None

Command Mode

Privileged Exec

Display Message

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.

7.2.3.6 show interface switchport

This command displays VLAN port information.

Syntax

show interface switchport {<slot/port> | all}

<slot/port> - Interface number.

all – Display the entire table.

Default Setting

None

Command Mode

Privileged Exec

Display Message

Interface: 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 untagged packets arriving on the port.

7.2.3.7 vlan database

This command is used to enter VLAN Interface configuration mode

Syntax

```
vlan database
```

Default Setting

None

Command Mode

Global Config

7.2.3.8 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 2-3965.

Syntax

```
vlan <vlan-list>
no vlan <vlan-list>
```

<vlan-list> - VLAN ID (Range: 2 –3965) – separate non-consecutive IDs with ',' and no spaces and no zeros in between the range; Use '-' for range.

no - 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 2-3965.

Default Setting

None

Command Mode

VLAN database

7.2.3.9 vlan name

This command changes the name of a VLAN. The name is an alphanumeric string of up to 32 characters, and the ID is a valid VLAN identification number. ID range is 1- 3965.

Syntax

```
vlan name <vlanid> <newname>
no vlan name <vlanid>
```

<vlanid> - VLAN ID (Range: 1 –3965).

<newname> - Configure a new VLAN Name (up to 16 alphanumeric characters).

no - This command sets the name of a VLAN to a blank string. The VLAN ID is a valid VLAN identification number. ID range is 1-3965.

Default Setting

The name for VLAN ID 1 is always Default. The name for other VLANs is defaulted to a blank string.

Command Mode

VLAN database

7.2.3.10 vlan association mac

This command associates a MAC address to a VLAN.

Syntax

```
vlan association mac <macaddr> <vlanid>
no vlan association mac <macaddr>
```

<macaddr> - enter a MAC Address to display the table entry for the requested MAC address.

<vlandid> - VLAN identification number. ID range is 1-3965.

no - This command removes the association of a MAC address to a VLAN.

Default Setting

None

Command Mode

VLAN database

7.2.3.11 vlan association subnet

This command removes the association of a MAC address to a VLAN.

Syntax

```
vlan association subnet <ipaddr> <netmask> <vlanid>
no vlan association subnet <ipaddr> <netmask>
```

<ipaddr> - The IP address.

<netmask> - The subnet mask.

<vlandid> - VLAN identification number. ID range is 1-3965.

no - This command removes association of a specific IP-subnet to a VLAN.

Default Setting

None

Command Mode

VLAN database

7.2.3.12 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 2-3965.

Syntax

vlan makestatic <vlanid>

<vlanid> - VLAN ID (Range: 2 –3965).

Default Setting

None

Command Mode

VLAN database

7.2.3.13 protocol group

This command attaches a <vlanid> to the protocol-based VLAN identified by <group-name>. A group may only be associated with one VLAN at a time, however the VLAN association can be changed.

Syntax

protocol group <group-name> <vlanid>
no protocol group <group-name> <vlanid>

<vlanid> - VLAN ID (Range: 1 –3965).

<group-name> - a VLAN Group Name (a character string of 1 to 16 characters).

no - This command removes the <vlanid> from this protocol-based VLAN group that is identified by this <group-name>.

Default Setting

None

Command Mode

VLAN database

7.2.3.14 switchport acceptable-frame-type

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.

Syntax

```
switchport acceptable-frame-type {tagged | all}
no switchport acceptable-frame-type {tagged | all}
```

tagged - VLAN only mode.

all - Admit all mode.

no - 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.

Default Setting

Admit all

Command Mode

Interface Config

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.

Syntax

```
switchport acceptable-frame-type all {tagged | all}
no switchport acceptable-frame-type all {tagged | all}
```

tagged - VLAN only mode.

all – One is for Admit all mode. The other one is for all interfaces.

no - 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.

Default Setting

Admit all

Command Mode

Global Config

7.2.3.15 switchport ingress-filtering

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.

Syntax

switchport ingress-filtering
no switchport ingress-filtering

no - 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.

Default Setting

Disabled

Command Mode

Interface Config

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.

Syntax

switchport ingress-filtering all
no switchport ingress-filtering all

all - All interfaces.

no - 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.

Default Setting

Disabled

Command Mode

Global Config

7.2.3.16 switchport native vlan

This command changes the VLAN ID per interface.

Syntax

switchport native vlan <vlanid>
no switchport native vlan <vlanid>

<vlanid> - VLAN ID (Range: 1 –3965).

no - This command sets the VLAN ID per interface to 1.

Default Setting

1

Command Mode

Interface Config

This command changes the VLAN ID for all interfaces.

Syntax

switchport native vlan all <vlanid>

<vlanid> - VLAN ID (Range: 1 –3965).

all - All interfaces.

no - This command sets the VLAN ID for all interfaces to 1.

Default Setting

1

Command Mode

Global Config

7.2.3.17 switchport allowed vlan

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**.**

Syntax

switchport allowed vlan {add [tagged | untagged] | remove} <vlan-list>

<vlan-list> - VLAN ID (Range: 1 –3965) – separate non-consecutive IDs with ',' and no spaces and no zeros in between the range; Use '-' for range.

add - The interface is always a member of this VLAN. This is equivalent to registration fixed.

tagged - All frames transmitted for this VLAN will be tagged.

untagged - All frames transmitted for this VLAN will be untagged.

remove - The interface is removed from the member of this VLAN. This is equivalent to registration forbidden.

Default Setting

None

Command Mode

Interface Config

This command configures the degree of participation for all interfaces in a VLAN. The ID is a valid VLAN identification number**.**

Syntax
switchport allowed vlan {add {tagged | untagged} | remove} all <vlanid>

<vlanid> - VLAN ID (Range: 1 –3965).

all - All interfaces.

add - The interface is always a member of this VLAN. This is equivalent to registration fixed.

tagged - all frames transmitted for this VLAN will be tagged.

untagged - all frames transmitted for this VLAN will be untagged.

remove - The interface is removed from the member of this VLAN. This is equivalent to registration forbidden.

Default Setting

None

Command Mode

Global Config

7.2.3.18 switchport tagging

This command configures the tagging behavior for a specific interface in a VLAN to enable. 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.

Syntax

```
switchport tagging <vlan-list>
no switchport tagging <vlan-list>
```

<vlan-list> - VLAN ID (Range: 1 –3965) – separate non-consecutive IDs with ',' and no spaces and no zeros in between the range; Use '-' for range.

no - 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.

Default Setting

Disabled

Command Mode

Interface Config

This command configures the tagging behavior for all interfaces in a VLAN to be 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.

Syntax

```
switchport tagging all <vlanid>
```

<vlanid> - VLAN ID (Range: 1 –3965).

all - All interfaces

no - 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.

Default Setting

Disabled

Command Mode

Global Config

7.2.3.19 switchport forbidden vlan

This command used to configure forbidden VLANs.

Syntax

```
switchport forbidden vlan {add | remove}   <vlan-list>
no switchport forbidden
```

<vlan-list> - VLAN ID (Range: 1 –3965) – separate non-consecutive IDs with ',' and no spaces and no zeros in between the range; Use '-' for range.

add - VLAND ID to add.

remove - VLAND ID to remove.

no - Remove the list of forbidden VLANs.

Default Setting

None

Command Mode

Interface Config

7.2.3.20 switchport priority

This command configures the default 802.1p port priority assigned for untagged packets for a specific interface.

Syntax

```
switchport priority <0-7>
```

<0-7> - The range for the priority is 0 - 7.

Default Setting

0

Command Mode

Interface Config

This command configures the port priority assigned for untagged packets for all ports presently plugged into the device. Any subsequent per port configuration will override this configuration setting.

Syntax

```
switchport priority all <0-7>
```

<0-7> - The range for the priority is 0-7.

all – All interfaces

Default Setting

0

Command Mode

Global Config

7.2.3.21 switchport protocol group

This command adds the physical <slot/port> interface to the protocol-based VLAN identified by <*group-name*>. 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.

Syntax

```
switchport protocol group <group-name>
no switchport protocol group <group-name>
```

<group-name> - a VLAN Group Name (a character string of 1 to 16 characters).

no - This command removes the *interface* from this protocol-based VLAN group that is identified by this <*group-name*>.

Default Setting

None

Command Mode

Interface Config

This command adds a protocol-based VLAN group to the system. The <*group-name*> 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.

Syntax

```
switchport protocol group <group-name>
no switchport protocol group <group-name>
```

<group-name> - a VLAN Group Name (a character string of 1 to 16 characters).

no - This command removes the protocol-based VLAN group that is identified by this <group-name>.

Default Setting

None

Command Mode

Global Config

This command adds all physical interfaces to the protocol-based VLAN identified by <*group-name*>. 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.

Syntax

```
switchport protocol group all <group-name>
no switchport protocol group all <group-name>
```

<group-name> - a VLAN Group Name (a character string of 1 to 16 characters).

all - All interfaces.

no - This command removes all interfaces from this protocol-based VLAN group that is identified by this <group-name>.

Default Setting

None

Command Mode

Global Config

This command adds the <protocol> to the protocol-based VLAN identified by <group-name>. 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*.

Syntax

```
switchport protocol group add protocol <group-name> {ip | arp | ipx}
no switchport protocol group add protocol <group-name> {ip | arp | ipx}
```

<group-name> - a VLAN Group Name (a character string of 1 to 16 characters).

ip - IP protocol.

arp - ARP protocol.

ipx - IPX protocol.

no - This command removes the <*protocol*> from this protocol-based VLAN group that is identified by this <*group-name*>. The possible values for protocol are *ip, arp,* and *ipx*.

Default Setting

None

Command Mode

Global Config

7.2.4 Double VLAN commands

7.2.4.1 show dvlan-tunnel/ dot1q-tunnel

This command is used without the optional parameters to display all interfaces enabled for Double VLAN Tunneling. Use the optional parameters to display detailed information about Double VLAN Tunneling for the specified interface or all interfaces.

Syntax

show {dot1q-tunnel|dvlan-tunnel} [interface {<slot/port>|all}]

Default Setting

None

Command Mode

Privileged Exec

Display Message

Interfaces Enabled for DVLAN Tunneling: Valid interface(s) support(s) DVLAN Tunneling.

When using 'show {dot1q-tunnel|dvlan-tunnel} interface':

Interface: Valid slot and port number separated by forward slashes.

Mode: This field specifies the administrative mode through which Double VLAN Tunneling can be enabled or disabled. The default value for this field is disabled.

EtherType This field represents a 2-byte hex EtherType to be used as the first 16 bits of the DVLAN tunnel. There are three different EtherType tags. The first is 802.1Q, which represents the commonly used value of 0x8100. The second is vMAN, which represents the commonly used value of 0x88A8. If EtherType is not one of these two values, then it is a custom tunnel value, representingany value in the range of 0 to 65535.

7.2.4.2 switchport dvlan-tunnel/ dot1q-tunnel ethertype

This command configures the ether-type for specific interface. The ether-type may have the values of *802.1Q*, *vMAN*, or *custom*. If the ether-type has a value of *custom*, the optional value of the custom ether type must be set to a value from 0 to 65535.

Syntax

switchport {dvlan-tunnel | dot1q-tunnel } ethertype {802.1Q|custom <0-65535>|vman}

Default Setting

Vman

Command Mode

Interface Config

7.2.4.3 switchport dvlan-tunnel/ dot1q-tunnel

This command is used to enable Double VLAN Tunneling on the specified interface.

Syntax
switchport {dvlan-tunnel|dot1q-tunnel} no switchport {dvlan-tunnel|dot1q-tunnel}

Default Setting

Disable

Command Mode

Interface Config

7.2.5 GVRP and Bridge Extension

7.2.5.1 show bridge-ext

This command displays Generic Attributes Registration Protocol (GARP) information.

Syntax
show bridge-ext

Default Setting

None

Command Mode

Privileged Exec

User Exec

Display Message

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.

7.2.5.2 show gvrp configuration

This command displays Generic Attributes Registration Protocol (GARP) information for one or all interfaces.

Syntax

show gvrp configuration {<slot/port> | all}

<slot/port> - An interface number.

all - All interfaces.

Default Setting

None

Command Mode

Privileged Exec

User Exec

Display Message

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 LeaveAll- Time 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 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.

7.2.5.3 show gmrp configuration

This command displays Generic Attributes Registration Protocol (GARP) information for one or All interfaces.

Syntax

show gmrp configuration {<slot/port> | all}

<slot/port> - An interface number.

all - All interfaces.

Default Setting

None

Command Mode

Privileged Exec

User Exec

Display Message

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 LeaveAll- Time 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.

7.2.5.4 show garp configuration

This command displays GMRP and GVRP configuration information for one or all interfaces.

Syntax

```
show garp configuration {<slot/port> | all}
```

<slot/port> - An interface number.

all - All interfaces.

Default Setting

None

Command Mode

Privileged Exec

User Exec

Display Message

Interface: This displays the slot/port of the interface that this row in the table describes.

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.

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.

7.2.5.5 bridge-ext gvrp

This command enables GVRP.

Syntax

```
bridge-ext gvrp
no bridge-ext gvrp
```

no - This command disables GVRP.

Default Setting

Disabled

Command Mode

Global Config

7.2.5.6 bridge-ext gmrp

This command enables GARP Multicast Registration Protocol (GMRP) on the system. The default value is disabled.

Syntax

```
bridge-ext gmrp
no bridge-ext gmrp
```

no - This command disables GARP Multicast Registration Protocol (GMRP) on the system.

Default Setting

Disabled

Command Mode

Global Config

7.2.5.7 switchport gvrp

This command enables GVRP (GARP VLAN Registration Protocol) for a specific port.

Syntax

```
switchport gvrp
no switchport gvrp
```

no - 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.

Default Setting

Disabled

Command Mode

Interface Config

This command enables GVRP (GARP VLAN Registration Protocol) for all ports.

Syntax

```
switchport gvrp all
no switchport gvrp all
```

all - All interfaces.

no - 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.

Default Setting

Disabled

Command Mode

Global Config

7.2.5.8 switchport gmrp

This command enables GMRP Multicast Registration Protocol on a selected interface. If an interface which has GMRP enabled is enabled for routing or is enlisted as a member of a port-channel (LAG), GMRP functionality will be disabled on that interface. GMRP functionality will subsequently be re-enabled if routing is disabled or port-channel (LAG) membership is removed from an interface that has GMRP enabled.

Syntax

```
switchport gmrp
no switchport gmrp
```

no - This command disables GMRP Multicast Registration Protocol on a selected interface. If an interface which has GMRP enabled is enabled for routing or is enlisted as a member of a port-channel (LAG), GMRP functionality will be disabled on that interface. GMRP functionality will subsequently be re-enabled if routing is disabled or port-channel (LAG) membership is removed from an interface that has GMRP enabled.

Default Setting

Disabled

Command Mode

Interface Config

This command enables GMRP Multicast Registration Protocol on all interfaces. If an interface which has GMRP enabled is enabled for routing or is enlisted as a member of a port-channel (LAG), GMRP functionality will be disabled on that interface. GMRP functionality will subsequently be re-enabled if routing is disabled and port-channel (LAG) membership is removed from an interface that has GMRP enabled.

Syntax

```
switchport gmrp all
no switchport gmrp all
```

all - All interfaces.

no - This command disables GMRP Multicast Registration Protocol on a selected interface.

Default Setting

Disabled

Command Mode

Global Config

7.2.5.9 garp timer

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 and GMRP are enabled. The time is from 10 to 100 (centiseconds).

Syntax

```
garp timer join <10-100>
no garp timer join
```

<10-100> - join time (Range: 10 – 100) in centiseconds.

no - 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 and GMRP are enabled.

Default Setting

20 centiseconds (0.2 seconds)

Command Mode

Interface Config

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 and GMRP are enabled. The time is from 10 to 100 (centiseconds).

Syntax

```
garp timer join all < 10-100 >
no garp timer join all
```

<10-100> - join time (Range: 10 – 100) in centiseconds.

all - All interfaces.

no - 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 and GMRP are enabled.

Default Setting

20 centiseconds (0.2 seconds)

Command Mode

Global Config

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. The time is from 20 to 600 (centiseconds).

This command has an effect only when GVRP and GMRP are enabled.

Syntax

```
garp timer leave < 20-600 >
no garp timer leave
```

<20-600> - leave time (Range: 20 – 600) in centiseconds.

no - This command sets the GVRP leave time per port to 60 centiseconds (0.6 seconds).

Default Setting

60 centiseconds (0.6 seconds)

Command Mode

Interface Config

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. The time is from 20 to 600 (centiseconds).

This command has an effect only when GVRP and GMRP are enabled.

Syntax

```
garp timer leave all < 20-600 >
no garp timer leave all
```

<20-600> - leave time (Range: 20 – 600) in centiseconds.

all - All interfaces.

no - This command sets the GVRP leave time for all ports to the default 60 centiseconds (0.6 seconds).

Default Setting

60 centiseconds (0.6 seconds)

Command Mode

Global Config

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).

This command has an effect only when GVRP and GMRP are enabled.

Syntax

garp timer leaveall < 200-6000 >
no garp timer leaveall

<200-6000> - leave time (Range: 200 – 6000) in centiseconds.

no - This command sets how frequently Leave All PDUs are generated per port to 1000 centiseconds (10 seconds).

Default Setting

1000 centiseconds (10 seconds)

Command Mode

Interface Config

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).

This command has an effect only when GVRP and GMRP are enabled.

Syntax

garp timer leaveall all < 200-6000 >
no garp timer leaveall all

<200-6000> - leave time (Range: 200 – 6000) in centiseconds.

all - All interfaces.

no - This command sets how frequently Leave All PDUs are generated for all ports to 1000 centiseconds (10 seconds).

Default Setting

1000 centiseconds (10 seconds)

Command Mode

Global Config

7.2.6 IGMP Snooping

7.2.6.1 ip igmp snooping

The user can go to the CLI Global Configuration Mode to set IGMP Snooping on the system, use the **ip igmp snooping** global configuration command. Use the **no ip igmp snooping** to disable IGMP Snooping on the system.

Syntax

```
ip igmp snooping
no ip igmp snooping
```

Default Setting

Disabled

Command Mode

Global Config

7.2.6.2 ip igmp snooping interfacemode

The user can go to the CLI Global/Interface Configuration Mode to set IGMP Snooping on one interface or all interfaces, use the **ip igmp snooping interfacemode** global/interface configuration command. Use the **no ip igmp snooping interfacemode** disable IGMP Snooping on all interfaces.

Syntax

```
ip igmp snooping interfacemode all
no ip igmp snooping interfacemode all
ip igmp snooping interfacemode
no ip igmp snooping interfacemode
```

Default Setting

None

Command Mode

Global Config

Interface Config

7.2.6.3 ip igmp snooping fast-leave

The user can go to the CLI Global/Interface Configuration Mode to set IGMP Snooping fast-leave admin mode on a selected interface or all interfaces, use the **ip igmpsnooping fast-leave** global/interface configuration command. Use the **no ip igmp snooping fast-leave** disable IGMP Snooping fast-leave admin mode.

Syntax

```
ip igmp snooping fast-leave
no ip igmp snooping fast-leave
```

Default Setting

Disabled

Command Mode

Global Config

Interface Config

7.2.6.4 ip igmp snooping groupmembershipinterval

The user can go to the CLI Global/Interface Configuration Mode to set the IGMP Group Membership Interval time on one interface or all interfaces, use the **ip igmp snooping groupmembershipinterval <2-3600>** global/interface configuration command. Use the **no ip igmp snooping groupmembershipinterval** return to default value 260.

Syntax

```
ip igmp snooping groupmembershipinterval <2-3600>
no ip igmp snooping groupmembershipinterval
```

<2-3600> -- This value must be greater than the IGMPv3 Maximum Response time value. The range is 2 to 3600 seconds.

Default Setting

260

Command Mode

Global Config

Interface Config

7.2.6.5 ip igmp snooping max-response-time

The user can go to the CLI Interface Global/Interface Configuration Mode to set the IGMP Maximum Response time for the system, on a particular interface, use the **ip igmp snooping max-response-time <1-25>** global/interface configuration command. Use the **no ip igmp snooping max-response-time** return to default value 10

Syntax

```
ip igmp snooping max-response-time <1-25>
no ip igmp snooping max-response-time
```

<1-25> -- This value must be less than the IGMP Query Interval time value. The range is 1 to 25 seconds.

Default Setting

10

Command Mode

Global Config

Interface Config

7.2.6.6 ip igmp snooping mcrtrexpiretime

The user can go to the CLI Interface Global/Interface Configuration Mode to set the Multicast Router Present Expiration time for the system or on a particular interface, use the **ip igmp snooping mcrtrexpiretime <0-3600>** global/interface configuration command. Use the **no ip igmp snooping mcrtrexpiretime** to return to default value 0.

Syntax

```
ip igmp snooping mcrtrexpiretime <0-3600>
no ip igmp snooping mcrtrexpiretime
```

<0-3600> -- The range is 0 to 3600 seconds. A value of 0 indicates an infinite time-out, i.e. no expiration.

Default Setting

0

Command Mode

Global Config

Interface Config

7.2.6.7 ip igmp snooping mrouter interface

The user can go to the CLI Interface Configuration Mode to configure the interface as a multicast router-attached interface or configure the VLAN ID for the VLAN that has the multicast router attached mode enabled, use the **ip igmp snooping mrouter interface|<vlanId>** interface configuration command. Use the **no ip igmp snooping mrouter interface|<vlanId>** disable multicast router attached mode for the interface or a VLAN.

Syntax

```
ip igmp snooping mrouter interface|<vlanId>
no ip igmp snooping mrouter interface|<vlanId>
```

<vlanid> - VLAN ID (Range: 1 – 3965).

Default Setting

None

Command Mode

Interface Config

7.2.6.8 set igmp

The user can go to the CLI VLAN Mode to set IGMP Snooping on a particular VLAN, use the **set ipgm <vlanid>** vlan configuration command. Use the **no set igmp <vlanid>** to disable IGMP Snooping on a particular VLAN.

Syntax

```
set igmp <vlanid>
no set igmp <vlanid>
```

<vlanid> - VLAN ID (Range: 1 – 3965).

Default Setting

Disabled

Command Mode

VLAN Mode

7.2.6.9 set igmp fast-leave

The user can go to the CLI VLAN Configuration Mode to set IGMP Snooping fast-leave admin mode on a particular VLAN, use the **set igmp fast-leave <vlanid>** vlan configuration command. Use the **no set igmp fast-leave <vlanid>** disable IGMP Snooping fast-leave admin mode.

Syntax

```
set igmp fast-leave <vlanid>
no set igmp fast-leave <vlanid>
```

<vlanid> - VLAN ID (Range: 1 – 3965).

Default Setting

Disabled

Command Mode

VLAN Mode

7.2.6.10 set igmp groupmembership-interval

The user can go to the CLI VLAN Configuration Mode to set the IGMP Group Membership Interval time on a particular VLAN, use the **set igmpgroupmembership-interval <vlanid> <2-3600>** vlan configuration command. Use the **no set igmp groupmembership-interval <vlanid>** return to default value 260.

Syntax

```
set igmp groupmembership-interval <vlanid> <2-3600>
no set igmp groupmembership-interval <vlanid>
```

<vlanid> - VLAN ID (Range: 1 – 3965).

<2-3600> - The range of group membership interval time is 2 to 3600 seconds.

Default Setting

260

Command Mode

VLAN Mode

7.2.6.11 set igmp maxresponse

The user can go to the CLI Interface VLAN Mode to set the IGMP Maximum Response time on a particular VLAN, use the **set igmp maxresponse <vlanid> <1-25>** vlan configuration command. Use the **no set igmp maxresponse <vlanid>** return to default value 10

Syntax

```
set igmp maxresponse <vlanid> <1-25>
no set igmp maxresponse <vlanid>
```

< vlanid > - VLAN ID (Range: 1 – 3965).

<1-25> -- This value must be less than the IGMP Query Interval time value. The range is 1 to 25 seconds.

Default Setting

10

Command Mode

VLAN Mode

7.2.6.12 set igmp mcrtrexpiretime

The user can go to the CLI Interface VLAN Configuration Mode to set the Multicast Router Present Expiration time on a particular VLAN, use the **set igmp mcrtrexpiretime <vlanid> <0-3600>** vlan configuration command. Use the **no set igmp mcrtrexpiretime <vlanid>** to return to default value 0.

Syntax
set igmp mcrtrexpiretime <vlanid> <0-3600> no set igmp mcrtrexpiretime <vlanid>

< vlanid > - VLAN ID (Range: 1 – 3965).

<0-3600> - The range of the Multicat Router Present Expire time is 0 to 3600 seconds

Default Setting

0

Command Mode

VLAN Mode

7.2.6.13 ip igmp snooping static

The user can go to the Global Mode and add a port to multicast group, use the **ip igmp snooping static** Global command. The MAC address of the L2Mcast Group in the format 01:00:5e:xx:xx:xx.

Syntax
ip igmp snooping static <macaddr> vlan <vlanid> interface <slot/port> no ip igmp snooping static <macaddr> vlan <vlanid> interface <slot/port>

< vlanid > - VLAN ID (Range: 1 – 3965).

<macaddr> - Static MAC address.

<slot/port> - Interface number.

Default Setting

None

Command Mode

Global Config

7.2.6.14 show ip igmp snooping

The user can go to the CLI Privilege Exec to get all of igmp snooping information, use the **show ip igmp snooping** Privilege command.

Syntax
show ip igmp snooping

Default Setting

None

Command Mode

Privilege Exec

Display Message

When the optional arguments <slot/port> or <vlanid> are not used, the command displays the following information.

Admin Mode: Indicates whether or not IGMP Snooping is active on the switch.

Interfaces Enabled for IGMP Snooping: Interfaces on which IGMP Snooping is enabled.

Multicast Control Frame Count: Displays the number of IGMP Control frames that are processed by the CPU.

VLANs Enabled for IGMP Snooping: VLANs on which IGMP Snooping is enabled.

When you specify the <slot/port> values, the following information displays.

IGMP Snooping Admin Mode: Indicates whether IGMP Snooping is active on the interface.

Fast Leave Mode: Indicates whether IGMP Snooping Fast Leave is active on the interface.

Group Membership Interval: Shows the amount of time in seconds that a switch will wait for a report from a particular group on a particular interface, which is participating on the interface, before deleting the interface from the entry. This value may be configured.

Max Response Time: Interface on which IGMP Snooping is enabled.

Multicast Router Expiry Time: Displays the amount of time to wait before removing an interface that is participating on the interface from the list of interfaces with multicast routers attached. The interface is removed if a query is not received. This value may be configured.

When you specify a value for <vlanid>, the following information appears.

VLAN ID: VLAN Id

IGMP Snooping Admin Mode: Indicates whether IGMP Snooping is active on the VLAN.

Fast Leave Mode: Indicates whether IGMP Snooping Fast Leave is active on the VLAN.

Group Membership Interval: Shows the amount of time in seconds that a switch will wait for a report from a particular group on a particular interface, which is participating in the VLAN, before deleting the interface from the entry. This value may be configured.

Max Response Time: VLANs on which IGMP Snooping is enabled.

Multicast Router Expiry Time: Displays the amount of time to wait before removing an interface that is participating in the VLAN from the list of interfaces with multicast routers attached. The interface is removed if a query is not received. This value may be configured.

7.2.6.15 show ip igmp snooping mrouter interface

The user can go to the CLI Privilege Exec to display information about statically configured multicast router-attached interfaces, use the **show ip igmp snooping mrouter interface** Privilege command.

Syntax

show ip igmp snooping mrouter interface <slot/port>

<slot/port> - Interface number.

Default Setting

None

Command Mode

Privilege Exec

Display Message

Slot/Port: Shows the interface on which multicast router information is being displayed.

Multicast Router Attached: Indicates whether multicast router is statically enabled on the interface.

7.2.6.16 show ip igmp snooping mrouter vlan

The user can go to the CLI Privilege Exec to display information about statically configured multicast router-attached interfaces, use the **show ip igmp snooping mrouter vlan** Privilege command.

Syntax

show ip igmp snooping mrouter vlan <slot/port>

<slot/port> - Interface number.

Default Setting

None

Command Mode

Privilege Exec

Display Message

VLAN ID: Displays the list of VLANs of which the interface is a member.

Slot/Port: Shows the interface on which multicast router information is being displayed.

7.2.6.17 show ip igmp snooping static

The user can go to the Privilege Exec to display IGMP snooping static information, use the **show ip igmp snooping static** Privilege command.

Syntax
show ip igmp snooping static

Default Setting

None

Command Mode

Privilege Exec

Display Message

VLAN: The VLAN ID used with the MAC address to fully identify packets you want L2Mcast Group.

MAC Address: The MAC address of the L2Mcast Group in the format 01:00:5e:xx:xx:xx.

Port: List the ports you want included into L2Mcast Group.

State: The active interface number belongs to this Multicast Group.

7.2.6.18 show mac-address-table igmpsnooping

The user can go to the CLI Privilege Exec to display the IGMP Snooping entries in the Multicast Forwarding Database (MFDB) table, use the **show mac-address-table igmpsnooping** Privilege command.

Syntax
show mac-address-table igmpsnooping

Default Setting

None

Command Mode

Privilege Exec

Display Message

MAC Address: A multicast MAC address for which the switch has forwarding or filtering information. The format is twodigit hexadecimal numbers that are separated by colons, for example 01:00:5e:67:89:AB.

Type: The type of entry, which is either static (added by the user) or dynamic (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:).

7.2.7 IGMP Snooping Querier

7.2.7.1 ip igmp snooping querier

The user can go to the CLI Global Configuration Mode to set IGMP snooping querier admin mode, use the **ip igmp snooping querier** global configuration command. Use the **no ip igmp snooping querier** to disable.

Syntax

```
ip igmp snooping querier
no ip igmp snooping querier
```

Default Setting

Disabled

Command Mode

Global Config

7.2.7.2 ip igmp snooping querier address

The user can go to the CLI Global Configuration Mode to set IGMP snooping querier address, use the **ip igmp snooping querier address <ip-address>** global configuration command. Use the **no ip igmp snooping querier address** return to default value zero.

Syntax

```
ip igmp snooping querier address <ip-address>
no ip igmp snooping querier address
```

<ip-address> - ip address

Default Setting

0.0.0.0

Command Mode

Global Config

7.2.7.3 ip igmp snooping querier query-interval

The user can go to the CLI Global Configuration Mode to set IGMP snooping querier query interval, use the **ip igmp snooping querier query-interval <1-1800>** global configuration command. Use the **no ip igmp snooping querier query-interval** return to default value zero.

Syntax

```
ip igmp snooping querier query-interval <1-1800>
no ip igmp snooping querier query-interval
```

<1-1800> - set IGMP snooping querier query interval

Default Setting

Disabled

Command Mode

Global Config

7.2.7.4 ip igmp snooping querier querier-expiry-interval

The user can go to the CLI Global Configuration Mode to set IGMP snooping querier querier expiry interval, use the **ip igmp snooping querier querier-expiry-interval <60-300>** global configuration command. Use the **no ip igmp snooping querier query-interval** return to default value zero.

Syntax

```
ip igmp snooping querier querier-expiry-interval <60-300>
no ip igmp snooping querier querier-expiry-interval
```

<60-300> - set igmp querier timer expiry

Default Setting

60 seconds

Command Mode

Global Config

7.2.7.5 ip igmp snooping querier version

The user can go to the CLI Global Configuration Mode to set IGMP snooping querier version, use the **ip igmp snooping querier version <1-2>** global configuration command. Use the **no ip igmp snooping querier version** return to default value zero.

Syntax

```
ip igmp snooping querier version <1-2>
no ip igmp snooping querier version
```

<1-2> - set IGMP version of the querier

Default Setting

1

Command Mode

Global Config

7.2.7.6 ip igmp snooping querier vlan

The user can go to the CLI Global Configuration Mode to set IGMP snooping querier vlan admin mode, use the **ip igmp snooping querier vlan <1-3965>** global configuration command. Use the **no ip igmp snooping querier vlan <1-3965>** return to disable.

Syntax

```
ip igmp snooping querier vlan <1-3965>
no ip igmp snooping querier vlan <1-3965>
```

< vlanid > - VLAN ID (Range: 1 - 3965).

Default Setting

Disabled

Command Mode

Global Config

7.2.7.7 ip igmp snooping querier vlan address

The user can go to the CLI Global Configuration Mode to set IGMP snooping querier vlan address, use the **ip igmp snooping querier vlan <1-3965> address <ip-address>** global configuration command. Use the **no ip igmp snooping querier vlan <1-3965> address** return to default value zero.

Syntax

```
ip igmp snooping querier vlan <1-3965> address <ip-address>
no ip igmp snooping querier vlan <1-3965> address
```

<vlanid> - VLAN ID (Range: 1 - 3965).

<ip-address> - ip address

Default Setting

0.0.0.0

Command Mode

Global Config

7.2.7.8 ip igmp snooping querier vlan election participate

The user can go to the CLI Global Configuration Mode to set IGMP snooping querier vlan election participate mode, use the **ip igmp snooping querier vlan election participate <1-3965>** global configuration command. Use the **no ip igmp snooping querier vlan election participate <1-3965>** return to disable.

Syntax

```
ip igmp snooping querier vlan election participate <1-3965>
no ip igmp snooping querier vlan election participate <1-3965>
```

<vlanid> - VLAN ID (Range: 1 - 3965).

Default Setting

Disabled

Command Mode

Global Config

7.2.7.9 show ip igmp snooping querier

This command display IGMP snooping querier global information on the system.

Syntax

show ip igmp snooping querier

Command Mode

Privilege Exec

Display Information

IGMP Snooping Querier Mode: Administrative mode for IGMP Snooping. The default is disable.

Querier Address: Specify the Snooping Querier Address to be used as source address in periodic IGMP queries. This address is used when no address is configured on the VLAN on which query is being sent.

IGMP Version: Specify the IGMP protocol version used in periodic IGMP queries.

Querier Query Interval: Specify the time interval in seconds between periodic queries sent by the snooping querier. The Query Interval must be a value in the range of 1 and 1800. The default value is 60.

Querier Expiry Interval: Specify the time interval in seconds after which the last querier information is removed. The Querier Expiry Interval must be a value in the range of 60 and 300. The default value is 60.

7.2.7.10 show ip igmp snooping querier vlan

This command display IGMP snooping querier vlan information on the system.

Syntax

show ip igmp snooping querier vlan <1-3965>

<vlanid> - VLAN ID (Range: 1 - 3965).

Command Mode

Privilege Exec

Display Information

IGMP Snooping Querier Vlan Mode: Display the administrative mode for IGMP Snooping for the switch.

Querier Election Participation Mode: Displays the querier election participate mode on the VLAN. When this mode is disabled, up on seeing a query of the same version in the vlan, the snooping querier move to non querier state. Only when this mode is enabled, the snooping querier will participate in querier election where in the least ip address will win the querier election and operates as the querier in that VLAN. The other querier moves to non-querier state.

Querier Vlan Address: Displays the Snooping Querier Address to be used as source address in periodic IGMP queries sent on the specified VLAN.

Operational State: Specifies the operational state of the IGMP Snooping Querier on a VLAN.

Operational Version: Displays the operational IGMP protocol version of the querier.

7.2.7.11 show ip igmp snooping querier detail

This command display all of IGMP snooping querier information on the system.

Syntax

show ip igmp snooping querier detail

Command Mode

Privilege Exec

Display Information

IGMP Snooping Querier Mode: Administrative mode for IGMP Snooping. The default is disable.

Querier Address: Specify the Snooping Querier Address to be used as source address in periodic IGMP queries. This address is used when no address is configured on the VLAN on which query is being sent.

IGMP Version: Specify the IGMP protocol version used in periodic IGMP queries.

Querier Query Interval: Specify the time interval in seconds between periodic queries sent by the snooping querier. The Query Interval must be a value in the range of 1 and 1800. The default value is 60.

Querier Expiry Interval: Specify the time interval in seconds after which the last querier information is removed. The Querier Expiry Interval must be a value in the range of 60 and 300. The default value is 60.

7.2.8 MLD Snooping

7.2.8.1 show ipv6 mld snooping

The user can go to the CLI Privilege Exec to get all of mld snooping information, use the **show ip mld snooping** Privilege command.

Syntax

show ipv6 mld snooping [<slot/port>|<vlan-id>]

Default Setting

None

Command Mode

Privileged Exec

User Exec

Display Message

When the optional arguments <slot/port> or <vlanid> are not used, the command displays the following information.

Admin Mode: Indicates whether or not MLD Snooping is active on the switch.

Interfaces Enabled for MLD Snooping: Interfaces on which MLD Snooping is enabled.

Multicast Control Frame Count: Displays the number of MLD Control frames that are processed by the CPU.

VLANs Enabled for MLD Snooping: VLANs on which MLD Snooping is enabled.

When you specify the <slot/port> values, the following information displays.

MLD Snooping Admin Mode: Indicates whether MLD Snooping is active on the interface.

Fast Leave Mode: Indicates whether MLD Snooping Fast Leave is active on the interface.

Group Membership Interval: Shows the amount of time in seconds that a switch will wait for a report from a particular group on a particular interface, which is participating on the interface, before deleting the interface from the entry. This value may be configured.

Max Response Time: Interface on which MLD Snooping is enabled.

Multicast Router Present Expiration Time: Displays the amount of time to wait before removing an interface that is participating on the interface from the list of interfaces with multicast routers attached. The interface is removed if a query is not received. This value may be configured.

When you specify a value for <vlanid>, the following information appears.

VLAN ID: VLAN Id.

MLD Snooping Admin Mode: Indicates whether MLD Snooping is active on the VLAN.

Fast Leave Mode: Indicates whether MLD Snooping Fast Leave is active on the VLAN.

Group Membership Interval: Shows the amount of time in seconds that a switch will wait for a report from a particular group on a particular interface, which is participating in the VLAN, before deleting the interface from the entry. This value may be configured.

Max Response Time: VLANs on which MLD Snooping is enabled.

Multicast Router Present Expiration Time: Displays the amount of time to wait before removing an interface that is participating in the VLAN from the list of interfaces with multicast routers attached. The interface is removed if a query is not received. This value may be configured.

7.2.8.2 show ipv6 mld snooping mrouter interface

The user can go to the CLI Privilege Exec to display information about statically configured multicast router-attached interfaces, use the **show ipv6 mld snooping mrouter interface** Privilege command.

Syntax

show ipv6 mld snooping mrouter interface <slot/port>

Default Setting

None

Command Mode

Privileged Exec

User Exec

Display Message

Interface: Shows the interface on which multicast router information is being displayed.

Multicast Router Attached: Indicates whether multicast router is statically enabled on the interface.

VLAN ID: Displays the list of VLANs of which the interface is a member.

7.2.8.3 show ipv6 mld snooping mrouter vlan

The user can go to the CLI Privilege Exec to display information about statically configured multicast router-attached interfaces, use the **show ipv6 mld snooping mrouter vlan** Privilege command.

Syntax

show ipv6 mld snooping mrouter vlan <slot/port>

Default Setting

None

Command Mode

Privileged Exec

User Exec

Display Message

VLAN ID: Displays the list of VLANs of which the interface is a member.

Interface: Shows the interface on which multicast router information is being displayed.

7.2.8.4 show ipv6 mld snooping static

The user can go to the Privilege Exec to display MLD snooping static information, use the **show ipv6 mld snooping static** Privilege command.

Syntax

show ipv6 mld snooping static

Default Setting

None

Command Mode

Privilege Exec

User Exec

Display Message

VLAN: The VLAN ID used with the MAC address to fully identify packets you want L2Mcast Group.

MAC Address: The MAC address of the L2Mcast Group in the format 33:33:xx:xx:xx:xx.

Port: List the ports you want included into L2Mcast Group.

State: The active interface number belongs to this Multicast Group.

7.2.8.5 show mac-address-table mldsnooping

The user can go to the CLI Privilege Exec to display the MLD Snooping entries in the Multicast Forwarding Database (MFDB) table, use the **show mac-address-table mldsnooping** Privilege command.

Syntax

show mac-address-table mldsnooping

Default Setting

None

Command Mode

Privileged Exec

Display Message

MAC Address: A multicast MAC address for which the switch has forwarding or filtering information. The format is twodigit hexadecimal numbers that are separated by colons, for example 33:33:45:67:89:AB.

Type: The type of entry, which is either static (added by the user) or dynamic (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:).

7.2.8.6 ipv6 mld snooping

The user can go to the CLI Global Configuration Mode to set MLD Snooping on the system , use the **ipv6 mld snooping** global configuration command. Use the **no ipv6 mld snooping** to disable MLD Snooping on the system.

Syntax

```
Ipv6 mld snooping
no ipv6 mld snooping
```

Default Setting

Disabled

Command Mode

Global Config

7.2.8.7 clear mld snooping

The user can go to the CLI Global/Interface Configuration Mode to clear MLD Snooping on the system, use the **clear mld snooping** priviledge configuration command.

Syntax

```
clear mld snooping
```

Default Setting

None

Command Mode

Privilege Exec

7.2.8.8 ipv6 mld snooping interfacemode

The user can go to the CLI Global/Interface Configuration Mode to set MLD Snooping on one interface or all interfaces, use the **ipv6 mld snooping interfacemode** global/interface configuration command. Use the **no ipv6 mld snooping interfacemode** disable MLD Snooping on all interfaces.

Syntax

```
Ipv6 mld snooping interfacemode <all>
no ipv6 mld snooping interfacemode <all>
```

Default Setting

Disabled

Command Mode

Global Config

Interface Config

7.2.8.9 ipv6 mld snooping fast-leave

The user can go to the CLI Global/Interface Configuration Mode to set MLD Snooping fast-leave admin mode on a selected interface or all interfaces, use the **ipv6 mld snooping fast-leave** global/interface configuration command. Use the **no ipv6 mld snooping fast-leave** disable MLD Snooping fast-leave admin mode.

Syntax
ipv6 mld snooping fast-leave no ipv6 mld snooping fast-leave

Default Setting

Disabled

Command Mode

Global Config

Interface Config

7.2.8.10 ipv6 mld snooping groupmembershipinterval

The user can go to the CLI Global/Interface Configuration Mode to set the MLD Group Membership Interval time on one interface or all interfaces, use the **ipv6 mld snooping groupmembershipinterval <2-3600>** global/interface configuration command. Use the **no ipv6 mld snooping groupmembershipinterval** return to default value 260.

Syntax
Ipv6 mld snooping groupmembershipinterval <2-3600> no ipv6 mld snooping groupmembershipinterval

Default Setting

260

Command Mode

Global Config

Interface Config

7.2.8.11 ipv6 mld snooping max-response-time

The user can go to the CLI Interface Global/Interface Configuration Mode to set the MLD Maximum Response time for the system, on a particular interface, use the **ipv6 mld snooping max-response-time <1-65>** global/interface configuration command. Use the **no ipv6 mld snooping max-response-time** return to default value 10.

Syntax

```
Ipv6 mld snooping max-response-time <1-65>
no ipv6 mld snooping max-response-time
```

Default Setting

10

Command Mode

Global Config

Interface Config

7.2.8.12 ipv6 mld snooping mcrtrexpiretime

The user can go to the CLI Interface Global/Interface Configuration Mode to set the Multicast Router Present Expiration time for the system or on a particular interface, use the **ipv6 mld snooping mcrtrexpiretime <0-3600>** global/interface configuration command. Use the **no ipv6 mld snooping mcrtrexpiretime** to return to default value 0.

Syntax

```
ipv6 mld snooping mcrtrexpiretime <0-3600>
no ipv6 mld snooping mcrtrexpiretime
```

Default Setting

0

Command Mode

Global Config

Interface Config

7.2.8.13 ipv6 mld snooping mrouter interface

The user can go to the CLI Interface Configuration Mode to configure the interface as a multicast router-attached interface or configure the VLAN ID for the VLAN that has the multicast router attached mode enabled, use the **ipv6 mld snooping mrouter interface interface|<vlanId>** interface configuration command. Use the **no ipv6 mld snooping mrouter interface|<vlanId>** disable multicast router attached mode for the interface or a VLAN.

Syntax

```
Ipv6 mld snooping mrouter interface interface|<vlanId>
no ipv6 mld snooping mrouter interface|<vlanId>
```

Default Setting

None

Command Mode

Interface Config

7.2.8.14 ipv6 mld snooping static

The user can go to the Global Mode and add a port to ipv6 multicast group, use the **ipv6 mld snooping static** Global command.

Syntax

```
ipv6 mld snooping static <macaddr> vlan <vlan-id> interface <slot/port>
no ipv6 mld snooping static <macaddr> vlan <vlan-id> interface <slot/port>
```

Default Setting

None

Command Mode

Global Config

7.2.8.15 set mld

The user can go to the CLI VLAN Mode to set MLD Snooping on a particular VLAN, use the **set mld <vlanid>** vlan configuration command. Use the **no set mld <vlanid>** to disable MLD Snooping on a particular VLAN.

Syntax

```
set mld <vlanid>
no set mld <vlanid>
```

Default Setting

Disabled

Command Mode

VLAN Mode

7.2.8.16 set mld fast-leave

The user can go to the CLI VLAN Configuration Mode to set MLD Snooping fast-leave admin mode on a particular VLAN, use the **set mld fast-leave <vlanid>** vlan configuration command. Use the **no set mld fast-leave <vlanid>** disable MLD Snooping fast-leave admin mode.

Syntax

```
set mld fast-leave <vlanid>
no set mld fast-leave <vlanid>
```

Default Setting

Disabled

Command Mode

VLAN Mode

7.2.8.17 set mld groupmembership-interval

The user can go to the CLI VLAN Configuration Mode to set the MLD Group Membership Interval time on a particular VLAN, use the **set mld groupmembership-interval <vlanid> <2-3600>** vlan configuration command. Use the **no set mld groupmembership-interval <vlanid>** return to default value 260.

Syntax

```
set mld groupmembership-interval <vlanid> <2-3600>
no set mld groupmembership-interval <vlanid>
```

Default Setting

260

Command Mode

VLAN Mode

7.2.8.18 set mld maxresponse

The user can go to the CLI Interface VLAN Mode to set the MLD Maximum Response time on a particular VLAN, use the **set mld max-response-time <vlanid> <1-65>** vlan configuration command. Use the **no set mld max-response-time <vlanid>** return to default value 10.

Syntax

```
set mld max-response-time <vlanid> <1-65>
no set mld max-response-time <vlanid>
```

Default Setting

10

Command Mode

VLAN Mode

7.2.8.19 set ipv6 mld mcrtrexpiretime

The user can go to the CLI Interface VLAN Configuration Mode to set the Multicast Router Present Expiration time on a particular VLAN, use the **set mld mcrtrexpiretime <vlanid> <0-3600>** vlan configuration command. Use the **no set mld mcrtrexpiretime <vlanid>** to return to default value 0.

Syntax

```
set mld mcrtrexpiretime <vlanid> <0-3600>
no set mld mcrtrexpiretime <vlanid>
```

Default Setting

0

Command Mode

VLAN Mode

7.2.9 MLD Snooping Querier

7.2.9.1 show ipv6 mld snooping querier

This command display MLD snooping querier global information on the system.

Syntax

```
show ipv6 mld snooping querier
```

Default Setting

None

Command Mode

Privileged Exec

User Exec

Display Message

MLD Snooping Querier Mode: Specify the Snooping Querier Address to be used as source address in periodic MLD queries. This address is used when no address is configured on the VLAN on which query is being sent.

Querier Address: Specify the Snooping Querier Address to be used as source address in periodic MLD queries. This address is used when no address is configured on the VLAN on which query is being sent.

MLD Version: Specify the MLD protocol version used in periodic MLD queries.

Querier Query Interval: Specify the time interval in seconds between periodic queries sent by the snooping querier. The Query Interval must be a value in the range of 1 and 1800. The default value is 60.

Querier Expiry Interval: Specify the time interval in seconds after which the last querier information is removed. The Querier Expiry Interval must be a value in the range of 60 and 300. The default value is 60.

7.2.9.2 show ipv6 mld snooping querier vlan

This command display MLD snooping querier vlan information on the system.

Syntax

show ipv6 mld snooping querier vlan <1-3965>

Default Setting

None

Command Mode

Privileged Exec

User Exec

Display Message

MLD Snooping Querier Vlan Mode: Displays the querier election participate mode on the VLAN. When this mode is disabled, up on seeing a query of the same version in the vlan, the snooping querier move to non querier state. Only when this mode is enabled, the snooping querier will participate in querier election where in the least ip address will win the querier election and operates as the querier in that VLAN. The other querier moves to non-querier state.

Querier Election Participation Mode: Displays the querier election participate mode on the VLAN. When this mode is disabled, up on seeing a query of the same version in the vlan, the snooping querier move to non querier state. Only when this mode is enabled, the snooping querier will participate in querier election where in the least ip address will win the querier election and operates as the querier in that VLAN. The other querier moves to non-querier state.

Querier Vlan Address: Displays the Snooping Querier Address to be used as source address in periodic MLD queries sent on the specified VLAN.

Operational State: Specifies the operational state of the MLD Snooping Querier on a VLAN.

Operational Version: Displays the operational MLD protocol version of the querier.

7.2.9.3 show ipv6 mld snooping querier detail

This command display all of MLD snooping querier information on the system.

Syntax

```
show ipv6 mld snooping querier detail
```

Default Setting

None

Command Mode

Privileged Exec

User Exec

Display Message

MLD Snooping Querier Mode: Administrative mode for MLD Snooping. The default is disable

Querier Address: Specify the Snooping Querier Address to be used as source address in periodic MLD queries. This address is used when no address is configured on the VLAN on which query is being sent.

MLD Version: Specify the MLD protocol version used in periodic IGMP queries.

Querier Query Interval: Specify the time interval in seconds between periodic queries sent by the snooping querier. The Query Interval must be a value in the range of 1 and 1800. The default value is 60.

Querier Expiry Interval: Specify the time interval in seconds after which the last querier information is removed. The Querier Expiry Interval must be a value in the range of 60 and 300. The default value is 60.

7.2.9.4 ipv6 mld snooping querier

The user can go to the CLI Global Configuration Mode to set MLD snooping querier admin mode, use the **ipv6 mld snooping querier** global configuration command. Use the **no ipv6 mld snooping querier** to disable.

Syntax

```
ipv6 mld snooping querier
no ipv6 mld snooping querier
```

Default Setting

Disabled

Command Mode

Global Config

7.2.9.5 ipv6 mld snooping querier address

The user can go to the CLI Global Configuration Mode to set MLD snooping querier address, use the **ipv6 mld snooping querier address <ipv6-address>** global configuration command. Use the **ipv6 mld snooping querier address <ipv6-address>** return to default value zero.

Syntax

```
ipv6 mld snooping querier address <ipv6-address>
no ipv6 mld snooping querier address <ipv6-address>
```

Default Setting

0

Command Mode

Global Config

7.2.9.6 ipv6 mld snooping querier querier-interval

The user can go to the CLI Global Configuration Mode to set MLD snooping querier querier interval, use the **ipv6 mld snooping querier querier-interval <1-1800>** global configuration command. Use the **no ipv6 mld snooping querier query-interval** return to default value zero.

Syntax

```
ipv6 mld snooping querier querier-interval <1-1800>
no ipv6 mld snooping querier querier-interval
```

Default Setting

0

Command Mode

Global Config

7.2.9.7 ipv6 mld snooping querier querier-expiry-interval

The user can go to the CLI Global Configuration Mode to set MLD snooping querier querier expiry interval, use the **ipv6 mld snooping querier querier-expiry-interval <60-300>** global configuration command. Use the **no ipv6 mld snooping querier querier-expiry-interval** return to default value zero.

Syntax

```
ipv6 mld snooping querier querier-expiry-interval <60-300>
no ipv6 mld snooping querier querier-expiry-interval
```

Default Setting

0

Command Mode

Global Config

7.2.9.8 ipv6 mld snooping querier vlan

The user can go to the CLI Global Configuration Mode to set MLD snooping querier vlan admin mode, use the **ipv6 mld snooping querier vlan <1-3965>** global configuration command. Use the **no ipv6 mld snooping querier vlan <1-3965>** return to disable.

Syntax

```
ipv6 mld snooping querier vlan <1-3965>
no ipv6 mld snooping querier vlan <1-3965>
```

Default Setting

Disabled

Command Mode

Global Config

7.2.9.9 ipv6 mld snooping querier vlan address

The user can go to the CLI Global Configuration Mode to set MLD snooping querier vlan address, use the **ipv6 mld snooping querier vlan <1-3965> address <ip-address>** global configuration command. Use the **no ipv6 mld snooping querier vlan <1-3965> address <ip-address>** return to default value zero.

Syntax

```
ipv6 mld snooping querier vlan <1-3965> address <ipv6-address>
no ipv6 mld snooping querier vlan <1-3965> address <ipv6-address>
```

Default Setting

Disabled

Command Mode

Global Config

7.2.9.10 ipv6 mld snooping querier vlan election participate

The user can go to the CLI Global Configuration Mode to set MLD snooping querier vlan election participate mode, use the **ipv6 mld snooping querier vlan election-participate <1-3965>** global configuration command. Use the **no ipv6 mld snooping querier vlan election participate <1-3965>** return to disable.

Syntax

```
ipv6 mld snooping querier vlan election participate <1-3965>
no ipv6 mld snooping querier vlan election participate <1-3965>
```

Default Setting

Disabled

Command Mode

Global Config

7.2.10 Port Channel

7.2.10.1 show port-channel

This command displays the static capability of all port-channels (LAGs) on the device as well as a summary of individual port-channels.

Syntax

```
show port-channel brief
```

Default Setting

None

Command Mode

Privileged Exec

Display Message

For each port-channel the following information is displayed:

Logical Interface: The field displays logical slot and the logical port.

Port-Channel Name: This field displays the name of the port-channel.

Link State: This field indicates whether the link is up or down.

Trap Flag: This object determines whether or not to send a trap when link status changes. The factory default is enabled.

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.

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.

This command displays an overview of a specificed port-channel (LAG) on the switch.

Syntax

```
show port-channel <logical slot/port>
```

<logical slot/port> - The port-channel interface number.

Default Setting

None

Command Mode

Privileged Exec

Display Message

Log. Intf: The logical slot and the logical port.

Channel 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.

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.

Load Balance Option: This field displays the load-balance status whether a particular port-channel (LAG) is maintained.

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).

Device Timeout: Thie field displays the device timout value of actor and parter. The value of device timeout should be short(1 second) or long(30 seconds).

Port Speed: Speed of the port-channel port.

Port Active: This field lists the ports that are actively participating in the port-channel (LAG).

This command displays an overview of all port-channels (LAGs) on the switch.

Syntax

```
show port-channel all
```

Default Setting

None

Command Mode

Privileged Exec

Display Message

Log. Intf: The logical slot and the logical port.

Channel Name: The name of this port-channel (LAG). You may enter any string of up to 15 alphanumeric characters.

Link: Indicates whether the Link is up or down.

Admin Mode: May be enabled or disabled. The factory default is enabled.

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.

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).

Device Timeout: Thie field displays the device timout value of actor and parter. The value of device timeout should be short(1 second) or long(30 seconds).

Port Speed: Speed of the port-channel port.

Port Active: This field lists the ports that are actively participating in the port-channel (LAG).

7.2.10.2 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.**

Before including a port in a port-channel, set the port physical mode. See **speed** command.

Syntax

```
port-channel <name> [<index>]
no port-channel {<logical slot/port> | all}
```

<logical slot/port> - The port-channel interface number.

<name> - The port-channel name (up to 15 alphanumeric characters).

<index> - The port-channel index number, the range is from 1 to 64.

all - all port-channel interfaces.

no - This command removes that port-channel.

Default Setting

None

Command Mode

Global Config

Command Usage

Max number of port-channels could be created by user are 64 and maximum number of members for each port-channel are 8.

7.2.10.3 port-channel adminmode all

This command sets every configured port-channel with the same administrative mode setting.

Syntax

```
port-channel adminmode all
no port-channel adminmode all
```

no - This command disables a port-channel (LAG). The option **all** sets every configured port-channel with the same administrative mode setting.

Default Setting

Enabled

Command Mode

Global Config

7.2.10.4 staticcapability

This command enables the static function to support on specific port-channel (static link aggregations - LAGs) on the device. By default, the static capability for all of port-channels is disabled.

Syntax

```
staticcapability
no staticcapability
```

no - This command disables to support static function on specific port-channel on this device.

Default Setting

Disabled

Command Mode

Interface Config

7.2.10.5 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.

Syntax

```
port-channel linktrap {<logical slot/port> | all}
no port-channel linktrap {<logical slot/port> | all}
```

<logical slot/port> - The port-channel interface number.

all - all port-channel interfaces.

no - 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.

Default Setting

Enabled

Command Mode

Global Config

7.2.10.6 port-channel load-balance

This command for CLI will configured the mode of load balance on the all Port Channels. The parameter "**src-mac | dst-mac | dst-src-mac | src-ip | dst-ip| dst-src-ip**" represent the mode used to be set for port-channel load balance.

Syntax
port-channel load-balance all { src-mac| dst-mac | dst-src-mac | src-ip | dst-ip| dst-src-ip } no port-channel load-balance all

src-mac - Sets the mode on the source MAC address.

dst-mac - Sets the mode on the destination MAC address.

dst-src-mac - Sets the mode on the source and destination MAC addresses.

src-ip - Sets the mode on the source IP address.

dst-ip - Sets the mode on the destination IP address.

dst-src-ip - Sets the mode on the source and destination IP addresses.

no - Restore the mode to be default value.

Default Setting

dst-src-ip

Command Mode

Global Config

This command for CLI will configured the mode of load balance on the specific Port Channel. The parameter "**src-mac | dst-mac | dst-src-mac | src-ip | dst-ip| dst-src-ip**" represent the mode used to be set for port-channel load balance.

Syntax

```
load-balance { src-mac| dst-mac | dst-src-mac | src-ip | dst-ip| dst-src-ip }
no load-balance
```

src-mac - Sets the mode on the source MAC address.

dst-mac - Sets the mode on the destination MAC address.

dst-src-mac - Sets the mode on the source and destination MAC addresses.

src-ip - Sets the mode on the source IP address.

dst-ip - Sets the mode on the destination IP address.

dst-src-ip - Sets the mode on the source and destination IP addresses.

no - Restore the mode to be default value.

Default Setting

dst-src-ip

Command Mode

Interface Config

7.2.10.7 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.

Syntax

```
port-channel name {<logical slot/port> | all} <name>
```

<logical slot/port> - The port-channel interface number.

all - all port-channel interfaces.

<name> - The port-channel name (up to 15 characters) to be configured.

Default Setting

None

Command Mode

Global Config

7.2.10.8 port-channel system priority

This command defines a system priority for the port-channel (LAG).

Syntax

port-channel system priority <priority-value>

<priority-value> - valid value 0-65535.

Default Setting

32768

Command Mode

Global Config

7.2.10.9 adminmode

This command enables a port-channel (LAG) members. The interface is a logical slot and port for a configured port-channel.

Syntax

adminmode
no adminmode

no - This command disables a configured port-channel (LAG).

Default Setting

Enabled

Command Mode

Interface Config

7.2.10.10 lacp

This command enables Link Aggregation Control Protocol (LACP) on a port.

Syntax

lacp
no lacp

no - This command disables Link Aggregation Control Protocol (LACP) on a port.

Default Setting

Enabled

Command Mode

Interface Config

This command enables Link Aggregation Control Protocol (LACP) on all ports.

Syntax

```
lacp all
no lacp all
```

all - All interfaces.

no - This command disables Link Aggregation Control Protocol (LACP) on all ports.

Default Setting

Enabled

Command Mode

Global Config

7.2.10.11 lacp actor or lacp partner

This command set <actor | partner> admin key value of Link Aggregation Control Protocol (LACP) on a port.

Syntax

```
lacp <actor|partner> admin key <key-value>
no lacp <actor|partner> admin key
```

<key-value>: 0-65535

no - This command restores <actor | partner> admin key value of Link Aggregation Control Protocol (LACP) on a port.

Default Setting

Interface Number

Command Mode

Interface Config

This command set <actor | partner> admin state value of Link Aggregation Control Protocol (LACP) on a port.

Syntax

```
lacp <actor|partner> admin state <individual|longtimeout|passive>
no lacp <actor|partner> admin state <individual|longtimeout|passive>
```

individual - Set lacp admin state to individual. Use no form to set to aggregation.

longtimeout - Set lacp admin state longtimeout. Use no form to set to shorttimeout.

passive - Set lacp admin state passive. Use no form to set to active.

no - This command restores <actor | partner> admin state value of Link Aggregation Control Protocol (LACP) on a port.

Default Setting

no Individual (aggregation)

no longtimeout (shorttimeout)

no passive (active)

Command Mode

Interface Config

This command set <actor | partner> port priority value of Link Aggregation Control Protocol (LACP) on a port.

Syntax

```
lacp <actor|partner> port priority <priority-value>
no lacp <actor|partner> port priority
```

<priority-value> – range 0-255.

no - This command restores <actor | partner> port priority value of Link Aggregation Control Protocol (LACP) on a port.

Default Setting

128

Command Mode

Interface Config

This command set <actor | partner> system priority value of Link Aggregation Control Protocol (LACP).

Syntax

```
lacp <actor|partner> system priority <priority-value>
no lacp <actor|partner> system priority
```

<priority-value> – range 0-65535.

no - This command restores <actor | partner> system priority value of Link Aggregation Control Protocol (LACP).

Default Setting

32768

Command Mode

Interface Config

This command set collector max-delay time of Link Aggregation Control Protocol (LACP) on a port-channel.

Syntax

```
lacp collector max-delay <delay-value>
no lacp collector max-delay
```

<delay-value>: 0-65535

no - This command restores collector max-delay time of Link Aggregation Control Protocol (LACP) on a port-channel

Default Setting

0

Command Mode

Interface Config

7.2.10.12 channel-group

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.

i Before adding a port to a port-channel, set the physical mode of the port. See ‘speed’ command.

Syntax

```
channel-group <logical slot/port>
```

<logical slot/port> - Port-Channel Interface number.

Default Setting

None

Command Mode

Interface Config

Command Usage

The maximum number of members for each Port-Channel is 8.

7.2.10.13 delete-channel-group

This command deletes the port from the port-channel (LAG). The interface is a logical slot and port number of a configured port-channel.

Syntax

```
delete-channel-group <logical slot/port>
```

<logical slot/port> - Port-Channel Interface number.

Default Setting

None

Command Mode

Interface Config

This command deletes all configured ports from the port-channel (LAG). The interface is a logical slot and port number of a configured port-channel.

Syntax

```
delete-channel-group <logical slot/port> all
```

<logical slot/port> - Port-Channel Interface number.

all - All members for specific Port-Channel.

Default Setting

None

Command Mode

Global Config

7.2.11 Storm Control

7.2.11.1 show storm-control

This command is used to display broadcast storm control information.

Syntax
show storm-control broadcast

Default Setting

None

Command Mode

Privileged Exec

Display Message

Intf: Displays interface number.

Mode: Displays status of storm control broadcast.

Level: Displays level for storm control broadcast.

Rate: Displays rate for storm control broadcast.

This command is used to display multicast storm control information.

Syntax
show storm-control multicast

Default Setting

None

Command Mode

Privileged Exec

Display Message

Intf: Displays interface number.

Mode: Displays status of storm control multicast.

Level: Displays level for storm control multicast

Rate: Displays rate for storm control multicast.

This command is used to display unicast storm control information

Syntax

show storm-control unicast

Default Setting

None

Command Mode

Privileged Exec

Display Message

Intf: Displays interface number.

Mode: Displays status of storm control unicast.

Level: Displays level for storm control unicast

Rate: Displays rate for storm control unicast.

7.2.11.2 storm-control broadcast

This command enables broadcast storm recovery mode on the selected interface. If the mode is enabled, broadcast storm recovery with high threshold 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 threshold percentage or less. The full implementation is depicted in the “Broadcast Storm Recovery Thresholds” table.

Syntax

storm-control broadcast
no storm-control broadcast

no - This command disables broadcast storm recovery mode on the selected interface. 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 threshold percentage or less. The full implementation is depicted in the “Broadcast Storm Recovery Thresholds” table.

Default Setting

Disabled

Command Mode

Interface Config

This command enables broadcast storm recovery mode on all interfaces.

Syntax

```
storm-control broadcast
no storm-control broadcast
```

no - This command disables broadcast storm recovery mode on all interfaces.

Default Setting

Disabled

Command Mode

Global Config

7.2.11.3 storm-control multicast

This command enables multicast storm recovery mode on the selected interface.

Syntax

```
storm-control multicast
no storm-control multicast
```

no - This command disables multicast storm recovery mode on the selected interface.

Default Setting

None

Command Mode

Interface Config

This command enables multicast storm recovery mode on all interfaces.

Syntax

```
storm-control multicast
no storm-control multicast
```

no - This command disables multicast storm recovery mode on all interfaces.

Default Setting

None

Command Mode

Global Config

7.2.11.4 storm-control unicast

This command enables unicast storm recovery mode on the selected interface.

Syntax

```
storm-control unicast
no storm-control unicast
```

no - This command disables unicast storm recovery mode on the selected interface.

Default Setting

None

Command Mode

Interface Config

This command enables unicast storm recovery mode on all interfaces.

Syntax

```
storm-control unicast
no storm-control unicast
```

no - This command disables unicast storm recovery mode on all interfaces.

Default Setting

None

Command Mode

Global Config

7.2.11.5 switchport broadcast packet-rate

This command will protect your network from broadcast storms by setting a threshold level for broadcast traffic on each port.

Syntax

switchport broadcast packet-rate {1 | 2 | 3 | 4}

1 - Threshold level represents 64 pps for 1G Port or 1042 pps for 10G port.

2 - Threshold level represents 128 pps for 1G Port or 2084 pps for 10G port.

3 - Threshold level represents 256 pps for 1G Port or 3124 pps for 10G port.

4 - Threshold level represents 512 pps for 1G Port or 4167 pps for 10G port.

Note: pps (packet per second)

Default Setting

Level 4

Command Mode

Interface Config

This command will protect your network from broadcast storms by setting a threshold level for broadcast traffic on all ports.

Syntax

switchport broadcast all packet-rate {1 | 2 | 3 | 4}

1 - Threshold level represents 64 pps for 1G Port or 1042 pps for 10G port.

2 - Threshold level represents 128 pps for 1G Port or 2084 pps for 10G port.

3 - Threshold level represents 256 pps for 1G Port or 3124 pps for 10G port.

4 - Threshold level represents 512 pps for 1G Port or 4167 pps for 10G port.

all - This command represents all interfaces.

Note: pps (packet per second)

Default Setting

Level 4

Command Mode

Global Config

7.2.11.6 switchport multicast packet-rate

This command will protect your network from multicast storms by setting a threshold level for multicast traffic on each port.

Syntax

switchport multicast packet-rate {1 | 2 | 3 | 4}

1 - Threshold level represents 64 pps for 1G Port or 1042 pps for 10G port.

2 - Threshold level represents 128 pps for 1G Port or 2084 pps for 10G port.

3 - Threshold level represents 256 pps for 1G Port or 3124 pps for 10G port.

4 - Threshold level represents 512 pps for 1G Port or 4167 pps for 10G port.

Note: pps (packet per second)

Default Setting

Level 4

Command Mode

Interface Config

This command will protect your network from multicast storms by setting a threshold level for multicast traffic on all ports.

Syntax

switchport multicast all packet-rate {1 | 2 | 3 | 4}

1 - Threshold level represents 64 pps for 1G Port or 1042 pps for 10G port.

2 - Threshold level represents 128 pps for 1G Port or 2084 pps for 10G port.

3 - Threshold level represents 256 pps for 1G Port or 3124 pps for 10G port.

4 - Threshold level represents 512 pps for 1G Port or 4167 pps for 10G port.

all - This command represents all interfaces.

Note: pps (packet per second)

Default Setting

Level 4

Command Mode

Global Config

7.2.11.7 switchport unicast packet-rate

This command will protect your network from unicast storms by setting a threshold level for unicast traffic on each port.

Syntax

```
switchport unicast packet-rate {1 | 2 | 3 | 4}
```

1 - Threshold level represents 64 pps for 1G Port or 1042 pps for 10G port.

2 - Threshold level represents 128 pps for 1G Port or 2084 pps for 10G port.

3 - Threshold level represents 256 pps for 1G Port or 3124 pps for 10G port.

4 - Threshold level represents 512 pps for 1G Port or 4167 pps for 10G port.

Note: pps (packet per second)

Default Setting

Level 4

Command Mode

Interface Config

This command will protect your network from unicast storms by setting a threshold level for unicast traffic on all ports.

Syntax

```
switchport unicast all packet-rate {1 | 2 | 3 | 4}
```

1 - Threshold level represents 64 pps for 1G Port or 1042 pps for 10G port.

2 - Threshold level represents 128 pps for 1G Port or 2084 pps for 10G port.

3 - Threshold level represents 256 pps for 1G Port or 3124 pps for 10G port.

4 - Threshold level represents 512 pps for 1G Port or 4167 pps for 10G port.

all - This command represents all interfaces.

Note: pps (packet per second)

Default Setting

Level 4

Command Mode

Global Config

7.2.12 L2 Priority

7.2.12.1 show queue cos-map

This command displays the class of service priority map on specific interface.

Syntax

```
show queue cos-map [<slot/port>]
```

<slot/port> - Interface number.

Default Setting

None

Command Mode

Privileged Exec

Display Message

User Priority: Displays the 802.1p priority to be mapped.

Traffic Class: Displays internal traffic class to map the corresponding 802.1p priority.

7.2.12.2 queue cos-map

This command is used to assign class of service (CoS) value to the CoS priority queue.

Syntax

```
queue cos-map <priority> <queue-id>
no queue cos-map
```

<queue-id> - The queue id of the CoS priority queue (Range: 0 - 7).

<priority> - The CoS value that is mapped to the queue id (Range: 0 - 7).

no - Sets the CoS map to the default values.

Default Setting

priority	queue
0	1
1	0
2	0
3	1
4	2
5	2
6	3
7	3

Command Mode

Interface Config

7.2.13 Port Mirror

7.2.13.1 show port-monitor session

This command displays the Port monitoring information for the specified session.

Syntax

show port-monitor session <Session Number>

<Session Number> - session number.

Default Setting

None

Command Mode

Privileged Exec

Display Message

Session ID: indicates the session ID.

Admin Mode: indicates whether the Port Monitoring feature is enabled or disabled. The possible values are enabled and disabled.

Dest.Port: is the slot/port that is configured as the probe port. If this value has not been configured, 'Not Configured' will be displayed.

Sour.Port: is the slot/port that is configured as the monitored port. If this value has not been configured, 'Not Configured' will be displayed.

Type: Direction in which source port configured for port mirroring.Types are tx for transmitted packets and rx for receiving packets.

7.2.13.2 port-monitor session

This command configures a probe port and a monitored port for monitor session (port monitoring). Use the source interface <slot/port> parameter to specify the interface to monitor. Use rx to monitor only ingress packets, or use tx to monitor only egress packets. If you do not specify an {rx | tx} option, the destination port monitors both ingress and egress packets. Use the destination interface <slot/port> to specify the interface to receive the monitored traffic.

Syntax

port-monitor session <session-id> {source interface <slot/port> [{rx | tx}] | destination interface <slot/port> }
no port-monitor session <session-id> { source interface <slot/port> | destination interface <slot/port>}

<slot/port> - Interface number.

tx/rx – Use to monitor ingress packets or egress packets.

no - This command removes the probe port or the mirrored port from a monitor session (port monitoring).

Default Setting

None

Command Mode

Global Config

This command removes all configured probe ports and mirrored port.

Syntax

no port-monitor

Default Setting

None

Command Mode

Global Config

7.2.13.3 port-monitor session mode

This command configures the mode parameter to enabled the administrative mode of the session. If enabled, the probe port monitors all the traffic received and transmitted on the physical monitored port.

Syntax

port-monitor session <session-id> mode no port-monitor session <session-id> mode

<session-id> - Session ID.

no - This command disables port-monitoring function for a monitor session.

Default Setting

None

Command Mode

Global Config

7.2.14 Link State

7.2.14.1 show link state

Show link state information.

Syntax
show link state

Command Mode

Global Config

Display Message

Admin Mode: the link state admin mode.

Group ID: The group ID for each displayed row.

Mode: This group was set which mode.

UpStream: Display such port was included to UpStream set.

DownStream: Display such port was included to DownStream set.

7.2.14.2 link state

Enable/Disable the link state admin mode. Use ‘link state’ to enable the admin mode of redundant function, and use no command to disable the function.

Create/Destroy the link state group. Use ‘link state group’ to create a group. Use no command to destroy the group.

Enable/Disable a link state group. Use link state group enable <group id> to enable individual group, and use no command to disable a group.

Syntax

```
link state [group | [enable <1-6>]]
no link state [group <1-6> | [enable <1-6>]]
```

no - This command disables link state function.

Command Mode

Global Config

7.2.14.3 link state group

Set upstream port or downstream port for a link state group. Use ‘link state group <group id> upstream’ to set the port to be monitored.

Syntax

```
link state group <1-6> {downstream | upstream}
no link state group <1-6> {downstream | upstream}
```

no - This command disables link state group function.

Command Mode

Interface Config

7.2.15 Port Backup

7.2.15.1 show port backup

Show port-backup information.

Syntax

```
show port-backup
```

Command Mode

Privileged EXEC

Display Message

Admin Mode: Indicates whether or not port-backup is active on the switch.

Group ID: The Group ID for each displayed row.

Mode: Indicates whether or not the group is active.

MAC Update: Indicates whether or not mac-move-update is enable on the group.

Active Port: Display the active port number.

Backup Port: Display the active port number.

Current Active Port: Display the current active port number.

7.2.15.2 port-backup

Enable/Disable the port backup admin mode. Use ‘port-backup’ to enable the admin mode of function, and use no command to disable the function.

Create/Destroy the port backup group. Use ‘port-backup group’ to create a group. Use no command to destroy the group.

Enable/Disable a port-backup group. Use ‘port-backup group enable <group id> to enable individual group, and use no command to disable a group.

Enable/Disable a port-backup group support the mac-move-update. Use ‘port-backup group <group id> mac-move-update to enable individual group, and use no command to disable a group.

Syntax

```
port-backup [group | {enable <1 - 6>| <1 - 6> [failback-time <0 - 60>| mac-move-update]}]
no port-backup [group | {enable <1 - 6>| <1 - 6> [failback-time <0 - 60>| mac-move-update]}]
```

no - This command disables port-backup function.

Command Mode

Global Config

7.2.15.3 port-backup group

Set active port or backup port for a port-backup group. Use ‘port-backup group <group id> <active | backup>’ to set the port to be configured active or configured backup port.

Syntax

```
port-backup group <1-6> {active | backup}
no port-backup group <1-6> {active | backup}
```

no - This command disables port-backup group function.

Command Mode

Interface Config

7.2.16 FIP Snooping

7.2.16.1 show fip-snooping

This command displays fip-snooping whether enable or disable.

Syntax

show fip-snooping

Default Setting

None

Command Mode

Privileged Exec

Display Message

FIP Snooping: fip-snooping function status.

7.2.16.2 show fip-snooping enode

This command displays the ENode connections for the entire system.

Syntax

show fip-snooping enode

Default Setting

None

Command Mode

Privileged Exec

Display Message

Interface: Name of the interface to which the ENode is connected.

VLAN ID: ID number of the VLAN to which the ENode belongs.

ENode Name ID: Name ID.

ENode MAC: MAC address of the ENode.

7.2.16.3 show fip-snooping session

This command displays all FIP snooping sessions for the entire system.

Syntax

show fip-snooping session

Default Setting

None

Command Mode

Privileged Exec

Display Message

FCF MAC: MAC address of the FCF..

ENode MAC: MAC address of the ENode.

FCoE MAC: FCoE MAC address that is used to send the FCoE packets

FCF Interface: The interface to which the FCF is connected

ENode Interface: The interface to which the ENode is connected

7.2.16.4 show fip-snooping fcf

This command displays to what interfaces the FCFs are connected for the entire system.

Syntax

show fip-snooping fcf

Default Setting

None

Command Mode

Privileged Exec

Display Message

Interface: Name of the interface to which the FCoE Forwarder (FCF) is connected.

VLAN ID: ID number of the VLAN to which the FCF belongs.

FC MAP: May FC-Map value used by the FCF.

FCF MAC: MAC address of the FCF.

Switch Name: Name ID.

Fabric Name: Name of the FCF.

7.2.16.5 show fip-snooping vlan

This command displays FIP snooping whether enable or disable on specific VLAN.

Syntax

```
show fip-snooping vlan {< 1-3965> | all}
```

<1 - 3965> - VLAN ID.

all - This command represents all interfaces.

Default Setting

None

Command Mode

Privileged Exec

Display Message

Vlan ID: fip-snooping function status on the specific VLAN.

7.2.16.6 fip-snooping

The FIP snooping function is disabled by default. Only after enabling it, are the FIP related CLIs under VLAN and interface mode visible. The FIP-snoop process also starts after the “fip-snooping” command is enabled. Once the feature is enabled, the FIP-snoop packets and FCoE packets are dropped, unless explicitly enabled on a per-VLAN basis. If FIP snooping is enabled, all the FIP frames are snooped and security ACLs are added. FCoE traffic is blocked on all ports until the device re-initializes with FIP. If the feature is disabled, snooping is removed and all programmed ACLs and internal data are cleaned up.

Syntax

```
fip-snooping
no fip-snooping
```

no - This command disables fip snooping function.

Default Setting

Disabled

Command Mode

Global Config

7.2.16.7 fip-snooping vlan

This command enables FIP snooping on a VLAN. VLAN must be configured before it can be used. Once VLAN is enabled, the FIP packets will be snooped only on the configured VLANs. FIP snooping is disabled on VLANs by default.

Syntax

fip-snooping vlan <vlan id>

no fip-snooping vlan <vlan id>

<1 - 3965> - VLAN ID.

no - This command disable snooping on a specific VLAN.

Default Setting

Disabled

Command Mode

Global Config

7.2.17 Enhanced Transmission Selection (ETS)

7.2.17.1 show queue ets

This command displays ETS mode on specific interface.

Syntax

show queue ets <slot/port>

<slot/port> - Interface number.

Default Setting

None

Command Mode

Privileged Exec

Display Message

Interface: Name of the interface.

Mode: ETS mode.

7.2.17.2 show queue ets scheduler-type

This command displays ETS function on specific interface for the entire system.

Syntax

show queue ets scheduler-type <slot/port>

<slot/port> - Interface number.

Default Setting

None

Command Mode

Privileged Exec

Display Message

Interface: Name of the interface to which the ETS is enabled.

Scheduler-type: ETS scheduler type.

7.2.17.3 show queue ets weight

This command displays ETS function on specific interface for the entire system.

Syntax

show queue ets weight <slot/port>

Default Setting

None

Command Mode

Privileged Exec

Display Message

Interface: Name of the interface to which the ETS is enabled.

Weight : ETS weight in percentage.

7.2.17.4 show queue ets pg-mapping

This command displays ETS function on specific interface for the entire system.

Syntax

```
show queue ets pg-mapping <slot/port>
```

Default Setting

None

Command Mode

Privileged Exec

Display Message

Interface: Name of the interface to which the ETS is enabled.

pg-mapping: ETS priority to priority group mapping list.

7.2.17.5 queue ets

The ETS function is disabled by default. Only after enabling it, the ETS process also starts.

Syntax

```
queue ets
no queue ets
```

no - This command disables ETS function.

Default Setting

Disabled

Command Mode

Interface Config

7.2.17.6 queue ets scheduler-type

This command configures the scheduler type for an interface. The scheduler type is WRR or WERR. When the ETS is enabled, the default scheduler type is WERR.

Syntax

```
queue ets scheduler-type [wrr|werr]
no queue ets scheduler-type
```

WRR - Set ETS scheduler type to WRR

WERR - Set ETS scheduler type to WERR

no - This command restores the scheduler type to WERR.

Default Setting

werr

Command Mode

Interface Config

7.2.17.7 queue ets weight

This command configures the weight ratio of the two priority groups (LAN and SAN) for an interface. The sum of these two weight values should meet 100 in percentage. The default weights are 50 to 50.

Syntax

queue ets weight <1-99> <1-99>

no queue ets weight

<1 - 99> - weight values.

no - This command restores the weight values to 50 and 50.

Default Setting

50(LAN), 50(SAN)

Command Mode

Interface Config

7.2.17.8 queue ets pg-mapping

This command configures the mapping list of priority to priority groups. The range of priority id is from 0 to 7. The priority groups are LAN, SAN and IPC. This command let you assign priority id to specific priority group. When the ETS is enabled, priority id 0 to 2 are assigned to LAN, priority 3 to 6 are assigned to SAN, and priority 7 is assigned to IPC.

Syntax

queue ets pg-mapping {lan|san|ipc} [<0-7> [<0-7> [<0-7> [<0-7> [<0-7> [<0-7> [<0-7>]]]]]]]

no queue ets pg-mapping

<0 - 7> - Priority Id from 0 to 7.

lan - Sets ETS Priority Id to LAN priority group

san - Sets ETS Priority Id to SAN priority group

ipc - Sets ETS Priority Id to IPC priority group

no - This command restores the priority to priority group mapping list to default value.

Default Setting

Priority id 0 to 2 in LAN, 3 to 6 in SAN and 7 in IPC

Command Mode

Interface Config

7.2.18 Congestion Notification

7.2.18.1 show congestion-notify

This command displays CN function global parameter on system.

Syntax
show congestion-notify

Default Setting

None

Command Mode

Privileged Exec

Display Message

Congestion Notify: Displays Congestion Notification function status.

Tag ethertype recognize: When set to 1 , CN-Tag ether type is recognized by parsing stages

Tag ethertype: A new tag that is being added by 802.1Qau as a part of the congestion management requirements.

Msg ethertype: A message generated by the CP which informs the reaction point(RP) about the level of congestion at the CP.

CPID devid: Congestion point ID, A 64 bit value associated with every CP in the network. It is sent back along with every CNM so that network adminiatrators can use the CNMs to debug their network.

CPID LSB:. Displays Control the LSB field of Congestion Point Identifier of CNM payload.

outer TPID:. Displays Outer TPID for Congestion Notification Message (CNM).

outer VLAN: Displays Outer VLAN ID for Congestion Notification Message (CNM).

outer Dot1p: Displays Outer Packet Priority for Congestion Notification Message

outer CFI: Displays Outer Packet CFI for Congestion Notification Message

inner CFI: Displays Inner Packet CFI for Congestion Notification Message

inner Dot1p: Displays Inner Packet Priority for Congestion Notification Message

no-generate: Generate CNM or not.

7.2.18.2 show congestion-notify interface

This command displays CN function global parameter on system.

Syntax

```
show congestion-notify interface {<slot/port> | all}
```

<slot/port> - Interface number.

all - This command represents all interfaces.

Default Setting

None

Command Mode

Privileged Exec

Display Message

Interface: Name of the interface to which the CN is enabled.

Priority Queue: Priority queue is enabled for CN function.

Mode: CN mode (Enable/Disable)

CNM Count: Counts the number of CN message generated by the congestion messaged queue.

7.2.18.3 congestion-notify priority

The CN function is disabled by default on all priorities for each port. User can use this command to enable/disable the priority queue on specific interface.

Syntax

```
congestion-notify priority <0 – 7> enable
no congestion-notify priority <0 – 7>
```

<0 – 7>: Priority Queue you want to enable CN function**.**

no - This command disables CN function on priority queue for specific interface.

Default Setting

Disabled

Command Mode

Interface Config

7.2.18.4 congestion-notify tag

The user can go to the CLI Global Configuration Mode to configure the CNTAG Ether Type is recognized by parsing stages. Use the ‘congestion-notify tag ethertype recognize’ global configuration command. Use the ‘no congestion-notify tag ethertype recognize’ to configure CNTAG Ether Type is unrecognized.

Syntax

```
congestion-notify tag ethertype recognize
no congestion-notify tag ethertype recognize
```

no - This command disables CN tag processing.

Default Setting

Disabled

Command Mode

Global Config

The user can go to the CLI Global Configuration Mode to configure the Ether Type of CN-TAG. Use the ‘congestion-notify tag ethertype <value>’ global configuration command. Use the ‘no congestion-notify tag ethertype’ to configure CN-TAG Ether Type to default value..

Syntax

```
congestion-notify tag ethertype <0-65535>
```

Default Setting

0x22e9

Command Mode

Global Config

7.2.18.5 congestion-notify enable

The user can go to the CLI Global Configuration Mode to enable handling congestion notification message. Use the ‘congestion-notify enable’ global configuration command. Use the ‘no congestion-notify enable’ to disable handling congestion notification message.

Syntax

```
congestion-notify enable
no congestion-notify enable
```

no - This command disables handling congestion notification message.

Default Setting

Disabled

Command Mode

Global Config

7.2.18.6 congestion-notify msg

The user can go to the CLI Global Configuration Mode to configure the Ether Type of CNM. Use the ‘congestion-notify msg ethertype <value>’ global configuration command. Use the ‘no congestion-notify msg ethertype’ to configure CNM Ether Type to default value

Syntax

```
congestion-notify msg ethertype <0-65535>
no congestion-notify msg ethertype
```

<0-65535> - This command sets the Ether Type value of CNM.

no - This command disables Ether Type for Congestion Notification Message (CNM).

Default Setting

0x22e7

Command Mode

Global Config

7.2.18.7 congestion-notify CPID

The user can go to the CLI Global Configuration Mode to configure the device identifier of CPID. Use the ‘congestion-notify CPID devid <value>’ global configuration command. Use the ‘no congestion-notify CPID devid’ to configure device identifier to default value.

Syntax

```
congestion-notify CPID devid < 0-16777215 >
no congestion-notify CPID devid
```

<0-16777215> - This command sets the Device ID of CPID

no - This command configure device identifier to default value.

Default Setting

0

Command Mode

Global Config

The user can go to the CLI Global Configuration Mode to configure the LSB field of CPID of CNM payload. Use the ‘congestion-notify CPID LSB Q_No’ global configuration command to set the CPID mode to use queue number of sampled packet. Use the ‘congestion-notify LSB CPIndex’ to configure device identifier to use congestion point index.

Syntax

```
congestion-notify CPID LSB { CPIndex | Q_No}
```

CPIndex - This command configures queue number of sampled packet.

Q_No - This command sets congestion point index.

Default Setting

0

Command Mode

Global Config

7.2.18.8 congestion-notify outer

This command set value of CNM's outer VLAN tag's CFI bits, value of CNM's outer VLAN tag's 802.1p bits, value of CNM's outer VLAN tag's TPID, and set the CNM's outer VLAN ID.

Syntax

```
congestion-notify outer { CFI <-1-1> | Dot1p <-1-7> | TPID <0-65535> | vlan <0-4095>}
```

no congestion-notify outer { CFI	Dot1p | TPID| vlan}

<-1-1> - This command sets value of CNM's outer VLAN tag's CFI bits.

<-1-7> - This command sets value of CNM's outer VLAN tag's 802.1p bits.

<0-65535> - This command sets value of CNM's outer VLAN tag's TPID.

<0-4095> - This command sets the CNM's outer VLAN ID.

no - This command restored default value.

Default Setting

Command Mode

Global Config

7.2.18.9 congestion-notify inner

This command set value of CNM's inner VLAN tag's CFI bits and value of CNM's inner VLAN tag's 802.1p bits.

Syntax
congestion-notify inner { CFI <-1-1> | Dot1p <-1-7>}
no congestion-notify inner { CFI | Dot1p}

<-1-1> - This command sets value of CNM's inner VLAN tag's CFI bits.

<-1-7> - This command sets value of CNM's inner VLAN tag's 802.1p bits.

no - This command restored default value..

Default Setting

Command Mode

Global Config

7.2.18.10 congestion-notify no-generate

The user can go to the CLI Global Configuration Mode to choose the CNM generation behavior when congestion notification threshold is reached but the incoming sampled packet does not have CN-TAG. Use the ‘congestion-notify no-generate’ global configuration command. Use the ‘no congestion-notify no-generate’ to keep generate CNM.

Syntax

congestion-notify no-generate

no congestion-notify no-generate

no - This command uses to keep generate CNM.

Default Setting

keep generate CNM.

Command Mode

Global Config

7.3 Management Commands

7.3.1 Network Commands

7.3.1.1 show ip interface

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.

Syntax

show ip interface

Default Setting

None

Command Mode

Privileged Exec

User Exec

Display Message

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.

Network Configuration Protocol Current: Indicates which network protocol is being used. The options are bootp | dhcp | none.

DHCP Client Identifier TEXT: DCHP client identifier in TEXT mode for this switch.

DHCP Client Identifier HEX: DHCP client identifier in HEX address for this switch.

Management VLAN ID: Specifies the management VLAN ID.

Web Mode: Specifies whether the switch may be accessed from a Web browser. The factory default is enabled.

Web Port: This field is used to set the HTTP Port Number. The value must be in the range of 1 to 65535. Port 80 is the default value.

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.

7.3.1.2 show ip filter

This command displays management IP filter status and all designated management stations.

Syntax

show ip filter

Default Setting

None

Command Mode

Privileged Exec

Display Message

Manegement IP Filter Address Table: The admin mode status for IP filter.

Index: The index of stations.

IP Address: The IP address of stations that are allowed to make configuration changes to the Switch.

7.3.1.3 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 <1518-9216> is a valid integer between 1518-9216.

Syntax

mtu <1518-9216>
no mtu

<1518-9216> - Max frame size (Range: 1518 - 9216).

no - This command sets the default maximum transmission unit (MTU) size (in bytes) for the interface.

Default Setting

1518

Command Mode

Interface Config

7.3.1.4 interface vlan

This command is used to enter Interface-vlan configuration mode.

Syntax

```
interface vlan <vlanid>
```

<vlanid> - VLAN ID (Range: 1 - 3965).

Default Setting

None

Command Mode

Global Config

7.3.1.5 ip address

This command sets the IP Address, and subnet mask. The IP Address and the gateway must be on the same subnet.

Syntax

```
ip address <ipaddr> <netmask>
no ip address
```

<ipaddr> - IP address

<netmask> - Subnet Mask

no - Restore the default IP address and Subnet Mask

Default Setting

IP address: 0.0.0.0

Subnet Mask: 0.0.0.0

Command Mode

Interface-Vlan Config

Command Usage

Once the IP address is set, the VLAN ID's value will be assigned to management VLAN.

7.3.1.6 ip default-gateway

This command sets the IP Address of the default gateway.

Syntax

```
ip default-gateway <gateway>
no ip default-gateway
```

< gateway > - IP address of the default gateway

no - Restore the default IP address of the default gateway

Default Setting

IP address: 0.0.0.0

Command Mode

Global Config

7.3.1.7 ip address protocol

This command specifies the network configuration protocol to be used. If you modify this value, the change is effective immediately.

Syntax

```
ip address protocol {bootp | dhcp | none}
```

<bootp> - Obtains IP address from BOOTP.

<dhcp> - Obtains IP address from DHCP.

<none> - Obtains IP address by setting configuration.

Default Setting

None

Command Mode

Interface-Vlan Config

7.3.1.8 ip filter

This command is used to enable the IP filter function.

Syntax

```
ip filter
no ip filter
```

no – Disable ip filter.

Default Setting

Disabled

Command Mode

Global Config

This command is used to set an IP address to be a filter.

Syntax

```
ip filter <ipaddr>
no ip filter <ipaddr>
```

<ipaddr> - Configure a IP address to the filter.

no - Remove this IP address from filter.

Default Setting

None

Command Mode

Global Config

7.3.2 Serial Interface Commands

7.3.2.1 show line console

This command displays serial communication settings for the switch.

Syntax

show line console

Default Setting

None

Command Mode

Privileged Exec

Display Message

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 bauds.

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: The Parity Method used on the Serial Port. The Parity Method is always None.

Password Threshold: When the logon attempt threshold is reached on the console port, the system interface becomes silent for a specified amount of time before allowing the next logon attempt. (Use the silent time command to set this interval.) When this threshold is reached for Telnet, the Telnet logon interface closes.

Silent Time (sec): Use this command to set the amount of time the management console is inaccessible after the number of unsuccessful logon attempts exceeds the threshold set by the password threshold command.

Terminal Length: The columns per page for terminal serial port.

7.3.2.2 line console

This command is used to enter Line configuration mode

Syntax

line console

Default Setting

None

Command Mode

Global Config

7.3.2.3 baudrate

This command specifies the communication rate of the terminal interface. The supported rates are 1200, 2400, 4800, 9600, 19200, 38400, 57600, 115200.

Syntax

```
baudrate {1200 | 2400 | 4800 | 9600 | 19200 | 38400 | 57600 | 115200}
no baudrate
```

no - This command sets the communication rate of the terminal interface to **115200**.

Default Setting

115200

Command Mode

Line Config

7.3.2.4 exec-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.

Syntax

```
exec-timeout <0-160>
```

<0-160> - max connect time (Range: 0 -160), 0: forever.

no - This command sets the maximum connect time (in minutes) without console activity to 5.

Default Setting

5

Command Mode

Line Config

7.3.2.5 password-threshold

This command is used to set the password instruction threshold limiting the number of failed login attempts.

Syntax

```
password-threshold <0-120>
no password-threshold
```

<threshold> - max threshold (Range: 0 - 120).

no - This command sets the maximum value to the default.

Default Setting

3

Command Mode

Line Config

7.3.2.6 silent-time

This command uses to set the amount of time the management console is inaccessible after the number of unsuccessful logon tries exceeds the threshold value.

Syntax

```
silent-time <0-65535>
```

<0-65535> - silent time (Range: 0 - 65535) in seconds.

no - This command sets the maximum value to the default.

Default Setting

0

Command Mode

Line Config

7.3.2.7 terminal length

This command uses to configure the columns per page for the management console.

Syntax

```
terminal-length <10-100>
```

<10-100> - Columns per page (Range: 10 - 100).

no - This command sets the value to the default.

Default Setting

24

Command Mode

Line Config

7.3.3 Telnet Session Commands

7.3.3.1 telnet

This command establishes a new outbound telnet connection to a remote host.

Syntax

```
telnet <host> [port] [debug] [line] [echo]
```

<host> - A hostname or a valid IP address.

[port] - A valid decimal integer in the range of 0 to 65535, where the default value is 23.

[debug] - Display current enabled telnet options.

[line] - Set the outbound telnet operational mode as ‘linemode’, where by default, the operational mode is ‘character mode’.

[echo] - Enable local echo.

Default Setting

None

Command Mode

Privileged Exec

User Exec

7.3.3.2 show line vty

This command displays telnet settings.

Syntax

```
show line vty
```

Default Setting

None

Command Mode

Privileged Exec

Display Message

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. 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.

Password Threshold: When the logon attempt threshold is reached on the console port, the system interface becomes silent for a specified amount of time before allowing the next logon attempt. (Use the silent time command to set this interval.) When this threshold is reached for Telnet, the Telnet logon interface closes.

Telnet Server Admin Mode: The telnet server admin mode status. The factory default is enable

Terminal Length: The columns per page for terminal vty port.

7.3.3.3 line vty

This command is used to enter vty (Telnet) configuration mode.

Syntax
line vty

Default Setting

None

Command Mode

Global Config

7.3.3.4 exec-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.

i 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.

Syntax

```
exec-timeout <1-160>
no exec-timeout
```

<sec> - max connect time (Range: 1 -160).

no - This command sets the remote connection session timeout value, in minutes, to the default.

Default Setting

5

Command Mode

Line Vty

7.3.3.5 password-threshold

This command is used to set the password instruction threshold limited for the number of failed login attempts.

Syntax

```
password-threshold <0-120>
no password-threshold
```

<threshold> - max threshold (Range: 0 - 120).

no - This command sets the maximum value to the default.

Default Setting

3

Command Mode

Line Vty

7.3.3.6 terminal length

This command uses to configure the columns per page for the vty session.

Syntax

```
terminal-length <10-100>
```

<10-100> - Columns per page (Range: 10 - 100).

no - This command sets the value to the default.

Default Setting

24

Command Mode

Line Vty

7.3.3.7 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.

Syntax

```
maxsessions <0-5>
no maxsessions
```

<0-5> - max sessions (Range: 0 - 5).

no - This command sets the maximum value to be 5.

Default Setting

5

Command Mode

Line Vty

7.3.3.8 server enable

This command enables/disables telnet server. If telnet server is enabled, all telnet sessions can be established until there are no more sessions available. If telnet server is disabled, all telnet sessions are closed.

Syntax

```
server enable
no server enable
```

no - This command disables telnet server. If telnet server is disabled, all telnet sessions are droped.

Default Setting

Enabled

Command Mode

Line Vty

7.3.3.9 sessions

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.

Syntax

```
sessions
no sessions
```

no - This command disables telnet sessions. If sessions are disabled, no new telnet sessions are established.

Default Setting

Enabled

Command Mode

Line Vty

7.3.3.10 telnet sessions

This command regulates new outbound telnet connections. If enabled, new outbound telnet sessions can be established until it reaches the maximum number of simultaneous outbound telnet sessions allowed. If disabled, no new outbound telnet session can be established. An established session remains active until the session is ended or an abnormal network error ends it.

Syntax

```
telnet sessions
no telnet sessions
```

no - This command disables new outbound telnet connections. If disabled, no new outbound telnet connection can be established.

Default Setting

Enabled

Command Mode

Global Config

7.3.3.11 telnet maxsessions

This command specifies the maximum number of simultaneous outbound telnet sessions. A value of 0 indicates that no outbound telnet session can be established.

Syntax

```
telnet maxsessions <0-5>
no maxsessions
```

<0-5> - max sessions (Range: 0 - 5).

no - This command sets the maximum value to be 5.

Default Setting

5

Command Mode

Global Config

7.3.3.12 telnet exec-timeout

This command sets the outbound telnet session timeout value in minute.

i 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.

Syntax

```
telnet exec-timeout <1-160>
no telnet exec-timeout
```

<1-160> - max connect time (Range: 1 -160).

no - This command sets the remote connection session timeout value, in minutes, to the default.

Default Setting

5

Command Mode

Global Config

7.3.3.13 show telnet

This command displays the current outbound telnet settings.

Syntax

show telnet

Default Setting

None

Command Mode

Privileged Exec

User Exec

Display Message

Outbound Telnet Login Timeout (in minutes) Indicates the number of minutes an outbound telnet session is allowed to remain inactive before being logged off. A value of 0, which is the default, results in no timeout.

Maximum Number of Outbound Telnet Sessions Indicates the number of simultaneous outbound telnet connections allowed.

Allow New Outbound Telnet Sessions Indicates whether outbound telnet sessions will be allowed.

7.3.4 SSH Client Session Commands

7.3.4.1 ssh

This command establishes a new outbound ssh connection to a remote host.

Syntax

ssh <ip-address|hostname> <username> { [port <1-65535>] [protocol <protocollevel>] | [protocol <protocollevel>] [port <1-65535>]}

<ip-address|hostname> - A hostname or a valid IP address.

<username> - user account.

[port] - A valid decimal integer in the range of 1 to 65535, where the default value is 22.

[protocol] - SSH Protocol Level (Version) 1 or 2.

Default Setting

None

Command Mode

Privileged Exec

7.3.4.2 sshc sessions

This command regulates new outbound ssh connections. If enabled, new outbound ssh sessions can be established until it reaches the maximum number of simultaneous outbound ssh sessions allowed. If disabled, no new outbound ssh session can be established. An established session remains active until the session is ended or an abnormal network error ends it.

Syntax

```
sshc sessions
no sshc sessions
```

no - This command disables new outbound ssh connections. If disabled, no new outbound ssh connection can be established.

Default Setting

Enabled

Command Mode

Global Config

7.3.4.3 sshc maxsessions

This command specifies the maximum number of simultaneous outbound ssh sessions. A value of 0 indicates that no outbound ssh session can be established.

Syntax

```
sshc maxsessions <0-5>
no maxsessions
```

<0-5> - max sessions (Range: 0 - 5).

no - This command sets the maximum value to be 5.

Default Setting

5

Command Mode

Global Config

7.3.4.4 sshc exec-timeout

This command sets the outbound ssh session timeout value in minute.

i

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.

Syntax

```
sshc exec-timeout <1-160>
no sshc exec-timeout
```

<1-160> - max connect time (Range: 1 -160).

no - This command sets the remote connection session timeout value, in minutes, to the default.

Default Setting

5

Command Mode

Global Config

7.3.4.5 show sshc

This command displays the current outbound sshc settings.

Syntax

```
show sshc
```

Default Setting

None

Command Mode

Privileged Exec

User Exec

Display Message

Outbound SSH Login Timeout (in minutes) Indicates the number of minutes an outbound ssh session is allowed to remain inactive before being logged off. A value of 0, which is the default, results in no timeout.

Maximum Number of Outbound SSH Sessions Indicates the number of simultaneous outbound ssh connections allowed.

Allow New Outbound SSH Sessions Indicates whether outbound ssh sessions will be allowed.

7.3.5 SNMP Server Commands

7.3.5.1 show snmp

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 versions 1, 2c, and 3 (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).

Syntax
show snmp

Default Setting

None

Command Mode

Privileged Exec

Display Message

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 the IP Address then the address is an authenticated 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. That is, 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.

7.3.5.2 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.

Syntax

show trapflags

Default Setting

None

Command Mode

Privileged Exec

Display Message

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: 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.

DVMRP Traps May be enabled or disabled. The factory default is disabled. Indicates whether DVMRP traps will be sent.

OSPFv2 Traps May be enabled or disabled. The factory default is disabled. Indicates whether OSPF traps will be sent.

OSPFv3 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.

7.3.5.3 snmp-server sysname

This command sets the name of the switch. The range for name is from 1 to 31 alphanumeric characters.

Syntax

snmp-server sysname <name>

<name> - Range is from 1 to 31 alphanumeric characters.

Default Setting

None

Command Mode

Global Config

7.3.5.4 snmp-server location

This command sets the physical location of the switch. The range for name is from 1 to 31 alphanumeric characters.

Syntax

```
snmp-server location <loc>
```

<loc> - range is from 1 to 31 alphanumeric characters.

Default Setting

None

Command Mode

Global Config

7.3.5.5 snmp-server contact

This command sets the organization responsible for the network. The range for contact is from 1 to 31 alphanumeric characters.

Syntax

```
snmp-server contact <con>
```

<con> - Range is from 1 to 31 alphanumeric characters.

Default Setting

None

Command Mode

Global Config

7.3.5.6 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 privilege level. The length of the name can be up to 16 case-sensitive characters.

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.

Syntax

```
snmp-server community <name>
no snmp-server community <name>
```

<name> - community name (up to 16 case-sensitive characters).

no - This command removes this community name from the table. The name is the community name to be deleted.

Default Setting

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.

Command Mode

Global Config

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.

Syntax

```
snmp-server community mode <name>
no snmp-server community mode <name>
```

<name> - community name.

no - 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.

Default Setting

The default public and private communities are enabled by default. The four undefined communities are disabled by default.

Command Mode

Global Config

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.

Syntax

```
snmp-server community ipmask <ipmask> <name>
no snmp-server community ipmask <name>
```

<name> - community name.

<ipmask> - a client IP mask.

no - 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.

Default Setting

0.0.0.0

Command Mode

Global Config

This command restricts access to switch information. The access mode is read-only (also called public) or read/write (also called private).

Syntax

```
snmp-server community {ro | rw} <name>
```

<name> - community name.

<ro> - access mode is read-only.

<rw> - access mode is read/write.

Default Setting

None

Command Mode

Global Config

7.3.5.7 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.

Syntax

```
snmp-server community ipaddr <ipaddr> <name>
no snmp-server community ipaddr <name>
```

<name> - community name.

<ipaddr> - a client IP address.

no - This command sets a client IP address for an SNMP community to **0.0.0.0**. The name is the applicable community name.

Default Setting

0.0.0.0

Command Mode

Global Config

7.3.5.8 snmp-server enable traps

This command enables the acl trap.

Syntax

```
snmp-server enable traps acl-trapflags
no snmp-server enable traps acl-trapflags
```

no - This command disables the acl trap.

Default Setting

Enabled

Command Mode

Global Config

This command enables the Authentication trap.

Syntax

```
snmp-server enable traps authentication
no snmp-server enable traps authentication
```

no - This command disables the Authentication trap.

Default Setting

Enabled

Command Mode

Global Config

This command enables the DVMRP trap.

Syntax

```
snmp-server enable traps dvmrp
no snmp-server enable traps dvmrp
```

no - This command disables the DVMRP trap.

Default Setting

Enabled

Command Mode

Global Config

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).

Syntax

```
snmp-server enable traps linkmode
no snmp-server enable traps linkmode
```

no - This command disables Link Up/Down traps for the entire switch.

Default Setting

Enabled

Command Mode

Global Config

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.

Syntax

```
snmp-server enable traps multiusers
no snmp-server enable traps multiusers
```

no - This command disables Multiple User trap.

Default Setting

Enabled

Command Mode

Global Config

This command enables OSPF traps.

Syntax

```
snmp-server enable traps ospf {all | errors {all | authentication-failure | bad-packet | config-error | virtauthentication-failure | virt-bad-packet | virt-config-error} | if-rx {all | if-rx-packet} | lsa {all | lsa-maxage | lsa-originate} | overflow {all | lsdb-overflow | lsdb-approaching-overflow} | retransmit {all | packets | virt-packets} | rtb {all, rtb-entry-info} | state-change {all | if-state-change | neighbor-state-change | virtif-statechange | virtneighbor-state-change}}
no snmp-server enable traps ospf {all | errors {all | authentication-failure | bad-packet | config-error | virtauthentication-failure | virt-bad-packet | virt-config-error} | if-rx {all | if-rx-packet} | lsa {all | lsa-maxage | lsa-originate} | overflow {all | lsdb-overflow | lsdb-approaching-overflow} | retransmit {all | packets | virt-packets} | rtb {all, rtb-entry-info} | state-change {all | if-state-change | neighbor-state-change | virtif-statechange | virtneighbor-state-change}}
```

no - This command disables OSPF trap.

Default Setting

Enabled

Command Mode

Global Config

This command enables OSPFv3 traps.

Syntax

```
snmp-server enable traps ospfv3 {all | errors {all | authentication-failure | bad-packet | config-error | virtauthentication-failure | virt-bad-packet | virt-config-error} | if-rx {all | if-rx-packet} | lsa {all | lsa-maxage
```

virtauthentication-failure | virt-bad-packet | virt-config-error} | if-rx {all | if-rx-packet} | lsa {all | lsa-maxage | lsa-originate} | overflow {all | lsdb-overflow | lsdb-approaching-overflow} | retransmit {all | packets | virt-packets} | rtb {all, rtb-entry-info} | state-change {all | if-state-change | neighbor-state-change | virtif-statechange | virtneighbor-state-change}} no snmp-server enable traps ospfv3 {all | errors {all | authentication-failure | bad-packet | config-error | virtauthentication-failure | virt-bad-packet | virt-config-error} | if-rx {all | if-rx-packet} | lsa {all | lsa-maxage | lsa-originate} | overflow {all | lsdb-overflow | lsdb-approaching-overflow} | retransmit {all | packets | virt-packets} | rtb {all, rtb-entry-info} | state-change {all | if-state-change | neighbor-state-change | virtif-statechange | virtneighbor-state-change}}

no - This command disables OSPFv3 trap.

Default Setting

Enabled

Command Mode

Global Config

This command enables PIM traps.

Syntax

snmp-server enable traps pim no snmp-server enable traps pim

no - This command disables PIM trap.

Default Setting

Enabled

Command Mode

Global Config

This command enables the sending of new root traps and topology change notification traps.

Syntax

snmp-server enable traps stpmode no snmp-server enable traps stpmode

no - This command disables the sending of new root traps and topology change notification traps.

Default Setting

Enabled

Command Mode

Global Config

7.3.6 SNMP Trap Commands

7.3.6.1 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.

Syntax
show snmptrap

Default Setting

None

Command Mode

Privileged Exec

Display Message

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.

SNMP Version: The trap version to be used by the receiver.

SNMP v1 – Uses SNMP v1 to send traps to the receiver.

SNMP v2 – Uses SNMP v2 to send traps to the receiver.

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.

7.3.6.2 snmptrap snmpversion

This command configures the version for snmp trap.

Syntax

```
snmptrap snmpversion <name> <ipaddr> <snmpversion>
```

Default Setting

Snmpv2

Command Mode

Global Config

7.3.6.3 snmp trap link-status

This command enables link status traps by interface.

This command is valid only when the Link Up/Down Flag is enabled. See ‘snmpserver enable traps linkmode’ command.

Syntax

```
snmp trap link-status
no snmp trap link-status
```

no - This command disables link status traps by interface.

Default Setting

Disabled

Command Mode

Interface Config

This command enables link status traps for all interfaces.

This command is valid only when the Link Up/Down Flag is enabled. See ‘snmpserver enable traps linkmode’ command.

Syntax

```
snmp trap link-status all
no snmp trap link-status all
```

all - All interfaces.

no - This command disables link status traps for all interfaces.

Default Setting

Disabled

Command Mode

Global Config

7.3.6.4 snmptrap <name> ipaddr <ipaddr> <snmpversion>

This command adds an SNMP trap name. The maximum length of the name is 16 case-sensitive alphanumeric characters.

Syntax

```
snmptrap <name> ipaddr <ipaddr> <snmpversion>
no snmptrap <name> <ipaddr> <snmpversion>
```

<name> - SNMP trap name (Range: up to 16 case-sensitive alphanumeric characters).

<ipaddr> - an IP address of the trap receiver.

<snmpversion> - SNMP trap version.

no - This command deletes trap receivers for a community.

Default Setting

None

Command Mode

Global Config

7.3.6.5 snmptrap ipaddr <name> <ipaddr> <ipaddrnew>

This command changes the IP address of the trap receiver for the specified community name. The maximum length of name is 16 case-sensitive alphanumeric characters.

i IP addresses in the SNMP trap receiver table must be unique for the same community name. If you make multiple entries using the same IP address and community name, the first entry is retained and processed. All duplicate entries are ignored.

Syntax

```
snmptrap ipaddr <name> <ipaddr> <ipaddrnew>
```

<name> - SNMP trap name.

<ipaddr> - an original IP address.

<ipaddrnew> - a new IP address.

Default Setting

None

Command Mode

Global Config

7.3.6.6 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).

Syntax

```
snmptrap mode <name> <ipaddr>
no snmptrap mode <name> <ipaddr>
```

<name> - SNMP trap name.

<ipadd> - an IP address.

no - This command deactivates an SNMP trap. Trap receivers are inactive (not able to receive traps).

Default Setting

None

Command Mode

Global Config

7.3.7 HTTP commands

7.3.7.1 show ip http

This command displays the http settings for the switch.

Syntax

```
show ip http
```

Default Setting

None

Command Mode

Privileged Exec

Display Message

HTTP Mode (Unsecure): This field indicates whether the HTTP mode is enabled or disabled.

HTTP Port: This field specifies the port configured for HTTP.

HTTP Mode (Secure): This field indicates whether the administrative mode of secure HTTP is enabled or disabled.

Secure Port: This field specifies the port configured for SSLT.

Secure Protocol Level(s): The protocol level may have the values of SSL3, TSL1, or both SSL3 and TSL1.

Hard-timeout: Display the hard timeout for secure HTTP sessions in hours.

Soft-timeout: Display the soft timeout for HTTP sessions in minutes.

Max-sessions: Display the number of allowable HTTP sessions.

Secure-hard-timeout: Display the hard timeout for secure HTTP sessions in hours.

Secure-soft-timeout: Display the soft timeout for HTTP sessions in minutes.

Secure-max-sessions: Display the number of allowable HTTP sessions.

7.3.7.2 ip javamode

This command specifies whether 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.

Syntax

```
ip javamode
no ip javamode
```

no - 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.

Default Setting

Enabled

Command Mode

Global Config

7.3.7.3 ip http port

This command is used to set the http port where port can be 1-65535 and the default is port 80.

Syntax

```
ip http port <1-65535>
no ip http port
```

<1-65535> - HTTP Port value.

no - This command is used to reset the http port to the default value.

Default Setting

80

Command Mode

Global Config

7.3.7.4 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 affected.

Syntax

```
ip http server
no ip http server
```

no - 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 Setting

Enabled

Command Mode

Global Config

7.3.7.5 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.

Syntax

```
ip http secure-port <portid>
```

```
no ip http secure-port
```

<portid> - SSLT Port value.

no - This command is used to reset the SSLT port to the default value.

Default Setting

443

Command Mode

Global Config

7.3.7.6 ip http secure-server

This command is used to enable the secure socket layer for secure HTTP.

Syntax

```
ip http secure-server
no ip http secure-server
```

no - This command is used to disable the secure socket layer for secure HTTP.

Default Setting

Disabled

Command Mode

Global Config

7.3.7.7 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.

Syntax

```
ip http secure-protocol <protocollevel1> [protocollevel2]
no ip http secure-protocol <protocollevel1> [protocollevel2]
```

<protocollevel1 - 2> - The protocol level can be set to TLS1, SSL3 or to both TLS1 and SSL3.

no - This command is used to remove protocol levels (versions) for secure HTTP.

Default Setting

SSL3 and TLS1

Command Mode

Global Config

7.3.8 Secure Shell (SSH) Commands

7.3.8.1 show ip ssh

This command displays the SSH settings.

Syntax
show ip ssh

Default Setting

None

Command Mode

Privileged Exec

Display Message

Administrative Mode: This field indicates whether the administrative mode of SSH is enabled or disabled.

Protocol Levels: The protocol level may have the values of version 1, version 2, or both versions.

SSH Sessions Currently Active: This field specifies the current number of SSH connections.

Max SSH Sessions Allowed: The maximum number of inbound SSH sessions allowed on the switch.

SSH Timeout: This field is the inactive timeout value for incoming SSH sessions to the switch.

Keys Present: Indicates whether the SSH RSA and DSA key files are present on the device.

Key Generation in Progress: Indicates whether RSA or DSA key files generation is currently in progress.

7.3.8.2 ip ssh

This command is used to enable SSH.

Syntax
ip ssh no ip ssh

no - This command is used to disable SSH.

Default Setting

Disabled

Command Mode

Global Config

7.3.8.3 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.

Syntax

```
ip ssh protocol <protocollevel1> [protocollevel2]
```

<protocollevel1 - 2> - The protocol level can be set to SSH1, SSH2 or to both SSH 1 and SSH 2.

Default Setting

SSH1 and SSH2

Command Mode

Global Config

7.3.8.4 ip ssh maxsessions

This command specifies the maximum number of SSH connection sessions that can be established. A value of 0 indicates that no ssh connection can be established. The range is 0 to 5.

Syntax

```
ip ssh maxsessions <0-5>
no ip ssh maxsessions
```

<0-5> - maximum number of sessions.

no - This command sets the maximum number of SSH connection sessions that can be established to the default value.

Default Setting

SSH1 and SSH2

Command Mode

Global Config

7.3.8.5 ip ssh timeout

This command sets the SSH 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. 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.

Syntax

```
ip ssh timeout <1-160>
no ip ssh timeout
```

<1-160> - timeout interval in seconds.

no - This command sets the SSH connection session timeout value, in minutes, to the default. 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 Setting

5

Command Mode

Global Config

7.3.9 Management Security Commands

7.3.9.1 crypto certificate generate

This commands is used to generation self-signed certificate for HTTPS.

Syntax

```
crypto certificate generate
no crypto certificate generate
```

no- This command is used to delete the HTTPS certificate file from the device, regardless of whether they are self-signed or download from an outside source.

Default Setting

None

Command Mode

Global Config

7.3.9.2 crypto key generate

This command is used to generate an RSA or DSA key pair for SSH.

Syntax

```
crypto key generate {RSA | DSA}
no crypto key generate {RSA | DSA}
```

no- This command is used to delete the RSA or DSA key from the device.

Default Setting

None

Command Mode

Global Config

7.3.10 DHCP Client Commands

7.3.10.1 ip dhcp restart

This command is used to initiate a BOOTP or DCHP client request.

Syntax

```
ip dhcp restart
```

Default Setting

None

Command Mode

Global Config

7.3.10.2 ip dhcp client-identifier

This command is used to specify the DCHP client identifier for this switch. Use the **no** form to restore to default value.

Syntax

```
ip dhcp client-identifier {text <text> | hex <hex>}
no ip dhcp client-identifier
```

<text> - A text string. (Range: 1-32 characters).

<hex> - The hexadecimal value (00:00:00:00:00:00).

no - This command is used to restore to default value.

Default Setting

System Burned In MAC Address

Command Mode

Global Config

7.3.11 DHCPv6 Client Commands

7.3.11.1 ipv6 address protocol

This command specifies the network of IPv6 configuration protocol to be used . If you modify this value, the change is effective immediately.

Syntax

```
ipv6 address protocol {dhcp6 | none}
```

<dhcp6> - Obtains IPv6 address from DHCPv6.

<none> - Obtains IPv6 address by setting configuration.

Default Setting

None

Command Mode

Interface-Vlan Config

7.3.11.2 ipv6 dhcp restart

This command is used to initiate a DHCPv6 client request by the network interface.

Syntax

```
ipv6 dhcp6 restart
```

Default Setting

None

Command Mode

Global Config

7.3.11.3 serviceport protocol

This command specifies the oob configuration protocol to be used. If you modify this value, the change is effective immediately.

Syntax

```
serviceport protocol {bootp | dhcp | dhcp6 | none [dhcp6]}
```

<bootp> - Obtains IP address from BOOTP.

<dhcp> - Obtains IP address from DHCP.

<dhcp6> - Obtains IPv6 address from DHCPv6.

<none> - Obtains IP address by setting configuration.

<none dhcp6> - Obtains IPv6 address by setting configuration.

Default Setting

None

Command Mode

Global Config

7.3.11.4 serviceport protocol dhcp6 restart

This command is used to initiate a DHCPv6 client request by oob interface.

Syntax

```
serviceport protocol dhcp6 restart
```

Default Setting

None

Command Mode

Global Config

7.3.12 DHCP Relay Commands

7.3.12.1 show bootpdhcprelay

This command is used to display the DHCP relay agent configuration information on the system.

Syntax

```
show bootpdhcprelay
```

Default Setting

None

Command Mode

Privileged Exec

Display Message

Maximum Hop Count - The maximum number of Hops a client request can go without being discarded.

Minimum Wait Time (Seconds) - 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.

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.

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.

7.3.12.2 bootpdhcprelay maxhopcount

This command is used to set the maximum relay agent hops for BootP/DHCP Relay on the system.

Syntax

```
bootpdhcprelay maxhopcount <1-16>
no bootpdhcprelay maxhopcount
```

<1-16> - maximum number of hops. (Range: 1-16).

no - This command is used to reset to the default value.

Default Setting

4

Command Mode

Global Config

7.3.13 sFlow Commands

7.3.13.1 show sflow agent

The user can go to the CLI Privilege Exec to get the sFlow agent information, use the **show sflow agent** Privilege command.

Syntax
show sflow agent

Default Setting

None

Command Mode

Privilege Exec

Display Message

sFlow Version: Uniquely identifies the version and implementation of this MIB.

IP Address: The IP address associated with this agent.

7.3.13.2 show sflow pollers

The user can go to the CLI Privilege Exec to get the sFlow polling instances created on the switch, use the **show sflow pollers** Privilege command.

Syntax
show sflow pollers

Default Setting

None

Command Mode

Privilege Exec

Display Message

Poller Data Source: The sFlowDataSource (slot/port) for this sFlow sampler. This agent will support Physical ports only.

Receiver Index: The sFlowReceiver associated with this sFlow counter poller.

Poller Interval: The number of seconds between successive samples of the counters associated with this data source.

7.3.13.3 show sflow receivers

The user can go to the CLI Privilege Exec to get the configuration information related to the sFlow receivers, use the **show sflow receivers** Privilege command.

Syntax
show sflow receivers

Default Setting

None

Command Mode

Privilege Exec

Display Message

Receiver Index: The sFlow Receiver associated with the sampler/poller.

Owner String: The identity string for receiver, the entity making use of this sFlowRcvrTable entry.

Time Out: The time (in seconds) remaining before the receiver is released and stops sending samples to sFlow receiver.

Max Datagram Size: The maximum number of bytes that can be sent in a single sFlow datagram.

Port: The destination Layer4 UDP port for sFlow datagrams.

IP Address: The sFlow receiver IP address.

7.3.13.4 show sflow samplers

The user can go to the CLI Privilege Exec to get the sFlow sampling instances created on the switch, use the **show sflow samplers** Privilege command.

Syntax
show sflow samplers

Default Setting

None

Command Mode

Privilege Exec

Display Message

Sampler Data Source: The sFlowDataSource (slot/port) for this sFlow sampler. This agent will support Physical ports only.

Receiver Index: The sFlowReceiver configured for this sFlow sampler.

Packet Sampling Rate: The statistical sampling rate for packet sampling from this source.

Max Header Size: The maximum number of bytes that should be copied from a sampled packet to form a flow sample.

7.3.13.5 set sflow rate

The user can go to the CLI Interface Configuration Mode to set sampling rate, use the **sflow rate <0-3600>** interface configuration command. Use the **no sflow rate** return to default value zero.

Syntax
sflow rate <0-3600> no sflow rate

Default Setting

0

Command Mode

Global Config

7.3.13.6 set sflow maximum header size

The user can go to the CLI Interface Configuration Mode to set maximum header size, use the **sflow maximum-header <20-256>** interface configuration command. Use the **no sflow maximum-header** return to default value 128.

Syntax
sflow sampler maxheadersize <20-256> no sflow sampler maxheadersize

Default Setting

128

Command Mode

Interface Config

7.3.13.7 set sflow maximum datagram size

The user can go to the CLI Global Configuration Mode to set maximum datagram size, use the **sflow receiver <index> maxdatagram <200-9116>** global configuration command. Use the **no sflow receiver <index> maxdatagram** return to default value 1400.

Syntax

```
sflow receiver <index> maxdatagram <200-9116>
no sflow receiver <index> maxdatagram
```

Default Setting

1400

Command Mode

Global Config

7.3.13.8 set sflow receiver address

The user can go to the CLI Global Configuration Mode to set receiver ip address, use the **sflow receiver <index> ip <ip>** global configuration command. Use the **no sflow receiver <index> ip** to clear collector ip address.

Syntax

```
sflow receiver <index> ip <ip>
no sflow receiver <index> ip
```

Default Setting

None

Command Mode

Global Config

7.3.13.9 set sflow receiver port

The user can go to the CLI Global Configuration Mode to set collector UDP port, use the **sflow receiver <index> port <1-65535>** global configuration command. Use the **no sflow collector-port** return to default UDP port 6343.

Syntax

```
sflow receiver <index> port <1-65535>
no sflow receiver <index> port
```

Default Setting

6343

Command Mode

Global Config

7.3.13.10 set sflow interval

The user can go to the CLI Interface Configuration Mode to set polling interval, use the **sflow poller interval <0-86400>** interface configuration command. Use the **no sflow poller interval** return to default value zero.

Syntax

```
sflow poller interval <0-86400>
no sflow poller interval
```

Default Setting

0

Command Mode

Interface Config

7.3.13.11 set sflow sampler index

The user can go to the CLI Interface Configuration Mode to configure a new sFlow sampler instance, use the **sflow sampler <index>** interface configuration command. Use the **no sflow sampler** return to default setting.

Syntax

```
sflow sampler <index>
no sflow sampler
```

Default Setting

None

Command Mode

Interface Config

7.3.13.12 set sflow poller index

The user can go to the CLI Interface Configuration Mode to configure a new sFlow poller instance, use the **sflow poller <index>** interface configuration command. Use the **no sflow poller** return to default setting.

Syntax

```
sflow poller <index>
no sflow poller
```

Default Setting

None

Command Mode

Interface Config

7.3.14 Service Port Commands

7.3.14.1 show serviceport

This command displays service port configuration information.

Syntax

```
show serviceport
```

Default Setting

None

Command Mode

Privileged Exec

Display Message

Interface Status: Indicates whether the interface is up or down.

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.

IPv6 Administrative Mode: Whether enabled or disabled. Default value is enabled.

IPv6 Address/Length: The IPv6 address and length. Default is Link Local format.

IPv6 Default Router: The default gateway address on the service port. The factory default value is an unspecified address.

ServPort Configured Protocol Current: Indicates what network protocol was used on thelast, or current power-up cycle, if any.

Burned In MAC Address: The burned in MAC address used for in-band connectivity.

7.3.14.2 show serviceport ndp

This command displays IPv6 Neighbor entries.

Syntax
show serviceport ndp

Default Setting

None

Command Mode

Privileged Exec

Display Message

IPv6 Address: Specifies the IPv6 address of neighbor or interface.

MAC Address: Specifies MAC address associated with an interface.

isRr:. Specifies router flag.

Neighbor State:

Incmp - Address resolution is being performed on the entry. A neighbor solicitation message has been sent to the solicited-node multicast address of the target, but the corresponding neighbor advertisement message has not yet been received.

Reach - Positive confirmation was received within the last Reachable Time milliseconds that the forward path to the neighbor was functioning properly. While in REACH state, the device takes no special action as packets are sent.

Stale - More than ReachableTime milliseconds have elapsed since the last positive confirmation was received that the forward path was functioning properly. While in STALE state, the device takes no action until a packet is sent.

Delay - More than ReachableTime milliseconds have elapsed since the last positive confirmation was received that the forward path was functioning properly. A packet was sent within the last DELAY_FIRST_PROBE_TIME seconds. If no reachability confirmation is received within DELAY_FIRST_PROBE_TIME seconds of entering the DELAY state, send a neighbor solicitation message and change the state to PROBE.

Probe - A reachability confirmation is actively sought by resending neighbor solicitation messages every RetransTimer milliseconds until a reachability confirmation is received.

Age Updated: Time since the address was confirmed to be reachable.

7.3.14.3 serviceport ip

This command sets the IP address, the netmask and the gateway of the network management port.

Syntax

```
serviceport ip <ipaddr> <netmask>
```

<ipaddr> - The user manually configures IP address for this switch.

<netmask> - The user manually configures Subnet Mask for this switch.

Default Setting

None

Command Mode

Global Config

7.3.14.4 serviceport protocol

This command specifies the network management port configuration protocol. If you modify this value, the change is effective immediately. If you use the bootp parameter, the switch periodically sends requests to a BootP server until a response is received. If you use the dhcp parameter, the switch periodically sends requests to a DHCP server until a response is received. If you use the none parameter, you must configure the network information for the switch manually.

Syntax

```
serviceport protocol {none | bootp | dhcp | dhcp6}
```

none - Configure the network information for the switch manually.

bootp - Periodically sends requests to a BootP server until a response is received.

dhcp - Periodically sends requests to a DHCP server until a response is received.

dhcp6 - Periodically sends requests to a DHCPv6 server until a response is received.

Default Setting

None

Command Mode

Global Config

7.3.14.5 serviceport ipv6 enable

Use this command to enable IPv6 operation on the service port.

Syntax

```
serviceport ipv6 enable
no serviceport ipv6 enable
```

no - This command is disable IPv6 operation on the service port.

Default Setting

None

Command Mode

Global Config

7.3.14.6 serviceport ipv6 address

Use this command to configure IPv6 global addressing (i.e. Default routers) information for the service port.

Syntax

```
serviceport ipv6 address <address>/<prefix-length> [eui64]
no serviceport ipv6 address [<address>/<prefix-length>]
```

no - This command remove all IPv6 prefixes on the service port interface.

<address>: IPv6 prefix in IPv6 global address format.

<prefix-length>: IPv6 prefix length value.

[eui64]: Formulate IPv6 address in eui64 address format.

i Multiple IPv6 prefixes can be configured for the service port.

Default Setting

None

Command Mode

Global Config

7.3.14.7 serviceport ipv6 gateway

Use this command to configure IPv6 gateway (i.e. Default routers) information for the service port.

Syntax

```
serviceport ipv6 gateway <gateway-address>
no serviceport ipv6 gateway
```

<gateway-address>: Gateway address in IPv6 global or link-local address format.

no - This command remove IPv6 gateways on the service port interface.

i Only a single IPv6 gateway address can be configured for the service port. There may be a combination of IPv6 prefixes and gateways that are explicitly configured and those that are set through auto-address configuration with a connected IPv6 router on their service port interface.

Default Setting

None

Command Mode

Global Config

7.4 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.

7.4.1 Show Commands

7.4.1.1 show spanning-tree

This command displays spanning tree settings for the common and internal spanning tree. The following details are displayed.

Syntax

```
show spanning-tree
```

Default Setting

None

Command Mode

Privileged Exec

Display Message

Bridge Priority: Configured value.

Bridge Identifier: The MAC Address for the Bridge from which the Bridge Identifiers used by the Spanning Tree Algorithm and Protocol.

Time Since Topology Change: In seconds.

Topology Change Count: Number of times changed.

Topology Change in progress: 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: The Bridge Identifier of the Root Bridge for the spanning tree instance identified by the MSTID.

Root Path Cost: Value of the Root Path Cost parameter for the common and internal spanning tree.

Root Port Identifier: The Root Port for the spanning tree instance identified by the MSTID.

Bridge Max Age: Maximum message age.

Bridge Max Hops: The maximum number of hops for the spanning tree.

Max Tx Hold Count: The max value of bridge tx hold count for the spanning tree.

Bridge Forwarding Delay: A timeout value to be used by all Bridges in the Bridged LAN. The value of Forward Delay is set by the Root.

Hello Time: The time interval between the generations of Configuration BPDUs.

Bridge Hold Time: Minimum time between transmissions of Configuration Bridge Protocol Data Units (BPDUs).

CST Regional Root: The Bridge Identifier of the current CST Regional Root.

Regional Root Path Cost: The path cost to the regional root.

Associated FIDs: List of forwarding database identifiers currently associated with this instance.

Associated VLANs: List of VLAN IDs currently associated with this instance.

7.4.1.2 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.

Syntax
show spanning-tree interface <slot/port>

<slot/port> - is the desired interface number.

Default Setting

None

Command Mode

Privileged Exec

Display Message

Hello Time: The hello time value. Not Configured means using default value.

Port Mode: The administration mode of spanning tree.

BPDU Guard: Enabled or disabled.

ROOT Guard: Enabled or disabled.

LOOP Guard: Enabled or disabled.

TCN Guard: Enabled or disabled.

BPDU Filter Mode: Enabled or disabled.

BPDU Flood Mode: Enabled or disabled.

Auto Edge: True or false.

Port Up Time Since Counters Last Cleared: Time since the 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.

RSTP 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.

7.4.1.3 show spanning-tree vlan

This command displays the association between a VLAN and a multiple spanning tree instance. The <1-3965> corresponds to an existing VLAN ID.

Syntax

```
show spanning-tree vlan <1-3965>
```

<vlanid> - VLAN ID (Range: 1 - 3965).

Default Setting

None

Command Mode

Privileged Exec

Display Message

VLAN Identifier: displays VLAN ID.

Associated Instance: Identifier for the associated multiple spanning tree instance or "CST" if associated with the common and internal spanning tree.

7.4.1.4 show spanning-tree mst

This command displays settings and parameters for the specified multiple spanning tree instance. The instance <0-4094> is a number that corresponds to the desired existing multiple spanning tree instance ID. The following details are displayed.

Syntax

show spanning-tree mst detailed <0-4094>

<0-4094> - multiple spanning tree instance ID.

Default Setting

None

Command Mode

Privileged Exec

Display Message

MST Instance ID: The multiple spanning tree instance ID.

MST Bridge Priority: The bridge priority of current MST.

MST Bridge Identifier: The bridge ID of current MST.

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.

This command displays summary information about all multiple spanning tree instances in the switch. On execution, the following details are displayed.

Syntax

show spanning-tree mst summary

Default Setting

None

Command Mode

Privileged Exec

Display Message

MST Instance ID List: List of multiple spanning trees IDs currently configured.

For each MSTID*:* The multiple spanning tree instance ID.

Associated FIDs: List of forwarding database identifiers associated with this instance.

Associated VLANs: List of VLAN IDs associated with this instance.

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.

Syntax
show spanning-tree mst port detailed <0-4094> <slot/port>

<0-4094> - multiple spanning tree instance ID.

<slot/port> - is the desired interface number.

Default Setting

None

Command Mode

Privileged Exec

Display Message

MST Instance ID: The multiple spanning tree instance ID.

Port Identifier: The unique value to identify a port on that Bridge.

Port Priority: The priority of the port within the MST.

Port Forwarding State: Current spanning tree state of this port.

Port Role: Indicate the port role is root or designate.

Auto-calculate Port Path Cost: Indicate the port auto-calculate port path cost.

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 <0-4094>, 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.

Auto-calculate Port Path Cost: Indicate the port auto-calculate port path cost

Port Path Cost: The configured path cost for the specified interface.

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.

External Port Path Cost - The External Path Cost of the specified port in the spanning tree.

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.

Transitions Into Loop Inconsistent State: The count number of transitions into loop inconsistent state.

Transitions Out Of Loop Inconsistent State: The count number of transitions out of loop inconsistent state.

This command displays the settings of one or all ports within the specified multiple spanning tree instance. The parameter <0-4094> 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 <0-4094>, then the status summary is displayed for one or all ports within the common and internal spanning tree.

Syntax

show spanning-tree mst port summary <0-4094> {<slot/port> | all}

<0-4094> - multiple spanning tree instance ID.

<slot/port> - is the desired interface number.

all - All interfaces.

Default Setting

None

Command Mode

Privileged Exec

Display Message

MST Instance ID: The MST instance associated with this port.

Interface: The interface being displayed.

STP Mode: Indicate STP mode.

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.

Desc: The port in loop inconsistence state will display "*LOOP_Inc".

7.4.1.5 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.

Syntax
show spanning-tree summary

Default Setting

None

Command Mode

Privileged Exec

Display Message

Spanning Tree Adminmode: Enabled or disabled.

Spanning Tree Forward BPDU: 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.

BPDU Guard Mode:Enabled or disabled.

BPDU Filter Mode: Enabled or disabled.

BPDU Uplinkfast Mode: Enabled or disabled.

Configuration Name: TConfigured 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.

7.4.1.6 show spanning-tree brief

This command displays spanning tree settings for the bridge. In this case, the following details are displayed.

Syntax

show spanning-tree brief

Default Setting

None

Command Mode

Privileged Exec

Display Message

Bridge Priority: Configured value.

Bridge Identifier: The bridge ID of current Spanning Tree.

Bridge Max Age: Configured value.

Bridge Max Hops: 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).

7.4.2 Configuration Commands

7.4.2.1 spanning-tree

This command sets the spanning-tree operational mode to be enabled.

Syntax

spanning-tree
no spanning-tree

no - This command sets the spanning-tree operational mode to be disabled. While disabled, the spanning-tree configuration is retained and can be changed, but is not activated.

Default Setting

Disabled

Command Mode

Global Config

7.4.2.2 spanning-tree protocol-migration

This command enables BPDU migration check on a given interface. The **all** option enables BPDU migration check on all interfaces.

Syntax

```
spanning-tree protocol-migration {<slot/port> | all}
no spanning-tree protocol-migration {<slot/port> | all}
```

<slot/port> - is the desired interface number.

all - All interfaces.

no - This command disables BPDU migration check on a given interface. The **all** option disables BPDU migration check on all interfaces.

Default Setting

None

Command Mode

Global Config

7.4.2.3 spanning-tree configuration

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 alphanumeric characters.

Syntax

```
spanning-tree configuration name <name>
no spanning-tree configuration name
```

<name> - is a string of at most 32 alphanumeric characters.

no - This command resets the Configuration Identifier Name to its default.

Default Setting

The base MAC address displayed using hexadecimal notation as specified in IEEE 802 standard.

Command Mode

Global Config

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.

Syntax

```
spanning-tree configuration revision <0-65535>
no spanning-tree configuration revision
```

<value> - Revision Level is a number in the range of 0 to 65535.

no - This command sets the Configuration Identifier Revision Level for use in identifying the configuration that this switch is currently using to the default value, that is, 0.

Default Setting

0

Command Mode

Global Config

7.4.2.4 spanning-tree mode

This command sets the Force Protocol Version parameter to a new value. The Force Protocol Version can be one of the following:

1. stp - ST BPDUs are transmitted rather than MST BPDUs (IEEE 802.1d functionality supported)
2. rstp - RST BPDUs are transmitted rather than MST BPDUs (IEEE 802.1w functionality supported)
3. mstp - MST BPDUs are transmitted (IEEE 802.1s functionality supported)

Syntax

```
spanning-tree mode {stp | rstp | mstp}
no spanning-tree mode
```

no - This command sets the Force Protocol Version parameter to the default value, that is, mstp.

Default Setting

mstp

Command Mode

Global Config

7.4.2.5 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".

Syntax

```
spanning-tree forward-time <4-30>
no spanning-tree forward-time
```

<4-30> - forward time value (Range: 4 – 30).

no - This command sets the Bridge Forward Delay parameter for the common and internal spanning tree to the default value, that is, 15.

Default Setting

15

Command Mode

Global Config

7.4.2.6 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".

Syntax

```
spanning-tree hello-time <1-10>
no spanning-tree hello-time
```

<1-10> - hellotime value (Range: 1 – 10).

no - This command sets the Hello Time parameter for the common and internal spanning tree to the default value, that is, 2.

Default Setting

2

Command Mode

Global Config

7.4.2.7 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)" and greater than or equal to “2 times (Bridge Hello Time + 1)”.

Syntax

```
spanning-tree max-age <6-40>
no spanning-tree max-age
```

<6-40> - the Bridge Max Age value (Range: 6 – 40).

no - This command sets the Bridge Max Age parameter for the common and internal spanning tree to the default value, that is, 20.

Default Setting

20

Command Mode

Global Config

7.4.2.8 spanning-tree max-hops

This command sets the MSTP Max Hops parameter to a new value for the common and internal spanning tree. The max-hops value is in a range of 1 to 127.

Syntax

```
spanning-tree max-hops <1-127>
no spanning-tree max-hops
```

<1-127> - the Maximum hops value (Range: 1-127).

no - This command sets the Bridge Max Hops parameter for the common and internal spanning tree to the default value.

Default Setting

20

Command Mode

Global Config

7.4.2.9 spanning-tree hold-count

This command sets the Bridge Tx Hold Count parameter to a new value for the common and internal spanning tree. The Tx Hold Count value is in a range of 1 to 110.

Syntax

```
spanning-tree hold-count <1-10>
no spanning-tree hold-count
```

<1-10> - the Maximum hold-count value (Range: 1-110).

no - This command sets the Bridge Tx Hold Count parameter for the common and internal spanning tree to the default value.

Default Setting

6

Command Mode

Global Config

7.4.2.10 spanning-tree mst

This command adds a multiple spanning tree instance to the switch. The instance <1-3965> is a number within a range of 1 to 3965 that corresponds to the new instance ID to be added. The maximum number of multiple instances supported is 4.

Syntax

```
spanning-tree mst instance <1-4094>
no spanning-tree mst instance <1-4094>
```

<1-4094> - multiple spanning tree instance ID.

no - 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 <1-4094> is a number that corresponds to the desired existing multiple spanning tree instance to be removed.

Default Setting

None

Command Mode

Global Config

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.

Syntax

```
spanning-tree mst priority <0-4094> <0-61440>
no spanning-tree mst priority <0-4094>
```

<0-4094> - multiple spanning tree instance ID.

<0-61440> - priority value (Range: 0 – 61440).

no - This command sets the bridge priority for a specific multiple spanning tree instance to the default value, that is, 32768. The instance <0-4094> 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 <0-4094>, then this command sets the Bridge Priority parameter for the common and internal spanning tree to the default value, that is, 32768.

Default Setting

32768

Command Mode

Global Config

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 <0-4094> is a number that corresponds to the desired existing multiple spanning tree instance. The <1-3965> corresponds to an existing VLAN ID.

Syntax

```
spanning-tree mst vlan <0-4094> <1-3965>
no spanning-tree mst vlan <0-4094> <1-3965>
```

<0-4094> - multiple spanning tree instance ID.

<1-3965> - VLAN ID (Range: 1 – 3965).

no - 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 <0-4094> is a number that corresponds to the desired existing multiple spanning tree instance. The <1-3965> corresponds to an existing VLAN ID.

Default Setting

None

Command Mode

Global Config

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 <1-4094> 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 <1-4094>, 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 <1-4094> 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.

Syntax

```
spanning-tree mst <1-4094> cost {<1-200000000> | auto}
no spanning-tree mst <1-4094> cost
```

<1-4094> - multiple spanning tree instance ID.

no - 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 <1-4094> 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 <1-4094>, 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 <1-4094> parameter, to the default value, that is, a pathcost value based on the Link Speed.

Default Setting

Cost : auto

Command Mode

Interface Config

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 <1-4094> 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 <1-4094>, then the configurations are performed for the common and internal spanning tree instance.

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 <1-4094> parameter. The port-priority value is a number in the range of 0 to 240 in increments of 16.

Syntax

spanning-tree mst <1-4094> port-priority <0-240>
no spanning-tree mst <1-4094> port-priority

<1-4094> - multiple spanning tree instance ID.

no - 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 <1-4094> 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 <1-4094>, then the configurations are performed for the common and internal spanning tree instance.

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 <1-4094> parameter, to the default value, that is, 128.

Default Setting

port-priorty : 128

Command Mode

Interface Config

7.4.2.11 spanning-tree port mode

This command sets the Administrative Switch Port State for this port to enabled.

Syntax

spanning-tree port mode
no spanning-tree port mode

no - This command sets the Administrative Switch Port State for this port to disabled.

Default Setting

Disabled

Command Mode

Interface Config

This command sets the Administrative Switch Port State for all ports to enabled.

Syntax

```
spanning-tree port mode all
no spanning-tree port mode all
```

all - All interfaces.

no - This command sets the Administrative Switch Port State for all ports to disabled.

Default Setting

Disabled

Command Mode

Global Config

7.4.2.12 spanning-tree auto-edge

This command sets the auto-edge for this port to enabled.

Syntax

```
spanning-tree auto-edge
no spanning-tree auto-edge
```

no - This command sets the auto-edge for this port to disabled.

Default Setting

Disabled

Command Mode

Interface Config

7.4.2.13 spanning-tree edgeport

This command sets the edguport function to Enabled or Disabled on this switch.

Syntax

```
spanning-tree edgeport
no spanning-tree edgeport
```

no - This command sets the Edgeport function to the default value, that is Enabled.

Default Setting

Enabled

Command Mode

Global Config

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.

Syntax

```
spanning-tree edgeport
no spanning-tree edgeport
```

no - This command specifies that this port is not an Edge Port within the common and internal spanning tree.

Default Setting

None

Command Mode

Interface Config

This command sets the Edgeport BPDU Filter enable/disable parameter for sending/receiving BPDUs on this switch. This command only works on dot1d mode.

Syntax

```
spanning-tree edgeport bpdufilter
no spanning-tree edgeport bpdufilter
```

no - This command sets the Edgeport BPDU Filter to the default value, that is Disabled.

Default Setting

Disabled

Command Mode

Global Config

This command sets the Edgeport BPDU Guard enable/disable parameter for accepting BPDUs on this switch. This command only works on dot1d mode.

Syntax

```
spanning-tree edgeport bpduguard
no spanning-tree edgeport bpduguard
```

no - This command sets the Edgeport BPDU Guard to the default value, that is, Disabled.

Default Setting

Disabled

Command Mode

Global Config

This command sets the Edgeport BPDU Filter enable/disable parameter for sending/receiving BPDUs on this interface. This command only works on dot1d mode.

Syntax

```
spanning-tree bpdufilter
no spanning-tree bpdufilter
```

no - This command sets the Edgeport BPDU Filter to the default value, that is Disabled.

Default Setting

Disabled

Command Mode

Interface Config

This command sets the Edgeport BPDU Guard enable/disable parameter for accepting BPDUs on this interface. This command only works on dot1d mode.

Syntax

```
spanning-tree bpduguard
no spanning-tree bpduguard
```

no - This command sets the Edgeport BPDU Guard to the default value, that is, Disabled.

Default Setting

Disabled

Command Mode

Interface Config

7.4.2.14 spanning-tree uplinkfast

This command sets the Uplink Fast parameter to a new value on this switch. This command only works on dot1d mode.

Syntax
spanning-tree uplinkfast no spanning-tree uplinkfast

no - This command sets the Uplink Fast parameter to the default value, that is Disabled.

Default Setting

Disabled

Command Mode

Global Config

7.4.2.15 spanning-tree guard {loop|none|root}

This command sets the Guard Mode parameter to a new value on this interface.

Syntax
spanning-tree guard {loop|none|root} no spanning-tree guard

loop –This command sets the Guard Mode to loop guard on this interface.

none –This command sets the Guard Mode to none.

root – This command sets the Guard Mode to root guard on this interface.

no - This command sets the Guard Mode to the default value, that is none.

Default Setting

None

Command Mode

Interface Config

7.4.2.16 spanning-tree tcnguard

This command sets the TCN Guard parameter to prevent a port from propagating topology change notifications.

Syntax

```
spanning-tree tcnguard
no spanning-tree tcnguard
```

no - This command sets the tcnguard parameter to the default value, that is Disabled.

Default Setting

Disabled

Command Mode

Interface Config

7.5 System Log Management Commands

7.5.1 Show Commands

7.5.1.1 show logging

This command displays logging.

Syntax

```
show logging
```

Default Setting

None

Command Mode

Privileged Exec

Display Message

Logging Client Local Port The port on the collector/relay to which syslog messages are sent

CLI Command Logging The mode for CLI command logging.

Console Logging The mode for console logging.

Console Logging Severity Filter The minimum severity to log to the console log. Messages with an equal or lower numerical severity are logged.

Buffered Logging The mode for buffered logging.

Syslog Logging The mode for logging to configured syslog hosts. If set to disable logging stops to all syslog hosts.

Terminal Monitor The mode for terminal logging.

Terminal Logging Severity Filter The minimum severity to log to the terminal log. Messages with an equal or lower numerical severity are logged.

Log Messages Received The number of messages received by the log process. This includes messages that are dropped or ignored

Log Messages Dropped The number of messages that could not be processed.

Log Messages Relayed The number of messages that are relayed.

7.5.1.2 show logging buffered

This command displays the message log maintained by the switch. The message log contains system trace information.

Syntax

show logging buffered

Default Setting

None

Command Mode

Privileged Exec

Display Message

Message: The message that has been logged.

i Message log information is not retained across a switch reset.

7.5.1.3 show logging traplog

This command displays the trap log maintained by the switch.

The trap log contains a maximum of 256 entries that wrap.

Syntax

show logging traplogs

Default Setting

None

Command Mode

Privileged Exec

Display Message

Number of Traps since last reset: The number of traps that have occurred since the last reset of this device.

Trap Log Capacity: The maximum number of traps that could be stored in the switch.

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.

Trap log information is not retained across a switch reset.

7.5.1.4 show logging hosts

This command displays all configured logging hosts.

Syntax
show logging hosts

Default Setting

None

Command Mode

Privileged Exec

Display Message

Index: used for deleting.

IP Address:IP Address of the configured server.

Severity: The minimum severity to log to the specified address.

Port Server Port Number:This is the port on the local host from which syslog messages are sent.

Status: The state of logging to configured syslog hosts. If the status is disable, no logging occurs.

7.5.2 Configuration Commands

7.5.2.1 logging buffered

This command enables logging to in-memory log where up to 128 logs are kept.

Syntax

```
logging buffered
no logging buffered
```

no - This command disables logging to in-memory log.

Default Setting

None

Command Mode

Global Config

This command enables wrapping of in-memory logging when full capacity reached. Otherwise when full capacity is reached, logging stops.

Syntax

```
logging buffered wrap
no logging buffered wrap
```

no - This command disables wrapping of in-memory logging when full capacity reached.

Default Setting

None

Command Mode

Global Config

7.5.2.2 logging console

This command enables logging to the console.

Syntax

```
logging console [<severitylevel> | <0-7>]
no logging console
```

[<severitylevel> | <0-7>] - The value is specified as either an integer from 0 to 7 or symbolically through one of the following keywords: emergency (0), alert (1), critical (2), error (3), warning (4), notice (5), informational (6), debug (7).

no - This command disables logging to the console.

Default Setting

None

Command Mode

Global Config

7.5.2.3 logging monitor

This command enables logging to the terminal monitor.

Syntax

```
logging console [<severitylevel> | <0-7>]
no logging console
```

[<severitylevel> | <0-7>] - The value is specified as either an integer from 0 to 7 or symbolically through one of the following keywords: emergency (0), alert (1), critical (2), error (3), warning (4), notice (5), informational (6), debug (7).

no - This command disables logging to the terminal monitor.

Default Setting

None

Command Mode

Globla Config

7.5.2.4 terminal monitor

This command enables logging for the terminal session.

Syntax

```
terminal monitor
no terminal monitor
```

no - This command disables logging for the terminal session.

Default Setting

None

Command Mode

Privileged Exec

7.5.2.5 logging host

This command enables logging to a host where up to eight hosts can be configured.

Syntax

logging host <hostaddress> [<port>] [[<severitylevel> | <0-7>]]

<hostaddress> - IP address of the log server.

<port> - Port number.

[<severitylevel> | <0-7>] - The value is specified as either an integer from 0 to 7 or symbolically through one of the following keywords: emergency (0), alert (1), critical (2), error (3), warning (4), notice (5), informational (6), debug (7).

Default Setting

None

Command Mode

Globla Config

This command disables logging to hosts.

Syntax

logging host remove <hostindex>

<hostindex> - Index of the log server.

Default Setting

None

Command Mode

Globla Config

This command reconfigures the IP address of the log server.

Syntax

```
logging host reconfigure <hostindex> <hostaddress>
```

<hostindex> - Index of the log server.

<hostaddress> - New IP address of the log server.

Default Setting

None

Command Mode

Globla Config

7.5.2.6 logging syslog

This command enables syslog logging.

Syntax

```
logging syslog
no logging syslog
```

no - Disables syslog logging.

Default Setting

None

Command Mode

Globla Config

This command sets the local port number of the LOG client for logging messages.

Syntax

```
logging syslog port <portid>
no logging syslog port
```

no - Resets the local logging port to the default.

Default Setting

None

Command Mode

Globla Config

7.5.2.7 clear logging buffered

This command clears all in-memory log.

Syntax

clear logging buffered

Default Setting

None

Command Mode

Privileged Exec

7.6 Script Management Commands

7.6.1 script apply

This command applies the commands in the configuration script to the switch. The apply command backs up the running configuration and then starts applying the commands in the script file. Application of the commands stops at the first failure of a command.

Syntax

script apply <scriptname>

<scriptname> - The name of the script to be applied.

Default Setting

None

Command Mode

Privileged Exec

7.6.2 script delete

This command deletes a specified script or all the scripts presented in the switch.

Syntax

script delete {<scriptname> | all}

<scriptname> - The name of the script to be deleted.

all - Delete all scripts presented in the switch.

Default Setting

None

Command Mode

Privileged Exec

7.6.2.1 script list

This command lists all scripts present on the switch as well as the total number of files present.

Syntax

script list

Default Setting

None

Command Mode

Privileged Exec

Display Message

Configuration Script Name: The filename of the script file.

Size(Bytes): The size of the script file.

7.6.3 script show

This command displays the content of a script file.

Syntax

script show <scriptname>

<scriptname> - Name of the script file.

Default Setting

None

Command Mode

Privileged Exec

7.6.4 script validate

This command displays the content of a script file.

Syntax
script validate <scriptname>

<scriptname> - Name of the script file.

Default Setting

None

Command Mode

Privileged Exec

7.7 User Account Management Commands

7.7.1 Show Commands

7.7.1.1 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.

Syntax
show users

Default Setting

None

Command Mode

Privileged Exec

Display Message

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.

User 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, admin has Read/Write access and 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 from 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.

7.7.1.2 show users account information

The user can go to the CLI Privilege Exec to get all of user information, use the **show users accounts** Privilege command.

Syntax
show users accounts

Default Setting

None

Command Mode

Privileged Exec

Display Message

User Name: The local user account's user name.

Access Mode: The user's access level (read-only or read/write).

Lockout Status: Indicates whether the user account is locked out (true or false).

Password Expiration Date: The current password expiration date in date format.

7.7.1.3 show passwords configuration

Use this command to display the configured password management settings.

Syntax

show passwords configuration

Default Setting

None

Command Mode

Privileged Exec

Display Message

Minimum Password Length: Minimum number of characters required when changing passwords**.**

Password History: Number of passwords to store for reuse prevention.

Password Aging: Length in days that a password is valid.

Lockout Attempts: Number of failed password login attempts before lockout.

7.7.2 Configuration Commands

7.7.2.1 username

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.

This command changes the password of an existing operator. User password should not be more than eight characters in length. If a user is authorized for authentication or encryption is enabled, the password must be eight alphanumeric characters in length. The username and password are not case-sensitive. When a password is changed, a prompt will ask for the operator’s former password. If none, press enter.

Syntax

username <username> {password <0|7> <password> | nopassword}
no username <username>

<username> - is a new user name (Range: up to 8 characters).

<0|7> - 0 means the password is plain-text. 7 means the password is encrypted.

no - This command removes a user name created before.

nopassword - 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.

i The admin user account cannot be deleted.

Default Setting

No password

Command Mode

Global Config

7.7.2.2 Unlock a locked user account

The user can go to the CLI Global Configuration Mode to unlock a locked user account, use the **username <name> unlock** global configuration command.

Syntax

username <username> unlock

<name> - is a user name (Range: up to 8 characters).

Default Setting

None

Command Mode

Global Config

7.7.2.3 username 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 will be used as the snmpv3 authentication password. The <username> is the login user name for which the specified authentication protocol will be used.

Syntax

username snmpv3 authentication <username> {none | md5 | sha}
no username snmpv3 authentication <username>

<username> - is the login user name.

md5 - md5 authentication method.

sha - sha authentication method.

none - no use authentication method.

no - 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.

Default Setting

No authentication

Command Mode

Global Config

7.7.2.4 username snmpv3 encryption

This command specifies the encryption protocol and key to be used for the specified login user. The valid encryption protocols are **none** or **des**. The **des** protocol requires a **key**, which can be specified on the command line. The **key** may be up to 16 characters. If the **des** protocol is specified but a key is not provided, the user will be prompted to enter the key. If **none** is specified, a key must not be provided. The <username> is the login user name for which the specified encryption protocol will be used.

Syntax

```
username snmpv3 encryption <username> {none | des [<key>]}
no username snmpv3 encryption <username>
```

<username> - is the login user name.

des - des encryption protocol.

none - no encryption protocol.

no - This command sets the encryption protocol to **none**. The <username> is the login user name for which the specified encryption protocol will be used.

Default Setting

No encryption

Command Mode

Global Config

7.7.2.5 Set the password aging

The user can go to the CLI Global Configuration Mode to set the password aging, use the **passwords aging <1-365>** Global configuration command. Use the **no passwords aging** return to default value 0.

If the passwords aging is set, the local user will be prompted to change it before logging in again when the local user's password expires.

Syntax

```
passwords aging <1-365>
no passwords aging
```

<1-365> - Number of days until password expires.

Default Setting

0

Command Mode

Global Config

7.7.2.6 Set the password history

The user can go to the CLI Global Configuration Mode to set the password history, use the **passwords history <0-10>** Global configuration command. Use the **no passwords history** return to default value 0.

If password history is set, the local user will not be able to reuse any password stored in password history when the local user changes his or her password.

Syntax

```
passwords history <0-10>
no passwords history
```

<0-10> - Number of passwords to be used in password history check.

Default Setting

0

Command Mode

Global Config

7.7.2.7 Set the password lock-out count

The user can go to the CLI Global Configuration Mode to set the password lock-out count, use the **passwords lock-out <1-5>** Global configuration command. Use the **no passwords lock-out** to return to default value 0.

Syntax

```
passwords lock-out <1-5>
no passwords lock-out
```

<1-5> - the number of password failures before account lock.

Default Setting

0

Command Mode

Global Config

7.7.2.8 Set the minimum password length

The user can go to the CLI Global Configuration Mode to set the minimum password length, use the **passwords min-length <8-64>** Global configuration command. Use the **no passwords min-length** return to default value 8.

Syntax

```
passwords min-length <8-64>
no passwords min-length
```

Default Setting

8

Command Mode

Global Config

7.8 Security Commands

7.8.1 Show Commands

7.8.1.1 show users authentication

This command displays all users and all authentication login information. It also displays the authentication login list assigned to the default user.

Syntax

```
show users authentication
```

Default Setting

None

Command Mode

Privileged Exec

Display Message

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: This field displays the authentication login list assigned to the user for 802.1x port security.

7.8.1.2 show authentication

This command displays the ordered authentication methods for all authentication login lists.

Syntax

show authentication

Default Setting

None

Command Mode

Privileged Exec

Display Message

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.

7.8.1.3 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.

Syntax

show authentication users <listname>

<listname> - the authentication login listname.

Default Setting

None

Command Mode

Privileged Exec

Display Message

User Name: 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.

7.8.1.4 show dot1x

This command is used to show the status of the dot1x Administrative mode.

Syntax

show dot1x

Default Setting

None

Command Mode

Privileged Exec

Display Message

Administrative mode: Indicates whether authentication control on the switch is enabled or disabled.

VLAN Assignment Mode: Indicates whether assignment of an authorized port to a RADIUS assigned VLAN is allowed (enabled) or not (disabled).

7.8.1.5 show dot1x detail

This command is used to show a summary of the global dot1x configuration and the detailed dot1x configuration for a specified port.

Syntax

show dot1x detail <slot/port>

<slot/port> - is the desired interface number.

Default Setting

None

Command Mode

Privileged Exec

Display Message

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.

Control Mode - The configured control mode for this port. Possible values are force-unauthorized, force-authorized, auto and mac-based.

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 of 0 to 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 to 65535.

Guest VLAN ID: The guest VLAN identifier configured on the interface.

Guest VLAN Period: The timer used by authenticator state machine on this port.

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 to 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 to 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 to 10.

Vlan ID: The VLAN assigned to the port by the radius server.

VLAN Assigned Reason: The reason the VLAN identified in the VLAN-assigned field has been assigned to the port. Possible values are RADIUS, Unauthenticated VLAN, Guest VLAN, default, and Not Assigned. When the VLAN Assigned Reason is ‘Not Assigned’t, it means that the port has not been assigned to any VLAN by dot1x.

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 to 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.

Maximum Users - The maximum number of clients that can get authenticated on the port in the MAC-based dot1x authentication mode.

Unauthenticated VLAN ID - Indicates the unauthenticated VLAN configured for this port.

Session Timeout - Indicates the time for which the given session is valid. The time period in seconds is returned by the RADIUS server on authentication of the port.

Session Termination Action - This value indicates the action to be taken once the session timeout expires. Possible values are Default, Radius-Request. If the value is Default, the session is

terminated the port goes into unauthorized state. If the value is Radius-Request, then a reauthentication of the client authenticated on the port is performed.

7.8.1.6 show dot1x statistics

This command is used to show a summary of the global dot1x configuration and the dot1x statistics for a specified port.

Syntax

show dot1x statistics <slot/port>

<slot/port> - is the desired interface number.

Default Setting

None

Command Mode

Privileged Exec

Display Message

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.

7.8.1.7 show dot1x summary

This command is used to show a summary of the global dot1x configuration and summary information of the dot1x configuration for a specified port or all ports.

Syntax

show dot1x summary {<slot/port> | all}

<slot/port> - is the desired interface number.

all - All interfaces.

Default Setting

None

Command Mode

Privileged Exec

Display Message

Interface: The interface whose configuration is displayed.

Control Mode: The configured control mode for this port. Possible values are force-unauthorized / force-authorized / auto / mac-based.

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.

Port Status: Indicates if the key is transmitted to the supplicant for the specified port.

7.8.1.8 show dot1x users

This command displays 802.1x port security user information for locally configured users.

Syntax

show dot1x users <slot/port>

<slot/port> - is the desired interface number.

Default Setting

None

Command Mode

Privileged Exec

Display Message

User: Users configured locally to have access to the specified port.

7.8.1.9 show dot1x client

This command displays 802.1x client information.

Syntax
show dot1x clients {<slot/port> | all}

<slot/port> - is the desired interface number.

all - All interfaces.

Default Setting

None

Command Mode

Privileged Exec

Display Message

Logical Interface: The logical port number associated with a client.

Interface: The physical port to which the supplicant is associated.

User Name: The user name used by the client to authenticate to the server.

Supplicant MAC Address: The supplicant device MAC address.

Session Time: The time since the supplicant is logged on.

Filter ID: Identifies the Filter ID returned by the RADIUS server when the client was authenticated. This is a configured DiffServ policy name on the switch.

VLAN ID: The VLAN assigned to the port.

VLAN Assigned: The reason the VLAN identified in the VLAN ID field has been assigned to the port. Possible values are RADIUS, Unauthenticated VLAN, or Default. When the VLAN Assigned reason is Default, it means that the VLAN was assigned to the port because the PVID of the port was that VLAN ID.

Session Timeout: This value indicates the time for which the given session is valid. The time period in seconds is returned by the RADIUS server on authentication of the port.

Session Termination Action: This value indicates the action to be taken once the session timeout expires. Possible values are Default and Radius-Request. If the value is Default, the session is terminated and client details are cleared. If the value is Radius-Request, then a reauthentication of the client is performed.

7.8.1.10 show radius servers

This command is used to display items of the configured RADIUS servers.

Syntax

show radius servers [<ipaddr|hostname>]

Default Setting

None

Command Mode

Privileged Exec

Display Message

<ipaddr|hostname>: The IP address or host name of the authenticating server.

Current: The '*' symbol preceeding the server host address specifies that the server is currently active.

Host Address: The IP address of the host.

Port: The port in use by this server

Type: Primary or secondary

Secret Configured: Yes / No

Message Authenticator: The message authenticator attribute configured for the radius server.

7.8.1.11 show radius

This command is used to display the various RADIUS configuration items for the switch.

Syntax

show radius

Default Setting

None

Command Mode

Privileged Exec

Display Message

Current Server IP Address: Indicates the configured server currently in use for authentication

Servers: The number of RADIUS Authentication servers that have been configured.

Number of Configured Accounting Servers: The number of RADIUS Accounting servers that have been configured.

Number of Named Authentication Server Groups: The number of configured named RADIUS server groups.

Number of Named Accounting Server Groups: The number of configured named RADIUS server groups.

Number of Retransmits: The configured value of the maximum number of times a request packet is retransmitted.

Time Duration: The configured timeout value, in seconds, for request re-transmissions.

RADIUS Accounting Mode: A global parameter to indicate whether the accounting mode for all the servers is enabled or not.

RADIUS Attribute 4 Mode: A global parameter to indicate whether the NAS-IP-Address attribute has been enabled to use in RADIUS requests.

RADIUS Attribute 4 Value: A global parameter that specifies the IP address to be used in the NAS-IP-Address attribute to be used in RADIUS requests.

7.8.1.12 show radius accounting

This command is used to display the configured RADIUS accounting mode, accounting server, and the statistics for the configured accounting server.

Syntax
show radius accounting [statistics {<ipaddr|hostname>}]

<ipaddr> - is an IP Address.

Default Setting

None

Command Mode

Privileged Exec

Display Message

If you do not specify any parameters, then only the accounting mode and the RADIUS accounting server details are displayed.

RADIUS Accounting 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.

RADIUS Accounting Server IP Address: IP Address of the configured RADIUS accounting server

Round Trip Time: The time interval in centiseconds, 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.

7.8.1.13 show radius statistics

This command is used to display the statistics for RADIUS or configured server. To show the configured RADIUS server statistic, the IP Address specified must match that of a previously configured RADIUS server. On execution, the following fields are displayed.

Syntax
show radius statistics [<ipaddr|hostname>]

<ipaddr|hostname> - is an IP Address or a hostname.

Default Setting

None

Command Mode

Privileged Exec

Display Message

If you do not specify the IP address, then only Invalid Server Address field is displayed. Otherwise other listed fields are displayed.

Invalid Server Addresses or Hostname - The number of RADIUS Access-Response packets received from unknown addresses.

Server IP Address /Hostname - IP address or hostname of the Server.

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.

7.8.1.14 show tacacs

This command display configured information and statistics of a TACACS+ server.

Syntax

```
show tacacs [<ipaddr|hostname>]
```

<ipaddr|hostname> - is an IP Address or a hostname.

Default Setting

None

Command Mode

Privileged Exec

Display Message

IP address or Hostname - The IP address or hostname of the configured TACACS+ server.

Port: Shows the configured TACACS+ server port number.

TimeOut: Shows the timeout in seconds for establishing a TCP connection.

Priority: Shows the preference order in which TACACS+ servers are contacted. If a server connection fails, the next highest priority server is contacted.

7.8.1.15 show port-security

This command shows the port-security settings for the entire system.

Syntax

```
show port-security
```

Default Setting

None

Command Mode

Privileged Exec

Display Message

Port Security Administration Mode: Port lock mode for the entire system.

This command shows the port-security settings for a particular interface or all interfaces.

Syntax

```
show port-security { <slot/port> | all }
```

Default Setting

None

Command Mode

Privileged Exec

Display Message

Intf Interface Number.

Interface Admin Mode Port Locking mode for the Interface.

Dynamic Limit Maximum dynamically allocated MAC Addresses.

Static Limit Maximum statically allocated MAC Addresses.

Violation Trap Mode Whether violation traps are enabled.

Violation Shutdown Whether violation shutdowns are enabled.

This command shows the dynamically locked MAC addresses for port.

Syntax

show port-security dynamic <slot/port>

Default Setting

None

Command Mode

Privileged Exec

Display Message

MAC address Dynamically locked MAC address.

This command shows the statically locked MAC addresses for port.

Syntax

show port-security static <slot/port>

Default Setting

None

Command Mode

Privileged Exec

Display Message

MAC address Statically locked MAC address.

This command displays the source MAC address of the last packet that was discarded on a locked port.

Syntax

show port-security violation <slot/port>

Default Setting

None

Command Mode

Privileged Exec

Display Message

MAC address MAC address of discarded packet on locked ports.

7.8.2 Configuration Commands

7.8.2.1 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 “method1”, “method 2”, and/or “method 3” 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 is 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, reject, and tacacs.**

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. The value of **tacacs** indicates that the user’s ID and password will be authenticated using the TACACS.

To authenticate a user, the authentication methods in the user’s login will be attempted in order until an authentication attempt succeeds or fails.

i The default login list included with the default configuration cannot be changed.

Syntax

```
authentication login <listname> [<method1>] [<method2>] [<method3>]
no authentication login <listname>
```

<listname> - creates an authentication login list (Range: up to 15 characters).

<method1 - 3> - The possible method values are local, radius, reject, and tacacs.

no - This command deletes the specified authentication login list. The attempt to delete will fail if any of the following conditions are true:

1. The login list name is invalid or does not match an existing authentication login list
2. The specified authentication login list is assigned to any user or to the nonconfigured user for any component.
3. The login list is the default login list included with the default configuration and was not created using ‘config authentication login create’. The default login list cannot be deleted.

Default Setting

None

Command Mode

Global Config

7.8.2.2 username 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.

Syntax

username defaultlogin <listname>

<listname> - an authentication login list.

Default Setting

None

Command Mode

Global Config

7.8.2.3 username login

This command assigns the specified authentication login list to the specified user for system login. The <**username>** must be a configured <**username>** 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.

i The login list associated with the 'admin' user cannot be changed to prevent accidental lockout from the switch.

Syntax

username login <user> <listname>

<user> - is the login user name.

<listname> - an authentication login list.

Default Setting

None

Command Mode

Global Config

7.8.3 Dot1x Configuration Commands

7.8.3.1 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.

Syntax

dot1x initialize <slot/port>

<slot/port> - is the desired interface number.

Default Setting

None

Command Mode

Privileged Exec

7.8.3.2 dot1x default-login

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.

Syntax

dot1x default-login <listname>

<listname> - an authentication login list.

Default Setting

None

Command Mode

Global Config

7.8.3.3 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.

Syntax

```
dot1x login <user> <listname>
```

<user> - is the login user name.

<listname> - an authentication login list.

Default Setting

None

Command Mode

Global Config

7.8.3.4 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.

Syntax

```
dot1x system-auth-control
no dot1x system-auth-control
```

no - This command is used to disable the dot1x authentication support on the switch.

Default Setting

Disabled

Command Mode

Global Config

7.8.3.5 dot1x user

This command adds the specified user to the list of users with access to the specified port or all ports. The <username> parameter must be a configured user.

Syntax

```
dot1x user <user> {<slot/port> | all}
no dot1x user <user> {<slot/port> | all}
```

<user> - Is the login user name.

<slot/port> - Is the desired interface number.

all - All interfaces.

no - This command removes the user from the list of users with access to the specified port or all ports.

Default Setting

None

Command Mode

Global Config

7.8.3.6 dot1x port-control

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.

mac-based: The authenticator PAE sets the controlled port mode to reflect the outcome of the authentication exchanges between the supplicant, authenticator, and the authentication server on a per supplicant basis.

Syntax

```
dot1x port-control all {auto | force-authorized | force-unauthorized | mac-based}
no dot1x port-control all
```

all - All interfaces.

no - This command sets the authentication mode to be used on all ports to 'auto'.

Default Setting

auto

Command Mode

Global Config

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.

mac-based: The authenticator PAE sets the controlled port mode to reflect the outcome of the authentication exchanges between the supplicant, authenticator, and the authentication server on a per supplicant basis.

Syntax

```
dot1x port-control {auto | force-authorized | force-unauthorized | mac-based}
no dot1x port-control
```

no - This command sets the authentication mode to be used on the specified port to 'auto'.

Default Setting

auto

Command Mode

Interface Config

7.8.3.7 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 <1-10> value must be in the range 1 - 10.

Syntax

```
dot1x max-req <1-10>
no dot1x max-req
```

<1-10> - maximum number of times (Range: 1 – 10).

no - 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, that is, 2.

Default Setting

2

Command Mode

Interface Config

7.8.3.8 dot1x max-user

This command configures the maximum users to a specified port, The system's default maximum users of an interface has no limitation. If '**no dot1x max-users**' command is executed, the system will reset the maximum users to infinity. If the maximum users is specified or modified, the system should use the new one.

Syntax

```
dot1x max-user <count>
no dot1x max-user
```

<count> - maximum users (Range: 1 – 16).

no - This command sets the system will reset the maximum users to infinity

Default Setting

16

Command Mode

Interface Config

7.8.3.9 dot1x re-authentication

This command enables re-authentication of the supplicant for the specified port.

Syntax

```
dot1x re-authentication
no dot1x re-authentication
```

no - This command disables re-authentication of the supplicant for the specified port.

Default Setting

Disabled

Command Mode

Interface Config

7.8.3.10 dot1x re-reauthenticate

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.

Syntax

dot1x re-authenticate <slot/port>

<slot/port> - is the desired interface number.

Default Setting

None

Command Mode

Privileged Exec

7.8.3.11 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.

guest-vlan-period: The time, in seconds, for which the authenticator waits to see if any EAPOL packets are received on a port before authorizing the port and placing the port in the guest vlan (if configured). The guest vlan timer is only relevant when guest vlan has been configured on that specific port.

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.

Syntax

```
dot1x timeout {guest-vlan-period | quiet-period | reauth-period | server-timeout | supp-timeout |
tx-period} <seconds>
no dot1x timeout { guest-vlan-period | quiet-period | reauth-period | server-timeout | supp-timeout |
tx-period}
```

<seconds> - Value in the range 0 – 65535.

no - 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.

Default Setting

guest-vlan-period: 90 seconds

reauth-period: 3600 seconds

quiet-period: 60 seconds

tx-period: 30 seconds

supp-timeout: 30 seconds

server-timeout: 30 seconds

Command Mode

Interface Config

7.8.3.12 dot1x guest vlan

This command configures the Guest VLAN capability on the interface. The command specifies an active VLAN as an IEEE 802.1x guest VLAN.

Syntax

```
dot1x guest- vlan <vlan-id>
no dot1x guest-vlan
```

no - This command disables the Guest VLAN capability on this interface.

Default Setting

Disabled

Command Mode

Interface Config

7.8.4 Radius Configuration Commands

7.8.4.1 radius accounting mode

This command is used to enable the RADIUS accounting function.

Syntax

radius accounting mode
no radius accounting mode

no - This command is used to set the RADIUS accounting function to the default value - that is, the RADIUS accounting function is disabled.

Default Setting

Disabled

Command Mode

Global Config

7.8.4.2 authorization network radius

Use this command to enable the switch to accept VLAN assignment by the radius server.

Syntax

authorization network radius
no authorization network radius

no - Use this command to disable the switch to accept VLAN assignment by the radius server.

Default Setting

Disabled

Command Mode

Global Config

7.8.4.3 radius server attribute 4

This command to set the NAS-IP address for the radius server.

Syntax

```
radius-server attribute 4 [ipaddr]
no radius-server attribute 4
```

no – use this command to reset the NAS-IP address for the radius server.

Default Setting

None

Command Mode

Global Config

7.8.4.4 radius-server dead-time

This command cnfiguresradius server dead time.

Syntax

```
radius-server dead-time <value>
no radius-server dead-time
```

Value - Set radius server dead time (sec). Range 1 – 255.

no - This command is used to set dead time to the default value.

Default Setting

255

Command Mode

Global Config

7.8.4.5 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.

Syntax

```
radius-server host {acct | auth} <ipaddr|hostname> [port <port>]
no radius-server host {acct | auth} <ipaddr|hostname>
```

<ipaddr|hostname > - is a IP address or a hostname.

<port> - Port number (Range: 1 – 65535)

no - 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.

Default Setting

None

Command Mode

Global Config

7.8.4.6 radius-sever 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.

Syntax

```
radius-server key {acct | auth} <ipaddr|hostname> [encrypted <password>]
```

<ipaddr|hostname > - is a IP address or hostname.

<password> is the password in encrypted format.

Default Setting

None

Command Mode

Global Config

7.8.4.7 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.

Syntax

```
radius-server retransmit <retries>
no radius-server retransmit
```

<retries> - the maximum number of times (Range: 1 - 15).

no - 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, that is, 10.

Default Setting

10

Command Mode

Global Config

7.8.4.8 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.

Syntax

```
radius-server timeout <seconds>
no radius-server timeout
```

<seconds> - the maximum timeout (Range: 1 - 30).

no - 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, that is, 6.

Default Setting

6

Command Mode

Global Config

7.8.4.9 radius-server msgauth

This command enables the message authenticator attribute for a specified server.

Syntax

radius-server msgauth <ipaddr|hostname >

<ipaddr|hostname > - is a IP address or hostname.

Default Setting

None

Command Mode

Global Config

7.8.4.10 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.

Syntax

radius-server primary <ipaddr|hostname>

<ipaddr|hostname > - is a IP address or a hostname.

Default Setting

None

Command Mode

Global Config

7.8.5 TACACS+ Configuration Commands

7.8.5.1 tacacs host

This command is used to enable /disable TACACS+ function and to configure the TACACS+ server IP address. The system has not any TACACS+ server configured for its initialization and support 5 TACACS+ servers.

Syntax

```
tacacs host <ip-address|hostname>
no tacacs host <ip-address|hostname>
```

<ip-address|hostname> - The IP address or hostname of the TACACS+ server.

no - This command is used to remove all of configuration.

Default Setting

None

Command Mode

Global Config

7.8.5.2 tacacs key

This command is used to configure the TACACS+ authentication and encryption key.

Syntax

```
tacacs key [<key-string>|encrypted <key-string>]
no tacacs key
```

Note that the length of the secret key is up to 128 characters.

< key-string > - The valid value of the key.

encrypted - the key string is encrypted.

no - This command is used to remove the TACACS+ server secret key.

Default Setting

None

Command Mode

Global Config

This command is used to configure the TACACS+ authentication and encryption key.

Syntax

key [<key-string> | encrypted <key-string>]

Note that the length of the secret key is up to 128 characters.

< key-string > - The valid value of the key.

encrypted - the key string is encrypted.

Default Setting

None

Command Mode

TACACS Host Config

This command is used to configure the TACACS+ authentication host port.

Syntax

port [<port-number>]

<port-number> - The valid port number. Range (0 – 65535)>

Default Setting

49

Command Mode

TACACS Host Config

This command is used to configure the TACACS+ authentication host priority.

Syntax

priority [<priority>]

<priority> - The valid priority number. Range (0 – 65535)>

Default Setting

0

Command Mode

TACACS Host Config

7.8.5.3 tacacs timeout

This command is used to configure the TACACS+ connection timeout value.

Syntax

```
tacacs timeout [<timeout>]
no tacacs timeout
```

<timeout> - The connection timeout value. Max timeout (Range: 1 to 30).

no - This command is used to reset the timeout value to the default value.

Default Setting

5

Command Mode

Global Config

This command is used to configure the TACACS+ connection timeout value.

Syntax

```
timeout [<timeout>]
```

<timeout> - The connection timeout value. Max timeout (Range: 1 to 30).

Default Setting

5

Command Mode

TACACS Host Config

7.8.6 Port Security Configuration Commands

7.8.6.1 port-security

This command enables port locking at the system level (Global Config) or port level (Interface Config).

Syntax

```
port-security
no port-security
```

Default Setting

None

Command Mode

Global Config

Interface Config

7.8.6.2 port-security max-dynamic

This command sets the maximum of dynamically locked MAC addresses allowed on a specific port.

Syntax

```
port-security max-dynamic [<0-600>]
no port-security max-dynamic
```

no - This command resets the maximum of dynamically locked MAC addresses allowed on a specific port to its default value.

Default Setting

600

Command Mode

Interface Config

7.8.6.3 port-security max-static

This command sets the maximum number of statically locked MAC addresses allowed on a specific port.

Syntax

```
port-security max-static [<0-20>]
no port-security max-static
```

no - This command resets the maximum number of statically locked MAC addresses allowed on a specific port to its default value.

Default Setting

20

Command Mode

Interface Config

7.8.6.4 port-security mac-address

This command adds a MAC address to the list of statically locked MAC addresses.

Syntax

```
port-security mac-address <mac-addr> <1-3965>
no port-security mac-address <mac-addr> <1-3965>
```

<1-3965> - VLAN ID

<mac-addr> - The statically locked MAC address.

no - This command removes a MAC address from the list of statically locked MAC addresses.

Default Setting

None

Command Mode

Interface Config

7.8.6.5 port-security mac-address move

This command converts dynamically locked MAC addresses to statically locked addresses.

Syntax

```
port-security mac-address move
```

Default Setting

None

Command Mode

Interface Config

7.8.6.6 port-security violation shutdown

This command configures the port violation shutdown mode. Once the violation happens, the interface will be shutdown.

Syntax

```
port-security violation shutdown
no port-security violation
```

no - This command restore violation mode to be default.

Default Setting

None

Command Mode

Interface Config

7.9 CDP (Cisco Discovery Protocol) Commands

7.9.1 Show Commands

7.9.1.1 show cdp

This command displays the CDP configuration information.

Syntax

```
show cdp
```

Default Setting

None

Command Mode

Privileged Exec

Display Message

CDP Admin Mode: CDP enable or disable

CDP Holdtime (sec): The length of time a receiving device should hold the L2 Network Switch CDP information before discarding it

CDP Transmit Interval (sec): A period of the L2 Network Switch to send CDP packet

Ports: Port number vs CDP status

CDP: CDP enable or disable

7.9.1.2 show cdp neighbors

This command displays the CDP neighbor information.

Syntax
show cdp neighbors

Default Setting

None

Command Mode

Privileged Exec

Display Message

Device Id: Identifies the device name in the form of a character string.

Local Interface: The CDP neighbor information receiving port.

Holdtime: The length of time a receiving device should hold CDP information before discarding it.

Capability: Describes the device's functional capability in the form of a device type, for example, a switch.

Platform: Describes the hardware platform name of the device, for example, Fortinet the L2 Network Switch.

Port Id: Identifies the port on which the CDP packet is sent.

7.9.1.3 show cdp neighbors detail

This command displays the CDP neighbor detail information.

Syntax
show cdp neighbors detail

Default Setting

None

Command Mode

Privileged Exec

Display Message

Device Id: Identifies the device name in the form of a character string.

Entry Address(es): The L3 addresses of the interface that has sent the update.

Platform: Describes the hardware platform name of the device, for example, Fortinet the L2 Network Switch.

Capability: Describes the device's functional capability in the form of a device type, for example, a switch.

Local Interface: The CDP neighbor information receiving port.

Port Id: Identifies the port on which the CDP packet is sent.

Holdtime: The length of time a receiving device should hold CDP information before discarding it.

Management Address: The first address of IP address which can use management address connect to switch.

7.9.1.4 show cdp traffic

This command displays the CDP traffic counters information.

Syntax
show cdp traffic

Default Setting

None

Command Mode

Privileged Exec

Display Message

Incoming packet number: Received legal CDP packets number from neighbors.

Outgoing packet number: Transmitted CDP packets number from this device.

Error packet number: Received illegal CDP packets number from neighbors.

7.9.2 Configuration Commands

7.9.2.1 cdp

This command is used to enable CDP Admin Mode.

Syntax

```
cdp
no cdp
```

no - This command is used to disable CDP Admin Mode.

Default Setting

Enabled

Command Mode

Global Config

7.9.2.2 cdp run

This command is used to enable CDP on a specified interface.

Syntax

```
cdp run
no cdp run
```

no - This command is used to disable CDP on a specified interface.

Default Setting

Enabled

Command Mode

Interface Config

This command is used to enable CDP for all interfaces.

Syntax

```
cdp run all
no cdp run all
```

all - All interfaces.

no - This command is used to disable CDP for all interfaces.

Default Setting

Enabled

Command Mode

Global Config

7.9.2.3 cdp timer

This command is used to configure an interval time (seconds) of the sending CDP packet.

Syntax

```
cdp timer <5-254>
no cdp timer
```

<5-254> - interval time (Range: 5 – 254).

no - This command is used to reset the interval time to the default value.

Default Setting

60

Command Mode

Global Config

7.9.2.4 cdp holdtime

This command is used to configure the hold time (seconds) of CDP.

Syntax

```
cdp holdtime <10-255>
```

<10-255> - interval time (Range: 10 – 255).

no - This command is used to hold time to the default value.

Default Setting

180

Command Mode

Global Config

7.10 SNTP (Simple Network Time Protocol) Commands

7.10.1 Show Commands

7.10.1.1 show sntp

This command displays the current time and configuration settings for the SNTP client, and indicates whether the local time has been properly updated.

Syntax

show sntp

Default Setting

None

Command Mode

Privileged Exec

Display Message

Last Update Time Time of last clock update.

Last Unicast Attempt Time Time of last transmit query (in unicast mode).

Last Attempt Status Status of the last SNTP request (in unicast mode) or unsolicited message (in broadcast mode).

Broadcast Count Current number of unsolicited broadcast messages that have been received and processed by the SNTP client since last reboot.

Time Zone Time zone configured.

This command displays SNTP client settings.

Syntax

show sntp client

Default Setting

None

Command Mode

Privileged Exec

Display Message

Client Supported Modes Supported SNTP Modes (Broadcast, Unicast, or Multicast).

SNTP Version The highest SNTP version the client supports.

Port SNTP Client Port

Client Mode: Configured SNTP Client Mode.

Unicast Poll Interval Poll interval value for SNTP clients in seconds as a power of two.

Poll Timeout (Seconds) Poll timeout value in seconds for SNTP clients.

Poll Retry Poll retry value for SNTP clients.

This command displays configured SNTP servers and SNTP server settings.

Syntax
show sntp server

Default Setting

None

Command Mode

Privileged Exec

Display Message

Server IP Address IP Address of configured SNTP Server

Server Type Address Type of Server.

Server Stratum Claimed stratum of the server for the last received valid packet.

Server Reference ID Reference clock identifier of the server for the last received valid packet.

Server Mode SNTP Server mode.

Server Max Entries Total number of SNTP Servers allowed.

Server Current Entries Total number of SNTP configured.

For each configured server:

IP Address IP Address of configured SNTP Server.

Address Type Address Type of configured SNTP server.

Priority IP priority type of the configured server.

Version SNTP Version number of the server. The protocol version used to query the server in unicast mode.

Port Server Port Number

Last Attempt Time Last server attempt time for the specified server.

Last Update Status Last server attempt status for the server.

Total Unicast Requests Number of requests to the server.

Failed Unicast Requests Number of failed requests from server.

7.10.2 Configuration Commands

7.10.2.1 sntp broadcast client poll-interval

This command will set the poll interval for SNTP broadcast clients in seconds as a power of two where <poll-interval> can be a value from 6 to 10.

Syntax

```
sntp broadcast client poll-interval <6-10>
no sntp broadcast client poll-interval
```

<6-10> - The range is 6 to 10.

no - This command will reset the poll interval for SNTP broadcast client back to its default value.

Default Setting

6

Command Mode

Global Config

7.10.2.2 sntp client mode

This command will enable Simple Network Time Protocol (SNTP) client mode and optionally setting the mode to either broadcast, multicast, or unicast.

Syntax

```
sntp client mode [broadcast | unicast | multicast]
no sntp client mode
```

no - This command will disable Simple Network Time Protocol (SNTP) client mode.

i

The SNTP IPv4 multicast address is 224.0.1.1.

The SNTP IPv6 multicast address is ff05::101.

IPv6 address doesn't support broadcast mode.

Default Setting

None

Command Mode

Global Config

7.10.2.3 sntp client port

This command will set the SNTP client port id and polling interval in seconds.

Syntax

```
sntp client port <portid>
no sntp client port
```

<portid> - SNTP client port id.

no - Resets the SNTP client port id.

Default Setting

The default portid is 123.

Command Mode

Global Config

7.10.2.4 sntp unicast client poll-interval

This command will set the poll interval for SNTP unicast clients in seconds.

Syntax

```
sntp unicast client poll-interval <6-10>
no sntp unicast client poll-interval
```

<6-10> - Polling interval. It's 2^(value) seconds where value is 6 to 10.

no - This command will reset the poll interval for SNTP unicast clients to its default value.

Default Setting

The default value is 6.

Command Mode

Global Config

7.10.2.5 sntp unicast client poll-timeout

This command will set the poll timeout for SNTP unicast clients in seconds.

Syntax

```
sntp unicast client poll-timeout <poll-timeout>
no sntp unicast client poll-timeout
```

< poll-timeout > - Polling timeout in seconds. The range is 1 to 30.

no - This command will reset the poll timeout for SNTP unicast clients to its default value.

Default Setting

The default value is 5.

Command Mode

Global Config

7.10.2.6 sntp unicast client poll-retry

This command will set the poll retry for SNTP unicast clients in seconds.

Syntax

```
sntp unicast client poll-retry <poll-retry>
no sntp unicast client poll-retry
```

< poll-retry> - Polling retry in seconds. The range is 0 to 10.

no - This command will reset the poll retry for SNTP unicast clients to its default value.

Default Setting

The default value is 1.

Command Mode

Global Config

7.10.2.7 sntp server

This command configures an SNTP server (with a maximum of three) where the server address can be an ip address or a domain name and the address type either IPv4, IPv6, dnsv6 or dns. The optional priority can be a value of 1-3, the version is a value of 1-4, and the port id is a value of 1-65535.

Syntax

```
sntp server <ipaddress/ipv6address/domain-name> <addresstype> [<1-3> [<version> [<portid>]]]
no sntp server remove <ipaddress/ipv6address/domain-name>
```

<ipaddress/ipv6address/domain-name > - IPv4 or IPv6 address or domain name of the SNTP server.

<addresstype > - The address type is ipv4 or ipv6 or dns or dnsv6.

<1-3> - The range is 1 to 3.

<version> - The range is 1 to 4.

<portid> - The range is 1 to 65535.

no - This command deletes an server from the configured SNTP servers.

Default Setting

None

Command Mode

Global Config

7.10.2.8 sntp clock timezone

This command sets the time zone for the switch's internal clock.

Syntax

```
sntp clock timezone <name> <0-12> <0-59> {before-utc | after-utc}
```

<name> - Name of the time zone, usually an acronym. (Range: 1-15 characters)

<0-12> - Number of hours before/after UTC. (Range: 0-12 hours)

<0-59> - Number of minutes before/after UTC. (Range: 0-59 minutes)

before-utc - Sets the local time zone before (east) of UTC.

after-utc - Sets the local time zone after (west) of UTC.

Default Setting

Taipei 08:00 After UTC

Command Mode

Global Config

7.10.2.9 sntp multicast client poll-internal

This command will set the poll interval for SNTP multicast clients in seconds.

Syntax

sntp multicast client poll-interval <poll-interval> no sntp multicast client poll-interval

<poll-interval> - Polling interval. It's 2^(value) seconds where the range of value is 6 to 10.

no – This command will reset the poll interval for SNTP multicast client to its default value.

Default Setting

The default value is 6.

Command Mode

Global Config

7.11 MAC-Based Voice VLAN Commands

7.11.1 Show Commands

7.11.1.1 show voice-vlan

This command uses to display the configuration status of the Voice VLAN on the switch.

Syntax
show voice-vlan

Default Setting

None

Command Mode

Privileged Exec

Display Message

Vlan Voice-Vlan status: The voice-vlan status (Enable/Disable).

Voice-Vlan ID: The specified VLAN to vloce vlan.

Voice Name: The voice-name is the name of the voice device, which is to help the device management.

MAC-Address: A 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.

Mask: The mac-mask is the last eight digit of the mask code of the MAC address, the valid values are: 0xff, 0xfe, 0xfc, 0xf8, 0xf0, 0xe0, 0xc0, 0x80 and 0x0.

Priority: The priority-id is the priority of the voice traffic; the valid range is 0 to 7.

7.11.1.2 show voice vlan

Use this command to display the configuration status of the Voice VLAN on the switch, When the interface parameter is not specified, only the global mode of the Voice VLAN is displayed.

Syntax

```
show voice vlan [ interface { <unit/slot/port> | all }]
```

Default Setting

None

Command Mode

Privileged Exec

User Exec

Display Message

Voice VLAN Mode: The admin mode of the Voice VLAN on the interface.

Voice VLAN ID: The Voice VLAN ID.

Voice VLAN Priority: The dot1p priority for the Voice VLAN on the port.

Voice VLAN Untagged: The tagging option for the Voice VLAN traffic.

Voice VLAN CoS Override: The Override option for the voice traffic arriving on the port.

Voice VLAN Status: The operational status of Voice VLAN on the port.

7.11.2 Configuration Commands

7.11.2.1 voice-vlan

This command is used to enable/disable Voice VLAN Admin Mode.

Syntax

```
voice-vlan
no voice-vlan
```

no - This command is used to disable Voice VLAN Admin Mode.

Default Setting

Disabled

Command Mode

Global Config

7.11.2.2 voice-vlan vlan

This command configures the specified VLAN to Voice VLAN.

Syntax

voice-vlan vlan <vlan-id>

Default Setting

None

Command Mode

Global Config

7.11.2.3 voice-vlan mac

This command is used to add a voice device to a Voice VLAN.

Syntax

voice-vlan mac <mac-address> mask <mac-mask> priority <priority-id> [name <voice-name>]
no voice-vlan {mac <mac-address>mask <mac-mask>|name <voice-name>| all}

<mac-address> - Configs voice vlan mac address.

<mac-mask> - Configs voice vlan mac mask.

<priority-id> - Configs voice vlan priority.

<voice-name> - Configs voice vlan name.

no - This commandcancels the Voice VLAN configuration of this VLAN.

Default Setting

None

Command Mode

Global Config

7.11.2.4 voice vlan

This command is used to enable/disable Voice VLAN Admin Mode.

Syntax

```
voice vlan
no voice vlan
```

no - This command disables the Voice VLAN capability on this switch.

Default Setting

Disabled

Command Mode

Global Config

This command configures the Voice VLAN capability on the interface.

Syntax

```
voice vlan { <vlanid-id> | dot1p <priority> | none | untagged }
no voice vlan
```

<vlan-id> - Configure the IP phone to forward all voice traffic through the specified VLAN.

<dot1p> - Configure th IP phone to use 802.1p priority tagging for voice traffic and to use the default native VLAN (0) to carry all traffic. The valid <priority> range is 0 to 7.

<none> - Allow the IP phone to use its own configuration to send untagged voice traffic.

<untagged> - Configure the phone to send untagged voice traffic.

no - This command disables the Voice VLAN capability on this switch.

Default Setting

Disabled

Command Mode

Interface Config

7.11.2.5 voice vlan data priority

Use this command to either trust or entrust the data traffic arriving one the Voice VLAN port.

Syntax

voice vlan data priority untrust | trust

Default Setting

trust

Command Mode

Interface Config

7.12 LLDP (Link Layer Discovery Protocol) Commands

7.12.1 Show Commands

7.12.1.1 show lldp

This command uses to display a summary of the current LLDP configuration.

Syntax

show lldp

Default Setting

None

Command Mode

Privileged Exec

Display Message

Transmit Interval: Shows how frequently the system transmits local data LLDPDUs, in seconds.

Transmit Hold Multiplier: Shows the multiplier on the transmit interval that sets the TTL in local data LLDPDUs.

Re-initialization Delay: Shows the delay before re-initialization, in seconds.

Notification Interval: Shows how frequently the system sends remote data change notifications, in seconds.

7.12.1.2 show lldp interface

This command uses to display a summary of the current LLDP configuration for a specific interface or for all interfaces.

Syntax

```
show lldp interface {<slot/port> | all}
```

<slot/port> - Configs a specific interface.

Default Setting

None

Command Mode

Privileged Exec

Display Message

Interface: Shows the interface in a slot/port format.

Link: Shows whether the link is up or down.

Transmit: Shows whether the interface transmits LLDPDUs.

Receive: Shows whether the interface receives LLDPDUs.

Notify: Shows whether the interface sends remote data change notifications.

TLVs: Shows whether the interface sends optional TLVs in the LLDPDUs. The TLV codes can be 0 (Port Description), 1 (System Name), 2 (System Description), or 3 (System Capability).

Mgmt: Shows whether the interface transmits system management address information in the LLDPDUs.

7.12.1.3 show lldp statistics

This command uses to display the current LLDP traffic and remote table statistics for a specific interface or for all interfaces.

Syntax

```
show lldp statistics {<slot/port> | all}
```

<slot/port> - Configs a specific interface.

Default Setting

None

Command Mode

Privileged Exec

Display Message

Last Update: Shows the amount of time since the last update to the remote table in days, hours, minutes, and seconds.

Total Inserts: Total number of inserts to the remote data table.

Total Deletes: Total number of deletes from the remote data table.

Total Drops: Total number of times the complete remote data received was not inserted due to insufficient resources.

Total Ageouts: Total number of times a complete remote data entry was deleted because the Time to Live interval expired.

The table contains the following column headings:

Interface: Shows the interface in slot/port format.

Transmit Total: Total number of LLDP packets transmitted on the port.

Receive Total: Total number of LLDP packets received on the port.

Discards: Total number of LLDP frames discarded on the port for any reason.

Errors: The number of invalid LLDP frames received on the port.

Ageouts: Total number of times a complete remote data entry was deleted for the port because the Time to Live interval expired.

TVL Discards: Shows the number of TLVs discarded

TVL Unknowns: Total number of LLDP TLVs received on the port where the type value is in the reserved range, and not recognized.

7.12.1.4 show lldp remote-device

This command uses to display summary information about remote devices that transmit current LLDP data to the system. You can show information about LLDP remote data received on all ports or on a specific port.

Syntax
show lldp remote-device {<slot/port> | all}

<slot/port> - Displays a specific interface.

Default Setting

None

Command Mode

Privileged Exec

Display Message

Local Interface: Identifies the interface that received the LLDPDU from the remote device.

Rem ID: Shows the ID of the remote device.

Chassis ID: The ID that is sent by a remote device as part of the LLDP message, it is usually a MAC address of the device.

Port ID: Shows the port number that transmitted the LLDPDU.

System Name: Shows the system name of the remote device.

7.12.1.5 show lldp remote-device detail

This command uses to display detailed information about remote devices that transmit current LLDP data to an interface on the system.

Syntax

show lldp remote-device detail <slot/port>

<slot/port> - Displays a specific interface.

Default Setting

None

Command Mode

Privileged Exec

Display Message

Local Interface: Identifies the interface that received the LLDPDU from the remote device.

Remote Identifier: An internal identifier to the switch to mark each remote device to the system.

Chassis ID Subtype: Shows the type of identification used in the Chassis ID field.

Chassis ID: Identifies the chassis of the remote device.

Port ID Subtype: Identifies the type of port on the remote device.

Port ID: Shows the port number that transmitted the LLDPDU.

System Name: Shows the system name of the remote device.

System Description: Describes the remote system by identifying the system name and versions of hardware, operating system, and networking software supported in the device.

Port Description: Describes the port in an alpha-numeric format. The port description is configurable.

System Capabilities Supported: Indicates the primary function(s) of the device.

System Capabilities Enabled: Shows which of the supported system capabilities are enabled.

Management Address: For each interface on the remote device with an LLDP agent, lists the type of address the remote LLDP agent uses and specifies the address used to obtain information related to the device.

Time To Live: Shows the amount of time (in seconds) the remote device's information received in the LLDPDU should be treated as valid information.

7.12.1.6 show lldp local-device

This command uses to display summary information about the advertised LLDP local data. This command can display summary information or detail for each interface.

Syntax

show lldp local-device {<slot/port> | all}

<slot/port> - Displays a specific interface.

Default Setting

None

Command Mode

Privileged Exec

Display Message

Interface: Identifies the interface in a slot/port format.

Port ID: Shows the port ID associated with this interface.

Port Description: Shows the port description associated with the interface.

7.12.1.7 show lldp local-device detail

This command uses to display detailed information about the LLDP data a specific interface transmits.

Syntax

show lldp local-device detail <slot/port>

<slot/port> - Displays a specific interface.

Default Setting

None

Command Mode

Privileged Exec

Display Message

Interface: Identifies the interface that sends the LLDPDU.

Chassis ID Subtype: Shows the type of identification used in the Chassis ID field.

Chassis ID: Identifies the chassis of the local device.

Port ID Subtype: Identifies the type of port on the local device.

Port ID: Shows the port number that transmitted the LLDPDU.

System Name: Shows the system name of the local device.

System Description: Describes the local system by identifying the system name and versions of hardware, operating system, and networking software supported in the device.

Port Description: Describes the port in an alpha-numeric format.

System Capabilities Supported: Indicates the primary function(s) of the device.

System Capabilities Enabled: Shows which of the supported system capabilities are enabled.

Management Address: Lists the type of address and the specific address the local LLDP agent uses to send and receive information.

7.12.1.8 show lldp med

The user can go to the CLI Privilege Exec to display a summary of the current LLDP-MED configuration, use the **show lldp med** Privilege command.

Syntax
show lldp med

Default Setting

None

Command Mode

Privileged Exec

Display Message

Fast Start Repeat Count: Specifies the number of LLDP PDUs that will be transmitted when the protocol is enabled. The range is from (1 to 10). Default value of fast repeat count is 3.

Device Class: Specifies local device's MED Classification. There are four different kinds of devices, three of them represent the actual end points (classified as Class I Generic [IP Communication Controller etc.], Class II Media [Conference Bridge etc.], Class III Communication [IP Telephone etc.]). The fourth device is Network Connectivity Device, which is typically a LAN Switch/Router, IEEE 802.1 Bridge, IEEE 802.11 Wireless Access Point etc.

7.12.1.9 show lldp med interface

The user can go to the CLI Privilege Exec to d display a summary of the current LLDP-MED configuration for a specific interface, use the **show lldp med interface {all | <unit/slot/port>}** Privilege command.

Syntax
show lldp med interface {all | <slot/port>}

<slot/port> - Displays a specific interface.

Default Setting

None

Command Mode

Privileged Exec

Display Message

Interface: Specifies all the ports on which LLDP-MED can be configured.

Link: Specifies the link status of the ports whether it is Up/Down.

ConfigMED: Specifies the LLDP-MED mode is enabled or disabled on this interface.

OperMED: Specifies the LLDP-MED TLVs are transmitted or not on this interface

ConfigNotify: Specifies the LLDP-MED topology notification mode of the interface.

TLVsTx: Specifies the LLDP-MED transmit TLV(s) that are included

7.12.1.10 show lldp med local-device detail

The user can go to the CLI Privilege Exec to display detailed information about the LLDP-MED data, use the **show lldp med local-device detail <unit/slot/port>** Privilege command.

Syntax
show lldp med local-device detail <slot/port>

<slot/port> - Displays a specific interface.

Default Setting

None

Command Mode

Privileged Exec

Display Message

Network Policies Specifies if network policy TLV is present in the LLDP frames.

Media Policy Application Type: Specifies the application type. Types of application types are unknown, voicesignaling, guestvoice, guestvoicesignalling, softphonevoice, videoconferencing, streammingvideo, vidoesignalling. Each application type that is received has the VLAN id, priority, DSCP, tagged bit status and unknown bit status. A port may receive one or many such application types. If a network policy TLV has been transmitted only then would this information be displayed.

Vlan ID: Specifies the VLAN id associated with a particular policy type.

Priority: Specifies the priority associated with a particular policy type.

DSCP: Specifies the DSCP associated with a particular policy type.

Unknown: Specifies the unknown bit associated with a particular policy type.

Tagged: Specifies the tagged bit associated with a particular policy type.

Inventory Specifies if inventory TLV is present in LLDP frames.

Hardware Rev: Specifies hardware version.

Firmware Rev: Specifies Firmware version.

Software Rev: Specifies Software version.

Serial Num: Specifies serial number.

Mfg Name: Specifies manufacturers name.

Model Name: Specifies model name.

Asset ID: Specifies asset id.

Location Specifies if location TLV is present in LLDP frames.

Subtype: Specifies type of location information.

Info: Specifies the location information as a string for given type of location id.

Extended POE Specifies if local device is a PoE device.

Device Type: Specifies power device type.

Extended POE PSE Specifies if extended PSE TLV is present in LLDP frame.

Available: Specifies available power sourcing equipment's power value in tenths of watts on the port of local device.

Source: Specifies power source of this port.

Priority: Specifies PSE port power priority.

Extended POE PD Specifies if extended PD TLV is present in LLDP frame.

Required: Specifies required power device power value in tenths of watts on the port of local device.

Source: Specifies power source of this port.

Priority: Specifies PD port power priority.

7.12.1.11 show lldp med remote-device

The user can go to the CLI Privilege Exec to d display the summary information about remote devices that transmit current LLDP-MED data to the system. use the **show lldp med remote-device {<slot/port> | all}** Privilege command.

Syntax
show lldp med remote-device {<slot/port> | all}

Default Setting

None

Command Mode

Privileged Exec

Display Message

Interface: Specifies the list of all the ports on which LLDP-MED is enabled.

Remote ID: An internal identifier to the switch to mark each remote device to the system.

Device Class: Specifies local device's MED Classification. There are four different kinds of devices, three of them represent the actual end points (classified as Class I Generic [IP Communication Controller etc.], Class II Media [Conference Bridge etc.], Class III Communication [IP Telephone etc.]). The fourth device is Network Connectivity Device, which is typically a LAN Switch/Router, IEEE 802.1 Bridge, IEEE 802.11 Wireless Access Point etc.

7.12.1.12 show lldp med remote-device detail

The user can go to the CLI Privilege Exec to d display detailed information about remote devices that transmit current LLDP-MED data to an interface on the system, use the **show lldp med remote-device detail <*slot/port*>** Privilege command.

Syntax
show lldp med remote-device detail <slot/port>

Default Setting

None

Command Mode

Privileged Exec

Display Message

Term Definition:

Capabilities: Specifies the supported and enabled capabilities that was received in MED TLV on this port.

MED Capabilities Supported: Specifies supported capabilities that was received in MED TLV on this port.

MED Capabilities Enabled: Specifies enabled capabilities that was received in MED TLV on this port.

Device Class: Specifies device class as advertised by the device remotely connected to the port.

Network Policies Specifies if network policy TLV is received in the LLDP frames on this port.

Media Policy Application Type: Specifies the application type. Types of application types are unknown, voicesignaling, guestvoice, guestvoicesignalling, softphonevoice, videoconferencing, streammingvideo, vidoesignalling. Each application type that is received has the VLAN id, priority, DSCP, tagged bit status and unknown bit status. A port may receive one or many such application types. If a network policy TLV has been receive on this port only then would this information be displayed.

Vlan ID: Specifies the VLAN id associated with a particular policy type.

Priority: Specifies the priority associated with a particular policy type.

DSCP: Specifies the DSCP associated with a particular policy type.

Unknown: Specifies the unknown bit associated with a particular policy type.

Tagged: Specifies the tagged bit associated with a particular policy type.

Inventory Specifies if inventory TLV is received in LLDP frames on this port.

Hardware Rev: Specifies hardware version of the remote device.

Firmware Rev: Specifies Firmware version of the remote device.

Software Rev: Specifies Software version of the remote device.

Serial Num: Specifies serial number of the remote device.

Mfg Name: Specifies manufacturers name of the remote device.

Model Name: Specifies model name of the remote device.

Asset ID: Specifies asset id of the remote device.

Location Specifies if location TLV is received in LLDP frames on this port.

Subtype: Specifies type of location information.

Info: Specifies the location information as a string for given type of location id.

Extended POE Specifies if remote device is a PoE device.

Device Type: Specifies remote device's PoE device type connected to this port.

Extended POE PSE Specifies if extended PSE TLV is received in LLDP frame on this port.

Available: Specifies the remote ports PSE power value in tenths of watts.

Source: Specifies the remote ports PSE power source.

Priority: Specifies the remote ports PSE power priority.

Extended POE PD Specifies if extended PD TLV is received in LLDP frame on this port.

Required: Specifies the remote port's PD power requirement.

Source: Specifies the remote port's PD power source.

Priority: Specifies the remote port's PD power priority.

7.12.2 Configuration Commands

7.12.2.1 lldp notification

This command uses to enable remote data change notifications.

Syntax
lldp notification

```
no lldp notification
```

no - This command is used to disable notifications.

Default Setting

Disbaled

Command Mode

Interface Config

7.12.2.2 lldp notification-interval

This command is used to configure how frequently the system sends remote data change notifications. The <interval-seconds> parameter is the number of seconds to wait between sending notifications. The valid interval range is 5-3600 seconds.

Syntax

```
lldp notification-interval <interval-seconds>
no lldp notification-interval
```

<interval-seconds> - Configures the number of seconds to wait between sending notifications.

no - This command is used to return the notification interval to the default value.

Default Setting

5

Command Mode

Global Config

7.12.2.3 lldp receive

This command uses to enable the LLDP receive capability.

Syntax

```
lldp receive
no lldp receive
```

no - This command is used to return the reception of LLDPDUs to the default value.

Default Setting

Disabled

Command Mode

Interface Config

7.12.2.4 lldp transmit

This command uses to enable the LLDP advertise capability.

Syntax

```
lldp transmit
no lldp transmit
```

no - This command is used to return the local data transmission capability to the default.

Default Setting

Disabled

Command Mode

Interface Config

7.12.2.5 lldp transmit-mgmt

This command uses to include transmission of the local system management address information in the LLDPDUs.

Syntax

```
lldp transmit-mgmt
no lldp transmit-mgmt
```

no - This command is used to cancel inclusion of the management information in LLDPDUs.

Default Setting

None

Command Mode

Interface Config

7.12.2.6 lldp transmit-tlv

This command is used to specify which optional type length values (TLVs) in the 802.1AB basic management set are transmitted in the LLDPDUs. Use sys-name to transmit the system name TLV. To configure the system name, please refer to “snmp-server” command. Use sys-descto transmit the system description TLV. Use sys-cap to transmit the system capabilities TLV. Use port-desc to transmit the port description TLV. To configure the port description, please refer to “description” command. Use org-spec to transmit the organization specific TLV.

Syntax

lldp transmit-tlv [sys-desc] [sys-name] [sys-cap] [port-desc] [org-spec]
no lldp transmit-tlv [sys-desc] [sys-name] [sys-cap] [port-desc] [org-spec]

no - This command is used to remove an optional TLV from the LLDPDUs. Use the command without parameters to remove all optional TLVs from the LLDPDU.

Default Setting

None

Command Mode

Interface Config

7.12.2.7 lldp timers

This command is used to set the timing parameters for local data transmission on ports enabled for LLDP. The <interval-seconds> determines the number of seconds to wait between transmitting local data LLDPDUs. The range is 1-32768 seconds. The <hold-value> is the multiplier on the transmit interval that sets the TTL in local data LLDPDUs. The multiplier range is 2-10. The <reinit-seconds> is the delay before re-initialization, and the range is 1-0 seconds.

Syntax

lldp timers [interval <interval-seconds>] [hold <hold-value>] [reinit <reinit-seconds>]
no lldp timers [interval] [hold] [reinit]

<interval-seconds> - Configures the number of seconds to wait between transmitting local data LLDPDUs

<hold-value> - Configures the multiplier on the transmit interval that sets the TTL in local data LLDPDUs

<reinit-seconds> - Configures the delay before re-initialization

no - This command is used to return any or all timing parameters for local data transmission on ports enabled for LLDP to the default values.

Default Setting

Interval-seconds 30

Hold-value 4

Reinit-seconds 2

Command Mode

Global Config

7.12.2.8 lldp tx-delay

This command is used to set the timing parameters for data transmission delay on ports enabled for LLDP. The <delay-seconds> determines the number of seconds to wait between transmitting local data LLDPDUs. The range is 1-8192 seconds.

Syntax

```
lldp tx-delay <delay-seconds>
no lldp tx-delay
```

no - This command is used to return return the transmit delay to the default value.

Default Setting

2

Command Mode

Global Config

7.12.2.9 lldp med

The user can go to the CLI Interface Configuration Mode to set MED to enable, use the **lldp med** Interface configuration command. Use the **no lldp med** to disable med function.

Syntax

```
lldp med
no lldp med
```

Default Setting

Disabled

Command Mode

Interface Config

7.12.2.10 lldp med confignotification

The user can go to the CLI Interface Configuration Mode to set all the ports to send the topology change notification, use the **lldp med confignotification** Interface configuration command. Use the **no lldp med confignotification** to disable notifications.

Syntax

```
lldp med confignotification
no lldp med confignotification
```

Default Setting

Disabled

Command Mode

Interface Config

7.12.2.11 lldp med transmit-tlv

The user can go to the CLI Interface Configuration Mode to set Type Length Values (TLVs) in the LLDP MED, use the **lldp med transmit-tlv [capabilities] [ex-pd] [ex-pse] [inventory] [location][network-policy]** Interface configuration command. Use the **no lldp med transmit-tlv [capabilities] [ex-pd] [ex-pse] [inventory] [location][network-policy]** to remove the TLVs.

Syntax

```
lldp med transmit-tlv [capabilities] [ex-pd] [ex-pse] [inventory] [location]
[network-policy]
no lldp med transmit-tlv [capabilities] [ex-pd] [ex-pse] [inventory] [location]
[network-policy]
```

capabilities -Transmit the LLDP capabilities TLV.

ex-pd - Transmit the LLDP extended PD TLV.

ex-pse - Transmit the LLDP extended PSE TLV.

inventory - Transmit the LLDP inventory TLV.

location - Transmit the LLDP location TLV.

network-policy - Transmit the LLDP network policy TLV.

Default Setting

None

Command Mode

Interface Config

7.12.2.12 lldp med all

The user can go to the CLI Global Configuration Mode to set LLDP-MED on all the ports, use the **lldp med all** Global configuration command. Use the **no lldp med all** to disable LLDP-MED on all the ports.

Syntax

```
lldp med all
no lldp med all
```

Default Setting

Disabled

Command Mode

Global config

7.12.2.13 lldp med confignotification all

The user can go to the CLI Global Configuration Mode to set all the ports to send the topology change notification, use the **lldp med confignotification all** Global configuration command. Use the **no lldp med confignotification all** to remove all the ports to send the topology change notification.

Syntax

```
lldp med confignotification all
no lldp med confignotification all
```

Default Setting

None

Command Mode

Global Config

7.12.2.14 lldp med faststartrepeatcount

The user can go to the CLI Global Configuration Mode to set the fast start repeat count, use the **lldp med faststartrepeatcount** Global configuration command. Use the **no lldp med faststartrepeatcount** to return the default value 3.

Syntax

```
lldp med faststartrepeatcount <1-10>
no lldp med faststartrepeatcount
```

Default Setting

3

Command Mode

Global Config

7.12.2.15 lldp med transmit-tlv all

The user can go to the CLI Global Configuration Mode to set Type Length Values (TLVs) in the LLDP-MED, use the **lldp med transmit-tlv all [capabilities] [ex-pd] [ex-pse] [inventory][location] [network-policy]**Global configuration command. Use the **no lldp med transmit-tlv all [capabilities] [ex-pd] [ex-pse] [inventory] [location] [network-policy]** to remove Type Length Values (TLVs) in the LLDP-MED

Syntax

```
lldp med transmit-tlv all [capabilities] [ex-pd] [ex-pse] [inventory] [location] [network-policy]
no lldp med transmit-tlv all [capabilities] [ex-pd] [ex-pse] [inventory] [location] [network-policy]
```

capabilities - Transmit the LLDP capabilities TLV.

ex-pd - Transmit the LLDP extended PD TLV.

ex-pse - Transmit the LLDP extended PSE TLV.

inventory - Transmit the LLDP inventory TLV.

location - Transmit the LLDP location TLV.

network-policy - Transmit the LLDP network policy TLV.

Default Setting

None

Command Mode

Global Config

7.13 Denial Of Service Commands

7.13.1 Show Commands

7.13.1.1 show dos-control

This command displays the Denial of Service configurations for the entire system.

Syntax
show dos-control

Default Setting

None

Command Mode

Privileged Exec

Display Message

TCP Fragment Mode: May be enabled or disabled. The factory default is disabled.

Min TCP Hdr Size: The range is 0-255. The factory default is 20.

ICMP Size Mode: May be enabled or disabled. The factory default is disabled.

Max ICMPv4 Pkt Size: The range is 0-16384. The factory default is 512.

Max ICMPv6 Pkt Size: The range is 0-16384. The factory default is 512.

ICMP Fragment Mode: May be enabled or disabled. The factory default is disabled.

TCP Port Mode: May be enabled or disabled. The factory default is disabled.

UDP Port Mode: May be enabled or disabled. The factory default is disabled.

SIPDIP Mode: May be enabled or disabled. The factory default is disabled.

SMACDMAC Mode: May be enabled or disabled. The factory default is disabled.

TCP FIN&URG&PSH Mode: May be enabled or disabled. The factory default is disabled.

TCP Flag&Sequence Mode: May be enabled or disabled. The factory default is disabled.

TCP SYN Mode: May be enabled or disabled. The factory default is disabled.

TCP SYN&FIN Mode: May be enabled or disabled. The factory default is disabled.

First Fragment Mode: May be enabled or disabled. The factory default is disabled.

TCP Fragment Offset Mode: May be enabled or disabled. The factory default is disabled.

7.13.2 Configuration Commands

7.13.2.1 dos-control sipdip

This command enables Source IP Address = Destination IP Address (SIP=DIP) Denial of Service protection. If the mode is enabled, Denial of Service prevention is active for this type of attack. If packets ingress with SIP=DIP, the packets will be dropped if the mode is enabled.

Syntax

```
dos-control sipdip
no dos-control sipdip
```

no - This command disables Source IP Address = Destination IP Address (SIP=DIP) Denial of Service prevention.

Default Setting

Disabled

Command Mode

Global Config

7.13.2.2 dos-control tcpfrag

This command enables Minimum TCP Header Size Denial of Service protection. If the mode is enabled, Denial of Service prevention is active for this type of attack. If packets ingress having a TCP Header Size smaller then the configured value, the packets will be dropped if the mode is enabled. The default is disabled. If you enable dos-control tcpfrag, but do not provide a Minimum TCP Header Size, the system sets that value to 20.

Syntax

```
dos-control tcpfrag [<0-255>]
no dos-control tcpfrag
```

<0-255> - This command sets minimum TCP header length

no - This command sets Minimum TCP Header Size Denial of Service protection to the default value of disabled.

Default Setting

Disabled, 20

Command Mode

Global Config

7.13.2.3 dos-control firstfrag

This command enables IP First Fragment Denial of Service protection. If the mode is enabled, Denial of Service prevention is active for this type of attack. If packets ingress having IP First Fragment Offset equal to one (1), the packets will be dropped if the mode is enabled.

Syntax

```
dos-control firstfrag
no dos-control firstfrag
```

no - This command disabled IP First Fragment Denial of Service protection.

Default Setting

Disabled

Command Mode

Global Config

7.13.2.4 dos-control tcpflag

This command enables TCP Flag Denial of Service protections. If the mode is enabled, Denial of Service prevention is active for this type of attacks. If packets ingress having TCP Flag SYN set and a source port less than 1024 or having TCP Control Flags set to 0 and TCP Sequence Number set to 0 or having TCP Flags FIN, URG, and PSH set and TCP Sequence Number set to 0 or having TCP Flags SYN and FIN both set, the packets will be dropped if the mode is enabled.

Syntax

```
dos-control tcpflag
no dos-control tcpflag
```

no - This command sets disables TCP Flag Denial of Service protections.

Default Setting

Disabled

Command Mode

Global Config

7.13.2.5 dos-control l4port

This command enables L4 Port Denial of Service protections. If the mode is enabled, Denial of Service prevention is active for this type of attack. If packets ingress having Source TCP/UDP Port Number equal to Destination TCP/UDP Port Number, the packets will be dropped if the mode is enabled.

Some applications mirror source and destination L4 ports - RIP for example uses 520 for both. If you enable dos-control l4port, applications such as RIP may experience packet loss which would render the application inoperable.

Syntax

```
dos-control l4port
no dos-control l4port
```

no - This command disables L4 Port Denial of Service protections.

Default Setting

Disabled

Command Mode

Global Config

7.13.2.6 dos-control tcpport

This command enables the TCP L4 source = destination port number (Source TCP Port = Destination TCP Port) Denial of Service protection. If the mode is enabled, Denial of Service prevention is active for this type of attack. If packets ingress with Source TCP Port =Destination TCP Port, the packets will be dropped if the mode is enabled.

Syntax

```
dos-control tcpport
no dos-control tcpport
```

no - This command disables the TCP L4 source = destination port number (Source TCP Port =Destination TCP Port) Denial of Service protection.

Default Setting

Disabled

Command Mode

Global Config

7.13.2.7 dos-control udpport

This command enables the UDP L4 source = destination port number (Source UDP Port = Destination UDP Port) Denial of Service protection. If the mode is enabled, Denial of Service prevention is active for this type of attack. If packets ingress with Source UDP Port =Destination UDP Port, the packets will be dropped if the mode is enabled.

Syntax

```
dos-control udpport
no dos-control udpport
```

no - This command disables the UDP L4 source = destination port number (Source UDP Port =Destination UDP Port) Denial of Service protection.

Default Setting

Disabled

Command Mode

Global Config

7.13.2.8 dos-control icmp

This command enables Maximum ICMP Packet Size Denial of Service protections. If the mode is enabled, Denial of Service prevention is active for this type of attack. If ICMP Echo Request (PING) packets ingress having a size greater than the configured value, the packets will be dropped if the mode is enabled.

Syntax

```
dos-control icmp
no dos-control icmp
```

no - This command disables Maximum ICMP Packet Size Denial of Service protections.

Default Setting

Disabled

Command Mode

Global Config

7.13.2.9 dos-control icmpv4

This command enables Maximum ICMPv4 Packet Size Denial of Service protections. If the mode is enabled, Denial of Service prevention is active for this type of attack. If ICMPv4 Echo Request (PING) packets ingress having a size greater than the configured value, the packets will be dropped if the mode is enabled.

Syntax

```
dos-control icmpv4 [<0-16384>]
no dos-control icmpv4
```

<0-16384> - This command sets maximum ICMPv4 packet size.

no - This command resets the Maximum ICMPv4 Packet Size Denial of Service protections to its default value.

Default Setting

512

Command Mode

Global Config

7.13.2.10 dos-control icmpv6

This command enables Maximum ICMPV6 Packet Size Denial of Service protections. If the mode is enabled, Denial of Service prevention is active for this type of attack. If ICMPV6 Echo Request (PING) packets ingress having a size greater than the configured value, the packets will be dropped if the mode is enabled.

Syntax

```
dos-control icmpv6 [<0-16384>]
no dos-control icmpv6
```

<0-16384> - This command sets maximum ICMPV6 packet size.

no - This command resets the Maximum ICMPV6 Packet Size Denial of Service protections to its default value.

Default Setting

512

Command Mode

Global Config

7.13.2.11 dos-control icmpfrag

This command enables the ICMP Fragment Denial of Service protection. If the mode is enabled, Denial of Service prevention is active for this type of attack. If packets ingress has fragmented ICMP packets, the packets will be dropped if the mode is enabled.

Syntax

```
dos-control icmpfrag
no dos-control icmpfrag
```

no - This command disables the ICMP Fragment Denial of Service protection.

Default Setting

Disabled

Command Mode

Global Config

7.13.2.12 dos-control smacdmac

This command enables the Source MAC address = Destination MAC address (SMAC=DMAC) Denial of Service protection. If the mode is enabled, Denial of Service prevention is active for this type of attack. If packets ingress with SMAC=DMAC, the packets will be dropped if the mode is enabled.

Syntax

```
dos-control smacdmac
no dos-control smacdmac
```

no - This command disables the Source MAC address = Destination MAC address (SMAC=DMAC) Denial of Service protection.

Default Setting

Disabled

Command Mode

Global Config

7.13.2.13 dos-control tcpfinurgpsh

This command enables the TCP FIN and URG and PSH and SEQ=0 checking Denial of Service protections. If the mode is enabled, Denial of Service prevention is active for this type of attack. If packets

ingress having TCP FIN, URG, and PSH all set and TCP Sequence Number set to 0, the packets will be dropped if the mode is enabled.

Syntax

```
dos-control tcpfinurgpsh
no dos-control tcpfinurgpsh
```

no - This command disables the TCP FIN and URG and PSH and SEQ=0 checking Denial of Service protections.

Default Setting

Disabled

Command Mode

Global Config

7.13.2.14 dos-control tcpsyn

This command enables the TCP SYN and L4 source = 0-1023 Denial of Service protection. If the mode is enabled, Denial of Service prevention is active for this type of attack. If packets ingress having TCP flag SYN set and an L4 source port from 0 to 1023, the packets will be dropped if the mode is enabled.

Syntax

```
dos-control tcpsyn
no dos-control tcpsyn
```

no - This command disables the TCP SYN and L4 source = 0-1023 Denial of Service protection.

Default Setting

Disabled

Command Mode

Global Config

7.13.2.15 dos-control tcpsynfin

This command enables the TCP SYN and FIN Denial of Service protection. If the mode is enabled, Denial of Service prevention is active for this type of attack. If packets ingress having TCP flags SYN and FIN set, the packets will be dropped if the mode is enabled.

Syntax

```
dos-control tcpsynfin
no dos-control tcpsynfin
```

no - This command disables the TCP SYN & FIN Denial of Service protection.

Default Setting

Disabled

Command Mode

Global Config

7.13.2.16 dos-control tcpoffset

This command enables the TCP Fragment Offset Denial of Service protection. If the mode is enabled, Denial of Service prevention is active for this type of attack. If packets ingress having TCP Header Offset equal to one (1), the packets will be dropped if the mode is enabled.

Syntax

```
dos-control tcpoffset
no dos-control tcpoffset
```

no - This command disables the TCP Fragment Offset Denial of Service protection.

Default Setting

Disabled

Command Mode

Global Config

7.13.2.17 dos-control all

This command enables the Denial of Service protection checks globally.

Syntax

```
dos-control all
no dos-control all
```

no - This command disables the Denial of Service protection checks globally.

Default Setting

Disabled

Command Mode

Global Config

7.14 VTP (VLAN Trunking Protocol) Commands

7.14.1 Show Commands

7.14.1.1 show vtp counters

This command displays the VTP packet statistics.

Syntax
show vtp counters

Default Setting

None

Command Mode

Privileged Exec

Display Message

Summary advertisements received: Number of summary advertisements received by this switch on its trunk ports.

Subset advertisements received: Number of subset advertisements received by this switch on its trunk ports.

Request advertisements received: Number of advertisement requests received by this switch on its trunk ports.

Summary advertisements transmitted: Number of summary advertisements sent by this switch on its trunk ports.

Subset advertisements transmitted: Number of subset advertisements sent by this switch on its trunk ports.

Request advertisements transmitted: Number of advertisement requests sent by this switch on its trunk ports.

Number of config revision errors: Number of revision errors.

Number of config digest errors: Number of MD5 digest errors.

7.14.1.2 show vtp password

This command displays the VTP domain password.

Syntax

show vtp password

Default Setting

None

Command Mode

Privileged Exec

Display Message

VTP Password: Displays the VTP domain password.

7.14.1.3 show vtp status

This command displays the VTP domain status.

Syntax

show vtp status

Default Setting

None

Command Mode

Privileged Exec

Display Message

VTP Status: Indicates whether VTP is enabled or disabled.

VTP Version: Displays the VTP version operating on the switch.

Configuration Revision: Displays the current configuration revision number on this switch.

Maximum VTP supported VLANs: Maximum number of VLANs supported locally.

VTP support VLAN number: Number of existing VLANs.

VTP Operating Mode: Displays the VTP operating mode, which can be server, client, or transparent.

VTP Domain Name: Displays the name that identifies the administrative domain for the switch.

VTP Pruning Mode: Displays whether pruning is enabled or disabled.

VTP V2 Mode: Displays if VTP version 2 mode is enabled. By default, all VTP version 2 switches operate in version 1 mode.

MD5 digest: Displays the checksum values for the VTP domain status.

Configuration last modified: Displays the time stamp of the last configuration modification and the IP address of the switch that caused the configuration change to the database.

Local updater ID: Displays the Local updater ID for the VTP domain status.

7.14.1.4 show vtp trunkport

This command displays the VTP trunkport status.

Syntax

```
show vtp trunkport
```

Default Setting

None

Command Mode

Privileged Exec

Display Message

Port: Displays the interface number.

Trunkport: Displays the trukport status (enable or disable) on the interface number.

7.14.2 Configuration Commands

7.14.2.1 vtp

This command uses to configure global VTP administrative mode.

Syntax

```
vtp
no vtp
```

no - This command disables global VTP administrative mode.

Default Setting

Disabled

Command Mode

Global Config

7.14.2.2 vtp domain

This command uses to set VTP administrative domain name.

Syntax

```
vtp domain <string>
no vtp domain
```

<string> - Configures the string for domain name. (maximum length 32 bytes)

no - This command resets the domain name to NULL.

The system disables the VTP for its initialization.

The maximum length of administrative domain name is 32 bytes.

The system's default administrative domain name is NULL.

Default Setting

None

Command Mode

Global Config

7.14.2.3 vtp mode

This command uses to set VTP device mode. There are theree modes you can configure, **Client**, **Server**, and **Transparent**.

Syntax

```
vtp mode { client | server | transparent }
no vtp mode
```

<client> **-** This command set client mode for VTP.

<server> **-** This command set server mode for VTP.

<transparent> - This command set transparent mode for VTP.

no - This command resets the VTP mode to default value.

Default Setting

Server

Command Mode

Global Config

7.14.2.4 vtp version

Use the no vtp version to reset the VTP version number to default value..

Syntax

```
vtp version <1-2>
no vtp version
```

no - This command resets the VTP version to default value.

Default Setting

1

Command Mode

Global Config

7.14.2.5 vtp password

This command uses to configure the VTP administrative domain password.

Syntax

```
vtp password <password>
no vtp password
```

<password> - Configures VTP administrative domain password.(Max. length 64 bytes)

no - This command resets the VTP domain password to default value.

Default Setting

None

Command Mode

Global Config

7.14.2.6 vtp pruning

This command uses to configure the adminstrative domain to permit pruning

Syntax

```
vtp pruning
no vtp pruning
```

no - This command resets the pruning mode to default value.

Default Setting

Disabled

Command Mode

Global Config

7.14.2.7 vtp trunkport

This command uses to configure the adminstrative domain trunk port for all of interfaces.

Syntax

```
vtp trunkport all
no vtp trunkport all
```

no - This command resets the adminstrative domain trunk port to default value.

Default Setting

Disabled

Command Mode

Global Config

This command uses to configure the adminstrative domain trunk port on specific interfaces.

Syntax

```
vtp trunkport
no vtp trunkport
```

no - This command resets the adminstrative domain trunk port to default value.

Default Setting

Disabled

Command Mode

Interface Config

7.15 Protected Ports Commands

7.15.1 Show Commands

7.15.1.1 show switchport protected

This command displays the status of all the interfaces, including protected and unprotected interfaces.

Syntax
show switchport protected {all|<0-2>}

Default Setting

None

Command Mode

Privileged Exec

Display Message

Name: An name of the protected port group.

Member Ports: List of ports, which are configured as protected for the group identified with <groupid>. If no port is configured as protected for this group, this field is blank.

7.15.1.2 show interface switchport protected

This command displays the status of the interface (protected/unprotected) under the groupid.

Syntax
show interface switchport protected <slot/port> <groupid>

Default Setting

None

Command Mode

Privileged Exec

Display Message

Name: An name of the protected port group.

Protected: Indicates whether the interface is protected or not. It shows TRUE or FALSE. If the group is a multiple groups then it shows TRUE in Group <groupid>.

7.15.2 Configuration Commands

7.15.2.1 switchport protected

This command used to modify a protected port group name. The <groupid> parameter identifies the set of protected ports. Use the name <name> pair to assign a name to the protected port group. The name can be up to 32 alphanumeric characters long, including blanks. The default is blank.

Port protection occurs within a single switch. Protected port configuration does not affect traffic between ports on two different switches. No traffic forwarding is possible between two protected ports.

Syntax

```
switchport protected <0-2> name <name>
no switchport protected <0-2> name
```

<name> - Assigns a name to the protected port group.

no - Remove a name from the protected port group.

Default Setting

None

Command Mode

Global Config

This command uses to add an interface to a protected port group. The <groupid> parameter identifies the set of protected ports to which this interface is assigned. You can only configure an interface as protected in one group.

Syntax

```
switchport protected <0-2>
no switchport protected <0-2>
```

no - This command uses to configure a port as unprotected.

Default Setting

None

Command Mode

Interface Config

7.16 Static MAC Filtering Commands

7.16.1 Show Commands

7.16.1.1 show mac-address-table static

This command displays the Static MAC Filtering information for all Static MAC Filters. If you select <all>, all the Static MAC Filters in the system are displayed. If you supply a value for <macaddr>, you must also enter a value for <vlanid>, and the system displays Static MAC Filter information only for that MAC address and VLAN.

Syntax

```
show mac-address-table static {<macaddr> <1-3965> | all}
```

<macaddr> - Static MAC address.

Default Setting

None

Command Mode

Privileged Exec

Display Message

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).

7.16.2 Configuration Commands

7.16.2.1 macfilter

This command adds a static MAC filter entry for the MAC address <macaddr> on the VLAN <vlanid>. The value of the <macaddr> parameter is 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. You can create up to 100 static MAC filters.

Syntax

```
macfilter <macaddr> <1-3965>
no macfilter <macaddr> <1-3965>
```

<macaddr> - Specified a 6-byte hexadecimal number in the format of b1:b2:b3:b4:b5:b6.

no - This command removes all filtering restrictions and the static MAC filter entry for the MAC address <macaddr> on the VLAN <vlanid>.

Default Setting

None

Command Mode

Global Config

7.16.2.2 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.

Syntax

```
macfilter addsrc <macaddr> <1-3965>
no macfilter addsrc <macaddr> <1-3965>
```

<macaddr> - Specified a 6-byte hexadecimal number in the format of b1:b2:b3:b4:b5:b6.

no - This command removes a port from the source filter set for the MAC filter with the MAC address of <macaddr> and VLAN of <vlanid>.

Default Setting

None

Command Mode

Interface Config

7.16.2.3 macfilter addsrc all

This command adds all interfaces to the source filter set for the MAC filter with the MAC address of <macaddr> and <vlanid>. You must specify the <macaddr> parameter as a 6-byte hexadecimal number in the format of b1:b2:b3:b4:b5:b6. The <vlanid> parameter must identify a valid VLAN.

Syntax
macfilter addsrc all <macaddr> <1-3965> no macfilter addsrc all <macaddr> <1-3965>

<macaddr> - Specified a 6-byte hexadecimal number in the format of b1:b2:b3:b4:b5:b6.

no - This command removes all interfaces to the source filter set for the MAC filter with the MAC address of <macaddr> and VLAN of <vlanid>.

Default Setting

None

Command Mode

Global Config

7.17 System Utilities

7.17.1 clear

7.17.1.1 clear arp

This command causes all ARP entries of type dynamic to be removed from the ARP cache.

Syntax
clear arp

Default Setting

None

Command Mode

Privileged Exec

7.17.1.2 clear traplog

This command clears the trap log.

Syntax

clear traplog

Default Setting

None

Command Mode

Privileged Exec

7.17.1.3 clear eventlog

This command is used to clear the event log, which contains error messages from the system.

Syntax

clear eventlog

Default Setting

None

Command Mode

Privileged Exec

7.17.1.4 clear logging buffered

This command is used to clear the message log maintained by the switch. The message log contains system trace information.

Syntax

clear logging buffered

Default Setting

None

Command Mode

Privileged Exec

7.17.1.5 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.

Syntax

clear config

Default Setting

None

Command Mode

Privileged Exec

7.17.1.6 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.

Syntax

clear pass

Default Setting

None

Command Mode

Privileged Exec

7.17.1.7 clear counters

This command clears the stats for a specified <slot/port> or for all the ports or for the entire switch based upon the argument.

Syntax

clear counters [<slot/port> | all]

<slot/port> - is the desired interface number.

all - All interfaces.

Default Setting

None

Command Mode

Privileged Exec

7.17.1.8 clear dns

This command sets the DNS configuration to default value. The command will only clear the DNS statistics(used option command **counter**) or only clear all entries from the DNS cache(used option command **cache**).

Syntax

clear dns [counter | cache]

counter - this command clear the DNS statistics.

cache - this command clear all entries from the DNS cache.

Default Setting

None

Command Mode

Privileged Exec

7.17.1.9 clear cdp

This command is used to clear the CDP neighbors information and the CDP packet counters.

Syntax

clear cdp [traffic]

traffic - this command is used to clear the CDP packet counters.

Default Setting

None

Command Mode

Privileged Exec

7.17.1.10 clear vlan

This command resets VLAN configuration parameters to the factory defaults.

Syntax

clear vlan

Default Setting

None

Command Mode

Privileged Exec

7.17.1.11 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.

Syntax

clear igmpsnooping

Default Setting

None

Command Mode

Privileged Exec

7.17.1.12 clear port-channel

This command clears all port-channels (LAGs).

Syntax

clear port-channel

Default Setting

None

Command Mode

Privileged Exec

7.17.1.13 clear ip filter

This command is used to clear all ip filter entries.

Syntax

clear ip filter

Default Setting

None

Command Mode

Privileged Exec

7.17.1.14 clear dot1x statistics

This command resets the 802.1x statistics for the specified port or for all ports.

Syntax

clear dot1x statistics {all | <slot/port>}

<slot/port> - is the desired interface number.

all - All interfaces.

Default Setting

None

Command Mode

Privileged Exec

7.17.1.15 clear radius statistics

This command is used to clear all RADIUS statistics.

Syntax

clear radius statistics

Default Setting

None

Command Mode

Privileged Exec

7.17.1.16 clear domain-list

This command is used to clear all entries domain names for incomplete host names.

Syntax

clear domain-list

Default Setting

None

Command Mode

Privileged Exec

7.17.1.17 clear hosts

This command is used to clear all static host name-to-address mapping.

Syntax

clear hosts

Default Setting

None

Command Mode

Privileged Exec

7.17.1.18 clear port-security dynamic address

This command is used to clear the Dynamic MAC address by using the specified port (**interface <slot/port>**) or mac address (**address <mac-addr>**).

Syntax

clear port-security dynamic {address <mac-addr> | interface <slot/port> }

<mac-addr> - mac address you want to remove.

<slot/port> - mac address learning on this interface will be removed.

Default Setting

None

Command Mode

Privileged Exec

7.17.1.19 clear ip 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. If interface keyword is specified, he dymanic entries of that interface on the ARP cache Table are purged.

Syntax

clear ip arp-cache [gateway | interface <slot/port>]

<slot/port> - Interface number.

Default Setting

None

Command Mode

Privileged Exec

7.17.1.20 clear lldp statistics

This command will use to reset all LLDP statistics.

Syntax

clear lldp statistics

Default Setting

None

Command Mode

Privileged Exec

7.17.1.21 clear lldp remote-data

This command will use to delete all information from the LLDP remote data table.

Syntax

clear lldp remote-data

Default Setting

None

Command Mode

Privileged Exec

7.17.1.22 enable passwd

This command changes Privileged EXEC password.

Syntax

enable passwd

Default Setting

None

Command Mode

Global Config.

7.17.1.23 enable passwd encrypted

This command allows the administrator to transfer the enable password between devices without having to know the password. The *<password>* parameter must be exactly 128 hexidecimal characters.

Syntax

enable passwd encrypted <password>

Default Setting

None

Command Mode

Global Config.

7.17.1.24 clear ipv6 neighbors

This command will use to clear all entries IPv6 neighbor table or an entry on a specific interface. Use the <slot/port> parameter to specify the interface.

Syntax

clear ipv6 neighbors [<slot/port>]

<slot/port> - Specify the interface.

Default Setting

None

Command Mode

Privileged Exec

7.17.1.25 clear ipv6 statistics

This command will use to clear IPv6 statistics for all interfaces or for a specific interface, including loopback and tunnel interfaces. IPv6 statistics display in the output of the show ipv6 traffic command. If you do not specify an interface, the counters for all IPv6 traffic statistics reset to zero.

Syntax

clear ipv6 statistics [{<slot/port> | loopback <loopback-id> | tunnel <tunnel-id>}]

<slot/port> - Specify the interface.

<loopback-id > - Specify loopback Interface ID. Range 0 -7.

<tunnel-id > - Specify the Tunnel ID. Range 0 -7.

Default Setting

None

Command Mode

Privileged Exec

7.17.1.26 clear ipv6 dhcp

This command will use to clear DHCPv6 statistics for all interfaces or for a specific interface. Use the <slot/port> parameter to specify the interface.

Syntax

```
clear ipv6 dhcp {statistics | interface <slot/port> statistics}
```

<slot/port> - Specify the interface.

Default Setting

None

Command Mode

Privileged Exec

7.17.2 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 config (startup-config), event log (eventlog), message log (msglog) and trap log (traplog). A URL is specified for the destination.

The command can also be used to download the startup config or code image by specifying the source as a URL and destination as startup-config or image respectively.

The command can be used to the save the running config to flash by specifying the source as running-config and the destination as startup-config {*filename*}.

The command can also be used to download ssh key files as sshkey-rsa, sshkey-rsa2, and sshkey-dsa and http secure-server certificates as sslpem-root, sslpem- server, sslpem-dhweak, and sslpem-dhstrong.

Upload file from switch

Syntax

```
copy startup-config <url> <sourcefilename>
copy {errorlog | log | traplog} <url>
copy script <sourcefilename> <url>
copy image <filename> <url>

where <url>={xmodem | tftp://ipaddr/path/file | ftp://user:pass@ipaddr/path/file}
```

<sourcefilename> - The filename of a configuration file or a script file.

<url> - xmodem, tftp://ipaddr/path/file or ftp://user:pass@ipaddr/path/file.

errorlog - event Log file.

log - message Log file.

traplog - trap Log file.

<filename> - Operation code file name.

Default Setting

None

Command Mode

Privileged Exec

Download file to switch

Syntax

```
copy <url> startup-config <destfilename>
copy <url> image <destfilename>
copy <url> {sshkey-rsa1 | sshkey-rsa2 | sshkey-dsa}
copy <url> {sslpem-root | sslpem-server | sslpem-dhweak | sslpem-dhstrong}
copy <url> script <destfilename>

where <url>={xmodem | tftp://ipaddr/path/file | ftp://user:pass@ipaddr/path/file }
```

<destfilename> - name of the image file or the script file.

<url> - xmodem, tftp://ipaddr/path/file or ftp://user:pass@ipaddr/path/file.

sshkey-rsa1 - SSH RSA1 Key file.

sshkey-rsa2 - SSH RSA2 Key file.

sshkey-dsa - SSH DSA Key file.

sslpem-root - Secure Root PEM file.

sslpem-server - Secure Server PEM file.

sslpem-dhweak - Secure DH Weak PEM file.

sslpem-dhstrong - Secure DH Strong PEM file.

Default Setting

None

Command Mode

Privileged Exec

Write running configuration file into flash

Syntax

```
copy running-config startup-config [filename]
```

<filename> - name of the configuration file.

Default Setting

None

Command Mode

Privileged Exec

This command upload or download the pre-login banner file

Syntax

```
copy clibanner <url>
copy <url> clibanner
no clibanner
```

<url> - xmodem, tftp://ipaddr/path/file or ftp://user:pass/ipaddr/path/file.

no - Delete CLI banner.

Default Setting

None

Command Mode

Privileged Exec

7.17.3 delete

This command is used to delete a configuration or image file.

Syntax

```
delete <filename>
```

<filename> - name of the configuration or image file.

Default Setting

None

Command Mode

Privileged Exec

7.17.4 dir

This command is used to display a list of files in Flash memory.

Syntax

dir [boot-rom | config | opcode [<filename>]]

<filename> - name of the configuration or image file.

boot-rom - bootrom.

config - configuration file.

opcode - run time operation code.

Default Setting

None

Command Mode

Privileged Exec

Display Message

Column Heading	Description
date	The date that the file was created.
file name	The name of the file.
file type	File types: Boot-Rom, Operation Code, and Config file.
startup	Shows if this file is used when the system is started.
size	The length of the file in bytes.

7.17.5 whichboot

This command is used to display which files were booted when the system powered up.

Syntax

whichboot

Default Setting

None

Command Mode

Privileged Exec

7.17.6 boot-system

This command is used to specify the file or image used to start up the system.

Syntax

boot-system {boot-rom | config | opcode} <filename>

<filename> - name of the configuration or image file.

boot-rom - bootrom.

config - configuration file.

opcode - run time operation code.

Default Setting

None

Command Mode

Privileged Exec

7.17.7 ping

7.17.7.1 ping <ipaddress|host>

This command checks if another computer is on the network and listens 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.

Syntax

```
ping <ipaddress|hostname> count <0-20000000> [size <32-512>]
ping <ipaddress|hostname> size <32-512> [count <0-20000000>]
```

< ipaddress|hostname> - a host name or an IP address.

<0-20000000> - number of pings (Range: 0 - 20000000). Note that 0 means infinite.

<size> - packet size (Range: 32 - 512).

Default Setting

Count = 5

Size = 32

Command Mode

Privileged Exec

7.17.7.2 ping ipv6 <ipv6-address|hostname>

This command use to determine whether another computer is on the network. To use the 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. Use the <ipv6-address> parameter to ping an interface by using the global IPv6 address of the interface, or use the <hostname> parameter to ping a interface by using the hostname of the target. Use the optional size keyword to specify the size of the ping packet.

Syntax

```
ping ipv6 <ipv6-address|hostname> [size <datagram-size>]
```

<ipv6-address|hostname> - A global IPv6 address or valid hostname.

<datagram-size> - Datagram size. Range 48 - 2048.

Default Setting

None

Command Mode

Privileged Exec

7.17.7.3 ping ipv6 interface

This command use to determine whether another computer is on the network. To use the 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. Use the interface keyword to ping an interface by using the link-local address. You can use a loopback, tunnel, or logical interface as the source. Use the optional size keyword to specify the size of the ping packet.

Syntax

ping ipv6 interface {<slot/port> | serviceport | switchport | tunnel <tunnel-id>} | loopback <loopback-id>} {<link-local-address>} [size <datagram-size>]

<slot/port> - Specify the interface.

<tunnel-id > - Specify the Tunnel ID. Range 0 -7.

<loopback-id > - Specify loopback Interface ID. Range 0 -7.

<link-local-address> - Specify link-local address.

<ipv6-address> - Specify the IPv6 address of the device.

<datagram-size> - Datagram size. Range 48 - 2048.

Default Setting

None

Command Mode

Privileged Exec

7.17.8 traceroute

7.17.8.1 traceroute

Use the traceroute command to discover the routes that packets actually take when traveling to their destination through the network on a hop-by-hop basis. Traceroute continues to provide a synchronous response when initiated from the CLI.

Syntax

traceroute <ipaddr|hostname> [initTtl <initTtl>] [maxTtl <maxTtl>] [interval <interval>] [count <count>]

<ipaddr|hostname> - The IP address or destination host you want to trace.

<initTtl> - The Use initTtl to specify the initial time-to-live (TTL), the maximum number of router hops between the local and remote system. Range is 1 to 255.

<maxTtl> - Use maxTtle to specify the maximum TTL. Range is 1 to 255.

<interval> - Use interval to specify the time between probes, in seconds. Range is 1 to 60 seconds.

<count> - Use the optional count parameter to specify the number of probes to send for each TTL value. Range is 1 to 10 probes.

Default Setting

None

Command Mode

Previledge Mode

7.17.8.2 traceroute ipv6

This command is used to discover the routes that packets actually take when traveling to their destination through the network on a hop-by-hop basis. The <ipv6-address|hostname> parameter must be a valid IPv6 address|hostname.

Syntax
traceroute ipv6 <ipv6-address|hostname > [initTtl <initTtl>] [maxTtl <maxTtl>] [interval <interval>] [count <count>]

<ipv6-address|hostname> - A valid IPv6 address or hostname.

<ipaddr> - The IP address or destination host you want to trace.

<initTtl> - The Use initTtl to specify the initial time-to-live (TTL), the maximum number of router hops between the local and remote system. Range is 1 to 255.

<maxTtl> - Use maxTtle to specify the maximum TTL. Range is 1 to 255.

<interval> - Use interval to specify the time between probes, in seconds. Range is 1 to 60 seconds.

<count> - Use the optional count parameter to specify the number of probes to send for each TTL value. Range is 1 to 10 probes.

Default Setting

None

Command Mode

Privileged Exec

7.17.9 logging cli-command

This command enables the CLI command Logging feature. The Command Logging component enables the switch to log all Command Line Interface (CLI) commands issued on the system.

Syntax

logging cli-command

Default Setting

None

Command Mode

Global Config

7.17.10 calendar set

This command is used to set the system clock.

Syntax

calendar set <hh:mm:ss> <1-31> <1-12> <2000-2099>

<hh:mm:ss> - hh in 24-hour format (Range: 0 - 23), mm (Range: 0 - 59), ss (Range: 0 - 59)

<1-31> - Day of month. (Range: 1 - 31).

<1-12> - Month. (Range: 1 - 12).

<2000-2099> - Year (4-digit). (Range: 2000 - 2099).

Default Setting

None

Command Mode

Privileged Exec

7.17.11 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.

Syntax

reload

Default Setting

None

Command Mode

Privileged Exec

7.17.12 configure

This command is used to activate global configuration mode.

Syntax

configure

Default Setting

None

Command Mode

Privileged Exec

7.17.13 disconnect

This command is used to close a telnet session.

Syntax

disconnect {<0-58> | all}

<0-11> - telnet session ID.

all - all telnet sessions.

Default Setting

None

Command Mode

Privileged Exec

7.17.14 hostname

This command is used to set the prompt string.

Syntax

hostname <prompt_string>

<prompt_string> - Prompt string.

Default Setting

Fortinet

Command Mode

Global Config

7.17.15 quit

This command is used to exit a CLI session.

Syntax

quit

Default Setting

None

Command Mode

Privileged Exec

7.17.16 cablestatus

This command returns the status of the specified port.

Syntax

cablestatus <slot/port>

<slot/port> - Interface Number.

Default Setting

None

Command Mode

Privileged Exec

Display Message

Cable Status: One of the following statuses is returned:

Normal: The cable is working correctly.

Open: The cable is disconnected or there is a faulty connector.

Short: There is an electrical short in the cable.

Cable Test Failed: The cable status could not be determined. The cable may in fact be working.

Cable Length: If this feature is supported by the PHY for the current link speed, the cable length is displayed as a range between the shortest estimated length and the longest estimated length. Note that if the link is down and a cable is attached to a 10/100 Ethernet adapter, then the cable status may display as Open or Short because some Ethernet adapters leave unused wire pairs unterminated or grounded. Unknown is displayed if the cable length could not be determined.

7.18 DHCP Snooping Commands

DHCP snooping is a security feature that monitors DHCP messages between a DHCP client and DHCP servers to filter harmful DHCP messages and to build a bindings database of {MAC address, IP address, VLAN ID, port} tuples that are considered authorized. You can enable DHCP snooping globally and on specific VLANs, and configure ports within the VLAN to be trusted or untrusted. DHCP servers must be reached through trusted ports.

The DHCP snooping binding table contains the MAC address, IP address, lease time, binding type, VLAN number, and interface information that corresponds to the local untrusted interfaces of a switch; it does not contain information regarding hosts interconnected with a trusted interface. An untrusted interface is an interface that is configured to receive messages from outside the network or firewall. A trusted interface is an interface that is configured to receive only messages from within the network.

DHCP snooping acts like a firewall between untrusted hosts and DHCP servers. It also gives you a way to differentiate between untrusted interfaces connected to the end-user and trusted interfaces connected to the DHCP server or another switch.

DHCP snooping enforces the following security rules:

- DHCP packets from a DHCP server (DHCPOFFER, DHCPACK, DHCPNAK, DHCPRELEASEQUERY) are dropped if received on an untrusted port.
- DHCPRELEASE and DHCPDECLINE messages are dropped if for a MAC address in the snooping database, but the binding's interface is other than the interface where the message was received.
- On untrusted interfaces, the switch drops DHCP packets whose source MAC address does not match the client hardware address. This feature is a configurable option.

The hardware identifies all incoming DHCP packets on ports where DHCP snooping is enabled. DHCP snooping is enabled on a port if (a) DHCP snooping is enabled globally, and (b) the port is a member of a VLAN where DHCP snooping is enabled. On untrusted ports, the hardware traps all incoming DHCP packets to the CPU. On trusted ports, the hardware forwards client messages and copies server messages to the CPU so that DHCP snooping can learn the binding.

7.18.1 Show Commands

7.18.1.1 show ip dhcp snooping

This command displays the DHCP Snooping global configurations and per port configurations.

Syntax
show ip dhcp snooping

Default Setting

None

Command Mode

Privileged Exec

Display Message

Interface: The interface for which data is displayed.

Trusted: If it is enabled, DHCP snooping considers the port as trusted. The factory default is disabled.

Log Invalid Pkts: If it is enabled, DHCP snooping application logs invalid packets on the specified interface.

7.18.1.2 show ip dhcp snooping binding

This command displays the DHCP Snooping binding entries. To restrict the output, use the following options:

- Dynamic: Restrict the output based on DCHP snooping.
- Interface: Restrict the output based on a specific interface.
- Static: Restrict the output based on static entries.
- VLAN: Restrict the output based on VLAN.

Syntax
show ip dhcp snooping binding [{static/dynamic}] [interface slot/port] [vlan id]

Default Setting

None

Command Mode

Privileged Exec

Display Message

MAC Address: Displays the MAC address for the binding that was added. The MAC address is the key to the binding database.

IP Address: Displays the valid IP address for the binding rule.

VLAN: The VLAN for the binding rule.

Interface: The interface to add a binding into the DHCP snooping interface.

Type: Binding type; statically configured from the CLI or dynamically learned.

Lease (Secs): he remaining lease time for the entry.

7.18.1.3 show ip dhcp snooping database

This command displays the DHCP Snooping configuration related to the database persistency.

Syntax
show ip dhcp snooping database

Default Setting

None

Command Mode

Privileged Exec

Display Message

Agent URL: Bindings database agent URL.

Write Delay: The maximum write time to write the database into local or remote.

Abort Timer: The maximum time to abort the database transfer process.

7.18.1.4 show ip dhcp snooping statistics

This command lists statistics for DHCP Snooping security violations on untrusted ports.

Syntax
show ip dhcp snooping statistics

Default Setting

None

Command Mode

Privileged Exec

Display Message

Interface: The IP address of the interface in slot/port format.

MAC Verify Failures: Represents the number of DHCP messages that were filtered on an untrusted interface because of source MAC address and client HW address mismatch.

Client Ifc Mismatch: Represents the number of DHCP release and Deny messages received on the different ports than learned previously.

DHCP Server Msgs Rec'd: Represents the number of DHCP server messages received on untrusted ports.

7.18.2 Configuration Commands

7.18.2.1 ip dhcp snooping

This command enables the DHCP Snooping globally.

Syntax
ip dhcp snooping no ip dhcp snooping

no - This command disables the DHCP Snooping globally.

Default Setting

Disabled

Command Mode

Global Config

7.18.2.2 ip dhcp snooping vlan

This command enables the DHCP Snooping on a list of comma-separated VLAN ranges.

Syntax
ip dhcp snooping vlan <vlan-list> no ip dhcp snooping vlan <vlan-list>

no - This command disables the DHCP Snooping on VLANs.

Default Setting

Disabled

Command Mode

Global Config

7.18.2.3 ip dhcp snooping verify mac-address

This command enables the verification of the source MAC address with the client hardware address in the received DCHP message.

Syntax

```
ip dhcp snooping verify mac-address
no ip dhcp snooping verify mac-address
```

no - This command disables the verification of the source MAC address with the client hardware address.

Default Setting

Disabled

Command Mode

Global Config

7.18.2.4 ip dhcp snooping database

This command configures the persistent location of the DHCP Snooping database. This can be local or a remote file on a given IP machine.

Syntax

```
ip dhcp snooping database {local|tftp://hostIP/filename}
```

Default Setting

Local

Command Mode

Global Config

7.18.2.5 ip dhcp snooping database write-delay

This command configures the interval in seconds at which the DHCP Snooping database will be persisted. The interval value ranges from 15 to 86400 seconds.

Syntax

```
ip dhcp snooping database write-delay <in seconds>
no ip dhcp snooping database write-delay
```

no - This command sets the write delay value to the default value.

Default Setting

300 seconds

Command Mode

Global Config

7.18.2.6 ip dhcp snooping database timeout

This command configures the DHCP snooping bindings store timeout in <15> to <86400> seconds. 0 is defined as an infinite duration.

Syntax

```
ip dhcp snooping database timeout <in seconds>
no ip dhcp snooping database timeout
```

no - This command sets the timeout value to the default value.

Default Setting

300 seconds

Command Mode

Global Config

7.18.2.7 ip dhcp snooping binding

This command configures the static DHCP Snooping binding..

Syntax

```
ip dhcp snooping binding <mac-address> vlan <vlan id> <ip address> interface <interface id>
no ip dhcp snooping binding <mac-address>
```

no - This command removes the DHCP static entry from the DHCP Snooping database.

Default Setting

None

Command Mode

Global Config

7.18.2.8 ip dhcp snooping limit

This command controls the rate at which the DHCP Snooping messages come. The default rate is 15 pps with a range from 0 to 300 pps. The default burst level is 1 second with a range of 1 to 15 seconds.

Syntax

```
ip dhcp snooping limit {rate <pps> [burst interval <seconds>]}
no ip dhcp snooping limit
```

no - This command sets the rate at which the DHCP Snooping messages come, and the burst level, to the defaults.

Default Setting

15 pps for rate limiting and 1 sec for burst interval

Command Mode

Interface Config

7.18.2.9 ip dhcp snooping log-invalid

This command controls the logging DHCP messages filtration by the DHCP Snooping application.

Syntax

```
ip dhcp snooping log-invalid
no ip dhcp snooping log-invalid
```

no - This command disables the logging DHCP messages filtration by the DHCP Snooping application.

Default Setting

Disabled

Command Mode

Interface Config

7.18.2.10 ip dhcp snooping trust

This command configures the port as trusted.

Syntax

```
ip dhcp snooping trust
no ip dhcp snooping trust
```

no - This command configures the port as untrusted.

Default Setting

Disabled

Command Mode

Interface Config

7.18.2.11 ip dhcp snooping information option

This command ip dhcp snooping information option enables the DHCP L2 option mode on the system.

Syntax

```
ip dhcp snooping information option
no ip dhcp snooping information option
```

no - This command disables the DHCP L2 option mode.

Default Setting

Disabled

Command Mode

Global Config

7.18.2.12 ip dhcp snooping information option allow-untrusted

This command ip dhcp snooping information option allow-untrusted is used to allow DHCP packet received form untrusted port with option 82 data.

Syntax

```
ip dhcp snooping information option allow-untrusted
no ip dhcp snooping information option allow-untrusted
```

no - This command disallows DHCP packet received form untrusted port with option 82 data.

Default Setting

Disabled

Command Mode

Global Config

7.19 IP Source Guard (IPSG) Commands

IP Source Guard (IPSG) is a security feature that filters IP packets based on source ID. The source ID may be either the source IP address or a {source IP address, source MAC address} pair. The DHCP snooping binding database and static IPSG entries identify authorized source IDs. You can configure:

- Whether enforcement includes the source MAC address.
- Static authorized source IDs.

Similar to DHCP snooping, this feature is enabled on a DHCP snooping untrusted Layer 2 port. Initially, all IP traffic on the port is blocked except for DHCP packets that are captured by the DHCP snooping process. When a client receives a valid IP address from the DHCP server, or when a static IP source binding is configured by the user, a per-port and VLAN Access Control List is installed on the port. This process restricts the client IP traffic to those source IP addresses configured in the binding; any IP traffic with a source IP address other than that in the IP source binding is filtered out. This filtering limits a host's ability to attack the network by claiming a neighbor host's IP address.

IPSG can be enabled on physical or LAG ports. IPSG is disabled by default. If you enable IPSG on a port where DHCP snooping is disabled or where DHCP snooping is enabled but the port is trusted, all IP traffic received on that port is dropped depending on the admin-configured IPSG entries. IPSG cannot be enabled on a port-based routing interface.

7.19.1 Show Commands

7.19.1.1 show ip verify

This command displays the IPSG interface configurations on all ports.

Syntax

```
show ip verify [interface <slot/port>]
```

Default Setting

None

Command Mode

Privileged Exec

Display Message

Interface: Interface address in slot/port format.

Filter Type: Is one of two values:

- **ip-mac:** User has configured MAC address filtering on this interface.
- **ip:** Only IP address filtering on this interface.

7.19.1.2 show ip verify source

This command displays the IPSG interface and binding configurations on all ports.

Syntax

```
show ip verify source [interface <slot/port>]
```

Default Setting

None

Command Mode

Privileged Exec

Display Message

Interface: Interface address in slot/port format.

Filter Type: Is one of two values:

- **ip-mac:** User has configured MAC address filtering on this interface.
- **ip:** Only IP address filtering on this interface.

IP Address: IP address of the interface.

MAC Address: If MAC address filtering is not configured on the interface, the MAC Address field is empty. If port security is disabled on the interface, then the MAC Address field displays "permit-all".

VLAN: The VLAN for the binding rule.

7.19.1.3 show ip source binding

This command displays the IPSG bindings.

Syntax

```
show ip source binding [{static/dhcp-snooping}] [interface <slot/port>] [vlan id]
```

Default Setting

None

Command Mode

Privileged Exec

Display Message

MAC Address: The MAC address for the entry that is added.

IP Address: The IP address of the entry that is added.

Type: Entry type; statically configured from CLI or dynamically learned from DHCP Snooping.

VLAN: VLAN for the entry.

Interface: IP address of the interface in slot/port format.

7.19.2 Configuration Commands

7.19.2.1 ip verify source

This command configures the IPSG source ID attribute to filter the data traffic in the hardware. Source ID is the combination of IP address and MAC address. Normal command allows data traffic filtration based on the IP address. With the "port-security" option, the data traffic will be filtered based on the IP and MAC addresses.

Syntax

```
ip verify source {port-security}
no ip verify source {port-security}
```

no - This command disables the IPSG configuration in the hardware.

Default Setting

Disabled

Command Mode

Interface Config

7.19.2.2 ip verify binding

This command configures static IP source guard (IPSG) entries.

Syntax

ip verify binding <mac-address> vlan <vlan id> <ip address> interface <slot/port>
no ip verify binding <mac-address> vlan <vlan id> <ip address> interface <slot/port>

no - This command removes the IPSG static entry from the IPSG database.

Default Setting

None

Command Mode

Global Config

7.20 Dynamic ARP Inspection (DAI) Command

Dynamic ARP Inspection (DAI) is a security feature that rejects invalid and malicious ARP packets. DAI prevents a class of man-in-the-middle attacks, where an unfriendly station intercepts traffic for other stations by poisoning the ARP caches of its unsuspecting neighbors. The miscreant sends ARP requests or responses mapping another station's IP address to its own MAC address.

To prevent ARP poisoning attacks, a switch must ensure that only valid ARP requests and responses are relayed. DAI prevents these attacks by intercepting all ARP requests and responses. Each of these intercepted packets is verified for valid MAC address to IP address bindings before the local ARP cache is updated or the packet is forwarded to the appropriate destination. Invalid ARP packets are dropped.

DAI determines the validity of an ARP packet based on valid MAC address to IP address bindings stored in a trusted database. This database is built at runtime by DHCP snooping, provided this feature is enabled on VLANs and on the switch. DAI relies on DHCP snooping. DHCP snooping listens to DHCP message exchanges and builds a binding database of valid {MAC address, IP address, VLAN, and interface} tuples. In addition, in order to handle hosts that use statically configured IP addresses, DAI can also validate ARP packets against user-configured ARP ACLs.

When DAI is enabled, the switch drops ARP packets whose sender MAC address and sender IP address do not match an entry in the DHCP snooping bindings database. You can optionally configure additional ARP packet validation.

7.20.1 Show Commands

7.20.1.1 show ip arp inspection statistics

This command displays the statistics of the ARP packets processed by Dynamic ARP Inspection. Give the vlan-list argument and the command displays the statistics on all DAI-enabled VLANs in that list. Give

the single vlan argument and the command displays the statistics on that VLAN. If no argument is included, the command lists a summary of the forwarded and dropped ARP packets.

Syntax

show ip arp inspection statistics [vlan <vlan-list>]

Default Setting

None

Command Mode

Privileged Exec

Display Message

VLAN: The VLAN ID for each displayed row.

Forwarded: The total number of valid ARP packets forwarded in this VLAN.

Dropped: The total number of not valid ARP packets dropped in this VLAN.

DHCP Drops: The number of packets dropped due to DHCP snooping binding database match failure.

ACL Drops: The number of packets dropped due to ARP ACL rule match failure.

DHCP Permits: The number of packets permitted due to DHCP snooping binding database match.

ACL Permits: The number of packets permitted due to ARP ACL rule match.

Bad Src MAC: The number of packets dropped due to Source MAC validation failure.

Bad Dest MAC: The number of packets dropped due to Destination MAC validation failure.

Invalid IP: The number of packets dropped due to invalid IP checks.

7.20.1.2 show ip arp inspection

This command displays the Dynamic ARP Inspection global configuration and configuration on all the VLANs. With the vlan-list argument (i.e. comma separated VLAN ranges), the command displays the global configuration and configuration on all the VLANs in the given VLAN list. The global configuration includes the source mac validation, destination mac validation and invalid IP validation information.

Syntax

show ip arp inspection [vlan <vlan-list>]

Default Setting

None

Command Mode

Privileged Exec

Display Message

Source MAC Validation: Displays whether Source MAC Validation of ARP frame is enabled or disabled.

Destination MAC Validation: Displays whether Destination MAC Validation is enabled or disabled.

IP Address Validation: Displays whether IP Address Validation is enabled or disabled.

VLAN: The VLAN ID for each displayed row.

Configuration: Displays whether DAI is enabled or disabled on the VLAN.

Log Invalid: Displays whether logging of invalid ARP packets is enabled on the VLAN.

ACL Name: The ARP ACL Name, if configured on the VLAN.

Static Flag: If the ARP ACL is configured static on the VLAN.

7.20.1.3 show ip arp inspection interfaces

This command displays the Dynamic ARP Inspection configuration on all the DAI-enabled interfaces. An interface is said to be enabled for DAI if at least one VLAN, that the interface is a member of, is enabled for DAI. Given a slot/port interface argument, the command displays the values for that interface whether the interface is enabled for DAI or not.

Syntax

show ip arp inspection interfaces [slot/port]

<slot/port> - Interface Number.

Default Setting

None

Command Mode

Privileged Exec

Display Message

Interface: The interface ID for each displayed row.

Trust State: Whether the interface is trusted or untrusted for DAI.

Rate Limit: The configured rate limit value in packets per second.

Burst Interval: The configured burst interval value in seconds.

7.20.1.4 show arp access-list

This command displays the configured ARP ACLs with the rules. Giving an ARP ACL name as the argument will display only the rules in that ARP ACL.

Syntax

```
show arp access-list [acl-name]
```

Default Setting

None

Command Mode

Privileged Exec

7.20.2 Configuration Commands

7.20.2.1 ip arp inspection validate

This command enables additional validation checks like source-mac validation, destination-mac validation, and ip address validation on the received ARP packets.

Syntax

```
ip arp inspection validate {[src-mac] [dst-mac] [ip]}
no ip arp inspection validate {[src-mac] [dst-mac] [ip]}
```

no - This command disables the additional validation checks on the received ARP packets.

Default Setting

Disabled

Command Mode

Global Config

7.20.2.2 ip arp inspection vlan

This command enables Dynamic ARP Inspection on a list of comma-separated VLAN ranges.

Syntax

```
ip arp inspection vlan <vlan-list>
no ip arp inspection vlan <vlan-list>
```

no - This command disables Dynamic ARP Inspection on a list of comma-separated VLAN ranges.

Default Setting

Disabled

Command Mode

Global Config

7.20.2.3 ip arp inspection vlan logging

This command enables logging of invalid ARP packets on a list of comma-separated VLAN ranges.

Syntax

```
ip arp inspection vlan <vlan-list> logging
no ip arp inspection vlan <vlan-list> logging
```

no - This command disables logging of invalid ARP packets on a list of comma-separated VLAN ranges.

Default Setting

Disabled

Command Mode

Global Config

7.20.2.4 ip arp inspection filter

This command configures the ARP ACL used to filter invalid ARP packets on a list of comma-separated VLAN ranges. If the static keyword is given, packets that do not match a permit statement are dropped without consulting the DHCP snooping bindings.

Syntax

```
ip arp inspection filter <acl-name> vlan <vlan-list> [static]
no ip arp inspection filter <acl-name> vlan <vlan-list> [static]
```

no - This command unconfigures the ARP ACL used to filter invalid ARP packets on a list of comma-separated VLAN ranges.

Default Setting

No ARP ACL is configured on a VLAN

Command Mode

Global Config

7.20.2.5 ip arp inspection trust

This command configures an interface as trusted for Dynamic ARP Inspection.

Syntax

```
ip arp inspection trust
no ip arp inspection trust
```

no - This command configures an interface as untrusted for Dynamic ARP Inspection.

Default Setting

Disabled

Command Mode

Interface Config

7.20.2.6 ip arp inspection limit

This command configures the rate limit and burst interval values for an interface. Configuring none for the limit means the interface is not rate limited for Dynamic ARP Inspections.

Syntax

```
ip arp inspection limit {rate <pps> [burst interval <seconds>] | none}
no ip arp inspection limit
```

no - This command sets the rate limit and burst interval values for an interface to the default values of 15 pps and 1 second, respectively.

Default Setting

15 pps for rate and 1 second for burst-interval

Command Mode

Interface Config

7.20.2.7 arp access-list

This command creates an ARP ACL.

Syntax

```
arp access-list <acl-name>
no arp access-list <acl-name>
```

no - This command deletes a configured ARP ACL.

Default Setting

None

Command Mode

Global Config

7.20.2.8 permit ip host mac host

This command configures a rule for a valid IP address and MAC address combination used in ARP packet validation.

Syntax

```
permit ip host <sender-ip> mac host <sender-mac>
no permit ip host <sender-ip> mac host <sender-mac>
```

no - This command deletes a rule for a valid IP and MAC combination.

Default Setting

None

Command Mode

ARP Access-list Config

7.20.2.9 clear ip arp inspection statistics

This command resets the statistics for Dynamic ARP Inspection on all VLANs.

Syntax

```
clear ip arp inspection statistics
```

Default Setting

None

Command Mode

Privileged Exec

7.21 Differentiated Service Command

This Switching Command function can only be used on the QoS software version.

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

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 (that is, 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 FortiSwitch-548B Series L3 Switch DiffServ design:

- nested class support limited to:

  - '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
  - that is, 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.

le

7.21.1 General Commands

The following characteristics are configurable for the platform as a whole.

7.21.1.1 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.

Syntax
diffserv

Command Mode

Global Config

7.21.1.2 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.

Syntax

no diffserv

Command Mode

Global Config

7.21.2 Class Commands

The 'class' command set is used in DiffServ to define:

Traffic Classification specifies Behavior Aggregate (BA) based on DSCP, and Multi- Field (MF) classes of traffic (name, match criteria)

Service Levels specifies the BA forwarding classes / service levels. Conceptually, DiffServ is a two-level 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***.

7.21.2.1 class-map

This command defines a new DiffServ class of type match-all, match-any or match-access-group.

Syntax

class-map [match-all] <class-map-name> [{ipv4 | ipv6}]

<class-map-name> is a case sensitive alphanumeric string from 1 to 31 characters uniquely identifying the class.

When used without any match condition, this command enters the class-map mode. The **<class-map-name>** is the name of an existing DiffServ class.

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 optional keywords [{ipv4 | ipv6}] specify the Layer 3 protocol for this class. If not specified, this parameter defaults to ‘ipv4’. This maintains backward compatibility for configurations defined on systems before IPv6 match items were supported.

The CLI mode is changed to Class-Map Config or Ipv6-Class-Map Config when this command is successfully executed depending on the [{ipv4 | ipv6}] keyword specified.

Command Mode

Global Config

7.21.2.2 no class-map

This command eliminates an existing DiffServ class.

Syntax

```
no class-map <class-map-name>
```

<class-map-name> is the name of an existing DiffServ class.

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.

Command Mode

Global Config

7.21.2.3 class-map rename

This command changes the name of a DiffServ class.

Syntax

```
class-map rename <class-map-name> <new-class-map-name>
```

<class-map-name> is the name of an existing DiffServ class.

<new-class-map-name> is a case-sensitive alphanumeric string from 1 to 31 characters uniquely identifying the class.

The class name ‘default’ is reserved and must not be used here.

Default Setting

None

Command Mode

Global Config

7.21.2.4 match any

This command adds to the specified class definition a match condition whereby all packets are considered to belong to the class.

Syntax

match any

Default Setting

None

Command Mode

Class-Map Config / Ipv6-Class-Map Config

7.21.2.5 match class-map

This command adds to the specified class definition the set of match conditions defined for another class.

Syntax

match class-map <refclassname>

<**refclassname>** is the name of an existing DiffServ class whose match conditions are being referenced by the specified class definition.

There is no [**not**] option for this match command.

Default Setting

None

Command Mode

Class-Map Config / Ipv6-Class-Map Config

Restrictions The class types of both <***classname>*** and <***refclassname>*** must be identical (that is, 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>*** (that is, 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.

7.21.2.6 no match class-map

This command removes from the specified class definition the set of match conditions defined for another class.

Syntax

no match class-map <refclassname>

<**refclassname>** is the name of an existing DiffServ class whose match conditions are being referenced by the specified class definition.

There is no [**not**] option for this match command.

Default Setting

None

Command Mode

Class-Map Config / Ipv6-Class-Map Config

7.21.2.7 match cos

This command adds to the specified class definition a match condition for the Class of Service value (the only tag in a single tagged packet or the first or outer 802.1Q tag of a double VLAN tagged packet). The value may be from 0 to 7.

This command is not available on the Broadcom 5630x platform.

Syntax

match cos <0-7>

Default Setting

None

Command Mode

Class-Map Config

7.21.2.8 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 <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 <mac-mask> 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).

i This command is not available on the Broadcom 5630x platform.

Syntax

match destination-address mac <address> <mac-mask>

<address> - Specifies any layer 2 MAC address.

<mac-mask> - Specifies a layer 2 MAC address bit mask.

Default Setting

None

Command Mode

Class-Map Config

7.21.2.9 match dstip

This command adds to the specified class definition a match condition based on the destination IP address of a packet.

Syntax

match dstip <ipaddr> <ipmask>

<ipaddr> specifies an IP address.

<**ipmask>** specifies an IP address bit mask; note that although similar to a standard subnet mask, this bit mask need not be contiguous.

Default Setting

None

Command Mode

Class-Map Config

7.21.2.10 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.

Syntax
match dstl4port {<portkey> | <0-65535>}

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.

Default Setting

None

Command Mode

Class-Map Config / Ipv6-Class-Map Config

7.21.2.11 match ethertype

This command adds to the specified class definition a match condition based on the value of the ethertype. The <ethertype> value is specified as one of the following keywords: **appletalk, arp, ibmsna, ipv4, ipv6, ipx, mplsmcast, mplsucast, netbios, novell, pppoe, rarp** or as a custom ethertype value in the range of 0x0600-0xFFFF.

i This command is not available on the Broadcom 5630x platform.

Syntax

match ethertype {<keyword> | <0x0600-0xFFFF>}

<keyword> - Specifies appletalk, arp, ibmsna, ipv4, ipv6, ipx, mplsmcast etc

<0x0600-0xFFFF> - Specifies ethertype value.

Default Setting

None

Command Mode

Class-Map Config

7.21.2.12 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).

Syntax

match ip dscp <value>

<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.

i 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.

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 Setting

None

Command Mode

Class-Map Config / Ipv6-Class-Map Config

7.21.2.13 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.

Syntax

match ip precedence <0-7>

i

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.

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 Setting

None

Command Mode

Class-Map Config

7.21.2.14 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.

Syntax

match ip tos <tosbits> <tosmask>

<**tosbits>** is a two-digit hexadecimal number from 00 to ff.

<**tosmask>** is a two-digit hexadecimal number from 00 to ff.

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).

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.

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 Setting

None

Command Mode

Class-Map Config

7.21.2.15 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.

Syntax

match protocol {<protocol-name> | <0-255>}

<**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.

This command does not validate the protocol number value against the current list defined by IANA.

Default Setting

None

Command Mode

Class-Map Config / Ipv6-Class-Map Config

7.21.2.16 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 may not be contiguous, and is formatted as six, two-digit hexadecimal numbers separated by colons (e.g., ff:07:23:ff:fe:dc).

i This command is not available on the Broadcom 5630x platform.

Syntax

match source-address mac <address> <macmask>

<address> - Specifies any layer 2 MAC address.

<macmask> - Specifies a layer 2 MAC address bit mask.

Default Setting

None

Command Mode

Class-Map Config

7.21.2.17 match srcip

This command adds to the specified class definition a match condition based on the source IP address of a packet.

Syntax

match srcip <ipaddr> <ipmask>

<ipaddr> - specifies an IP address.

<**ipmask> -** specifies an IP address bit mask; note that although it resembles a standard subnet mask, this bit mask need not be contiguous.

Default Setting

None

Command Mode

Class-Map Config

7.21.2.18 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.

Syntax

match srcl4port {<portkey> | <0-65535>}

<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, 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.

Default Setting

None

Command Mode

Class-Map Config / IPv6-Class-Map Config

7.21.2.19 match vlan

This command adds to the specified class definition a match condition based on the value of the layer 2 VLAN Identifier field (the only tag in a single tagged packet or the first or outer tag of a double VLAN tagged packet). The VLAN ID is an integer from 1 to 4095.

This command is not available on the Broadcom 5630x platform.

Syntax

match vlan <1-4095>

Default Setting

None

Command Mode

Class-Map Config

7.21.2.20 match dstip6

This command adds to the specified class definition a match condition based on the destination IPv6 address of a packet.

Syntax

match dstip6 <destination-ipv6-prefix/prefix-length>

Default Setting

None

Command Mode

IPv6-Class-Map Config

7.21.2.21 match srcip6

This command adds to the specified class definition a match condition based on the source IP address of a packet.

Syntax

match srcip6 <source-ipv6-prefix/prefix-length>

Default Setting

None

Command Mode

IPv6-Class-Map Config

7.21.2.22 match ip6flowlbl

This command adds to the specified class definition a match condition based on the IPv6 flow label value.

Syntax

match ip6flowlbl <0- 1048575>

Default Setting

None

Command Mode

IPv6-Class-Map Config

7.21.3 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***.

7.21.3.1 assign-queue

This command modifies the queue id to which the associated traffic stream is assigned. The queueid is an integer from 0 to n-1, where n is the number of egress queues supported by the device.

Syntax

```
assign-queue <0-7>
```

<0-7> - Queue ID.

Command Mode

Policy-Class-Map Config

Incompatibilities

Drop

7.21.3.2 drop

This command specifies that all packets for the associated traffic stream are to be dropped at ingress.

Syntax

```
drop
```

Command Mode

Policy-Class-Map Config

Incompatibilities

Assign Queue, Mark (all forms), Mirror, Police, Redirect

7.21.3.3 mirror

This command specifies that all incoming packets for the associated traffic stream are copied to a specific egress interface (physical port or LAG).

i This command is not available on the Broadcom 5630x platform.

Syntax

```
mirror <slot/port>
```

<slot/port> - Interface Number.

Default Setting

None

Command Mode

Policy-Class-Map Config

Incompatibilities

Drop, Redirect

7.21.3.4 redirect

This command specifies that all incoming packets for the associated traffic stream are redirected to a specific egress interface (physical port or port-channel).

Syntax

```
redirect <slot/port>
```

Command Mode

Policy-Class-Map Config

Incompatibilities

Drop, Mirror

7.21.3.5 conform-color

This command is used to enable color-aware traffic policing and define the conform-color class maps used. Used in conjunction with the police command where the fields for the conform level (for simple, single-rate, and two-rate policing) are specified. The <class-map-name> parameter is the name of an existing Diffserv class map, where different ones must be used for the conform and exceed colors.

Syntax

```
conform-color <class-map-name>
```

<class-map-name> - Name of an existing Diffserv class map, where different ones must be used for the conform colors.

Command Mode

Policy-Class-Map Config

Incompatibilities

Drop, Mirror

7.21.3.6 mark cos

This command marks all packets for the associated traffic stream with the specified class of service value in the priority field of the 802.1p header. If the packet does not already contain this header, one is inserted. The CoS value is an integer from 0 to 7.

Syntax

```
mark cos <0-7>
```

<0-7> - The range of COS value is 0 to 7.

Command Mode

Policy-Class-Map Config

Policy Type

In

Incompatibilities

Drop, Mark IP DSCP, IP Precedence, Police

7.21.3.7 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.

Syntax

```
class <classname>
```

<***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.

Command Mode

Policy-Class-Map Config

7.21.3.8 no class

This command deletes the instance of a particular class and its defined treatment from the specified policy.

Syntax

```
no class <classname>
```

<**classname>** is the name of an existing DiffServ class. Note that this command removes the reference to the class definition for the specified policy.

Command Mode

Policy-Class-Map Config

7.21.3.9 mark ip-dscp

This command marks all packets for the associated traffic stream with the specified IP DSCP value.

Syntax

```
mark ip-dscp <value>
```

<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.

Command Mode

Policy-Class-Map Config

Policy Type

In

Incompatibilities

Drop, Mark CoS, Mark IP Precedence, Police

7.21.3.10 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.

Syntax

```
mark ip-precedence <0-7>
```

Command Mode

Policy-Class-Map Config

Policy Type

In

Incompatibilities

Drop, Mark (all forms)

7.21.3.11 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 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) and is an integer from 1 to 128.

For each outcome, the only possible actions are drop, set-cos-transmit, set-dscp-transmit, setprec-transmit, or transmit. In this simple form of the police command, the conform action defaults to transmit and the violate action defaults to drop.

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.

For set-cos-transmit an 802.1p priority value is required and is specified as an integer from 0-7.

Syntax

```
police-simple {<1-4294967295> <1-128> conform-action {drop | set-prec-transmit <0-7> |
set-dscp-transmit <0-63> | set-cos-transmit <0-7> | transmit} [violate-action {drop | set-prectransmit
<0-7> | set-dscp-transmit <0-63> | set-cos-transmit <0- 7> | transmit}]}
```

The simple form of the police command uses a single data rate and burst size, resulting in two outcomes:

<conform-action & violate-action> - 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 set-cos-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. Beside, the set-cos-transmit is to combine only with drop between the conform-action and the violate-action.

<set-cos-transmit> - an priority value is required and is specified as an integer from 0-7.
<set-dscp-transmit> - 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**.

<set-prec-transmit> - an IP Precedence value is required and is specified as an integer from 0-7.

Command Mode

Policy-Class-Map Config

Incompatibilities

Drop, Mark(all forms)

7.21.3.12 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 the inbound traffic direction as indicated by the in parameter.

Syntax

```
policy-map <policyname> [ in ]
no policy-map <policyname>
```

Command Mode

Global Config

Policy Type

In

7.21.3.13 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.

Syntax

```
policy-map rename <policyname> <newpolicyname>
```

<policyname> - Old Policy name.

<newpolicyname> - New policy name.

Command Mode

Global Config

Policy Type

In

7.21.4 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***

7.21.4.1 service-policy

This command attaches a policy to an interface in a particular direction.

Syntax
service-policy in <policy-map-name>

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.

<policy-map-name> - 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.

This command effectively enables DiffServ on an interface (in a particular direction). There is no separate interface administrative 'mode' command for DiffServ.

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.

Command Mode

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.

7.21.4.2 no service-policy

This command detaches a policy from an interface in a particular direction.

Syntax

no service-policy in <policy-map-name>

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.

<policy-map-name> - is the name of an existing DiffServ policy. Note that this command causes a service to remove its reference to the policy.

This command effectively disables DiffServ on an interface (in a particular direction).There is no separate interface administrative 'mode' command for DiffServ.

Command Mode

Global Config (for all system interfaces)

Interface Config (for a specific interface)

7.21.5 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.

7.21.5.1 show class-map

This command displays all configuration information for the specified class.

Syntax

show class-map [<classname>]

<classname> is the name of an existing DiffServ class.

Default Setting

None

Command Mode

Privileged Exec

User Exec

Display Message

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.

L3 Proto: The Layer 3 protocol for this class. Possible values are IPv4 and IPv6.

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.

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: A class type of 'all' means every match criterion defined for the class is evaluated simultaneously and must all be true to indicate a class match.

Reference Class Name: The name of an existing DiffServ class whose match conditions are being referenced by the specified class definition.

7.21.5.2 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.

Syntax

show diffserv

Default Setting

None

Command Mode

Privileged Exec

User Exec

Display Message

DiffServ Admin mode: The current value of the DiffServ administrative mode.

Class Table Size Current/Max: The current or maximum number of entries (rows) in the Class Table.

Class Rule Table Size Current/Max: The current or maximum number of entries (rows) in the Class Rule Table.

Policy Table Size Current/Max: The current or maximum number of entries (rows) in the Policy Table.

Policy Instance Table Size Current/Max: The current or maximum number of entries (rows) in the Policy Instance Table.

Policy Attribute Table Size Current/Max: The current or maximum number of entries (rows) in the Policy Attribute Table.

Service Table Size Current/Max: The current or maximum number of entries (rows) in the Service Table.

7.21.5.3 show diffserv service

This command displays policy service information for the specified interface and direction.

Syntax

show diffserv service <slot/port> in

<slot/port> - specifies a valid slot number and port number for the system. The direction parameter indicates the interface direction of interest.

Default Setting

None

Command Mode

Privileged Exec

Display Message

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.

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).

7.21.5.4 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.

Syntax
show diffserv service brief [in]

Default Setting

None

Command Mode

Privileged Exec

Display Message

DiffServ Admin 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.

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.

7.21.5.5 show policy-map

This command displays all configuration information for the specified policy.

Syntax

show policy-map [<policy-map-name>]

<policy-map-name> - is the name of an existing DiffServ policy.

Default Setting

None

Command Mode

Privileged Exec

Display Message

Policy Name: The name of this policy.

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 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.

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.

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 COS Value: This field shows the priority mark value if the conform action is markcos.

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.

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.

Assign Queue: Directs traffic stream to the specified QoS queue. This allows a traffic classifier to specify which one of the supported hardware queues are used for handling packets belonging to the class.

Drop: Drop a packet upon arrival. This is useful for emulating access control list operation using DiffServ, especially when DiffServ and ACL cannot co-exist on the same interface.

Mirror: Copies a classified traffic stream to a specified egress port (physical port or LAG). This can occur in addition to any marking or policing action. It may also be specified along with a QoS queue assignment.

Redirect: Forces a classified traffic stream to a specified egress port (physical port or LAG). This can occur in addition to any marking or policing action. It may also be specified along with a QoS queue assignment.

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.

7.21.5.6 show policy-map interface

This command displays policy-oriented statistics information for the specified interface and direction.

Syntax
show policy-map interface <slot/port> in

<slot/port> - specifies a valid slot number and port number for the system. The direction parameter indicates the interface direction of interest.

Command Mode

Privileged Exec

Display Message

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.

The following information is repeated for each class instance within this policy:

Class Name: The name of this class instance.

In Offered Packets: A count of the packets offered to this class instance before the defined DiffServ treatment is applied. Only displayed for the 'in' direction.

In Discarded Packets: A count of the packets discarded for this class instance for any reason due to DiffServ treatment of the traffic class. Only displayed for the 'in' direction.

None of the counters listed here are guaranteed to be supported on all platforms. Only supported counters are shown in the display output.

7.21.5.7 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.***

Syntax
show service-policy in

Command Mode

Privileged Exec

Display Message

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).

Operational Status: The current operational status of this DiffServ service interface.

Policy Name: The name of the policy attached to the interface.

None of the counters listed here are guaranteed to be supported on all platforms. Only supported counters are shown in the display output.

7.22 ACL Command

7.22.1 Show Commands

7.22.1.1 show mac access-lists name

This command displays a MAC access list and all of the rules that are defined for the ACL. The <name> parameter is used to identify a specific MAC ACL to display.

Syntax

show mac access-lists <name>

<name> - ACL name which uniquely identifies the MAC ACL to display.

Default Setting

None

Command Mode

Privileged Exec

Display Message

MAC ACL Name: The name of the MAC ACL rule.

Rule Number: The ordered rule number identifier defined within the ACL.

Action: Displays the action associated with each rule. The possible values are Permit or Deny.

Source MAC Address: Displays the source MAC address for this rule.

Source MAC Mask: Displays the source MAC mask for this rule.

Destination MAC Address: Displays the destination MAC address for this rule.

Destination MAC Mask: Displays the destination MAC mask for this rule.

Ethertype: Displays the Ethertype keyword or custom value for this rule.

VLAN ID: Displays the VLAN identifier value or range for this rule.

CoS Value: Displays the COS (802.1p) value for this rule.

Assign Queue: Displays the queue identifier to which packets matching this rule are assigned.

Redirect Interface: Displays the slot/port to which packets matching this rule are forwarded.

Mirror Interface: Displays the slot/port to which packets matching this rule are copied.

7.22.1.2 show mac access-lists

This command displays a summary of all defined MAC access lists in the system.

Syntax

```
show mac access-lists
```

Default Setting

None

Command Mode

Privileged Exec

Display Message

Current number of all ACLs: The number of user-configured rules defined for this ACL.

Maximum number of all ACLs: The maximum number of ACL rules.

MAC ACL Name: The name of the MAC ACL rule.

Rules: The number of rule in this ACL.

Direction: Denotes the direction in which this MAC ACL is attached to the set of interfaces listed. The value is Inbound.

Interfaces: Displays the list of interfaces (slot/port) to which this MAC ACL is attached in a given direction.

VLANs: VLAN(s) to which the MAC ACL applies.

7.22.1.3 show ip access-lists

This command displays an Access Control List (ACL) and all of the rules that are defined for the ACL.

Syntax

```
show ip access-lists [<1-199> | <name>]
```

<1-199> - is the number used to identify the ACL.

<name> - is the name of the ACL.

Default Setting

None

Command Mode

Privileged Exec

User Exec

Display Message

Current number of ACLs: The number of user-configured rules defined for this ACL.

Maximum number of ACLs: The maximum number of ACL rules.

ACL ID: The identifier of this ACL.

Rule: 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.

Match ALL: Match all packets or not.

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 L4 Port Keyword: This field displays the source port 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 L4 Port Keyword: This field displays the destination port for this rule.

IP DSCP: This field displays the IP DSCP value for this rule.

IP Precedence: This field displays the IP Precedence value for this rule.

IP TOS: This field displays the IP TOS value for this rule.

Log: This field displays when you enable logging for this rule.

Assign Queue: This field displays the queue identifier to which packets matching this rule are assigned.

Mirror Interface: This field displays the slot/port to which packets matching this rule are copied.

Redirect Interface: This field displays the slot/port to which packets matching this rule are forwarded.

7.22.1.4 show access-lists interface

This command displays Access List information for a particular interface and the 'in' direction.

Syntax
show access-lists { interface <slot/port> | vlan <vlan id> } in

<slot/port> - is the interface number.

Default Setting

None

Command Mode

Privileged Exec

Display Message

ACL Type: This displays ACL type is IP, IPv6 or MAC.

ACL ID: Access List name for a MAC or IPv6 access list or the numeric identifier for an IP access list.

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 is used. Valid range is (1 to 4294967295).

7.22.2 Configuration Commands

7.22.2.1 mac access-list extended

This command creates a MAC Access Control List (ACL) identified by <name>, consisting of

classification fields defined for the Layer 2 header of an Ethernet frame. The <name> parameter is a case-sensitive alphanumeric string from 1 to 31 characters uniquely identifying the MAC access list. If a MAC ACL by this name already exists, this command enters Mac-Access-List config mode to allow updating the existing ACL.

Syntax

```
mac access-list extended <name>
no mac access-list extended <name>
```

<name> - It uniquely identifies the MAC access list.

Default Setting

None

Command Mode

Global Config

7.22.2.2 mac access-list extended rename

This command changes the name of a MAC Access Control List (ACL). The <name> parameter is the name of an existing MAC ACL. The <newname> parameter is a case-sensitive alphanumeric string from 1 to 31 characters uniquely identifying the MAC access list. This command fails if a MAC ACL by the name <newname> already exists.

Syntax

```
mac access-list extended rename <oldname> <newname>
```

<oldname> - Old name which uniquely identifies the MAC access list.

<newname> - New name which uniquely identifies the MAC access list.

Default Setting

None

Command Mode

Global Config

7.22.2.3 mac access-group in

This command attaches a specific MAC Access Control List (ACL) identified by <name> to an

interface, or associates it with a VLAN ID, in a given direction. The <name> parameter must be the name of an exsiting MAC ACL.

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 for this command, a sequence number that is one greater than the highest sequence number currently in use for this interface and direction will be used.

This command specified in 'Interface Config' mode only affects a single interface, whereas the 'Global Config' mode setting is applied to all interfaces. The 'Interface Config' mode command is only available on platforms that support independent per-port class of service queue configuration. The VLAN keyword is only valid in the 'Global Config' mode.

Syntax

```
mac access-group <name> [vlan <vlan-id>] in [<1-4294967295>]
no mac access-group <name> [vlan <vlan-id>] in
```

<no> - This command removes a MAC ACL identified by <name> from the interface or vlan in a given direction.

Default Setting

None

Command Mode

Global Config

Interface Config

7.22.2.4 mac access-list

This command creates a new rule for the current MAC access list. Each rule is appended to the list of configured rules for the list. Note that an implicit 'deny all' MAC rule always terminates the access list. Note: The 'no' form of this command is not supported, as the rules within an ACL cannot be deleted individually. Rather, the entire ACL must be deleted and re-specified.

A rule may either deny or permit traffic according to the specified classification fields. At a minimum, the source and destination MAC value and mask pairs must be specified, each of which may be substituted using the keyword any to indicate a match on any value in that field. The bpdu keyword may be specified for the destination MAC value/mask pair indicating a well-known BPDU MAC value of 01-80-c2-xx-xx-xx (hex), where 'xx' indicates a don't care. The remaining command parameters are all optional.

The Ethertype may be specified as either a keyword or a four-digit hexadecimal value from 0x0600-0xFFFF. The currently supported <ethertypekey> values are: appletalk, arp, ibmsna, ipv4, ipv6, ipx, mplsmcast, mplsucast, netbios, novell, pppoe, rarp. Each of these translates into its equivalent Ethertype value(s).

The vlan and cos parameters refer to the VLAN identifier and 802.1p user priority fields, respectively, of the VLAN tag. For packets containing a double VLAN tag, this is the first (or outer) tag.

The assign-queue parameter allows specification of a particular hardware queue for handling traffic that matches this rule. The allowed <queue-id> value is 0-(n-1), where n is the number of user configurable queues available for the hardware platform.

The mirror parameter allows the traffic matching this rule to be copied to the specified <slot/port>, while the redirect parameter allows the traffic matching this rule to be forwarded to the specified <slot/port> The assign-queue and redirect parameters are only valid for a 'permit' rule.

Syntax

{del-rule-id | deny | permit} {{<srcmac> <srcmask>} | any} {{<dstmac> <dstmask>} | any | bpdu} [<ethertypekey> | <0x0600-0xFFFF>] [vlan {{eq <0-4095>}} [cos <0-7>] [log] [assign-queue <queue-id>] [{mirror | redirect} <slot/port>] [<rule-id>]

Default Setting

None

Command Mode

Mac Access-list Config

7.22.2.5 access-list

This command creates an Access Control List (ACL) that is identified by the parameter.

Syntax

access-list {(<1-99> {deny | permit} {every | <srcip> <srcm ask>}) | ({<100-199> {deny | permit} {every | {{icmp | igmp | ip | tcp | udp | <number>} any | <srcip> <srcmask> [{eq {<0-65535> | <portkey>}](any | <dstip> <dstmask>) [{eq {<0-65535> | <portkey>}] {[precedence <precedence>] | [tos <tos> <tosmask>] | [dscp <dscp>] [log] [assign-queue <queue-id>] [{mirror | redirect} <slot/port>] [<rule-id>]}}}}}

<accesslistnumber> - The ACL number is an integer from 1 to 199. The range 1 to 99 is for the normal ACL List and 100 to 199 is for the extended ACL List.

permit or deny - The ACL rule is created with two options. The protocol to filter for an ACL rule is specified by giving the protocol to be used like **i*cmp ,igmp ,ip ,tcp, udp***. The command specifies a source ip address 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 is specified by the *port key p*arameter.

<portkey> - 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 ip address 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 Setting

None

Command Mode

Global Config

7.22.2.6 no access-list

This command deletes an ACL that is identified by the parameter <*accesslistnumber*> from the system or remove an ACL rule that is identified by the parameter <1-28> from the an IP ACL <accesslistnumber>.

Syntax

```
no access-list {<1-99> | <100-199>} [<rule-id>]
```

The ACL number is an integer from 1 to 199. The range 1 to 99 is for the normal ACL List and 100 to 199 is for the extended ACL List.

Default Setting

None

Command Mode

Global Config

7.22.2.7 ip access-group

This command attaches a specified access-control list to an interface or associates with a VLAN ID in a given direction. The parameter <name> is the name of the Access Control List.

An optional sequence number may be specified to indicate the order of this IP access list relative to other IP 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 IP access list using that sequence number. If the sequence number is not specified for this command, a sequence number that is one greater than the highest sequence number currently in use for this interface and direction is used.

This command specified in 'Interface Config' mode only affects a single interface, whereas the 'Global Config' mode setting is applied to all interfaces. The VLAN keyword is only valid in the 'Global Config' mode.

Syntax

```
ip access-group {<1- 199> | <name>} [vlan <vlan-id>] in [<1-4294967295>]
no ip access-group {<1-199> | <name>} [vlan <vlan-id>] in
```

<1- 199> The identifier of this ACL.

<name> The name of this ACL.

<vlan-id> The associated VLAN ID of this ACL.

<1-4294967295> The sequence number of this ACL.

no - This command removes a ACL by identifier or name from the interface or vlan in a given direction.

Default Setting

None

Command Mode

Global Config

Interface Config

7.22.2.8 ip access-list

Use this command to create an extended IP Access Control List (ACL) identified by <name>, consisting of classification fields defined for the IP header of an IPv4 frame. The <name> parameter is a case-sensitive alphanumeric string from 1 to 31 characters uniquely identifying the IP access list.

If an IP ACL by this name already exists, this command enters IPv4-Access_List config mode to allow updating the existing IP ACL.

The CLI mode changes to IPv4-Access-List Configuration mode when you successfully execute this command.

Syntax

```
Ip access-list <name>
no ip access-list <name>
```

no - This command removes the IP ACL identified by <name> from the system.

Default Setting

None

Command Mode

Global Config

7.22.2.9 ip access-list rename

Use this command to change the name of an IP Access Control List (ACL). The <name> parameter is the names of an existing IP ACL. The <newname> parameter is a case-sensitive alphanumeric string from 1 to 31 characters uniquely identifying the IP access list.

Syntax

ip access-list rename <name> <newname>

Default Setting

None

Command Mode

Global Config

7.23 IPv6 ACL Command

7.23.1 Show Commands

7.23.1.1 show ipv6 access-lists

This command displays an IPv6 access list and all of the rules that are defined for the IPv6 ACL. Use the [name] parameter to identify a specific IPv6 ACL to display.

Syntax

show ipv6 access-lists [<name>]

<name> - ACL name which uniquely identifies the IPv6 ACL to display.

Default Setting

None

Command Mode

Privileged EXEC

User EXEC

Display Message

Rule Number: The ordered rule number identifier defined within the IPv6 ACL.

Action: The action associated with each rule. The possible values are Permit or Deny.

Match All: Indicates whether this access list applies to every packet. Possible values are True or False.

Protocol: The protocol to filter for this rule.

Source IP Address: The source IP address for this rule.

Source L4 Port Keyword: The source port for this rule.

Destination IP Address: The destination IP address for this rule.

Destination L4 Port Keyword: The destination port for this rule.

IP DSCP: The value specified for IP DSCP.

Flow Label: The value specified for IPv6 Flow Label.

Log: Displays when you enable logging for the rule.

Assign Queue: The queue identifier to which packets matching this rule are assigned.

Mirror Interface: The slot/port to which packets matching this rule are copied.

Redirect Interface: The slot/port to which packets matching this rule are forwarded.

7.23.2 Configuration Commands

7.23.2.1 ipv6 access-list

This command creates an IPv6 Access Control List (ACL) identified by <name>, consisting of classification fields defined for the IP header of an IPv6 frame. The <name> parameter is a case-sensitive alphanumeric string from 1 to 31 characters

uniquely identifying the IPv6 access list.

If an IPv6 ACL by this name already exists, this command enters IPv6-Access-List config mode to allow updating the existing IPv6 ACL.

Syntax

```
ipv6 access-list <name>
no ipv6 access-list <name>
```

<name> - access-list name up to 31 characters in length.

no - This command deletes the IPv6 ACL identified by <name> from the system.

i The CLI mode changes to IPv6-Access-List Config mode when you successfully execute this command.

Default Setting

None

Command Mode

Global Config

7.23.2.2 ipv6 access-list rename

This command changes the name of an IPv6 ACL. The <name> parameter is the name of an existing IPv6 ACL. The <newname> parameter is a case-sensitive alphanumeric string from 1 to 31 characters uniquely identifying the IPv6 access list.

This command fails is an IPv6 ACL by the name <newname> already exists.

Syntax

ipv6 access-list rename <oldname> <newname>

<oldname> - current Access Control List name.

<newname> - new Access Control List name.

Default Setting

None

Command Mode

Global Config

7.23.2.3 {deny | permit} (IPv6)

This command creates a new rule for the current IPv6 access list. Each rule is appended to the list of configured rules for the list.

The ‘no’ form of this command is not supported, since the rules within an IPv6 ACL cannot be deleted individually. Rather, the entire IPv6 ACL must be deleted and respecified.

An implicit ‘deny all’ IPv6 rule always terminates the access list.

A rule may either deny or permit traffic according to the specified classification fields. At a minimum, either the ‘every’ keyword or the protocol, source address, and destination address values must be specified. The source and destination IPv6 address fields may be specified using the keyword ‘any’ to indicate a match on any value in that field. The remaining command parameters are all optional, but the most frequently used parameters appear in the same relative order as shown in the command format.

The assign-queue parameter allows specification of a particular hardware queue for handling traffic that matches this rule. The allowed <queue-id> value is 0-(n-1), where n is the number of user configurable queues available for the hardware platform. The assign-queue parameter is valid only for a permit rule.

The mirror parameter allows the traffic matching this rule to be copied to the specified <slot/port>, while the redirect parameter allows the traffic matching this rule to be forwarded to the specified <slot/port>. The assign-queue and redirect parameters are only valid for a permit rule.

Syntax

{del-rule-id | deny | permit} {every | {{icmpv6 | ipv6 | tcp | udp | <number>} [log] [assign-queue <queue-id>] [{mirror | redirect} <slot/port>] [rule-id]

Default Setting

None

Command Mode

IPv6-Access-List Config

7.23.2.4 ipv6 traffic-filter

This command either attaches a specific IPv6 ACL identified by <name> to an interface or associates with a VLAN ID in a given direction. The <name> parameter must be the name of an existing IPv6 ACL.

An optional sequence number may be specified to indicate the order of this mac access list relative to other IPv6 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 specifiedIPv6 access list replaces the currently attached IPv6 access list using that sequence number. If the sequence number is not specified for this command, a sequence number that is one greater than the highest sequence number currently in use for this interface and direction is used.

This command specified in Interface Config mode only affects a single interface, whereas the Global Config mode setting is applied to all interfaces. The vlan keyword is only valid in the Global Config mode. The Interface Config mode command is only available on platforms that support independent per-port class of service queue configuration.

Syntax

ipv6 traffic-filter <name> [vlan <vlan-id>] in [<1-4294967295>]
no ipv6 traffic-filter <name> [vlan <vlan-id>] in [<1-4294967295>]

no - This command removes an IPv6 ACL identified by <name> from the interface(s) in a given direction

Default Setting

None

Command Mode

Global Config

Interface Config

7.24 CoS (Class of Service) Command

7.24.1 Show Commands

7.24.1.1 show queue cos-map

This command displays the current Dot1p (802.1p) priority mapping to internal traffic classes for a specific interface. The slot/port parameter is optional and is only valid on platforms that support independent per-port class of service mappings. If specified, the 802.1p mapping table of the interface is displayed. If omitted, the most recent global configuration settings are displayed.

Syntax
show queue cos-map <slot/port>

< slot/port > - The interface number.

Default Setting

None

Command Mode

Privileged EXEC

User EXEC

Display Message

The following information is repeated for each user priority.

User Priority: The 802.1p user priority value.

Traffic Class: The traffic class internal queue identifier to which the user priority value is mapped.

7.24.1.2 show queue ip-dscp-mapping

This command maps an IP DSCP value to an internal traffic class. The <ipdscp> 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.

The <trafficclass> values can range from 0-6, although the actual number of available traffic classes depends on the platform.

Syntax

show queue ip-dscp-mapping

Default Setting

None

Command Mode

Privileged EXEC

Display Message

IP DSCP: Displays IP DSCP value.

Traffic Class: Displays the queue mapping.

7.24.1.3 show queue trust

This command displays the current trust mode setting for a specific interface. The slot/port parameter is optional and is only valid on platforms that support independent per-port class of service mappings. If specified, the port trust mode of the interface is displayed. If omitted, the port trust mode of each interface in the system is shown. If the platform does not support independent per-port class of service mappings, the output represents the system-wide port trust mode used for all interfaces.

Syntax

show queue trust <slot/port>

< slot/port > The interface number.

Default Setting

None

Command Mode

Privileged Exec

User Exec

Display Message

Class of Service Trust Mode: The trust mode of this interface.

Non-IP Traffic Class: The traffic class used for non-IP traffic. This is only displayed when the COS trust mode is set to either 'trust ip-dscp' or 'trust ip-precedence'.

Untrusted Traffic Class: The traffic class used for all untrusted traffic. This is only displayed when the COS trust mode is set to 'untrusted'.

7.24.1.4 show queue cos-queue

This command displays the class-of-service queue configuration for the specified interface. The slot/port parameter is optional and is only valid on platforms that support independent per-port class of service mappings. If specified, the class-of-service queue configuration of the interface is displayed. If omitted, the most recent global configuration settings are displayed.

Syntax
show queue cos-queue <slot/port>

< slot/port > The interface number.

Default Setting

None

Command Mode

Privileged Exec

Display Message

Interface: This displays the slot/port of the interface. If displaying the global configuration, this output line is replaced with a Global Config indication.

Interface Shaping Rate: The maximum transmission bandwidth limit for the interface as a whole. It is independent of any per-queue maximum bandwidth value(s) in effect for the interface. This is a configured value.

The following information is repeated for each queue on the interface.

Queue Id: An interface supports n queues numbered 0 to (n-1). The specific n value is platform dependent.

Minimum Bandwidth: The minimum transmission bandwidth guarantee for the queue, expressed as a percentage. A value of 0 means bandwidth is not guaranteed and the queue operates using best-effort. This is a configured value.

Scheduler Type: Indicates whether this queue is scheduled for transmission using a strict priority or a weighted scheme. This is a configured value.

Queue Mgmt Type: The queue depth management technique used for this queue, either tail drop or weighted random early discard (WRED). This is a configured value.

7.24.2 Configuration Commands

7.24.2.1 queue cos-map

This command maps an 802.1p priority to an internal traffic class on a "per-port" basis.

Syntax

```
queue cos-map <0-7> <0-7>
no queue cos-map
```

< 0-7 > - The range of queue priority is 0 to 7.

< 0-7 > - The range of mapped traffic class is 0 to 7**.**

no - Reset to the default mapping of the queue priority and the mapped traffic class.

Default Setting

None

Command Mode

Interface Config.

This command maps an 802.1p priority to an internal traffic class for a device.

Syntax

```
queue cos-map all <0-7> <0-7>
no queue cos-map all
```

< 0-7 > - The range of queue priority is 0 to 7.

< 0-7 > - The range of mapped traffic class is 0 to 7**.**

no - Reset to the default mapping of the queue priority and the mapped traffic class.

Default Setting

None

Command Mode

Global Config.

7.24.2.2 queue trust

This command sets the class of service trust mode of an interface. You can set the mode to trust one of the Dot1p (802.1p) or IP DSCP packet markings. You can also set the interface mode to untrusted. If you configure an interface to use Dot1p, the mode does not appear in the output of the show running config command because Dot1p is the default.

Syntax

```
queue trust {dot1p | ip-dscp | untrusted } all
no queue trust all
```

no - This command sets the class of service trust mode to untrusted for all interfaces.

Default Setting

None

Command Mode

Global Config.

7.24.2.3 queue cos-queue min-bandwidth

This command specifies the minimum transmission bandwidth guarantee for each interface queue.

Syntax

```
queue cos-queue min-bandwidth <bw-0> <bw-1> … <bw-6>
no queue cos-queue min-bandwidth
```

<bw-0> <bw-1> … <bw-6>- Each Valid range is (0 to 100) in increments of 5 and the total sum is less than or equal to 100.

no - This command restores the default for each queue's minimum bandwidth value.

Default Setting

None

Command Mode

Interface Config.

This command specifies the minimum transmission bandwidth guarantee for each interface queue in the device.

Syntax

```
queue cos-queue min-bandwidth all <bw-0> <bw-1> … <bw-6>
no queue cos-queue min-bandwidth all
```

<bw-0> <bw-1> … <bw-6>- Each Valid range is (0 to 100) in increments of 5 and the total sum is less than or equal to 100.

no - This command restores the default for each queue's minimum bandwidth value in the device.

Default Setting

None

Command Mode

Global Config.

7.24.2.4 queue cos-queue strict

This command activates the strict priority scheduler mode for each specified queue on a "per-port" basis.

Syntax

```
queue cos-queue strict <queue-id-0> [<queue-id-1> … <queue-id-6>]
no queue cos-queue strict <queue-id-0> [<queue-id-1> … <queue-id-6>]
```

no - This command restores the default weighted scheduler mode for each specified queue on a "per-port" basis.

Default Setting

None

Command Mode

Interface Config.

This command activates the strict priority scheduler mode for each specified queue on a device.

Syntax

```
queue cos-queue strict all <queue-id-0> [<queue-id-1> … <queue-id-6>]
no queue cos-queue strict all <queue-id-0> [<queue-id-1> … <queue-id-6>]
```

no - This command restores the default weighted scheduler mode for each specified queue on a device.

Default Setting

None

Command Mode

Global Config.

7.24.2.5 queue cos-queue traffic-shape

This command specifies the maximum transmission bandwidth limit for the interface as a whole. Also known as rate shaping, this has the effect of smoothing temporary traffic bursts over time so that the transmitted traffic rate is bounded.

Syntax

```
queue cos-queue traffic-shape <bw>
no queue cos-queue traffic-shape
```

<bw> - Valid range is (0 to 100) in increments 5.

no - This command restores the default shaping rate value.

Default Setting

None

Command Mode

Interface Config.

This command specifies the maximum transmission bandwidth limit for all interfaces. Also known as rate shaping, this has the effect of smoothing temporary traffic bursts over time so that the transmitted traffic rate is bounded.

Syntax

```
queue cos-queue traffic-shape all <bw>
no queue cos-queue traffic-shape all
```

<bw> - Valid range is (0 to 100) in increments 5.

no - This command restores the default shaping rate value for all interfaces.

Default Setting

None

Command Mode

Global Config.

7.25 Domain Name Server Relay Commands

7.25.1 Show Commands

7.25.1.1 show hosts

This command displays the static host name-to-address mapping table.

Syntax

show hosts

Default Setting

None

Command Mode

Privileged Exec

Display Message

Domain Name List: Domain Name.

IP Address: IPv4 or IPv6 address of the Host.

7.25.1.2 show dns

This command displays the configuration of the DNS server.

Syntax

show dns

Default Setting

None

Command Mode

Privileged Exec

Display Message

Domain Lookup Status: Enable or disable the IP Domain Naming System (DNS)-based host name-to-address translation function.

Default Domain Name: The default domain name that will be used for querying the IP address of a host.

Domain Name List: A list of domain names that will be used for querying the IP address of a host.

Name Server List: A list of domain name servers, including IPv4 and IPv6.

Request: Number of the DNS query packets been sent.

Response: Number of the DNS response packets been received.

7.25.1.3 show dns cache

This command displays all entries in the DNS cache table.

Syntax

```
show dns cache
```

Default Setting

None

Command Mode

Privileged Exec

Display Message

Domain Name List: Domain Name

IP Address: IP address of the corresponding domain name, including IPv4 and IPv6.

TTL: Time in seconds that this entry will remain in the DNS cache table

Flag: Indicates if this entry is reliable. A value of 8 is not as reliable as a value of 10.

7.25.2 Configuration Commands

7.25.2.1 ip hosts

This command creates a static entry in the DNS table that maps a host name to an IP address.

There are maximum 8 entries for IPv4 and 8 entries for IPv6.

Syntax

```
ip host <name> <ipaddr>
no ip host <name>
```

<name> - Host name.

<ipaddr> - IPv4 or IPv6 address of the host.

<no> - Remove the corresponding name to IP address mapping entry.

Default Setting

None

Command Mode

Global Config

7.25.2.2 clear hosts

This command clears the entire static host name-to-address mapping table.

Syntax

```
clear hosts
```

Default Setting

None

Command Mode

Privileged Exec

7.25.2.3 ip domain-name

This command defines the default domain name to be appended to incomplete host names (i.e., host names passed from a client are not formatted with dotted notation).

Syntax

```
ip domain-name <name>
no ip domain-name <name>
```

<name> - Default domain name used to complete unqualified host names. Do not include the initial period that separates an unqualified name from the domain name. (Range: 1-64 characters)

Default Setting

None

Command Mode

Global Config

7.25.2.4 ip domain-list

This command defines the domain name that can be appended to incomplete host names (i.e., host names passed from a client are not formatted with dotted notation). The domain name table can contain maximum 6 entries.

Syntax

```
ip domain-list <name>
no ip domain-list <name>
```

<name> - Default domain name used to complete unqualified host names. Do not include the initial period that separates an unqualified name from the domain name. (Range: 1-64 characters)

i When an incomplete host name is received by the DNS server on this switch, it will work through the domain name list, append each domain name in the list to the host name, and check with the specified name servers for a match. If there is no domain name list, the domain name specified with the "*ip domain-name*" command is used. If there is a domain name list, the default domain name is not used.

Default Setting

None

Command Mode

Global Config

7.25.2.5 ip name-server

This command specifies the address of one or more domain name servers to use for name-to-address resolution. There are maximum 6 entries for IPv4 and 6 entries for IPv6 in the Domain Name Server Table.

Syntax

```
ip name-server <ipaddr>
no ip name-server <ipaddr>
```

< ipaddr > - IP address of the Domain Name Servers.

<no> - Remove the corresponding Domain Name Server entry from the table.

Note - The listed name servers are queried in the specified sequence until a response is received, or the end of the list is reached with no response.

Default Setting

None

Command Mode

Global Config

7.25.2.6 ip domain-lookup

This command enables the IP Domain Naming System (DNS)-based host name-to-address translation.

Syntax

```
ip domain-lookup
no ip domain-lookup
```

<no> - This command disables the IP Domain Naming System (DNS)-based host name-to-address translation.

Default Setting

None

Command Mode

Global Config

7.25.2.7 clear domain-list

This command clears all entries in the domain name list table.

Syntax

```
clear domain-list
```

Default Setting

None

Command Mode

Privileged Exec

7.25.2.8 clear dns

This command sets the DNS configuration to default value.

Syntax

```
clear dns
```

Default Setting

None

Command Mode

Privileged Exec

7.25.2.9 clear dns cache

This command clears all entries in the DNS cache table.

Syntax

clear dns cache

Default Setting

None

Command Mode

Privileged Exec

7.25.2.10 clear dns counter

This command clears the statistics of all entries in the DNS cache table.

Syntax

clear dns counter

Default Setting

None

Command Mode

Privileged Exec

8. Routing Commands

8.1 Address Resolution Protocol (ARP) Commands

8.1.1 Show Commands

8.1.1.1 show ip arp

This command displays the Address Resolution Protocol (ARP) cache.

Syntax
show ip arp

Default Setting

None

Command Mode

Privileged Exec

Display Message

Age Time: 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: 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 aged 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 Configured/Active/Max: Field listing configured static entry count, active static entry count, 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).

8.1.1.2 show ip arp brief

This command displays the brief Address Resolution Protocol (ARP) table information.

Syntax

show ip arp brief

Default Setting

None

Command Mode

Privileged Exec

Display Message

Age Time: 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: 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 aged 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 Configured/Active/Max: Field listing the configured static entry count, active static entry count, and maximum static entry count in the ARP table.

8.1.1.3 show ip arp static

This command displays the static Address Resolution Protocol (ARP) table information.

Syntax

show ip arp static

Default Setting

None

Command Mode

Privileged Exec

Display Message

IP address: Is the IP address of a device on a subnet attached to an existing routing interface.

MAC address: Is the MAC address for that device.

8.1.2 Configuration Commands

8.1.2.1 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. The value for <macaddress> is a unicast MAC address for that device.

Syntax

```
arp <ipaddr> <macaddr>
no arp <ipaddr> <macaddr>
```

<ipaddr> - Is the IP address of a device on a subnet attached to an existing routing interface.

<macaddr> - Is a MAC address for that device. The format is 6 two-digit hexadecimal numbers that are separated by colons, for example, 00:06:29:32:81:40.

no - This command deletes an ARP entry.

Default Setting

None

Command Mode

Global Config

8.1.2.2 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.

Syntax

```
ip proxy-arp
no ip proxy-arp
```

no - This command disables proxy ARP on a router interface.

Default Setting

Enabled

Command Mode

Interface Config

8.1.2.3 ip local-proxy-arp

This command enables or disables Local Proxy ARP on an interface.

Syntax

```
ip local-proxy-arp
no ip local-proxy-arp
```

no - This command disables Local Proxy ARP on a router interface.

Default Setting

Disabled

Command Mode

Interface Config

8.1.2.4 arp cachesize

This command configures the maximum number of entries in the ARP cache.

Syntax

```
arp cachesize <384-4096>
no arp cachesize
```

<384-3968> - The range of cache size is 384 to 4096.

no - This command configures the default ARP cache size.

Default Setting

The default cache size is 4096.

Command Mode

Global Config

8.1.2.5 arp dynamicrenew

This command enables ARP component to automatically renew ARP entries of type dynamic when they age out.

Syntax

```
arp dynamicrenew
no arp dynamicrenew
```

no - This command disables ARP component from automatically renewing ARP entries of type dynamic when they age out.

Default Setting

Disabled

Command Mode

Global Config

8.1.2.6 arp purge

This command causes the specified IP address to be removed from the ARP table. Only entries of type dynamic or gateway are affected by this command.

Syntax

```
arp purge <ipaddr>
```

<ipaddr> - The IP address to be removed from the ARP table.

Default Setting

None

Command Mode

Privileged Exec

8.1.2.7 arp resptime

This command configures the ARP request response timeout.

Syntax

```
arp resptime <1-10>
no arp resptime
```

<1-10> - The range of default response time is 1 to 10 seconds.

no - This command configures the default response timeout time.

Default Setting

The default response time is 1.

Command Mode

Global Config

8.1.2.8 arp retries

This command configures the ARP count of maximum request for retries.

Syntax

```
arp retries <0-10>
no arp retries
```

<0-10> - The range of maximum request for retries is 0 to 10.

no - This command configures the default count of maximum request for retries.

Default Setting

The default value is 4.

Command Mode

Global Config

8.1.2.9 arp timeout

This command configures the ARP entry ageout time.

Syntax

```
arp timeout <15-21600>
no arp timeout
```

<15-21600> - Represents the IP ARP entry ageout time in seconds. The range is 15 to 21600 seconds.

no - This command configures the default ageout time for IP ARP entry.

Default Setting

The default value is 1200.

Command Mode

Global Config

8.1.2.10 clear ip arp-cache

This command causes all ARP entries of type dynamic to be removed form the ARP cache. If the [gateway] parameter is specified, the dynamic entries of type gateway are purged as well.

Syntax

clear ip arp-cache [gateway | interface <slot/port>]

Default Setting

None

Command Mode

Privileged Exec

8.2 IP Routing Commands

8.2.1 Show Commands

8.2.1.1 show ip brief

This command displays all the summary information of the IP.

Syntax

show ip brief

Default Setting

None

Command Mode

Privileged Exec

User Exec

Display Message

Default Time to Live: The computed TTL (Time to Live) of forwarding a packet from the local router to the final destination.

Routing Mode: Show whether the routing mode is enabled or disabled.

IP Forwarding Mode: Disable or enable the forwarding of IP frames.

Maximum Next Hops: The maximum number of hops supported by this switch.

8.2.1.2 show ip interface port

This command displays all pertinent information about the IP interfaces.

Syntax
show ip interface port <slot/port>

Default Setting

None

Command Mode

Privileged Exec

User Exec

Display Message

IP Address: Is an IP address representing the subnet configuration of the router interface.

Subnet Mask: Is a mask of the network and host portion of the IP address for the router interface.

Routing Mode: Is the administrative mode of router interface participation. The possible values are enable or disable.

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.

Forward Net Directed Broadcasts: Displays whether forwarding of network-directed broadcasts is enabled or disabled.

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 physical address of the specified interface.

Encapsulation Type: Is the encapsulation type for the specified interface.

IP MTU: Is the Maximum Transmission Unit size of the IP packet.

Bandwidth: Shows the bandwidth of the interface.

Destination Unreachables: Shows whether ICMP Destination Unreachable messages may be sent (enabled) or not (disabled).

ICMP Redirects: Shows whether ICMP Redirect mode is enabled or disabled.

8.2.1.3 show ip interface brief

This command displays summary information about IP configuration settings for all ports in the router.

Syntax

show ip interface brief

Default Setting

None

Command Mode

Privileged Exec

User Exec

Display Message

Interface: Valid slot, and port number separated by forward slashes.

IP Address: The IP address of the routing interface.

IP Mask: The IP mask of the routing interface.

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.

8.2.1.4 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 longerprefixes 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, or static**. Use the all parameter to display all routes including best and nonbest routes. If you do not use the all parameter, the command only displays the best route.

If you use the connected keyword for **<protocol>**, the all option is not available because there are no best or non-best connected routes.

Syntax

show ip route [{<ip-address> [<protocol>] | {<ip-address> <mask> [longer-prefixes] [<protocol>] | <protocol>} [all] | all}]

Default Setting

None

Command Mode

Privileged Exec

Display Message

Route Codes: Displays the key for the routing protocol codes that might appear in the routing table output.

The command displays the routing tables in the following format:

Code IP-Address/Mask [Preference/Metric] via Next-Hop, Interface

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

8.2.1.5 show ip route bestroutes

This command displays router route table information for the best routes.

Syntax
show ip route bestroutes

Default Setting

None

Command Mode

Privileged Exec

Display Message

Total Number of Routes: The total number of routes.

Network Address: Is an IP route prefix for the destination.

Subnet Mask: Is a mask of the network and host portion of the IP address for the router interface.

Protocol: Tells which protocol added the specified route. The possibilities are: local, static, OSPF, or RIP.

for each next hop

Next Hop Intf: The outgoing router interface to use when forwarding traffic to the next destination.

Next Hop IP Address: The outgoing router IP address to use when forwarding traffic to the next router (if any) in the path toward the destination.

8.2.1.6 show ip route entry

This command displays the router route entry information.

Syntax

show ip route entry <networkaddress>

<networkaddress> - Is a valid network address identifying the network on the specified interface.

Default Setting

None

Command Mode

Privileged Exec

Display Message

Network Address: Is a valid network address identifying the network on the specified interface.

Subnet Mask: Is a mask of the network and host portion of the IP address for the attached network.

Protocol: Tells which protocol added the specified route. The possibilities are: local, static, OSPF, or RIP.

Total Number of Routes: The total number of routes.

for each next hop

Next Hop Intf: The outgoing router interface to use when forwarding traffic to the next destination.

Next Hop IP Address: The outgoing router IP address to use when forwarding traffic to the next router (if any) in the path toward the destination.

Preference: The preference value that is used for this route entry.

Metric: Specifies the metric for this route entry.

8.2.1.7 show ip route connected

This command displays directly connected routes.

Syntax

show ip route connected

Default Setting

None

Command Mode

Privileged Exec

Display Message

Route Codes: Displays the key for the routing protocol codes that might appear in the routing table output.

The command displays the routing tables in the following format:

Code IP-Address/Mask [Preference/Metric] via Next-Hop, Interface

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.

8.2.1.8 show ip route ospf

This command displays Open Shortest Path First (OSPF) routes. The option **all** command displays all (best and non-best) routes.

Syntax
show ip route ospf [all]

Default Setting

None

Command Mode

Privileged Exec

Display Message

Route Codes: Displays the key for the routing protocol codes that might appear in the routing table output.

The command displays the routing tables in the following format:

Code IP-Address/Mask [Preference/Metric] via Next-Hop, Interface

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.

8.2.1.9 show ip route rip

This command displays Routing Information Protocol (RIP) routes. The option **all** command displays all (best and non-best) routes.

Syntax
show ip route rip [all]

Default Setting

None

Command Mode

Privileged Exec

Display Message

Route Codes: Displays the key for the routing protocol codes that might appear in the routing table output.

The command displays the routing tables in the following format:

Code IP-Address/Mask [Preference/Metric] via Next-Hop, Interface

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.

8.2.1.10 show ip route static

This command displays Static Routes. The option **all** command displays all (best and non-best) routes.

Syntax

show ip route static [all]

Default Setting

None

Command Mode

Privileged Exec

Display Message

Route Codes: Displays the key for the routing protocol codes that might appear in the routing table output.

The command displays the routing tables in the following format:

Code IP-Address/Mask [Preference/Metric] via Next-Hop, Interface

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.

8.2.1.11 show ip route summary

This command displays 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.

Syntax

show ip route summary [all]

Default Setting

None

Command Mode

Privileged Exec

Display Message

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.

OSPF Routes: Total number of routes installed by OSPF protocol.

Total Routes: Total number of routes in the routing table.

8.2.1.12 show ip route precedence

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.

Syntax
show ip route preferences

Default Setting

None

Command Mode

Privileged Exec

User Exec

Display Message

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 Type-1 route preference value.

OSPF Ext T2: This field displays the OSPF Type-2 route preference value.

RIP: This field displays the RIP route preference value.

8.2.2 Configuration Commands

8.2.2.1 routing

This command enables routing for an interface.

Syntax
routing

```
no routing
```

no - Disable routing for an interface.

Default Setting

Disabled

Command Mode

Interface Config

8.2.2.2 ip routing

This command enables the IP Router Admin Mode for the master switch.

Syntax

```
ip routing
no ip routing
```

no - Disable the IP Router Admin Mode for the master switch.

Default Setting

Disabled

Command Mode

Global Config

8.2.2.3 ip address

This command configures an IP address on an interface. The IP address may be a secondary IP address.

Syntax

```
ip address <ipaddr> <subnet-mask> [secondary]
no ip address <ipaddr> <subnet-mask> [secondary]
```

<ipaddr> - IP address of the interface.

<subnet-mask> - Subnet mask of the interface.

[secondary] - It is a secondary IP address.

no - Delete an IP address from an interface.

Default Setting

None

Command Mode

Interface Config

8.2.2.4 ip route

This command configures a static route.

Syntax

```
ip route <networkaddr> <subnetmask> [ <nexthopip> [<1-255 >] ]
no ip route <networkaddr> <subnetmask> [ { <nexthopip> | <1-255 > } ]
```

<ipaddr> - A valid IP address .

<subnetmask> - A valid subnet mask.

<nexthopip> - IP address of the next hop router.

<1-255> - The precedence value of this route. The range is 1 to 255.

no - delete all next hops to a destination static route. If the optional <nextHopRtr> parameter is designated, the next hop is deleted and if the optional precedence value is designated, the precedence value of the static route is reset to its default value 1.

Default Setting

None

Command Mode

Global Config

8.2.2.5 ip route default

This command configures the default route.

Syntax

```
ip route default <nexthopip> [1-255]
```

<nexthopip> - IP address of the next hop router.

<1-255> - Precedence value of this route.

Default Setting

None

Command Mode

Global Config

8.2.2.6 ip route precedence

This command sets the default precedence for static routes. Lower route preference values are preferred when determining the best route. The "ip route" and "ip default-next-hop" commands allow you to optionally set the precedence of an individual static route. The default precedence is used when no precedence is specified in these commands. Changing the default precedence does not update the precedence of existing static routes, even if they were assigned the original default precedence. The new default precedence will only be applied to static routes created after invoking the "ip route precedence" command.

Syntax

```
ip route precedence <1-255>
```

<1-255> - Default precedence value of static routes. The range is 1 to 255.

Default Setting

The default precedence value is 1.

Command Mode

Global Config

8.2.2.7 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.

Syntax

```
ip mtu <68-1500>
no ip mtu <68-1500>
```

<68-9198> - The IP MTU on a routing interface. The range is 68 to 1500.

no - Reset the ip mtu to the default value.

Default Setting

The default value is 1500.

Command Mode

Interface Config

8.2.2.8 encapsulation

This command configures the link layer encapsulation type for the packet.

Syntax

encapsulation {ethernet | snap}

ethernet - The link layer encapsulation type is ethernet.

snap - The link layer encapsulation type is SNAP.

Default Setting

The default value is ethernet.

Command Mode

Interface Config

Restrictions

Routed frames are always Ethernet encapsulated when a frame is routed to a VLAN.

8.3 Open Shortest Path First (OSPF) Commands

8.3.1 Show Commands

8.3.1.1 show ip ospf

This command displays information relevant to the OSPF router.

Syntax

show ip ospf

Default Setting

None

Command Mode

Privileged Exec

Display Messages

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 : Indicates 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 learned by other protocols) or disabled (if the router is not configured for the same).

RFC 1583 Compatibility : Indicates whether 1583 compatibility is enabled or disabled. This is a configured value.

External LSDB Limit : The maximum number of non-default AS-external-LSA (link state advertisement) entries that can be stored in the link-state database.

Exit Overflow Interval : The number of seconds that, after entering overflow state, a router will attempt to leave overflow state.

Spf Delay Time : The number of seconds between two subsequent changes of LSAs, during which time the routing table calculation is delayed.

Spf Hold Time: The number of seconds between two consecutive spf calculations.

Opaque Capability: Shows whether the router is capable of sending Opaque LSAs. This is a configured value.

Autocost Ref BW: Shows the value of auto-cost reference bandwidth configured on the router.

ABR Status: Shows whether the router is an OSPF Area Border Router.

ASBR Status: Reflects whether the ASBR mode is enabled or disabled. Enable implies that the router is an autonomous system border router. The router automatically becomes an ASBR when it is configured to redistribute routes learnt from other protocols. The possible values for the ASBR status is enabled (if the router is configured to redistribute routes learned by other protocols) or disabled (if the router is not configured for the same).

Stub Router: When OSPF runs out of resources to store the entire link state database, or any other state information, OSPF goes into stub router mode. As a stub router, OSPF re-originates its own router LSAs, setting the cost of all non-stub interfaces to infinity. To restore OSPF to normal operation, disable and re-enable OSPF.

Exit Overflow Interval: The number of seconds that, after entering overflow state, a router will attempt to leave overflow state.

External LSDB Overflow: When the number of non-default external LSAs exceeds the configured limit, External LSDB Limit, OSPF goes into LSDB overflow state. In this state, OSPF withdraws all of its self-originated non-default external LSAs. After the Exit Overflow Interval, OSPF leaves the overflow state, if the number of external LSAs has been reduced.

External LSA Count: The number of external (LS type 5) link-state advertisements in the link-state database.

External LSA Checksum: The sum of the LS checksums of external link-state advertisements contained in the link-state database.

AS_OPAQUE LSA Count: Shows the number of AS Opaque LSAs in the link-state database.

AS_OPAQUE LSA Checksum: Shows the sum of the LS Checksums of AS Opaque LSAs contained in the link-state database.

New LSAs Originated: The number of new link-state advertisements that have been originated.

LSAs Received: The number of link-state advertisements received determined to be new instantiations.

LSA Count: The total number of link state advertisements currently in the link state database.

Maximum Number of LSAs: The maximum number of LSAs that OSPF can store.

LSA High Water Mark: The maximum size of the link state database since the system started.

Retransmit List Entries: The total number of LSAs waiting to be acknowledged by all neighbors. An LSA may be pending acknowledgment from more than one neighbor.

Maximum Number of Retransmit Entries: The maximum number of LSAs that can be waiting for acknowledgment at any given time.

Retransmit Entries High Water Mark: The highest number of LSAs that have been waiting for acknowledgment.

External LSDB Limit: 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 Passive Setting: Shows whether the interfaces are passive by default.

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: The metric of the routes being redistributed. If the metric is not configured, this field is blank.

Metric Type: Shows whether the routes are External Type 1 or External Type 2.

Number of Active Areas: The number of active OSPF areas. An “active” OSPF area is an area with at least one interface up.

AutoCost Ref BW: Shows the value of auto-cost reference bandwidth configured on the router.

Maximum Paths: 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: The source protocol/routes that are being redistributed. Possible values are static, connected, BGP, or RIP.

Tag: The decimal value attached to each external route.

Subnets: For redistributing routes into OSPF, the scope of redistribution for the specified protocol.

Distribute-List: The access list used to filter redistributed routes.

8.3.1.2 show ip ospf abr

This command displays the internal OSPF routing table entries to Area Border Routers (ABR). This command takes no options

Syntax

```
show ip ospf abr
```

Default Setting

None

Command Mode

Privileged Eexc

User Exec

Display Messages

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.

8.3.1.3 show ip ospf area

This command displays information about the area. The <areaid> identifies the OSPF area that is being displayed.

Syntax

```
show ip ospf area <areaid>
```

Default Setting

None

Command Mode

Privileged Exec

User Exec

Display Messages

AreaID: The area id of the requested OSPF area.

External Routing: A number representing the external routing capabilities for this area.

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.

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: 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: The metric value for the default route advertised into the NSSA.

Default Metric Type: The metric type for the default route advertised into the NSSA.

Translator Role: The NSSA translator role of the ABR, which is always or candidate.

Translator Stability Interval: 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.

8.3.1.4 show ip ospf asbr

This command displays the internal OSPF routing table entries to Autonomous System Boundary Routers (ASBR). This command takes no options.

Syntax

show ip ospf asbr

Default Setting

None

Command Mode

Privileged Exec

User Exec

Display Messages

Type: The type of the route to the destination. It can be one of the following values:

- 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.

8.3.1.5 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.

Syntax

sow ip ospf [<areaid>] database [{database-summary | [{asbr-summary network | nssa-external | opaque-area | opaque-as | opaque-link | mmary}] [<lsid>] [{adv-router [<ipaddr>] | self-originate}]}]

asbr-summary - Use asbr-summary to show the autonomous system boundary router (ASBR) summary LSAs.

external - Use external to display the external LSAs.

Network - Use network to display the network LSAs.

nssa-external - Use nssa-external to display NSSA external LSAs.

opaque-area - Use opaque-area to display area opaque LSAs.

opaque-as - Use opaque-as to display AS opaque LSAs.

opaque-link - Use opaque-link to display link opaque LSAs.

router - Use router to display router LSAs.

summary - Use summary to show the LSA database summary information.

Lsid - 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.

adv-router - Use adv-router to show the LSAs that are restricted by the advertising router.

self-originate - Use self-originate to display the LSAs in that are self originated. The information below is only displayed if OSPF is enabled

Default Setting

None

Command Mode

Privileged Exec

User Exec

Display Messages

Link Id: A number that uniquely identifies an LSA that a router originates from all other self originated LSAs of the same LS type.

Adv Router: The Advertising Router. Is a 32 bit dotted decimal number representing the LSDB interface.

Age: A number representing the age of the link state advertisement in seconds.

Sequence: A number that represents which LSA is more recent.

Checksum: 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.

8.3.1.6 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.

Syntax
show ip ospf database database-summary

Default Setting

None

Command Mode

Privileged Exec

User Exec

Display Messages

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.

Opaque AS: Number of opaque AS LSAs in the database.

Total: Number of entries for all areas.

8.3.1.7 show ip ospf interface

This command displays the information for the IFO object or virtual interface tables.

Syntax
show ip ospf interface {<slot/port> | loopback <loopback-id>}

Default Setting

None

Command Mode

Privileged Exec

User Exec

Display Messages

IP Address: The IP address for the specified interface.

Subnet Mask: A mask of the network and host portion of the IP address for the OSPF interface.

Secondary IP Address(es): The secondary IP addresses if any are configured on the interface.

OSPF Admin Mode: States whether OSPF is enabled or disabled on a router interface.

OSPF Area ID: The OSPF Area ID for the specified interface.

OSPF Network Type: The type of network on this interface that the OSPF is running on.

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 Acknowledgment 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.

Metric Cost: The cost of the OSPF interface.

Passive Status: Shows whether the interface is passive or not.

OSPF MTU-ignore: Indicates whether to ignore MTU mismatches in database descriptor packets sent from neighboring routers.

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.

Local Link LSAs: The number of Link Local Opaque LSAs in the link-state database.

Local Link LSA Checksum: The sum of LS Checksums of Link Local Opaque LSAs in the link-state database.

8.3.1.8 show ip ospf interface brief

This command displays brief information for the IFO object or virtual interface tables.

Syntax
show ip ospf interface brief

Default Setting

None

Command Mode

Privileged Exec

User Exec

Display Messages

Interface: Valid slot and port number separated by a forward slash.

OSPF Admin Mode: States whether OSPF is enabled or disabled on a router interface.

OSPF Area ID: 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 Acknowledgment Interval for the specified interface.

8.3.1.9 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.

Syntax
show ip ospf interface stats <slot/port>

Default Setting

None

Command Mode

Privileged Exec

User Exec

Display Messages

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: Discards The number of received OSPF packets discarded because of an error in the packet or an error in processing the packet.

Bad Version: 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.

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.

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.

No Neighbor at Source Address: The number of OSPF packets dropped because the sender is not an existing neighbor or the sender's address does not match the previously recorded IP address for that neighbor.

Invalid OSPF Packet Type: The number of OSPF packets discarded because the packet type field in the OSPF header is not a known type.

Hellos Ignored: The number of received Hello packets that were ignored by this router from the new neighbors after the limit has been reached for the number of neighbors on an interface or on the system as a whole.

8.3.1.10 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.

Syntax

show ip ospf neighbor [interface <slot/port>] [<ip-address>]

Default Setting

None

Command Mode

Privileged Exec

User Exec

Display Messages

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: The 4-digit dotted-decimal number of the neighbor router.

Priority: 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: The IP address of the neighbor.

Interface: The interface of the local router in slot/port format.

State: 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 - no recent information has been received from the neighbor but a more concerted effort should be made to contact the neighbor.
- Init - an Hello packet has recently been seen from the neighbor, but bidirectional 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 neighboring 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: 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 a forward slash.

Neighbor IP Address: The IP address of the neighbor router.

Interface Index: The interface ID of the neighbor router.

Area ID: 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: 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: The amount of time, in seconds, to wait before the router assumes the neighbor is unreachable.

Up Time: Neighbor uptime; how long since the adjacency last reached the Full state.

State: 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: An integer representing the current length of the retransmission queue of the specified neighbor router Id of the specified interface.

8.3.1.11 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..

Syntax
show ip ospf range <areaid>

Default Setting

None

Command Mode

Privileged Exec

User Exec

Display Messages

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.

8.3.1.12 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.

Syntax

show ip ospf statistics

Default Setting

None

Command Mode

Privileged Exec

User Exec

Display Messages

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

8.3.1.13 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..

Syntax

show ip ospf stub table

Default Setting

None

Command Mode

Privileged Exec

User Exec

Display Messages

Area ID: A 32-bit identifier for the created stub area.

Type of Service: The type of service associated with the stub metric. only supports 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.

8.3.1.14 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.

Syntax
show ip ospf virtual-link <areaid> <neighbor>

Default Setting

None

Command Mode

Privileged Exec

User Exec

Display Messages

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.

8.3.1.15 show ip ospf virtual-link brief

This command displays the OSPF Virtual Interface information for all areas in the system.

Syntax

show ip ospf virtual-link brief

Default Setting

None

Command Mode

Privileged Exec

User Exec

Display Messages

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.

8.3.2 Configuration Commands

8.3.2.1 router ospf

Use this command to enter Router OSPF mode.

Syntax

router ospf

Default Setting

None

Command Mode

Global Config

8.3.2.2 enable

Use **enable** command resets the default administrative mode of OSPF in the router (active). **no enable** command sets the administrative mode of OSPF in the router to inactive

Syntax

enable
no enable

Default Setting

Enabled

Command Mode

Router OSPF Config Mode

8.3.2.3 network area

Use **network area** command to enable OSPFv2 on an interface and set its area ID if the IP address of an interface is covered by this network command. Use **no network area** command to disable the OSPFv2 on a interface if the IP address of an interface was earlier covered by this network command

Syntax

network <ip-address> <wildcard-mask> area <area-id>
no network <ip-address> <wildcard-mask> area <area-id>

Default Setting

Disabled

Command Mode

Router OSPF Config Mode

8.3.2.4 ip ospf area

Use **ip ospf area** command to enable OSPFv2 and set the area ID of an interface. The <*area-id*> is an IP address formatted as a 4-digit dotted-decimal number or a decimal value in the range of <0-4294967295>. This command supersedes the effects of the **network area** command. It can also be used to configure the advertiseability of the secondary addresses on this interface into the OSPFv2 domain. Use **no ip ospf area** command to disable OSPF on an interface.

Syntax

ip ospf area <area-id> [secondaries none]
no ip ospf area [secondaries none]

Default Setting

Disabled

Command Mode

Interface Config

8.3.2.5 1583compatibility

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.
1583compatibility command enables OSPF 1583 compatibility. **no 1583compatibility** command disables OSPF 1583 compatibility

Syntax

1583compatibility
no 1583compatibility

Default Setting

Enabled

Command Mode

Router OSPF Config Mode

8.3.2.6 area default-cost

This command configures the default cost for the stub area. You must specify the area ID and an integer value between 1-16777215

Syntax

area <areaid> default-cost <1-16777215>

Default Setting

None

Command Mode

Router OSPF Config Mode

8.3.2.7 area nssa

area nssa command configures the specified areaid to function as an NSSA. **no area nssa** command disables nssa from the specified area id.

Syntax

```
area <areaid> nssa
no area <areaid> nssa
```

Default Setting

None

Command Mode

Router OSPF Config Mode

8.3.2.8 area nssa default-info-originate

area nssa default-info-originate 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). This command disables the default route advertised into the NSSA . **no area nssa default-info-originate** command disables the default route advertised into the NSSA.

Syntax

```
area <areaid> nssa default-info-originate [<metric>] [{comparable | noncomparable}]
no area <areaid> nssa default-info-originate [<metric>] [{comparable | noncomparable}]
```

Default Setting

None

Command Mode

Router OSPF Config Mode

8.3.2.9 area nssa no-redistribute

area nssa no-redistribute command configures the NSSA Area Border router (ABR) so that learned external routes will not be redistributed to the NSSA. **no area nssa no-redistribute** command disables the NSSA ABR so that learned external routes are redistributed to the NSSA

Syntax

```
area <areaid> nssa no-redistribute
no area <areaid> nssa no-redistribute
```

Default Setting

None

Command Mode

Router OSPF Config Mode

8.3.2.10 area nssa no-summary

area nssa no-summary command configures the NSSA so that summary LSAs are not advertised into the NSSA. **no area nssa no-summary** command disables nssa from the summary LSAs

Syntax

area <areaid> nssa no-summary
no area <areaid> nssa no-summary

Default Setting

None

Command Mode

Router OSPF Config Mode

8.3.2.11 area nssa translator-role

area nssa translator-role 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. **no area nssa translator-role** command disables the nssa translator role from the specified area id.

Syntax

area <areaid> nssa translator-role {always | candidate}
no area <areaid> nssa translator-role {always | candidate}

Default Setting

None

Command Mode

Router OSPF Config Mode

8.3.2.12 area nssa translator-stab-intv

area nssa translator-stab-intv 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. **no area nssa translator-stab-intv** command disables the nssa translator's <*stabilityinterval*> from the specified area id.

Syntax

```
area <areaid> nssa translator-stab-intv <stabilityinterval>
no area <areaid> nssa translator-stab-intv <stabilityinterval>
```

Default Setting

None

Command Mode

Router OSPF Config Mode

8.3.2.13 area range

area range 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. **no area range** command deletes a specified area range. The <*ipaddr*> is a valid IP address. The <*subnetmask*> is a valid subnet mask.

Syntax

```
area <areaid> range <ipaddr> <subnetmask> {summarylink | nssaexternallink} [advertise |
not-advertise]
no area <areaid> range <ipaddr> <subnetmask>
```

Default Setting

None

Command Mode

Router OSPF Config Mode

8.3.2.14 area stub

area stub 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. **no area stub** command deletes a stub area for the specified area ID.

Syntax

```
area <areaid> stub
no area <areaid> stub
```

Default Setting

None

Command Mode

Router OSPF Config Mode

8.3.2.15 area stub no-summary

area stub no-summary command configures the Summary LSA mode for the stub area identified by <*areaid*>. Use this command to prevent LSA Summaries from being sent. **no area stub no-summary** command configures the default Summary LSA mode for the stub area identified by <*areaid*>.

Syntax

```
area <areaid> stub no-summary
no area <areaid> stub no-summary
```

Default Setting

Disabled

Command Mode

Router OSPF Config Mode

8.3.2.16 area virtual-link

area virtual-link command creates the OSPF virtual interface for the specified <*areaid*> and <*neighbor*>. The <*neighbor*> parameter is the Router ID of the neighbor. **no area virtual-link** 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.

Syntax

```
area <areaid> virtual-link <neighbor>
no area <areaid> virtual-link <neighbor>
```

Default Setting

None

Command Mode

Router OSPF Config Mode

8.3.2.17 area virtual-link authentication

area virtual-link authentication 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.

no area virtual-link authentication 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.

Syntax

area <areaid> virtual-link <neighbor> authentication {none | {simple <key>} | {encrypt <key> <keyid>}}
no area <areaid> virtual-link <neighbor> authentication

Default Setting

None

Command Mode

Router OSPF Config Mode

8.3.2.18 area virtual-link dead-interval

area virtual-link dead-interval 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. **no area virtual-link dead-interval** 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

Syntax

area <areaid> virtual-link <neighbor> dead-interval <seconds>
no area <areaid> virtual-link <neighbor> dead-interval

Default Setting

40

Command Mode

Router OSPF Config Mode

8.3.2.19 area virtual-link hello-interval

area virtual-link hello-interval 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. **no area virtual-link hello-interval** 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

Syntax

```
area <areaid> virtual-link <neighbor> hello-interval <1-65535>
no area <areaid> virtual-link <neighbor> hello-interval
```

Default Setting

10

Command Mode

Router OSPF Config Mode

8.3.2.20 area virtual-link retransmit-interval

area virtual-link retransmit-interval 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.. **no area virtual-link retransmit -interval** 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

Syntax

```
area <areaid> virtual-link <neighbor> retransmit-interval <seconds>
no area <areaid> virtual-link <neighbor> retransmit-interval
```

Default Setting

5

Command Mode

Router OSPF Config Mode

8.3.2.21 area virtual-link transmit-delay

area virtual-link transmit-delay 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). **no area virtual-link transmit-delay** command resets the default transmit delay for the OSPF virtual interface to the default value.

Syntax

```
area <areaid> virtual-link <neighbor> transmit-delay <seconds>
no area <areaid> virtual-link <neighbor> transmit-delay
```

Default Setting

1

Command Mode

Router OSPF Config Mode

8.3.2.22 auto-cost

By default, OSPF computes the link cost of each interface from the interface bandwidth. Faster links have lower metrics,making them more attractive in route selection. The configuration parameters in the **auto-cost reference bandwidth** and **bandwidth** commands give you control over the default link cost. You can configure for OSPF an interface bandwidth that is independent of the actual link speed. A second configuration parameter allows you to control the ratio of interface bandwidth to link cost. The link cost is computed as the ratio of a reference bandwidth to the interface bandwidth (ref_bw /interface bandwidth), where interface bandwidth is defined by the **bandwidth** command. Because the default reference bandwidth is 100 Mbps, OSPF uses the same default link cost for all interfaces whose bandwidth is 100 Mbps or greater. Use the **auto-cost** command to change the reference bandwidth, specifying the reference bandwidth in megabits per second (Mbps). The reference bandwidth range is 1-4294967 Mbps. The different reference bandwidth can be independently configured for OSPFv2 and OSPFv3.

Use **no auto-cost** command to set the reference bandwidth to the default value.

Syntax

```
auto-cost reference-bandwidth <1 to 4294967>
no auto-cost reference-bandwidth
```

Default Setting

100Mbps

Command Mode

Router OSPF Config Mode

8.3.2.23 bandwidth

By default, OSPF computes the link cost of an interface as the ratio of the reference bandwidth to the interface bandwidth. Reference bandwidth is specified with the **auto-cost** command. For the purpose of the OSPF link cost calculation, use the bandwidth command to specify the interface bandwidth. The bandwidth is specified in kilobits per second. If no bandwidth is configured, the bandwidth defaults to the actual interface bandwidth for port-based routing interfaces and to 10 Mbps for VLAN routing interfaces. This command does not affect the actual speed of an interface. Use **no bandwidth** command to set the interface bandwidth to its default value

Syntax

```
bandwidth <1-10000000>
no bandwidth
```

Default Setting

Actual interface bandwidth

Command Mode

Interface Config

8.3.2.24 capability opaque

Use **capability opaque** command to enable Opaque Capability on the Router. The information contained in Opaque LSAs may be used directly by OSPF or indirectly by an application wishing to distribute information throughout the OSPF domain. Supports the storing and flooding of Opaque LSAs of different scopes. Use **no capability opaque** command to disable opaque capability on the router

Syntax

capability opaque
no capability opaque

Default Setting

Disabled

Command Mode

Router OSPF Config Mode

8.3.2.25 clear ip ospf

Use this command to disable and re-enable OSPF.

Syntax

clear ip ospf

Default Setting

None

Command Mode

Privileged Exec

8.3.2.26 clear ip ospf configuration

Use this command to reset the OSPF configuration to factory defaults.

Syntax

clear ip ospf configuration

Default Setting

None

Command Mode

Privileged Exec

8.3.2.27 clear ip ospf counters

Use this command to reset global and interface statistics

Syntax
clear ip ospf counters

Default Setting

None

Command Mode

Privileged Exec

8.3.2.28 clear ip ospf neighbor

Use this command to drop the adjacency with all OSPF neighbors. On each neighbor's interface, send a one-way hello.Adjacencies may then be re-established. To drop all adjacencies with a specific router ID, specify the neighbor's Router ID using the optional parameter [neighbor-id].

Syntax
clear ip ospf neighbor [neighbor-id]

Default Setting

None

Command Mode

Privileged Exec

8.3.2.29 clear ip ospf neighbor interface

To drop adjacency with all neighbors on a specific interface, use the optional parameter [slot/port]. To drop adjacency with a specific router ID on a specific interface, use the optional parameter [neighbor-id].

Syntax

clear ip ospf neighbor interface [slot/port] [neighbor-id]

Default Setting

None

Command Mode

Privileged Exec

8.3.2.30 clear ip ospf redistribution

Use this command to flush all self-originated external LSAs. Reapply the redistribution configuration and re-originate prefixes as necessary.

Syntax

clear ip ospf redistribution

Default Setting

None

Command Mode

Privileged Exec

8.3.2.31 default-information originate

default-information originate command is used to control the advertisement of default routes.

no default-information originate command is used to control the advertisement of default routes.

Syntax

default-information originate [always] [metric <0-16777214>] [metric-type {1 | 2}]
no default-information originate [metric] [metric-type]

Default Setting

metric—unspecified

type—2

Command Mode

Router OSPF Config Mode

8.3.2.32 default-metric

default-metric command is used to set a default for the metric of distributed routes.

no default-metric command is used to set a default for the metric of distributed routes.

Syntax

```
default-metric <1-16777214>
no default-metric
```

Default Setting

None

Command Mode

Router OSPF Config Mode

8.3.2.33 distance ospf

distance ospf 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 route can be intra, inter, or external. All the external type routes are given the same preference value. The range of <preference> value is 1 to 255. **no distance ospf** command sets the default route preference value of OSPF routes in the router. The type of OSPF can be intra, inter, or external. All the external type routes are given the same preference value.

Syntax

```
distance ospf {intra-area <1-255> | inter-area <1-255> | external <1-255>}
no distance ospf {intra-area | inter-area | external}
```

Default Setting

110

Command Mode

Router OSPF Config Mode

8.3.2.34 distribute-list out

Use **distribute-list out** command to specify the access list to filter routes received from the source protocol.

no distribute-list ou command to specify the access list to filter routes received from the source protocol.

Syntax

```
distribute-list <1-199> out {rip | bgp | static | connected}
no distribute-list <1-199> out {rip | bgp | static | connected}
```

Default Setting

None

Command Mode

Router OSPF Config Mode

8.3.2.35 exit-overflow-interval

exit-overflow-interval 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. **no exit-overflow-interval** command configures the default exit overflow interval for OSPF.

Syntax

```
exit-overflow-interval <seconds>
no exit-overflow-interval
```

Default Setting

0

Command Mode

Router OSPF Config Mode

8.3.2.36 external-lsdb-limit

external-lsdb-limit 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. **no external-lsdb-limit** command configures the default external LSDB limit for OSPF.

Syntax

```
external-lsdb-limit <limit>
no external-lsdb-limit
```

<limit> - The range for limit is -1 to 2147483647. If the value is -1, then there is no limitation.

Default Setting

-1

Command Mode

Router OSPF Config Mode

8.3.2.37 ip ospf authentication

ip ospf authentication 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. There is no default value for this command.

no ip ospf authentication command sets the default OSPF Authentication Type for the specified interface.

Syntax
ip ospf authentication {none | {simple <key>} | {encrypt <key> <keyid>}} no ip ospf authentication

Default Setting

None

Command Mode

Interface Config

8.3.2.38 ip ospf cost

ip ospf cost command configures the cost on an OSPF interface. The <cost> parameter has a range of 1 to 65535. **no ip ospf cost** command configures the default cost on an OSPF interface.

Syntax
ip ospf cost <1–65535> no ip ospf cost

Default Setting

10

Command Mode

Interface Config

8.3.2.39 ip ospf dead-interval

ip ospf dead-interval 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 in seconds from 1 to 2147483647. **no ip ospf dead-interval** command sets the default OSPF dead interval for the specified interface.

Syntax

ip ospf dead-interval <seconds>
no ip ospf dead-interval

Default Setting

40

Command Mode

Interface Config

8.3.2.40 ip ospf hello-interval

ip ospf hello-interval 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. **no ip ospf hello-interval** command sets the default OSPF hello interval for the specified interface.

Syntax

ip ospf hello-interval <seconds>
no ip ospf hello-interval

Default Setting

10

Command Mode

Interface Config

8.3.2.41 ip ospf network

ip ospf network command to configure OSPF to treat an interface as a point-to-point rather than broadcast interface. The broadcast option sets the OSPF network type to broadcast. The point-to-point option sets the OSPF network type to point-to-point. OSPF treats interfaces as broadcast interfaces by default. (Loopback interfaces have a special loopback network type, which cannot be changed.) When there are only two routers on the network, OSPF can operate more efficiently by treating the network as a

point-to-point network. For point-to-point networks, OSPF does not elect a designated router or generate a network link state advertisement (LSA). Both endpoints of the link must be configured to operate in point-to-point mode..

no ip ospf network command to return the OSPF network type to the default.

Syntax

```
ip ospf network {broadcast|point-to-point}
no ip ospf network
```

Default Setting

Broadcast

Command Mode

Interface Config

8.3.2.42 ip ospf priority

ip ospf priority 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. **no ip ospf priority** command sets the default OSPF priority for the specified router interface.

Syntax

```
ip ospf priority <0-255>
no ip ospf priority
```

Default Setting

1, which is the highest router priority

Command Mode

Interface Config

8.3.2.43 ip ospf retransmit-interval

ip ospf retransmit 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). **no ip ospf retransmit** command sets the default OSPF retransmit Interval for the specified interface.

Syntax

```
ip ospf retransmit-interval <0-3600>
no ip ospf retransmit-interval
```

Default Setting

5

Command Mode

Interface Config

8.3.2.44 ip ospf transmit-delay

ip ospf transmit-delay 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). **no ip ospf transmit-delay** command sets the default OSPF Transit Delay for the specified interface

Syntax

```
ip ospf transmit-delay <1-3600>
no ip ospf transmit-delay
```

Default Setting

1

Command Mode

Interface Config

8.3.2.45 ip ospf mtu-ignore

ip ospf mtu-ignore 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. **no ip ospf mtu-ignore** command enables the OSPF MTU mismatch detection.

Syntax

```
ip ospf mtu-ignore
no ip ospf mtu-ignore
```

Default Setting

Enabled

Command Mode

Interface Config

8.3.2.46 router-id

router-id command sets a 4-digit dotted-decimal number uniquely identifying the router ospf id. The <ipaddress> is a configured value.

Syntax

router-id <ipaddress>

Default Setting

None

Command Mode

Router OSPF Config Mode

8.3.2.47 redistribute

redistribute command configures OSPF protocol to allow redistribution of routes from the specified source protocol/routers. **no redistribute** command configures OSPF protocol to prohibit redistribution of routes from the specified source protocol/routers.

Syntax

redistribute {rip | bgp | static | connected} [metric <0-16777214>] [metric-type {1 | 2}] [tag <0-4294967295>] [subnets]
no redistribute {rip | bgp | static | connected} [metric <0-16777214>] [metric-type {1 | 2}] [tag <0-4294967295>] [subnets]

Default Setting

metric—unspecified

type—2

tag—0

Command Mode

Router OSPF Config Mode

8.3.2.48 maximum-paths

maximum-paths command sets the number of paths that OSPF can report for a given destination where maxpaths is platform dependent. **no maximum-paths** command resets the number of paths that OSPF can report for a given destination back to its default value.

Syntax

```
maximum-paths <maxpaths>
no maximum-paths
```

Default Setting

4

Command Mode

Router OSPF Config Mode

8.3.2.49 passive-interface default

passive-interface default command to enable global passive mode by default for all interfaces. It overrides any interface level passive mode. OSPF will not form adjacencies over a passive interface. **no passive-interface default** command to disable the global passive mode by default for all interfaces. Any interface previously configured to be passive reverts to non-passive mode.

Syntax

```
passive-interface default
no passive-interface default
```

Default Setting

Disabled

Command Mode

Router OSPF Config Mode

8.3.2.50 passive-interface

passive-interface command to set the interface or tunnel as passive. It overrides the global passive mode that is currently effective on the interface or tunnel. **no passive-interface** command to set the interface or tunnel as non-passive. It overrides the global passive mode that is currently effective on the interface or tunnel..

Syntax

```
passive-interface {<slot/port> | tunnel <tunnel-id>}
no passive-interface {<slot/port> | tunnel <tunnel-id>}
```

Default Setting

Disabled

Command Mode

Router OSPF Config Mode

8.3.2.51 timers spf

Use this command to configure the SPF delay time and hold time. The valid range for both parameters is 0-65535 seconds..

Syntax

timers spf <delay-time> <hold-time>

Default Setting

delay-time—5

hold-time—10

Command Mode

Router OSPF Config Mode

8.4 BOOTP/DHCP Relay Commands

8.4.1 Show Commands

8.4.1.1 show bootpdhcprelay

This command displays the BootP/DHCP Relay information.

Syntax

show bootpdhcprelay

Default Setting

None

Command Mode

Privileged Exec

User Exec

Display Message

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 of requests received.

Requests Relayed Is the number of requests relayed.

Packets Discarded Is the number of packets discarded.

8.4.2 Configuration Commands

8.4.2.1 bootpdhcprelay cidoptmode

This command enables the circuit ID option mode for BootP/DHCP Relay on the system.

Syntax

```
bootpdhcprelay cidoptmode
no bootpdhcprelay cidoptmode
```

Default Setting

Disabled

Command Mode

Global Config

8.4.2.2 bootpdhcprelay enable

This command enables the forwarding of relay requests for BootP/DHCP Relay on the system.

Syntax

```
bootpdhcprelay enable
no bootpdhcprelay enable
```

no - Disable the forwarding of relay requests for BootP/DHCP Relay on the system.

Default Setting

Disabled

Command Mode

Global Config

8.4.2.3 bootpdhcprelay maxhopcount

This command configures the maximum allowable relay agent hops for BootP/DHCP Relay on the system.

Syntax

```
bootpdhcprelay maxhopcount <1-16>
no bootpdhcprelay maxhopcount
```

<count> - The range of maximum hop count is 1 to 16.

no - Set the maximum hop count to 4.

Default Setting

The default value is 4.

Command Mode

Global Config

8.4.2.4 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.

Syntax

```
bootpdhcprelay minwaittime <0-100>
no bootpdhcprelay minwaittime
```

<seconds> - The range of minimum wait time is 0 to 100.

no - Set the minimum wait time to 0 seconds.

Default Setting

The default value is 0.

Command Mode

Global Config

8.4.2.5 bootpdhcprelay serverip

This command configures the server IP Address for BootP/DHCP Relay on the system.

Syntax

```
bootpdhcprelay serverip <ipaddr>
no bootpdhcprelay serverip
```

<ipaddr> - The IP address of the BootP/DHCP server.

no - Clear the IP address of the BootP/DHCP server.

Default Setting

None

Command Mode

Global Config

8.5 Routing Information Protocol (RIP) Commands

8.5.1 Show Commands

8.5.1.1 show ip rip

This command displays information relevant to the RIP router.

Syntax

```
show ip rip
```

Default Setting

None

Command Mode

Privileged Exec

Display Message

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 disabled.

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 enabled.

Host Routes Accept Mode: Select enable or disable from the pulldown menu. If you select enable the router will be accept host routes. The default is enabled.

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 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.

Distance: Configured distance value for rip routes.

8.5.1.2 show ip rip interface

This command displays information related to a particular RIP interface.

Syntax
show ip rip interface <slot/port>

< slot/port > - Interface number

Default Setting

None

Command Mode

Privileged Exec

Display Message

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, and 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.

RIP Admin Mode: RIP administrative mode of router RIP operation; enable, disable 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.

Authentication Key: 16 alpha-numeric characters for authentication key when uses simple or encrypt authentication.

Authentication Key ID: It is a Key ID when uses MD5 encryption for RIP authentication.

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.

8.5.1.3 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).

Syntax
show ip rip interface brief

Default Setting

None

Command Mode

Privileged Exec

Display Message

Interfacet: 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, disable it.

Link State: The mode of the interface (up or down).

8.5.2 Configuration Commands

8.5.2.1 enable rip

This command resets the default administrative mode of RIP in the router (active).

Syntax

```
enable
no enable
```

no - This command sets the administrative mode of RIP in the router to inactive.

Default Setting

Enabled

Command Mode

Router RIP Config

8.5.2.2 ip rip

This command enables RIP on a router interface.

Syntax

```
ip rip
no ip rip
```

no - This command disables RIP on a router interface.

Default Setting

Disabled

Command Mode

Interface Config

8.5.2.3 auto-summary

This command enables the RIP auto-summarization mode.

Syntax

```
auto-summary
no auto-summary
```

no - This command disables the RIP auto-summarization mode.

Default Setting

Disabled

Command Mode

Router RIP Config

8.5.2.4 default-information originate

This command is used to set the advertisement of default routes.

Syntax

```
default-information originate
no default-information originate
```

no - This command is used to cancel the advertisement of default routes.

Default Setting

Not configured

Command Mode

Router RIP Config

8.5.2.5 default-metric

This command is used to set a default for the metric of distributed routes.

Syntax

```
default-metric <1-15>
no default-metric
```

<1 - 15> - a value for default-metric.

no - This command is used to reset the default metric of distributed routes to its default value.

Default Setting

Not configured

Command Mode

Router RIP Config

8.5.2.6 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.

Syntax

```
distance rip <1-255>
no distance rip
```

<1 - 255> - the value for distance.

no - This command sets the default route preference value of RIP in the router.

Default Setting

15

Command Mode

Router RIP Config

8.5.2.7 hostrouteaccept

This command enables the RIP hostroutesaccept mode.

Syntax

```
hostrouteaccept
no hostrouteaccept
```

no - This command disables the RIP hostroutesaccept mode.

Default Setting

Enabled

Command Mode

Router RIP Config

8.5.2.8 split-horizon

This command sets the RIP split horizon mode. **None mode** will not use RIP split horizon mode. **Simple mode** will be that a route is not advertised on the interface over which it is learned. **Poison mode** will be that routes learned over this interface should be re-advertised on the interface with a metric of infinity (16).

Syntax

```
split-horizon {none | simple | poison}
no split-horizon
```

none - This command sets without using RIP split horizon mode.

simple - This command sets to use simple split horizon mode.

poison - This command sets to use poison reverse mode.

no - This command cancel to set the RIP split horizon mode and sets none mode.

Default Setting

Simple

Command Mode

Router RIP Config

8.5.2.9 distribute-list

This command is used to specify the access list to filter routes received from the source protocol. Source protocols have OSPF, Static, and Connected.

Syntax

```
distribute-list <1-199> out {ospf | static | connected}
no distribute-list <1-199> out {ospf | static | connected}
```

<1 - 199> - Access List ID value. The Access List filters the routes to be redistributed by the source protocol.

no - This command is used to cancel the access list to filter routes received from the source protocol.

Default Setting

0

Command Mode

Router RIP Config

8.5.2.10 redistribute

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 <matchtype> the match-type or types specified are added to any match types presently being redistributed. Internal routes are redistributed by default. Source protocols have OSPF, Static, and Connetced. Match types will have internal, external 1, external 2, nssa-external 1, and nssa-external 2.

Syntax

Format for OSPF as source protocol:
redistribute ospf [metric <1-15>] [match [internal] [external 1] [external 2] [nssa-external 1] [nssa-external 2]]
Format for other source protocols:
redistribute {static | connected} [metric <1-15>]
no redistribute {ospf | static | connected} [metric] [match [internal] [external 1] [external 2] [nssa-external 1] [nssa-external 2]]

<1 - 15> - a value for metric.

no - This command de-configures RIP protocol to redistribute routes from the specified source protocol/routers.

Default Setting

Metric - not-configured

Match - internal

Command Mode

Router RIP Config

8.5.2.11 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.

Syntax

ip rip authentication {none | {simple <key>} | {encrypt <key> <keyid>}}
no ip rip authentication

none - This command uses no authentication.

simple - This command uses simple authentication for RIP authentication .

encrypt - This command uses MD5 encryption for RIP authentication.

<key> - 16 alpha-numeric characters to be used for authentication key.

<keyid> - a value in the range of 0 – 255 to be used for MD5 encryption.

no - This command sets the default RIP Version 2 Authentication Type.

Default Setting

None

Command Mode

Interface Config

8.5.2.12 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

Syntax

```
ip rip receive version {rip1 | rip2 | both | none}
no ip rip receive version
```

no - This command configures the interface to allow RIP control packets of the default version(s) to be received.

Default Setting

Both

Command Mode

Interface Config

8.5.2.13 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.

Syntax

```
ip rip send version {rip1 | rip1c | rip2 | none}
no ip rip send version
```

no - This command configures the interface to allow RIP control packets of the default version to be sent.

Default Setting

rip2

Command Mode

Interface Config

8.6 Router Discovery Protocol Commands

8.6.1 Show Commands

8.6.1.1 show ip irdp

This commands displays the router discovery information for all interfaces, or a specified interface.

Syntax

show ip irdp {<slot/port> | all}

<slot/port> - Show router discovery information for the specified interface.

<all> - Show router discovery information for all interfaces.

Default Setting

None

Command Mode

Privileged Exec

User Exec

Display Message

Ad Mode: Displays the advertise mode which indicates whether router discovery is enabled or disabled on this interface.

Advertise Address: Addresses to be used to advertise the router for the interface.

Max Int: Displays the maximum advertise interval which is the maximum time allowed

between sending router advertisements from the interface in seconds.

Min Int: Displays the minimum advertise interval which is the minimum time allowed

between sending router advertisements from the interface in seconds.

Hold Time: Displays advertise holdtime which is the value of the holdtime field of the router advertisement sent from the interface in seconds.

Preferences: Displays the preference of the address as a default router address, relative to other router addresses on the same subnet.

8.6.2 Configuration Commands

8.6.2.1 ip irdp

This command enables Router Discovery on an interface.

Syntax

```
ip irdp
no ip irdp
```

<no> - Disable Router Discovery on an interface.

Default Setting

Disabled

Command Mode

Interface Config

8.6.2.2 ip irdp broadcast

This command configures the address to be used to advertise the router for the interface.

Syntax

```
ip irdp broadcast
no ip irdp broadcast
```

broadcast - The address used is 255.255.255.255.

no - The address used is 224.0.0.1.

Default Setting

The default address is 224.0.0.1

Command Mode

Interface Config

8.6.2.3 ip irdp holdtime

This commands configures the value, in seconds, of the holdtime field of the router advertisement sent from this interface.

Syntax

```
ip irdp holdtime < maxadvertinterval-9000 >
no ip irdp holdtime
```

< maxadvertinterval-9000 > The range is the maxadvertinterval to 9000 seconds.

no - This command configures the default value, in seconds, of the holdtime field of the router advertisement sent from this interface.

Default Setting

The default value is 3* maxadvertinterval (600) =1800.

Command Mode

Global Config

8.6.2.4 ip irdp maxadvertinterval

This commands configures the maximum time, in seconds, allowed between sending router advertisements from the interface.

Syntax

```
ip irdp maxadvertinterval < minadvertinterval-1800 >
no ip irdp maxadvertinterval
```

< minadvertinterval-1800 > - The range is 4 to 1800 seconds.

no - This command configures the default maximum time, in seconds.

Default Setting

The default value is 600.

Command Mode

Global Config

8.6.2.5 ip irdp minadvertinterval

This command configures the minimum time, in seconds, allowed between sending router advertisements from the interface.

Syntax

```
ip irdp minadvertinterval < 3-maxadvertinterval>
no ip irdp minadvertinterval
```

< 3-maxadvertinterval> - The range is 3 to maxadvertinterval seconds.

no - This command sets the minimum time to 450.

Default Setting

The default value is 450.

Command Mode

Global Config

8.6.2.6 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.

Syntax

```
ip irdp preference < -2147483648-2147483647>
no ip irdp preference
```

< -2147483648-2147483647> - The range is -2147483648 to 2147483647.

no - This command sets the preference to 0.

Default Setting

The default value is 0.

Command Mode

Global Config

8.7 VLAN Routing Commands

8.7.1 show ip vlan

This command displays the VLAN routing information for all VLANs with routing enabled in the system.

Syntax

```
show ip vlan
```

Default Setting

None

Command Mode

Privileged Exec

User Exec

Display Message

MAC Address used by Routing VLANs: Is the MAC Address associated with the internal bridgerouter 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: Indicates 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.

.

8.7.2 vlan routing

This command creates routing on a VLAN.

Syntax

```
vlan routing <vlanid> [<vlan-index>]
no vlan routing <vlanid>
```

<vlanid> - The range is 1 to 3965.

<vlan-index> - VLAN routing index, the range is 1 to 128.

no - Delete routing on a VLAN.

Default Setting

None

Command Mode

VLAN Database

8.8 Virtual Router Redundancy Protocol (VRRP) Commands

8.8.1 Show Commands

8.8.1.1 show ip vrrp

This command displays whether VRRP functionality is enabled or disabled. It also displays some global parameters which are required for monitoring.

Syntax

show ip vrrp

Default Setting

None

Command Mode

Privileged Exec

User Exec

Display Message

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.

8.8.1.2 show ip vrrp brief

This command displays information about each virtual router configured on the switch.

Syntax

show ip vrrp brief

Default Setting

None

Command Mode

Privileged Exec

User Exec

Display Message

Interface: Valid slot and port number separated by forward slashes.

VRID: Represents the router ID of the virtual router.

IP Address: Is the IP Address that was configured on the virtual router

Mode: Represents whether the virtual router is enabled or disabled.

State: Represents the state (Master/backup) of the virtual router.

8.8.1.3 show ip vrrp interface

This command displays all configuration information of a virtual router configured on a specific interface. Note that the information will be displayed only when the IP address of the specific interface is configured.

Syntax

```
show ip vrrp interface <slot/port> [ <vrid>]
```

<slot/port> - Valid slot and port number separated by forward slashes.

<vrid> - Virtual router ID.

Default Setting

None

Command Mode

Privileged Exec

User Exec

Display Message

VRID: Represents the router ID of the virtual router.

Primary 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 specific virtual router

8.8.1.4 show ip vrrp interface stats

This command displays the statistical information about each virtual router configured on the switch.

Syntax

```
show ip vrrp interface stats <slot/port> [ <vrid>]
```

<slot/port> - Valid slot and port number separated by forward slashes.

<vrid> - Virtual router ID.

Default Setting

None

Command Mode

Privileged Exec

User Exec

Display Message

VRID: Represents the router ID of the virtual router.

Uptime: Is 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 Errors: Represents the total number of VRRP advertisements received for which advertisement 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.

8.8.2 Configuration Commands

8.8.2.1 ip vrrp

This command enables the administrative mode of VRRP in the router.

Syntax

```
ip vrrp
no ip vrrp
```

Default Setting

Disabled

Command Mode

Global Config

This command sets the virtual router ID on an interface for Virtual Router configuration in the router.

Syntax

```
ip vrrp <1-255>
no ip vrrp <1-255>
```

<1-255> - The range of virtual router ID is 1 to 255.

<no> - This command removes all VRRP configuration details of the virtual router configured on a specific interface.

Default Setting

None

Command Mode

Interface Config

8.8.2.2 ip vrrp ip

This commands also designates the configured virtual router IP address as a secondary IP address on an interface.

Syntax

```
ip vrrp <1-255> ip <addr> [secondary]
no ip vrrp <1-255> ip <addr> [secondary]
```

<1-255> - The range of virtual router ID is 1 to 255.

<addr> - Secondary IP address of the router ID.

<no> - This command removes all VRRP configuration details of the virtual router configured on a specific interface.

Default Setting

None

Command Mode

Interface Config

8.8.2.3 ip vrrp mode

This command enables the virtual router configured on the specified interface. Enabling the status field starts a virtual router.

Syntax

```
ip vrrp <1-255> mode
no ip vrrp <1-255> mode
```

<1-255> - The range of virtual router ID is 1 to 255.

<no> - Disable the virtual router configured on the specified interface. Disabling the status field stops a virtual router.

Default Setting

Disabled

Command Mode

Interface Config

8.8.2.4 ip vrrp authentication

This command sets the authorization details value for the virtual router configured on a specified interface.

Syntax

```
ip vrrp <1-255> authentication <key>
no ip vrrp <1-255> authentication
```

<1-255> - The range of virtual router ID is 1 to 255.

<key> - A text password used for authentication.

<no> - This command sets the default authorization details value for the virtual router configured on a specified interface.

Default Setting

no authentication

Command Mode

Interface Config

8.8.2.5 ip vrrp preempt

This command sets the preemption mode value for the virtual router configured on a specified interface.

Syntax

```
ip vrrp <1-255> preempt
no ip vrrp <1-255> preempt
```

<1-255> - The range of virtual router ID is 1 to 255.

<no> - This command sets the default preemption mode value for the virtual router configured on a specified interface.

Default Setting

Enabled

Command Mode

Interface Config

8.8.2.6 ip vrrp priority

This command sets the priority value for the virtual router configured on a specified interface.

The router with the highest priority is elected master. If a router is configured with the address used as the address of the virtual router, the router is called the "address owner". The priority of the address owner is always 255 so that the address owner is always master. If the master has a priority less than 255 (it is not the address owner) and you configure the priority of another router in the group higher than the master's priority, the router will take over as master only if preempt mode is enabled.

Syntax

```
ip vrrp <1-255> priority <1-254>
no ip vrrp <1-255> priority
```

<1-255> - The range of virtual router ID is 1 to 255.

<1-254> - The range of priority is 1 to 254.

<no> - This command sets the default priority value for the virtual router configured on a specified interface.

Default Setting

The default priority value is 100 unless the router is the address owner, in which case its priority is automatically set to 255.

Command Mode

Interface Config

8.8.2.7 ip vrrp timers advertise

This command sets the advertisement value for a virtual router in seconds.

Syntax

```
ip vrrp <1-255> timers advertise <1-255>
ip vrrp <1-255> timers advertise
```

<1-255> - The range of virtual router ID is 1 to 255.

< 1-255 > - The range of advertisement interval is 1 to 255.

<no> - This command sets the default advertisement value for a virtual router.

Default Setting

The default value of advertisement interval is 1.

Command Mode

Interface Config

8.8.2.8 ip vrrp track interface

This command alters the priority of the VRRP router based on the availability of its interfaces. This command is useful for tracking interfaces that are not configured for VRRP. Only IP interfaces are tracked. A tracked interface is up if the IP on that interface is up. Otherwise, the tracked interface is down.

When the tracked interface is down or the interface has been removed from the router, the priority of the VRRP router will be decremented by the value specified in the decrement argument. When the interface is up for IP protocol, the priority will be incremented by the decrement value.

A VRRP configured interface can track more than one interface. When a tracked interface goes down, then the priority of the router will be decreased by 10 (the default priority decrement) for each downed interface. The default priority decrement is changed using the decrement argument. The default priority of the virtual router is 100, and the default decrement priority is 10. By default, no interfaces are tracked. If you specify just the interface to be tracked, without giving the optional priority, then the default priority will be set. The default priority decrement is 10.

Syntax

```
ip vrrp <1-255> track interface <slot/port> [decrement <1-254>]
no ip vrrp <1-255> track interface <slot/port> [decrement]
```

<1-255> - The range of virtual router ID is 1 to 255.

< 1-254 > - The range of decrement is 1 to 254.

<no> - This command removes the interface from the tracked list or to restore the priority decrement to its default.

Default Setting

Decrement: 10

Command Mode

Interface Config

8.8.2.9 ip vrrp track ip route

This command tracks the route reachability. When the tracked route is deleted, the priority of the VRRP router will be decremented by the value specified in the decrement argument. When the tracked route is added, the priority will be incremented by the same.

A VRRP configured interface can track more than one route. When a tracked route goes down, then the priority of the router will be decreased by 10 (the default priority decrement) for each downed route. By default no routes are tracked. If you specify just the route to be tracked, without giving the optional priority, then the default priority will be set. The default priority decrement is 10. The default priority decrement is changed using the decrement argument.

Syntax

```
ip vrrp <1-255> track ip route <ip-address/prefix-length> [decrement <1-254>]
no ip vrrp <1-255> track ip route <ip-address/prefix-length> [decrement]
```

<1-255> - The range of virtual router ID is 1 to 255.

< 1-254 > - The range of decrement is 1 to 254.

<no> - This command removes the route from the tracked list or to restore the priority decrement to its default. When removing a tracked IP route from the tracked list, the priority should be incremented by the decrement value if the route is not reachable.

Default Setting

Decrement : 10

Command Mode

Interface Config

9. IP Multicast Commands

9.1 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.

9.1.1 Show Commands

9.1.1.1 show ip dvmrp

This command displays the system-wide information for DVMRP.

Syntax
show ip dvmrp

Default Setting

None

Command Mode

Privileged Exec

User EXEC

Admin Mode This field indicates whether DVMRP is enabled or disabled. This is a configured value.

Display Message

Admin Mode: Enable or disable DVMRP function.

Version: This field indicates the version of DVMRP being used.

Total 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-infinitemetrics. The following fields are displayed for each interface**.**

Slot/Port: Valid 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.

9.1.1.2 show ip dvmrp interface

This command displays the interface information for DVMRP on the specified interface.

Syntax

show ip dvmrp interface <slot/port>

<slot/port> - Valid slot and port number separated by forward slashes.

Default Setting

None

Command Mode

Privileged Exec

User EXEC

Display Message

Interface Mode: This field indicates whether DVMRP is enabled or disabled on the specified interface. This is a configured value.

Interface 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.

9.1.1.3 show ip dvmrp neighbor

This command displays the neighbor information for DVMRP.

Syntax

show ip dvmrp neighbor

Default Setting

None

Command Mode

Privileged Exec

User EXEC

Display Message

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.

9.1.1.4 show ip dvmrp nexthop

This command displays the next hop information on outgoing interfaces for routing multicast datagrams.

Syntax
show ip dvmrp nexthop

Default Setting

None

Command Mode

Privileged Exec

User Exec

Display Message

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 slot/port format for the outgoing interface for this next hop.

Type: This field states whether the network is a LEAF or a BRANCH.

9.1.1.5 show ip dvmrp prune

This command displays the table listing the router's upstream prune information.

Syntax

show ip dvmrp prune

Default Setting

None

Command Mode

Privileged Exec

User Exec

Display Message

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.

9.1.1.6 show ip dvmrp route

This command displays the multicast routing information for DVMRP.

Syntax

show ip dvmrp route

Default Setting

None

Command Mode

Privileged Exec

User Exec

Display Message

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.

9.1.2 Configuration Commands

9.1.2.1 ip dvmrp

This command sets administrative mode of DVMRP in the router to active. IGMP must be enabled before DVMRP can be enabled.

Syntax

```
ip dvmrp
no ip dvmrp
```

no - This command sets administrative mode of DVMRP in the router to inactive. IGMP must be enabled before DVMRP can be enabled.

Default Setting

Disabled

Command Mode

Global Config

This command sets the administrative mode of DVMRP on an interface to active.

Syntax

```
ip dvmrp
no ip dvmrp
```

no - This command sets administrative mode of DVMRP on an interface to inactive.

Default Setting

Disabled

Command Mode

Interface Config

9.1.2.2 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.

Syntax

```
ip dvmrp metric <value>
no ip dvmrp metric <value>
```

<value> - This field has a range of 1 to 31.

no - 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.

Default Setting

1

Command Mode

Interface Config

9.2 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.

9.2.1 Show Commands

9.2.1.1 show ip igmp

This command displays the system-wide IGMP information.

Syntax

```
show ip igmp
```

Default Setting

None

Command Mode

Privileged Exec

User EXEC

Display Message

IGMP Admin Mode: This field displays the administrative status of IGMP. This is a configured value.

Interface: Valid 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.

9.2.1.2 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.

Syntax
show ip igmp groups <slot/port> [detail]

<slot/port> - Valid slot and port number separated by forward slashes.

[detail] - Display details of subscribed multicast groups.

Default Setting

None

Command Mode

Privileged Exec

Display Message

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: TThis 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 Compatibilty Mode: The group compatibility mode (v1, v2 or v3) for this group on the specified interface.

9.2.1.3 show ip igmp interface

This command displays the IGMP information for the interface.

Syntax
show ip igmp interface <slot/port>

<slot/port> - Valid slot and port number separated by forward slashes.

Default Setting

None

Command Mode

Privileged Exec

User EXEC

Display Message

Slot/Port: Valid 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 (secs): 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 (1/10 of a second): 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 (secs): 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 (1/10 of a second): 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.

9.2.1.4 show ip igmp interface membership

This command displays the list of interfaces that have registered in the multicast group.

Syntax
show ip igmp interface membership <multiipaddr> [detail]

< multiipaddr > - A multicast IP address..

[detail] - Display details of subscribed multicast groups.

Default Setting

None

Command Mode

Privileged Exec

User EXEC

Display Message

Iinterface: Valid 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 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.

9.2.1.5 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.

Syntax
show ip igmp interface stats <slot/port>

<slot/port> - Valid slot and port number separated by forward slashes.

Default Setting

None

Command Mode

Privileged Exec

User EXEC

Display Message

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.

9.2.2 Configuration Commands

9.2.2.1 ip igmp

This command sets the administrative mode of IGMP in the router to active.

Syntax

```
ip igmp
no ip igmp
```

no - This command sets the administrative mode of IGMP in the router to inactive.

Default Setting

Disabled

Command Mode

Global Config

This command sets the administrative mode of IGMP on an interface to active.

Syntax

```
ip igmp
no ip igmp
```

no - This command sets the administrative mode of IGMP on an interface to inactive.

Default Setting

Disabled

Command Mode

Interface Config

9.2.2.2 ip igmp version

This command configures the version of IGMP for an interface.

Syntax

```
ip igmp version {1 | 2 | 3}
no ip igmp version
```

<1- 3> - The igmp version number.

no - This command resets the version of IGMP for this interface. The version is reset to the default value.

Default Setting

3

Command Mode

Interface Config

9.2.2.3 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.

Syntax

```
ip igmp last-member-query-count <1-20>
no ip igmp last-member-query-count
```

<1-20> - The range for <1-20> is 1 to 20.

no - This command resets the number of Group-Specific Queries to the default value.

Default Setting

2

Command Mode

Interface Config

9.2.2.4 ip 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.

Syntax

```
ip igmp last-member-query-interval <0-255>
no ip igmp last-member-query-interval
```

<0-255> - The range for <0-255> is 0 to 255 tenths of a second.

no - 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.

Default Setting

10 tenths of a second

Command Mode

Interface Config

9.2.2.5 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.

Syntax

```
ip igmp query-interval <1-3600>
no ip igmp query-interval
```

<1-3600> - The range for <1-3600> is 1 to 3600 seconds.

no - 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.

Default Setting

125 seconds

Command Mode

Interface Config

9.2.2.6 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.

Syntax

```
ip igmp query-max-response-time <0-255>
no ip igmp query-max-response-time
```

<0-255> - The range for <0-255> is 0 to 255 tenths of a second.

no - 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.

Default Setting

100

Command Mode

Interface Config

9.2.2.7 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.

Syntax

```
ip igmp robustness <1-255>
no ip igmp robustness
```

<1-255> - The range for <1-255> is 1 to 255.

no - This command sets the robustness value to default.

Default Setting

2

Command Mode

Interface Config

9.2.2.8 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.

Syntax

```
ip igmp startup-query-count <1-20>
no ip igmp startup-query-count
```

<1-20> - The range for <1-20> is 1 to 20.

no - This command resets the number of Queries sent out on startup, separated by the Startup Query Interval on the interface to the default value.

Default Setting

2

Command Mode

Interface Config

9.2.2.9 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.

Syntax

```
ip igmp startup-query-interval <1-300>
no ip igmp startup-query-interval
```

<1-300> - The range for <1-300> is 1 to 300 seconds.

no - This command resets the interval between General Queries sent by a Querier on startup on the interface to the default value.

Default Setting

31

Command Mode

Interface Config

9.3 MLD Commands

This section provides a detailed explanation of the MLD 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.

9.3.1 Show Commands

9.3.1.1 show ipv6 mld groups

Use this command to display information about multicast groups that MLD reported. The information is displayed only when MLD is enabled on at least one interface. If MLD was not enabled on even one interface, there is no group information to be displayed.

Syntax

```
show ipv6 mld groups {<slot/port> | <group-address>}
```

Default Setting

None

Command Mode

Privileged Exec

Display Message

The following fields are displayed as a table when <slot/port> is specified.

Group Address: The address of the multicast group.

Interface: Interface through which the multicast group is reachable.

Up Time: Time elapsed in hours, minutes, and seconds since the multicast group has been known.

Expiry Time: Time left in hours, minutes, and seconds before the entry is removed from the MLD membership table.

When <group-address> is specified, the following fields are displayed for each multicast group and each interface.

Interface: Interface through which the multicast group is reachable.

Group Address: The address of the multicast group.

Last Reporter: The IP Address of the source of the last membership report received for this multicast group address on that interface.

Filter Mode: The filter mode of the multicast group on this interface. The values it can take are *include* and *exclude*.

Version 1 Host Timer: The time remaining until the router assumes there are no longer any MLD version-1 Hosts on the specified interface.

Group Compat Mode: The compatibility mode of the multicast group on this interface. The values it can take are *MLDv1* and MLDv2

9.3.1.2 show ipv6 mld interface [<slot/port>]

Use this command to display MLD-related information for the interface.

Syntax
show ipv6 mld interface [<slot/port>]

Default Setting

None

Command Mode

Privileged Exec

Display Message

The following information is displayed for each of the interfaces or for only the specified interface.

Interface: The interface number in unit/slot/port format.

MLD Mode: Displays the configured administrative status of MLD.

Operational Mode: The operational status of MLD on the interface.

MLD Version: Indicates the version of MLD configured on the interface.

Query Interval: Indicates the configured query interval for the interface.

Query Max Response Time: Indicates the configured maximum query response time (in seconds) advertised in MLD queries on this interface.

Robustness: Displays the configured value for the tuning for the expected packet loss on a subnet attached to the interface.

Startup Query interval: This valued indicates the configured interval between General Queries sent by a Querier on startup.

Startup Query Count: This value indicates the configured number of Queries sent out on startup, separated by the Startup Query Interval.

Last Member Query Interval: This value indicates the configured Maximum Response Time inserted into Group-Specific Queries sent in response to Leave Group messages.

Last Member Query Count: This value indicates the configured number of Group-Specific Queries sent before the router assumes that there are no local members.

The following information is displayed if the operational mode of the MLD interface is enabled.

Querier Status: This value indicates whether the interface is an MLD querier or non-querier on the subnet it is associated with.

Querier Address: The IP address of the MLD querier on the subnet the interface is associated with.

Querier Up Time: Time elapsed in seconds since the querier state has been updated.

Querier Expiry Time: Time left in seconds before the Querier loses its title as querier.

Wrong Version Queries: Indicates the number of queries received whose MLD version does not match the MLD version of the interface.

Number of Joins: The number of times a group membership has been added on this interface.

Number of Leaves: The number of times a group membership has been removed on this interface.

Number of Groups: The current number of membership entries for this interface.

9.3.1.3 show ipv6 mld traffic

Use this command to display MLD statistical information for the router.

Syntax
show ipv6 mld traffic

Default Setting

None

Command Mode

Privileged Exec

Display Message

Valid MLD Packets Received: The number of valid MLD packets received by the router.

Valid MLD Packets Sent: The number of valid MLD packets sent by the router.

Queries Received: The number of valid MLD queries received by the router.

Queries Sent: The number of valid MLD queries sent by the router.

Reports Received: The number of valid MLD reports received by the router.

Reports Sent: The number of valid MLD reports sent by the router.

Leaves Received: The number of valid MLD leaves received by the router.

Leaves Sent: The number of valid MLD leaves sent by the router.

Bad Checksum MLD Packets: The number of bad checksum MLD packets received by the router.

Malformed MLD Packets: The number of malformed MLD packets received by the router.

9.3.2 Configuration Commands

9.3.2.1 ipv6 mld query-interval

Use this command to set the MLD router's query interval for the interface. The query-interval is the amount of time between the general queries sent when the router is the querier on that interface. The range for <*query-interval*> is 1 to 3600 seconds.

Syntax
ipv6 mld query-interval <1-3600> no ipv6 mld query-interval

no – Use this command to reset the MLD query interval to the default value for that interface.

Default Setting

125

Command Mode

Interface Config

9.3.2.2 ipv6 mld query-max-response-time

Use this command to set the MLD querier's maximum response time for the interface and this value is used in assigning the maximum response time in the query messages that are sent on that interface. The range for <*query-max-responsetime*> is 0 to 65535 milliseconds.

Syntax
ipv6 mld query-max-response-time <1-65535> no ipv6 mld query-max-response-time

no - This command resets the MLD query max response time for the interface to the default value.

Default Setting

1000 milliseconds

Command Mode

Interface Config

9.3.2.3 ipv6 mld last-member-query-interval

Use this command to set the last member query interval for the MLD interface, which is the value of the maximum response time parameter in the group specific queries sent out of this interface. The range for <*last-member-query-interval*> is 0 to 65535 milliseconds.

Syntax

```
ipv6 mld last-member-query-interval <1-65535>
no ipv6 mld last-member-query-interval
```

no - Use this command to reset the <*last-member-query-interval*> parameter of the interface to the default value.

Default Setting

1000 milliseconds

Command Mode

Interface Config

9.3.2.4 ipv6 mld last-member-query- count

Use this command to set the number of listener-specific queries sent before the router assumes that there are no local members on the interface. The range for <*last-member-query-count*> is 1 to 20.

Syntax

```
ipv6 mld last-member-query-count <1-20>
no ipv6 mld last-member-query-count
```

no - Use this command to reset the <*last-member-query-count*> parameter of the interface to the default value.

Default Setting

2

Command Mode

Interface Config

9.3.2.5 ipv6 mld router

Use this command, in the administrative mode of the router, to enable MLD in the router.

Syntax

```
ipv6 mld router
no ipv6 mld router
```

Default Setting

Disabled

Command Mode

Global Config

Interface Config

9.3.2.6 clear ipv6 mld counters

The user can go to the CLI Privilege Configuration Mode to clear MLD counters on the system, use the **clear ipv6 mld counters [<slot/port>]** priviledge configuration command.

Syntax

```
clear ipv6 mld counters [<slot/port>]
```

Default Setting

None

Command Mode

Privilege Exec

9.3.2.7 clear ipv6 mld traffic

The user can go to the CLI Privilege Configuration Mode to clear MLD traffec on the system, use the **clear ipv6 mld traffic** priviledge configuration command.

Syntax

```
clear ipv6 mld traffic
```

Default Setting

None

Command Mode

Privilege Exec

9.3.2.8 ipv6 mld version

This command configures the version of MLD for an interface.

Syntax

```
ipv6 mld version {1 | 2}
no ipv6 mld version
```

<1- 2> - The mld version number.

no - This command resets the version of MLD for this interface. The version is reset to the default value.

Default Setting

2

Command Mode

Interface Config

9.4 Multicast Commands

9.4.1 Show Commands

9.4.1.1 show ip mcast

This command displays the system-wide multicast information

Syntax

```
show ip mcast
```

Default Setting

None

Command Mode

Privileged Exec

User Exec

Display Message

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.

Protocol: This field displays the multicast protocol running on the router. Possible values are PIMDM, PIMSM, or DVMRP.

Forwarding Multicast Stream Entry Count: This field displays the number of entries in the multicast table.

9.4.1.2 show ip mcast boundary

This command displays all the configured administrative scoped multicast boundaries.

Syntax
show ip mcast boundary {<slot/port> | all}

<slot/port > - Interface number.

all - This command represents all interfaces.

Default Setting

None

Command Mode

Privileged Exec

User Exec

Display Message

Interface: Valid slot and port number separated by forward slashes.

Group IP: The group IP address.

Mask: The group IP mask.

9.4.1.3 show ip mcast interface

This command displays the multicast information for the specified interface.

Syntax

```
show ip mcast interface <slot/port>
```

<slot/port > - Interface number.

Default Setting

None

Command Mode

Privileged Exec

User Exec

Display Message

Interface: Valid slot and port number separated by forward slashes.

TTL: This field displays the time-to-live value for this interface.

9.4.1.4 show ip mcast mroute

This command displays a summary or all the details of the multicast table.

Syntax

```
show ip mcast mroute {detail | summary}
```

detail - displays the multicast routing table details.

summary - displays the multicast routing table summary.

Default Setting

None

Command Mode

Privileged Exec

User Exec

Display Message

If the "**detail**" parameter is specified, the following fields are displayed:

Source IP: This field displays the IP address of the multicast data source.

Group IP: This field displays the IP address of the destination of the multicast packet.

Expiry Time (secs): This field displays the time of expiry of this entry in seconds.

Up Time (secs): 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: This field displays the IP address of the multicast data source.

Group IP: 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.

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>.

Syntax

show ip mcast mroute group <groupipaddr> {detail |summary}

< groupipaddr > - the IP Address of the destination of the multicast packet.

detail - Display the multicast routing table details.

summary - Display the multicast routing table summary.

Default Setting

None

Command Mode

Privileged Exec

User Exec

Display Message

If the **detail** parameter is specified the follow fields are displayed:

Source IP: This field displays the IP address of the multicast data source.

Group IP: This field displays the IP address of the destination of the multicast packet.

Expiry Time (secs): This field displays the time of expiry of this entry in seconds.

Up Time (secs): 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: This field displays the IP address of the multicast data source.

Group IP: 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.

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.

Syntax

show ip mcast mroute source <sourceipaddr> {summary | <groupipaddr>}

< sourceipaddr > - the IP Address of the multicast data source.

summary - display the multicast routing table summary

< groupipaddr > - the IP Address of the destination of the multicast packet.

Default Setting

None

Command Mode

Privileged Exec

User Exec

Display Message

If the **< groupipaddr >** parameter is specified the follow fields are displayed:

Source IP: This field displays the IP address of the multicast data source.

Group IP: This field displays the IP address of the destination of the multicast packet.

Expiry Time (secs): This field displays the time of expiry of this entry in seconds.

Up Time (secs): 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: This field displays the IP address of the multicast data source.

Group IP: 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 arrives.

Outgoing Interface List: This field displays the list of outgoing interfaces on which this packet is forwarded.

9.4.2 Configuration Commands

9.4.2.1 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.

Syntax

```
ip multicast
no ip multicast
```

no - 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.

Default Setting

Disbaled

Command Mode

Global Config

9.4.2.2 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.

Syntax

```
ip mcast boundary <groupipaddr> <mask>
no ip mcast boundary <groupipaddr> <mask>
```

<groupipaddr> - 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> - mask to be applied to the multicast group address.

no - 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.

Default Setting

None

Command Mode

Interface Config

9.4.2.3 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.

Syntax

```
ip multicast ttl-threshold <0 - 255>
no ip multicast ttl-threshold
```

<0 - 255> - the TTL threshold.

no - 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.

Default Setting

1

Command Mode

Interface Config

9.5 Protocol Independent Multicast – Dense Mode (PIM-DM) Commands

9.5.1 Show Commands

9.5.1.1 show ip pimdm

This command displays the system-wide information for PIM-DM.

Syntax

show ip pimdm

Default Setting

None

Command Mode

Privileged Exec

User Exec

Display Message

Admin Mode: This field indicates whether PIM-DM is enabled or disabled. This is a configured value.

Interface: Valid 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.

Operational State: This field indicates the current state of PIM-DM on this interface. Possible values are Operational or Non-Operational.

9.5.1.2 show ip pimdm interface

This command displays the interface information for PIM-DM on the specified interface.

Syntax

show ip pimdm interface <slot/port>

<slot/port > - Interface number.

Default Setting

None

Command Mode

Privileged Exec

User Exec

Display Message

Interface Mode: This field indicates whether PIM-DM is enabled or disabled on the specified interface. This is a configured value.

Hello Interval (secs): This field indicates the frequency at which PIM hello messages are transmitted on this interface. By default, the value is 30 seconds.

9.5.1.3 show ip pimdm interface stats

This command displays the statistical information for PIM-DM on the specified interface.

Syntax

show ip pimdm interface stats {<slot/port> | all}

<slot/port> - Interface number.

all - this command represents all interfaces.

Default Setting

None

Command Mode

Privileged Exec

User Exec

Display Message

Interface: Valid 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.

9.5.1.4 show ip pimdm neighbor

This command displays the neighbor information for PIM-DM on the specified interface.

Syntax

show ip pimdm neighbor [<slot/port> | all]

<slot/port> - Interface number.

all - this command represents all interfaces.

Default Setting

None

Command Mode

Privileged Exec

User Exec

Display Message

Neighbor Addr: This field displays the IP Address of the neighbor on an interface.

Interface: Valid 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.

9.5.2 Configuration Commands

9.5.2.1 ip pimdm

This command enables the administrative mode of PIM-DM in the router.

Syntax
ip pimdm no ip pimdm

no - This command disables the administrative mode of PIM-DM in the router. IGMP must be enabled before PIM-DM can be enabled.

Default Setting

Disabled

Command Mode

Global Config

9.5.2.2 ip pimdm

This command sets administrative mode of PIM-DM on an interface to enabled.

Syntax
ip pimdm no ip pimdm

no - This command sets administrative mode of PIM-DM on an interface to disabled.

Default Setting

Disabled

Command Mode

Interface Config

9.5.2.3 ip pimdm hello-interval

This command configures the transmission frequency of hello messages between PIM enabled neighbors. This field has a range of 10 to 3600 seconds.

Syntax

```
ip pimdm hello-interval <10 - 3600>
no ip pimdm hello-interval
```

<10 - 3600> - This is time interval in seconds.

no - This command resets the transmission frequency of hello messages between PIM enabled neighbors to the default value.

Default Setting

30

Command Mode

Interface Config

9.6 Protocol Independent Multicast – Sparse Mode (PIM-SM) Commands

9.6.1 Show Commands

9.6.1.1 show ip pimsm

This command displays the system-wide information for PIM-SM.

Syntax

```
show ip pimsm
```

Default Setting

None

Command Mode

Privileged Exec

User Exec

Display Message

Admin Mode: This field indicates whether PIM-SM is enabled or disabled. This is a configured value.

Data Threshold Rate (Kbps): This field shows the data threshold rate for the PIM-SM router. This is a configured value.

Register Threshold Rate (Kbps): This field indicates the threshold rate for the RP router to switch to the shortest path. This is a configured value.

Interface: Valid 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.

Operational State: This field indicates the current state of the PIM-SM protocol on the interface. Possible values are Operational or Non-Operational.

9.6.1.2 show ip pimsm bsr

This command displays displays the bootstrap router (BSR) information. The output includes elected BSR information and information about the locally configured candidate rendezvous point (RP) advertisement.

Syntax
show ip pimsm bsr

Default Setting

None

Command Mode

Privileged Exec

User Eexc

Display Message

BSR Address: IP address of the BSR.

Uptime: Length of time that this router has been up (in hours, minutes, and seconds).

BSR Priority: Priority as configured in the ip pimsm bsr-candidate command.

Hash Mask Length: Length of a mask (maximum 32 bits) that is to be ANDed with the group address before the hash function is called. This value is configured in the ip pimsm bsr-candidate command.

Next Bootstrap Message In: Time (in hours, minutes, and seconds) in which the next bootstrap message is due from this BSR.

Next Candidate RP advertisement in: Time (in hours, minutes, and seconds) in which the next candidate RP advertisement will be sent.

9.6.1.3 show ip pimsm interface

This command displays the interface information for PIM-SM on the specified interface.

Syntax

```
show ip pimsm interface <slot/port>
```

<slot/port> - Interface number.

Default Setting

None

Command Mode

Privileged Exec

User Exec

Display Message

Slot/Port: Valid 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.

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.

Join Prune Interval: This field indicates the join/prune interval for the PIM-SM router. The interval is in seconds.

Neighbor Count: This field indicates the neighbor count for the PIM-SM interface.

Designated Route: This field indicates the IP address of the Designated Router for this interface.

DR Priority: This field indicates the priority of the Designated Router.

BSR Border: This field indicates the bootstrap router border interface. Possible values are enabled or disabled.

9.6.1.4 show ip pimsm neighbor

This command displays the neighbor information for PIM-SM on the specified interface.

Syntax

```
show ip pimsm neighbor [<slot/port> | all]
```

<slot/port> - Interface number.

all - this command represents all interfaces.

Default Setting

None

Command Mode

Privileged Exec

User Exec

Display Message

Interface: Valid 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.

9.6.1.5 show ip pimsm rphash

This command displays which rendezvous point (RP) is being used for a specified group.

Syntax

show ip pimsm rphash <group-address>

<group-address> - the IP multicast group address.

Default Setting

None

Command Mode

Privileged Exec

User Exec

Display Message

RP: The IP address of the RP for the group specified.

Origin: Indicates the mechanism (BSR or static) by which the RP was selected.

9.6.1.6 show ip pimsm rp mapping

This command displays all group-to-RP mappings of which the router is a aware (either configured or learned from the bootstrap router (BSR)). If no RP is specified, all active RPs are displayed.

Syntax

show ip pimsm rp mapping [rp address]

Default Setting

None

Command Mode

Privileged Exec

User Exec

9.6.2 Configuration Commands

9.6.2.1 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.

Syntax

```
ip pimsm
no ip pimsm
```

no - 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.

Default Setting

Disbaled

Command Mode

Global Config

9.6.2.2 ip pimsm join-prune-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 0 to 18000.

Syntax

```
ip pimsm join-prune-interval <0 - 18000>
no ip pimsm join-prune-interval
```

<0 - 18000> - This is time interval in seconds.

no - This command is used to reset the global join/prune interval for PIM-SM router to the default value.

Default Setting

60

Command Mode

Interface Config

9.6.2.3 ip pimsm register-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 Kilobits per second. The possible values are 0 to 2000.

Syntax

```
ip pimsm register-threshold <0 - 2000>
no ip pimsm register-threshold
```

<0 - 2000> - This is kilobits per seconds.

no - This command is used to reset the Threshold rate for the RP router to switch to the shortest path to the default value.

Default Setting

0

Command Mode

Global Config

9.6.2.4 ip pimsm spt-threshold

This command is used to configure the Data Threshold rate for the last-hop router to switch to the shortest path. The rate is specified in Kilobits per second. The possible values are 1 to 2000.

Syntax

```
ip pimsm spt-threshold <1 - 2000>
no ip pimsm spt-threshold
```

<1 - 2000> - This is kilobits per seconds.

no - This command is used to reset the Data Threshold rate for the last-hop router to switch to the shortest path to the default value.

Default Setting

0

Command Mode

Global Config

9.6.2.5 ip pimsm rp-address

This command is used to create RP IP address for the PIM-SM router. The parameter <rp-address> is the IP address of the RP. The parameter <group-address> is the group address supported by the RP. The parameter <group-mask> is the group mask for the group address. The optional keyword override indicates that if there is a conflict, the RP configured with this command prevails over the RP learned by BSR.

Syntax

```
ip pimsm rp-address <rp-address> <group-address> <group-mask> [override]
no ip pimsm rp-address <rp-address> <group-address> <group-mask>
```

<rp-address> - the IP Address of the RP.

<group-address> - the group address supported by the RP.

<group-mask> - the group mask for the group address.

no - This command is used to delete RP IP address for the PIM-SM router. The parameter <rp-address> is the IP address of the RP. The parameter <group-address> is the group address supported by the RP. The parameter <group-mask> is the group mask for the group address.

Default Setting

None

Command Mode

Global Config

9.6.2.6 ip pimsm

This command sets administrative mode of PIM-SM multicast routing on a routing interface to enable.

Syntax

```
ip pimsm
no ip pimsm
```

no - This command sets administrative mode of PIM-SM multicast routing on a routing interface to disabled.

Default Setting

Disbaled

Command Mode

Interface Config

9.6.2.7 ip pimsm hello-interval

This command configures the transmission frequency of hello messages in seconds between PIM enabled neighbors. This field has a range of 0 to 18000 seconds.

Syntax

```
ip pimsm query-interval <0 - 18000>
no ip pimsm query-interval
```

<0 - 18000> - This is time interval in seconds.

no - This command resets the transmission frequency of hello messages between PIM enabled neighbors to the default value.

Default Setting

30

Command Mode

Interface Config

9.6.2.8 ip pimsm bsr-border

This command is used to prevent bootstrap router (BSR) messages from being sent or received through an interface.

Syntax

```
ip pimsm bsr-border
no ip pimsm bsr-border
```

no - This command is used to disable the interface from being the BSR border.

Default Setting

Disabled

Command Mode

Interface Config

9.6.2.9 ip pimsm dr-priority

This command is used to set the priority value for which a router is elected as the designated router (DR).

Syntax

```
ip pimsm dr-priority <0-2147483647>
no ip pimsm dr-priority
```

no - This command is used to reset the priority to default value.

Default Setting

1

Command Mode

Interface Config

9.6.2.10 ip pimsm bsr-candidate

This command is used to configure the router to announce its candidacy as a bootstrap router (BSR).

Syntax

```
ip pimsm bsr-candidate interface <slot/port> [hash-mask-length] [priority]
no ip pimsm bsr-candidate interface <slot/port> [hash-mask-length] [priority]
```

hash-mask-length - Length of a mask (32 bits maximum) that is to be ANDed with the group address before the hash function is called. All groups with the same seed hash correspond to the same RP. For example, if this value was 24, only the first 24 bits of the group addresses matter. This allows you to get one RP for multiple groups.

priority - Priority of the candidate BSR. The range is an integer from 0 to 255. The BSR with the larger priority is preferred. If the priority values are the same, the router with the larger IP address is the BSR. The default value is 0.

no - This command is used to disable the router to announce its candidacy as a bootstrap router (BSR).

Default Setting

None

Command Mode

Global Config

9.6.2.11 ip pimsm rp-candidate

This command is used to configure the router to advertise itself as a PIM candidate rendezvous point (RP) to the bootstrap router (BSR).

Syntax

ip pimsm rp-candidate interface <*slot/port*> <*group-address*> <*group-mask*> no ip pimsm rp-candidate interface <*slot/port*> <*group-address*> <*group-mask*>

no - This command is used to disable the router to advertise itself as a PIM candidate rendezvous point (RP) to the bootstrap router (BSR).

Default Setting

None

Command Mode

Global Config

9.6.2.12 ip pimsm ssm default

Use this command to define the Source Specific Multicast (SSM) range of IP multicast addresses.

Syntax

ip pimsm ssm *{default* | <*group-address*> <*group-mask*>*}* no ip pimsm ssm

no - This command is used to disable the Source Specific Multicast (SSM) range.

Default Setting

Disabled

Command Mode

Global Config

9.7 IGMP Proxy Commands

The IGMP Proxy is used by IGMP Router (IPv4 system) to enable the system to issue IGMP host messages on behalf of hosts that the system discovered through standard IGMP router interfaces. With IGMP Proxy enabled, the system acts as proxy to all the hosts residing on its router interfaces.

9.7.1 Show Commands

9.7.1.1 show ip igmp-proxy

This command displays a summary of the host interface status parameters. It displays the following parameters only when you enable IGMP Proxy.

Syntax

show ip igmp-proxy

Default Setting

None

Command Mode

Privileged Exec

User Exec

Display Message

Interface index: The interface number of the IGMP Proxy.

Admin Mode: States whether the IGMP Proxy is enabled or not. This is a configured value.

Operational Mode: States whether the IGMP Proxy is operationally enabled or not. This is a status parameter.

Version: The present IGMP host version that is operational on the proxy interface.

Number of Multicast Groups: States the number of multicast groups that are associated with the IGMP Proxy interface.

Unsolicited Report Interval: The time interval at which the IGMP Proxy interface sends unsolicited group membership report.

Querier IP Address on Proxy Interface: The IP address of the Querier, if any, in the network attached to the upstream interface (IGMP-Proxy interface).

Older Version 1 Querier Timeout: The interval used to timeout the older version 1 queriers.

Older Version 2 Querier Timeout: The interval used to timeout the older version 2 queriers.

Proxy Start Frequency: The number of times the IGMP Proxy has been stopped and started.

9.7.1.2 show ip igmp-proxy groups

This command displays information about the subscribed multicast groups that IGMP Proxy reported. It displays a table of entries with the following as the fields of each column.

Syntax

show ip igmp-proxy groups

Default Setting

None

Command Mode

Privileged Exec

User Exec

Display Message

Interface: The interface number of the IGMP Proxy.

Group Address: The IP address of the multicast group.

Last Reporter: The IP address of host that last sent a membership report.

Up Time (in secs): The time elapsed since last created.

Member State: The status of the entry. Possible values are IDLE_MEMBER or DELAY_MEMBER.

- **IDLE_MEMBER** - interface has responded to the latest group membership query for this group.
- **DELAY_MEMBER** - interface is going to send a group membership report to respond to a group membership query for this group.

Filter Mode: Possible values are Include or Exclude.

Sources: The number of sources attached to the multicast group.

9.7.1.3 show ip igmp-proxy groups detail

This command displays complete information about multicast groups that IGMP Proxy reported. It displays a table of entries with the following as the fields of each column.

Syntax
show ip igmp-proxy groups detail

Default Setting

None

Command Mode

Privileged Exec

User Exec

Display Message

Interface: The interface number of the IGMP Proxy.

Group Address: The IP address of the multicast group.

Last Reporter: The IP address of host that last sent a membership report for the current

group, on the network attached to the IGMP-Proxy interface (upstream interface).

Up Time (in secs): The time elapsed since last created.

Member State: The status of the entry. Possible values are IDLE_MEMBER or DELAY_MEMBER.

- **IDLE_MEMBER** - interface has responded to the latest group membership query for this group.
- **DELAY_MEMBER** - interface is going to send a group membership report to respond to a group membership query for this group.

Filter Mode: Possible values are include or exclude.

Sources: The number of sources attached to the multicast group.

Group Source List: The list of IP addresses of the sources attached to the multicast group.

Expiry Time: Time left before a source is deleted.

9.7.1.4 show ip igmp-proxy interface

This command displays a detailed list of the host interface status parameters. It displays the following parameters only when you enable IGMP Proxy.

Syntax

```
show ip igmp-proxy interface
```

Default Setting

None

Command Mode

Privileged Exec

User Exec

Display Message

Interface Index: Shows the slot/port of the IGMP proxy.

The column headings of the table associated with the interface are as follows:

Ver: Shows the IGMP version.

Query Rcvd: Number of IGMP queries received.

Report Rcvd: Number of IGMP reports received.

Report Sent: Number of IGMP reports sent.

Leaves Rcvd: Number of IGMP leaves received.

Leaves Sent: Number of IGMP leaves sent.

9.7.2 Configuration Commands

9.7.2.1 ip igmp-proxy

This command enables the IGMP Proxy on the router. To enable the IGMP Proxy on the router, you must enable multicast forwarding. Also, make sure that there are no multicast routing protocols enabled on the router.

Syntax

```
ip igmp-proxy
no ip igmp-proxy
```

no - This command disables the IGMP Proxy on the router.

Default Setting

Disabled

Command Mode

Interface Config

9.7.2.2 ip igmp-proxy reset-status

This command resets the host interface status parameters of the IGMP Proxy router. This command is valid only when you enable IGMP Proxy on the interface.

Syntax

```
ip igmp-proxy reset-status
```

Default Setting

None

Command Mode

Interface Config

9.7.2.3 ip igmp-proxy unsolicit-rprt-interval

This command sets the unsolicited report interval for the IGMP Proxy router. This command is valid only when you enable IGMP Proxy on the interface. The value of <interval> can be 1-260 seconds.

Syntax

```
ip igmp-proxy unsolicit-rprt-interval <1-260>
no ip igmp-proxy unsolicit-rprt-interval
```

no - This command resets the unsolicited report interval of the IGMP Proxy router to the default value.

Default Setting

None

Command Mode

Interface Config

9.8 MLD Proxy Commands

MLD-Proxy is the IPv6 equivalent of IGMP-Proxy. MLD-Proxy commands allow you to configure the network device as well as to view device settings and statistics using either serial interface or telnet session. The operation of MLD-Proxy commands is the same as for IGMP-Proxy: MLD is for IPv6 and IGMP is for IPv4.MGMD is a term used to refer to both IGMP and MLD.

9.8.1 Show Commands

9.8.1.1 show ipv6 mld-proxy

This command displays a summary of the host interface status parameters.

Syntax
show ipv6 mld-proxy

Default Setting

None

Command Mode

Privileged Exec

User Exec

Display Message

Interface index: The interface number of the MLD-Proxy.

Admin Mode: States whether the MLD-Proxy is enabled or not. This is a configured value.

Operational Mode: States whether the MLD-Proxy is operationally enabled or not. This is a status parameter.

Version: The present MLD host version that is operational on the proxy interface.

Number of Multicast Groups: States the number of multicast groups that are associated with the MLD-Proxy interface.

Unsolicited Report Interval: The time interval at which the MLD-Proxy interface sends unsolicited group membership report.

Querier IP Address on Proxy Interface: The IP address of the Querier, if any, in the network attached to the upstream interface (MLD-Proxy interface).

Older Version 1 Querier Timeout: The interval used to timeout the older version 1 queriers.

Proxy Start Frequency: The number of times the MLD-Proxy has been stopped and started.

9.8.1.2 show ipv mld-proxy groups

This command displays information about multicast groups that the MLD-Proxy reported.

Syntax

show ipv6 mld-proxy groups

Default Setting

None

Command Mode

Privileged Exec

User Exec

Display Message

Interface: The interface number of the MLD-Proxy.

Group Address: The IP address of the multicast group.

Last Reporter: The IP address of the host that last sent a membership report for the current group, on the network attached to the MLD-Proxy interface (upstream interface).

Up Time (in secs): The time elapsed since last created.

Member State: Possible values are:

- **Idle_Member** - interface has responded to the latest group membership query for this group.
- **Delay_Member** - interface is going to send a group membership report to respond to a group membership query for this group.

Filter Mode: Possible values are Include or Exclude.

Sources: The number of sources attached to the multicast group.

9.8.1.3 show ipv6 mld-proxy groups detail

This command displays information about multicast groups that MLD-Proxy reported.

Syntax

show ipv6 mld-proxy groups detail

Default Setting

None

Command Mode

Privileged Exec

User Exec

Display Message

Interface: The interface number of the MLD-Proxy.

Group Address: The IP address of the multicast group.

Last Reporter: The IP address of host that last sent a membership report for the current

group, on the network attached to the MLD-Proxy interface (upstream interface).

Up Time (in secs): The time elapsed since last created.

Member State: Possible values are:

- **Idle_Member** - interface has responded to the latest group membership query for this group.
- **Delay_Member** - interface is going to send a group membership report to respond to a group membership query for this group.

Filter Mode: Possible values are include or exclude.

Sources: The number of sources attached to the multicast group.

Group Source List: The list of IP addresses of the sources attached to the multicast group.

Expiry Time: Time left before a source is deleted.

9.8.1.4 show ipv6 mld-proxy interface

This command displays a detailed list of the host interface status parameters. It displays the following parameters only when you enable MLD-Proxy.

Syntax

show ipv6 mld-proxy interface

Default Setting

None

Command Mode

Privileged Exec

User Exec

Display Message

Interface Index: Shows the slot/port of the MLD-proxy.

The column headings of the table associated with the interface are as follows:

Ver: Shows the MLD version.

Query Rcvd: Number of MLD queries received.

Report Rcvd: Number of MLD reports received.

Report Sent: Number of MLD reports sent.

Leaves Rcvd: Number of MLD leaves received. Valid for version 2 only.

Leaves Sent: Number of MLD leaves sent on the Proxy interface. Valid for version 2 only.

9.8.2 Configuration Commands

9.8.2.1 ipv6 mld-proxy

This command enables MLD-Proxy on the router. To enable MLD-Proxy on the router, you must enable multicast forwarding. Also, make sure that there are no other multicast routing protocols enabled n the router.

Syntax

```
ipv6 mld-proxy
no ipv6 mld-proxy
```

no - This command disables the MLD-Proxy on the router.

Default Setting

Disabled

Command Mode

Interface Config

9.8.2.2 ipv6 mld-proxy reset-status

This command resets reset the host interface status parameters of the MLD-Proxy router. This command is only valid when you enable MLD-Proxy on the interface.

Syntax

```
ipv6 mld-proxy reset-status
```

Default Setting

None

Command Mode

Interface Config

9.8.2.3 ipv6 mld-proxy unsolicit-rprt-interval

This command sets the unsolicited report interval for the MLD-Proxy router. This command is only valid when you enable MLD-Proxy on the interface. The value of <interval> is 1-260 seconds.

Syntax

```
ipv6 mld-proxy unsolicit-rprt-interval <1-260>
```

```
no ipv6 mld-proxy unsolicit-rprt-interval
```

no - This command resets the unsolicited report interval of the MLD-Proxy router to the default value.

Default Setting

None

Command Mode

Interface Config

10. IPv6 Commands

10.1 Tunnel Interface Commands

The commands in this section describe how to create, delete, and manage tunnel interfaces.Several different types of tunnels provide functionality to facilitate the transition of IPv4 networks to IPv6 networks. These tunnels are divided into two classes: configured and automatic. The distinction is that configured tunnels are explicitly configured with a destination or endpoint of the tunnel. Automatic tunnels, in contrast, infer the endpoint of the tunnel from the destination address of packets routed into the tunnel. To assign an IP address to the tunnel interface, please refer to “ip address” command. To assign an IPv6 address to the tunnel interface, please refer to “ipv6 address” command.

10.1.1 Show Commands

10.1.1.1 show interface tunnel

This command displays the parameters related to tunnel such as tunnel mode, tunnel source address and tunnel destination address.

Syntax
show interface tunnel [<0-7>]

Default Setting

None

Command Mode

Privileged Exec

Display Message

If you do not specify a tunnel ID, the command shows the following information for each configured tunnel:

Tunnel ID: Shows the tunnel identification number.

Interface: Shows the name of the tunnel interface.

Tunnel Mode: Shows the tunnel mode.

Source Address: Shows the source transport address of the tunnel.

Destination Address: Shows the destination transport address of the tunnel.

If you specify a tunnel ID, the command shows the following information for the tunnel:

Interface Link Status: Shows whether the link is up or down.

MTU Size: Shows the maximum transmission unit for packets on the interface.

IPv6 Address/Length: If you enable IPv6 on the interface and assign an address, the IPv6

address and prefix display.

10.1.2 Configuration Commands

10.1.2.1 interface tunnel

This command uses to enter the Interface Config mode for a tunnel interface. The <tunnel-id> range is 0 to 7.

Syntax

```
interface tunnel <0-7>
no interface tunnel <0-7>
```

no - This command removes the tunnel interface and associated configuration parameters for the specified tunnel interface.

Default Setting

None

Command Mode

Global Config

10.1.2.2 tunnel source

This command specifies the source transport address of the tunnel, either explicitly or by reference to an interface.

Syntax

```
tunnel source {<ipv4-address> | <ethernet> <slot/port>}
```

<slot/port> - The Interface number.

<ipv4-address> - A valid IP Address.

Default Setting

None

Command Mode

Interfacel Tunnel Mode

10.1.2.3 tunnel destination

This command specifies the destination transport address of the tunnel.

Syntax

tunnel destination {<ipv4-address>}

<ipv4-address> - A valid IP Address.

Default Setting

None

Command Mode

Interfacel Tunnel Mode

10.1.2.4 tunnel mode ipv6ip

This command specifies the mode of the tunnel. With the optional 6to4 argument, the tunnel mode is set to 6to4 automatic. Without the optional 6to4 argument, the tunnel mode is configured.

Syntax

tunnel mode ipv6ip [6to4]

Default Setting

None

Command Mode

Interfacel Tunnel Mode

10.2 Loopback Interface Commands

The commands in this section describe how to create, delete, and manage loopback interfaces. A loopback interface is always expected to be up. This interface can provide the source address for sent packets and can receive both local and remote packets. The loopback interface is typically used by routing protocols. To assign an IP address to the loopback interface, please refer to “ip address” command. To assign an IPv6 address to the loopback interface, please refer to “ipv6 address” command.

10.2.1 Show Commands

10.2.1.1 show interface loopback

This command displays information about configured loopback interfaces.

Syntax

show interface loopback [<0-7>]

Default Setting

None

Command Mode

Privileged Exec

Display Message

If you do not specify a loopback ID, the following information appears for each loopback interface on the system:

Loopback ID: Shows the loopback ID associated with the rest of the information in the row.

Interface: Shows the interface name.

IP Address: Shows the IPv4 address of the interface

Received Packets: Shows the number of packets received on this interface.

Sent Packets: Shows the number of packets transmitted from this interface.

IPv6 Address: Shows the IPv6 address of this interface

If you specify a loopback ID, the following information appears:

Interface Link Status: Shows whether the link is up or down.

IP Address: Shows the IPv4 address of the interface.

IPv6 is enabled (disabled): Show whether IPv6 is enabled on the interface

IPv6 Address/Length: Shows the IPv6 address of the interface.

MTU size: Shows the maximum transmission size for packets on this interface, in bytes.

10.2.2 Configuration Commands

10.2.2.1 interface loopback

This command uses to enter the Interface Config mode for a loopback interface. The range of the loopback ID is 0 to 7.

Syntax

```
interface loopback <0-7>
no interface loopback <0-7>
```

no - This command removes the loopback interface and associated configuration parameters for the specified loopback interface.

Default Setting

Disabled

Command Mode

Global Config

10.3 IPv6 Routing Commands

This section describes the IPv6 commands you use to configure IPv6 on the system and on the interfaces. This section also describes IPv6 management commands and show commands.

10.3.1 Show Commands

10.3.1.1 show ipv6 brief

This command displays the IPv6 status of forwarding mode and IPv6 unicast routing mode.

Syntax

```
show ipv6 brief
```

Default Setting

None

Command Mode

Privileged Exec

User Exec

Display Message

IPv6 Forwarding Mode: Shows whether the IPv6 forwarding mode is enabled.

IPv6 Unicast Routing Mode: Shows whether the IPv6 unicast routing mode is enabled.

IPv6 Hop Limit Shows the unicast hop count used in IPv6 packets originated by the node. For more information, see “ipv6 hot-limit”

ICMPv6 Rate Limit Error Interval Shows how often the token bucket is initialized with burst-size tokens. For more information, see “ipv6 icmp error-interval”

ICMPv6 Rate Limit Burst Size Shows the number of ICMPv6 error messages that can be sent during one burst-interval. For more information, see “ipv6 icmp error-interval”

Maximum Routes Shows the maximum IPv6 route table size.

10.3.1.2 show ipv6 interface port

This command displays the usability status of IPv6 interfaces.

Syntax

show ipv6 interface [{ brief | port <slot/port> [prefix]}]

<slot/port> - Valid slot and port number separated by forward slashes.

Default Setting

None

Command Mode

Privileged Exec

User Exec

Display Message

If you use the brief parameter, the following information displays for all configured IPv6 interfaces:

Interface: Shows the interface in slot/port format.

IPv6 Routing Operational Mode: Shows whether the mode is enabled or disabled.

IPv6 Address/Length: Shows the IPv6 address and length on interfaces with IPv6 enabled.

If you specify an interface, the following information also appears.

Routing Mode: Shows whether IPv6 routing is enabled or disabled.

Administrative Mode: Shows whether the interface administrative mode is enabled or disabled.

IPv6 Implicit Mode: Shows IPv6 implicit mode is enabled or disabled.

IPv6 Routing Operational Mode: Shows whether the operational state of an interface is enabled or disabled.

Bandwidth: Shows the bandwidth of the interface.

Interface Maximum Transmission Unit: Shows the MTU size, in bytes.

Router Duplicate Address Detection Transmits: Shows the number of consecutive duplicate address detection probes to transmit.

Router Advertisement NS Interval: Shows the interval, in milliseconds, between router advertisements for advertised neighbor solicitations.

Router Lifetime Interval: Shows the router lifetime value of the interface in router advertisements

Router Advertisement Reachable Time: Shows the amount of time, in milliseconds, to consider a neighbor reachable after neighbor discovery confirmation.

Router Advertisement Interval: Shows the frequency, in seconds, that router advertisements are sent.

Router Advertisement Managed Config Flag: Shows whether the managed configuration flag is set (enabled) for router advertisements on this interface.

Router Advertisement Other Config Flag: Shows whether the other configuration flag is set (enabled) for router advertisements on this interface.

Router Advertisement Suppress Flag: Shows whether router advertisements are suppressed (enabled) or sent (disabled).

IPv6 Destination Unreachables: Shows whether ICMPv6 Destination Unreachable messages may be sent (enabled) or not (disabled).

If an IPv6 prefix is configured on the interface, the following information also appears.

IPv6 Prefix: Shows the IPv6 prefix for the specified interface.

Preferred Lifetime: Shows the amount of time the advertised prefix is a preferred prefix.

Valid Lifetime: Shows the amount of time the advertised prefix is valid.

Onlink Flag: Shows whether the onlink flag is set (enabled) in the prefix.

Autonomous Flag: Shows whether the autonomous address-configuration flag (autoconfig) is set (enabled) in the prefix.

10.3.1.3 show ipv6 interface neighbors

This command displays information about the IPv6 neighbors.

Syntax
show ipv6 interface neighbors

Default Setting

None

Command Mode

Privileged Exec

Display Message

Count of Learned Neighbors the number of neighbor mac address be learned.

Interface: Shows the interface in slot/port format.

IPv6 Address: IPV6 address of neighbor or interface.

MAC Address: Link-layer Address.

IsRtr: Shows whether the neighbor is a router. If the value is TRUE, the neighbor is known to be a router, and FALSE otherwise. A value of FALSE might not mean Note that routers are not always known to be routers.

Neighbor State: State of neighbor cache entry. Possible values are Incomplete, Reachable, Stale, Delay, Probe, and Unknown.

Age(Seconds): Shows the system uptime when the information for the neighbor was last updated.

10.3.1.4 show ipv6 interface neighbors static

This command display static neighbor cache table on the system each interface port.

Syntax

show ipv6 interface neighbors static

Default Setting

None

Command Mode

Privileged Exec

User Exec

Display Message

IPv6 Address: Specifies the IPv6 address of neighbor.

MAC Address: Specifies the MAC address of neighbor.

isRtr: Specifies the router flag.

Neighbor State: The state of the neighbor cache entry. Possible values are: Reachable, Delay.

Age Updated: The time in seconds that has elapsed since an entry was added to the cache.

10.3.1.5 show ipv6 ndp

This command displays NDP cache information for the management port.

Syntax

show ipv6 ndp

Default Setting

None

Command Mode

Privilege Exec

Display Message

IPv6 Address: The IPv6 address of the interface.

MAC Address: The MAC Address used.

isRtr: Specifies the router flag.

Neighbor State: The state of the neighbor cache entry. Possible values are: Reachable, Delay.

Age Updated: The time in seconds that has elapsed since an entry was added to the cache.

10.3.1.6 show ipv6 route

This command displays the IPv6 routing table The **<ipv6-address>** specifies a specific IPv6 address for which the best-matching route would be displayed. The **<ipv6-prefix/ipv6-prefix-length>** specifies a specific IPv6 network for which the matching route would be displayed. The **<interface>** specifies that the routes with next-hops on the **<interface>** be displayed. The **<protocol>** specifies the protocol that installed the routes. The **<protocol>** is one of the following keywords: **connected, ospf, static.** The all specifies that all routes including best and non-best routes are displayed. Otherwise, only the best routes are displayed.

If you use the connected keyword for **<protocol>,** the all option is not available because there are no best or non-best connected routes.

Syntax

show ipv6 route [{<ipv6-address> [<protocol>] | {{<ipv6-prefix/ipv6-prefix-length> | <slot/port>} [<protocol>] | <protocol> | summary} [all] | all}]

Default Setting

None

Command Mode

Privileged Exec

User Exec

Display Message

The **show ipv6 route** command displays the routing tables in the following format:

Codes: C - connected, S - static

O - OSPF Intra, OI - OSPF Inter, OE1 - OSPF Ext 1, OE2 - OSPF Ext 2

ON1 - OSPF NSSA Ext Type 1, ON2 - OSPF NSSA Ext Type 2

The columns for the routing table display the following information:

Code: The code for the routing protocol that created this routing entry.

IPv6-Prefix/IPv6-Prefix-Length: The IPv6-Prefix and prefix-length of the destination IPv6 network corresponding to this route.

Preference/Metric: The administrative distance (preference) and cost (metric) associated with this route. An example of this output is [1/0], where 1 is the preference and 0 is the metric.

Tag: Displays the decimal value of the tag associated with a redistributed route, if it is not 0.

Next-Hop: The outgoing router IPv6 address to use when forwarding traffic to the next router (if any) in the path toward the destination

Route-Timestamp: The last updated time for dynamic routes. The format of Route-Timestamp will be

- Days:Hours:Minutes if days > = 1
- Hours:Minutes:Seconds if days < 1

Interface: The outgoing router interface to use when forwarding traffic to the next destnation.

To administratively control the traffic destined to a particular network and prevent it from being forwarded through the router, you can configure a static reject route on the router. Such traffic would be discarded and the ICMP destination unreachable message is sent back to the source. This is typically used for preventing routing loops. The reject route added in the RTO is of the type OSPF Inter-Area. Reject routes (routes of REJECT type installed by any protocol) are not redistributed by OSPF/RIP. Reject routes are supported in both OSPFv2 and OSPFv3.

10.3.1.7 show ipv6 route preferences

This command displays the preference value associated with the type of route. Lower numbers have a greater preference. A route with a preference of 255 cannot be used to forward traffic.

Syntax
show ipv6 route preferences

Default Setting

None

Command Mode

Privileged Exec

Display Message

Local: Preference of directly-connected routes.

Static: Preference of static routes.

OSPF Intra: Preference of routes within the OSPF area.

OSPF Inter: Preference of routes to other OSPF routes that are outside of the area.

OSPF External: Preference of OSPF external routes.

10.3.1.8 show ipv6 route summary

This command displays the summary of the routing table. Use all to display the count summary for all routes, including best and non-best routes. Use the command without parameters to display the count summary for only the best routes.

Syntax

show ipv6 route summary [all]

Default Setting

None

Command Mode

Privileged Exec

Display Message

Connected Routes: Total number of connected routes in the routing table.

Static Routes: Shows whether the IPv6 unicast routing mode is enabled.

OSPF Routes: Total number of routes installed by OSPFv3 protocol.

Reject Routes : Total number of reject routes installed by all protocols.

Number of Prefixes: Summarizes the number of routes with prefixes of different lengths.

Total Routes: Shows the total number of routes in the routing table.

10.3.1.9 show ipv6 vlan

This command displays IPv6 VLAN routing interface addresses.

Syntax

show ipv6 vlan

Default Setting

None

Command Mode

Privileged Exec

Display Message

MAC Address used by Routing VLANs: Shows the MAC address.

The rest of the output for this command is displayed in a table with the following column headings:

VLAN ID: Shows the VLAN ID of a configured VLAN.

Logical Interface: Shows the interface in slot/port format that is associated with the VLAN ID.

IPv6 Address/Prefix Length: Shows the IPv6 prefix and prefix length associated with the VLAN ID.

10.3.1.10 show ipv6 traffic

This command displays traffic and statistics for IPv6 and ICMPv6. Specify a logical, loopback, or tunnel interface to view information about traffic on a specific interface. If you do not specify an interface, the command displays information about traffic on all interfaces.

Syntax

show ipv6 traffic [{<slot/port> | loopback <loopback-id> | tunnel <tunnel-id>}]

Default Setting

None

Command Mode

Privileged Exec

Display Message

Total Datagrams Received: Total number of input datagrams received by the interface, including those received in error.

Received Datagrams Locally Delivered: Total number of datagrams successfully delivered to IPv6 user-protocols (including ICMP). This counter increments at the interface to which these datagrams were addressed, which might not necessarily be the input interface for some of the datagrams.

Received Datagrams Discarded Due To Header Errors: Number of input datagrams discarded due to errors in their IPv6 headers, including version number mismatch, other format errors, hop count exceeded, errors discovered in processing their IPv6 options, etc.

Received Datagrams Discarded Due To MTU: Number of input datagrams that could not be forwarded because their size exceeded the link MTU of outgoing interface.

Received Datagrams Discarded Due To No Route: Number of input datagrams discarded because no route could be found to transmit them to their destination.

Received Datagrams With Unknown Protocol: Number of locally-addressed datagrams received successfully but discarded because of an unknown or unsupported protocol. This counter increments at the interface to which these datagrams were addressed, which might not be necessarily the input interface for some of the datagrams.

Received Datagrams Discarded Due To Invalid Address: Number of input datagrams discarded because the IPv6 address in their IPv6 header's destination field was not a valid address to be received at this entity. This count includes invalid addresses (for example, ::0) and unsupported addresses (for example, addresses with unallocated prefixes). Forentities which are not IPv6 routers and therefore do not forward datagrams, this counter includes datagrams discarded because the destination address was not a local address.

Received Datagrams Discarded Due To Truncated Data: Number of input datagrams discarded because datagram frame didn't carry enough data.

Received Datagrams Discarded Other: Number of input IPv6 datagrams for which no problems were encountered to prevent their continue processing, but which were discarded (e.g., for lack of buffer space). Note that this counter does not include datagrams discarded while awaiting re-assembly.

Received Datagrams Reassembly Required: Number of IPv6 fragments received which needed to be reassembled at this interface. Note that this counter increments at the interface to which these fragments were addressed, which might not be necessarily the input interface for some of the fragments.

Datagrams Successfully Reassembled: Number of IPv6 datagrams successfully reassembled. Note that this counter increments at the interface to which these datagrams were addressed, which might not be necessarily the input interface for some of the fragments.

Datagrams Failed To Reassemble: Number of failures detected by the IPv6 reassembly algorithm (for whatever reason: timed out, errors, etc.). Note that this is not necessarily a count of discarded IPv6 fragments since some algorithms (notably the algorithm in by combining them as they are received. This counter increments at the interface to which these fragments were addressed, which might not be necessarily the input interface for some of the fragments.

Datagrams Forwarded: Number of output datagrams which this entity received and forwarded to their final destinations. In entities which do not act as IPv6 routers, this counter will include only those packets which were Source-Routed via this entity, and the Source-Route processing was successful. Note that for a successfully forwarded datagram the counter of the outgoing interface increments.

Datagrams Locally Transmitted: Total number of IPv6 datagrams which local IPv6 user-protocols (including ICMP) supplied to IPv6 in requests for transmission. Note that this counter does not include any datagrams counted in ipv6IfStatsOutForwDatagrams.

Datagrams Transmit Failed: Number of output IPv6 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 ipv6IfStatsOutForwDatagrams if any such packets met this (discretionary) discard criterion.

Fragments Created: Number of output datagram fragments that have been generated as a result of fragmentation at this output interface.

Datagrams Successfully Fragmented: Number of IPv6 datagrams that have been successfully fragmented at this output interface.

Datagrams Failed To Fragment: Number of IPv6 datagrams that have been discarded because they needed to be fragmented at this output interface but could not be.

Multicast Datagrams Received: Number of multicast packets received by the interface.

Multicast Datagrams Transmitted: Number of multicast packets transmitted by the interface.

Total ICMPv6 messages received: Total number of ICMP messages received by the interface which includes all those counted by ipv6IfIcmpInErrors. Note that this interface is the interface to which the ICMP messages were addressed which may not be necessarily the input interface for the messages.

ICMPv6 Messages with errors: Number of ICMP messages which the interface received but determined as having ICMP-specific errors (bad ICMP checksums, bad length, etc.).

ICMPv6 Destination Unreachable Messages: Number of ICMP Destination Unreachable messages received by the interface.

ICMPv6 Messages Prohibited Administratively: Number of ICMP destination unreachable/communication administratively prohibited messages received by the interface.

ICMPv6 Time Exceeded Messages: Number of ICMP Time Exceeded messages received by the interface.

ICMPv6 Parameter Problem Messages: Number of ICMP Parameter Problem messages received by the interface.

ICMPv6 messages with too big packets: Number of ICMP Packet Too Big messages received by the interface.

ICMPv6 Echo Request Messages Received: Number of ICMP Echo (request) messages received by the interface.

ICMPv6 Echo Reply Messages Received: Number of ICMP Echo Reply messages received by the interface.

ICMPv6 Router Solicit Messages Received: Number of ICMP Router Solicit messages received by the interface.

ICMPv6 Router Advertisement Messages Received: Number of ICMP Router Advertisement messages received by the interface.

ICMPv6 Neighbor Solicit Messages Received: Number of ICMP Neighbor Solicit messages received by the interface.

ICMPv6 Neighbor Advertisement Messages Received: Number of ICMP Neighbor Advertisement messages received by the interface.

ICMPv6 Redirect Messages Received: Number of Redirect messages received by the interface.

Transmitted: Number of ICMPv6 Group Membership Query messages received by the interface.

Total ICMPv6 Messages Transmitted: Total number of ICMP messages which this interface attempted to send. Note that this counter includes all those counted by icmpOutErrors.

ICMPv6 Messages Not Transmitted Due To Error: Number of ICMP messages which this interface 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 IPv6 to route the resultant datagram. In some implementations there may be no types of error which contribute to this counter's value.

ICMPv6 Destination Unreachable Messages Transmitted: Number of ICMP Destination Unreachable messages sent by the interface.

ICMPv6 Messages Prohibited Administratively Transmitted: Number of ICMP destination unreachable/communication administratively prohibited messages sent.

ICMPv6 Time Exceeded Messages Transmitted: Number of ICMP Time Exceeded messages sent by the interface.

ICMPv6 Parameter Problem Messages Transmitted: Number of ICMP Parameter Problem messages sent by the interface.

ICMPv6 Packet Too Big Messages Transmitted: Number of ICMP Packet Too Big messages sent by the interface.

ICMPv6 Echo Request Messages Transmitted: Number of ICMP Echo (request) messages sent by the interface.ICMP echo messages sent.

ICMPv6 Echo Reply Messages Transmitted: Number of ICMP Echo Reply messages sent by the interface.

ICMPv6 Router Solicit Messages Transmitted: Number of ICMP Router Solicitation messages sent by the interface.

ICMPv6 Router Advertisement Messages Transmitted: Number of ICMP Router Advertisement messages sent by the interface.

ICMPv6 Neighbor Solicit Messages Transmitted: Number of ICMP Neighbor Solicitation messages sent by the interface.

ICMPv6 Neighbor Advertisement Messages Transmitted: Number of ICMP Neighbor Advertisement messages sent by the interface.

ICMPv6 Redirect Messages Received Number of Redirect messages sent. For a host, this object will always be zero, since hosts do not send redirects.

ICMPv6 Group Membership Query Messages Received: Number of ICMPv6 Group Membership Query messages sent.

ICMPv6 Group Membership Response Messages Receiveda: Number of ICMPv6 Group Membership Response messages sent.

ICMPv6 Group Membership Reduction Messages Receivedb: Number of ICMPv6 Group Membership Reduction messages sent.

ICMPv6 Duplicate Address Detects: Number of duplicate addresses detected by interface.

10.3.2 Configuration Commands

10.3.2.1 ipv6 forwarding

This command enables IPv6 forwarding on the switch.

Syntax

```
Ipv6 forwarding
no ipv6 forwarding
```

no - This command disables IPv6 forwarding on the switch.

Default Setting

Enabled

Command Mode

Global Config

10.3.2.2 ipv6 hop-limit

This command defines the unicast hop count used in ipv6 packets originated by the node. The value is also included in router advertisements. Valid values for <hops> are 1-64 inclusive. The default “not configured” means that a value of zero is sent in router advertisements and a value of 64 is sent in packets originated by the node. Note that this is not the same as configuring a value of 64.

Syntax

```
ipv6 hop-limit <hops>
no ipv6 hop-limit
```

no – Use this command to disable the forwarding of IPv6 hop-limit.

Default Setting

not configured

Command Mode

Global Config

10.3.2.3 ipv6 unicast-routing

Use this command to enable the forwarding of IPv6 unicast packets.

Syntax

```
ipv6 unicast-routing
no ipv6 unicast-routing
```

no – Use this command to disable the forwarding of IPv6 unicast packets.

Default Setting

Disabled

Command Mode

Global Config

10.3.2.4 ipv6 enable

Use this command to enable IPv6 routing on an interface, including a tunnel and loopback interface that has not been configured with an explicit IPv6 address. When you use this command, the interface is automatically configured with a link-local address. You do not need to use this command if you configured an IPv6 global address on the interface.

Syntax

```
ipv6 enable
no ipv6 enable
```

no – Use this command to disable IPv6 routing on an interface.

Default Setting

Disabled

Command Mode

Interface Config

Interface VLAN

10.3.2.5 ipv6 address

Use this command to configure an IPv6 address on an interface, including tunnel and loopback interfaces, and to enable IPv6 processing on this interface. You can assign multiple globally reachable addresses to an interface by using this command. You do not need to assign a linklocal address by using

this command since one is automatically created. The <prefix> field consists of the bits of the address to be configured. The <prefix_length> designates how many of the high-order contiguous bits of the address make up the prefix.

You can express IPv6 addresses in eight blocks. Also of note is that instead of a period, a colon now separates each block. For simplification, leading zeros of each 16 bit block can be omitted. One sequence of 16 bit blocks containing only zeros can be replaced with a double colon "::", but not more than one at a time (otherwise it is no longer a unique representation).

- **Dropping zeros:** 3ffe:ffff:100:f101:0:0:0:1 becomes 3ffe:ffff:100:f101::1
- **Local host**: 0000:0000:0000:0000:0000:0000:0000:0001 becomes ::1
- **Any host:** 0000:0000:0000:0000:0000:0000:0000:0000 becomes ::

The hexadecimal letters in the IPv6 addresses are not case-sensitive. An example of an IPv6 prefix and prefix length is 3ffe:1::1234/64.

The optional [eui-64] field designates that IPv6 processing on the interfaces was enabled using an EUI-64 interface ID in the low order 64 bits of the address. If you use this option, the value of <prefix_length> must be 64 bits.

Syntax

```
ipv6 address <prefix> / <prefix_length> [eui64]
no ipv6 address [<prefix> / <prefix_length>] [eui64]
```

<prefix> - parameter consists of the bits of the address to be configured.

<prefix_length> - It designates how many of the high-order contiguous bits of the address comprise the prefix.

[eui-64] – This field designates that IPv6 processing on the interfaces was enabled using an EUI-64 interface ID in the low order 64 bits of the address. If you do not supply any parameters, the command deletes all the IPv6 addresses on an interface.

no – Use this command to remove all IPv6 addresses on an interface or specified IPv6 address.

Default Setting

None

Command Mode

Interface Config

Interface VLAN

10.3.2.6 ipv6 gateway

Use this command to configure IPv6 gateway (i.e. default routers) information for the network port.

Syntax

```
ipv6 gateway <gateway-address>
no ipv6 gateway
```

<gateway-address> - Gateway address in IPv6 global or link-local address format.

no – Use this command remove IPv6 gateways on the network port interface.

Command Mode

Interface vlan

10.3.2.7 ipv6 route

Use this command to configure an IPv6 static route. The <ipv6-prefix> is the IPv6 network that is the destination of the static route. The <prefix_length> is the length of the IPv6 prefix — a decimal value (usually 0-64) that shows how many of the high-order contiguous bits of the address comprise the prefix (the network portion of the address). A slash mark must precede the <prefix_length>. The <next-hop-address> is the IPv6 address of the next hop that can be used to reach the specified network. The <preference> parameter is a value the router uses to compare this route with routes from other route sources that have the same destination. The range for <preference> is 1 - 255, and the default value is 1. The interface <slot/port> identifies direct static routes from point-to-point and broadcast interfaces, and must be specified when using a link-local address as the next hop. A route with a preference of 255 cannot be used to forward traffic.

Syntax

```
ipv6 route <ipv6-prefix>/<prefix_length> {<next-hop-address> [<preference>] | interface <slot/port>
<next-hop-address> [<preference>]}
no ipv6 route <ipv6-prefix>/<prefix_length> [{<next-hopaddress> | interface
<slot/port> <next-hop-address> | <preference>}]
```

no – Use this command to delete an IPv6 static route. Use the command without the optional parameters to delete all static routes to the specified destination. Use the <preference> parameter to revert preference of a route to default preference.

Default Setting

Disabled

Command Mode

Global Config

10.3.2.8 ipv6 route distance

This command sets the default distance (preference) for IPv6 static routes. Lower route distance values are preferred when determining the best route. The ipv6 route command allows you to optionally set the distance (preference) of an individual static route. The default distance is used when no distance is specified in this command.

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 ipv6 route distance command.

Syntax

```
ipv6 route distance <1-255>
no ipv6 route distance
```

no – This command resets the default static route preference value in the router to the original default preference. Lower routepreference values are preferred when determining the best route.

Default Setting

1

Command Mode

Global Config

10.3.2.9 ipv6 mtu

This command sets the maximum transmission unit (MTU) size, in bytes, of IPv6 packets on an interface. This command replaces the default or link MTU with a new MTU value.

Syntax

```
ipv6 mtu <1280-1500>
no ipv6 mtu
```

no – This command resets maximum transmission unit value to default value.

Default Setting

0 or link speed (MTU value is 1500)

Command Mode

Interface Config

10.3.2.10 ipv6 nd dad attempts

This command sets the number of duplicate address detection probes transmitted. Duplicate address detection verifies that an IPv6 address on an interface is unique.

Syntax

```
ipv6 nd dad attempts <0 – 600>
```

```
no ipv6 nd dad attempts
```

no – This command resets to number of duplicate address detection value to default value.

Default Setting

1

Command Mode

Interface Config

10.3.2.11 ipv6 nd managed-config-flag

This command sets the “managed address configuration” flag in router advertisements. When the value is true, end nodes use DHCPv6. When the value is false, end nodes automatically configure addresses.

Syntax

```
ipv6 nd managed-config-flag
no ipv6 nd managed-config-flag
```

no – This command resets the “managed address configuration” flag in router advertisements to the default value.

Default Setting

False

Command Mode

Interface Config

10.3.2.12 ipv6 nd ns-interval

This command sets the interval between router advertisements for advertised neighbor solicitations, in milliseconds. An advertised value of 0 means the interval is unspecified.

Syntax

```
ipv6 nd ns-interval { <1000 – 4294967295> | 0 }
no ipv6 nd ns-interval
```

no – This command resets the neighbor solicit retransmission interval of the specified interface to the default value.

Default Setting

0

Command Mode

Interface Config

10.3.2.13 ipv6 nd other-config-flag

This command sets the “other stateful configuration” flag in router advertisements sent from the interface.

Syntax

```
ipv6 nd other-config-flag
no ipv6 nd other-config-flag
```

no – This command resets the “other stateful configuration” flag back to its default value in router advertisements sent from the interface.

Default Setting

False

Command Mode

Interface Config

10.3.2.14 ipv6 nd ra-interval

This command sets the transmission interval between router advertisements.

Syntax

```
ipv6 nd ra-interval <4 – 1800 >
no ipv6 nd ra-interval
```

no – This command sets router advertisement interval to the default.

Default Setting

600

Command Mode

Interface Config

10.3.2.15 ipv6 nd ra-lifetime

This command sets the value, in seconds, that is placed in the Router Lifetime field of the router advertisements sent from the interface. The <lifetime> value must be zero, or it must be an integer between the value of the router advertisement transmission interval and 9000. A value of zero means this router is not to be used as the default router.

Syntax

```
ipv6 nd ra-lifetime <lifetime>
no ipv6 nd ra-lifetime
```

no – This command resets router lifetime to the default value.

Default Setting

1800

Command Mode

Interface Config

10.3.2.16 ipv6 nd reachable-time

This command sets the router advertisement time to consider a neighbor reachable after neighbor discovery confirmation. Reachable time is specified in milliseconds. A value of zero means the time is unspecified by the router.

Syntax

```
ipv6 nd reachable-time <0 - 4294967295>
no ipv6 nd reachable-time
```

no – This command means reachable time is unspecified for the router.

Default Setting

0

Command Mode

Interface Config

10.3.2.17 ipv6 nd suppress-ra

This command suppresses router advertisement transmission on an interface.

Syntax

```
ipv6 nd suppress-ra
no ipv6 nd suppress-ra
```

no –This command enables router transmission on an interface.

Default Setting

Disabled

Command Mode

Interface Config

10.3.2.18 ipv6 nd prefix

This command sets the IPv6 prefixes to include in the router advertisement. The first optional parameter is the valid lifetime of the router, in seconds. You can specify a value or indicate that the lifetime value is infinite. The second optional parameter is the preferred lifetime of the router.

Syntax

```
ipv6 nd prefix <prefix/prefix_length> [{<0-4294967295> | infinite}
{<0-4294967295> | infinite}] [no-autoconfig off-link]
no ipv6 nd prefix
```

no – This command sets prefix configuration to default values.

The router advertises its global IPv6 prefixes in its router advertisements (RAs). An RA only includes the prefixes of the IPv6 addresses configured on the interface where the RA is transmitted. Addresses are configured using the ipv6 address interface configuration command. Each prefix advertisement includes information about the prefix, such as its lifetime values and whether hosts should use the prefix for on-link determination or address auto-configuration. Use the ipv6 nd prefix command to configure these values.

The ipv6 nd prefix command allows you to preconfigure RA prefix values before you configure the associated interface address. In order for the prefix to be included in RAs, you must configure an address that matches the prefix using the ipv6 address command. Prefixes specified using ipv6 nd prefix without associated interface address will not be included in RAs and will not be committed to the device configuration.

Default Setting

Valid-lifetime – 604800

Preferred-lifetime – 2592000

Autoconfig – enabled

On-link - enabled

Command Mode

Interface Config

10.3.2.19 ipv6 unreachables

Use this command to enable the generation of ICMPv6 Destination Unreachable messages. By default, the generation of ICMPv6 Destination Unreachable messages is enabled.

Syntax

```
ipv6 unreachables
no ipv6 unreachables
```

no – This command prevent the generation of ICMPv6 Destination Unreachable messages.

Default Setting

Enabled

Command Mode

Interface Config

10.3.2.20 ipv6 icmp error-interval

Use this command to limit the rate at which ICMPv6 error messages are sent. The rate limit is configured as a token bucket, with two configurable parameters, burst-size and burst-interval.

Syntax

```
ipv6 icmp error-interval <burst-interval> [<burst-size>]
no ipv6 icmp error-interval
```

<burst-interval> - Specifies how often the token bucket is initialized with burst-size tokens. burst-interval is from 0 to 2147483647 milliseconds (msec).

<burst-size> - The number of ICMPv6 error messages that can be sent during one burst-interval. The range is from 1 to 200 messages. To disable ICMP rate limiting, set burst-interval to zero (0).

no – This command return burst-interval and burst-size to their default values.

Default Setting

burst-interval of 1000 msec.

burst-size of 100 messages

Command Mode

Global Config

10.3.2.21 ipv6 neighbors static

The user can add/delete a static neighbor into neighbor cache table.

Syntax

```
ipv6 neighbors static <ipv6-address> <mac-address>
no ipv6 neighbors static <ipv6-address>
```

<ipv6-address> - Enter the IPv6 Address.

<mac-address> - Enter the MAC Address.

no – This command sets IPv6 neighbor configuration to default values.

Default Setting

None

Command Mode

Global Config

10.4 OSPFv3 Commands

This section describes the commands you use to configure OSPFv3, which is a link-state routing protocol that you use to route traffic within a network.

10.4.1 Show Commands

10.4.1.1 show ipv6 ospf

This command displays information relevant to the OSPF router.

Syntax

```
show ipv6 ospf
```

Default Setting

None

Command Mode

Privileged Exec

Display Messages

NOTE: Some of the information below displays only if you enable OSPF and configure certain features.

Router ID: Is 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).

ABR Status: Shows whether the router is an OSPF Area Border Router.

Exit Overflow Interval: Shows the number of seconds that, after entering Overflow State, a router will attempt to leave Overflow State.

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, 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.

10.4.1.2 show ip ospf abr

This command displays the internal OSPFv3 routes to reach Area Border Routers (ABR).This command takes no options.

Syntax

```
show ipv6 ospf abr
```

Default Setting

None

Command Mode

Privileged Exec

User Exec

Display Messages

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.

10.4.1.3 show ipv6 ospf area

This command displays information about the area. The <areaid> identifies the OSPF area that is being displayed.

Syntax

```
show ipv6 ospf area <areaid>
```

Default Setting

None

Command Mode

Privileged Exec

User Exec

Display Messages

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 LSAs.

Area LSA Checksum: A number representing the Area LSA Checksum for the specified AreaID excluding the external (LS type 5) link-state advertisements.

Stub Mode: Represents whether the specified Area is a stub area or not. The possible values are enabled and disabled. This is a configured value.

Import Summary LSAs: Shows whether to import summary LSAs (enabled).

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.

10.4.1.4 show ipv6 ospf asbr

This command displays the internal OSPFv3 routes to reach Autonomous System Boundary Routers (ASBR). This command takes no options.

Syntax
show ipv6 ospf asbr

Default Setting

None

Command Mode

Privileged Exec

User Exec

Display Messages

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.

10.4.1.5 show ipv6 ospf database

This command displays information about the link state database when OSPFv3 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 other optional parameters to specify the type of link state advertisements to display. Use external to display the external LSAs. Use inter-area to display the inter-area LSAs. Use link to display the link LSAs. Use network to display the network LSAs. Use nssa-external to display NSSA external LSAs. Use prefix to display intra-area Prefix LSAs. Use router to display router LSAs. Use unknown area, unknown as, or unknown link to display unknown area, AS or link-scope LSAs, respectively. Use <lsid> to specify the link state ID (LSID). Use adv-router to show the LSAs that are restricted by the advertising router. Use selforiginate to display the LSAs in that are self originated. The information below is only displayed if OSPF is enabled.

Syntax
show ipv6 ospf [<areaid>] database [{external | inter-area {prefix | router} | link | network | nssa-external | prefix | router | unknown {area | as | link}}] [<lsid>] [{adv-router [<rtrid>] | self-originate}]

<areaid> - Configures to display database information about a specific area.

<lsid>- Specify the link state ID.

<rtrid>- Specify an IP Address.

Default Setting

None

Command Mode

Privileged Exec

User Exec

Display Messages

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.

10.4.1.6 show ipv6 ospf database database-summary

This command displays the number of each type of LSA in the database and the total number of LSAs in the database.

Syntax
show ipv6 ospf database database-summary

Default Setting

None

Command Mode

Privileged Exec

User Exec

Display Messages

Router: Total number of router LSAs in the OSPFv3 link state database.

Network: Total number of network LSAs in the OSPFv3 link state database.

Inter-area Prefix: Total number of inter-area prefix LSAs in the OSPFv3 link state database.

Inter-area Router: Total number of inter-area router LSAs in the OSPFv3 link state database.

Type-7 Ext: Total number of NSSA external LSAs in the OSPFv3 link state database.

Link: Total number of link LSAs in the OSPFv3 link state database.

Intra-area Prefix: Total number of intra-area prefix LSAs in the OSPFv3 link state database.

Link Unknown: Total number of link-source unknown LSAs in the OSPFv3 link state database.

Area Unknown: Total number of area unknown LSAs in the OSPFv3 link state database.

AS Unknown: Total number of as unknown LSAs in the OSPFv3 link state database.

Type-5 Ext: Total number of AS external LSAs in the OSPFv3 link state database.

Self-Originated Type-5: Total number of self originated AS external LSAs in the OSPFv3 link state database.

Total: Total number of router LSAs in the OSPFv3 link state database.

10.4.1.7 show ipv6 ospf interface

This command displays the information for the IFO object or virtual interface tables.

Syntax

show ipv6 ospf interface {<slot/port> | loopback <0-7> | tunnel <0-7>}

<slot/port> - Interface number.

<0-7> - Loopback/Tunnel Interface ID.

Default Setting

None

Command Mode

Privileged Exec

User Exec

Display Messages

IP Address: Shows the IPv6 address of the interface.

ifIndex: Shows the interface index number associated with the interface.

OSPF Admin Mode: Shows whether the admin mode is enabled or disabled.

OSPF Area ID: Shows the area ID associated with this interface.

Router Priority: Shows the router priority. The router priority determines which router is the designated router.

Retransmit Interval: Shows the frequency, in seconds, at which the interface sends LSA.

Hello Interval: Shows the frequency, in seconds, at which the interface sends Hello packets.

Dead Interval: Shows the amount of time, in seconds, the interface waits before assuming a neighbor is down.

LSA Ack Interval: Shows the amount of time, in seconds, the interface waits before sending an LSA acknowledgement after receiving an LSA.

Iftransit Delay Interval: Shows the number of seconds the interface adds to the age of LSA packets before transmission.

Authentication Type: Shows the type of authentication the interface performs on LSAs it receives.

Metric Cost: Shows the priority of the path. Low costs have a higher priority than high costs.

OSPF MTU-ignore: Shows whether to ignore MTU mismatches in database descriptor packets sent from neighboring routers.

The following information only displays if OSPF is initialized on the interface:

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.

10.4.1.8 show ipv6 ospf interface brief

This command displays brief information for the IFO object or virtual interface tables.

Syntax
show ipv6 ospf interface brief

Default Setting

None

Command Mode

Privileged Exec

User Exec

Display Messages

Interface: Valid slot and port number separated by forward slashes.

OSPF Admin Mode: States whether OSPF is enabled or disabled on a router interface. This is a configured value.

OSPF Area ID: Represents the OSPF Area Id for the specified interface. This is a configured value.

Router Priority: Shows the router priority. The router priority determines which router is the designated router.

Hello Interval: Shows the frequency, in seconds, at which the interface sends Hello packets.

Dead Interval: Shows the amount of time, in seconds, the interface waits before assuming a neighbor is down.

Retransmit Interval: Shows the frequency, in seconds, at which the interface sends LSA.

Retransmit Delay Interval: Shows the number of seconds the interface adds to the age of LSA packets before transmission.

LSA Ack Interval: Shows the amount of time, in seconds, the interface waits before sending an LSA acknowledgement after receiving an LSA.

10.4.1.9 show ipv6 ospf interface stats

This command displays the statistics for a specific interface. The command only displays information if OSPF is enabled

Syntax

show ipv6 ospf interface stats <slot/port>

<slot/port> - Interface number.

Default Setting

None

Command Mode

Privileged Exec

User Exec

Display Messages

OSPFv3 Area ID: The area id of this OSPF interface.

IP Address: The IP address associated with this OSPF interface.

OSPFv3 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.

Packets Received: The number of OSPFv3 packets received on the interface.

Packets Transmitted: The number of OSPFv3 packets sent on the interface.

LSAs Sent: The total number of LSAs flooded on the interface.

LSA Acks Received: The total number of LSA acknowledged from this interface.

LSA Acks Sent: The total number of LSAs acknowledged to this interface.

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.

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.

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.

10.4.1.10 show ipv6 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 **<ipaddr>** 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.

Syntax

```
show ipv6 ospf neighbor [interface {<slot/port> | tunnel <0-7>}] [<ipaddr>]
```

<ipaddr> - IP address of the neighbor.

<slot/port> - Interface number.

Default Setting

None

Command Mode

Privileged Exec

User Exec

Display Messages

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.

Intf ID: Shows the interface ID 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 - no recent information has been received from the neighbor but a more concerted effort should be made to contact the neighbor.
- Init - an Hello packet has recently been seen from the neighbor, but bidirectional 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 neighboring 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: Shows the interface of the local router in slot/port format.

Area ID: The area ID associated with the interface.

Options: An integer value that indicates the optional OSPF capabilities supported by the neighbor. These are 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 router priority for the specified interface.

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: An integer representing the current length of the retransmission queue of the specified neighbor router Id of the specified interface.

10.4.1.11 show ipv6 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.

Syntax

```
show ipv6 ospf range <areaid>
```

<areaid> - The area id of the requested OSPF area

Default Setting

None

Command Mode

Privileged Exec

User Exec

Display Messages

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.

10.4.1.12 show ipv6 ospf stub table

This command displays the OSPF stub table. The information bello will only be displayed if OSPF is initialized on the switch.

Syntax

```
show ipv6 ospf stub table
```

Default Setting

None

Command Mode

Privileged Exec

User Exec

Display Messages

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. Only supports 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.

10.4.1.13 show ipv6 ospf virtual-link

This command displays the OSPF Virtual Interface information for a specific area and neighbor.

Syntax

```
show ip ospfv6 virtual-link <areaid> <neighbor>
```

<areaid> - Area ID.

<neighbor> - Neighbor's router ID.

Default Setting

None

Command Mode

Privileged Exec

User Exec

Display Messages

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: Shows the type of authentication the interface performs on LSAs it receives.

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.

10.4.1.14 show ipv6 ospf virtual-link brief

This command displays the OSPFv4 Virtual Interface information for all areas in the system.

Syntax
show ipv6 ospf virtual-link brief

Default Setting

None

Command Mode

Privileged Exec

User Exec

Display Messages

Area Id: Is the area id of the requested OSPFv3 area.

Neighbor: Is the neighbor interface of the OSPFv3 virtual interface.

Hello Interval: Is the configured hello interval for the OSPFv3 virtual interface.

Dead Interval: Is the configured dead interval for the OSPFv3 virtual interface.

Retransmit Interval: Is the configured retransmit interval for the OSPFv3 virtual interface.

Transit Delay: Is the configured transit delay for the OSPFv3 virtual interface.

10.4.2 Configuration Commands

10.4.2.1 ipv6 ospf

This command enables OSPF on a router interface or loopback interface.

Syntax

```
ipv6 ospf
no ipv6 ospf
```

<no> - This command disables OSPF on a router interface or loopback interface.

Default Setting

Disabled

Command Mode

Interface Config

10.4.2.2 ipv6 ospf areaid

This command sets the OSPF area to which the specified router interface belongs. The <areaid> is an IPv6 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.

Syntax

```
ipv6 ospf areaid <areaid>
```

<areaid> - is an IPv6 address, formatted as a 4-digit dotted-decimal number or a decimal value in the range of <0-4294967295>.

Default Setting

None

Command Mode

Interface Config

10.4.2.3 ipv6 ospf cost

This command configures the cost on an OSPF interface. The <cost> parameter has a range of 1 to 65535.

Syntax

```
ipv6 ospf cost <1-65535>
no ipv6 ospf cost
```

<no> - This command configures the default cost on an OSPF interface.

Default Setting

None

Command Mode

Interface Config

10.4.2.4 ipv6 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.

Syntax

```
ipv6 ospf dead-interval <seconds>
no ipv6 ospf dead-interval
```

<no> - This command sets the default OSPF dead interval for the specified interface.

Default Setting

40

Command Mode

Interface Config

10.4.2.5 ipv6 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 for <seconds> range from 1 to 65535.

Syntax

```
ipv6 ospf hello-interval <seconds>
no ipv6 ospf hello-interval
```

<no> - This command sets the default OSPF hello interval for the specified interface.

Default Setting

10

Command Mode

Interface Config

10.4.2.6 ipv6 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.

Syntax

```
ipv6 ospf mtu-ignore
no ipv6 ospf mtu-ignore
```

<no> - This command enables the OSPF MTU mismatch detection.

Default Setting

Enabled

Command Mode

Interface Config

10.4.2.7 ipv6 ospf network

This command changes the default OSPF network type for the interface. Normally, the network type is determined from the physical IP network type. By default all Ethernet networks are OSPF type broadcast. Similarly, tunnel interfaces default to point-to-point. When an Ethernet port is used as a single large

bandwidth IP network between two routers, the network type can be point-to-point since there are only two routers. Using point-to-point as the network type eliminates the overhead of the OSPF designated router election. It is normally not useful to set a tunnel to OSPF network type broadcast.

Syntax

```
ipv6 ospf network {broadcast | point-to-point}
no ipv6 ospf network {broadcast | point-to-point}
```

<no> - This command sets the interface type to the default value.

Default Setting

Broadcast

Command Mode

Interface Config

10.4.2.8 ipv6 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.

Syntax

```
ipv6 ospf priority <0-255>
no ipv6 ospf priority
```

<no> - This command sets the default OSPF priority for the specified router interface.

Default Setting

1, which is the highest router priority

Command Mode

Interface Config

10.4.2.9 ipv6 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).

Syntax

```
ipv6 ospf retransmit-interval <seconds>
no ipv6 ospf retransmit-interval
```

<no> - This command sets the default OSPF retransmit Interval for the specified interface.

Default Setting

5

Command Mode

Interface Config

10.4.2.10 ipv6 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).

Syntax

```
ipv6 ospf transmit-delay <seconds>
no ipv6 ospf transmit-delay
```

<no> - This command sets the default OSPF Transit Delay for the specified interface.

Default Setting

1

Command Mode

Interface Config

10.4.2.11 ipv6 router ospf

Use this command to enter Router OSPFv3 Config mode.

Syntax

```
ipv6 router ospf
```

Default Setting

None

Command Mode

Global Config

10.4.2.12 area default-cost

This command configures the monetary default cost for the stub area. The operator must specify the area id and an integer value between 1-16777215.

Syntax

```
area <areaid> default-cost <1-16777215>
```

<areaid> - Area ID.

Default Setting

None

Command Mode

Router OSPFv3 Config

10.4.2.13 area nssa

This command configures the specified areaid to function as an NSSA.

Syntax

```
area <areaid> nssa
no area <areaid> nssa
```

<areaid> - Area ID.

no - This command disables nssa from the specified area id.

Default Setting

None

Command Mode

Router OSPFv3 Config

10.4.2.14 area nssa default-info-originate

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 10. The metric type can be comparable (nssa-external 1) or non-comparable (nssa-external 2).

Syntax

```
area <areaid> nssa default-info-originate [<1-16777215>] [{comparable | non-comparable}]
no area <areaid> nssa default-info-originate [<1-16777215>] [{comparable | non-comparable}]
```

<areaid> - Area ID.

<1-16777215> - The metric of the default route. The range is 1 to 16777215.

comparable - It's NSSA-External 1.

non-comparable - It's NSSA-External 2.

no - This command disables the default route advertised into the NSSA.

Default Setting

None

Command Mode

Router OSPFv3 Config

10.4.2.15 area nssa no-redistribute

This command configures the NSSA ABR so that learned external routes will not be redistributed to the NSSA.

Syntax

```
area <areaid> nssa no-redistribute
no area <areaid> nssa no-redistribute
```

<areaid> - Area ID.

no - This command disables the NSSA ABR so that learned external routes are redistributed to the NSSA.

Default Setting

None

Command Mode

Router OSPFv3 Config

10.4.2.16 area nssa no-summary

This command configures the NSSA so that summary LSAs are not advertised into the NSSA

Syntax

```
area <areaid> nssa no-summary
no area <areaid> nssa no-summary
```

<areaid> - Area ID.

no - This command disables nssa from the summary LSAs.

Default Setting

None

Command Mode

Router OSPFv3 Config

10.4.2.17 area nssa translator-role

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.

Syntax

```
area <areaid> nssa translator-role {always | candidate}
no area <areaid> nssa translator-role
```

<areaid> - Area ID.

always - A value of *always* will cause the router to assume the role of the translator when it becomes a border router.

candidate - a value of *candidate* will cause the router to participate in the translator election process when it attains border router status.

no - This command disables the nssa translator role from the specified area id.

Default Setting

None

Command Mode

Router OSPFv3 Config

10.4.2.18 area nssa translator-stab-intv

This command configures the translator stability interval 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.

Syntax

```
area <areaid> nssa translator-stab-intv <0-3600>
no area <areaid> nssa translator-stab-intv
```

<areaid> - Area ID.

<0-3600> - The range is 0 to 3600.

no - Disables the nssa translator's <stabilityinterval> from the specified area id.

Default Setting

None

Command Mode

Router OSPFv3 Config

10.4.2.19 area range

This command creates a specified area range for a specified NSSA. The **<ipv6-prefix>** is a valid IPv6 address. The **<prefix-length>** 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.

Syntax

```
area <areaid> range <ipv6-prefix>/<prefix-length> {summarylink | nssaexternallink} [advertise |
not-advertise]
no area <areaid> range <ipv6-prefix>/<prefix-length>
```

<areaid> - Area ID.

<ipv6-prefix> - IP Address.

<prefix-length> - The subnetmask.

summarylink - The lsdb type. The value is summarylink or nssaexternallink

nssaexternallink - The lsdb type. The value is summarylink or nssaexternallink

advertise - Allow advertising the specified area range.

not-advertise - Disallow advertising the specified area range.

no - This command deletes a specified area range.

Default Setting

None

Command Mode

Router OSPFv3 Config

10.4.2.20 area stub

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.

Syntax

```
area <areaid> stub
no area <areaid> stub
```

<areaid> - Area ID.

<no> - This command deletes a stub area for the specified area ID.

Default Setting

None

Command Mode

Router OSPFv3 Config

10.4.2.21 area stub no-summary

This command disables the import of Summary LSAs for the stub area identified by <areaid>.

Syntax

```
area <areaid> stub no-summary
no area <areaid> stub no-summary
```

<areaid> - Area ID.

no - This command sets the Summary LSA import mode to the default for the stub area identified by <areaid>.

Default Setting

Enabled

Command Mode

Router OSPFv3 Config

10.4.2.22 area virtual-link

This command creates the OSPF virtual interface for the specified <areaid> and <neighbor>. The <neighborid> parameter is the Router ID of the neighbor.

Syntax

```
area <areaid> virtual-link <neighborid>
no area <areaid> virtual-link <neighborid>
```

<areaid> - Area ID.

<neighborid> - Router ID of the neighbor.

no - This command deletes the OSPF virtual interface from the given interface, identified by **<areaid>** and **<neighborid>**. The **<neighborid>** parameter is the Router ID of the neighbor.

Default Setting

The default authentication type is none.

Command Mode

Router OSPFv3 Config

10.4.2.23 area virtual-link dead-interval

This command configures the dead interval for the OSPF virtual interface on the virtual interface identified by **<areaid>** and **<neighborid>**.

Syntax

```
area <areaid> virtual-link <neighborid> dead-interval <1-65535>
no area <areaid> virtual-link <neighborid> dead-interval
```

<areaid> - Area ID.

<neighborid> - Router ID of the neighbor.

<1-65535> - The range of the dead interval is 1 to 65535.

no - 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.

Default Setting

40 seconds.

Command Mode

Router OSPFv3 Config

10.4.2.24 area virtual-link hello-interval

This command configures the hello interval for the OSPF virtual interface on the interface identified by **<areaid>** and **<neighborid>**.

Syntax

```
area <areaid> virtual-link <neighborid> hello-interval <1-65535>
no area <areaid> virtual-link <neighborid> hello-interval
```

<areaid> - Area ID.

<neighborid> - Router ID of the neighbor.

<1-65535> - The range of the hello interval is 1 to 65535.

no - This command configures the default hello interval for the OSPF virtual interface on the interface identified by **<areaid>** and **<neighborid>**.

Default Setting

10 seconds.

Command Mode

Router OSPFv3 Config

10.4.2.25 area virtual-link retransmit-interval

This command configures the retransmit interval for the OSPF virtual interface on the interface identified by **<areaid>** and **<neighborid>**.

Syntax

```
area <areaid> virtual-link <neighborid> retransmit-interval <0-3600>
no area <areaid> virtual-link <neighborid> retransmit-interval
```

<areaid> - Area ID.

<neighborid> - Router ID of the neighbor.

<0-3600> - The range of the retransmit interval is 0 to 3600.

no - This command configures the default retransmit interval for the OSPF virtual interface on the interface identified by <areaid> and <neighborid>.

Default Setting

5 seconds.

Command Mode

Router OSPFv3 Config

10.4.2.26 area virtual-link transmit-delay

This command configures the transmit delay for the OSPF virtual interface on the virtual interface identified by **<areaid>** and **<neighborid>**.

Syntax

```
area <areaid> virtual-link <neighborid> transmit-delay <0-3600>
no area <areaid> virtual-link <neighborid> transmit-delay
```

<areaid> - Area ID.

<neighborid> - Router ID of the neighbor.

<0-3600> - The range of the transmit delay is 0 to 3600.

no - This command configures the default transmit delay for the OSPF virtual interface on the virtual interface identified by <areaid> and <neighborid>.

Default Setting

1 second.

Command Mode

Router OSPFv3 Config

10.4.2.27 auto-cost

By default, OSPF computes the link cost of each interface from the interface bandwidth. Faster links have lower metrics, making them more attractive in route selection. The configuration parameters in the auto-cost reference bandwidth and bandwidth commands give you control over the default link cost. You can configure for OSPF an interface bandwidth that is independent of the actual link speed. A second configuration parameter allows you to control the ratio of interface bandwidth to link cost. The link cost is computed as the ratio of a reference bandwidth to the interface bandwidth (ref_bw /interface bandwidth), where interface bandwidth is defined by the bandwidth command. Because the default reference bandwidth is 100 Mbps, OSPF uses the same default link cost for all interfaces whose bandwidth is 100 Mbps or greater. Use the auto-cost command to change the reference bandwidth, specifying the reference bandwidth in megabits per second (Mbps). The reference bandwidth range is 1–4294967 Mbps. The different reference bandwidth can be independently configured for OSPFv2 and OSPFv3.

Syntax

```
auto-cost reference-bandwidth <1 to 4294967>
no auto-cost reference-bandwidth
```

Default Setting

100Mbps

Command Mode

Router OSPFv3 Config

10.4.2.28 default-information originate

This command is used to control the advertisement of default routes.

Syntax

```
default-information originate [always] [metric <1-16777215>] [metric-type {1 | 2}]
no default-information originate [metric] [metric-type]
```

[always] - Sets the router advertise 0.0.0.0/0.0.0.0.

metric - The range of the metric is 1 to 16777215.

metric type - The value of metric type is type 1 or type 2.

no - This command configures the default advertisement of default routes.

Default Setting

Metric: unspecified

Type: 2

Command Mode

Router OSPFv3 Config

10.4.2.29 default-metric

This command is used to set a default for the metric of distributed routes.

Syntax

```
default-metric <1-16777215>
no default-metric
```

<1-16777215> - The range of default metric is 1 to 16777215.

<no> - This command is used to set a default for the metric of distributed routes.

Default Setting

None

Command Mode

Router OSPFv3 Config

10.4.2.30 distance 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.

Syntax

```
distance ospf {intra | inter | type1 | type2} <preference>
no distance ospf {intra | inter | type1 | type2}
```

<preference> - The range for intra is 1 to 252. The range for inter is 2 to 253. The range for type1 is 3 to 254. The range for type2 is 4 to 255.

no - This command sets the default route preference value of OSPF in the router.

Default Setting

Intra is 8.

Inter is 10.

Type 1 is 13.

Type 2 is 150.

Command Mode

Router OSPFv3 Config

10.4.2.31 enable

This command resets the default administrative mode of OSPF in the router (active).

Syntax

```
enable
no enable
```

<no> - This command sets the administrative mode of OSPF in the router to inactive.

Default Setting

Enabled

Command Mode

Router OSPFv3 Config

10.4.2.32 exit-overflow-interval

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.

Syntax

```
exit-overflow-interval <0-2147483647>
no exit-overflow-interval
```

<0-2147483674> - The range of exit overflow interval for OSPF is 0 to 2147483674.

no - This command configures the default exit overflow interval for OSPF.

Default Setting

0

Command Mode

Router OSPFv3 Config

10.4.2.33 external-lsdb-limit

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.

Syntax

```
external-lsdb-limit <-1-2147483647>
no external-lsdb-limit
```

<-1-2147483647> - The range of external LSDB limit for OSPF is -1 to 2147483674.

no - This command configures the default external LSDB limit for OSPF.

Default Setting

-1

Command Mode

Router OSPFv3 Config

10.4.2.34 maximum-paths

This command sets the number of paths that OSPF can report for a given destination where <maxpaths> is platform dependent.

Syntax

```
maximum-paths <1-2>
no maximum-paths
```

<1-2> - The maximum number of paths that OSPF can report for a given destination. The range of the value is 1 to 2.

no - This command resets the number of paths that OSPF can report for a given destination back to its default value.

Default Setting

1

Command Mode

Router OSPFv3 Config.

10.4.2.35 passive-interface default

Use this command to enable global passive mode by default for all interfaces. It overrides any interface level passive mode.OSPF shall not form adjacencies over a passive interface.

Syntax

```
passive-interface default
no passive-interface default
```

Default Setting

Disabled

Command Mode

Router OSPFv3 Config.

10.4.2.36 passive-interface

Use this command to set the interface or tunnel as passive. It overrides the global passive mode that is currently effective on the interface or tunnel.

Syntax

```
passive-interface {<unit/slot/port> | tunnel <tunnel-id>}
no passive-interface {<unit/slot/port> | tunnel <tunnel-id>}
```

Default Setting

Disabled

Command Mode

Router OSPFv3 Config.

10.4.2.37 redistribute

This command configures the OSPFv3 protocol to allow redistribution of routes from the specified source protocol/routers.

Syntax

```
redistribute {static | connected} [metric <0-16777214>] [metric-type {1 | 2}] [tag <0-4294967295>]
no redistribute { static | connected} [metric] [metric-type] [tag]
```

<0-16777215> - The range of metric is 0 to 16777214.

<0-4294967295> - The range of tag is 0 to 4294967295.

Default Setting

Metric is unspecified.

Type is 2.

Tag is 0.

Command Mode

Router OSPFv3 Config

10.4.2.38 router-id

This command sets a 4-digit dotted-decimal number uniquely identifying the router ospf id.

Syntax

```
router-id <ipaddress>
```

<ipaddress> - IP Address.

Default Setting

None

Command Mode

Router OSPFv3 Config

10.5 RIPng Commands

RIPng is intended to allow routers to exchange information for computing routes through an IPv6-based network. RIPng is a distance vector protocol. RIPng should be implemented only in routers. Any router that uses RIPng is assumed to have interfaces to one or more networks, otherwise it isn't really a router. These are referred to as its directly-connected networks. The protocol relies on access to certain information about each of these networks, the most important of which is its metric. The RIPng metric of a network is an integer between 1 and 15, inclusive. It is set in some manner not specified in this protocol; however, given the maximum path limit of 15, a value of 1 is usually used. Implementations should allow the system administrator to set the metric of each network. In addition to the metric, each network will have an IPv6 destination address prefix and prefix length associated with it. These are to be set by the system administrator in a manner not specified in this protocol.

10.5.1 Show Commands

10.5.1.1 show ipv6 rip

This command displays information relevant to the RIPng router

Syntax
show ipv6 rip

Default Setting

None

Command Mode

Privileged Exec

Display Messages

RIPng Admin Mode: Select enable or disable from the pulldown menu. If you select enable RIPng will be enabled for the switch. The default is disabled.

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.

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.

Distance: Configured value.

Update Time: Configured value.

Garbage Time: Configured value.

Info Time: Configured value.

Enable Ripng of interfaces: List all interfaces enabled RIPng.

Enable passive mode of interfaces: List all interfaces enabled RIPng passive.

10.5.2 Configuration Commands

10.5.2.1 enable

This command resets the default administrative mode of RIPng in the router (active).

Syntax
enable no enable

no - This command sets the administrative mode of RIPng in the router to inactive.

Default Setting

Enabled

Command Mode

IPv6 Router RIP Config

10.5.2.2 ipv6 rip

This command enables RIPng on a router interface.

Syntax
Ipv6 rip no ipv6 rip

no - This command disables RIPng on a router interface.

Default Setting

Disabled

Command Mode

Interface Config

10.5.2.3 ipv6 router rip

Use this command to enter Router RIPng mode.

Syntax

```
ipv6 router rip
```

Default Setting

Disabled

Command Mode

Global Config

10.5.2.4 default-information originate

This command is used to set the advertisement of default routes.

Syntax

```
default-information originate
no default-information originate
```

no - This command is used to cancel the advertisement of default routes.

Default Setting

Disabled

Command Mode

IPv6 Router RIP Config

10.5.2.5 default-metric

This command is used to set a default for the metric of distributed routes.

Syntax

```
default-metric <1-15>
no default-metric
```

<1-15> - a value for default-metric.

no - This command is used to reset the default metric of distributed routes to its default value.

Default Setting

Not configured

Command Mode

IPv6 Router RIP Config

10.5.2.6 distance rip

This command sets the route preference value of RIPng in the router. Lower route preference values are preferred when determining the best route.

Syntax

```
distance rip <1-255>
no distance rip
```

<1-255> - the value for distance.

no - This command sets the default route preference value of RIPng in the router.

Default Setting

15

Command Mode

IPv6 Router RIP Config

10.5.2.7 split-horizon

This command sets the RIPngplit horizon mode. None mode will not use RIPngplit horizon mode. Simple mode will be that a route is not advertised on the interface over which it is learned. Poison mode will be that routes learned over this interface should be re-advertised on the interface with a metric of infinity (16).

Syntax

```
split-horizon {none | simple | poison}
no split-horizon
```

none - This command sets without using RIPngplit horizon mode.

simple - This command sets to use simple split horizon mode.

poison - This command sets to use poison reverse mode.

no - This command cancel to set the RIPngplit horizon mode and sets none mode.

Default Setting

Simple

Command Mode

IPv6 Router RIP Config

10.5.2.8 redistribute

This command configures RIPng protocol to redistribute routes from the specified source protocol/routers. Source protocols have OSPF, Static, and Connetced.

Syntax

Format for OSPF as source protocol:
redistribute ospf [metric <1-15>]
Format for other source protocols:
redistribute {static | connected} [metric <1-15>]
no redistribute {ospf | static | connected} [metric]

<1 - 15> - a value for metric.

no - This command de-configures RIPng protocol to redistribute routes from the specified source protocol/routers.

Default Setting

Metric – not-configured

Command Mode

IPv6 Router RIP Config

10.5.2.9 ipv6 rip timer

The user can go to the CLI Global Configuration Mode to set ipv6 rip timer, use the **ipv6 rip timer {update|garbage|info} <5-2147483647>** global configuration command. Use the **no ipv6 rip timer {update|garbage|info}** return to the default value.

Syntax

ipv6 rip timer {update|garbage|info} <5-2147483647>
no ipv6 rip timer {update|garbage|info}

update - This command sets to the RIPng update time.

garbage - This command sets to the RIPng garbage time.

info - This command sets to the RIPng info time.

no - This command sets the RIPng timer to default value.

Default Setting

update **-** the default value is 30 (seconds)

garbage **-** the default value is 120 (seconds)

info **-** the default value is 180 (seconds)

Command Mode

Global Config

10.5.2.10 ipv6 rip passive-interface

The user can go to the CLI Interface Configuration Mode to set ipv6 rip passive, use the **ipv6 rip passive-interface** interface configuration command. Use the **no ipv6 rip passive-interface** return to the default value.

Syntax

```
ipv6 rip passive-interface
no ipv6 rip passive-interface
```

no - This command sets the RIPng timer to default value.

Default Setting

Disabled

Command Mode

Interface Config

10.6 Protocol Independent Multicast – Dense Mode (PIM-DM) Commands

10.6.1 Show Commands

10.6.1.1 show ipv6 pimdm

Use this command to display PIM-DM Global Configuration parameters and PIM-DM interface status.

Syntax

```
show ipv6 pimdm
```

Default Setting

None

Command Mode

Privileged Exec

User Exec

Display Message

PIM-DM Admin Mode: Indicates whether PIM-DM is enabled or disabled.

Interface: Valid unit, slot, and port number separated by forward slashes.

Interface Mode: Indicates whether PIM-DM is enabled or disabled on this interface.

Operational State: The current state of PIM-DM on this interface. Possible values are Operational or Non-Operational.

10.6.1.2 show ipv6 pimdm interface

Use this command to display PIM-DM configuration information for all interfaces or for the specified interface. If no interface is specified, configuration of all interfaces is displayed.

Syntax

```
show ipv6 pimdm interface {<slot/port>/all }
```

Default Setting

None

Command Mode

Privileged Exec

User Exec

Display Message

Interface Mode: Indicates whether PIM-DM is enabled or disabled on the specified interface.

PIM-DM Interface Hello Interval: The frequency at which PIM hello messages are transmitted on this interface. By default, the value is 30 seconds.

10.6.1.3 show ipv6 pimdm neighbor

Use this command to display the PIM-DM neighbor information for all interfaces or for the specified interface.

Syntax

```
show ipv6 pimdm neighbor [<slot/port>|all]
```

Default Setting

None

Command Mode

Privileged Exec

User Exec

Display Message

Interface: Valid unit, slot, and port number separated by forward slashes.

Neighbor Address: The IP address of the neighbor on an interface.

Up Time: The time since this neighbor has become active on this interface.

Expiry Time: The expiry time of the neighbor on this interface.

10.6.2 Configuration Commands

10.6.2.1 ipv6 pimdm

Use this command to administratively enable PIM-DM Multicast Routing Mode either across the router (Global Config) or on a particular router (Interface Config).

Syntax

```
ipv6 pimdm
no ipv6 pimdm
```

no - Use this command to administratively disable PIM-DM Multicast Routing Mode either across the router (Global Config) or on a particular router (Interface Config).

Default Setting

Disabled

Command Mode

Global Config

Interface Config

10.6.2.2 ipv6 pimdm hello-interval

Use this command to configure the PIM-DM hello interval for the specified router interface. The hello-interval is specified in seconds and is in the range 30–3600.

Syntax

```
ipv6 pimdm hello-interval <30-3600>
no ipv6 pimdm hello-interval
```

no - Use this command to set the PIM-DM hello interval to the default value.

Default Setting

Disabled

Command Mode

Interface Config

10.7 Protocol Independent Multicast – Sparse Mode (PIM-SM) Commands

10.7.1 Show Commands

10.7.1.1 show ipv6 pimsm

This command displays the system-wide information for PIM-SM.

Syntax

```
show ipv6 pimsm
```

Default Setting

None

Command Mode

Privileged Exec

User Exec

Display Message

Admin Mode: Indicates whether PIM-SM is enabled or disabled.

Data Threshold Rate (Kbps): The data threshold rate for the PIM-SM router.

Register Threshold Rate (Kbps): The threshold rate for the RP router to switch to the shortest path.

SSM Range Table Group Address/Prefix Length

PIM-SM Interface Status:

Interface: Valid unit, slot, and port number separated by forward slashes.

Interface Mode: Indicates whether PIM-SM is enabled or disabled on the interface.

Operational State: The current state of the PIM-SM protocol on the interface. Possible values are Operational or Non- Operational.

10.7.1.2 show ipv6 pimsm bsr

This command displays the bootstrap router (BSR) information. The output includes elected BSR information and information about the locally configured candidate rendezvous point (RP) advertisement.

Syntax

show ipv6 pimsm bsr

Default Setting

None

Command Mode

Privileged Exec

User Exec

Display Message

BSR Address: IP address of the BSR.

Uptime: Length of time that this router has been up (in hours, minutes, and seconds).

BSR Priority: Priority as configured in the **ip pimsm bsr-candidate** command.

Hash Mask Length: Length of a mask (maximum 32 bits) that is to be ANDed with the group address before the hash function is called. This value is configured in the **ip pimsm bsr-candidate** command.

Next Bootstrap Message In: Time (in hours, minutes, and seconds) in which the next bootstrap message is due from this BSR.

Next Candidate RP advertisement in: Time (in hours, minutes, and seconds) in which the next candidate RP advertisement will be sent.

10.7.1.3 show ipv6 pimsm interface

This command displays interface configuration parameters for PIM-SM on the specified interface. If no interface is specified,all interfaces are displayed.

Syntax

show ipv6 pimsm interface [<*unit/slot/port*>]

Default Setting

None

Command Mode

Privileged Exec

User Exec

Display Message

Slot Port: Valid unit, slot, and port number separated by forward slashes.

IP Address: The IP address of the specified interface.

Subnet Mask: The Subnet Mask for the IP address of the PIM interface.

Hello Interval (secs): The frequency at which PIM hello messages are transmitted on this interface. By default, the value is 30 seconds.

Join Prune Interval (secs): The join/prune interval for the PIM-SM router. The interval is in seconds.

Neighbor Count: The neighbor count for the PIM-SM interface.

Designated Router: The IP address of the Designated Router for this interface.

DR Priority: The priority of the Designated Router.

BSR Border: The bootstrap router border interface. Possible values are enabled or disabled.

10.7.1.4 show ipv6 pimsm neighbor

This command displays the neighbor information for PIM-SM on the specified interface.

Syntax
show ipv6 pimsm neighbor {<unit/slot/port> | all}

Default Setting

None

Command Mode

Privileged Exec

User Exec

Display Message

Interface: Valid unit, slot, and port number separated by forward slashes.

IP Address: The IP address of the neighbor on an interface.

Up Time: The time since this neighbor has become active on this interface.

Expiry Time: The expiry time of the neighbor on this interface.

10.7.1.5 show ipv6 pimsm rphash

This command displays which rendezvous point (RP) is being used for a specified group.

Syntax

show ipv6 pimsm rphash <group-address>

<group-address> - the IP multicast group address.

Default Setting

None

Command Mode

Privileged Exec

User Exec

Display Message

RP: The IP address of the RP for the group specified.

Origin: Indicates the mechanism (BSR or static) by which the RP was selected.

10.7.1.6 show ipv6 pimsm rp mapping

Use this command to display all group-to-RP mappings of which the router is a aware (either configured or learned from the bootstrap router (BSR)). If no RP is specified, all active RPs are displayed.

Syntax

show ipv6 pimsm rp mapping [rp address]

Default Setting

None

Command Mode

Privileged Exec

User Exec

Display Message

RP Address: This field displays the IP address of the RP.

Type: Indicates the mechanism (BSR or static) by which the RP was selected.

10.7.2 Configuration Commands

10.7.2.1 ipv6 pimsm

This command sets administrative mode of PIM-SM multicast routing across the router to enabled. MLD must be enabled before PIM-SM can be enabled.

Syntax

ipv6 pimsm
no ipv6 pimsm

no - This command sets administrative mode of PIM-SM multicast routing across the router to disabled. MLD must be enabled before PIM-SM can be enabled.

Default Setting

Disbaled

Command Mode

Global Config

Interface Config

10.7.2.2 ipv6 pimsm bsr-candidate

This command is used to configure the router to announce its candidacy as a bootstrap router (BSR).

Syntax

ipv6 pimsm bsr-candidate interface *<slot/port> [hash-mask-length] [priority]*
no ipv6 pimsm bsr-candidate

hash-mask-length - Length of a mask (32 bits maximum) that is to be ANDed with the group address before the hash function is called. All groups with the same seed hash correspond to the same RP. For example, if this value was 24, only the first 24 bits of the group addresses matter. This allows you to get one RP for multiple groups.

priority - Priority of the candidate BSR. The range is an integer from 0 to 255. The BSR with the larger priority is preferred. If the priority values are the same, the router with the larger IP address is the BSR. The default value is 0.

no - This command is used to disable the router to announce its candidacy as a bootstrap router (BSR).

Default Setting

None

Command Mode

Global Config

10.7.2.3 ipv6 pimsm register-threshold

This command configures the Register Threshold rate for the Rendezvous Point router to switch to a source-specific shortest path. The valid values are from (0 to 2000 kilobits/sec).

Syntax

ipv6 pimsm register-threshold <*0-2000*>
no ipv6 pimsm register-threshold

no - This command resets the register threshold rate for the Rendezvous Pointer router to the default value.

Default Setting

0

Command Mode

Global Config

10.7.2.4 ipv6 pimsm rp-address

This command is used to statically configure the RP address for one or more multicast groups. The parameter <*rpaddress*> 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. The optional keyword **override** indicates that if there is a conflict, the RP configured with this command prevails over the RP learned by BSR.

Syntax

ipv6 pimsm rp-address <*rp-address*> <*group-address*> <*group-mask*> [override]
no ipv6 pimsm rp-address <*rp-address*> <*group-address*> <*group-mask*>

no - This command is used to statically remove the RP address for one or more multicast groups.

Default Setting

0

Command Mode

Global Config

10.7.2.5 ipv6 pimsm rp-candidate

This command is used to configure the router to advertise itself as a PIM candidate rendezvous point (RP) to the bootstrap router (BSR).

Syntax

ipv6 pimsm rp-candidate interface <*slot/port*> <*group-address*> <*group-mask*>
no ipv6 pimsm rp-candidate interface <*slot/port*> <*group-address*> <*group-mask*>

no - This command is used to disable the router to advertise itself as a PIM candidate rendezvous point (RP) to the bootstrap router (BSR).

Default Setting

0

Command Mode

Global Config

10.7.2.6 ipv6 pimsm spt-threshold

This command is used to configure the Data Threshold rate for the last-hop router to switch to the shortest path. The rate is specified in Kilobits per second. The possible values are 0 to 2000.

Syntax

iipv6 pimsm spt-threshold <*1-2000*>
no ipv6 pimsm spt-threshold

no - This command is used to set the Data Threshold rate for the RP router to the default value.

Default Setting

0

Command Mode

Global Config

10.7.2.7 ipv6 pimsm ssm

Use this command to define the Source Specific Multicast (SSM) range of IP multicast addresses.

Syntax

ipv6 pimsm ssm *{default* | <*group-address*> <*group-mask*>*}*
no ipv6 pimsm ssm

default - Defines the SSM range access list to 232/8.

no - This command is used to disable the Source Specific Multicast (SSM) range.

Default Setting

Disbaled

Command Mode

Global Config

10.7.2.8 ipv6 pimsm bsr-border

Use this command to prevent bootstrap router (BSR) messages from being sent or received through an interface.

Syntax

```
ipv6 pimsm bsr-border
no ipv6 pimsm bsr-border
```

no - Use this command to disable the interface from being the BSR border.

Default Setting

Disbaled

Command Mode

Interface Config

10.7.2.9 ipv6 pimsm dr-priority

Use this command to set the priority value for which a router is elected as the designated router (DR).

Syntax

```
ipv6 pimsm dr-priority <0-2147483647>
no ipv6 pimsm dr-priority
```

no - Use this command to disable the interface from being the BSR border.

Default Setting

Disabled

Command Mode

Interface Config

10.7.2.10 ipv6 pimsm join-prune-interval

This command is used to configure the interface join/prune interval for the PIM-SM router. The join/prune interval is specified in seconds. This parameter can be configured to a value from 0 to 18000.

Syntax

```
ipv6 pimsm join-prune-interval <10-3600>
no ipv6 pimsm join-prune-interval
```

no - Use this command to set the join/prune interval to the default value.

Default Setting

60

Command Mode

Interface Config

10.7.2.11 ipv6 pimsm hello-interval

This command is used to configure the PIM-SM hello interval for the specified interface. The hello interval range is 0-18000 is specified in seconds.

Syntax

```
ipv6 pimsm hello-interval <0-18000>
no ipv6 pimsm hello-interval
```

no - This command is used to set the hello interval to the default value.

Default Setting

30

Command Mode

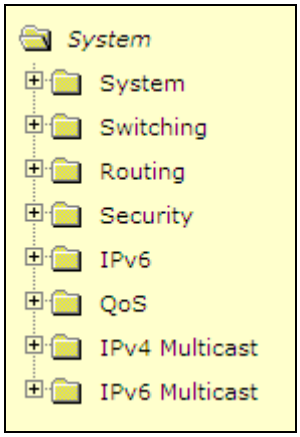
Interface Config

11. Web-Based Management Interface

11.1 Overview

The Layer 3 Network Switch provides a built-in browser software interface that lets you configure and manage it remotely using a standard Web browser such as Microsoft Internet Explorer or Netscape Navigator. This software interface also allows for system monitoring and management of the Network Switch. When you configure this Network Switch for the first time from the console, you have to assign an IP address and subnet mask to the Network Switch. Thereafter, you can access the Network Switch's Web software interface directly using your Web browser by entering the switch's IP address into the address bar. In this way, you can use your Web browser to manage the Switch from any remote PC station, just as if you were directly connected to the Network Switch's console port.

The 8 menu options available are: System, Switching, Routing, Security, IPv6, QOS, IPv4 Multicast and IPv6 Multicast.



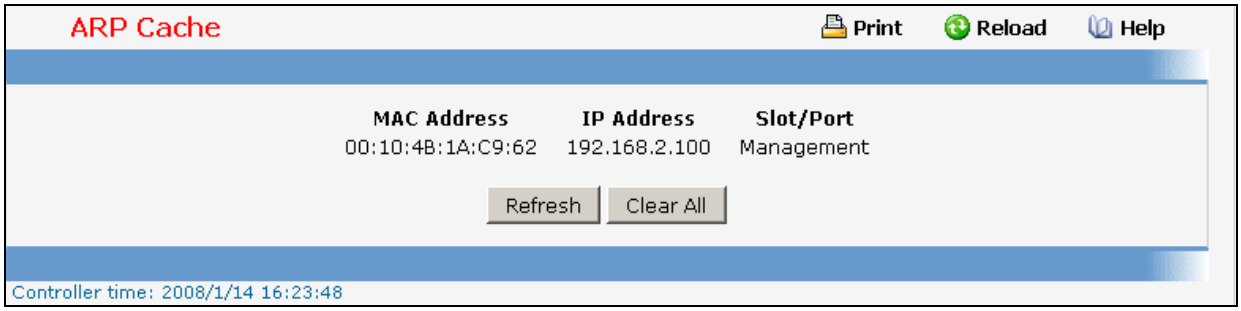
1. **System Menu:** This section provides information for configuring switch interface (port), SNMP and trap manager, Ping, DHCP client, DNS Relay, SNTP, system time, defining system parameters including telnet session and console baud rate, etc, downloading switch module software, and resetting the switch module, switch statistics and Layer 2 Mac address.
2. **Switching Menu:** This section provides users to configure switch DHCP Snooping, VLAN, Protected Ports, Protocol-Based VLAN, IP Subnet-based VLAN, MAC-based VLAN, MAC-Based Voice VLAN, Voice VLAN, Filters, GARP, Dynamic Arp Inspection, IGMP Snooping, IGMP Snooping Querier, MLD Snooping, MLD Snooping Querier, Port Channel, Multicast Forwarding Database, Spanning Tree, Class of Service, Port Security, LLDP, CDP, VTP, Link State, Port Backup and FIP Snooping.
3. **Routing Menu:** This section provides users to configure ARP, IP, OSPF, BOOTP/DHCP Relay Agent, RIP, Router Discovery, Router, VLAN Routing, VRRP, Tunnels and Loopbacks.
4. **Security Menu:** This section provides users to configure switch securities including Port Access Control, RADIUS, TACACS+, IP Filter, Secure HTTP, and Secure Shell.
5. **IPv6 Menu:** This section provides users to configure OSPFv3, RIPv6, IPv6 Static Route, and IPv6 Routing Interface.
6. **QOS Menu:** This section provides users to configure Access Control Lists, Differentiated Service, DiffServ Wizard, and Class of Service.

7. **IPv4 Multicast Menu:** This section provides users to configure IGMP, DVMRP, Multicast, PIM-DM, PIM-SM. It also provides information for a multicast distribution tree.
8. **IPv6 Multicast Menu:** This section provides users to configure MLD, PIM-DM, PIM-SM. It also provides information for a multicast distribution tree.

11.2 System Menu

11.2.1 View 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

Command Buttons

Refresh - Refresh the page with the latest data.

Clear all - Clean all MAC entries in system ARP table.

11.2.2 Viewing Inventory Information

Use this panel to display the switch's Vital Product Data, stored in non-volatile memory at the factory.

Non-Configurable Data

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.

Part Number - The manufacturing part number.

Base MAC Address - The burned-in universally administered MAC address of this switch.

Hardware Version - The hardware version of this switch. It is divided into four parts. The first byte is the major version and the second byte represents the minor version.

Loader Version - The release-version number of the loader code currently running on the switch. For example, if the release was 1, and the version was 2, the format would be '1.2'.

Boot Rom Version - The release-version number of the boot rom code currently running on the switch. For example, if the release was 1, and the version was 2, the format would be '1.2'.

Label Revision Number - The label revision serial number of this switch is used for manufacturing purpose.

Runtime Version - The release-version number of the code currently running on the switch. For example, if the release was 1, and the version was 2, the format would be '1.2..

Operating System - The operating system currently running on the switch.

Network Processing Device - Identifies the network processor hardware.

ADT7460_1: Now Temperature: The temperature of sensor of ADT7460 1.

ADT7460_2: Now Temperature: The temperature of sensor of ADT7460 2.

Depend on air flow FAN 1 – 4 connected ADT7460-1 or ADT7460-2:

Front-To-Back: (Connected ADT7460-1)

ADT7460_1: Fan 1 Status: Status of Fan1. It could be active or inactive.

ADT7460_1: Fan 2 Status: Status of Fan2. It could be active or inactive.

ADT7460_1: Fan 3 Status: Status of Fan3. It could be active or inactive.

ADT7460_1: Fan 4 Status: Status of Fan3. It could be active or inactive.

Back-To-Front: (Connected ADT7460-2)

ADT7460_2: Fan 1 Status: Status of Fan1. It could be active or inactive.

ADT7460_2: Fan 2 Status: Status of Fan2. It could be active or inactive.

ADT7460_2: Fan 3 Status: Status of Fan3. It could be active or inactive.

ADT7460_2: Fan 4 Status: Status of Fan3. It could be active or inactive.

Switch Power+ y…… Power Supply (The yth power supply information of switch 1).

Name: Name provided by Power Supply vendor.

Model: Model Number provided by Power Supply vendor.

Revision Number: Revision Number provided by Power Supply vendor.

Manufacturer Location: Location provided by Power Supply vendor.

Date of Manufacturing: Date of Manufacturing provided by Power Supply vendor.

Serial Numbe: Serial Number provided by Power Supply vendor.

Temperature 1:. Inner temperature 1 of Power Supply now

Temperature 2: Inner temperature 2 of Power Supply now

Fan Speed: Inner fan speed(rpm) of Power Supply now

Fan Duty: Inner fan duty(%) of Power Supply now

Below 10-Giga Interface information depend on plugging SFP+ Transceiver

Interface = y..... SFP+(The yth 10-Giga information of switch 1).

10 Gigabit Ethernet Compliance Codes: Transceiver's compliance codes.

Vendor Name: The SFP transceiver vendor name shall be the full name of the corporation, a commonly accepted abbreviation of the name of the corporation, the SCSI company code for the corporation, or the stock exchange code for the corporation.

Vendor Part Number: Part number provided by SFP transceiver vendor.

Vendor Serial Number: Serial number provided by vendor.

Vendor Revision Number: Revision level for part number provided by vendor.

Vendor Manufacturing Date: The vendor's manufacturing date.

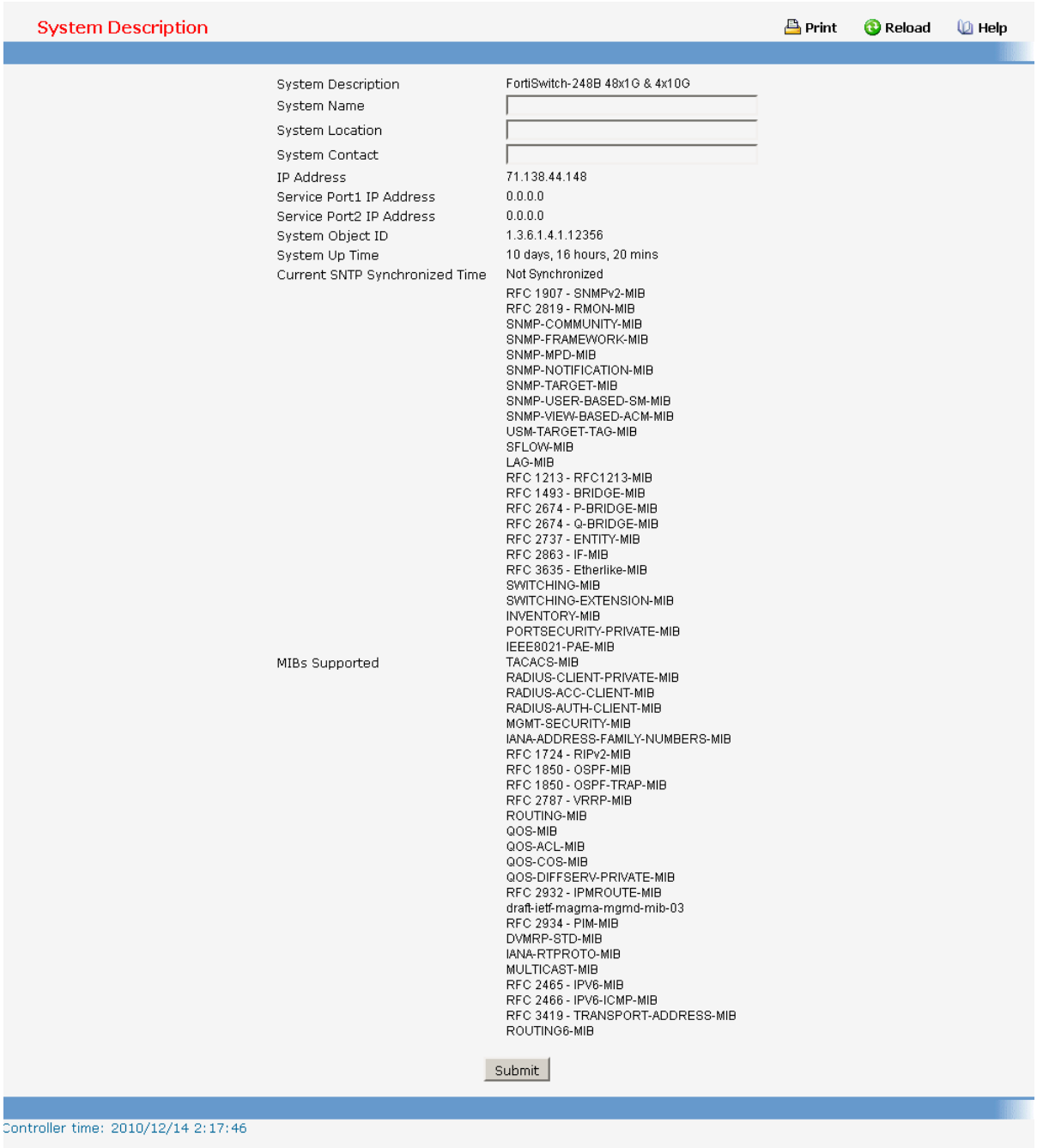
Additional Packages - A list of the optional software packages installed on the switch, if any.

Command Buttons

Refresh - Updates the information on the page.

11.2.3 Configuring Management Session and Network Parameters

11.2.3.1 Viewing System Description Page



Configurable Data

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.

Non-Configurable Data

IP Address - The IP Address assigned to the network interface.

Service Port IP Address - The IP Address assigned to the Service Port.

System Object ID - 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.

Current SNTP Syncronized Time - Displays currently synchronized SNTP time in UTC. If time is not syncronised, it displays "Not Syncronized."

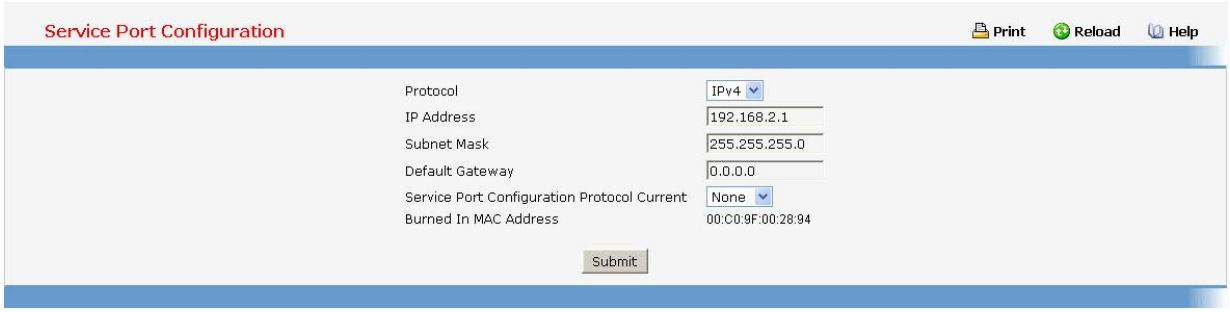
MIBs Supported - The list of MIBs supported by the management agent running on this switch.

Command Buttons

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

11.2.3.2 Configuring Service Port Page

You use this panel to specify the parameters needed to communicate with the switch over a network using the service port.



Selection Criteria

Service Port 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 None.

You cannot make this choice for both the network configuration protocol and the service port. You will only be given the choices for Bootp or DHCP here if the network configuration protocol is configured to None.

Protocol - Choose IPv4 or IPv6 protocol.

IPv6 Mode - Enable/Disable IPv6.

IPv6 Prefix - Choose a IPv6 prefix.

DHCP6 Client - Selects if the DHCP6 Client is enabled or disabled.

You cannot make this choice for both the In-Band Mgmt and the Out-of-Band Mgmt. You will only be given the choices for Enable here if the In-Band Mgmt is configured to Disable.

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

IPv6 Gateway - The default gateway for the IPv6 interface. The factory default value is None

Non-Configurable Data

Burned-in MAC Address - The burned-in MAC address used for in-band connectivity.

Default Routers - The IPv6 default routers.

Command Buttons

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

Delete - Delete a IPv6 prefix.

11.2.3.3 Configuring ServicePort NDP Summary

This screen displays IPv6 Service Port Neighbor entries.

Non-configurable Data

IPv6 Address - The Ipv6 Address of a neighbor switch visible to the Service Port.

Mac Address - The MacAddress of the neighboring switch.

isRtr -true(1) if the neighbor machine is a router, false(2) otherwise.

Neighbor State -The state of the neighboring switch: reachable(1) - The neighbor is reachable by this switch. stale(2) - Information about the neighbor is scheduled for deletion. delay(3) - No information has been received from neighbor during delay period. probe(4) - Switch is attempting to probe for this neighbor. unknown(6) - Unknown status.

Last Updated -The last sysUpTime that this neighbor has been updated.

Command Buttons

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

11.2.3.4 Configuring Network Connectivity Page

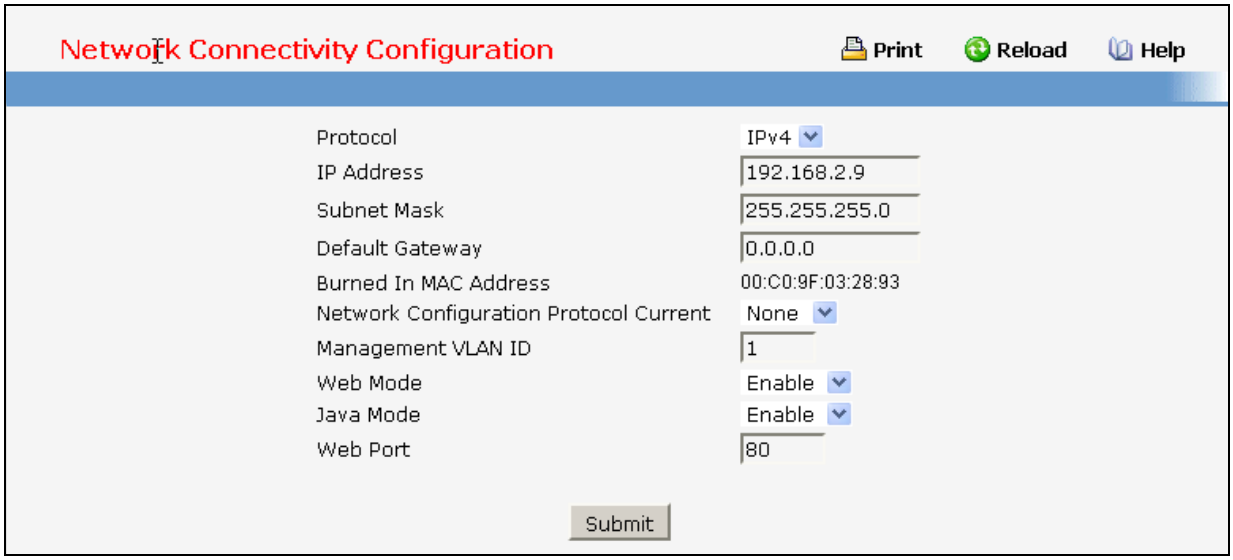
The network interface is the logical interface used for in-band connectivity with the switch via any of the switch's front panel ports. The configuration parameters associated with the switch's network interface do not affect the configuration of the front panel ports through which traffic is switched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

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**



Selection Criteria

Network Configuration Protocol Current - Specify what the switch should do following power-up: transmit a Bootp request, transmit a DHCP request, or do nothing (None). The factory default is None. You cannot make this choice for both the network configuration protocol and the service port. You will only be given the choices for Bootp or DHCP here if the service port protocol is configured to None.

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 enabled.

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

Management VLAN ID - Specifies the management VLAN ID of the switch. It may be configured to any value in the range of 1 - 3965. The management VLAN is used for management of the switch. This field is configurable for administrative users and read-only for other users.

Web Port - This field is used to set the HTTP Port Number. The value must be in the range of 1 to 65535. Port 80 is the default value. The currently configured value is shown when the web page is displayed.

Non-Configurable Data

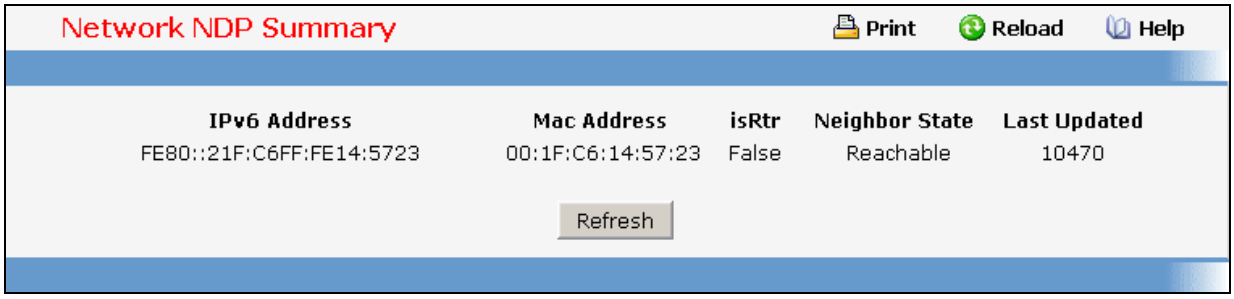
Burned-in MAC Address - The burned-in MAC address used for in-band connectivity if you choose not to configure a locally administered address.

Command Buttons

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

11.2.3.5 Configuring Network Connection NDP Summary Page

This screen displays IPv6 Network Port Neighbor entries.



Non-Configurable Data

IPv6 Address - The Ipv6 Address of a neighbor switch visible to the Network Port.

Mac Address - The Mac Address of the neighboring switch.

isRtr - true(1) if the neighbor machine is a router, false(2) otherwise.

Neighbor State - The state of the neighboring switch:

reachable(1) - The neighbor is reachable by this switch.

stale(2) - Information about the neighbor is scheduled for deletion.

delay(3) - No information has been received from neighbor during delay period.

robe(4) - Switch is attempting to probe for this neighbor.

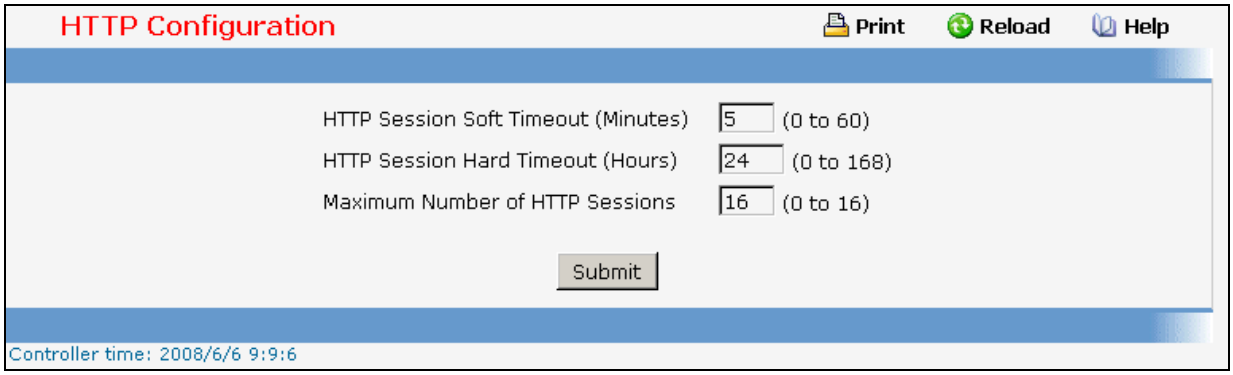
unknown(6) - Unknown status.

Last Updated - The last sysUpTime that this neighbor has been updated.

Command Buttons

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

11.2.3.6 HTTP Configuration



Configurable Data

HTTP Session Soft Timeout - This field is used to set the inactivity timeout for HTTP sessions. The value must be in the range of (0 to 60) minutes. A value of zero corresponds to an infinite timeout. The default value is 5 minutes. The currently configured value is shown when the web page is displayed.

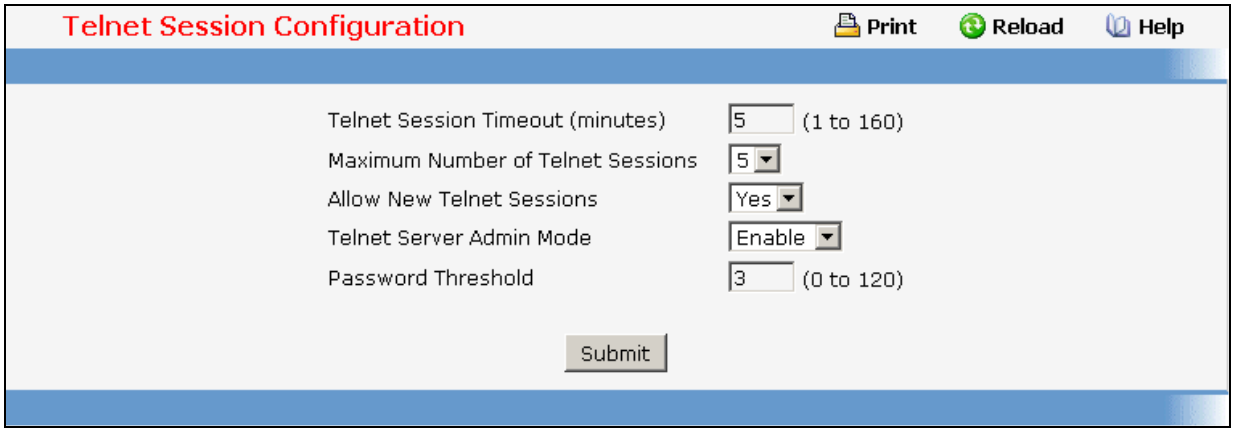
HTTP Session Hard Timeout - This field is used to set the hard timeout for HTTP sessions. This timeout is unaffected by the activity level of the session. The value must be in the range of (0 to 168) hours. A value of zero corresponds to an infinite timeout. The default value is 24 hours. The currently configured value is shown when the web page is displayed.

Maximum Number of HTTP Sessions - This field is used to set the maximum allowable number of HTTP sessions. The value must be in the range of (0 to 16). The default value is 16. 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.

11.2.3.7 Configuring Telnet Session Page



Selection Criteria

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 Server Admin Mode - Administrative mode for inbound telnet sessions. Setting this value to disable shuts down the telnet port. If the admin mode is set to disable, then all existing telnet connections are disconnected. The default value is Enable.

Configurable Data

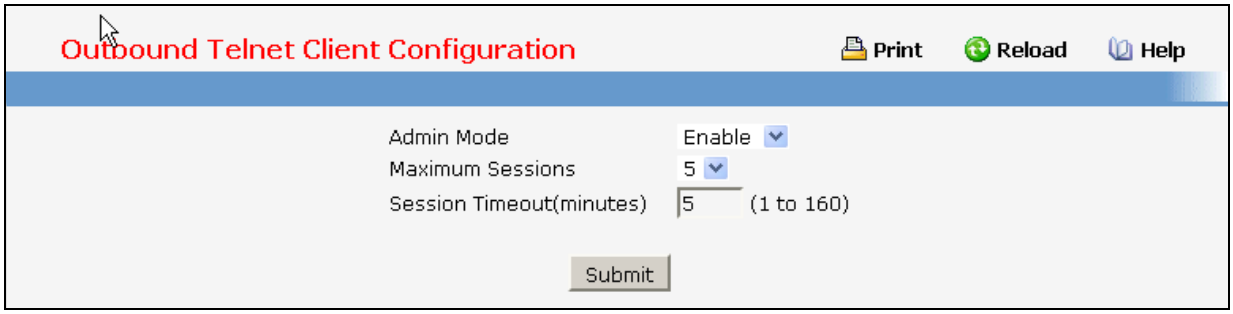
Telnet Session Timeout (minutes) - Specify how many minutes of inactivity should occur on a telnet session before the session is logged off. You may enter any number from 1 to 160. The factory default is 5.

Password Threshold - When the logon attempt threshold is reached on the console port, the system interface becomes silent for a specified amount of time before allowing the next logon attempt. (Use the silent time command to set this interval.) When this threshold is reached for Telnet, the Telnet logon interface closes. The default value is 3.

Command Buttons

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

11.2.3.8 Configuring Outbound Telnet Client Configuration Page



Selection Criteria

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).

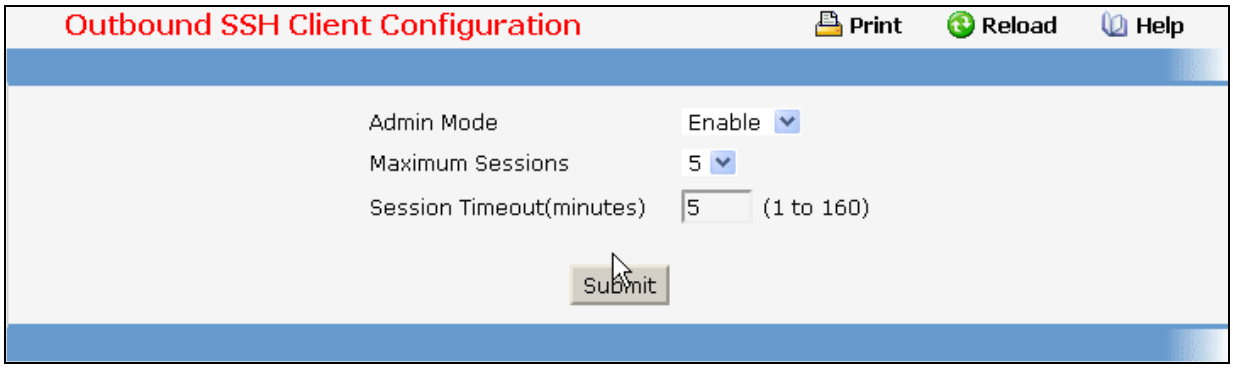
Configurable Data

Session Timeout - Specifies the Outbound Telnet login inactivity timeout. Default value is 5. Valid Range is (1 to 160).

Command Buttons

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

11.2.3.9 Configuring Outbound SSH Client Configuration Page



Selection Criteria

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).

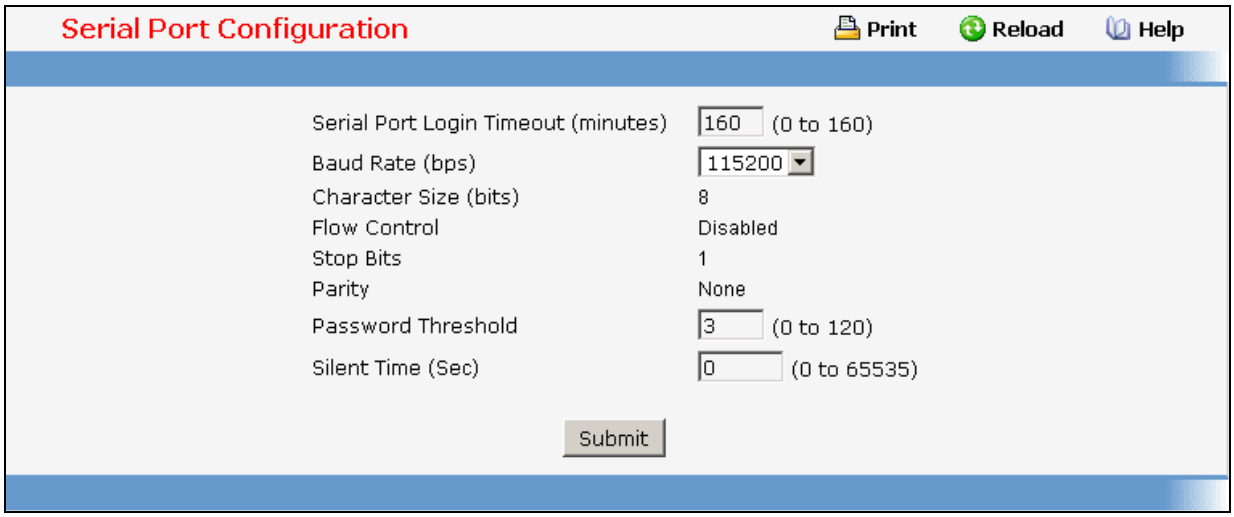
Configurable Data

Session Timeout - Specifies the Outbound Telnet login inactivity timeout. Default value is 5. Valid Range is (1 to 160).

Command Buttons

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

11.2.3.10 Configuring Serial Port Page



Selection Criteria

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 9600 baud.

Configurable Data

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.***

Password Threshold - When the logon attempt threshold is reached on the console port, the system interface becomes silent for a specified amount of time before allowing the next logon attempt. (Use the silent time command to set this interval.) When this threshold is reached for Telnet, the Telnet logon interface closes. The default value is 3.

Silent Time (Sec) - Use this command to set the amount of time the management console is inaccessible after the number of unsuccessful logon attempts exceeds the threshold set by the password threshold command. The default value is 0.

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.

Stop Bits - The number of stop bits per character. It is always 1.

Parity - The parity method used on the serial port. It is always None.

Command Buttons

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

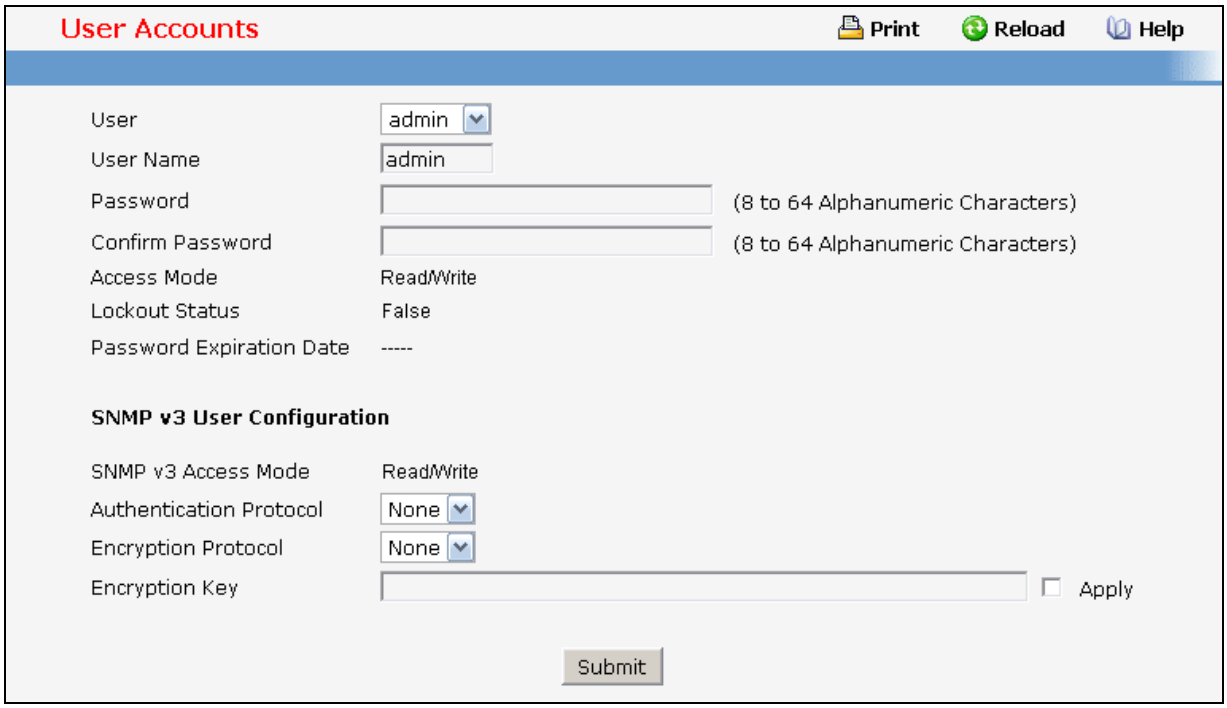
11.2.3.11 Defining User Accounts Page

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 (that is, 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 pulldown 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.

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.

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.

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 (*).

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 8 to 64 characters. 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.

Lockout Status - Indicates whether the user account is locked due to excessive failed login attempts. The threshold for number of attempts before lockout is specified by 'lockout attempts' on the password management page.

Password Expiration Date - Displays the date after which the user will be required to change passwords if password aging is enabled.

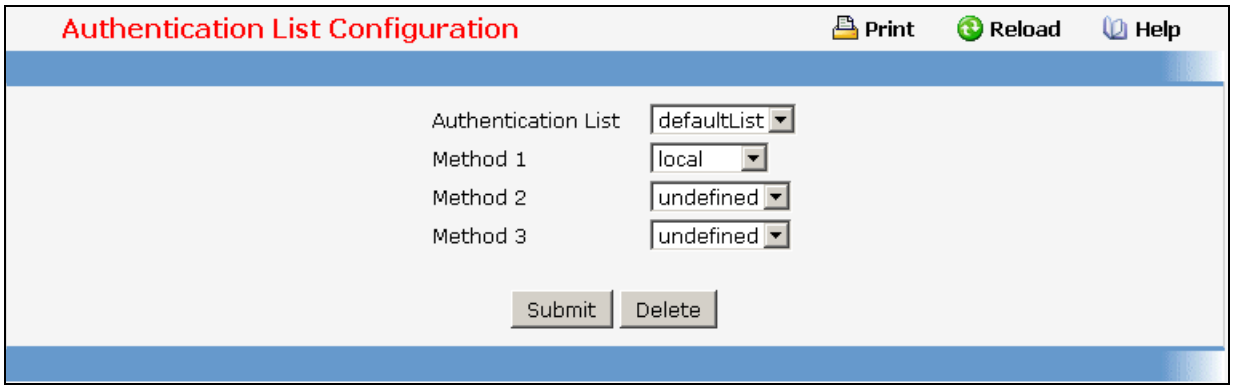
Command Buttons

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 currently selected user account. If you want the switch to retain the new values across a power cycle, you must perform a save. This button is only visible when you have selected a user account with 'Read Only' access. You cannot delete the 'Read/Write' user.

11.2.3.12 Defining Authentication List Configuration Page

You 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.

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

Tacacs- the user's ID and password will be authenticated using the TACACS 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.

Configurable Data

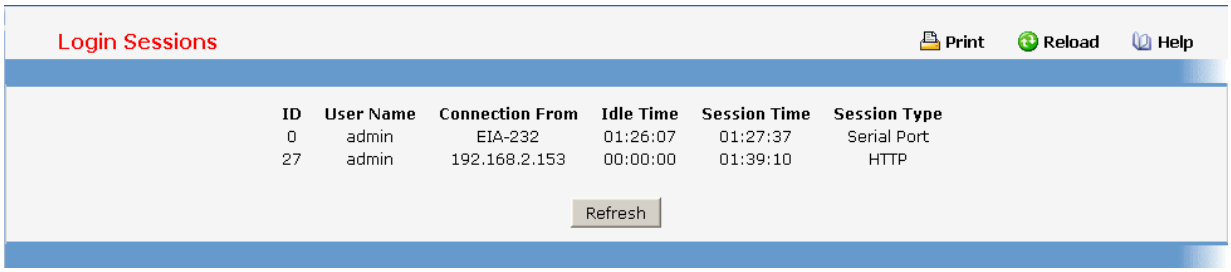
Authentication List Name - If you are creating a new login list, enter the name you want to assign. It can be up to 15 alphanumeric characters and is not case sensitive.

Command Buttons

Submit - Sends the updated screen to the switch and causes the changes to take effect on the switch. These changes will not be retained across a power cycle unless you perform a save.

Delete - Remove the selected authentication login list from the configuration. The delete will fail if the selected login list is assigned to any user (including the default user) for system login or IEEE 802.1x port access control. You can only use this button if you have Read/Write access. The change will not be retained across a power cycle unless you perform a save.

11.2.3.13 Viewing Login Session Page



Non-Configurable Data

ID - Identifies the ID of this row.

User Name - Shows the user name of user who made the session.

Connection From - Shows the IP from which machine the user is connected.

Idle Time - Shows the idle session time.

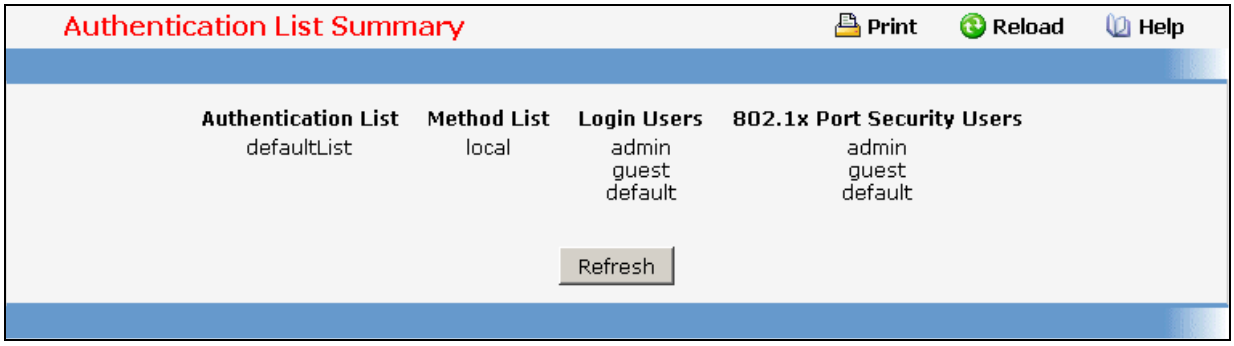
Session Time - Shows the total session time.

Session Type – Shows the type of session: telnet, serial or SSH.

Command Buttons

Refresh - Update the information on the page.

11.2.3.14 Viewing Authentication List Summary Page



Non-Configurable Data

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.

Command Buttons

Refresh - Update the information on the page.

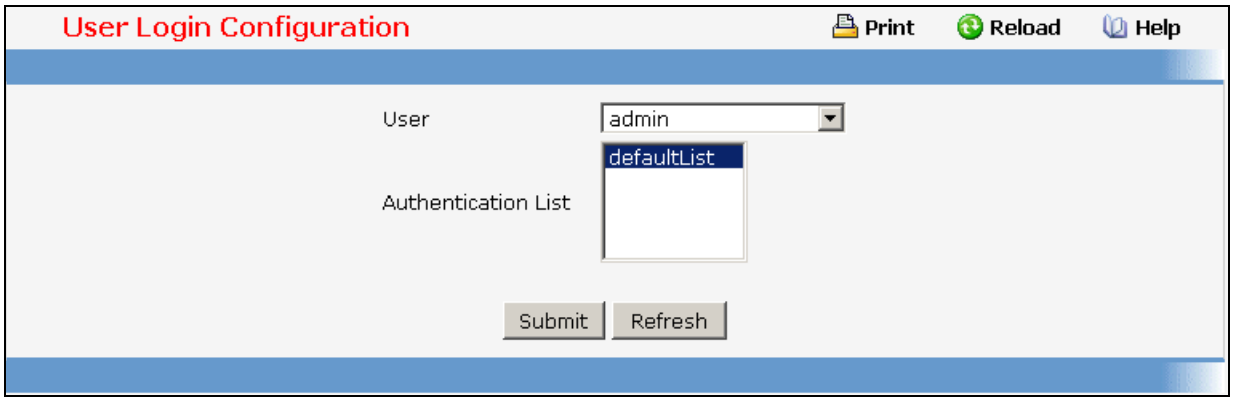
11.2.3.15 Defining User Login Page

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.

This page provides a user account (from those already created) to be added into the Authentication List.



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

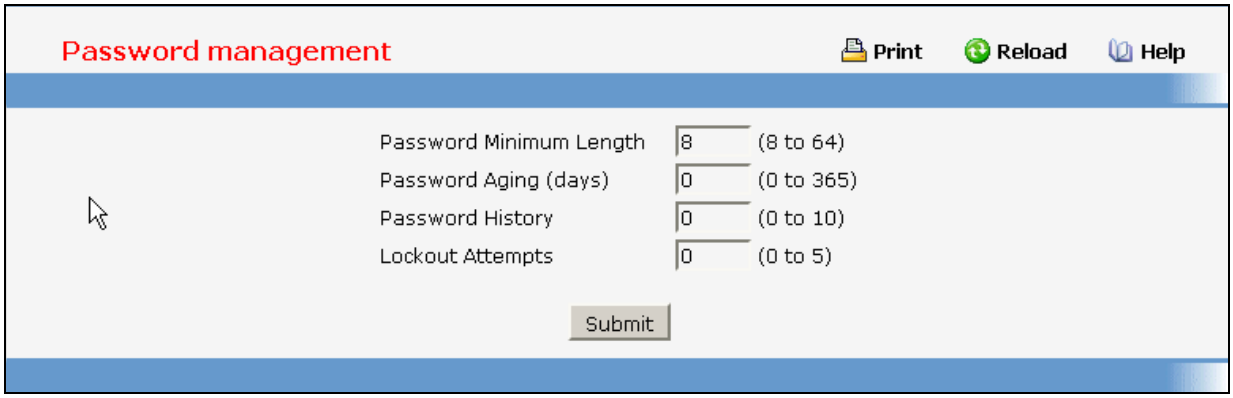
Authentication List - Select the authentication login list you want to assign to the user for system login.

Command Buttons

Submit - Sends the updated screen to the switch and causes the changes to take effect on the switch. These changes will not be retained across a power cycle unless you perform a save.

Refresh - Updates the information on the page.

11.2.3.16 Defining Password Management



Configurable Data

Password Minimum Length - All new local user passwords must be at least this many characters in length.

Password Aging (days) - The maximum time that user passwords are valid, in days, from the time the password is set. Once a password expires, the user will be required to enter a new password following the first login after password expiration. A value of 0 indicates that passwords never expire.

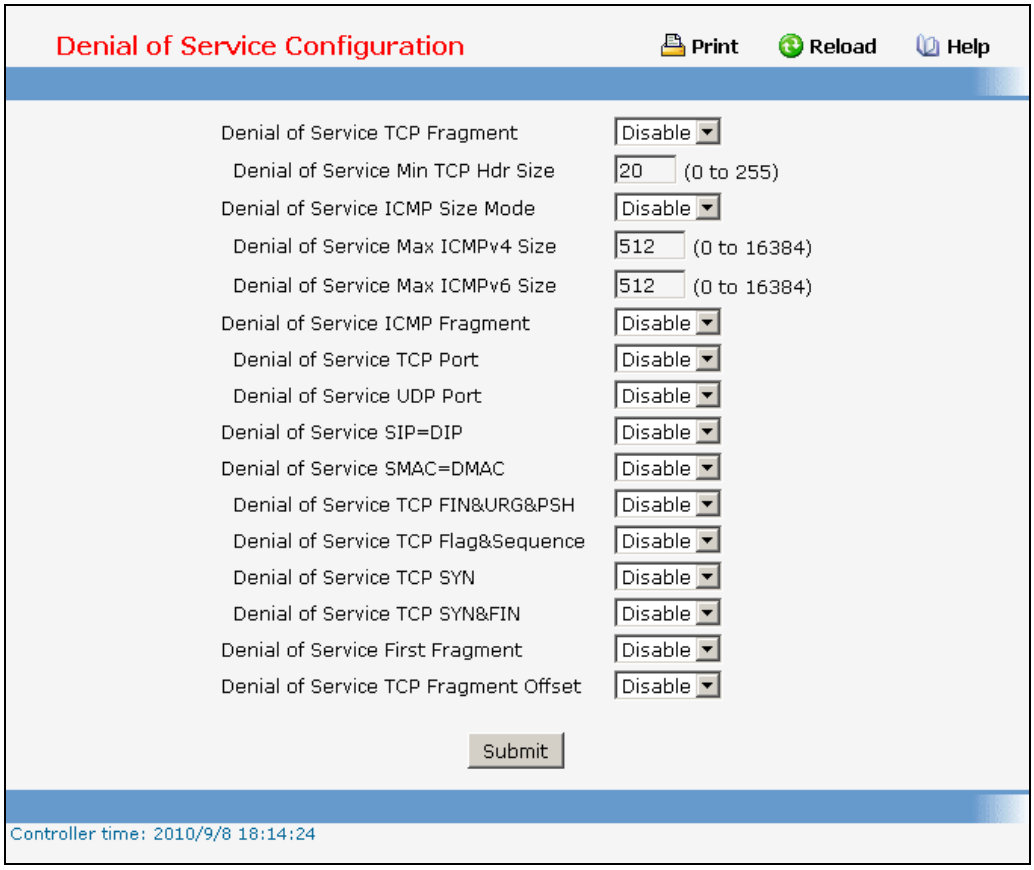
Password History - The number of previous passwords to store for prevention of password reuse. This ensures that each user does not reuse passwords often. A value of 0 indicates that no previous passwords will be stored.

Lockout Attempts - The number of allowable failed local authentication attempts before the user's account is locked. A value of 0 indicates that user accounts will never be locked.

Command Buttons

Submit - Send the updated screen to the switch and cause the changes to take effect on the switch. These changes will not be retained across a power cycle unless you perform a save.

11.2.3.17 Defining Denial Of Service Page



Selection Criteria

TCP Fragment - Enable or disable this option by selecting the corresponding line on the pulldown entry field. Enabling TCP Fragment DoS prevention causes the switch to drop packets that have a TCP header smaller then the configured Min TCP Hdr Size. The factory default is disabled.

ICMP - Enable or disable this option by selecting the corresponding line on the pulldown entry field. Enabling ICMP DoS prevention causes the switch to drop ICMP packets that have a type set to ECHO_REQ (ping) and a size greater than the configured ICMP Pkt Size. The factory default is disabled.

ICMP Fragment - Enable or disable this option by selecting the corresponding line on the pulldown entry field. Enabling ICMP Fragment DoS prevention causes the switch to drop ICMP Fragmented packets. The factory default is disabled.

TCP Port - Enable or disable this option by selecting the corresponding line on the pulldown entry field. Enabling TCP Port DoS prevention causes the switch to drop packets that have TCP source port equal to TCP destination port. The factory default is disabled.

UDP Port - Enable or disable this option by selecting the corresponding line on the pulldown entry field. Enabling UDP Port DoS prevention causes the switch to drop packets that have UDP source port equal to UDP destination port. The factory default is disabled.

SIP=DIP - Enable or disable this option by selecting the corresponding line on the pulldown entry field. Enabling SIP=DIP DoS prevention causes the switch to drop packets that have a source IP address equal to the destination IP address. The factory default is disabled.

SMAC=DMAC - Enable or disable this option by selecting the corresponding line on the pulldown entry field. Enabling SMAC=DMAC DoS prevention causes the switch to drop packets that have a source MAC address equal to the destination MAC address. The factory default is disabled.

TCP FIN&URG&PSH - Enable or disable this option by selecting the corresponding line on the pulldown entry field. Enabling TCP FIN & URG & PSH DoS prevention causes the switch to drop

packets that have TCP Flags FIN, URG, and PSH set and TCP Sequence Number=0. The factory default is disabled.

TCP Flag&Sequence - Enable or disable this option by selecting the corresponding line on the pulldown entry field. Enabling TCP Flag DoS prevention causes the switch to drop packets that have TCP control flags set to 0 and TCP sequence number set to 0. The factory default is disabled.

TCP SYN - Enable or disable this option by selecting the corresponding line on the pulldown entry field. Enabling TCP SYN DoS prevention causes the switch to drop packets that have TCP Flags SYN set. The factory default is disabled.

TCP SYN&FIN - Enable or disable this option by selecting the corresponding line on the pulldown entry field. Enabling TCP SYN & FIN DoS prevention causes the switch to drop packets that have TCP Flags SYN and FIN set. The factory default is disabled.

First Fragment - Enable or disable this option by selecting the corresponding line on the pulldown entry field. Enabling First Fragment DoS prevention causes the switch to drop packets that have a More fragment equal to 1 and coorperate with other DoS options. The factory default is disabled.

TCP Offset - Enable or disable this option by selecting the corresponding line on the pulldown entry field. Enabling TCP Offset DoS prevention causes the switch to drop packets that have a TCP header Offset=1. The factory default is disabled.

Configurable Data

Min TCP Hdr Size - Specify the Min TCP Hdr Size allowed. If First Fragment DoS prevention is enabled, the switch will drop packets that have a TCP header smaller then this configured Min TCP Hdr Size. The factory default value is 20.

Max ICMPv4 Pkt Size - Specify the Max ICMPv4 Pkt Size allowed. If ICMP DoS prevention is enabled, the switch will drop IPv4 ICMP ping packets that have a size greater then this configured Max ICMP Pkt Size. The factory default value is 512.

Max ICMPv6 Pkt Size - Specify the Max IPv6 ICMP Pkt Size allowed. If ICMP DoS prevention is enabled, the switch will drop IPv6 ICMP ping packets that have a size greater then this configured Max ICMP Pkt Size. The factory default value is 512.

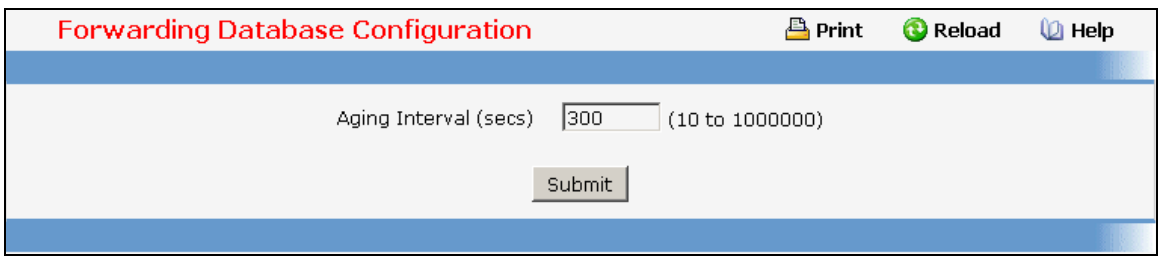
Command Buttons

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

11.2.4 Defining Forwarding Database

11.2.4.1 Configuring MAC Table aging interval time Page

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



Configurable Data

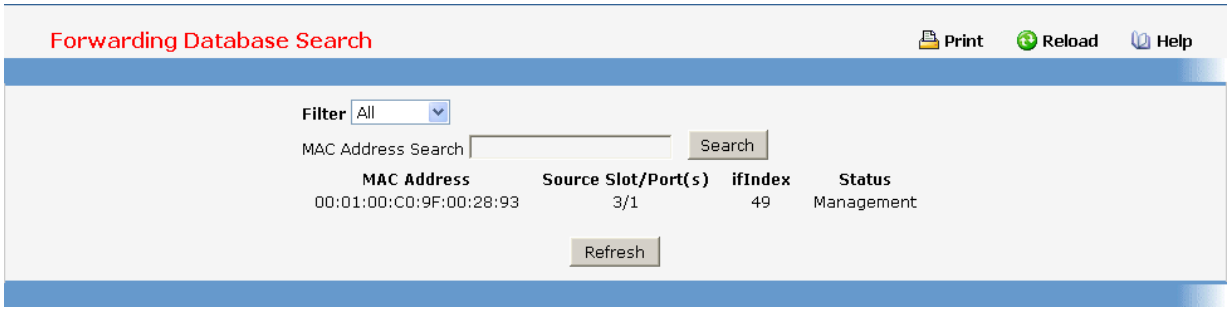
Aging Interval(secs) - The forwarding database contains static entries, which are never aged out, and dynamically learned entries, which are removed if they are not updated within a given time. You specify that time by entering a value for the Address Ageing Timeout. You may enter any number of seconds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

Command Buttons

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

11.2.4.2 Viewing Forwarding Database Page

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.



Selection Criteria

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.

Configurable Data

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.

Non-Configurable Data

MAC Address - A unicast MAC address for which the switch has forwarding and/or filtering information. The format is a two byte hexadecimal VLAN ID number followed by a six byte MAC address with each byte 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.

Source Slot/Port - the port where this address was learned -- that is, the port through which the MAC address can be reached.

ifIndex - The ifIndex of the MIB interface table entry associated with the source port.

Status - The status of this entry. The possible values are:

Static: the entry was added when a static MAC filter was defined.

Learned: the entry was learned by observing the source MAC addresses of incoming traffic, and is currently in use.

Management: the system MAC address, which is identified with interface 0.1.

Self: the MAC address of one of the switch's physical interfaces.

Command Buttons

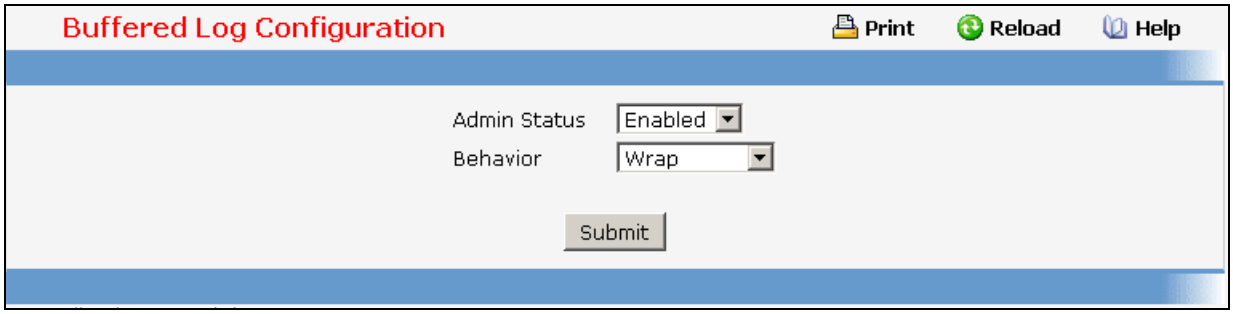
Search - Search for the specified MAC address.

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

11.2.5 Viewing Logs

11.2.5.1 Viewing Buffered Log Configuration Page

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.



Selection Criteria

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.

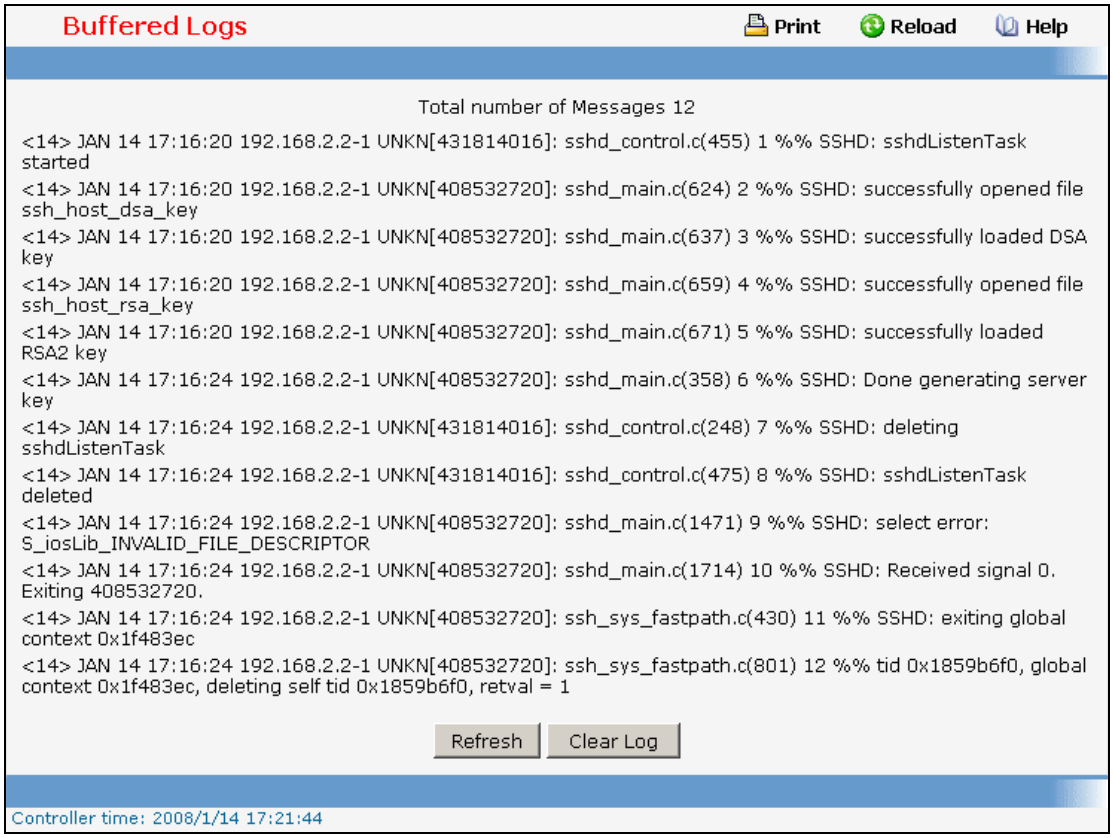
Behavior - Indicates the behavior of the log when it is full. It can either wrap around or stop when the log space is filled.

Command Buttons

Submit - Update the switch with the values you entered.

11.2.5.2 Viewing Buffered Log Page

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

<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.

Note for buffered log

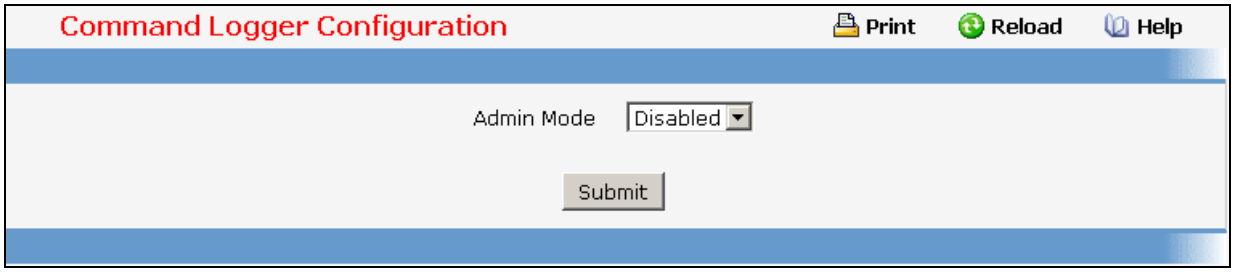
Number of log messages displayed: For the buffered log, only the latest 128 entries are displayed on the webpage

Command Buttons

Refresh - Refresh the page with the latest log entries.

Clear Log - Clear all entries in the log.

11.2.5.3 Configuring Command Logger Page



Selection Criteria

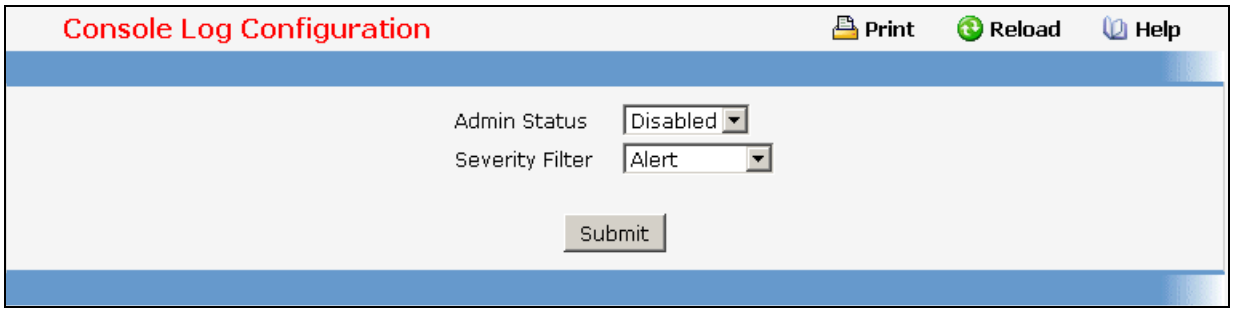
Admin Mode - Enable/Disable the operation of the CLI Command logging by selecting the corresponding pulldown field and clicking Submit.

Command Buttons

Submit - Update the switch with the values you entered.

11.2.5.4 Configuring Console Log Page

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



Selection Criteria

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

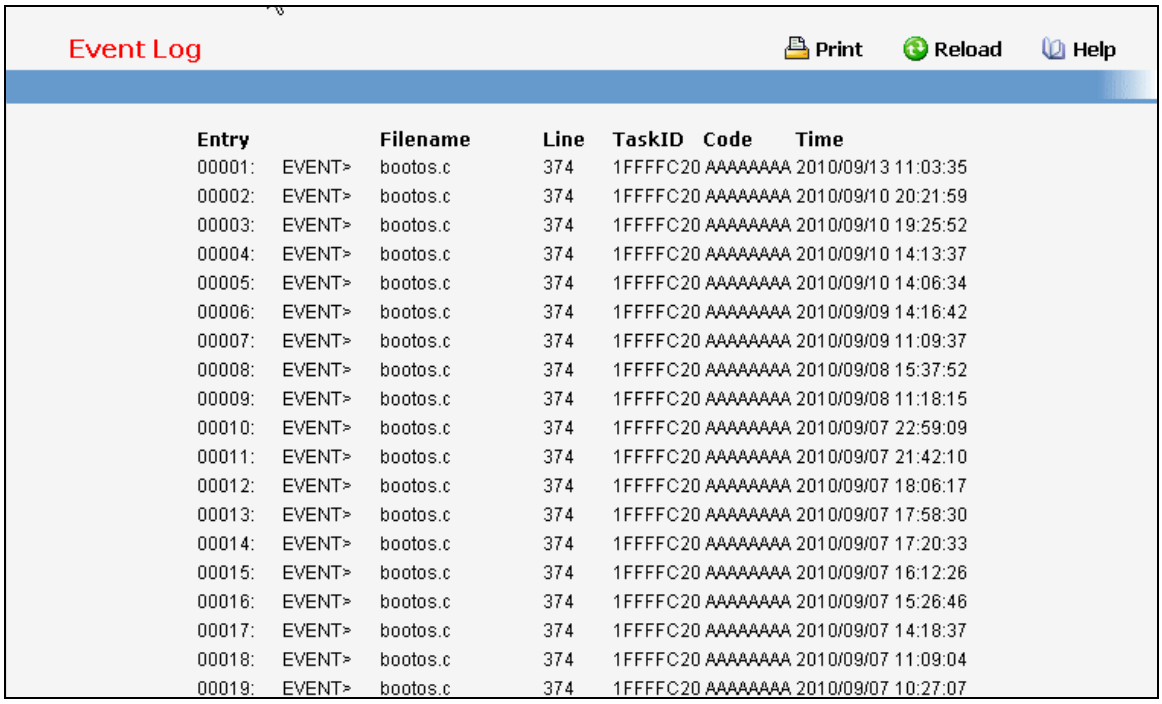
- Info (6): informational messages
- Debug(7): debug-level messages

Command Buttons

Submit - Update the switch with the values you entered.

11.2.5.5 Viewing Event Log Page

Use this panel to display the event log, which is used to hold error messages for catastrophic events. After the event is logged and the updated log is saved in FLASH memory, the switch will be reset. The log can hold at least 2,000 entries (the actual number depends on the platform and OS), and is erased when an attempt is made to add an entry after it is full. The event log is preserved across system resets.



Entry		Filename	Line	TaskID	Code	Time
00001:	EVENT>	bootos.c	374	1FFFFC20	AAAAAAAA	2010/09/13 11:03:35
00002:	EVENT>	bootos.c	374	1FFFFC20	AAAAAAAA	2010/09/10 20:21:59
00003:	EVENT>	bootos.c	374	1FFFFC20	AAAAAAAA	2010/09/10 19:25:52
00004:	EVENT>	bootos.c	374	1FFFFC20	AAAAAAAA	2010/09/10 14:13:37
00005:	EVENT>	bootos.c	374	1FFFFC20	AAAAAAAA	2010/09/10 14:06:34
00006:	EVENT>	bootos.c	374	1FFFFC20	AAAAAAAA	2010/09/09 14:16:42
00007:	EVENT>	bootos.c	374	1FFFFC20	AAAAAAAA	2010/09/09 11:09:37
00008:	EVENT>	bootos.c	374	1FFFFC20	AAAAAAAA	2010/09/08 15:37:52
00009:	EVENT>	bootos.c	374	1FFFFC20	AAAAAAAA	2010/09/08 11:18:15
00010:	EVENT>	bootos.c	374	1FFFFC20	AAAAAAAA	2010/09/07 22:59:09
00011:	EVENT>	bootos.c	374	1FFFFC20	AAAAAAAA	2010/09/07 21:42:10
00012:	EVENT>	bootos.c	374	1FFFFC20	AAAAAAAA	2010/09/07 18:06:17
00013:	EVENT>	bootos.c	374	1FFFFC20	AAAAAAAA	2010/09/07 17:58:30
00014:	EVENT>	bootos.c	374	1FFFFC20	AAAAAAAA	2010/09/07 17:20:33
00015:	EVENT>	bootos.c	374	1FFFFC20	AAAAAAAA	2010/09/07 16:12:26
00016:	EVENT>	bootos.c	374	1FFFFC20	AAAAAAAA	2010/09/07 15:26:46
00017:	EVENT>	bootos.c	374	1FFFFC20	AAAAAAAA	2010/09/07 14:18:37
00018:	EVENT>	bootos.c	374	1FFFFC20	AAAAAAAA	2010/09/07 11:09:04
00019:	EVENT>	bootos.c	374	1FFFFC20	AAAAAAAA	2010/09/07 10:27:07

Non-Configurable Data

Entry - The number of the entry within the event log. The most recent entry is first.

Filename - The FASTPATH source code filename identifying the code that detected the event.

Line - The line number within the source file of the code that detected the event.

Task ID - The OS-assigned ID of the task reporting the event.

Code - The event code passed to the event log handler by the code reporting the event.

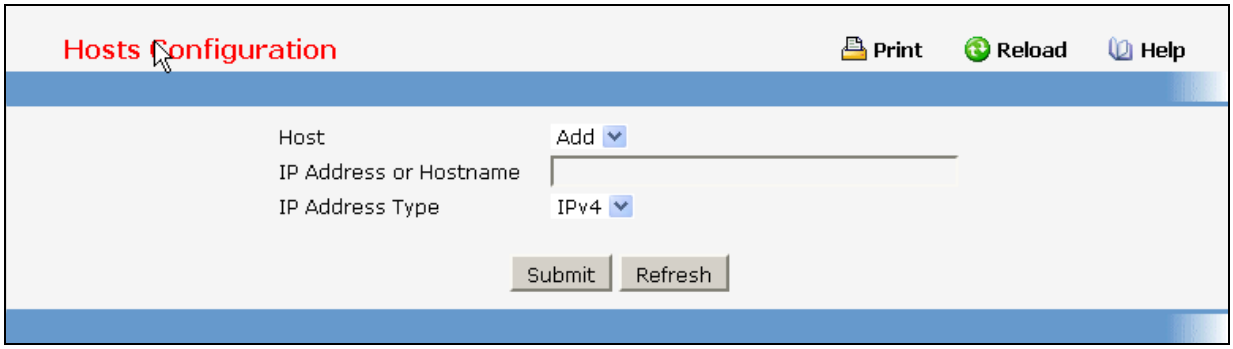
Time - The time the event occurred, measured from the previous reset.

Command Buttons

Refresh - Update the information on the page.

Clear Log - Remove all log information.

11.2.5.6 Configuring Hosts configuration Page



Selection Criteria

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.

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

Configurable Data

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. Specify the port in the text field.

Non-Configurable Data

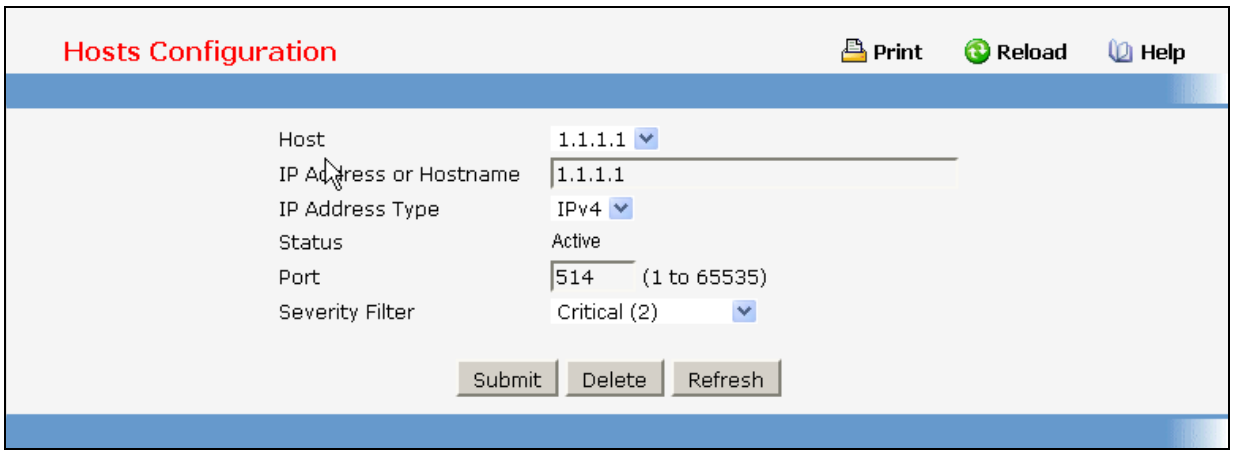
Status -This specifies wether the host has been configured to be actively logging or not.

Command Buttons

Submit - Update the switch with the values you entered.

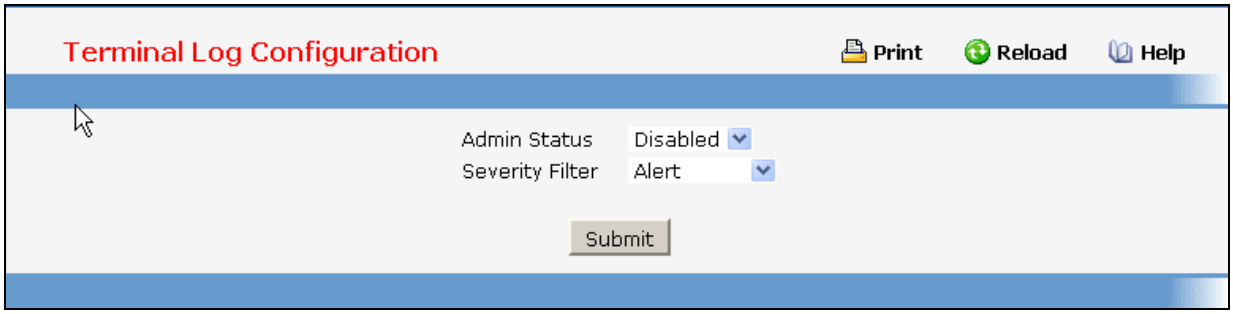
Refresh - Refetch the database and display it again starting with the first entry in the table.

Delete - Delete a configured host.



11.2.5.7 Configuring Terminal Log Configuration Page

This allows logging to any terminal client connected to the switch via telnet or SSH. To receive the log messages, terminals have to enable "terminal monitor" via CLI command.



Selection Criteria

Admin Status -A log that is "Disabled" shall not log messages to connected terminals. A log that is "Enabled" shall log messages to connected terminals. 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:

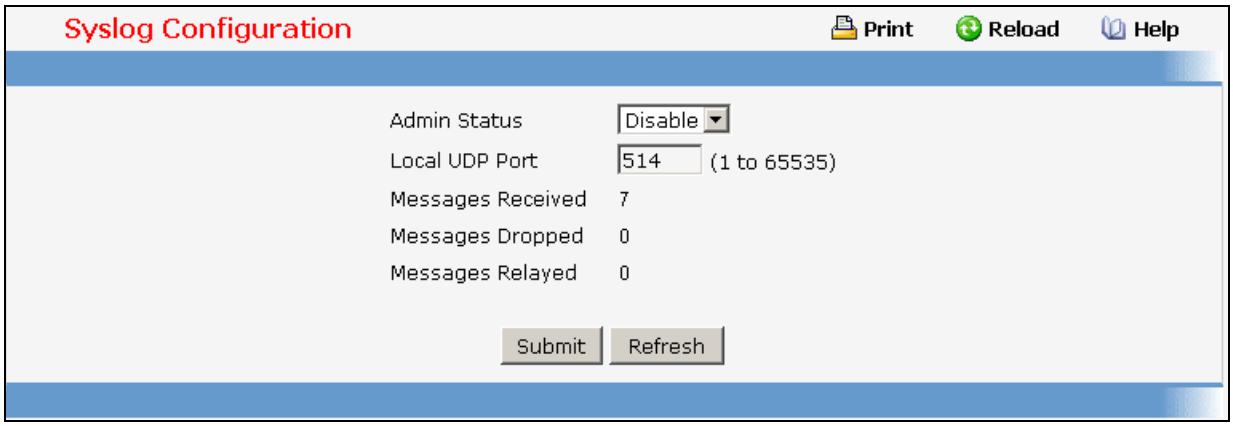
- Emergency (0): system is unusable
- Alert (1): action must be taken immediately
- Critical (2): critical conditions
- Error (3): error conditions
- Warning (4): warning conditions
- Notice(5): normal but significant conditions

- Informational(6): informational messages
- Debug(7): debug-level messages

Command Buttons

Submit - Update the switch with the values you entered.

11.2.5.8 Configuring syslog configuration Page



Selection Criteria

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.

Configurable Data

Local UDP Port This is the port on the local host from which syslog messages are sent. The default port is 514. Specify the local port in the text field.

Non-Configurable Data

Messages Received - The number of messages received by the log process. This includes messages that are dropped or ignored.

Messages Dropped - The number of messages that could not be processed due to error or lack of resources.

Messages Relayed - The number of messages forwarded by the syslog function to a syslog host. Messages forwarded to multiple hosts are counted once for each host.

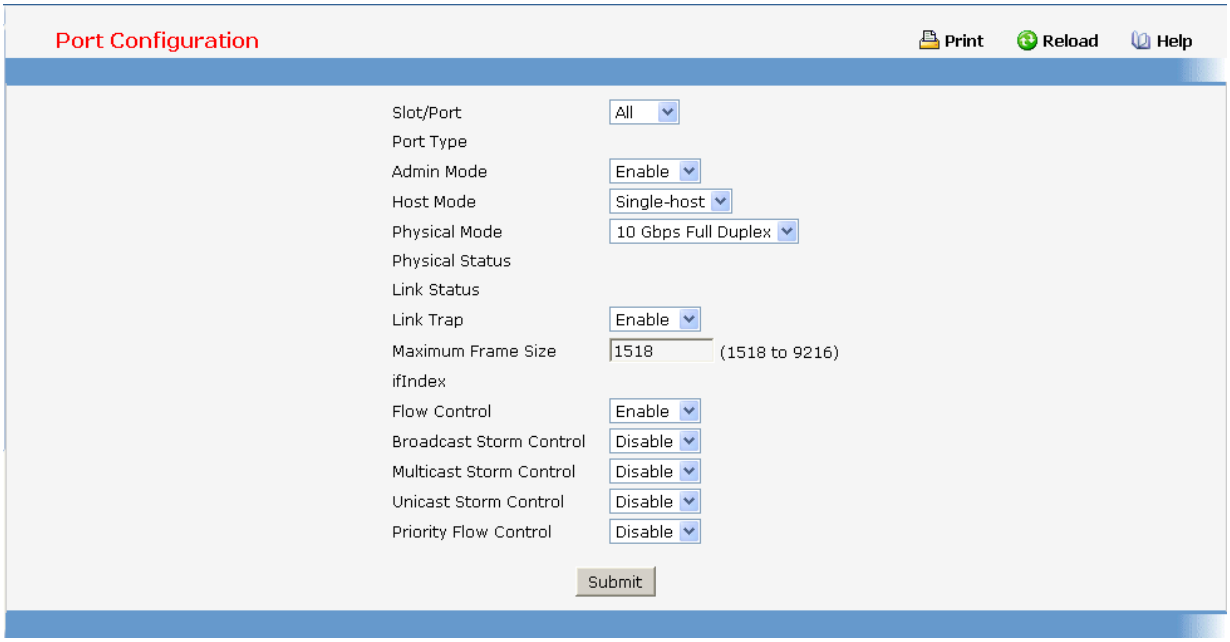
Command Buttons

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.

11.2.6 Managing Switch Interface

11.2.6.1 Configuring Switch Interface Page



Selection Criteria

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

Admin Mode - Use the pulldown 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 pulldown entry field. The factory default is enabled.

Host Mode - Selects the dot1x protocol host type. Single-host means accept only one user on this port. Multi-host means accept multi users on this port.

Physical Mode - Use the pulldown 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.

Flow Control - Used to enable or disable flow control feature on the selected interface.

Broadcast Storm Control - Used to enable or disable the broadcast storm feature on the selected interface. The broadcast storm control value can be set to Level 1, Level 2, Level 3, and Level 4.

The following description is for the broadcast storm, multicast storm, and unicast storm control.

The actual packet rate for switch will convert from the input level and the speed of that interface. (see table 1 and table 2)

Table 1. For 10/100Mbps/1Gbps		Table 2. For 10Gbps	
Level	**Packet Rate (pps)**	**Level**	**Packet Rate (pps)**
1	64	**1**	1042
2	128	**2**	2048
3	256	**3**	3124
4	512	**4**	4167

Multicast Storm Control - Used to enable or disable the multicast storm feature on the selected interface. Multicast storm control value could be set Level 1, Level 2, Level 3, and Level 4.

Unicast Storm Control - Used to enable or disable unicast storm feature on the selected interface. Unicast storm control value could be set Level 1, Level 2, Level 3, and Level 4.

Priority Flow Control - Used to enable or disable Priority flow control feature on the selected interface.

Configurable Data

Maximum Frame Size - The maximum Ethernet frame size the interface supports or is configured, including Ethernet header, CRC, and payload. (1518 to 9216). The default maximum frame size is 1518.

Capability - You could advertise the port capabilities of a given interface during auto-negotiation.

Port Description - The description for the port. The max length of the description is 64.

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.

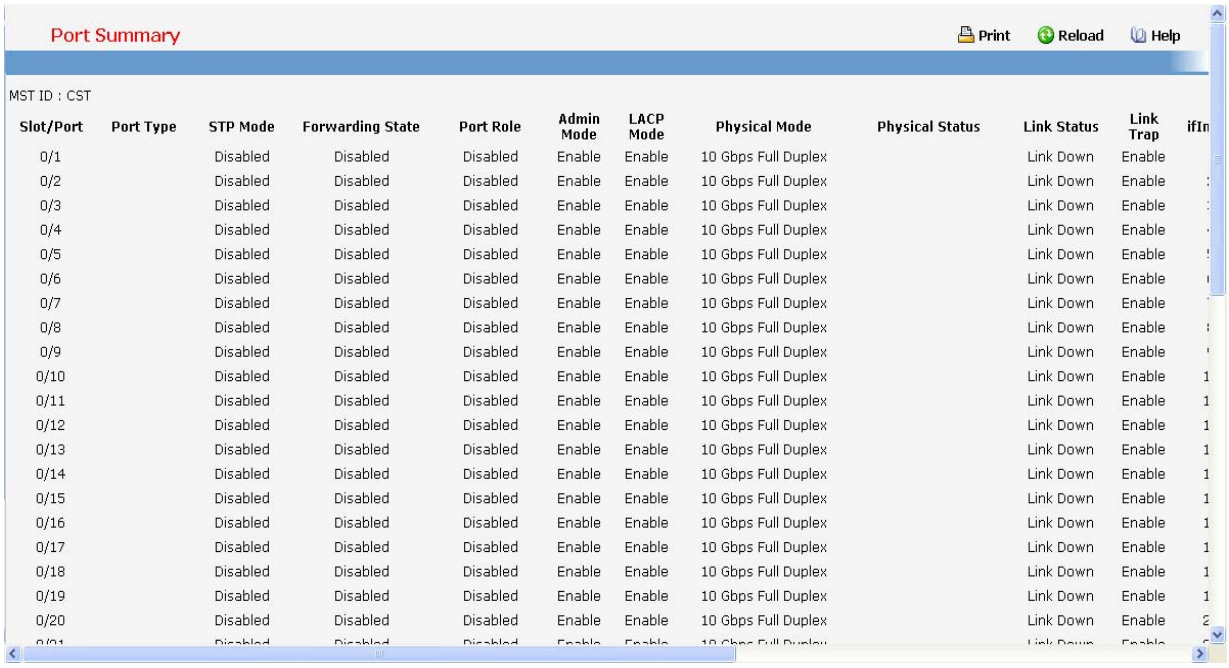
ifIndex - The ifIndex of the interface table entry associated with this port.

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.

11.2.6.2 Viewing Switch Interface Configuration Page

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



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.

Flow Control - Indicates the status of flow control on this port.

Packet Burst - Indicates the packet burst used in the rate limit function if the rate limit admin mode is enabled.

Broadcast Storm Control - Indicates the status of the broadcast storm control, disable or Level 1, Level 2, Level 3, Level 4.

Multicast Storm Control - Indicates the status of the multicast storm control, disable or Level 1, Level 2, Level 3, Level 4.

Unicast Storm Control - Indicates the status of the unicast storm control, disable or Level 1, Level 2, Level 3, Level 4.

Priority Flow Control - Indicates the status of the Priority flow control feature.

Capability - Indicates the port capabilities during auto-negotiation.

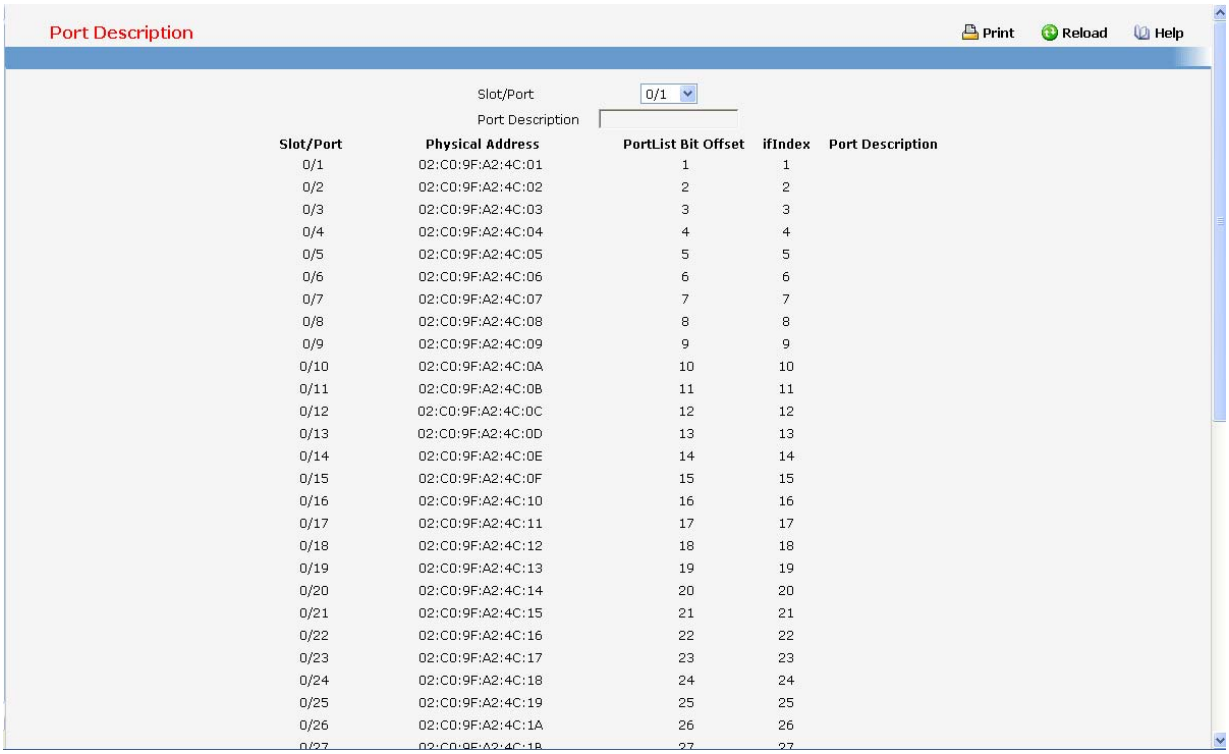
Port Description - The description for the port.

Command Buttons

Refresh – Refresh the configuration value again.

11.2.6.3 Configuring Port Description Function Page

This screen configures and displays the description for all ports in the box.



Selection Criteria

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

Configurable Data

Port Description Enter the Description string to be attached to a port. It can be up to 64 characters in length.

Non-Configurable Data

Slot/Port - Identifies the port

Physical Address - Displays the physical address of the specified interface.

PortList Bit Offset - Displays the bit offset value which corresponds to the port when the MIB object type PortList is used to manage in SNMP.

IfIndex - Displays the interface index associated with the port.

Port Desciption - Description string attached to a port. It can be of up to 64 characters in length.

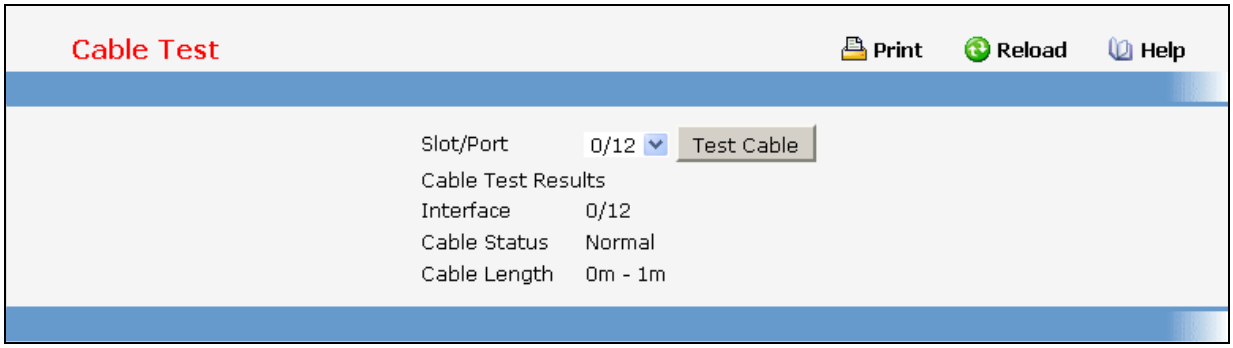
Command Buttons

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

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

11.2.6.4 Configuring Cable Test Function Page

⚠ Below 10-Giga Interface doesn't have this feature



Selection Criteria

Slot/Port - This field indicates the interface to which the cable to be tested is connected.

Non-Configurable Data

Interface - Displays the interface tested in the Slot/Port notation. This field is displayed after the "Test Cable" button has been clicked and results are available. This field is not visible when the page is initially displayed.

Cable Status - This displays the cable status as Normal, Open or Short.

Normal: the cable is working correctly.

Open: the cable is disconnected or there is a faulty connector.

Short: there is an electrical short in the cable.

Cable Test Failed: The cable status could not be determined. The cable may in fact be working. This field is displayed after the "Test Cable" button has been clicked and results are available. This field is not visible when the page is initially displayed.

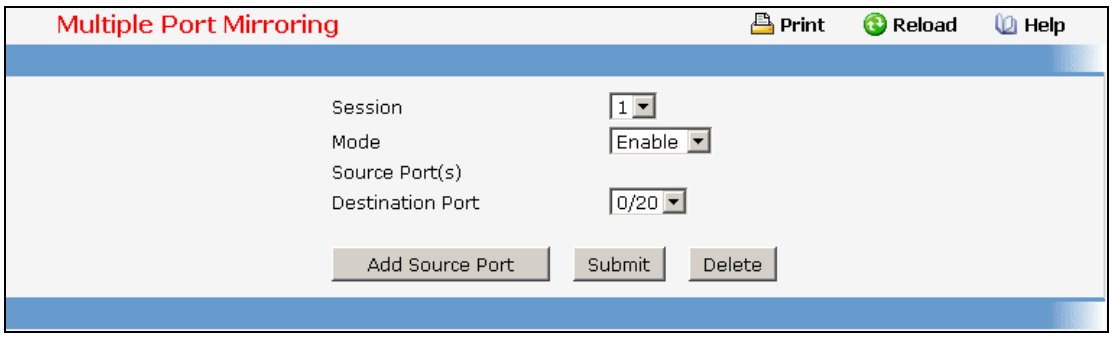
Cable Length - The estimated length of the cable in meters. The length is displayed as a range between the shortest estimated length and the longest estimated length. Unknown is displayedif the cable length could not be determined. The Cable Length is only displayed if the cable status is Normal. This field is displayed after the "Test Cable" button has been clicked and results are available. This field is not visible when the page is initially displayed.

Failure Location - The estimated distance in meters from the end of the cable to the failure location. The failure location is only displayed if the cable status is Open or Short. This field is displayed after the "Test Cable" button has been clicked and results are available. This field is not visible when the page is initially displayed.

Command Buttons

Test Cable - Perform a cable test on the selected interface. The cable test may take up to 2 seconds to complete. If the port has an active link then the link is not taken down and the cable status is always "Normal". The command returns a cable length estimate if this feature is supported by the PHY for the current link speed. Note that if the link is down and a cable is attached to a 10/100 Ethernet adapter then the cable status may be "Open" or "Short" because some Ethernet adapters leave unused wire pairs unterminated or grounded.

11.2.6.5 Configuring Multiple Port Mirroring Function Page



Selection Criteria

Session - Select a port mirroring session from the list. The number of sessions allowed is platform specific. By default the First Session is selected. Up to 1 sessions are supported.

Mode - Specifies the Session Mode for a selected session ID. The default Session Mode is disabled.

Destination Port - Acts as a probe port and will receive all the traffic from configured mirrored port(s). Default value is blank.

Configurable Data

Source Port(s) - Specifies the source port(s) with directions as mirrored port(s). Traffic of the source port(s) is sent to the probe port. Up to 20 source ports can be selected per session.

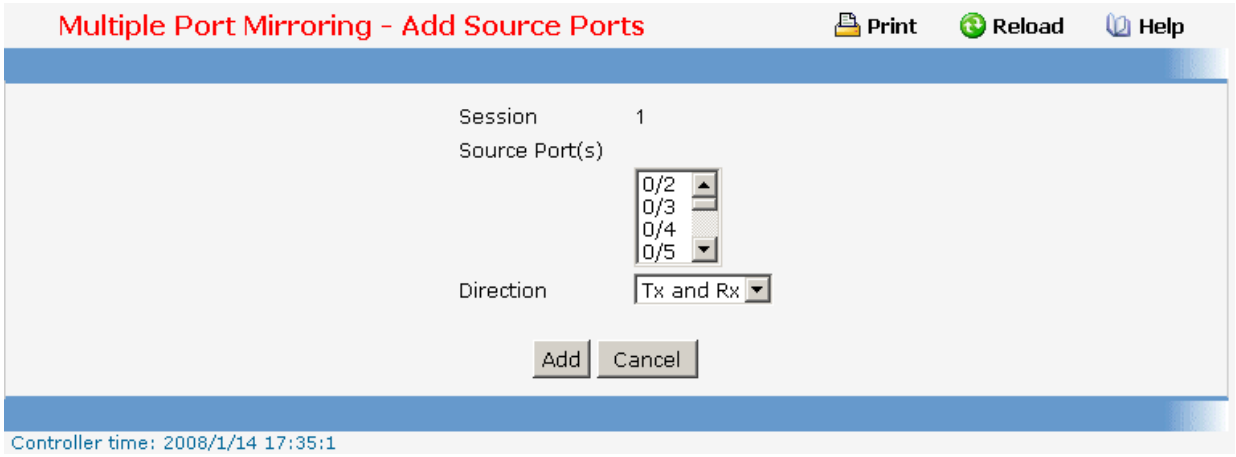
Command Buttons

Add Source Ports - To add Source Port(s) to the selected session.

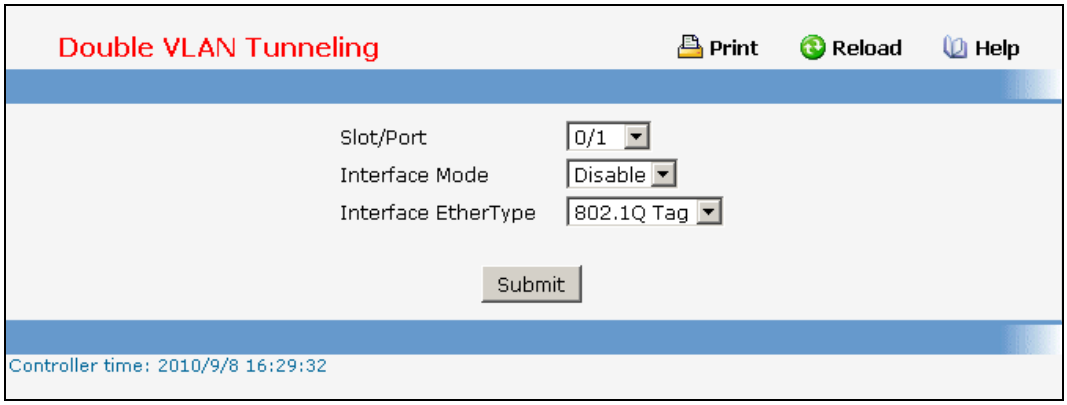
Remove Source Ports - To remove the configured Source Port(s) of the selected session.

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

Delete - Remove the selected session configuration.



11.2.6.6 Configuring Double VLAN Tunneling Function Page



Selection Criteria

Slot/Port - Select the physical interface for which you want to display or configure data.

Configurable Data

Interface Mode - This specifies the administrative mode via which Double VLAN Tagging can be enabled or disabled. The default value for this is Disabled.

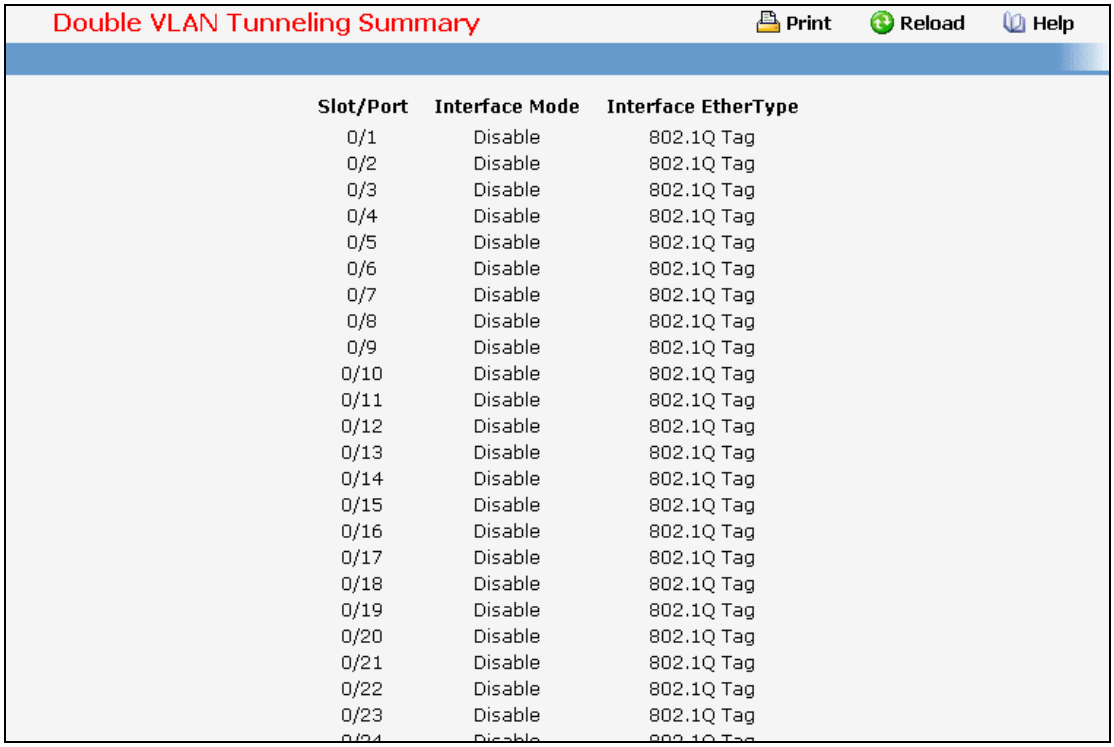
Interface EtherType - The two-byte hex EtherType to be used as the first 16 bits of the DVlan tag.

- ***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.

11.2.6.7 Configuring Double VLAN Tnuueling Summary Function Page



Non-Configurable Data

Slot/Port - The physical interface for which data is being displayed.

Interface Mode - This specifies the administrative mode via which Double VLAN Tagging can be enabled or disabled. The default value for this is Disabled.

Interface EtherType - The two-byte hex EtherType to be used as the first 16 bits of the DVlan tag.

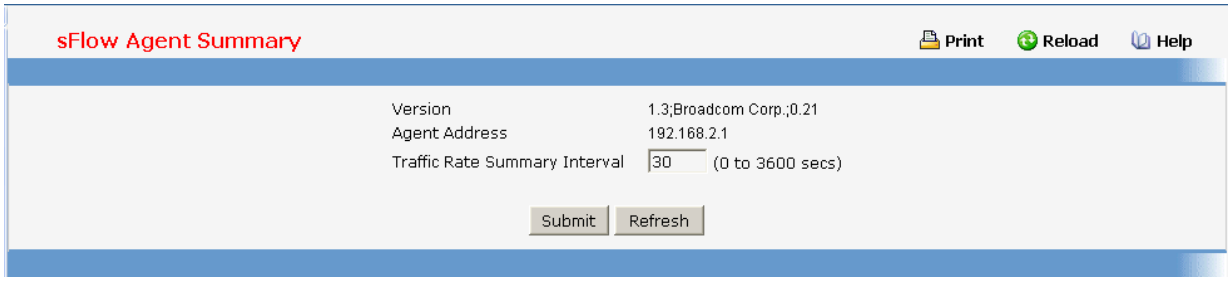
- ***802.1Q Tag*** - Commonly used tag representing 0x8100
- ***vMAN Tag*** - Commonly used tag representing 0x88A8
- ***Custom Tag*** - Configure the EtherType in any range from (0 to 65535)

Command Buttons

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

11.2.7 Defining sFlow

11.2.7.1 Configuring sFlow Agent Summary Configuration Page



Configurable Data

Version - Uniquely identifies the version and implementation of this MIB. The version string must have the following structure: **MIB Version;Organization;Software Revision** where:

- MIB Version: '1.3', the version of this MIB.
- Organization: Broadcom Corp.
- Revision: 1.0.

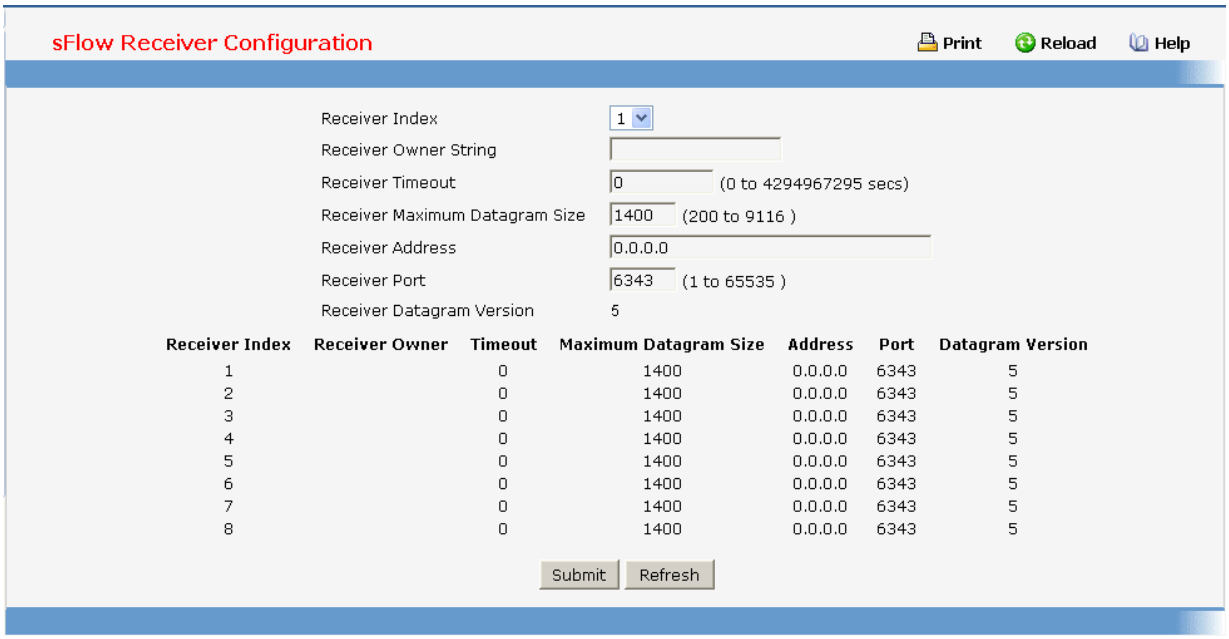
Agent Address - The IP address associated with this agent.

Traffic Rate Summary Interval - The maximum number of seconds between successive summary of the counters associated with all interface. A summary interval of 0 disables traffic rate summary.

Command Buttons

Submit - Send the updated data to the switch and cause the changes to take effect on the switch.
Refresh - Refresh the data on the screen with present state of data in the switch.

11.2.7.2 Configuring sFlow Receiver Configuration Page



Selection Criteria

Receiver Index - Selects the receiver for which data is to be displayed or configured. Allowed range is (1 to 8)

Configurable Data

Receiver Owner - The entity making use of this sFlowRcvrTable entry. The empty string indicates that the entry is currently unclaimed and the receiver configuration is reset to default values. An entity wishing to claim an sFlowRcvrTable entry must ensure that the entry is unclaimed before trying to claim it. The entry is claimed by setting the owner string. The entry must be claimed before any changes can be made to other sampler objects.

sFlow Receiver Timeout - The time (in seconds) remaining before the sampler is released and stops sampling. A management entity wanting to maintain control of the sampler is responsible for setting a new value before the old one expires. Allowed range is (0 to 4294967295 secs) A value of zero sets the selected receiver configuration to its default values.

sFlow Receiver Maximum Datagram Size - The maximum number of data bytes that can be sent in a single sample datagram. The manager should set this value to avoid fragmentation of the sFlow datagrams. Default Value: 1400. Allowed range is (200 to 9116)

sFlow Receiver Address - The IP address of the sFlow collector. If set to 0.0.0.0 no sFlow datagrams will be sent.

sFlow Receiver Port - The destination port for sFlow datagrams. Allowed range is (1 to 65535)

Non-Configurable Data

Receiver Index - The index of this receiver.

Receiver Owner - The entity making use of this sFlowRcvrTable entry. The empty string indicates that the entry is currently unclaimed.

sFlow Receiver Timeout - The time (in seconds) remaining before the sampler is released and stops sampling.

sFlow Receiver Maximum Datagram Size - The maximum number of data bytes that can be sent in a single sample datagram.

sFlow Receiver Address - The IP address of the sFlow collector.

sFlow Receiver Port - The destination port for sFlow datagrams.

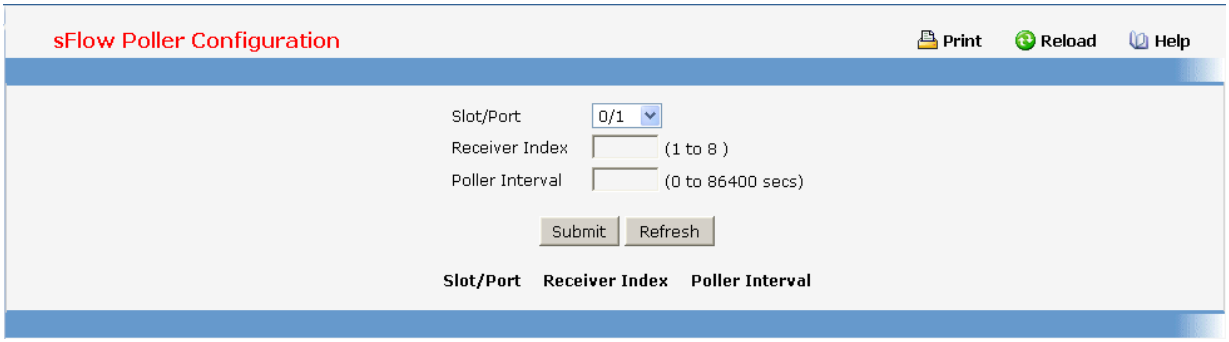
sFlow Receiver Datagram Version - The version of sFlow datagrams that should be sent.

Command Buttons

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

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

11.2.7.3 Configuring sFlow Poller Configuration Page



sFlow agent collects time-based sampling of network interface statistics and sends them to the configured sFlow receivers. A data source configured to collect counter samples is called a poller.

Selection Criteria

sFlow Poller Datasource(Slot/Port) - sFlowDataSource for this sFlow sampler. This Agent will support Physical ports only.

Configurable Data

Receiver Index - The sFlowReceiver associated with this counter poller. Allowed range is (1 to 8)

Poller Interval - The maximum number of seconds between successive samples of the counters associated with this data source. A sampling interval of 0 disables counter sampling. Allowed range is (0 to 86400 secs)

Non-Configurable Data

Slot/Port - The interface for which data is being displayed.

Receiver Index - The sFlowReceiver for this sFlow Counter Poller. If set to 0, the poller configuration is set to default and the poller is deleted. Only active receivers can be set. If a receiver expires then all pollers associated with the receiver will also expire. Allowed range is (1 to 8)

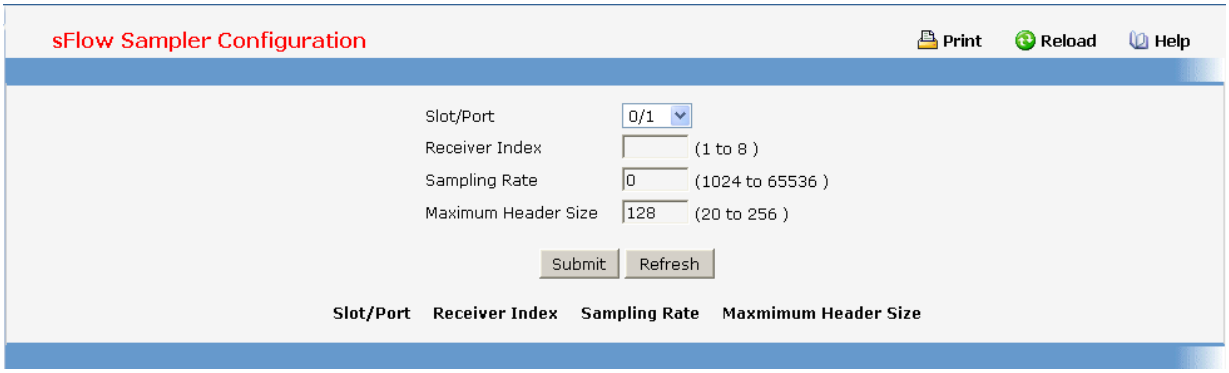
Poller Interval - The maximum number of seconds between successive samples of the counters associated with this data source.

Command Buttons

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

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

11.2.7.4 Configuring sFlow Sampler Configuration Page



sFlow agent collects statistical packet-based sampling of switched flows and sends them to the configured receivers. A data source configured to collect flow samples is called a sampler.

Selection Criteria

sFlow Sampler Datasource(Slot/Port) - sFlowDataSource for this flow sampler. This Agent will support Physical ports only.

Configurable Data

Receiver Index - The sFlow Receiver for this flow sampler. If set to 0, the sampler configuration is set to default and the sampler is deleted. Only active receivers can be set. If a receiver expires then all samplers associated with the receiver will also expire. Allowed range is (1 to 8)

Sampling Rate - The statistical sampling rate for packet sampling from this source. A sampling rate of 1 counts all packets. A sampling rate of 0 disables sampling. Allowed range is (1024 to 65536)

Maximum Header Size - The maximum number of bytes that should be copied from a sampled packet. Allowed range is (20 to 256)

Non-Configurable Data

Slot/Port - The interface for which data is being displayed.

Receiver Index - The sFlowReceiver for this sFlow sampler.

Sampling Rate - The statistical sampling rate for packet sampling from this source.

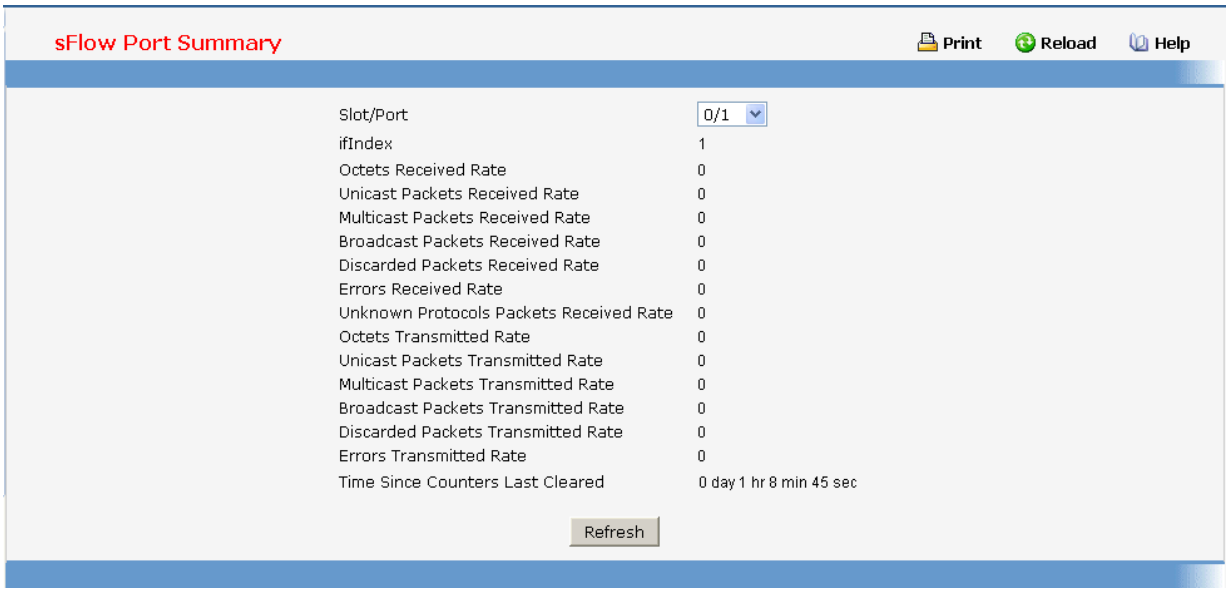
Maximum Header Size - The maximum number of bytes that should be copied from a sampled packet.

Command Buttons

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

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

11.2.7.5 Viewing sFlow Port Summary Page



Selection Criteria

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

Non-Configurable Data

Slot/Port - The interface for which data is being displayed.

ifIndex - This object indicates the ifIndex of the interface table entry associated with this port on an adapter.

Octets Received Rate - The total number of octets of data received rates by the processor (excluding framing bits but including FCS octets).

Unicast Packets Received Rate - The number of subnetwork-unicast packets rates delivered to a higher-layer protocol.

Multicast Packets Received Rate - The total number of packets received rates that were directed to a multicast address. Note that this number does not include packets directed to the broadcast address.

Broadcast Packets Received Rate - The total number of packets received rates that were directed to the broadcast address. Note that this does not include multicast packets.

Discarded Packets Received Rate - The number of inbound packets which were chosen to be discarded rates 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.

Errors Received Rate - The errors received rate of Single, Multiple, and Excessive Collisions.

Unknown Protocols Packets Received Rate - For packet-oriented interfaces, the number of packets received rates via the interface which were discarded because of an unknown or unsupported protocol. For character-oriented or fixed-length interfaces that support protocol multiplexing the number of transmission units received via the interface which were discarded because of an unknown or unsupported protocol. For any interface that does not support protocol multiplexing, this counter will always be 0.

Octets Transmitted Rate - The total number of octets transmitted rates out of the interface, including framing characters.

Unicast Packets Transmitted Rate - The total number of packets rates that higher-level protocols requested be transmitted to a subnetwork-unicast address, including those that were discarded or not sent.

Multicast Packets Transmitted Rate - The total number of packets rates that higher-level protocols requested be transmitted to a Multicast address, including those that were discarded or not sent.

Broadcast Packets Transmitted Rate - The total number of packets rates that higher-level protocols requested be transmitted to the Broadcast address, including those that were discarded or not sent.

Discarded Packets Transmitted Rate - The number of outbound packets rates 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.

Errors Transmitted Rate - The errors transmitted rate of Single, Multiple, and Excessive Collisions.

Time Since Counters Last Cleared - The elapsed time, in days, hours, minutes, and seconds since the statistics for this port were last cleared.

Command Buttons

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

11.2.8 Defining SNMP

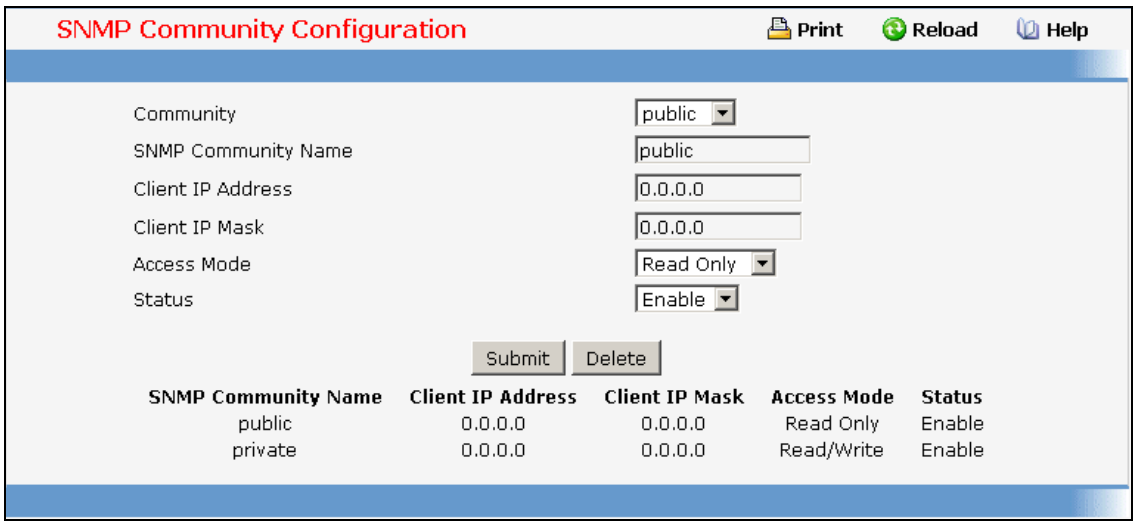
11.2.8.1 Configuring SNMP Community Configuration Page

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.



Selection Criteria

Community - You can use this screen to reconfigure an existing community, or to create a new one. Use this pulldown menu to select one of the existing community names, or select 'Create' to add a new one.

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.

Configurable Data

SNMP Community Name - The Snmp Community Name, it identifies each SNMP community. Community names in the SNMP community must be unique. 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.

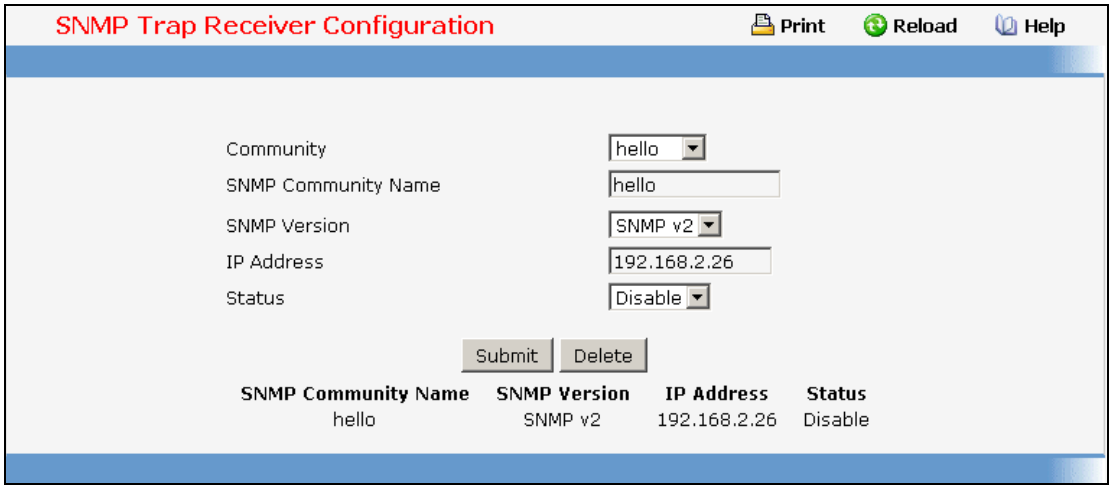
Command Buttons

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 currently selected Community Name. If you want the switch to retain the new values across a power cycle, you must perform a save.

11.2.8.2 Configuring SNMP Trap Receiver Configuration Page

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



Selection Criteria

Community - You can use this screen to reconfigure an existing community, or to create a new one. Use this pulldown menu to select one of the existing community names, or select 'Create' to add a new one.

SNMP Version - Select the trap version to be used by the receiver from the pull down menu:

SNMP v1 - Uses SNMP v1 to send traps to the receiver.

SNMP v2 - Uses SNMP v2 to send traps to the receiver.

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

Enable - send traps to the receiver.

Disable - do not send traps to the receiver.

Configurable Data

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.

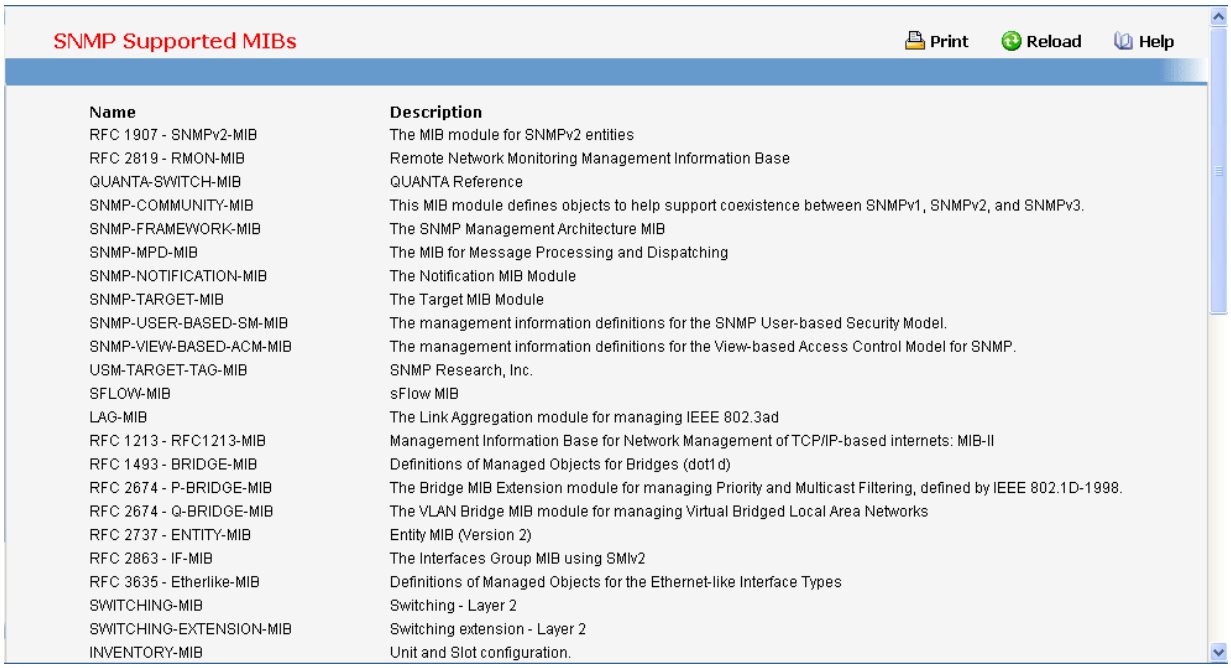
Command Buttons

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 currently selected Community Name. If you want the switch to retain the new values across a power cycle, you must perform a save.

11.2.8.3 Viewing SNMP supported MIBs Page

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



Name	Description
RFC 1907 - SNMPv2-MIB	The MIB module for SNMPv2 entities
RFC 2819 - RMON-MIB	Remote Network Monitoring Management Information Base
QUANTA-SWITCH-MIB	QUANTA 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.
SFLOW-MIB	sFlow 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 2674 - P-BRIDGE-MIB	The Bridge MIB Extension module for managing Priority and Multicast Filtering, defined by IEEE 802.1D-1998.
RFC 2674 - Q-BRIDGE-MIB	The VLAN Bridge MIB module for managing Virtual Bridged Local Area Networks
RFC 2737 - ENTITY-MIB	Entity MIB (Version 2)
RFC 2863 - IF-MIB	The Interfaces Group MIB using SMIv2
RFC 3635 - Etherlike-MIB	Definitions of Managed Objects for the Ethernet-like Interface Types
SWITCHING-MIB	Switching - Layer 2
SWITCHING-EXTENSION-MIB	Switching extension - Layer 2
INVENTORY-MIB	Unit and Slot configuration.

Non-configurable Data

Name - The RFC number if applicable and the name of the MIB.

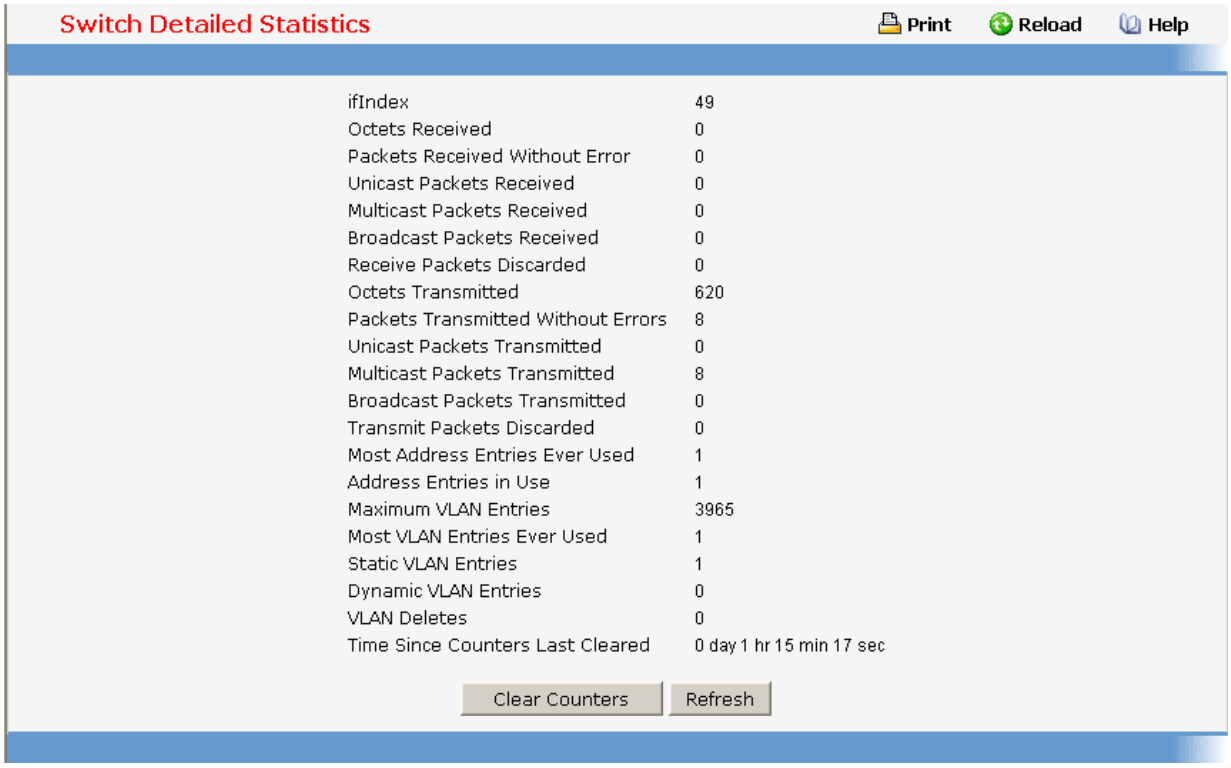
Description - The RFC title or MIB description.

Command Buttons

Refresh - Update the data.

11.2.9 Viewing Statistics

11.2.9.1 Viewing the whole Switch Detailed Statistics Page



Non-Configurable 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.

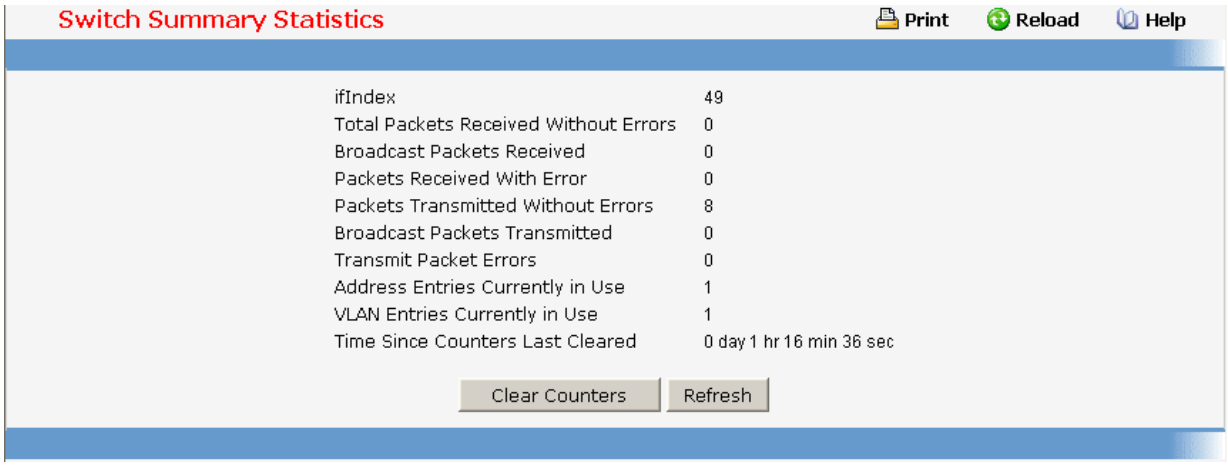
Time Since Counters Last Cleared - The elapsed time, in days, hours, minutes, and seconds, since the statistics for this switch were last cleared.

Command Buttons

Clear Counters - Clear all the counters, resetting all switch summary and detailed statistics to default values. The discarded packets count cannot be cleared.

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

11.2.9.2 Viewing the whole Switch Summary Statistics Page



Non-Configurable Data

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 Errors - 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.

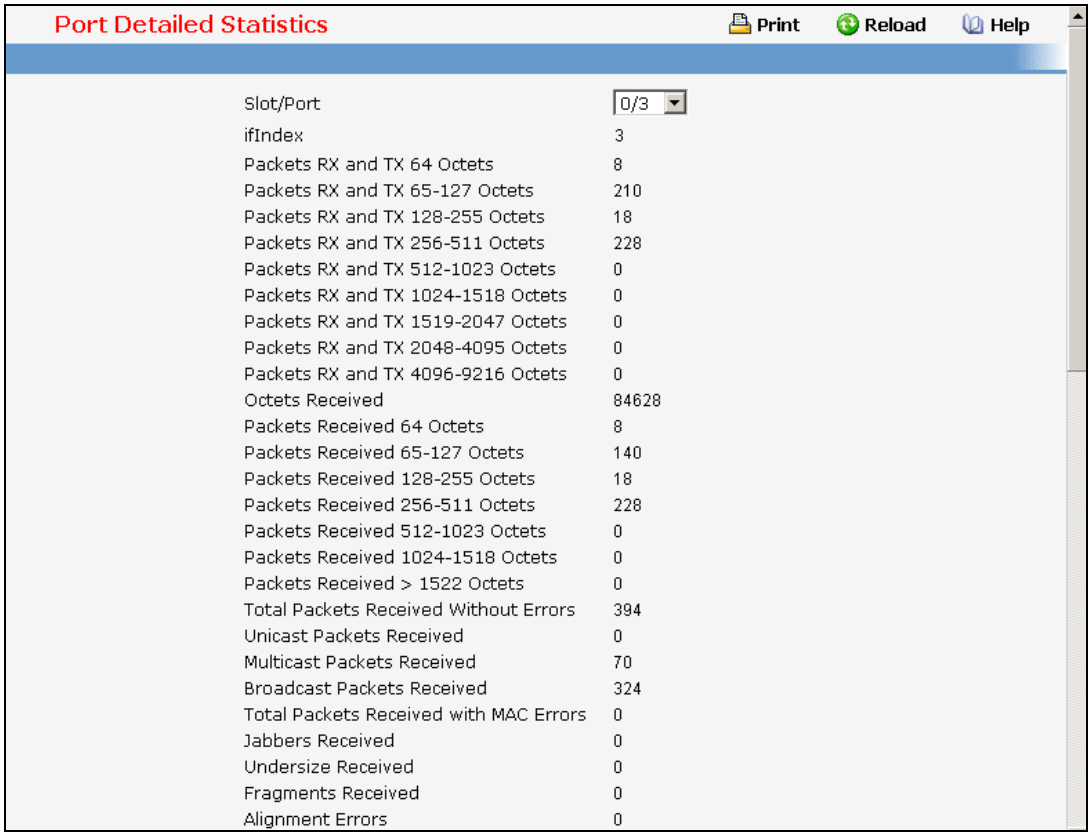
Time Since Counters Last Cleared - The elapsed time, in days, hours, minutes, and seconds since the statistics for this switch were last cleared.

Command Buttons

Clear Counters - Clear all the counters, resetting all summary and switch detailed statistics to defaults. The discarded packets count cannot be cleared.

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

11.2.9.3 Viewing Each Port Detailed Statistics Page



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 1519-2047 Octets - The total number of packets (including bad packets) received or transmitted that were between 1519 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 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 > 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.

Undersize Received - The total number of packets received that were less than 64 octets in length with GOOD CRC(excluding framing bits but including FCS octets).

Fragments Received - The total number of packets received that were less than 64 octets in length with ERROR CRC(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 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 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).

Maximum Frame Size - The maximum ethernet frame size the interface supports or is configured, including ethernet header, CRC, and payload. (1518 to 9216). 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 nummber 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.

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.

GMRP Failed Registrations - The number of times attempted GMRP registrations could not be completed.

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.

Time Since Counters Last Cleared - The elapsed time, in days, hours, minutes, and seconds since the statistics for this port were last cleared.

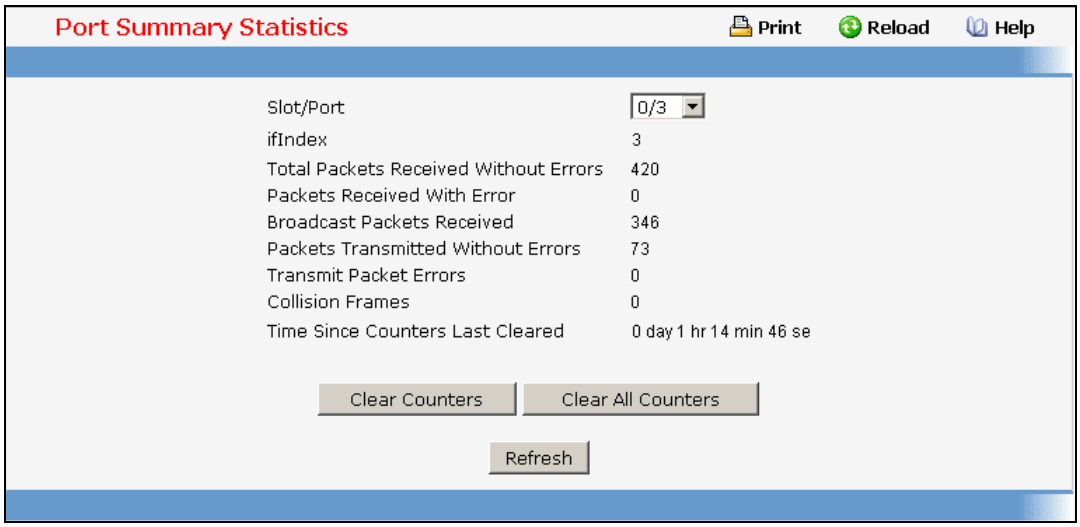
Command Buttons

Clear Counters - Clear all the counters, resetting all statistics for this port to default values.

Clear All Counters - Clear all the counters for all ports, resetting all statistics for all ports to default values.

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

11.2.9.4 Viewing Each Port Summary Statistics Page



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 Errors - 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.

Command Buttons

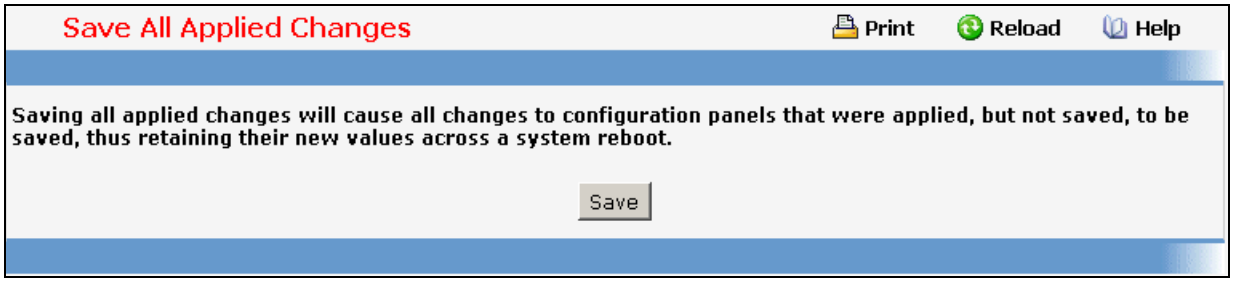
Clear Counters - Clears all the counters, resetting all statistics for this port to default values.

Clear All Counters - Clears all the counters for all ports, resetting all statistics for all ports to default values.

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

11.2.10 Managing System Utilities

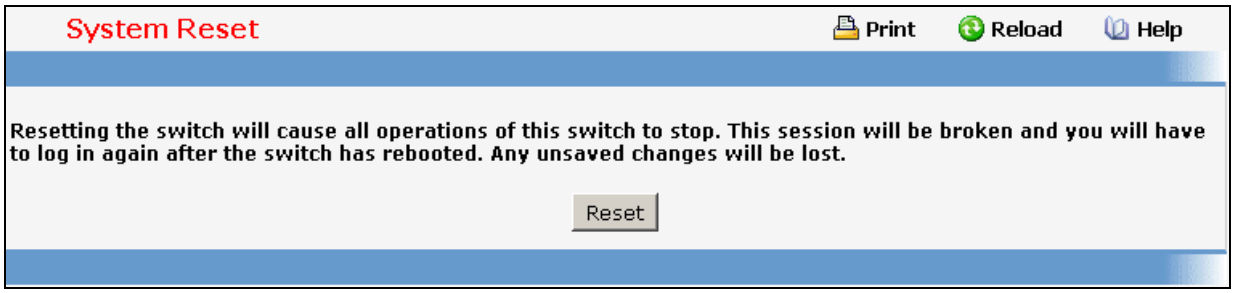
11.2.10.1 Saving All Configuration Changed Page



Command Buttons

Save - Click this button to have configuration changes you have made saved across a system reboot. All changes submitted since the previous save or system reboot will be retained by the switch.

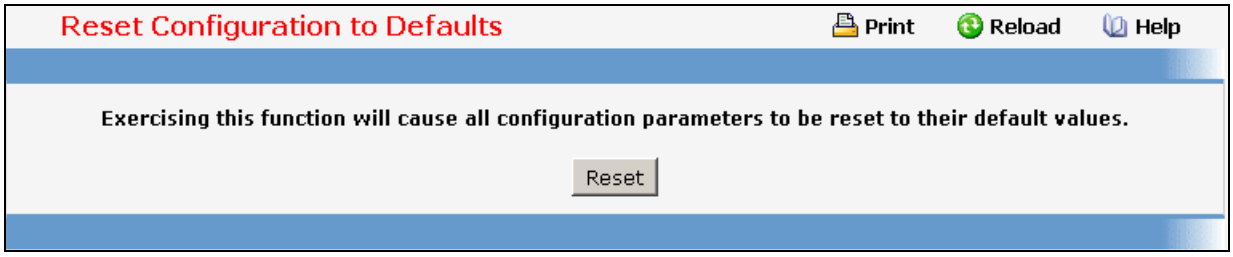
11.2.10.2 Resetting the Switch Page



Command Buttons

Reset - Select this button to 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.

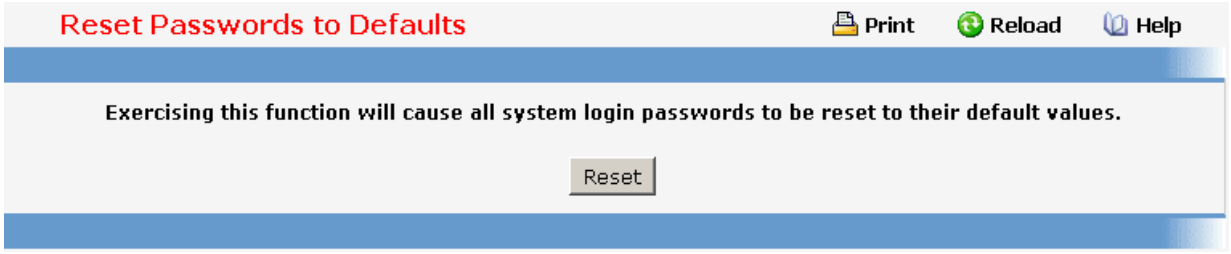
11.2.10.3 Restoring All Configuration to Default Values Page



Command Buttons

Reset - Clicking the Reset button will 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.

11.2.10.4 Resetting the Passwords to Default Values Page

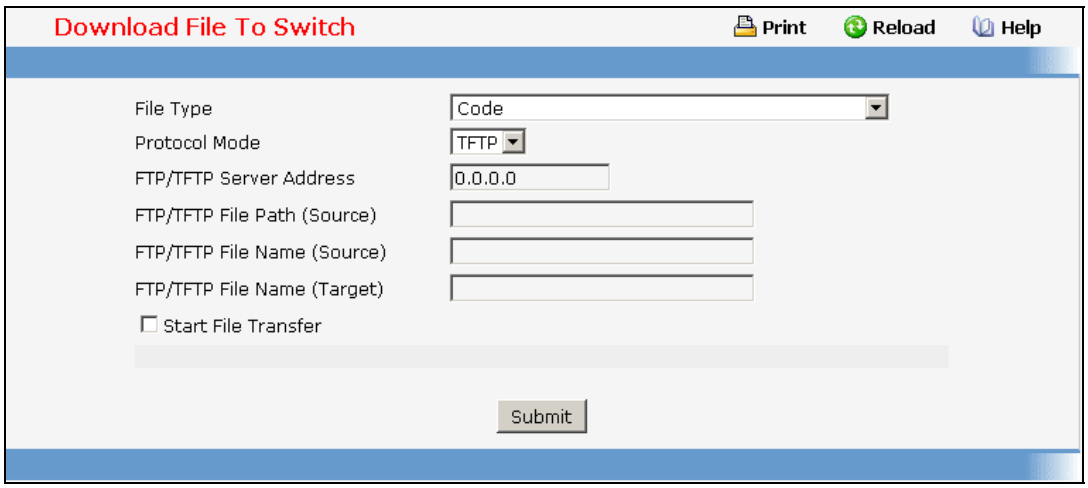


Command Buttons

Reset - Select this button to have all passwords reset to their factory default values.

11.2.10.5 Downloading Specific Files to Switch Flash Page

Use this menu to download a file to the switch.



Selection Criteria

File Type - Specify what type of file you want to download:

Script - specify configuration script when you want to update the switch's script file.

CLI Banner - Specify the banner that you want to display before user login to the switch.

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)

To download SSH key files SSH must be administratively disabled and there can be no active SSH sessions.

Protocol Mode - Specify the protocol of mode to upload. The available options are FTP and TFTP.

Configurable Data

User Account - Specify the user account of the FTP site.

User Password - Specify the user password of the FTP site.

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

FTP/TFTP File Path (Source) - Enter the path on the TFTP server where the selected file is located. You may enter up to 96 characters. The factory default is blank.

FTP/TFTP File Name (Source) - 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.

FTP/TFTP File Name (Target) - Enter the name on the switch of the file you want to save. You may enter up to 30 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.

Non-Configurable Data

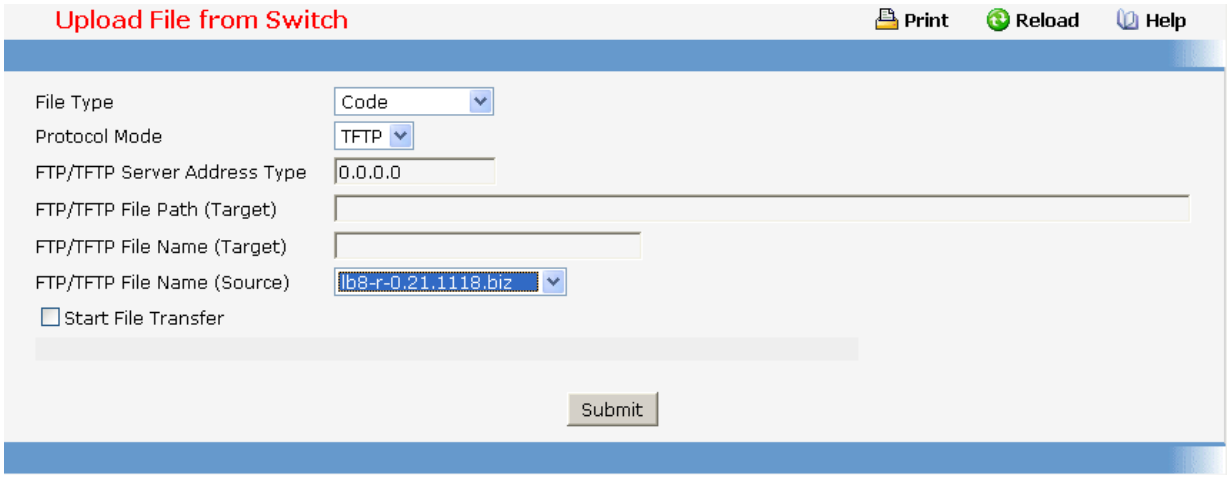
The last row of the table is used to display information about the progress of the file transfer. The screen will refresh automatically until the file transfer completes.

Command Buttons

Submit - Send the updated screen to the switch and perform the file download.

11.2.10.6 Uploading Specific Files from Switch Flash Page

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



Selection Criteria

File Type - Specify the type of file you want to upload. The available options are Script, Code, CLI Banner, Configuration, Error Log, Buffered Log, and Trap Log. The factory default is Error Log.

Protocol Mode - Specify the protocol of mode to upload. The available options are FTP and TFTP.

Configurable Data

User Account - Specify the user account of the FTP site.

User Password - Specify the user password of the FTP site.

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

FTP/TFTP File Path (Target) - Enter the path on the TFTP server where you want to put the file being uploaded. You may enter up to 96 characters. The factory default is blank.

FTP/TFTP File Name (Target) - Enter the name you want to give the file being uploaded. You may enter up to 32 characters. The factory default is blank.

FTP/TFTP File Name (Source) - Specify the file witch you want to upload from switch.

Start File Transfer - To initiate the upload you need to check this box and then select the submit button.

Non-Configurable Data

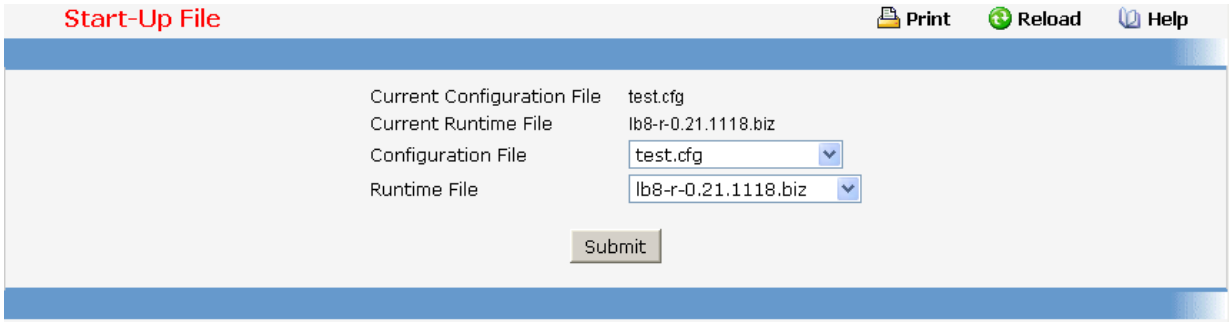
The last row of the table is used to display information about the progress of the file transfer. The screen will refresh automatically until the file transfer completes.

Command Buttons

Submit - Send the updated screen to the switch and perform the file upload.

11.2.10.7 Defining Configuration and Runtime Startup File Page

Specify the file used to start up the system.



Selection Criteria

Configuration File - Configuration files.

Runtime File - Run-time operation codes.

Non-Configurable Data

Current Configuration File - Current Configuration files.

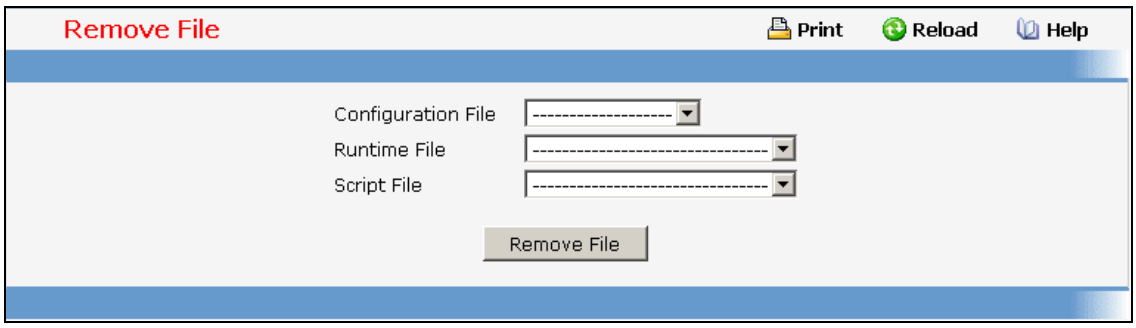
Current Runtime File - Current Run-time operation codes.

Command Buttons

Submit - Send the updated screen to the switch and specify the file start-up.

11.2.10.8 Removing Specific File Page

Delete files in flash. If the file type is used for system startup, then this file cannot be deleted.



Configurable Data

Configuration File - Configuration files.

Runtime File - Run-time operation codes.

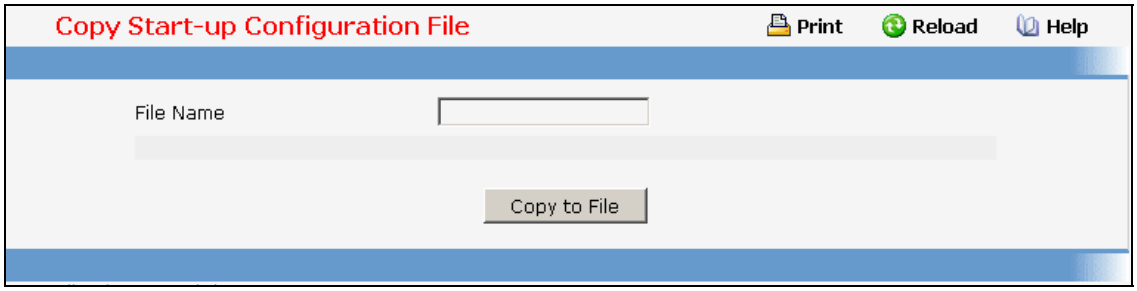
Script File - Configuration script files.

Command Buttons

Remove File - Send the updated screen to the switch and perform the file remove.

11.2.10.9 Copying Running Configuration to Flash Page

Use this menu to copy a start-up configuration file from the running configuration file on switch.



Configurable Data

File Name - Enter the name you want to give the file being copied. You may enter up to 32 characters. The factory default is blank.

Non-Configurable Data

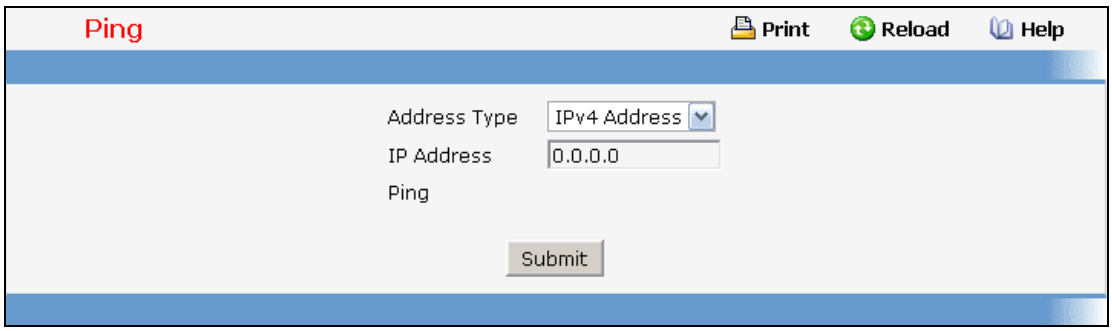
The last row of the table is used to display information about the progress of the file copy. The screen will refresh automatically until the file copy completes.

Command Buttons

Copy to File - Send the updated screen to the switch perform the file copy.

11.2.10.10 Defining Ping Function Page

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 = 5, receive count = n).**



Selection Criteria

Address Type - Select the address type for IPv4 Address or Host Name.

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.

Host Name - Enter the host name of the station you want the switch to ping.

Non-Configurable Data

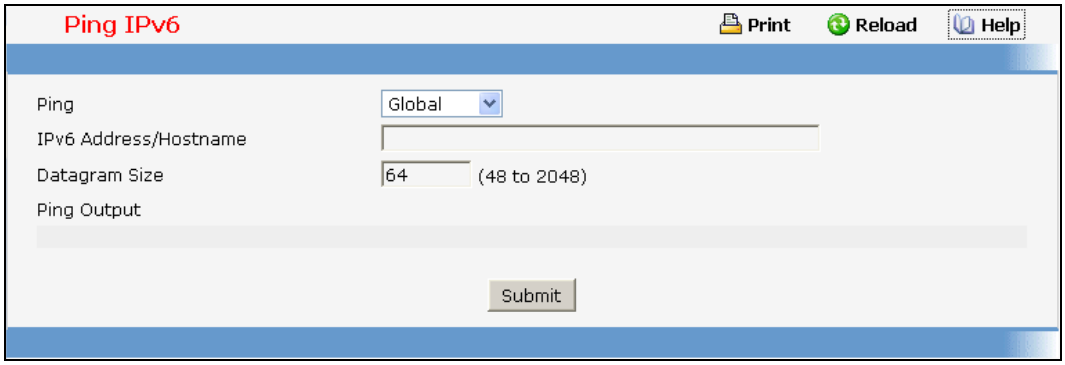
Ping – The reply result received from switch.

Command Buttons

Submit - This will initiate the Ping.

11.2.10.11 Defining Ping IPv6 Function Page

This screen is used to send a Ping request to a specified IPv6 address. You can use this to check whether the switch can communicate with a particular IPv6 station. Once you click the Submit button, the switch will send three pings and the results will be displayed below the configurable data. The output will be **Send count=3, Receive count=n from (IPv6 Address). Average round trip time = n ms.**



Selection Criteria

Ping - Select either global IPv6 Address or Link Local Address to ping.

Interface - Select a IPv6 interface.

Configurable Data

IPv6 Address - Enter the IPv6 address of the station you want the switch to ping. The initial value is blank. The IPv6 Address you enter is not retained across a power cycle.

Host name - Enter the host name of the station you want the switch to ping.

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

Datagram Size - Enter the datagram size. The valid range is 48 to 2048.

Non-Configurable Data

Ping Output– The reply result received from switch.

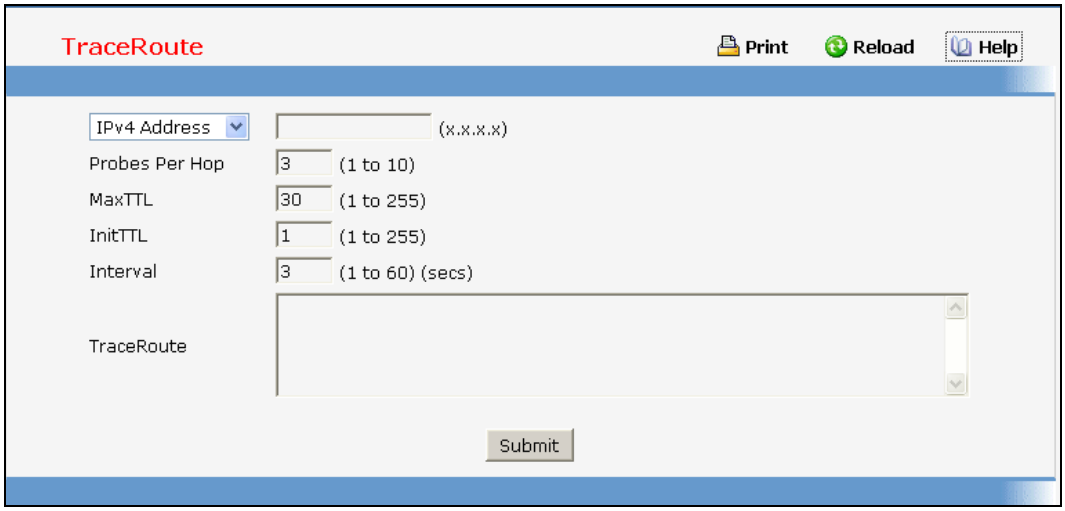
Command Buttons

Submit - This will initiate the ping.

11.2.10.12 TraceRoute Function

Use this screen to tell the switch to send a TraceRoute request to a specified IP address.You can use this to discover the paths packets take to a remote destination. Once you click the Submit button, the switch will send traceroute and the results will be displayed below the configurable data. If a reply to the traceroute is you will see

1 x.y.z.w 9869 usec 9775 usec 10584 usec
2 0.0.0.0 0 usec * 0 usec * 0 usec *
3 0.0.0.0 0 usec * 0 usec * 0 usec *
Hop Count = w Last TTL = z Test attempt = x Test Success = y.



Selection Criteria

IPv4 Address - Select the way "IPv4 Address" to trace.

Host Name - Select the way "host name" to trace.

Host Name V6 - Select the way "Host Name V6" to trace.

IPv6 Address - Select the way "IPv6 Address" to trace.

Configurable Data

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

Probes Per Hop - Enter the number of probes per hop. The initial value is default. The Probes per Hop you enter is not retained across a power cycle.

MaxTTL - Enter the maximum TTL for the destination. The initial value is default value. The MaxTTL you enter is not retained across a power cycle.

InitTTL - Enter the initial TTL to be used. The initial value is default value. The InitTTL you enter is not retained across a power cycle.

MaxFail - Enter the maximum Failures allowed in the session. The initial value is default value. The MaxFail you enter is not retained across a power cycle.

Interval - Enter the Time between probes in seconds. The initial value is default value. The Interval you enter is not retained across a power cycle.

Traceroute - Display the result of traceroute.

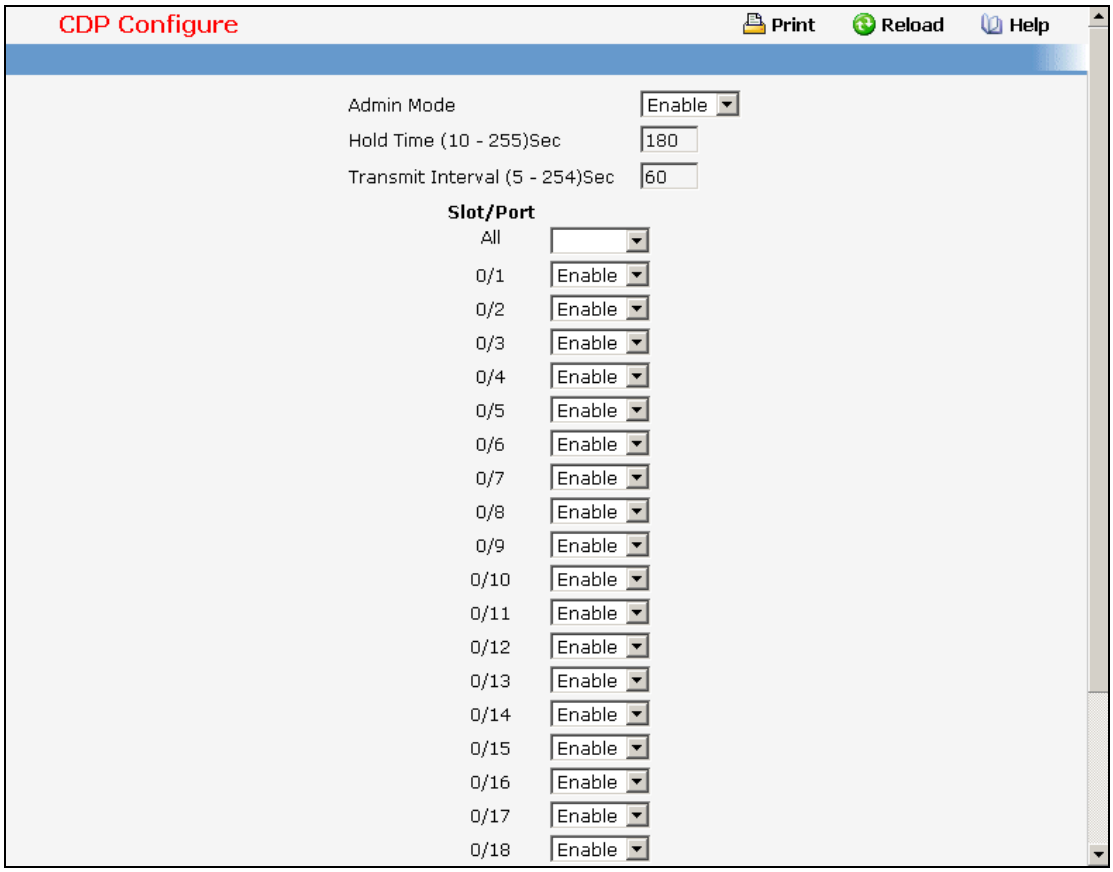
Command Buttons

Submit - This will initiate the traceroute.

11.2.11 Managing CDP Function

11.2.11.1 Defining CDP Configuration Page

Use this menu to configure the parameters for CDP, which is used to discover a CISCO device on the LAN.



Selection Criteria

Admin Mode - CDP administration mode which are Enable and Disable.

Slot/Port - Specifies the list of ports.

Configurable Data

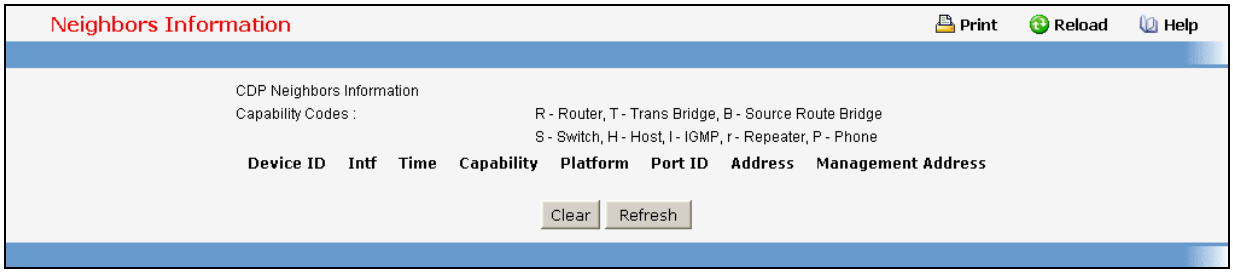
Hold Time - the legal time period of a received CDP packet.

Transmit Interval - the CDP packet sending interval.

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.

11.2.11.2 Viewing Neighbors Information Page



Non-Configurable Data

Device ID - Identifies the device name in the form of a character string.

Intf - The CDP neighbor information receiving port.

Time - The length of time a receiving device should hold CDP information before discarding it.

Capability - Describes the device's functional capability in the form of a device type, for example, a switch.

Platform - Describes the hardware platform name of the device, for example, FSC the L2 Network Switch.

Port ID - Identifies the port on which the CDP packet is sent.

Address - The L3 addresses of the interface that has sent the update.

Management Address - The first address of IP address which can use management address connect to switch.

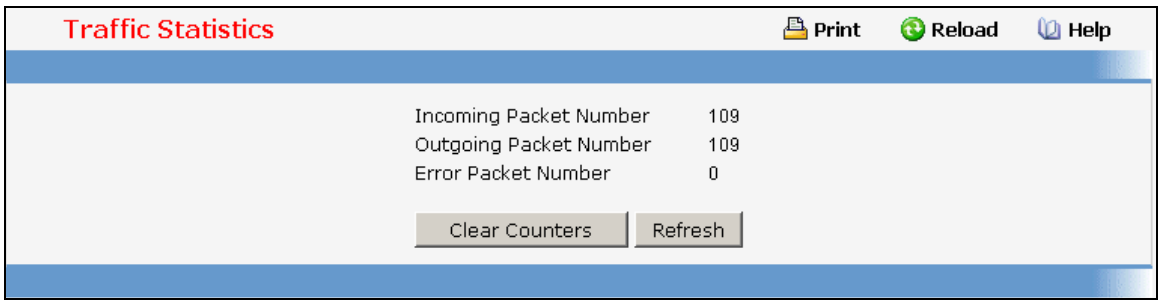
Command Buttons

Clear - Clear all the counters, resetting all switch summary and detailed statistics to default values. The discarded packets count cannot be cleared.

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

11.2.11.3 Viewing Traffic Statistics Page

Use this menu to display CDP traffic statistics.



Non-Configurable Data

Incoming Packet Number - Received legal CDP packets number from neighbors.

Outgoing Packet Number - Transmitted CDP packets number from this device.

Error Packet Number - Received illegal CDP packets number from neighbors.

Command Buttons

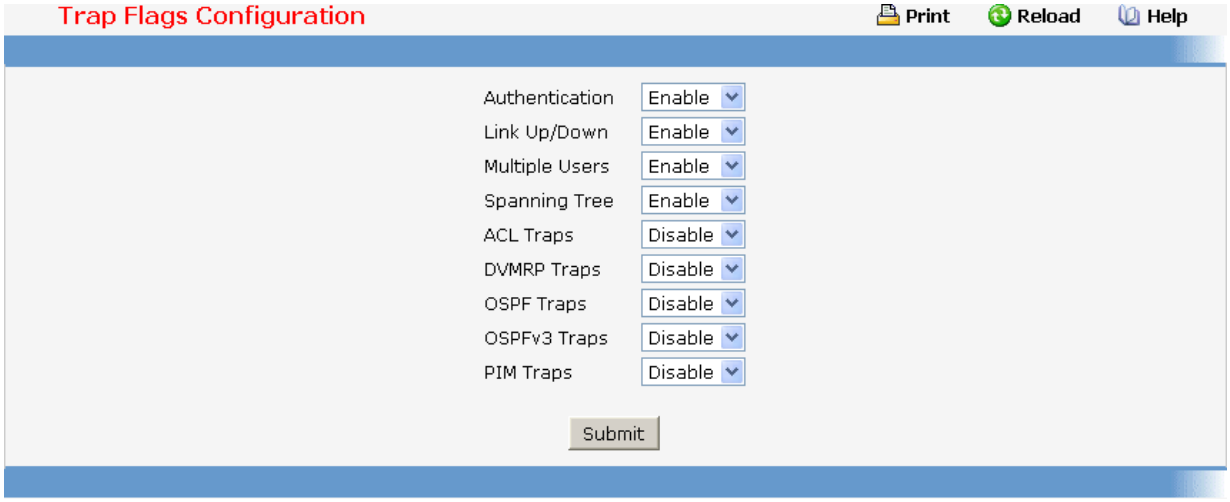
Clear Counters - Clear all the counters, resetting all switch summary and detailed statistics to default values. The discarded packets count cannot be cleared.

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

11.2.12 Defining Trap Manager

11.2.12.1 Configuring Trap Flags Page

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.



Selection Criteria

Authentication - Enable or disable activation of authentication failure traps by selecting the corresponding line on the pull down entry field. The factory default is enabled.

Link Up/Down - Enable 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 - Enable 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 - Enable or disable activation of spanning tree traps by selecting the corresponding line on the pull down entry field. The factory default is enabled.

ACL Traps - Enable or disable activation of ACL traps by selecting the corresponding line on the pulldown entry field. The factory default is disabled.

DVMRP Traps - Enabled or disable activation of DVMRP traps by selecting the corresponding line on the pulldown entry field. The factory default is disabled.

OSPF Traps - Enabled or disable activation of OSPF traps by selecting the corresponding line on the pulldown entry field. The factory default is disabled. This field can be configured only if the OSPF admin mode is enabled.

PIM Traps - Enabled or disable activation of PIM traps by selecting the corresponding line on the pulldown entry field. The factory default is disabled.

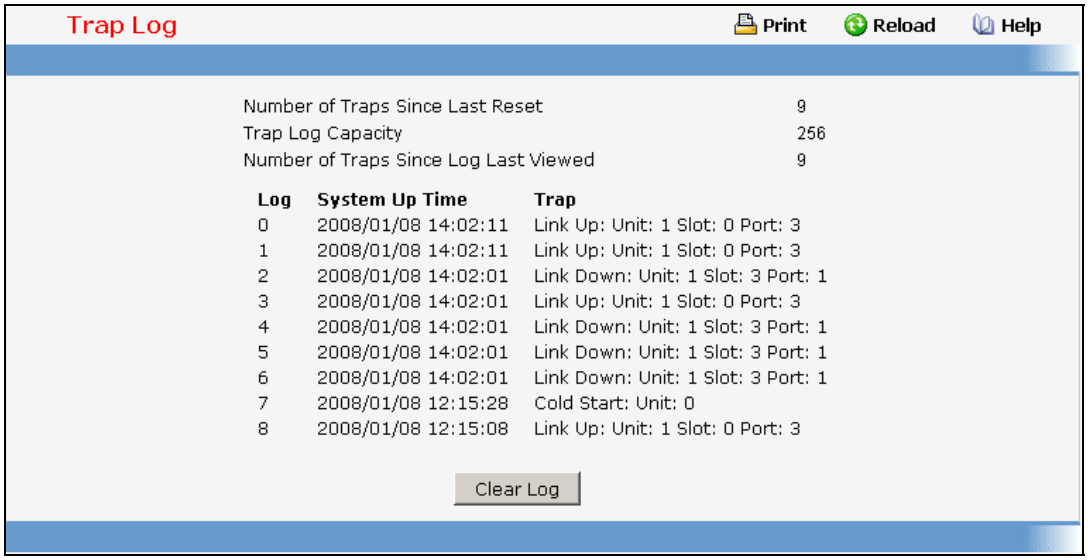
OSPFv3 Traps - Enabled or disable activation of OSPFv3 traps by selecting the corresponding line on the pulldown entry field. The factory default is disabled. This field can be configured only if the OSPFv3 admin mode is enabled.

Command Buttons

Submit - Sends the updated screen to the switch and causes the changes to take effect on the switch. These changes will not be retained across a power cycle unless a save is performed.

11.2.12.2 Viewing Trap Log Page

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 switch were last reset.

Trap Log Capacity - The maximum number of traps stored in the log. If the number of traps exceeds the capacity, the entries will overwrite the oldest entries.

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.

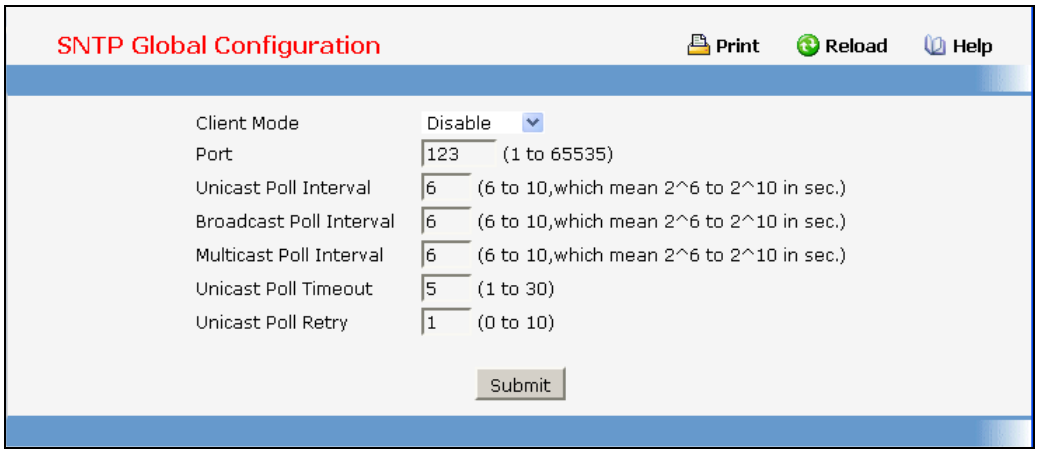
Trap - Information identifying the trap.

Command Buttons

Clear Log - Clear all entries in the log. Subsequent displays of the log will only show new log entries.

11.2.13 Configuring SNTP

11.2.13.1 Configuring SNTP Global Configuration Page



Selection Criteria

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.
- ***Multicast*** - SNTP operates in the same manner as multicast mode and uses a local multicast address.

Configurable Data

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.

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

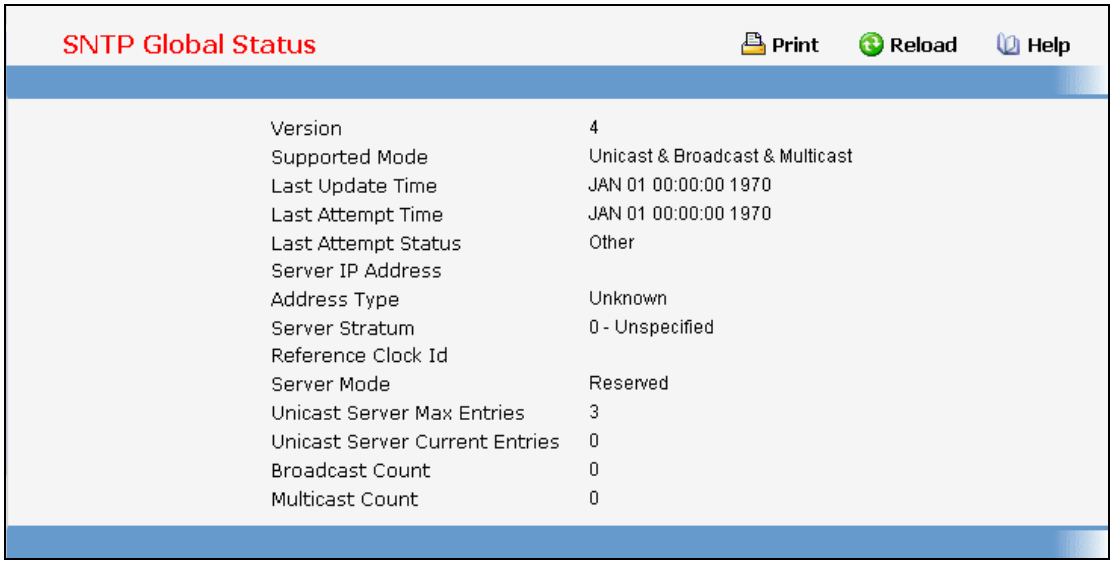
Unicast Poll Timeout - Specifies the number of seconds to wait for an SNTP response when configured in unicast mode. Allowed range is (1 to 30). Default value is 5.

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.

11.2.13.2 Viewing SNTP Global Status Page



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.

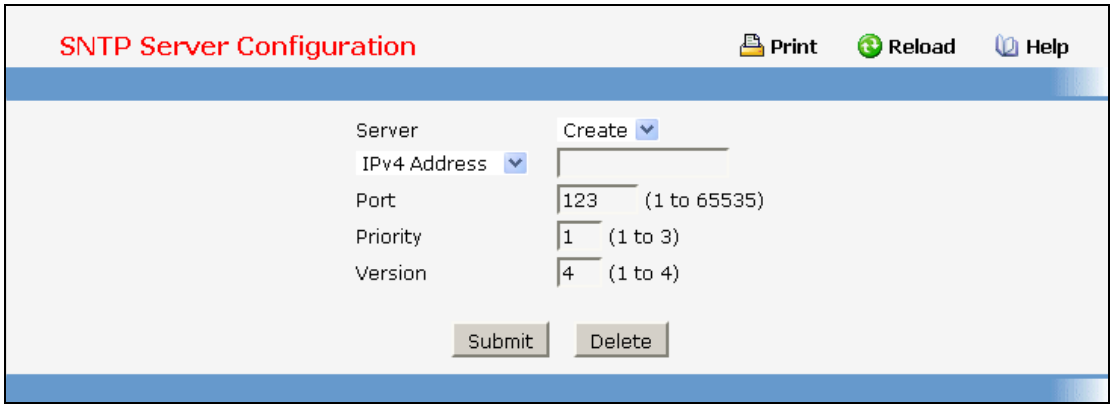
Unicast Sever Max Entries - Specifies the maximum number of unicast server entries that can be configured on this client.

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.

Multicast Count - Specifies the number of unsolicited muticast SNTP messages that have been received and processed by the SNTP client since last reboot.

11.2.13.3 Configuring SNTP Server Page



Selection Criteria

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 Type - Specifies the address type of the configured SNTP Server address. Allowed types are :

- IPv4 Address
- IPv6 Address
- Host Name
- Host Name V6

Configurable Data

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.

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.

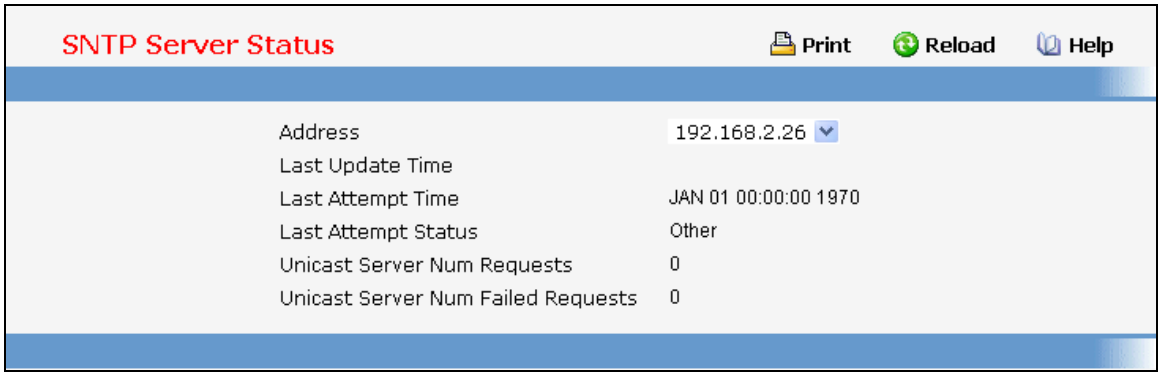
Version - Specifies the NTP Version running on the server. Allowed range is (1 to 4). Default value is 4.

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.

11.2.13.4 Viewing SNTP Server Status Page



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.

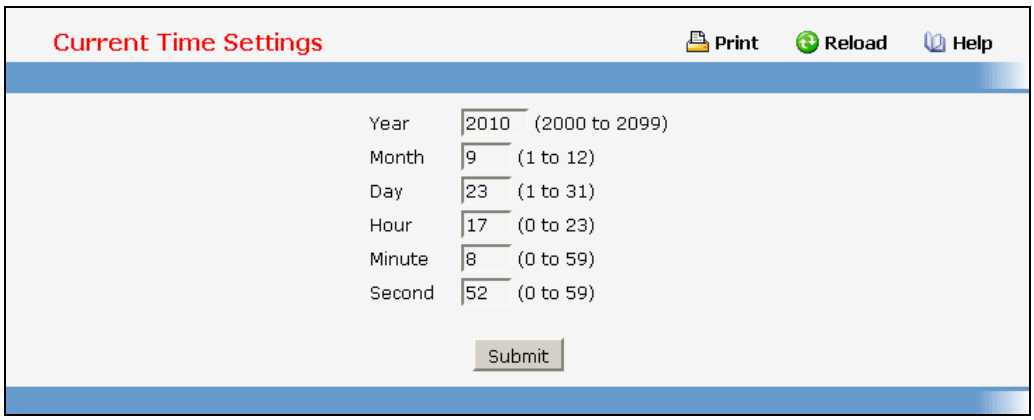
Last Attempt Status - Specifies the status of the last SNTP request to this server. If no packet has been received from this server, a status of Other is displayed.

- ***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*** - The SNTP 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 time agent reboot.

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

11.2.13.5 Configuring Current Time Settings Page



Configurable Data

Year - Year (4-digit). (Range: 2000 - 2099).

Month - Month. (Range: 1 - 12).

Day - Day of month. (Range: 1 - 31).

Hour - Hour in 24-hour format. (Range: 0 - 23).

Minute - Minute. (Range: 0 - 59).

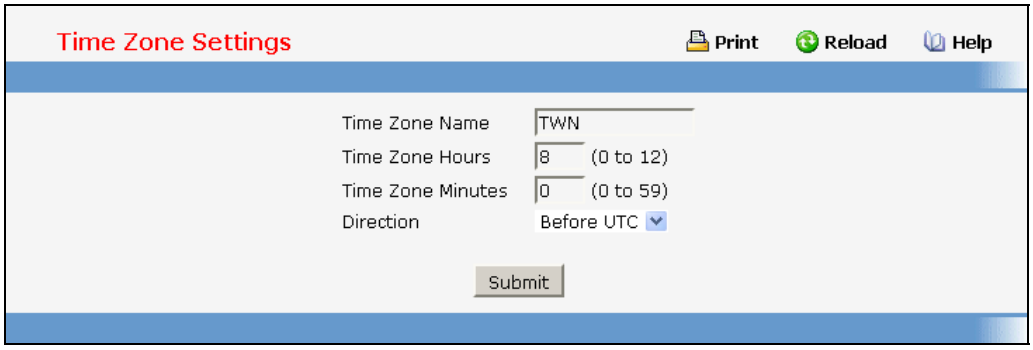
Second - Second. (Range: 0 - 59).

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.

11.2.13.6 Configuring Time Zone Settings Page

Simple Network Time Protocol (SNTP) allows the switch to set its internal clock based on periodic updates from a time server. Maintaining an accurate time on the switch enables the system log to record meaningful dates and times for event entries. You can also manually set the clock using the CLI. If the clock is not set, the switch will only record the time from the factory default set at the last bootup.



Selection Criteria

Direction

- before-utc - Sets the local time zone before (east) of UTC
- after-utc - Sets the local time zone after (west) of UTC

Configurable Data

Time Zone Name - The name of time zone, usually an acronym. (Range: 1-15 characters).

Time Zone Hours - The number of hours before/after UTC. (Range: 0-12 hours).

Time Zone Minutes - The number of minutes before/after UTC. (Range: 0-59 minutes).

- before-utc - Sets the local time zone before (east) of UTC
- after-utc - Sets the local time zone after (west) of UTC

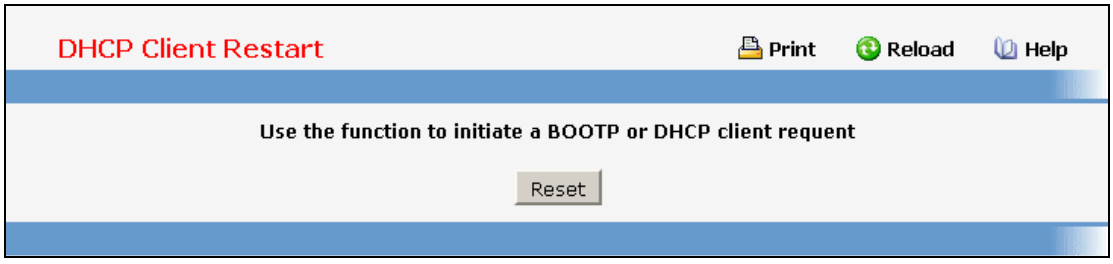
Command Buttons

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.

11.2.14 Defining DHCP Client

11.2.14.1 Configuring DHCP Restart Page

This command issues a BOOTP or DHCP client request for any IP interface that has been set to BOOTP or DHCP mode via the IP address command. DHCP requires the server to reassign the client's last address if available. If the BOOTP or DHCP server has been moved to a different domain, the network portion of the address provided to the client will be based on this new domain.

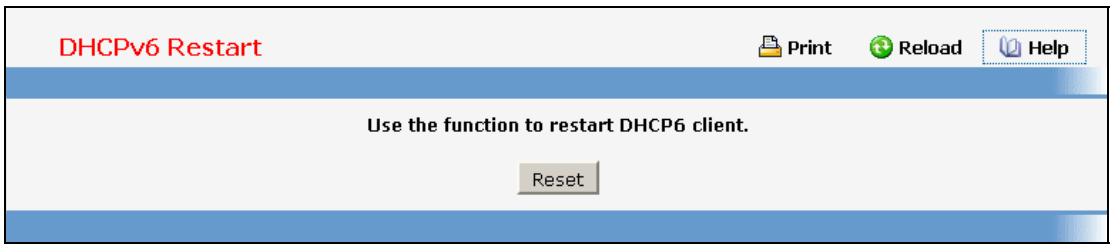


Command Buttons

Reset - Send the updated screen to the switch to restart the DHCP client.

11.2.14.1.1 Configurating DHCPv6 Restart Page

This command issues a DHCP6 client request for any IP interface that has been set to DHCP mode via the ip address command. DHCP requires the server to reassign the client's last address if available. If the DHCP server has been moved to a different domain, the network portion of the address provided to the client will be based on this new domain.

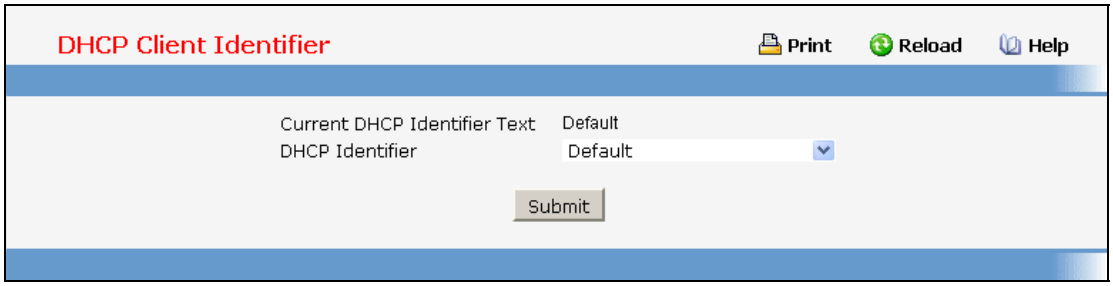


Command Buttons

Reset - Send the updated screen to the switch perform the restart DHCP6 client.

11.2.14.2 Configuring DHCP Client-identifier Page

Specify the DCHP client identifier for the switch. The DCHP client identifier is used to include a client identifier in all communications with the DHCP server. The identifier type depends on the requirements of your DHCP server.



Selection Criteria

DHCP Identifier - Specifies the type of DHCP Identifier.

- Default
- Specific Text String
- Specific Hexadecimal Value

Non-Configurable Data

Current DHCP Identifier (Hex/Text) - Shows the current setting of DHCP identifier.

Configurable Data

Text String - A text string.

Hex Value - The hexadecimal value.

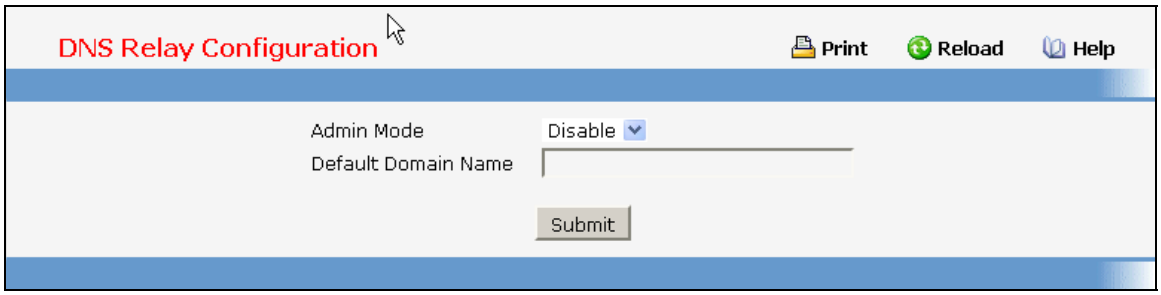
Command Buttons

Submit - Send the updated screen to the switch perform the setting DHCP client identifier.

11.2.15 Defining DNS Relay Function

11.2.15.1 Configuring DNS Relay Configuration Page

The DNS protocol controls the Domain Name System (DNS), a distributed database with which you can map host names to IP addresses. When you configure DNS on your switch, you can substitute the host name for the IP address with all IP commands, such as ping, telnet, traceroute, and related Telnet support operations. To keep track of domain names, IP has defined the concept of a domain name server, which holds a cache (or database) of names mapped to IP addresses. To map domain names to IP addresses, you must first identify the host names, specify the name server that is present on your network, and enable the DNS.



Selection Criteria

Admin Mode - Select enable or disable from the pull down menu. When you select 'enable', the IP Domain Naming System (DNS)-based host name-to-address translation will be enabled.

Configurable Data

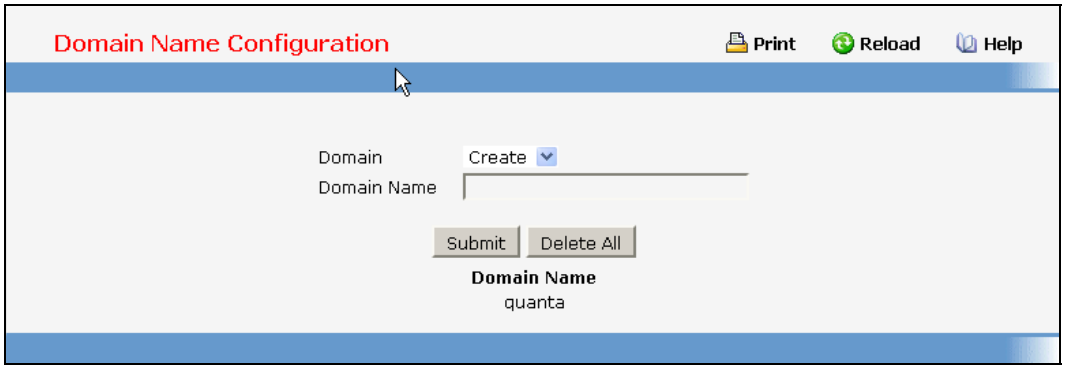
Default Domain Name - Default domain name used to complete unqualified host names. Do not include the initial period that separates an unqualified name from the domain name. This is a text string of up to 63 characters.

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.

11.2.15.2 Configuring Domain Name Configuration Page

You can use this screen to change the configuration parameters for the domain names that can be appended to incomplete host names (i.e., host names passed from a client that are not formatted with dotted notation). You can also use this screen to display the contents of the table.



Selection Criteria

Domain - Specifies all the existing domain names along with an additional option "Create". When the user selects "Create" another text box "Domain Name" appears where the user may enter domain name to be configured.

Configurable Data

Domain Name - Specifies the domain name. Do not include the initial period that separates an unqualified name from the domain name. This is a text string of up to 63 characters.

Command Buttons

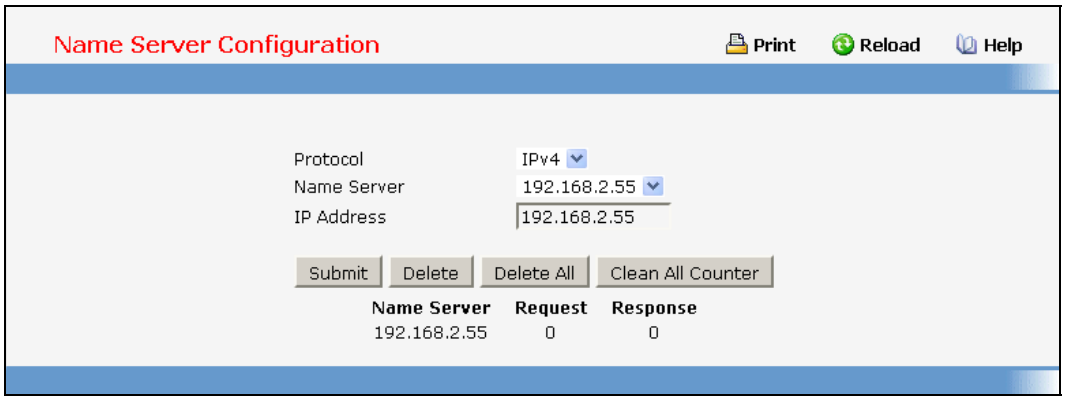
Submit - Sends the updated configuration to the switch. Configuration changes take effect immediately.

Delete - Deletes the domain name entry. Sends the updated configuration to the switch. Configuration changes take effect immediately.

Delete All - Deletes all the domain name entries. Sends the updated configuration to the switch. Configuration changes take effect immediately.

11.2.15.3 Configuring Name Server Configuration Page

You can use this screen to change the configuration parameters for the domain name servers. You can also use this screen to display the contents of the table.



Selection Criteria

Protocol - Select IPv4 or IPv6 to configure the corresponding attributes.

Name Server - Specifies all the existing domain name servers along with an additional option "Create". When the user selects "Create" another text box "IP Address" appears where the user may enter domain name server to be configured.

Configurable Data

IP Address - Specifies the address of the domain name server.

Non-Configurable Data

Request - Specifies the number of DNS requests since last agent reboots.

Response - Specifies the number of DNS Server responses since last agent reboots.

Command Buttons

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

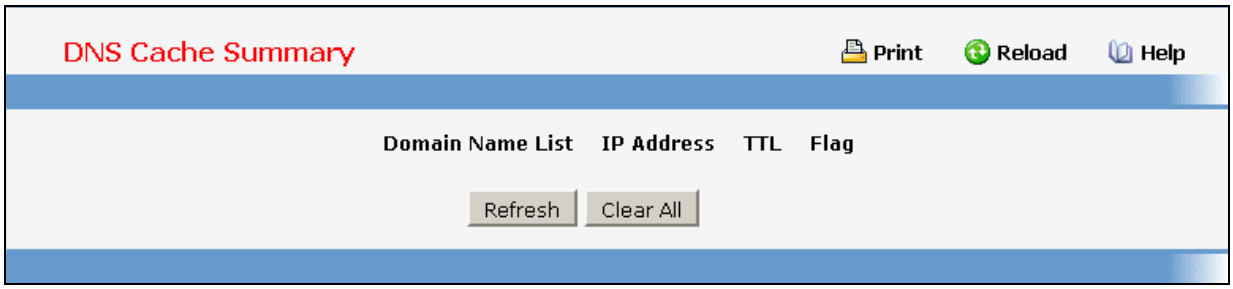
Delete - Deletes the domain name server entry. Sends the updated configuration to the switch. Configuration changes take effect immediately.

Delete All - Deletes all the domain name server entries. Sends the updated configuration to the switch. Configuration changes take effect immediately.

Clear All Counter - Cleans all the name server counters.

11.2.15.4 Configuring DNS Cache Summary Page

The Domain Name System (DNS) dynamically maps domain name to Internet (IP) addresses. This panel displays the current contents of the DNS cache.



Non-Configurable Data

Domain Name List - The domain name associated with this record.

IP address - The IP address associated with this record.

TTL - The time to live reported by the name server.

Flag - The flag of the record.

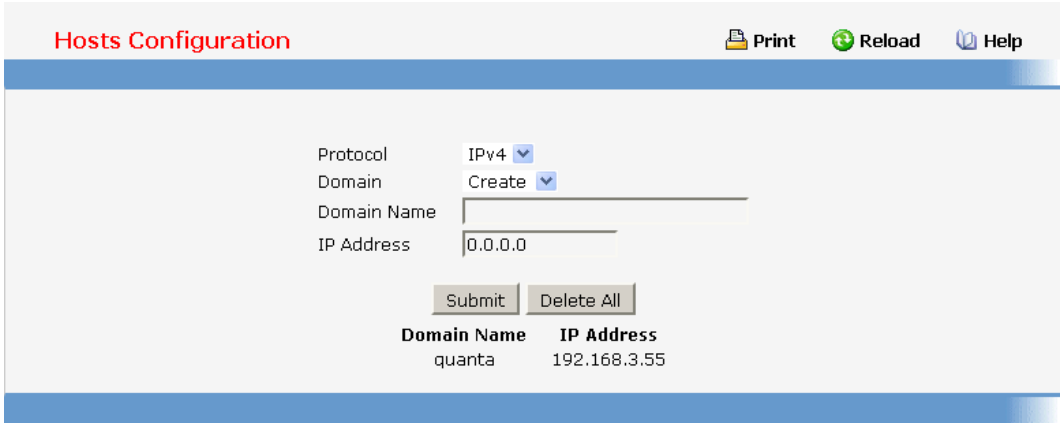
Command Buttons

Refresh - Refresh the page with the latest DNS cache entries.

Clear All - Clear all entries in the DNS cache.

11.2.15.5 Configuring Hosts Configuration Page

You can use this screen to change the configuration parameters for the static entry in the DNS table. You can also use this screen to display the contents of the table.



Selection Criteria

Protocol - Select IPv4 or IPv6 to configure the corresponding attributes.

Domain - Specifies all the existing hosts along with an additional option "Create". When the user selects "Create" another text box "Domain Name" appears where the user may enter host to be configured.

Configurable Data

Domain Name - Specifies the domain name of the host. This is a text string of up to 63 characters.

IP Address - Specifies the address of the host.

Command Buttons

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

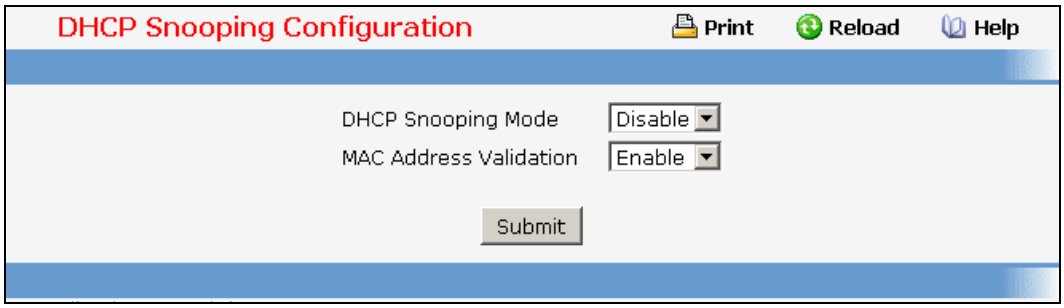
Delete - Deletes the host entry. Sends the updated configuration to the switch. Configuration changes take effect immediately.

Delete All - Deletes all the host entries. Sends the updated configuration to the switch. Configuration changes take effect immediately.

11.3 Switching Menu

11.3.1 Managing DHCP Snooping

11.3.1.1 Configuring DHCP Snooping Configuration Page



Configurable Data

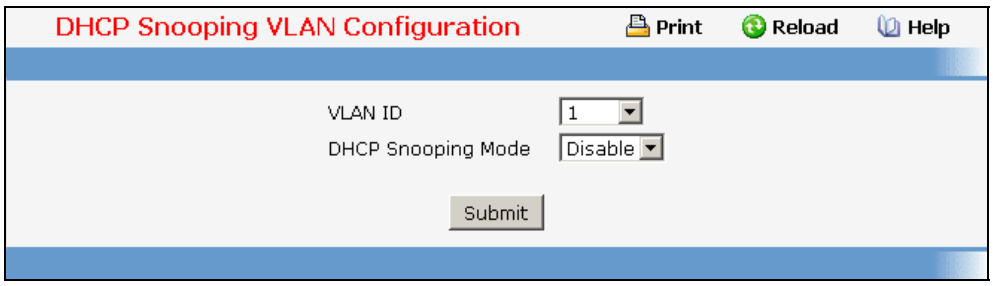
DHCP Snooping Mode - Enables or disables the DHCP Snooping feature. The factory default is disabled.

MAC Address Validation - Enables or disables the validation of sender MAC Address for DHCP Snooping. The factory default is enabled.

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.

11.3.1.2 Configuring DHCP Snooping VLAN Configuration Page



Selection Criteria

VLAN ID - Select the VLAN for which information to be displayed or configured for DHCP Snooping Application.

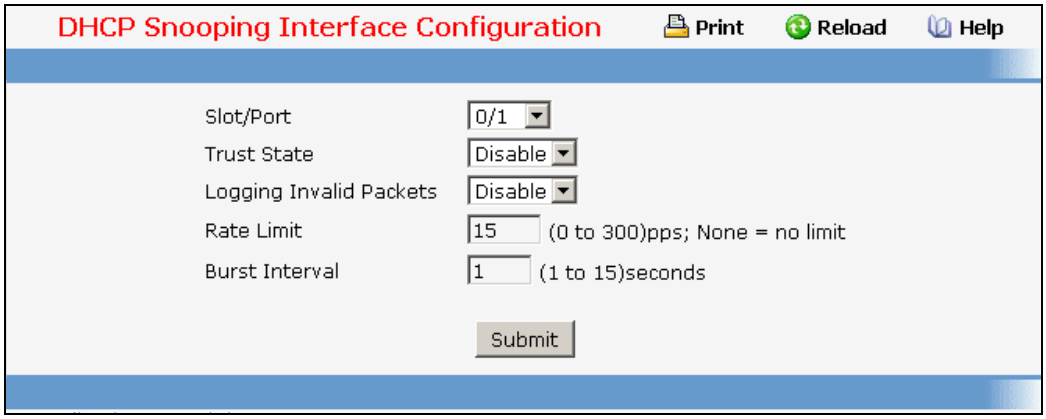
Configurable Data

DHCP Snooping Mode - Enables or disables the DHCP Snooping feature on selected VLAN. The factory default is disabled.

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.

11.3.1.3 Configuring DHCP Snooping Interface Configuration Page



Selection Criteria

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

Configurable Data

Trust State - If it is Enabled DHCP snooping application considers as port trusted. The factory default is disabled.

Logging Invalid Packets - If it is Enabled DHCP snooping application logs invalid packets on this interface. The factory default is disabled.

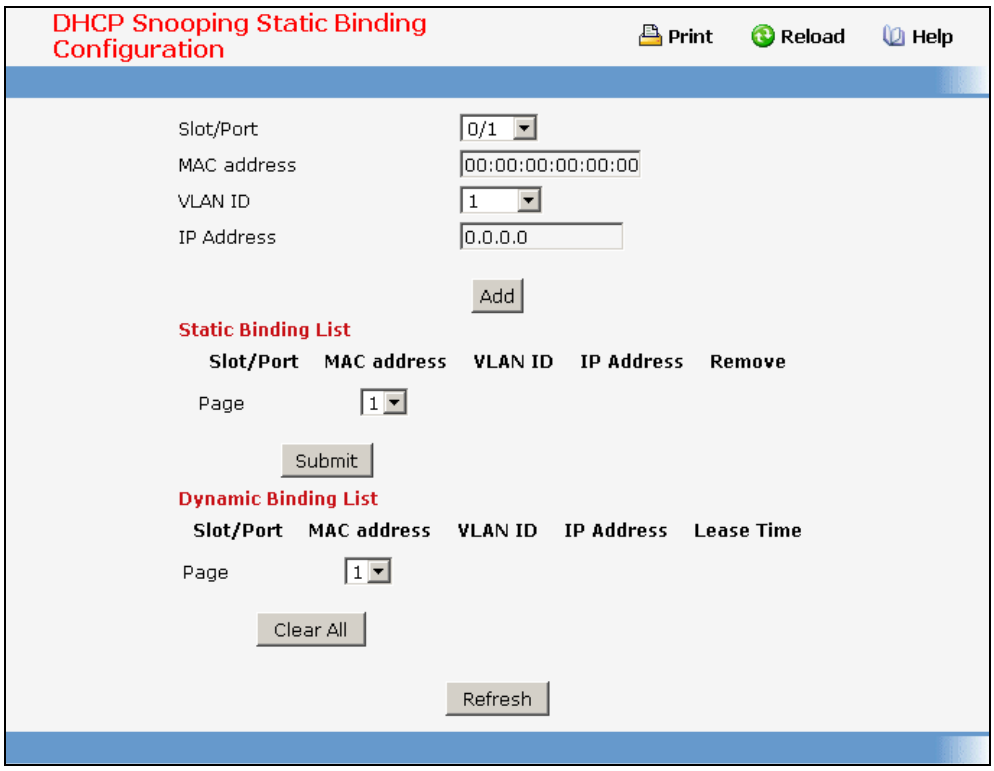
Rate Limit - Specifies rate limit value for DHCP Snooping purpose. If the incoming rate of DHCP packets exceeds the value of this object for consecutively burst interval seconds, the port will be shutdown. If this value is None there is no limit. The factory default is 15pps (packets per second). The range of Rate Limit is (0 to 300).

Burst Interval - This Specifies the burst interval value for rate limiting purpose on this interface. If the rate limit is None burst interval has no meaning shows it as N/A. The factory default is 1 second. The range of Burst Interval is (1 to 15).

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.

11.3.1.4 Configuring DHCP Snooping Static Binding Configuration Page



Configurable Data

Slot/Port - Selects the interface to add a binding into the DHCP snooping database.

MAC Address - Specify the MAC address for the binding to be added. This is the Key to the binding database.

VLAN ID - Selects the VLAN from the list for the binding rule. The range of the VLAN ID is (1 to 3965).

IP Address - Specify valid IP Address for the binding rule.

Non-configurable data

Static Binding List - Lists all the DHCP snooping static binding entries page by page. Ex: Page 1 displays first 15 available static entries. Page 2 displays Next 15 available static entries.

- ***Slot/Port*** - Interface
- ***MAC Address*** - MAC address
- ***VLAN ID*** - VLAN ID
- ***IP Address*** - IP address
- ***Remove*** - This is to be selected to remove the particular binding entry.
- ***Page*** - Lists the Number of Pages the static binding entries occupied. Select the Page Number from this list to display the particular Page entries.

Dynamic Binding List - Lists all the DHCP snooping dynamic binding entries page by page. Ex: Page 1 displays first available up to 15 dynamic entries. Page 2 displays Next available up to 15 dynamic entries.

- ***Slot/Port*** - Interface
- ***MAC Address*** - MAC address
- ***VLAN ID*** - VLAN ID
- ***IP Address*** - IP address

- ***Lease Time*** - This is the remaining Lease time for the Dynamic entries
- ***Page*** - Lists the Number of Pages the dynamic binding entries occupied. Select the Page Number from this list to display the particular Page entries.

Command Buttons

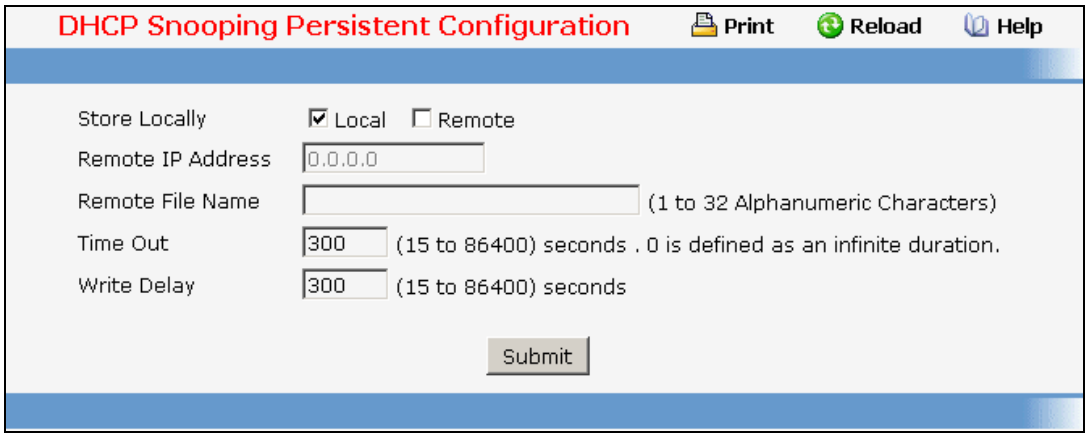
Add - Adds DHCP snooping binding entry into the database.

Submit - Deletes selected static entries from the database.

ClearAll - Deletes all DHCP Snooping binding entries.

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

11.3.1.5 Configuring DHCP Snooping Persistent Configuration Page



Selection Criteria

Local - Check the Local Checkbox to disable the Remote objects like Remote File Name and Remote IP.

Remote - Check the Remote Checkbox to Enable the Remote objects like Remote File Name and Remote IP.

Configurable Data

Remote IP - Configures Remote IP Address on which the snooping database will be stored when Remote checkbox is selected.

Remote File Name - Configures Remote file name to store the database when Remote checkbox is selected.

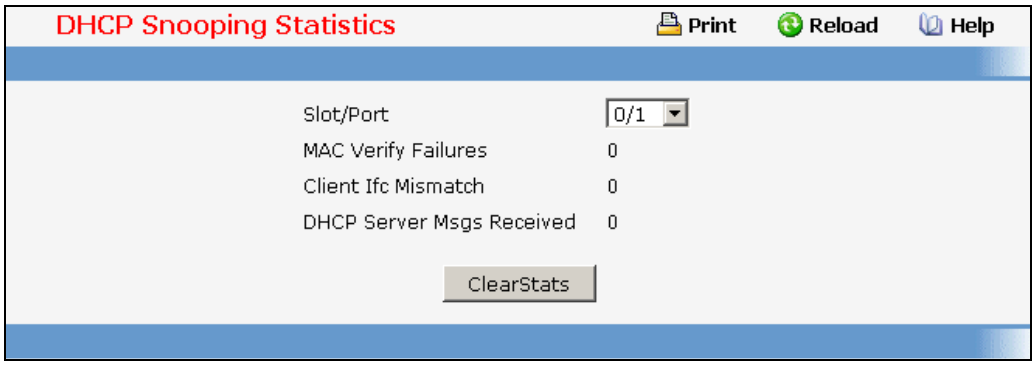
Time Out - Configure DHCP snooping bindings store timeout. The range of Time Out is (15 to 86400) . 0 is defined as an infinite duration.

Write Delay - Configures the maximum write time to write the database into local or remote. The range of Write Delay is (15 to 86400).

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.

11.3.1.6 DHCP Snooping Interface Statistics Page



Selection Criteria

Slot/Port - Select the un trusted and snooping enabled interface for which statistics to be displayed.

Non-Configurable Data

MAC Verify Failures - Number of packets that were dropped by DHCP Snooping as there is no matching DHCP Snooping binding entry found.

Client Ifc Mismatch - The number of DHCP messages that are dropped based on source MAC address and client HW address verification.

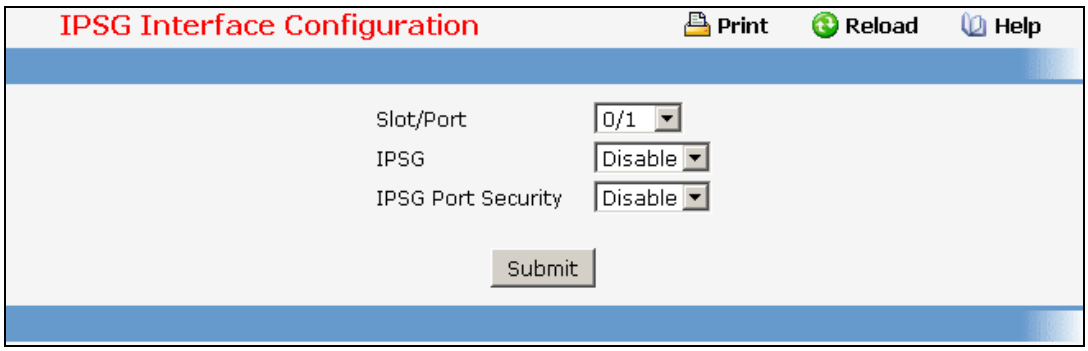
DHCP Server Msgs Received - The number of Server messages that are dropped on an un trusted port.

Command Buttons

ClearStats - Clears all interfaces statistics.

11.3.2 Managing IP Source Guard (IPSG)

11.3.2.1 Configuring IPSG Configuration Page



Configurable Data

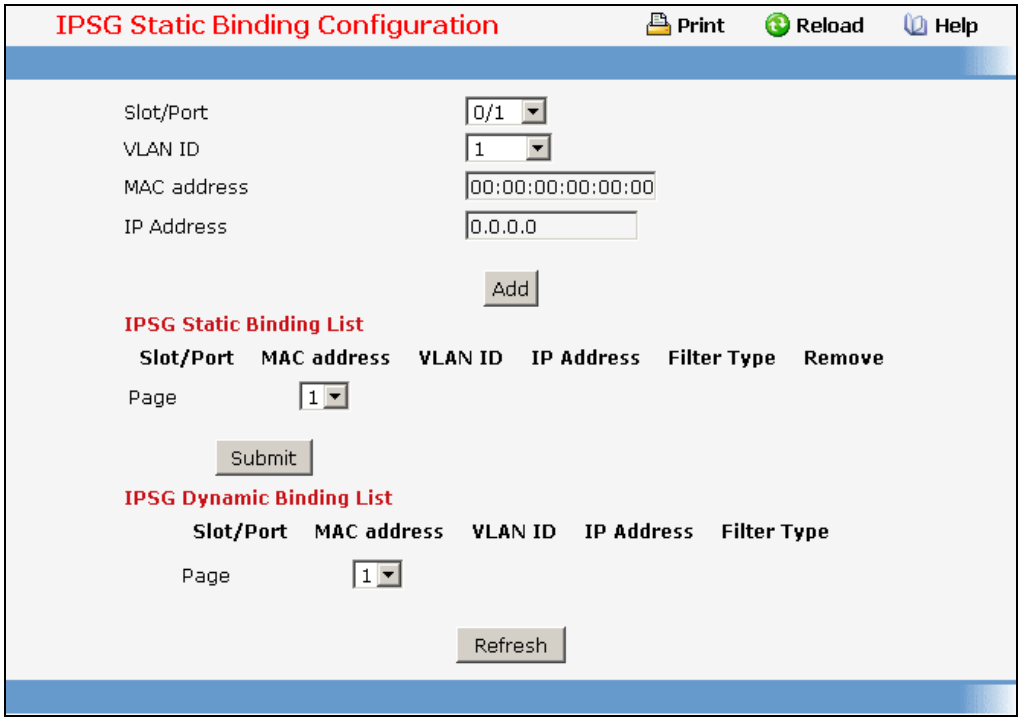
IPSG - Enables or disables validation of Sender IP Address on this interface. If IPSG is Enabled Packets will not be forwarded if Sender IP Address is not in DHCP Snooping Binding database. The factory default is disabled.

IPSG Port Security - Enables or disables the IPSG Port Security on the selected interface. If IPSG Port Security is enabled then the packets will not be forwarded if the sender MAC Address is not in FDB table and it is not in DHCP snooping binding database. To enforce filtering based on MAC address other required configurations are - Enable port-security Globally - Enable port-security on the interface level. IPSG Port Security Can't be Enabled if IPSG is Disabled. The factory default is disabled.

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.

11.3.2.2 Configuring IPSG Static Binding Configuration Page



Configurable Data

Slot/Port - Selects the interface to add a binding into the IPSG database.

MAC Address - Specify the MAC address for the binding.

VLAN ID - Selects the VLAN from the list for the binding rule.

IP Address - Specify valid IP Address for the binding rule.

Non-configurable Data

IPSG Static Binding List - Lists all the IPSG static binding entries page by page. Ex: Page 1 displays first 15 static entries. Page 2 displays Next 15 static entries.

- **Slot/Port** - interface
- **MAC Address** - MAC address.
- **VLAN ID** - VLAN id
- **IP Address** -IP address
- **Filter Type** - Filter Type
- **Remove** - This is to be selected to remove the particular binding entry.
- **Page** - Lists the Number of Pages the IPSG static binding entries occupied. Select the Page Number from this list to display the particular Page entries.

IPSG Dynamic Binding List - Lists all the IPSG dynamic binding entries page by page. Ex: Page 1 displays first available up to 15 dynamic entries. Page 2 displays Next available up to 15 dynamic entries.

- **Slot/Port** - interface
- **MAC Address** - MAC address.
- **VLAN ID** - VLAN id
- **IP Address** -IP address
- **Filter Type** - This tells you the IPSG filtering Type.

- **Page** - Lists the Number of Pages the IPSG dynamic binding entries occupied. Select the Page Number from this list to display the particular Page entries.

Command Buttons

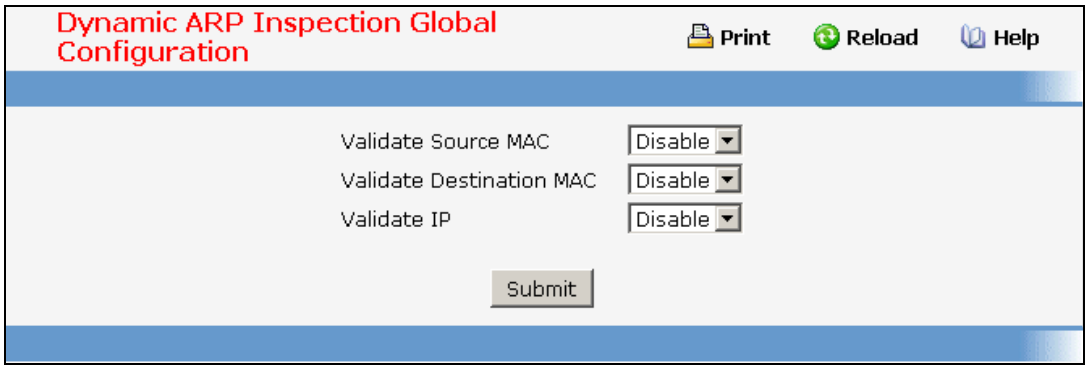
Add - Adds DHCP snooping binding entry into the database.

Submit - Deletes selected static entries from the database.

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

11.3.3 Managing Dynamic ARP Inspection (DAI)

11.3.3.1 Configuring DAI Global Configuration Page



Configurable Data

Validate Source MAC - Choose the DAI Source MAC Validation Mode for the switch by selecting Enable or Disable from the pull down menu. If you select Enable, Sender MAC validation for the ARP packets will be enabled. The factory default is disable.

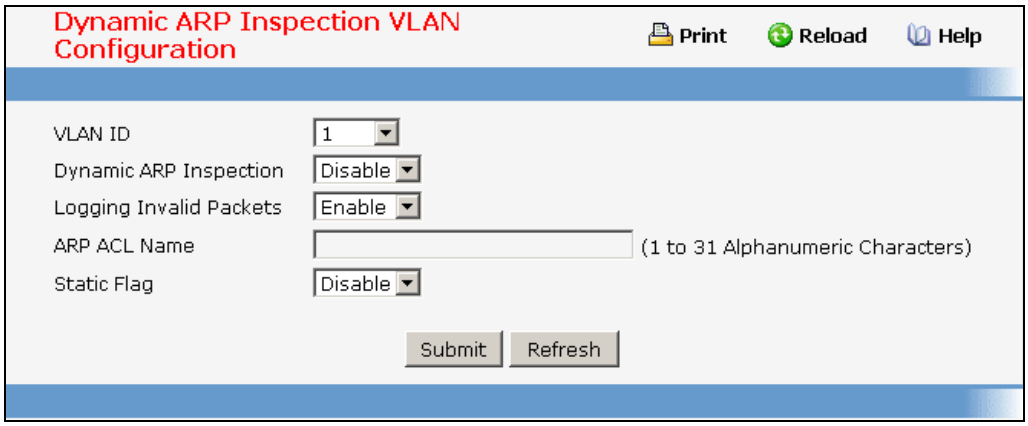
Validate Destination MAC - Choose the DAI Destination MAC Validation Mode for the switch by selecting Enable or Disable from the pull down menu. If you select Enable, Destination MAC validation for the ARP Response packets will be enabled. The factory default is disable.

Validate IP - Choose the DAI IP Validation Mode for the switch by selecting Enable or Disable from the pull down menu. If you select Enable, IP Address validation for the ARP packets will be enabled. The factory 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.

11.3.3.2 Configuring DAI VLAN Configuration Page



Selection Criteria

VLAN List - Select the DAI Capable VLANs for which information has to be displayed or configured.

Configurable Data

Dynamic ARP Inspection - Indicates whether the Dynamic ARP Inspection is enabled on this VLAN. If this object is set to 'Enable' Dynamic ARP Inspection is enabled. If this object is set to 'Disable', Dynamic ARP Inspection is disabled.

Logging Invalid Packets - Indicates whether the Dynamic ARP Inspection logging is enabled on this VLAN. If this object is set to 'Enable' it will log the Invalid ARP Packets information. If this object is set to 'Disable', Dynamic ARP Inspection logging is disabled.

ARP ACL Name - Name of ARP Access list. A vlan can be configured to use this ARP ACL containing rules as the filter for ARP packet validation. The name can contain up to <1-31> alphanumeric characters.

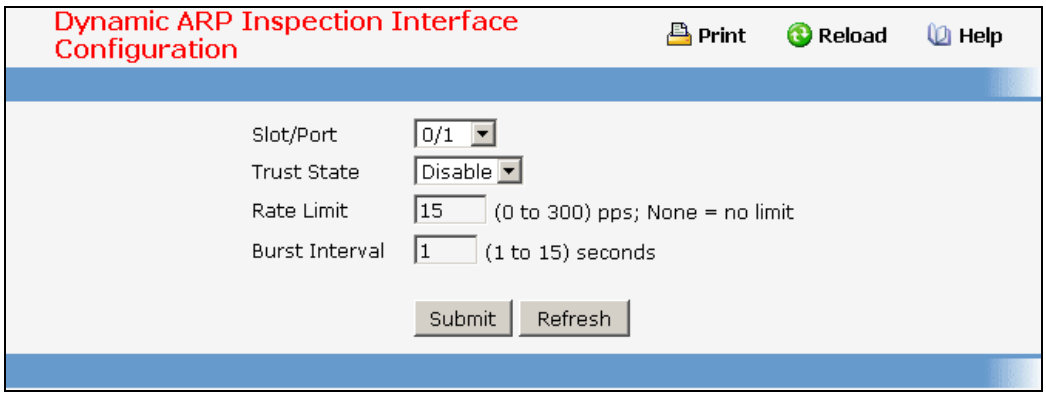
Static Flag - This flag is used to determine whether the ARP packet needs validation using the DHCP snooping database in case ARP ACL rules don't match. If the flag is enabled then the ARP Packet will be validated by the ARP ACL Rules only. If the flag is disabled then the ARP Packet needs further validation by using the DHCP Snooping entries. The factory default is disable.

Command Buttons

Submit - Update the switch with the values you entered.

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

11.3.3.3 Configuring DAI Interface Configuration Page



Selection Criteria

Slot/Port - Select the physical interface for which data is to be displayed or configured.

Configurable Data

Trusted State - Indicates whether the interface is trusted for Dynamic ARP Inspection purpose. If this object is set to 'Enable', the interface is trusted. ARP packets coming to this interface will be forwarded without checking. If this object is set to 'Disable', the interface is not trusted. ARP packets coming to this interface will be subjected to ARP inspection. The factory default is disable.

Rate Limit - Specifies rate limit value for Dynamic ARP Inspection purpose. If the incoming rate of ARP packets exceeds the value of this object for consecutively burst interval seconds, ARP packets will be dropped. If this value is None there is no limit. The factory default is 15pps (packets per second).

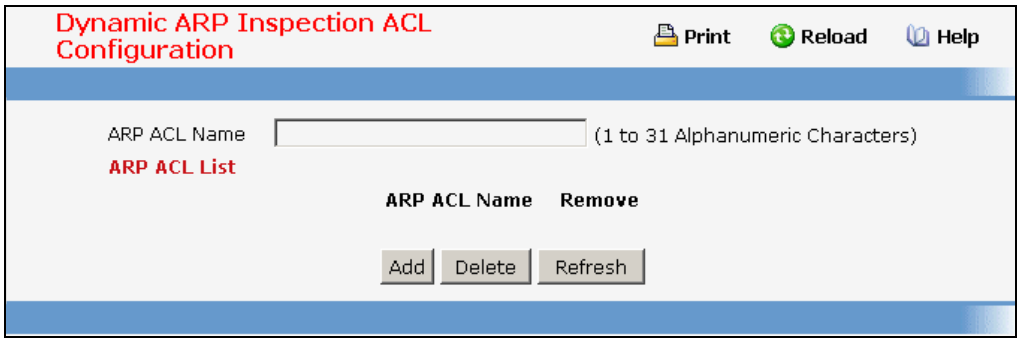
Burst Interval - This Specifies the burst interval value for rate limiting purpose on this interface. If the rate limit is None burst interval has no meaning shows it as N/A. The factory default is 1 second.

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.

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

11.3.3.4 Configuring DAI ARP ACL Configuration Page



Configurable Data

ARP ACL Name - This is used to create New ARP ACL for DAI.

Remove - This is used to select the particular ACLs which you want to delete.

Non-Configurable Data

ARP ACL Name - This will list all the configured ARP ACL List.

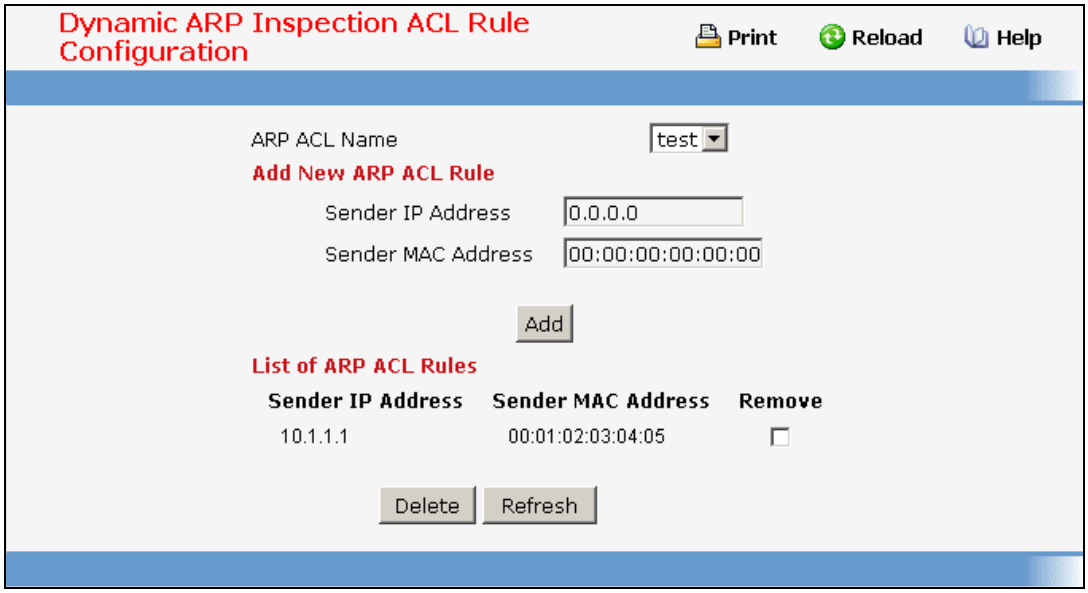
Command Buttons

Add - This is used to create New ARP ACL.

Delete - This is used to delete the entries selected using checkbox under Remove field.

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

11.3.3.5 Configuring DAI ARP ACL Rule Configuration Page



Selection Criteria

ARP ACL Name - Select the ARP ACL for which information want to be displayed or configured.

Configurable Data

Sender IP Address - This is used to create new Rule for the Selected ARP ACL. This indicates Sender IP address match value for the ARP ACL.

Sender MAC Address - This is used to create new Rule for the Selected ARP ACL. This indicates Sender MAC address match value for the ARP ACL.

Remove - This is used to select the particular ACL Rules which you want to delete.

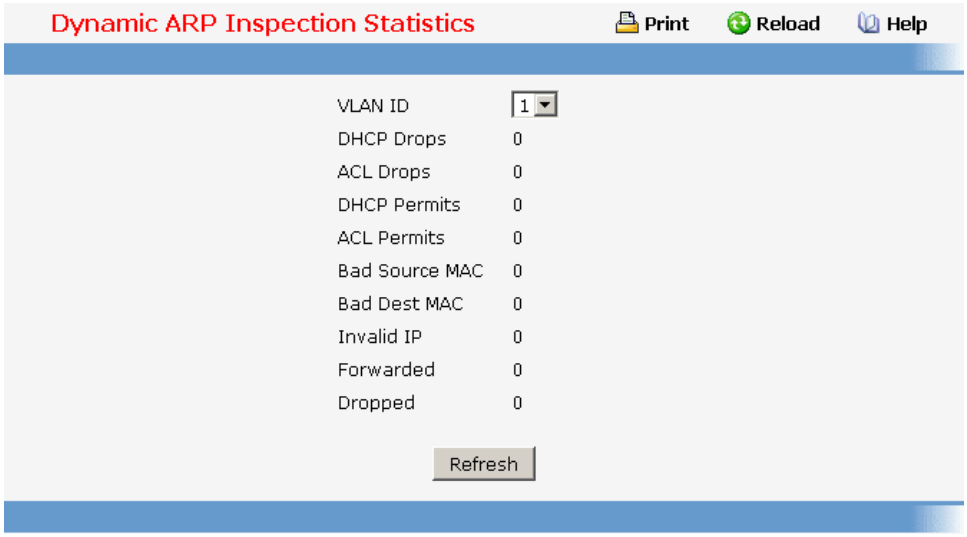
Command Buttons

Add - This is used to add new ACL Rule.

Submit - This is used to delete the entries selected using checkbox under Remove field.

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

11.3.3.6 Configuring DAI Statistics Page



Selection Criteria

VLAN ID - Select the DAI enabled VLAN ID for which statistics to be displayed.

Non-Configurable Data

DHCP Drops - Number of ARP packets that were dropped by DAI as there is no matching DHCP Snooping binding entry found.

ACL Drops - Number of ARP packets that were dropped by DAI as there is no matching ARP ACL rule found for this VLAN and the static flag is set on this VLAN.

DHCP Permits - Number of ARP packets that were forwarded by DAI as there is a matching DHCP Snooping binding entry found.

ACL Permits - Number of ARP packets that were permitted by DAI as there is a matching ARP ACL rule found for this VLAN.

Bad Source MAC - Number of ARP packets that were dropped by DAI as the sender MAC address in ARP packet didn't match the source MAC in ethernet header.

Bad Dest MAC - Number of ARP packets that were dropped by DAI as the target MAC address in ARP reply packet didn't match the destination MAC in ethernet header.

Invalid IP - Number of ARP packets that were dropped by DAI as the sender IP address in ARP packet or target IP address in ARP reply packet is invalid. Invalid addresses include 0.0.0.0, 255.255.255.255, IP multicast addresses, class E addresses (240.0.0.0/4), loopback addresses (127.0.0.0/8).

Forwarded - Number of valid ARP packets forwarded by DAI.

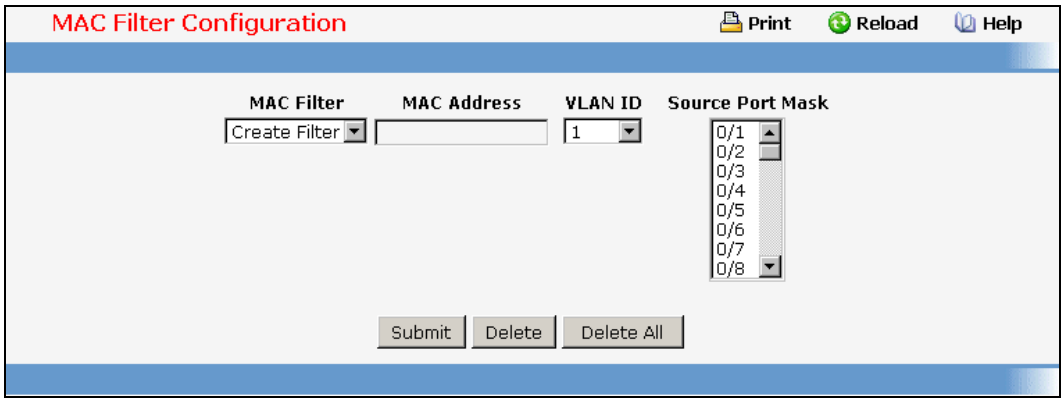
Dropped - Number of invalid ARP packets dropped by DAI.

Command Buttons

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

11.3.4 Managing Filters

11.3.4.1 Configuring MAC filter Configuration Page



Selection Criteria

MAC Filter - This is the list of MAC address and VLAN ID pairings for all configured filters. To change the port mask(s) for an existing filter, select the entry you want to change. To add a new filter, select "Create Filter" from the top of the list.

VLAN ID - The VLAN ID used with the MAC address to fully identify packets you want filtered. You can only change this field when you have selected the "Create Filter" option.

Configurable Data

MAC Address - The MAC address of the filter in the format 00:01:1A:B2:53:4D. You can only change this field when you have selected the "Create Filter" option.
You cannot define filters for these MAC addresses:

- 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
- FF:FF:FF:FF:FF:FF

Source Port Members - List the ports you want included in the inbound filter. If a packet with the MAC address and VLAN ID you selected is received on a port that is not in the list, it will be dropped.

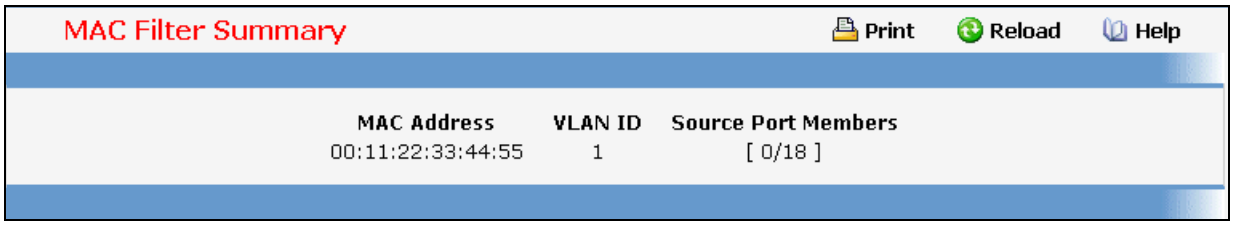
Command Buttons

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

Delete - Remove the currently selected filter.

Delete All - Remove all configured filters.

11.3.4.2 MAC filter Summary Page



Non-Configurable Data

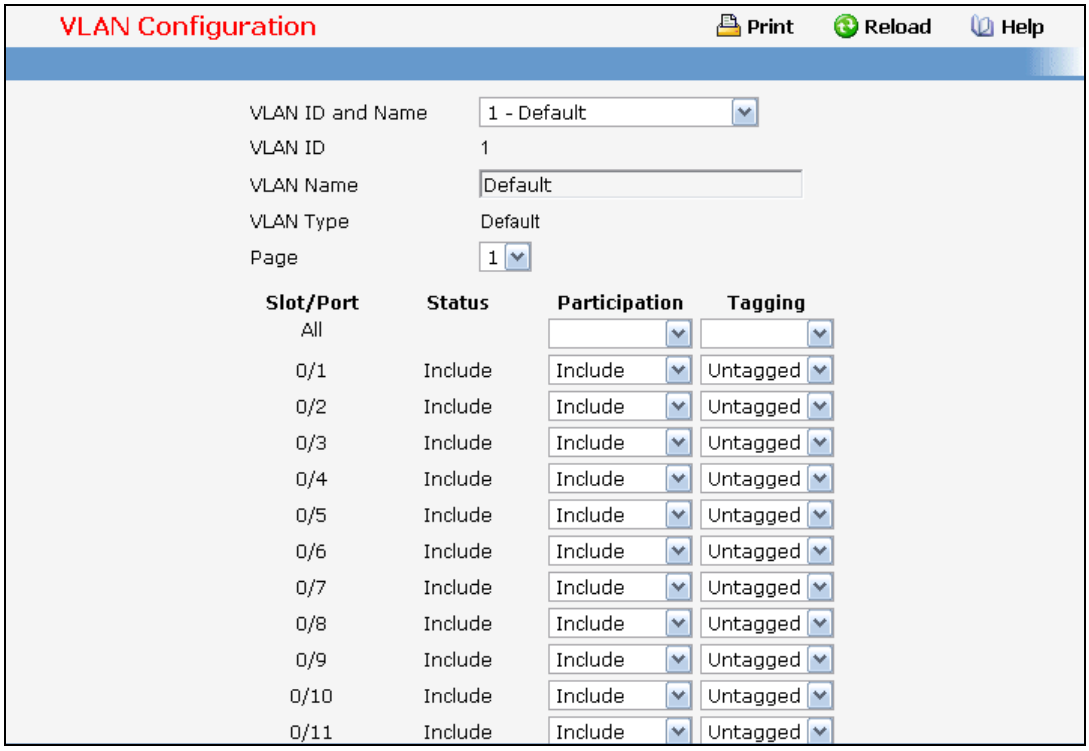
MAC Address - The MAC address of the filter in the format 00:01:1A:B2:53:4D.

VLAN ID - The VLAN ID associated with the filter.

Source Port Members - A list of ports to be used for filtering inbound packets.

11.3.5 Managing Port-based VLAN

11.3.5.1 Configuring Port-based VLAN Configuration Page



Selection Criteria

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

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.

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 3965).

VLAN Name - Use this optional field to specify a name for the VLAN. It can be up to 32 alphanumeric characters, 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'.

Non-Configurable Data

Slot/Port - Indicates which port is associated with the fields on this line.

Status - Indicates the current value of the participation parameter for the port.

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 this VLAN. You are not allowed to delete the default VLAN.

11.3.5.2 Viewing Port-based VLAN Information Page

This page displays the status of all currently configured VLANs.

Non-Configurable Data

VLAN ID - The VLAN Identifier (VID) of the VLAN. The range of the VLAN ID is (1 to 3965).

VLAN Name - The name of the VLAN. VLAN ID 1 is always named `Default`.

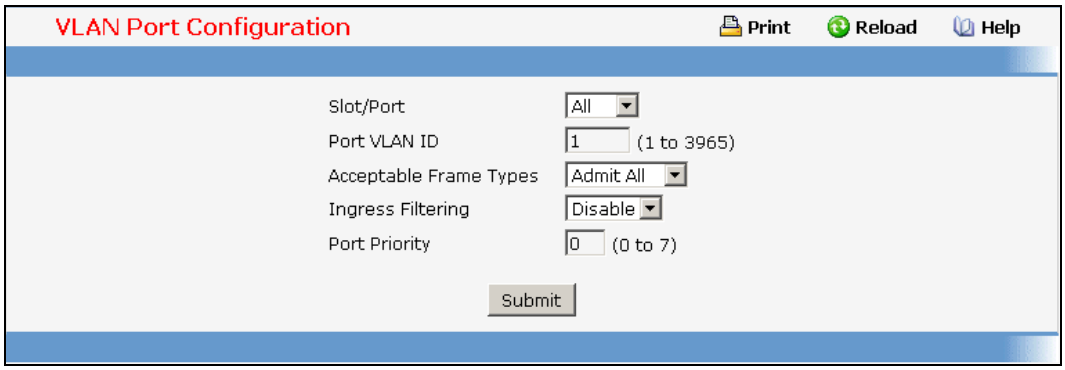
VLAN Type - The VLAN type:

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.

11.3.5.3 Configuring VLAN Port Configuration Page



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.

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 pull down 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 pull down menu, all tagged frames will be accepted. The factory default is disabled.

Configurable Data

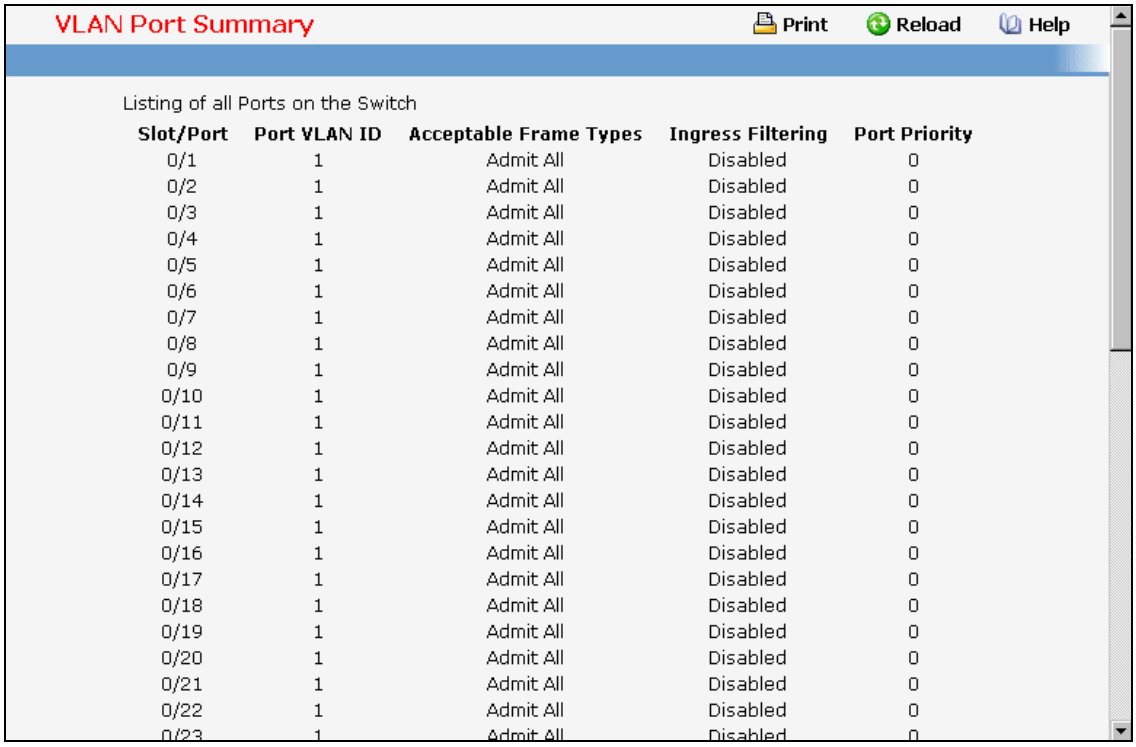
Port VLAN ID - Specify the VLAN ID you want assigned to untagged or priority tagged frames received on this port. The factory default is 1.

Port Priority - Specify the default 802.1p priority assigned to untagged packets arriving at the port.

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.

11.3.5.4 Viewing VLAN Port Summary Page



Non-Configurable Data

Slot/Port - The interface.

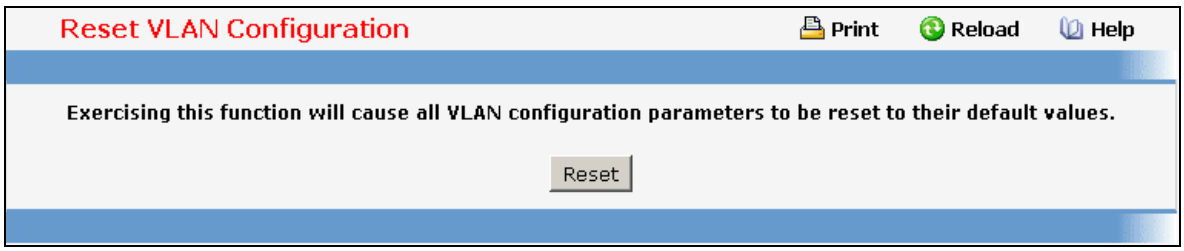
Port VLAN ID - The VLAN ID that this port will assign to untagged frames or priority tagged frames received on this port.

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.

Port Priority - Specifies the default 802.1p priority assigned to untagged packets arriving at the port.

11.3.5.5 Resetting VLAN Configuration Page



Command Buttons

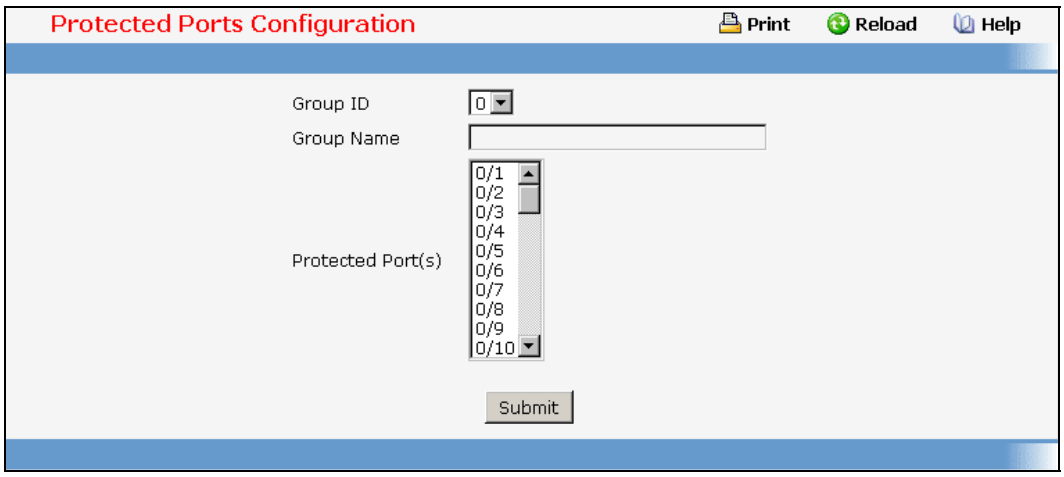
Reset - If you select this button and confirm your selection on the next screen, all VLAN configuration parameters will be reset to their factory default values. Also, all VLANs, except for the default VLAN, will be deleted. The factory default values are:

- 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.
- GMRP is disabled on all ports and all dynamic entries are cleared.
- GMRP is disabled for the switch and all dynamic entries are cleared.

11.3.6 Managing Protected Ports

11.3.6.1 Protected Ports Configuration Page

Use this menu to configure the ports as protected or unprotected. You need read-write access privileges to modify the configuration.



Selection Criteria

Group ID - The protected ports can be combined into a logical group. Traffic can flow between protected ports belonging to different groups, but not within the same group. The selection box lists all the possible protected port Group IDs supported for the current platform. The valid range of the Group ID is (0 to 2) .

Configurable Data

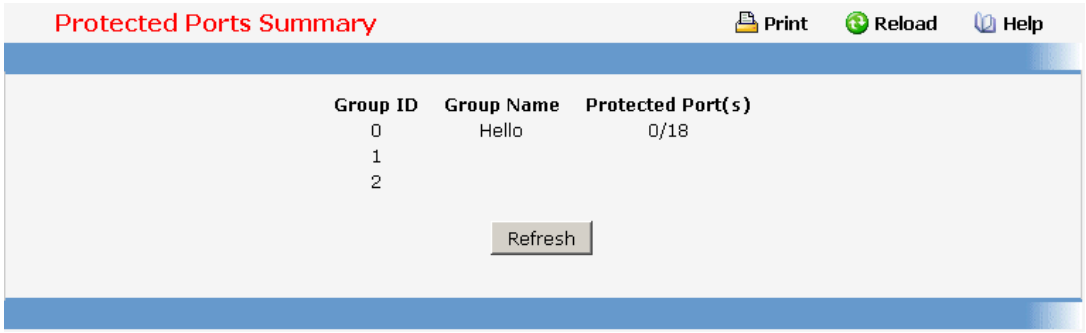
Group Name - It is a name associated with the protected ports group used for identification purposes. It can be up to 32 alphanumeric characters long, including blanks. The default is blank. This field is optional.

Protected Ports - The selection list consists of physical ports, protected as well as unprotected. The protected ports are highlighted to differentiate between them. No traffic forwarding is possible between two protected ports. If left unconfigured, the default state is unprotected.

Command Buttons

Submit - Update the switch with the values entered. For the switch to retain new values across a power cycle, a save operation is a must.

11.3.6.2 Protected Ports Summary Page



Non-Configurable Data

Group ID - The protected ports can be combined into a logical group. Traffic can flow between protected ports belonging to different groups, but not within the same group. The valid range of the Group ID is (0 to 2) .

Group Name - Displays the alphanumeric string associated with a Group ID.

Protected Ports - The display list consists of all the protected ports. It is to be noted that no traffic forwarding is possible between two protected ports of a same group, but traffic can flow between protected ports of different groups.

Command Buttons

Refresh - Refresh the data on the screen to obtain data on current state of the ports.

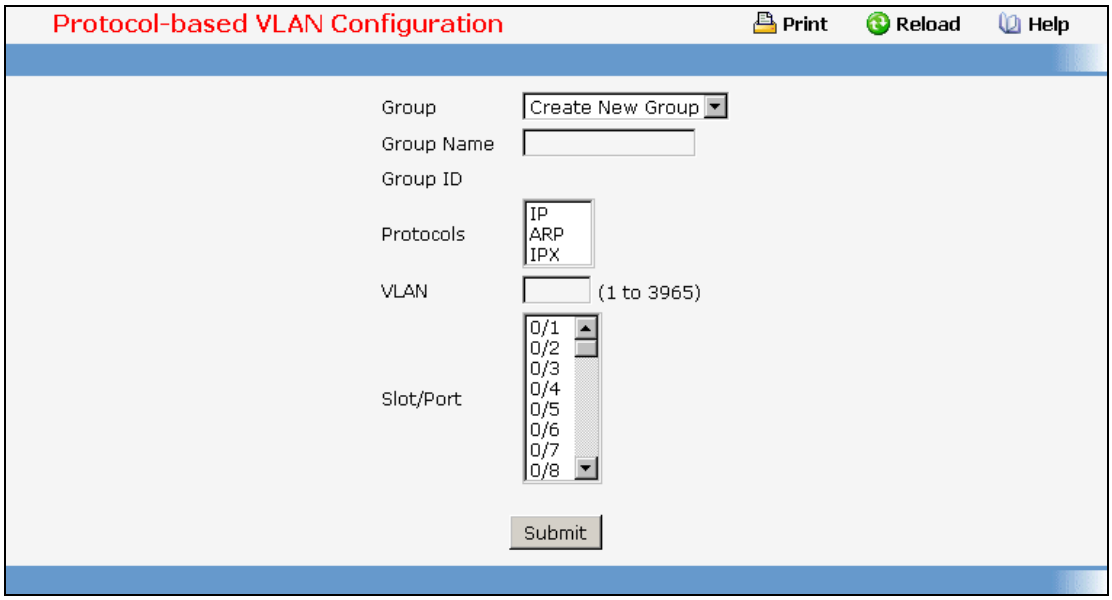
11.3.7 Managing Protocol-based VLAN

11.3.7.1 Protocol-based VLAN Configuration Page

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.



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 pull down 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, and 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 3965) . 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.

Non-Configurable Data

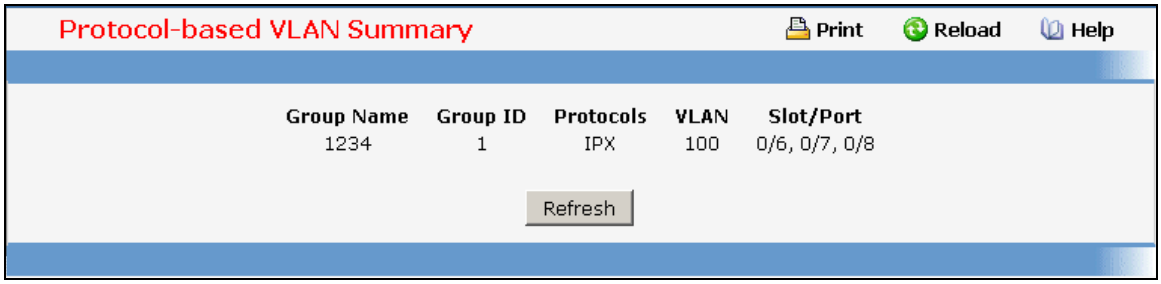
Group ID - A number used to identify the group created by the user. Group IDs are automatically assigned when a group is created by the user.

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 - Remove the Protocol Based VLAN group identified by the value in the Group ID field. If you want the switch to retain the deletion across a power cycle, you must perform a save.

11.3.7.2 Viewing Protocol-based VLAN Information Page



Non-Configurable Data

Group Name - The name associated with the group. Group names can be up to 16 characters. 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, and 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.

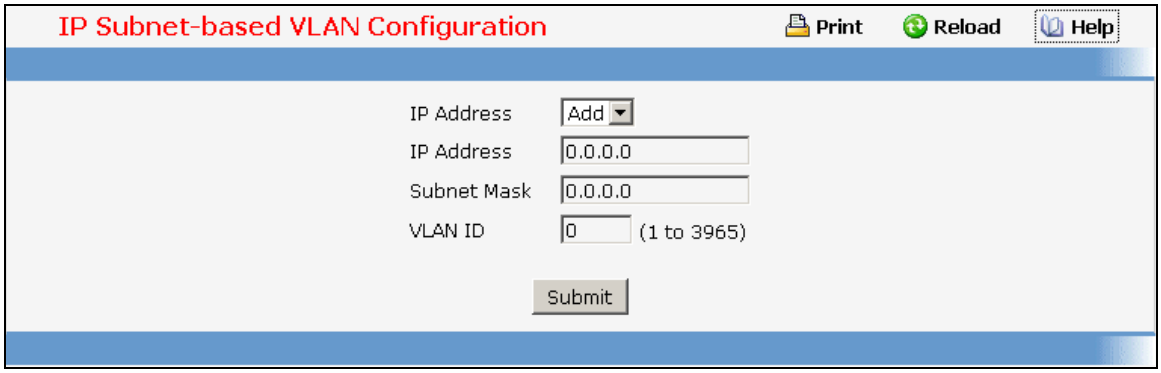
Command Buttons

Refresh - Update the screen with the latest information.

11.3.8 Managing IP Subnet-based VLAN

11.3.8.1 IP Subnet-based VLAN Configuration Page

IP Subnet to VLAN mapping is defined by configuring an entry in the IP Subnet to VLAN table. An entry is specified via a source IP address, network mask, and the desired VLAN ID. The IP Subnet to VLAN configurations are shared across all ports of the device.



Selection Criteria

IP Address - Selects the IP Address bound to a VLAN ID. To add another IP Subnet-based VLAN, select "Add" option.

Configurable Data

IP Address - Valid IP Address bound to VLAN ID. This field is configurable only when a new IP Subnet Based VLAN is being created. IP Address in dotted decimal notation.

Subnet Mask - Valid Subnet Mask of the IP Address. This field is configurable only when a new IP Subnet-based VLAN is being created. Subnet mask should be in dotted decimal notation.

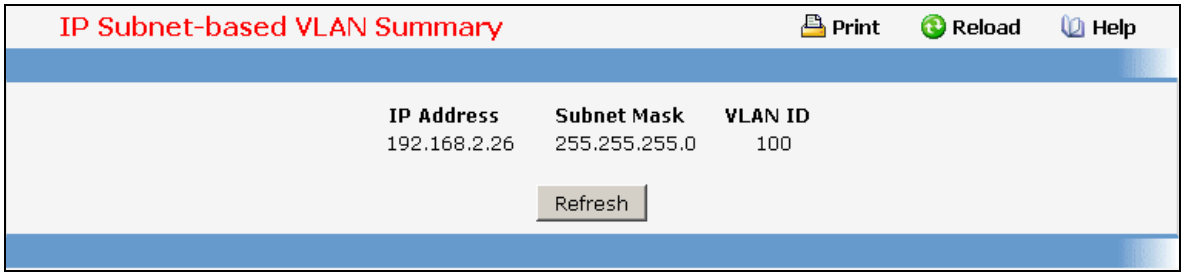
VLAN ID - VLAN ID can be any number in the range of (1 to 3965).

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 an entry of IP Subnet to VLAN mapping.

11.3.8.2 Viewing IP Subnet-based VLAN Information Page



Non-Configurable Data

IP Address - The IP Address of the subnet that is being bound to a VLAN ID.

Subnet Mask - Subnet mask of the IP Address bound to VLAN ID.

VLAN ID - VLAN ID to which above mentioned IP Subnet is being bound to. VLAN ID can be any number in the range of (1 to 3965).

Command Buttons

Refresh - Update the screen with the latest information.

11.3.9 Managing MAC-based VLAN

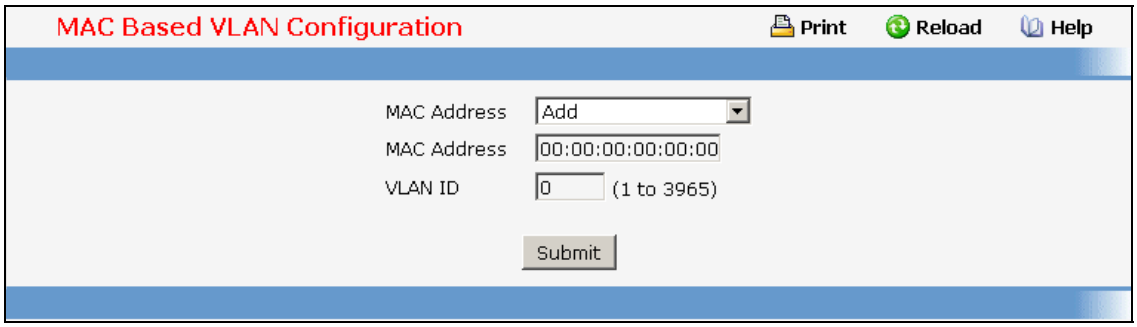
11.3.9.1 MAC-based VLAN Configuration Page

MAC-based VLAN feature allows incoming untagged packets to be assigned to a VLAN and thus classify traffic based on the source MAC address of the packet.

A MAC to VLAN mapping is defined by configuring an entry in the MAC to VLAN table. An entry is specified via a source MAC address and the desired VLAN ID. The MAC to VLAN configurations are shared across all ports of the device (i.e. there is a system wide table that has MAC address to VLAN ID mappings).

When untagged or priority tagged packets arrive at the switch and entries exist in the MAC to VLAN table, the source MAC address of the packet is looked up. If an entry is found the corresponding VLAN ID is assigned to the packet. If the packet is already priority tagged it will maintain this value, otherwise the priority will be set to zero. The assigned VLAN ID is verified against the VLAN table, if the VLAN is valid

ingress processing on the packet continues, otherwise the packet is dropped. This implies that the user is allowed to configure a MAC address mapping to a VLAN that has not been created on the system.



Configurable Data

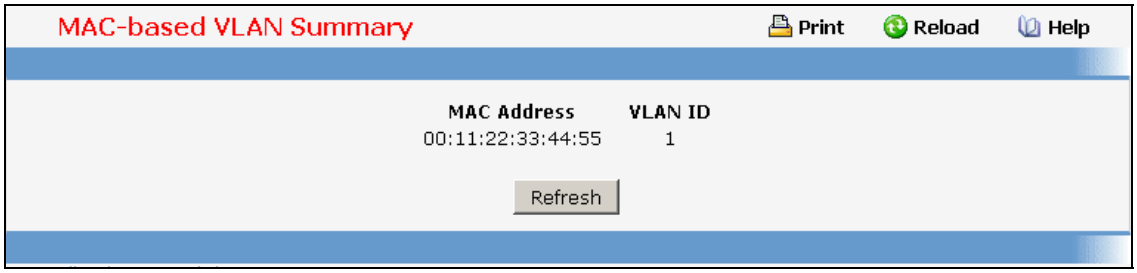
MAC Address - Valid MAC Address which is to be bound to a VLAN ID. This field is configurable only when a MAC-based VLAN is created.

VLAN ID - VLAN ID can be any number in the range of (1 to 3965).

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.

11.3.9.2 Viewing MAC-based VLAN Information Page



Non-Configurable Data

MAC Address - MAC Address bound to a VLAN ID.

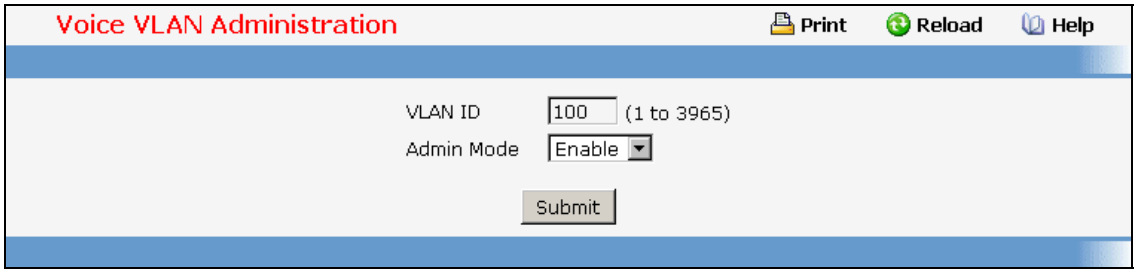
VLAN ID - The VLAN ID to which a MAC Address is bound.

Command Buttons

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

11.3.10 Managing MAC-based Voice VLAN

11.3.10.1 Voice VLAN Administration Page



Configurable Data

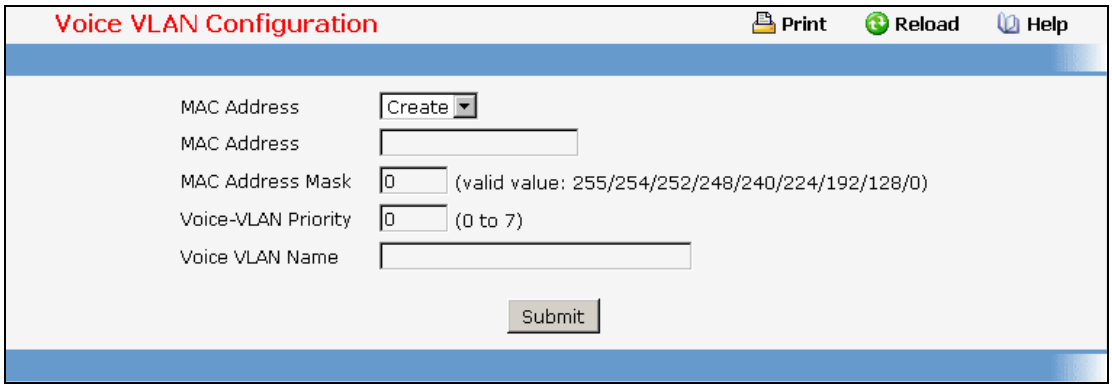
VLAN ID - Sets the VLAN as a Voice VLAN.

Admin Mode - Enables or disables the Voice VLAN function.

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.

11.3.10.2 Voice VLAN Configuration Page



Selection Criteria

MAC Address - You can use this screen to create a new one. Use this pulldown menu to select one of the existing Voice VLANs, or select 'Create' to add a new one.

You cannot define MAC for these addresses:

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

01:00:5E:00:00:00 to 01:00:5E:FF:FF:FF

33:33:00:00:00:00 to 33:33:FF:FF:FF:FF

FF:FF:FF:FF:FF:FF

Configurable Data

MAC Address - Specify the MAC Address for the new Voice VLAN. (You can only enter data in this field when you are creating a new Voice VLAN.).

MAC Address Mask - Use this optional field to specify a mask for the Voice VLAN. The mac-mask is the last eight digit of the mask code of the MAC address, the valid values are: 0xff, 0xfe, 0xfc, 0xf8, 0xf0, 0xe0, 0xc0, 0x80 and 0x0.

Voice-VLAN Priority - This field identifies the priority of the Voice VLAN you are configuring. The priority-id is the priority of the voice traffic; the valid range is 0 to 7.

Voice VLAN Name - Use this field to specify the name of the voice device. It is to help the device management.

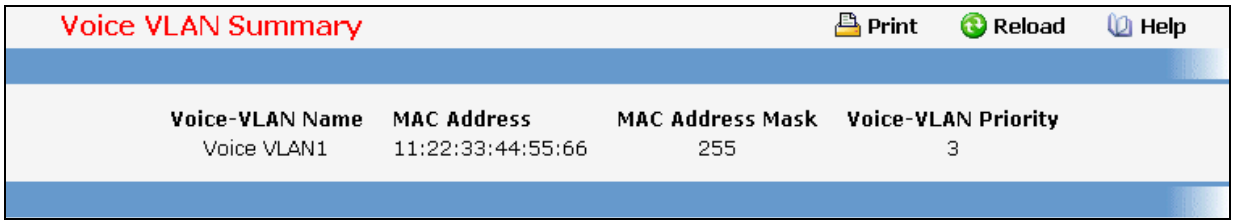
Command Buttons

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 this VLAN. You are not allowed to delete the default VLAN.

11.3.10.3 Viewing Voice VLAN Information Page

This page displays the status of all currently configured Voice VLANs.



Non-Configurable Data

Voice-VLAN Name - The name of the voice device.

MAC Address - The MAC Address for the new Voice VLAN.

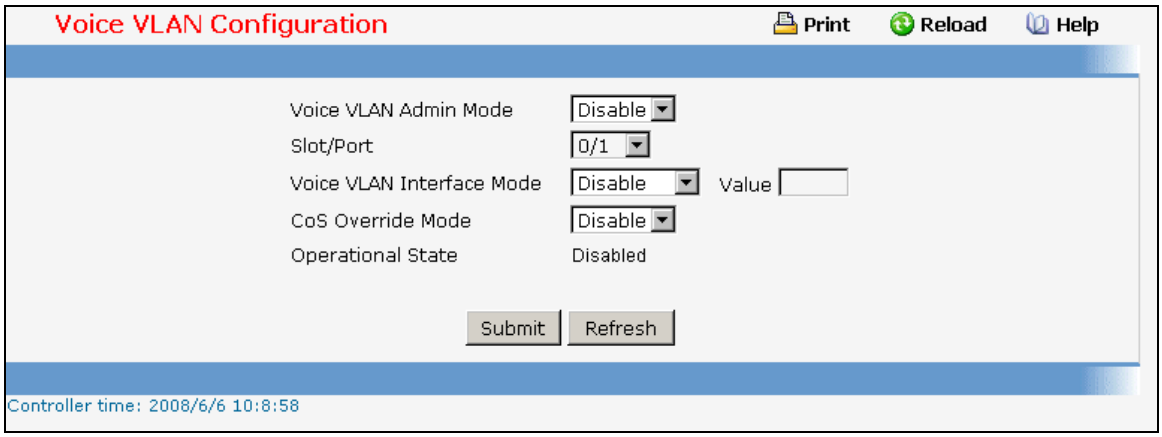
MAC Address Mask - The MAC Address Mask for the Voice VLAN. The value is the last eight digit of the mask code of the MAC address.

Voice-VLAN Priority - The priority-id is the priority of the voice traffic.

11.3.11 Managing Voice VLAN

11.3.11.1 Voice VLAN Configuration Page

Use this menu to configure the parameters for Voice VLAN Configuration. Note that only a user with Read/Write access privileges may change the data on this screen.



Selection Criteria

Voice VLAN Admin Mode - Select the administrative mode for Voice VLAN for the switch from the pulldown menu. The default is disable.

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

Voice VLAN Interface Mode - Select the Voice VLAN mode for selected interface.

Disable - Default value

None - Allow the IP phone to use its own configuration to send untagged voice traffic

VLAN ID - Enter the Voice Vlan Id

dot1p - Configure Voice Vlan 802.1p priority tagging for voice traffic.

Untagged - Configure the phone to send untagged voice traffic.

CoS Override Mode - Select the Cos Override mode for selected interface. The default is disable.

Non-Configurable Data

Operational State - This is the operational status of the voice vlan on the given interface.

Command Buttons

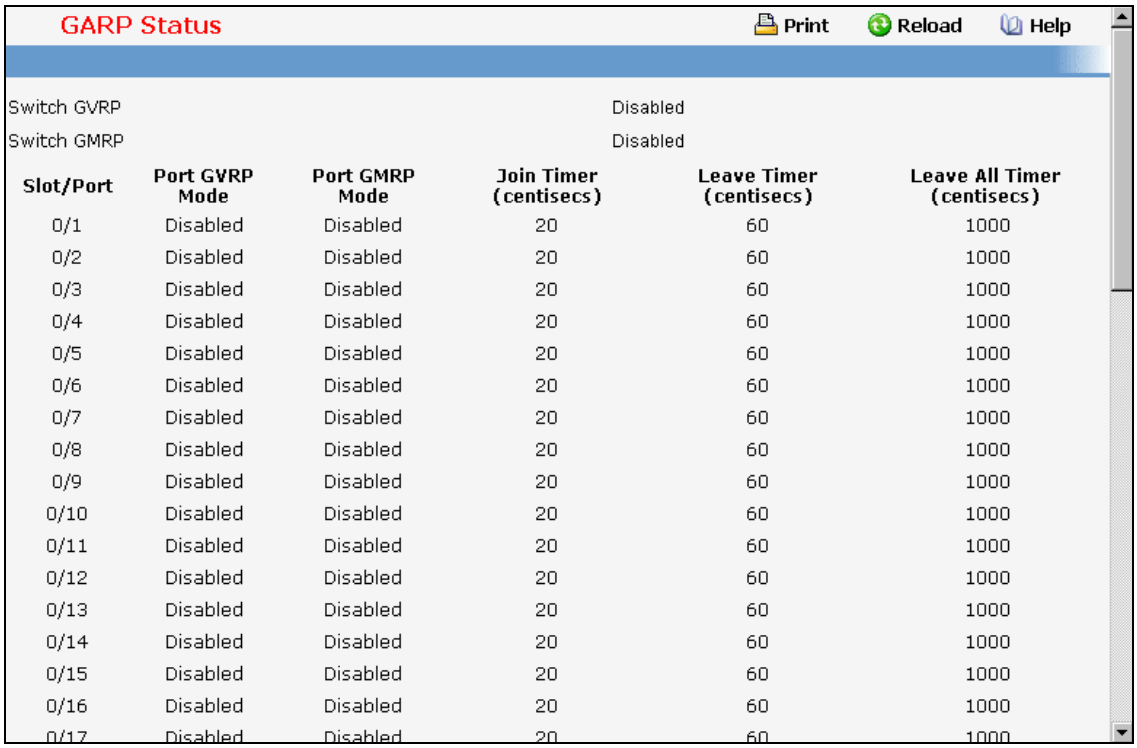
Submit - Update the switch with the values you entered. If you want the switch to retain the new values across a power cycle you must perform a save. You will only see this button if you have Read/Write access privileges.

Refresh - Reload the contents of the configuration page.

11.3.12 Defining GARP

11.3.12.1 Viewing GARP Information Page

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.



Slot/Port	Port GVRP Mode	Port GMRP Mode	Join Timer (centisecs)	Leave Timer (centisecs)	Leave All Timer (centisecs)
0/1	Disabled	Disabled	20	60	1000
0/2	Disabled	Disabled	20	60	1000
0/3	Disabled	Disabled	20	60	1000
0/4	Disabled	Disabled	20	60	1000
0/5	Disabled	Disabled	20	60	1000
0/6	Disabled	Disabled	20	60	1000
0/7	Disabled	Disabled	20	60	1000
0/8	Disabled	Disabled	20	60	1000
0/9	Disabled	Disabled	20	60	1000
0/10	Disabled	Disabled	20	60	1000
0/11	Disabled	Disabled	20	60	1000
0/12	Disabled	Disabled	20	60	1000
0/13	Disabled	Disabled	20	60	1000
0/14	Disabled	Disabled	20	60	1000
0/15	Disabled	Disabled	20	60	1000
0/16	Disabled	Disabled	20	60	1000
0/17	Disabled	Disabled	20	60	1000

Non-Configurable Data

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.

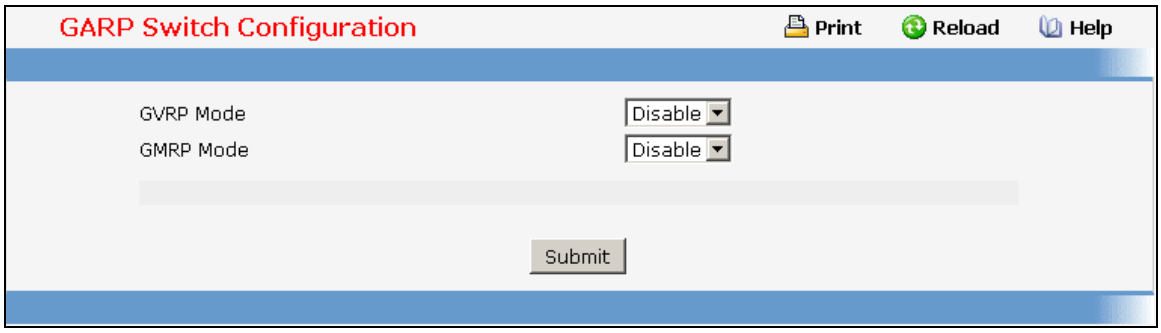
Join Time (centiseconds) - Specifies the time between the transmission of GARP PDUs registering (or re-registering) membership for a VLAN or multicast group in centiseconds. An instance of this timer exists for each GARP participant for each port. Permissible values are 10 to 100 centiseconds (0.1 to 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).

11.3.12.2 Configuring the whole Switch GARP Configuration Page



It can take up to 10 seconds for GARP configuration changes to take effect.

Selection Criteria

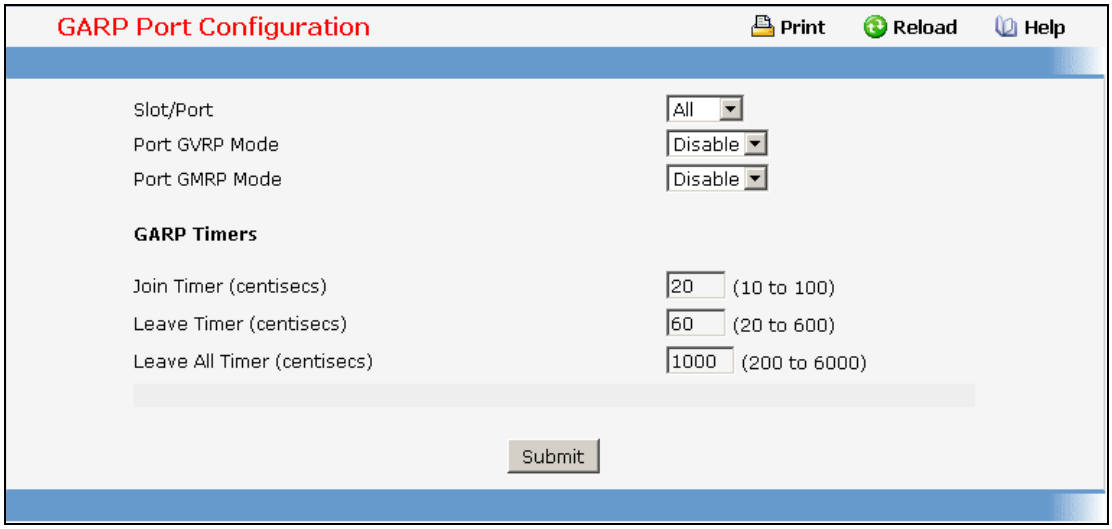
GVRP Mode - Choose the GARP VLAN Registration Protocol administrative mode for the switch by selecting enable or disable from the pull down menu. The factory default is disabled.

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.

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.

11.3.12.3 Configuring each Port GARP Configuration Page



It can take up to 10 seconds for GARP configuration changes to take effect.

Selection Criteria

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.

Configurable Data

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.

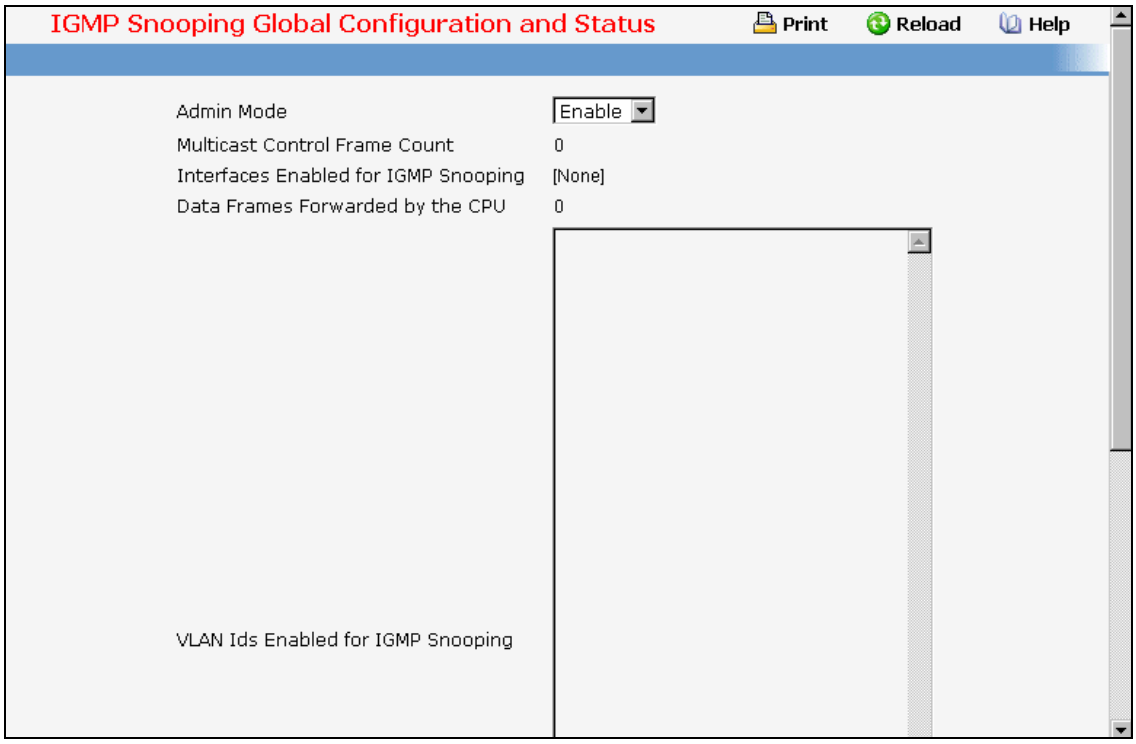
Command Buttons

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.

11.3.13 Managing IGMP Snooping

11.3.13.1 Configuring IGMP Snooping Global Configuration Page

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.



Selection Criteria

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.

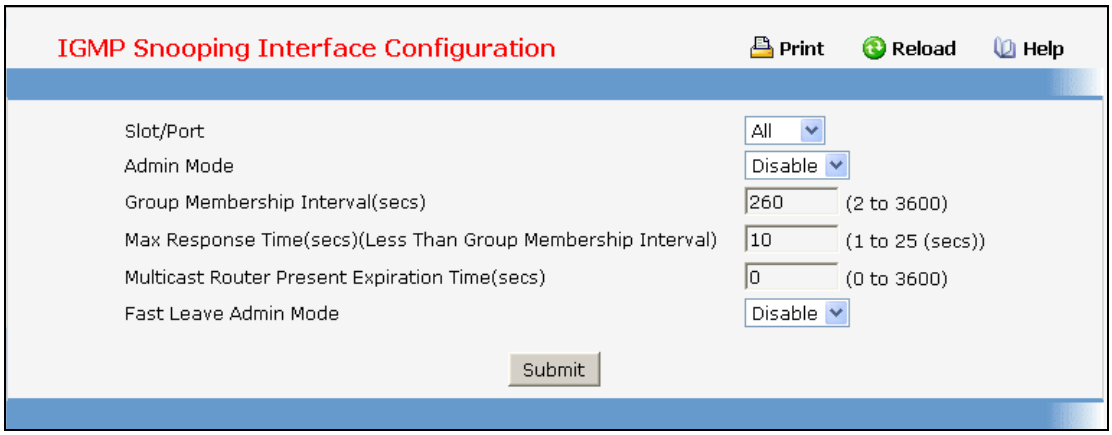
Data Frames Forwarded by the CPU - The number of data frames forwarded by the CPU.

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.

11.3.13.2 Defining IGMP Snooping Interface Configuration Page



Selection Criteria

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.

Fast Leave Admin mode - Select the Fast Leave mode for the a particular interface from the pulldown menu. The default is disable.

Configurable Data

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.

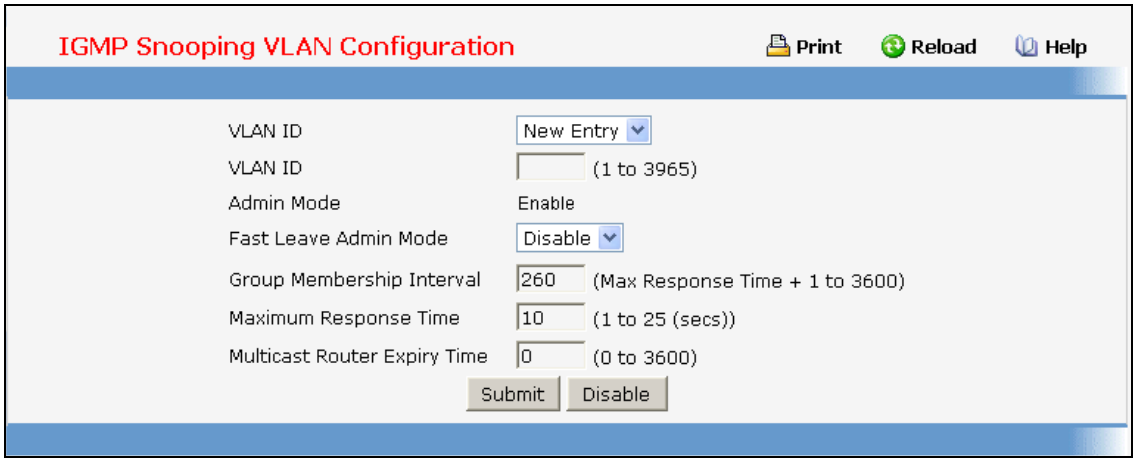
Max Response Time - Specify the amount of time you want the switch to wait after sending a query on an interface because it did not receive a report for a particular group on that interface. Enter a value greater or equal to 1 and less than the Group Membership Interval in seconds. The default is 10 seconds. The configured value must between 1 to 25 (secs). 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.

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.

11.3.13.3 Configuring IGMP Snooping VLAN Page



Selection Criteria

VLAN ID - Specifies list of VLAN IDs for which IGMP Snooping is enabled.

Fast Leave Admin Mode - Enable or disable the Igmp Snooping Fast Leave Mode for the specified VLAN ID.

Configurable Data

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 or disable the Igmp Snooping 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 25. Its value should be less 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.

Disable - Update the switch with the default values.

11.3.13.4 Viewing IGMP Snooping VLAN Status Page

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.

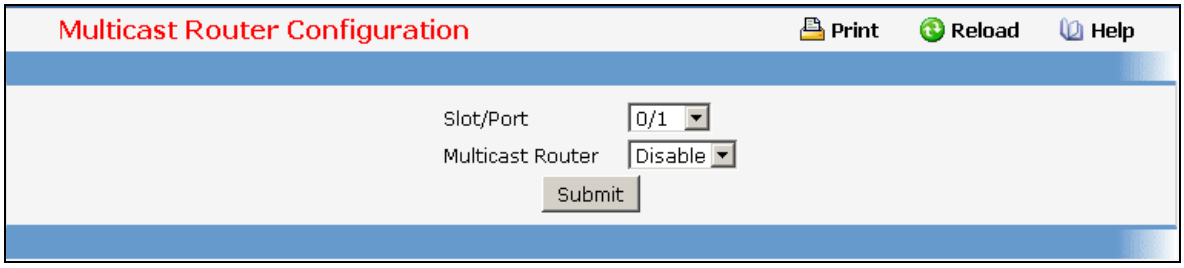
Maximum Response Time - Maximum Response Time of IGMP Snooping for the specified VLAN ID. Valid range is 1 to 3599.Its value should be greater than group membership interval value.

Multicast Router Expiry Time - Multicast Router Expiry Time of IGMP Snooping for the specified VLAN ID. Valid range is 0 to 3600.

Configurable Data

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

11.3.13.5 Configuring Multicast Router Page



Selection Criteria

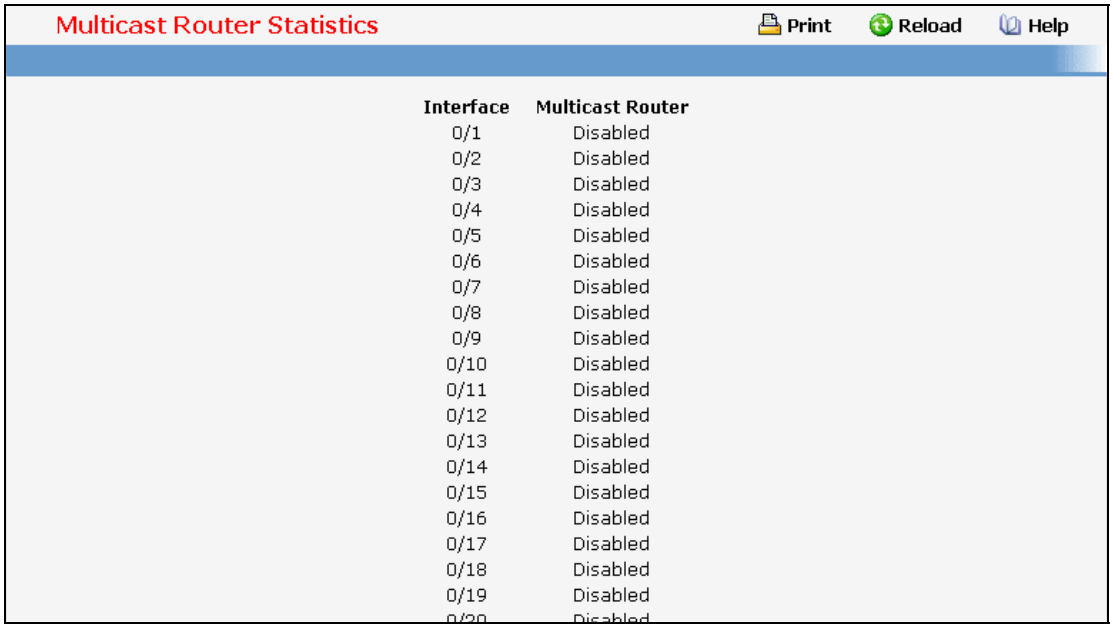
Slot/Port - The select box lists all Slot/Ports. Select the interface for which you want Multicast Router to be enabled .

Multicast Router - Enable or disable Multicast Router on the selected Slot/Port.

Command Buttons

Submit - Update the switch with the values you entered.

11.3.13.6 Viewing Multicast Router Statistics Page



Selection Criteria

Slot/Port - The single select box lists all physical and LAG interfaces. Select the interface for which you want to display the statistics.

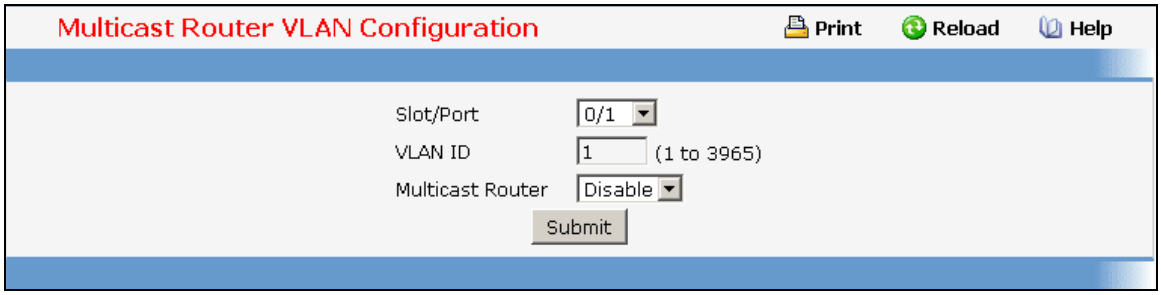
Non-Configurable Data

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.

11.3.13.7 Configuring Multicast Router VLAN Page



Selection Criteria

Slot/Port - The select box lists all Slot/Ports.Select the interface for which you want Multicast Router to be enabled.

Multicast Router - For the Vlan ID, multicast router may be enabled or disabled using this.

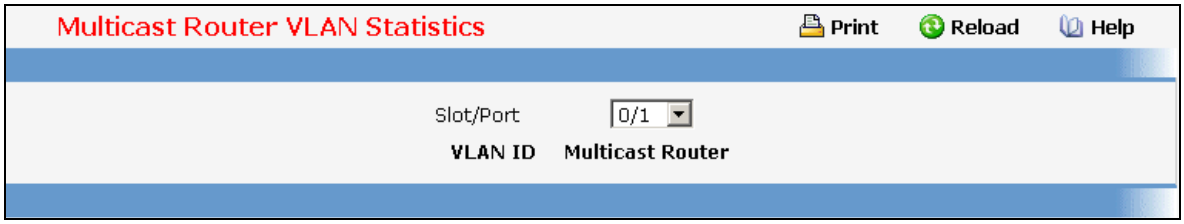
Configurable Data

VLAN ID - VLAN ID for which the Multicast Router Mode is to be Enabled or Disabled.

Command Buttons

Submit - Update the switch with the values you entered.

11.3.13.8 Viewing Multicast Router VLAN Statistics Page



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

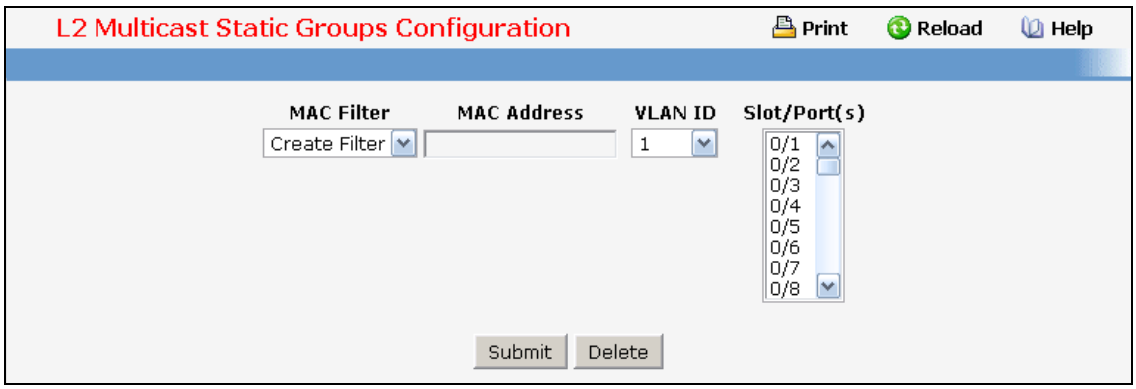
VLAN ID - All Vlan Ids for which the Multicast Router Mode is Enabled

Multicast Router - Multicast Router Mode for Vlan ID.

Command Buttons

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

11.3.13.9 Configuring L2 Static Multicast Group Configuration Page



Selection Criteria

MAC Filter - This is the list of MAC address and VLAN ID pairings for all configured L2Mcast Groups. To change the port mask(s) for an existing L2Mcast Group, select the entry you want to change. To add a new L2Mcast Group, select "Create Filter" from the top of the list.

VLAN ID - The VLAN ID used with the MAC address to fully identify packets you want L2Mcast Group. You can only change this field when you have selected the "Create Filter" option.

Configurable Data

MAC Address - The MAC address of the L2Mcast Group in the format 01:00:5E:xx:xx:xx. You can only change this field when you have selected the "**Create Filter**" option. You cannot define L2Mcast Group for these MAC addresses:

00:00:00:00:00:00

01:00:5E:00:00:01 to 01:00:5E:00:00:FF

FF:FF:FF:FF:FF:FF

Solt/Port(s) - List the ports you want included into L2Mcast Group.

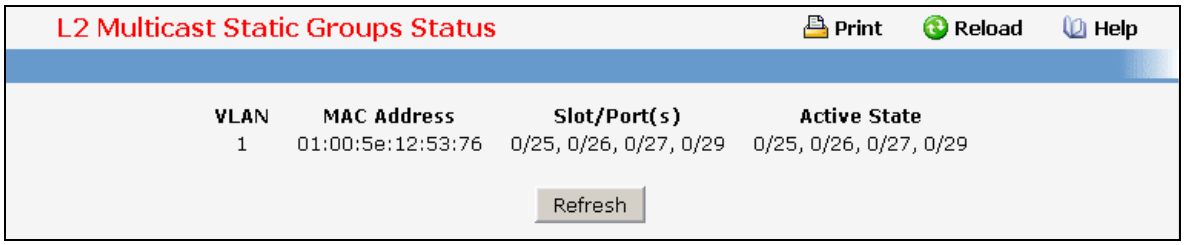
Command Buttons

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

Delete - Remove the currently selected L2Mcast Group.

11.3.13.10 Viewing L2 Multicast Group Status Page

Use this panel to display information about entries in the L2Mcast Static/Dynamic Groups. These entries are used by the transparent bridging function to determine how to forward a received frame.



Non-Configurable Data

VLAN - L2Mcast Group's VLAN ID value.

MAC Address - A multicast MAC address for which the switch has forwarding information. The format is a six-byte MAC address. For example: 01:00:5E:00:11:11.

Slot/Ports - the interface number belongs to this Multicast Group.

Active State - The active interface number belongs to this Multicast Group.

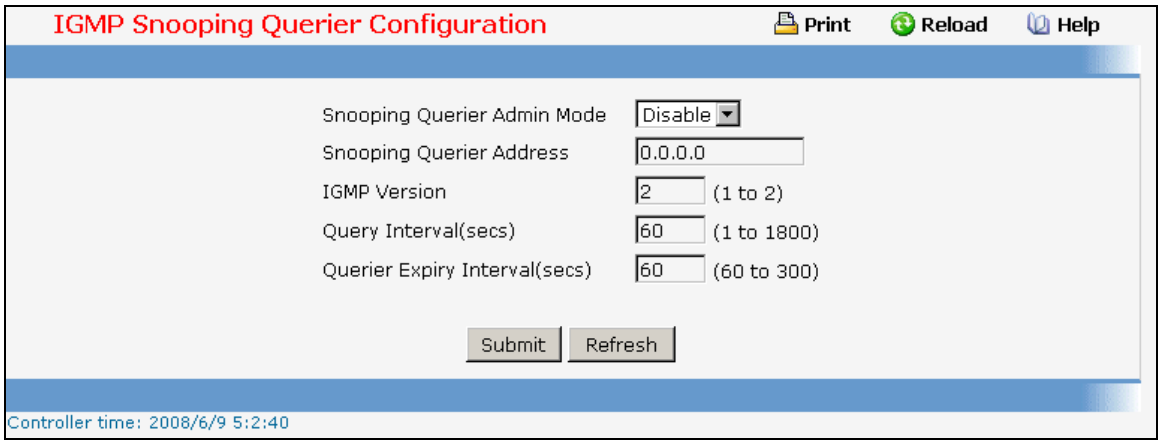
Command Buttons

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

11.3.14 Managing IGMP Snooping Querier

11.3.14.1 Configuring IGMP Snooping Querier Configuration Page

Use this menu to configure the parameters for IGMP Snooping Querier, Note that only a user with Read/Write access privileges may change the data on this screen.



Selection Criteria

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

Configurable Data

Snooping Querier Address - Specify the Snooping Querier Address to be used as source address in periodic IGMP queries. This address is used when no address is configured on the VLAN on which query is being sent.

IGMP Version - Specify the IGMP protocol version used in periodic IGMP queries. IGMP queries.

Query Interval - Specify the time interval in seconds between periodic queries sent by the snooping querier. The Query Interval must be a value in the range of 1 and 1800. The default value is 60.

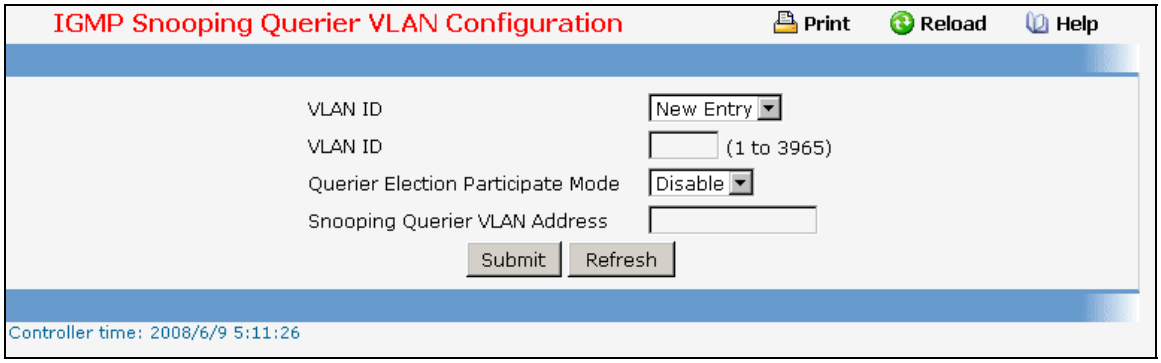
Querier Expiry Interval - Specify the time interval in seconds after which the last querier information is removed. The Querier Expiry Interval must be a value in the range of 60 and 300. The default value is 60.

Command Buttons

Submit - Update the switch with the configured values.

Refresh - Reload the information on the page.

11.3.14.2 Configuring IGMP Snooping Querier VLAN Configuration Page



Selection Criteria

VLAN ID - Selects the VLAN ID on which IGMP Snooping Querier is enabled.

Querier Election Participate Mode - Enable or disable the Igmp Snooping Querier participate in election mode. When this mode is disabled, up on seeing other querier of same version in the vlan, the snooping querier move to non querier state. Only when this mode is enabled, the snooping querier will participate in querier election where in the least ip address will win the querier election and operates as the querier in that VLAN. The other querier moves to non-querier state.

Configurable Data

VLAN ID - Appears when "New Entry" is selected in VLAN ID selection list. Specifies VLAN ID for which IGMP Snooping Querier is to be enabled. User can also set pre-configurable Snooping Querier parameters.

Snooping Querier VLAN Address - Specify the Snooping Querier Address to be used as source address in periodic IGMP queries sent on the specified VLAN.

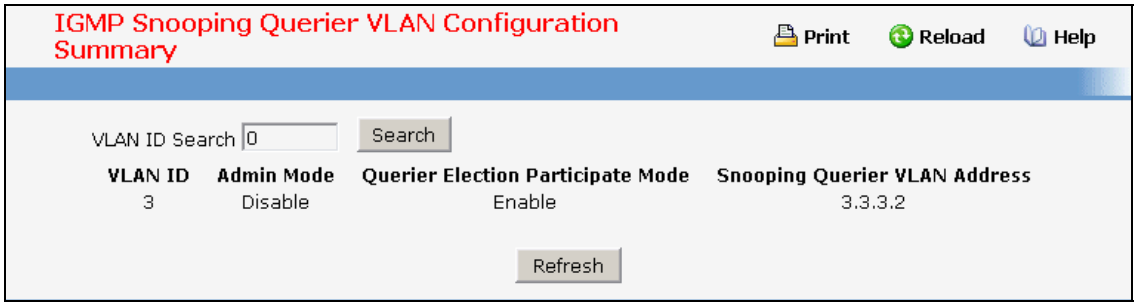
Configurable Button

Submit - Update the switch with the configured values.

Delete - To disable Snooping Querier on the selected VLAN. This button is not visible when a VLAN is not selected.

Refresh - Reload the information on the page.

11.3.14.3 IGMP Snooping Querier VLAN Configuration Summary Page



Configurable Data

VLAN ID Search- Enter VLAN ID, then click on the search button. If the record exists, that entry will be displayed. An exact match is required.

Non-Configurable Data

Admin Mode - Display the administrative mode for IGMP Snooping for the switch.

VLAN ID Search- Enter VLAN ID, then click on the search button. If the record exists, that entry will be displayed. An exact match is required.

Querier Election Participate Mode - Displays the querier election participate mode on the VLAN. When this mode is disabled, up on seeing a query of the same version in the vlan, the snooping querier move to non querier state. Only when this mode is enabled, the snooping querier will participate in querier election where in the least ip address will win the querier election and operates as the querier in that VLAN. The other querier moves to non-querier state.

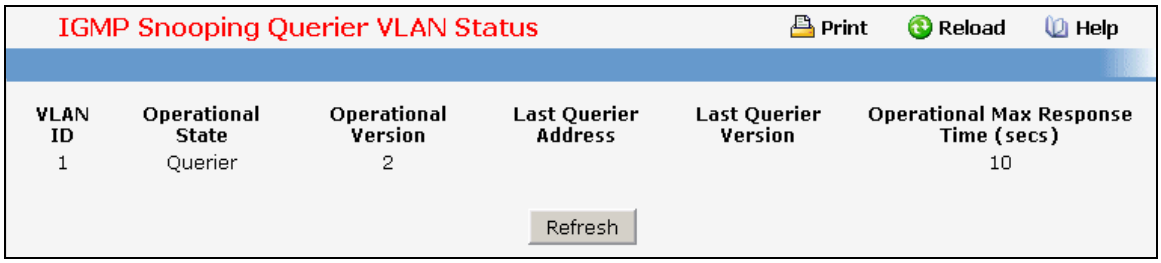
Snooping Querier VLAN Address - Displays the Snooping Querier Address to be used as source address in periodic IGMP queries sent on the specified VLAN.

Command Buttons

Search - Search for the specified Vlan ID.

Refresh - Reload the information on the page.

11.3.14.4 IGMP Snooping Querier VLAN Status Page



Non-Configurable Data

VLAN ID - Specifies the VLAN ID on which IGMP Snooping Querier is administratively enabled and VLAN exists in the VLAN database.

Operational State - Specifies the operational state of the IGMP Snooping Querier on a VLAN. It can be in any of the following states:

Querier - Snooping switch is the Querier in the VLAN. The Snooping switch will send out periodic queries with a time interval equal to the configured querier query interval. If the snooping switch sees a better querier in the VLAN, it moves to non-querier mode.

Non-Querier - Snooping switch is in Non-Querier mode in the VLAN. If the querier expiry interval timer is expires, the snooping switch will move into querier mode.

Disabled - Snooping Querier is not operational on the VLAN. The Snooping Querier moves to disabled mode when IGMP Snooping is not operational on the VLAN or when the querier address is not configured or the network management address is also not configured.

Operational Version - Displays the operational IGMP protocol version of the querier.

Last Querier Address - Displays the IP address of the last querier from which a query was snooped on the VLAN.

Last Querier Version - Displays the IGMP protocol version of the last querier from which a query was snooped on the VLAN.

Operational Max Response Time - Displays maximum response time to be used in the queries that are sent by the Snooping Querier.

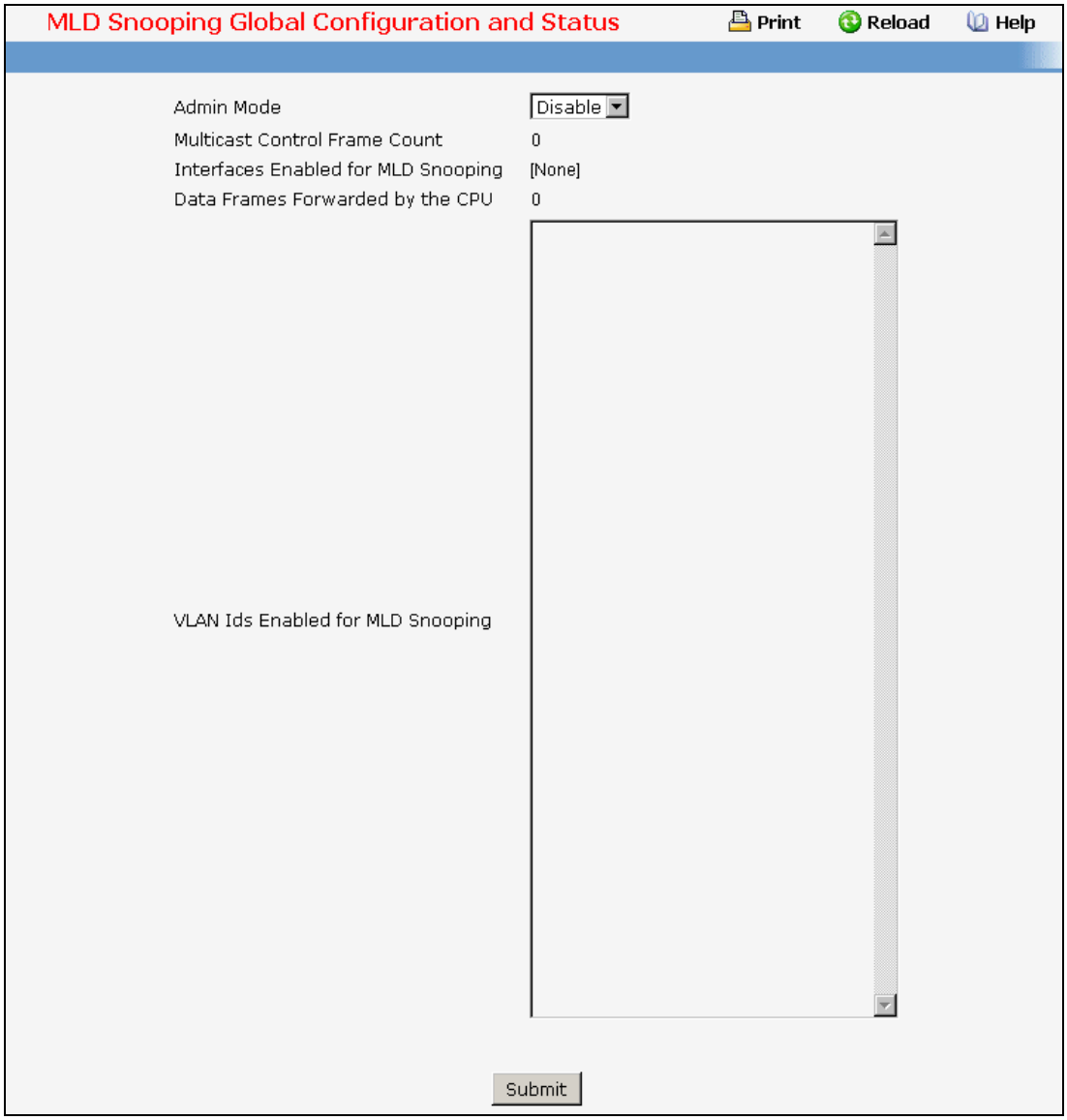
Command Buttons

Refresh - Reload the information on the page.

11.3.15 Managing MLD Snooping

11.3.15.1 Configuring MLD Snooping Global Configuration and Status Page

Use this menu to configure the parameters for MLD 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.



Selection Criteria

Admin Mode - Select the administrative mode for MLD 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 MLD Snooping - A list of all the interfaces currently enabled for MLD Snooping.

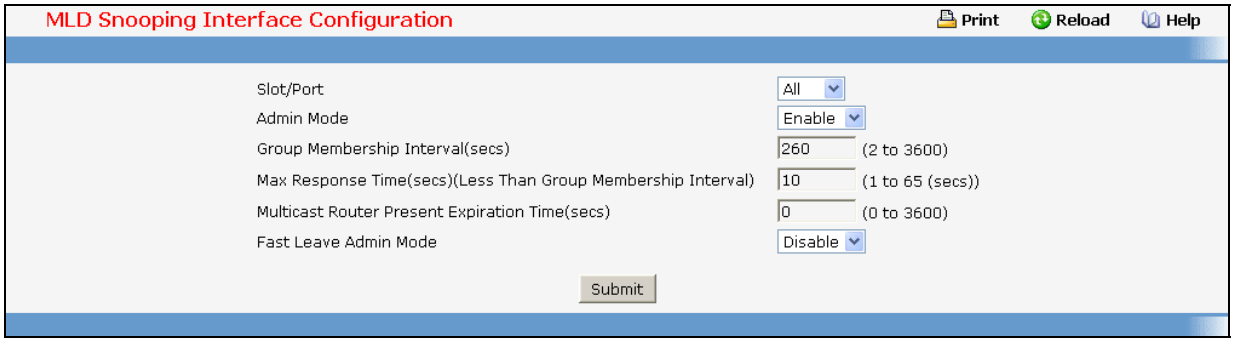
Data Frames Forwarded by the CPU - The number of data frames forwarded by the CPU.

VLAN Ids Enabled For MLD Snooping - Displays VLAN Ids enabled for MLD 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.

11.3.15.2 Configuring MLD Snooping Interface Configuration Page



Selection Criteria

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 MLD Snooping for the switch from the pulldown menu. The default is disable.

Fast Leave Admin mode - Select the Fast Leave mode for the a particular interface from the pulldown menu. The default is disable.

Configurable Data

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. The valid range is from (2 to 3600) seconds. The configured value must be greater than Max Response Time. The default is 260 seconds.

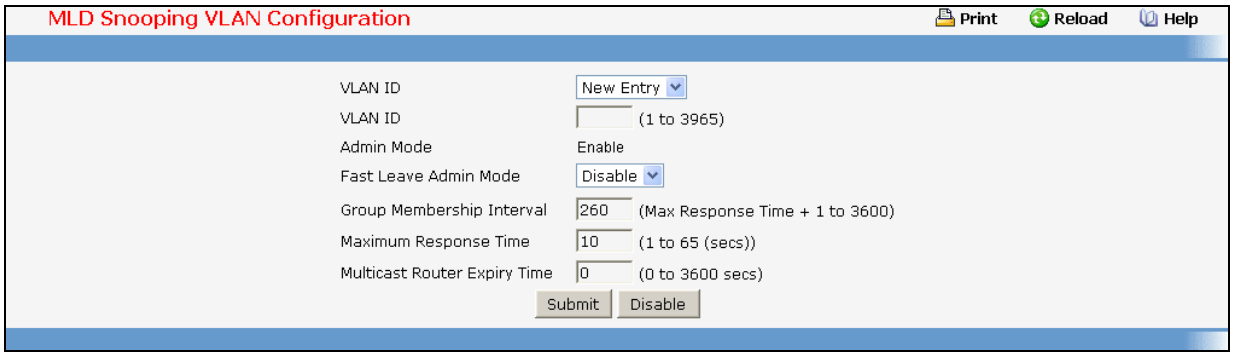
Max Response Time - Specify the amount of time you want the switch to wait after sending a query on an interface because it did not receive a report for a particular group on that interface. Enter a value greater or equal to 1 and less than the Group Membership Interval in seconds. The default is 10 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.

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.

11.3.15.3 Configuring MLD Snooping VLAN Configuration Page



Selection Criteria

VLAN ID - Specifies list of VLAN IDs for which MLD Snooping is enabled.

Fast Leave Admin Mode - Enable or disable the MLD Snooping Fast Leave Mode for the specified VLAN ID.

Configurable Data

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.

Group Membership Interval - Sets the value for group membership interval of MLD 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 MLD Snooping for the specified VLAN ID. Valid range is 1 to (Group Membership Interval - 1).Its value should be less than group membership interval value.

Multicast Router Expiry Time - Sets the value for multicast router expiry time of MLD Snooping for the specified VLAN ID. Valid range is 0 to 3600.

None-Configurable Data

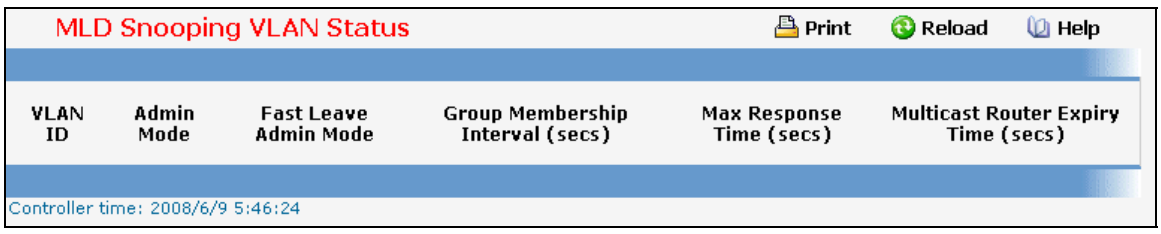
Admin Mode - Enable MLD Snooping for the specified VLAN ID.

Command Buttons

Submit - Update the switch with the values you entered.

Delete - Update the switch with the default values.

11.3.15.4 Configuring MLD Snooping VLAN Status Page



Non-Configurable Data

VLAN ID - All Vlan Ids for which the MLD Snooping mode is Enabled.

Admin Mode - MLD Snooping Mode for Vlan ID.

Fast Leave Admin Mode - Fast Leave Mode for Vlan ID.

Group Membership Interval - Group Membership Interval of MLD Snooping for the specified VLAN ID. Valid range is 2 to 3600.

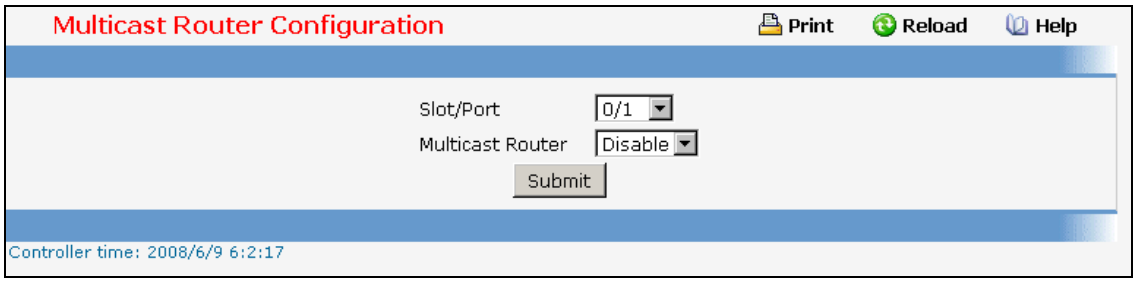
Maximum Response Time - Maximum Response Time of MLD Snooping for the specified VLAN ID. Valid range is 1 to 65. Its value should be greater than group membership interval value.

Multicast Router Expiry Time - Multicast Router Expiry Time of MLD Snooping for the specified VLAN ID. Valid range is 0 to 3600.

Command Buttons

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

11.3.15.5 Configuring Multicast Router Status Page



Selection Criteria

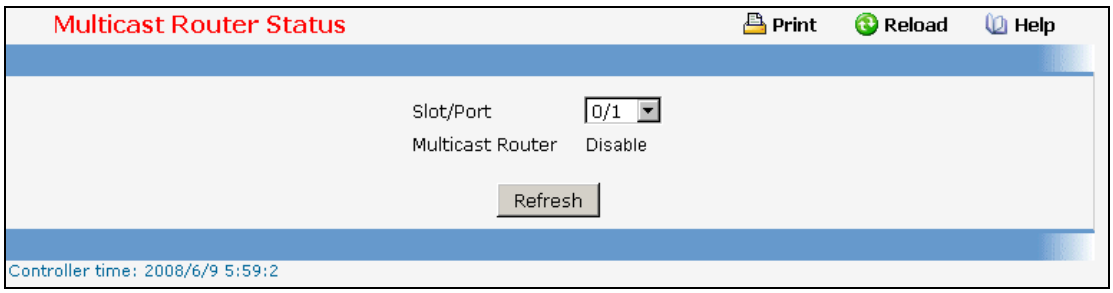
Slot/Port - The select box lists all Slot/Ports. Select the interface for which you want Multicast Router to be enabled.

Multicast Router - Enable or disable Multicast Router on the selected Slot/Port.

Command Buttons

Submit - Update the switch with the values you entered.

11.3.15.6 Configuring Multicast Router Status Page



Selection Criteria

Slot/Port - The single select box lists all physical and LAG interfaces. Select the interface for which you want to display the status.

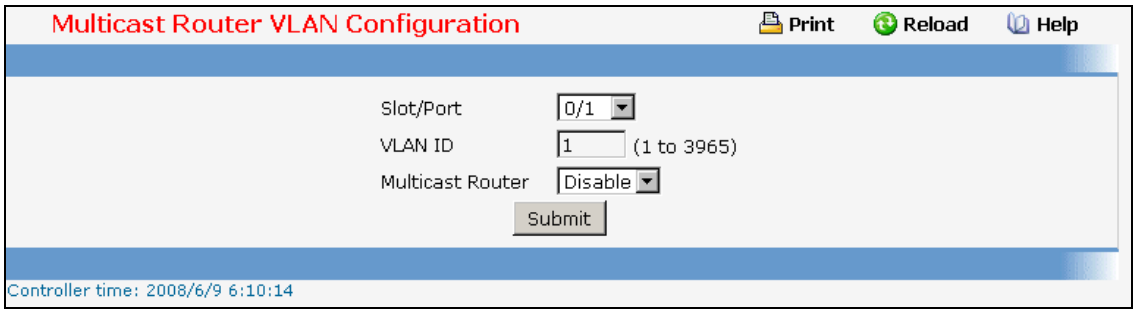
Non-Configurable Data

Multicast Router - Specifies for the selected interface whether multicast router is enable or disabled.

Command Buttons

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

11.3.15.7 Configuring Multicast VLAN Configuration Page



Selection Criteria

Slot/Port - The select box lists all Slot/Ports.Select the interface for which you want Multicast Router to be enabled

Multicast Router - For the Vlan ID, multicast router may be enabled or disabled using this.

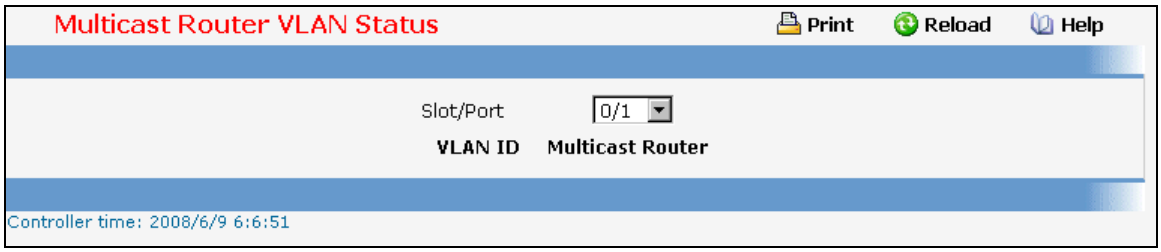
Configurable Data

VLAN ID - VLAN ID for which the Multicast Router Mode is to be Enabled or Disabled.

Command Buttons

Submit - Update the switch with the values you entered.

11.3.15.8 Configuring Multicast Router VLAN Status Page



Selection Criteria

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

Non-Configurable Data

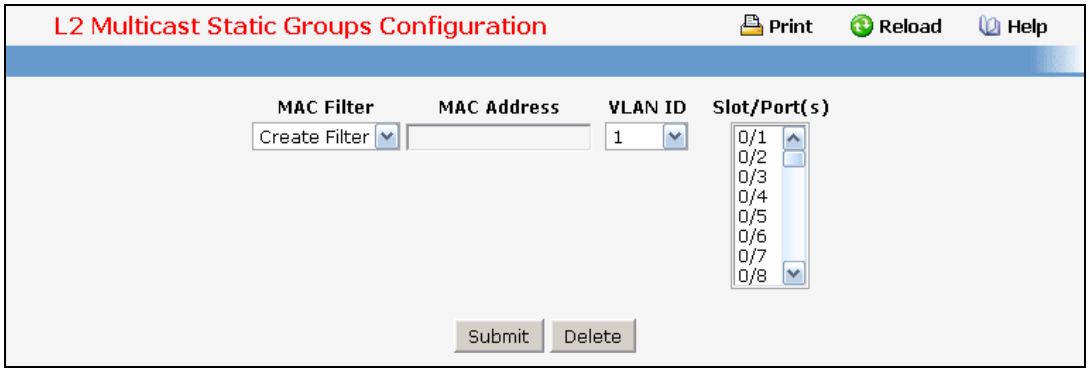
VLAN ID - All Vlan Ids for which the Multicast Router Mode is Enabled.

Multicast Router - Multicast Router Mode for Vlan ID.

Command Buttons

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

11.3.15.9 Configuring L2 Static Multicast Group Configuration Page



Selection Criteria

MAC Filter - This is the list of MAC address and VLAN ID pairings for all configured L2 Mcast Groups. To change the port mask(s) for an existing L2Mcast Group, select the entry you want to change. To add a new L2Mcast Group, select "Create Filter" from the top of the list.

VLAN ID - The VLAN ID used with the MAC address to fully identify packets you want L2Mcast Group. You can only change this field when you have selected the "Create Filter" option.

Configurable Data

MAC Address - The MAC address of the L2Mcast Group in the format 01:00:5E:xx:xx:xx. You can only change this field when you have selected the "Create Filter" option.

You cannot define L2Mcast Group for these MAC addresses:

00:00:00:00:00:00

33:33:00:00:00:01 to 33:33:00:00:00:FF

FF:FF:FF:FF:FF:FF

Solt/Port(s) - List the ports you want included into L2Mcast Group.

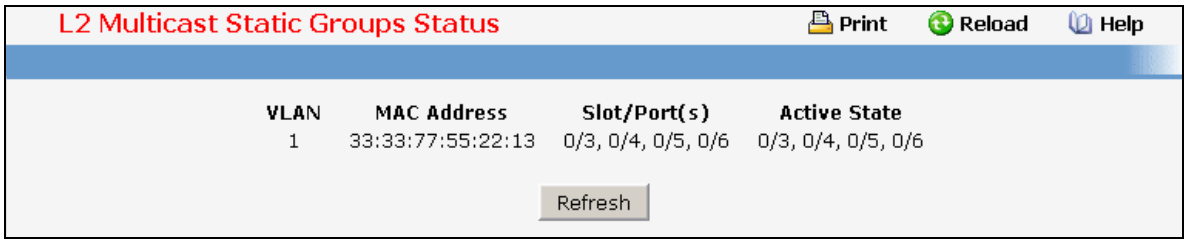
Command Buttons

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

Delete - Remove the currently selected L2Mcast Group.

11.3.15.10 Viewing L2 Multicast Group Status Page

Use this panel to display information about entries in the L2Mcast Static/Dynamic Groups. These entries are used by the transparent bridging function to determine how to forward a received frame.



Non-Configurable Data

VLAN - L2Mcast Group's VLAN ID value.

MAC Address - A multicast MAC address for which the switch has forwarding information. The format is a six-byte MAC address. For example: 33:33:00:00:11:11.

Slot/Ports - the interface number belongs to this Multicast Group.

Active State - The active interface number belongs to this Multicast Group.

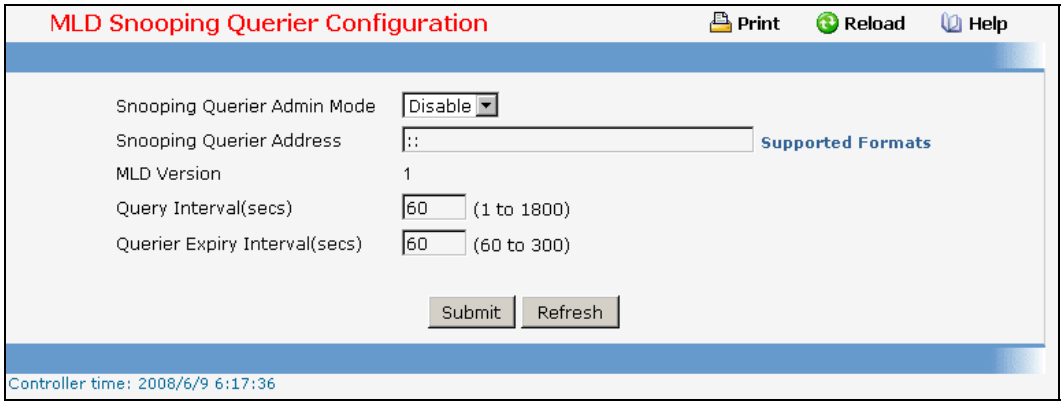
Command Buttons

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

11.3.16 Managing MLD Snooping Querier

11.3.16.1 Configuring MLD Snooping Querier Configuration Page

Use this menu to configure the parameters for MLD Snooping Querier, Note that only a user with Read/Write access privileges may change the data on this screen.



Selection Criteria

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

Configurable Data

Snooping Querier Address - Specify the Snooping Querier Address to be used as source address in periodic MLD queries. This address is used when no address is configured on the VLAN on which query is being sent.

MLD Version - Specify the MLD protocol version used in periodic MLD queries. MLD queries.

Query Interval - Specify the time interval in seconds between periodic queries sent by the snooping querier. The Query Interval must be a value in the range of 1 and 1800. The default value is 60.

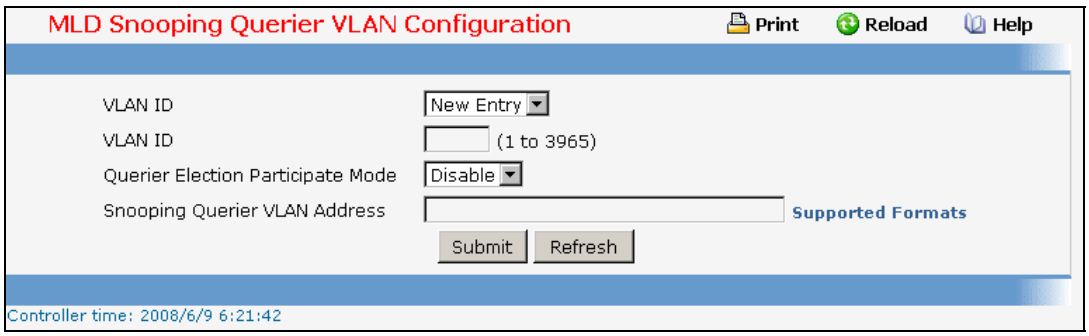
Querier Expiry Interval - Specify the time interval in seconds after which the last querier information is removed. The Querier Expiry Interval must be a value in the range of 60 and 300. The default value is 60.

Configurable Data

Submit - Update the switch with the configured values.

Refresh - Reload the information on the page.

11.3.16.2 Configuring MLD Snooping VLAN Configuration Page



Selection Criteria

VLAN ID - Selects the VLAN ID on which MLD Snooping Querier is enabled.

Querier Election Participate Mode - Enable or disable the Igmp Snooping Querier participate in election mode. When this mode is disabled, up on seeing other querier of same version in the vlan, the snooping querier move to non querier state. Only when this mode is enabled, the snooping querier will participate in querier election where in the least ip address will win the querier election and operates as the querier in that VLAN. The other querier moves to non-querier state.

Configurable Data

VLAN ID - Appears when "New Entry" is selected in VLAN ID selection list. Specifies VLAN ID for which MLD Snooping Querier is to be enabled. User can also set pre-configurable Snooping Querier parameters.

Snooping Querier VLAN Address - Specify the Snooping Querier Address to be used as source address in periodic MLD queries sent on the specified VLAN.

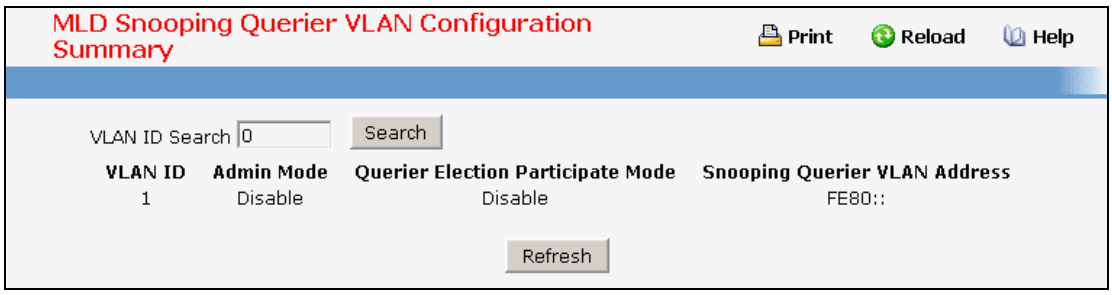
Command Buttons

Submit - Update the switch with the configured values.

Delete - To disable Snooping Querier on the selected VLAN. This button is not visible when a VLAN is not selected.

Refresh - Reload the information on the page.

11.3.16.3 Configuring MLD Snooping VLAN Configuration Summary Page



Configurable Data

VLAN ID Search - Enter VLAN ID, then click on the search button. If the record exists, that entry will be displayed. An exact match is required.

Non-Configurable Data

VLAN ID - Specifies the VLAN ID on which MLD Snooping Querier is administratively enabled.

Admin Mode - Display the administrative mode for MLD Snooping for the switch.

Querier Election Participate Mode - Displays the querier election participate mode on the VLAN. When this mode is disabled, up on seeing a query of the same version in the vlan, the snooping querier move to non querier state. Only when this mode is enabled, the snooping querier will participate in querier election where in the least ip address will win the querier election and operates as the querier in that VLAN. The other querier moves to non-querier state.

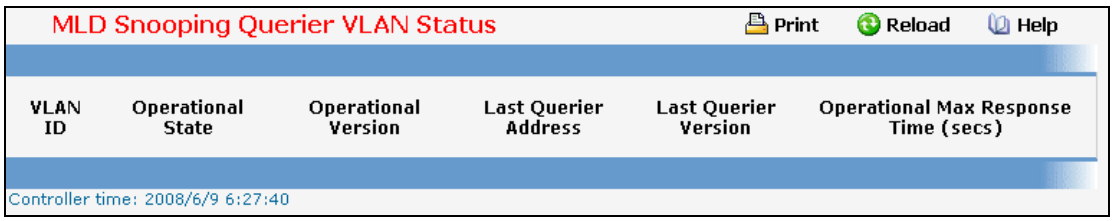
Snooping Querier VLAN Address - Displays the Snooping Querier Address to be used as source address in periodic MLD queries sent on the specified VLAN.

Command Buttons

Search - Search for the specified Vlan ID.

Refresh - Reload the information on the page.

11.3.16.4 Configuring MLD Snooping Querier VLAN Status Page



Non-Configurable Data

VLAN ID - Specifies the VLAN ID on which MLD Snooping Querier is administratively enabled and VLAN exists in the VLAN database.

Operational State - Specifies the operational state of the MLD Snooping Querier on a VLAN. It can be in any of the following states:

Querier - Snooping switch is the Querier in the VLAN. The Snooping switch will send out periodic queries with a time interval equal to the configured querier query interval. If the snooping switch sees a better querier in the VLAN, it moves to non-querier mode.

Non-Querier - Snooping switch is in Non-Querier mode in the VLAN. If the querier expiry interval timer is expires, the snooping switch will move into querier mode.

Disabled - Snooping Querier is not operational on the VLAN. The Snooping Querier moves to disabled mode when MLD Snooping is not operational on the VLAN or when the querier address is not configured or the network management address is also not configured.

Operational Version - Displays the operational MLD protocol version of the querier.

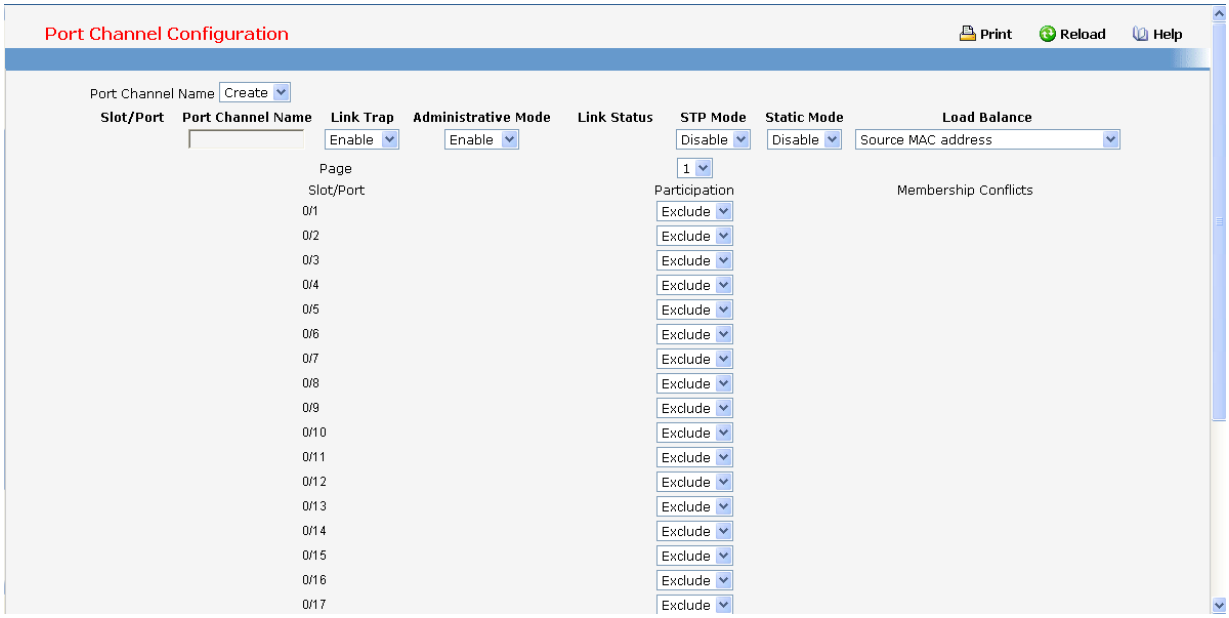
Last Querier Address - Displays the IP address of the last querier from which a query was snooped on the VLAN.

Last Querier Version - Displays the IGMP protocol version of the last querier from which a query was snooped on the VLAN.

Operational Max Response Time - Displays maximum response time to be used in the queries that are sent by the Snooping Querier.

11.3.17 Managing Port-Channel

11.3.17.1 Configuring Port-Channel Configuration Page



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.

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 enabled.

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.

Static Mode - Select static or dynamic from the pull down menu. The factory default is disabled.

Load Balance Mode - Select load balance mode from the pull down menu. The factory default is Source XOR Destination MAC address.

- Source MAC address - Sets the mode on the source MAC address.
- Destination MAC address - Sets the mode on the destination MAC address.

- Source and destination MAC address - Sets the mode on the source and destination MAC addresses.
- Source IP address - Sets the mode on the source IP address.
- Destination IP address - Sets the mode on the destination IP address.
- Source and destination IP address - Sets the mode on the source and destination IP addresses.

Participation - For each port specify whether it is to be included as a member of this Port Channel or not. The default is excluded. There can be a maximum of 8 ports assigned to a Port Channel.

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.

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.

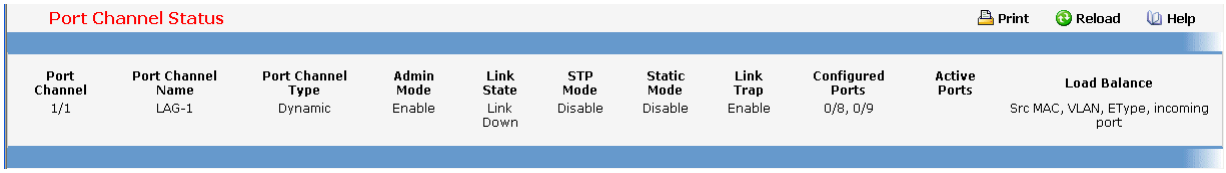
Membership Conflicts - Shows ports that are already members of other Port Channels. A port may only be a member of one Port Channel at a time. If the entry is blank, it is not currently a member of any Port Channel.

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 - Removes the currently selected configured Port Channel. All ports that were members of this Port Channel are removed from the Port Channel and included in the default VLAN. This field will not appear when a new Port Channel is being created. **Refresh** - Refresh the data on the screen with the present state of the data in the switch.

11.3.17.2 Viewing Port-Channel Information Page



Non-Configurable Data

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.

Static Mode – Indicates whether port channel is static or dynamic.

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.

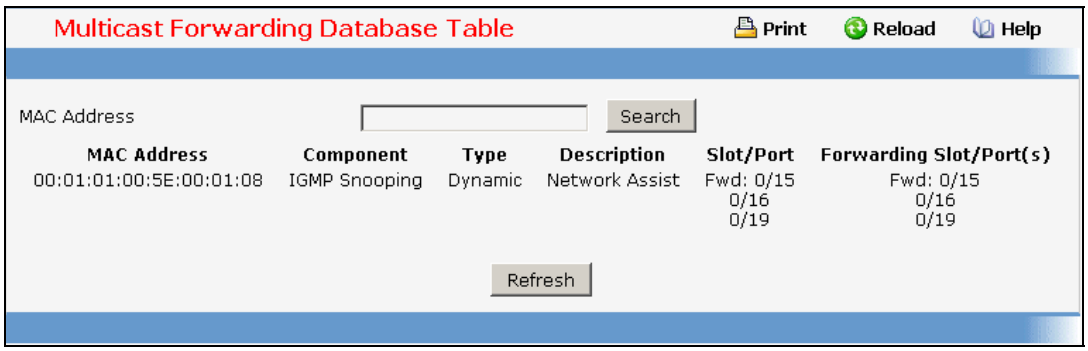
Load Balance – Indicates load-balnace mode of port channel. The possible values are:

- Source MAC address - Sets the mode on the source MAC address.
- Destination MAC address - Sets the mode on the destination MAC address.
- Source and destination MAC address - Sets the mode on the source and destination MAC addresses.
- Source IP address - Sets the mode on the source IP address.
- Destination IP address - Sets the mode on the destination IP address.
- Source and destination IP address - Sets the mode on the source and destination IP addresses.

11.3.18 Viewing Multicast Forwarding Database

11.3.18.1 Viewing All of Multicast Forwarding Database Tables Page

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.



Configurable Data

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.

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.

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. 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 Slot/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.

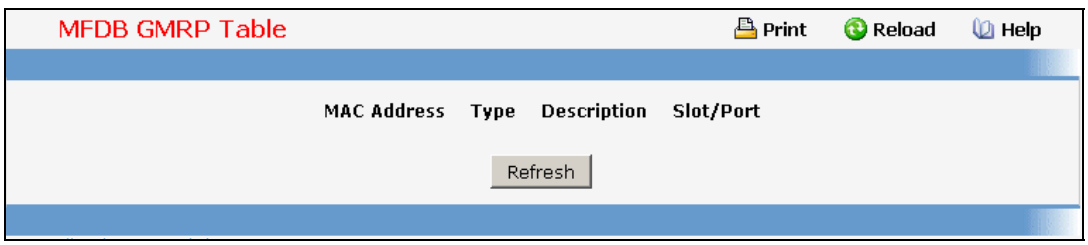
Command Buttons

Search - Search MFDB table entry by VLAN ID - MAC Address pair.

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

11.3.18.2 Viewing GMRP MFDB Table Page

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



Non-Configurable Data

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.

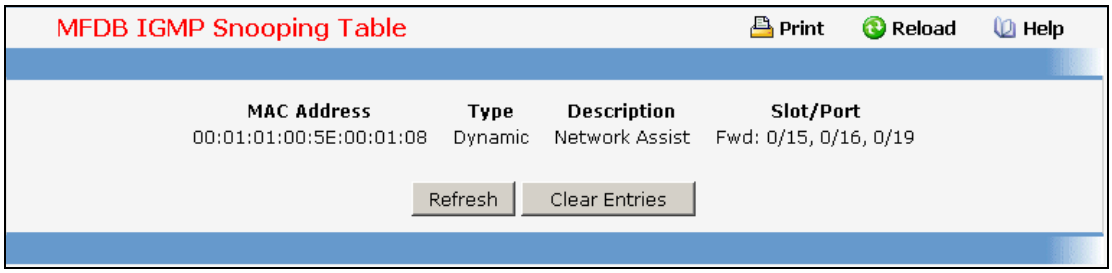
Description - The text description of this multicast table entry. Possible values are Management Configured, Network Configured, and Network Assisted.

Slot/Port(s) - The list of interfaces that are designated for forwarding (Fwd:) and filtering (Flt:).

Command Buttons

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

11.3.18.3 Viewing IGMP Snooping MFDB Table Page



Non-Configurable Data

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.

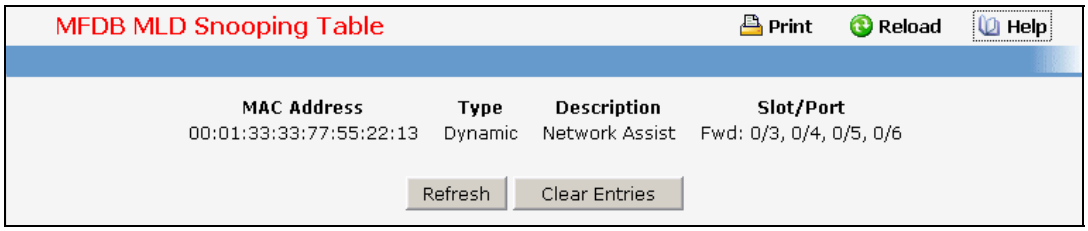
Slot/Port(s) - The list of interfaces that are designated for forwarding (Fwd:) and filtering (Flt:).

Command Buttons

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

Clear Entries - Clicking this button tells the IGMP Snooping component to delete all of its entries from the multicast forwarding database.

11.3.18.4 Viewing MLD Snooping MFDB Table Page



Non-Configurable Data

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.

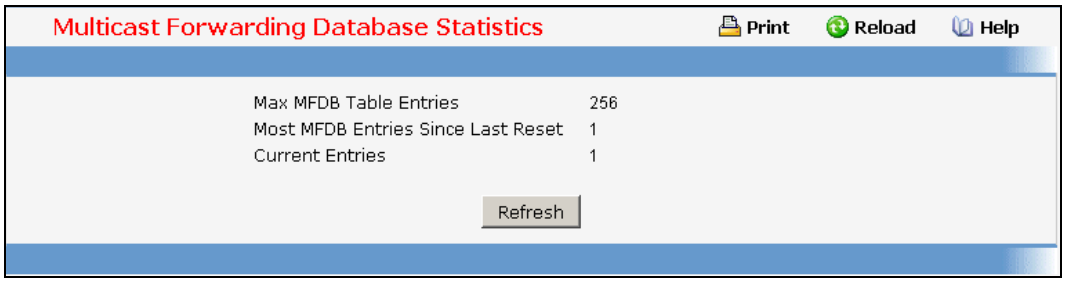
Slot/Port(s) - The list of interfaces that are designated for forwarding (Fwd:) and filtering (Flt:).

Command Buttons

Clear Entries - Clicking this button tells the MLD Snooping component to delete all of its entries from the multicast forwarding database.

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

11.3.18.5 Viewing Multicast Forwarding Database Statistics Page



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.

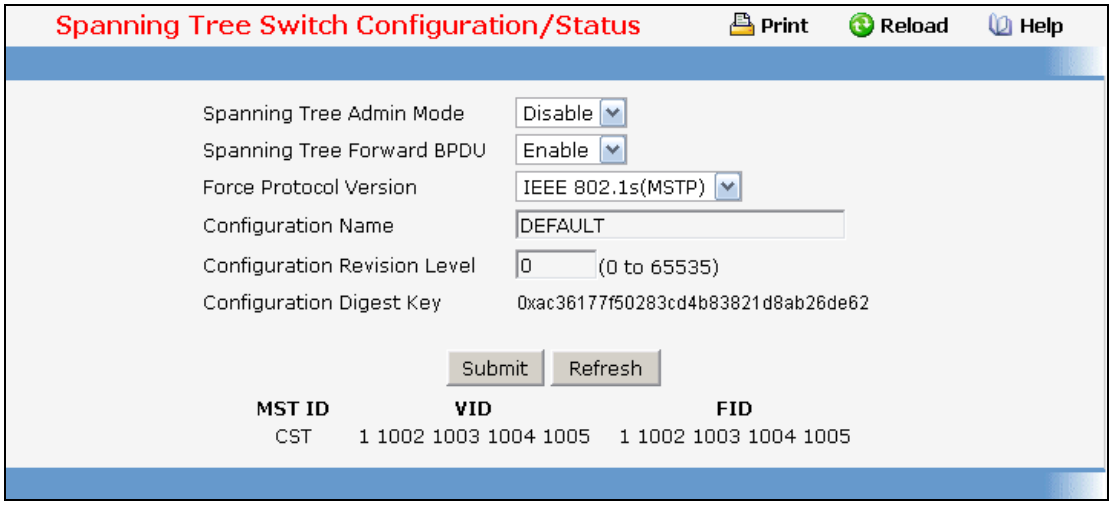
Current Entries - The current number of entries in the Multicast Forwarding Database table.

Command Buttons

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

11.3.19 Managing Spanning Tree

11.3.19.1 Configuring Switch Spanning Tree Configuration Page



Selection Criteria

Spanning Tree Mode - Specifies whether spanning tree operation is enabled on the switch. Value is enabled or disabled

Spanning Tree Forward BPDU - Specifies whether spanning tree for BPDU is enabled on the switch. Value is enabled or disabled.

Force Protocol Version - Specifies the Force Protocol Version parameter for the switch. The options are IEEE 802.1d, IEEE 802.1w, and IEEE 802.1s The default value is IEEE 802.1w.

Configurable Data

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.

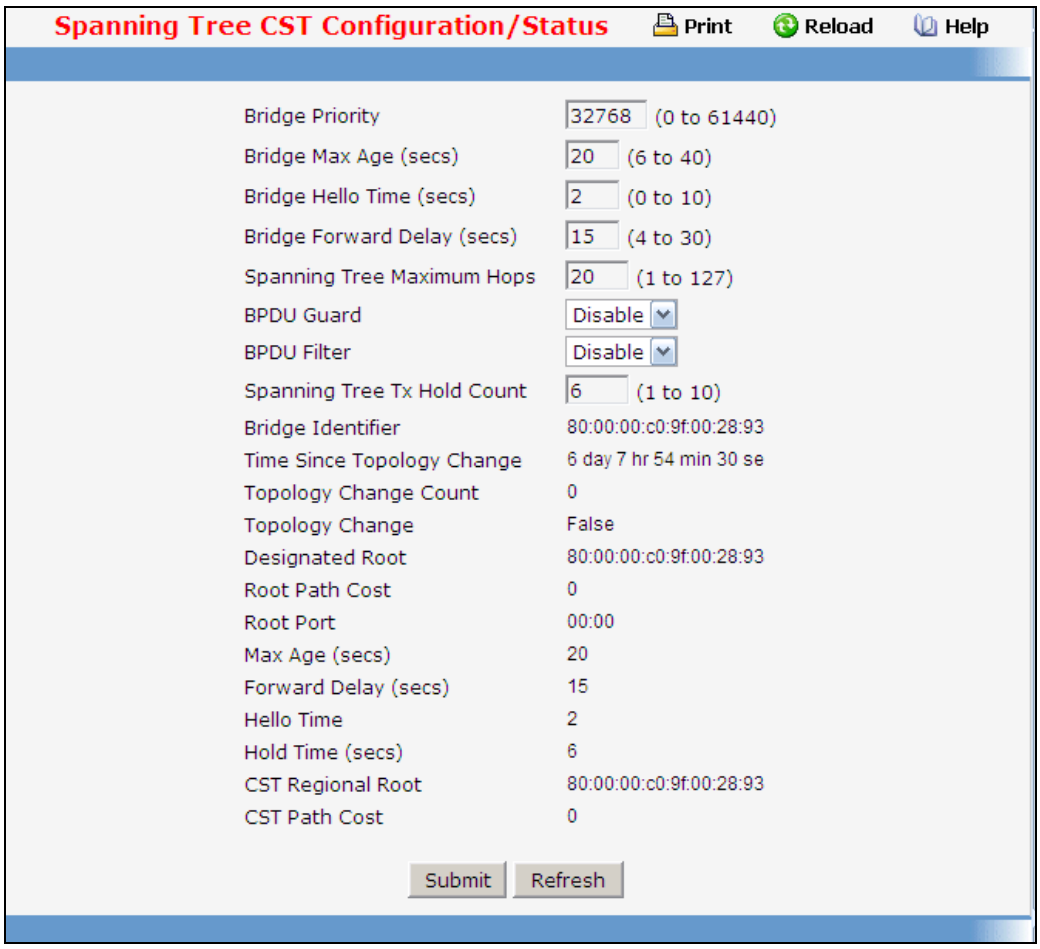
FID Table - Table consisting of the FIDs and the corresponding VLAN IDs associated with each of them.

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.

Refresh - Refreshes the screen with most recent data.

11.3.19.2 Configuring Spanning Tree CST Configuration Page



Selection Criteria

BPDU Guard - Specifies whether BPDU Guard is enabled for the Common and Internal Spanning tree (CST). Value is enabled or disabled

BPDU Filter - Specifies whether BPDU Filter is enabled for the Common and Internal Spanning tree (CST). Value is enabled or disabled

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 you set the priority 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.

Spanning Tree Maximum Hops- Configure the maximum number of hops for the Spanning tree.

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.

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 CST. It takes a value if 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.

Hello Time - Derived value of the Root Port Bridge Hello Time parameter.

Hold Time - Minimum time between transmission of Configuration BPDUs.

CST Regional Root - Priority and base MAC address of the CST Regional Root.

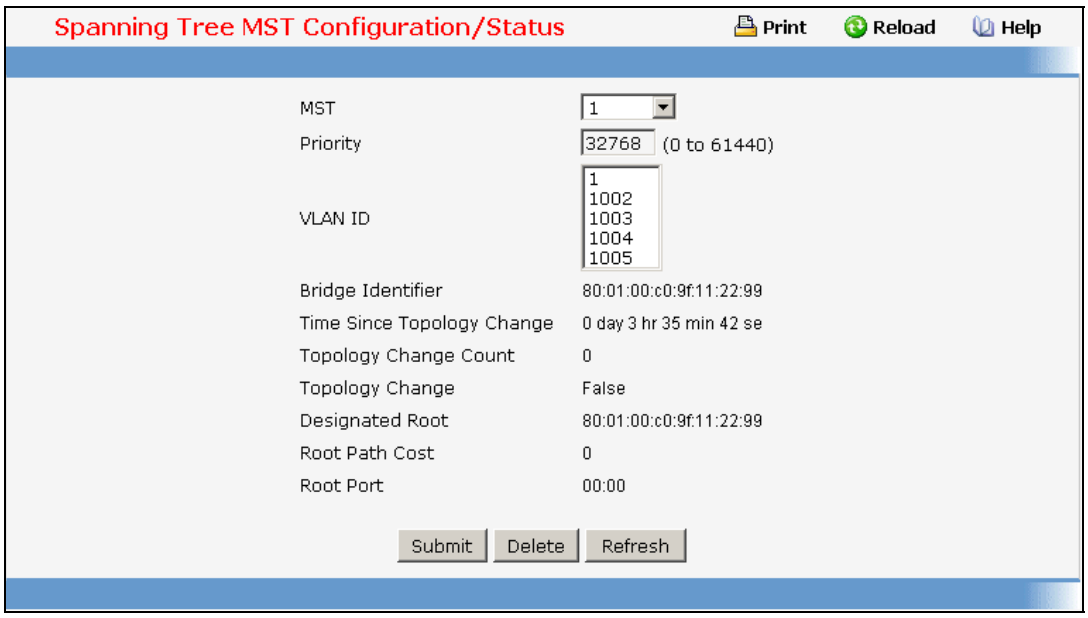
CST Path Cost - Path Cost to the CST tree Regional Root.

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.

Refresh - Refreshes the screen with most recent data.

11.3.19.3 Configuring Spanning Tree MST Configuration Page



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 4054.

Priority - The bridge priority for the MST instance selected. The bridge priority is set in multiples of 4096. For example if you attempt to set the priority to any value between 0 and 4095, it will be set to 0. If you attempt to set 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 the 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 if 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.

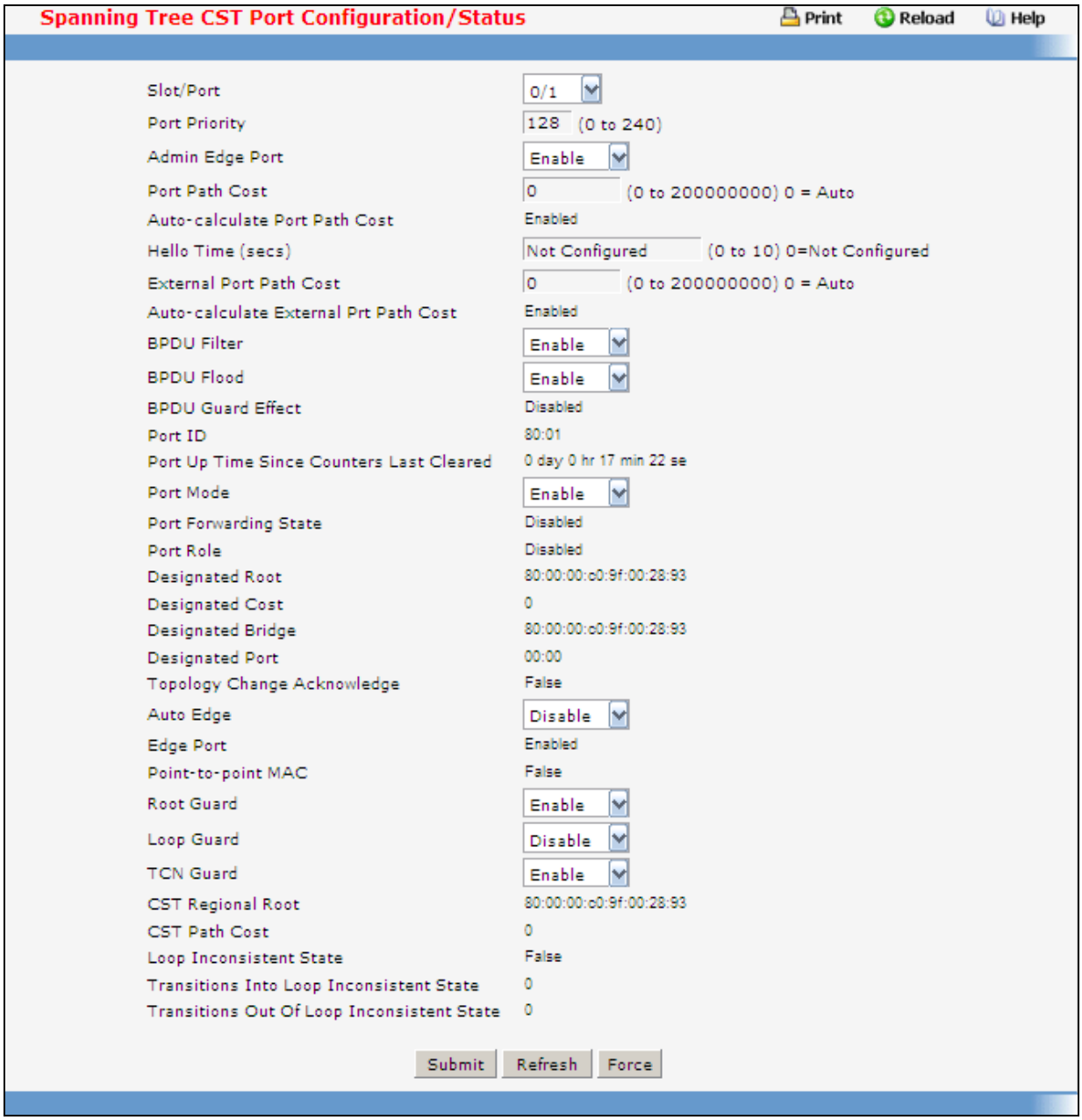
Command Buttons

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.

Delete - Deletes the selected MST instance. All VLANs associated with the instance are associated with the CST

Refresh - Refreshes the screen with most recent data.

11.3.19.4 Configuring each Port CST Configuration Page



Selection Criteria

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

Admin Edge Port - Specifies if the specified port is an Edge Port within the CIST. It takes a value of Enable or Disable, where the default value is Disable.

BPDU Guard - Specifies whether BPDU Guard is enabled for the Common and Internal Spanning tree (CST). Value is enabled or disabled

BPDU Filter - Specifies whether BPDU Filter is enabled for the Common and Internal Spanning tree (CST). Value is enabled or disabled

Port Mode - Spanning Tree Protocol Administrative Mode associated with the port or port channel. The possible values are Enable or Disable.

Auto Edge - Configuring the auto edge mode of a port allows the port to become an edge port if it does not see BPDUs for some duration. The possible values are Enable or Disable.

Root Guard - Configuring the root guard mode sets a port to discard any superior information received by the port and thus protect against root of the device from changing. The port gets put into discarding state and does not forward any packets.The possible values are Enable or Disable.

Loop Guard - Configuring the loop guard mode prevents a port from erroneously transitioning from blocking state to forwarding when the port stops receiving BPDUs. The port is marked as being in loop-inconsistent state. In this state, the port does not forward packets. The possible values are Enable or Disable.

TCN Guard - Configuring the TCN guard for a port restricts the port from propagating any topology change information received through that port.The possible values are Enable or Disable.

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 you attempt to set the priority to any value between 0 and 15, it will be set to 0. If you attempt to set 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 common and internal spanning tree. It takes a value in the range of 1 to 200000000.

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.

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.

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.

BPDU Guard Effect – Displays whether BPDU Guard Effect is enabled or disabled.

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.

Loop Inconsistent State - This parameter identifies whether the port is in loop inconsistent state.

Transitions Into Loop Inconsistent State - The number of times this interface has transitioned into loop inconsistent state.

Transitions Out Of Loop Inconsistent State - The number of times this interface has transitioned out of loop inconsistent state.

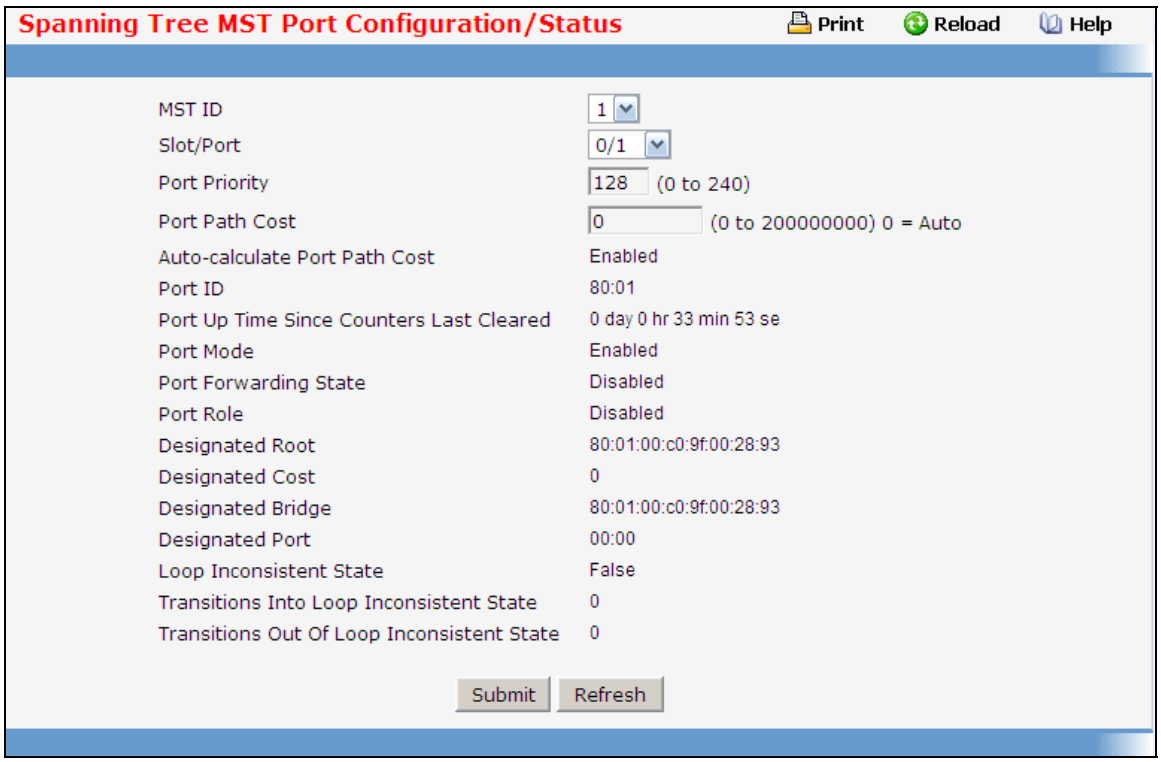
Command Buttons

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.

Refresh - Refreshes the screen with most recent data.

Force - Clicking this button will force the port to send out 802.1w or 802.1s BPDUs.

11.3.19.5 Configuring each Port MST Configuration Page



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 you set the priority 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.

Loop Inconsistent State - This parameter identifies whether the port is in loop inconsistent state.

Transitions Into Loop Inconsistent State - The number of times this interface has transitioned into loop inconsistent state.

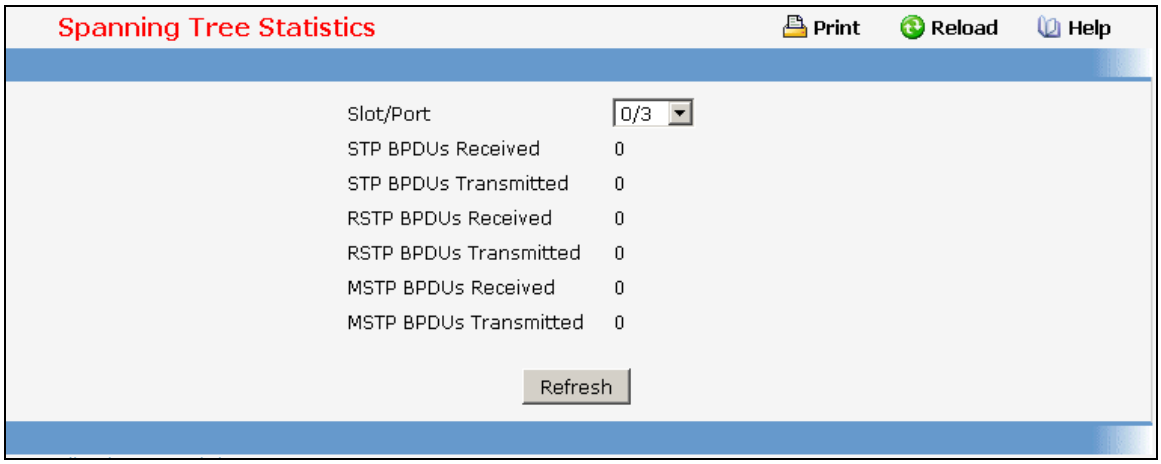
Transitions Out Of Loop Inconsistent State - The number of times this interface has transitioned out of loop inconsistent state.

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.

Refresh - Refreshes the screen with most recent data.

11.3.19.6 Viewing Spanning Tree Statistics Page



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.

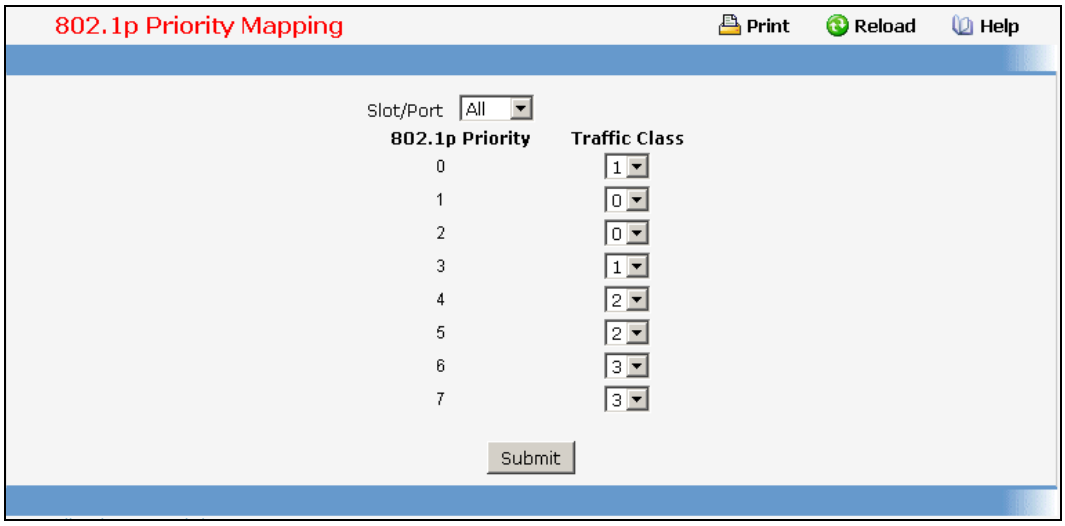
MSTP BPDUs Transmitted - Number of MSTP BPDUs transmitted from the selected port.

Command Buttons

Refresh - Refreshes the screen with most recent data.

11.3.20 Defining 802.1p priority

11.3.20.1 Defining 802.1p Priority Mapping Page



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 the same values.

Configurable Data

Traffic Class - Specify which internal traffic class to map the corresponding 802.1p priority.

Non-Configurable Data

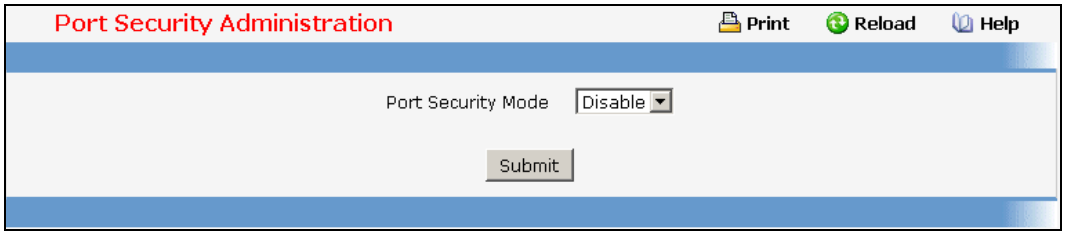
802.1p Priority - Displays the 802.1p priority to be mapped.

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.

11.3.21 Managing Port Security

11.3.21.1 Configuring Port Security Administration Mode Page



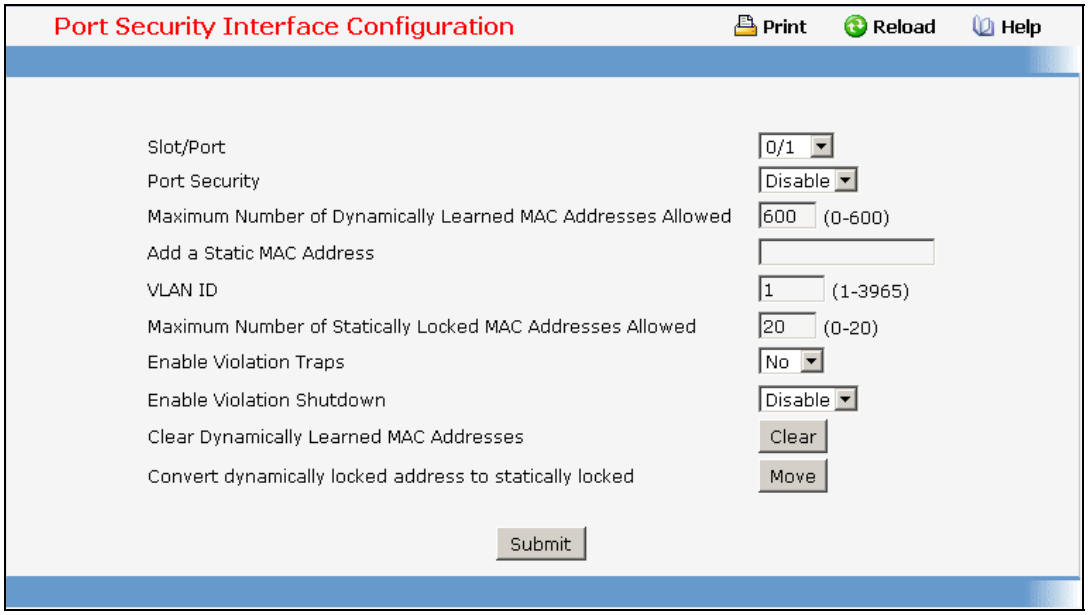
Selection Criteria

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.

11.3.21.2 Configuring Port Security Interface Page



Selection Criteria

Slot/Port - Selects the interface to be configured.

Port Security - Enables or disables the Port Security feature for 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.

Enable violation Shutdown- Enables or disables the Port Security Violation Shutdown mode for the selected interface.

Configurable Data

Maximum Number of Dynamically Learned 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 Number of Statically Locked MAC Addresses Allowed - Sets the maximum number of statically locked MAC addresses on the selected interface.

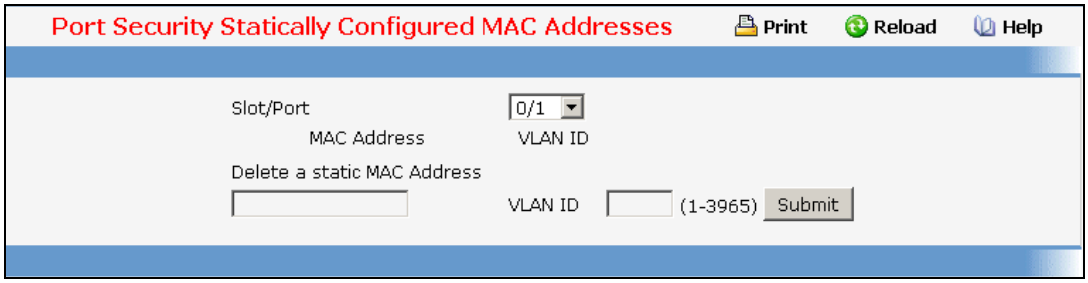
Command Buttons

Clear - Clears the Dynamic MAC addresses of the selected interface.

Move - Convert a dynamically locked MAC address to a statically locked address. The Dynamic MAC address entries are converted to Static MAC address entries in a numerically ascending order till the Static limit is reached.

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.

11.3.21.3 Deleting Port Security Statically Configured MAC Address Page



Selection Criteria

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

Configurable data

Delete a Static MAC Address - Accepts user input for the MAC address to be deleted.

VLAN ID - Accepts user input for the VLAN ID corresponding to the MAC address being deleted.

Non-configurable data

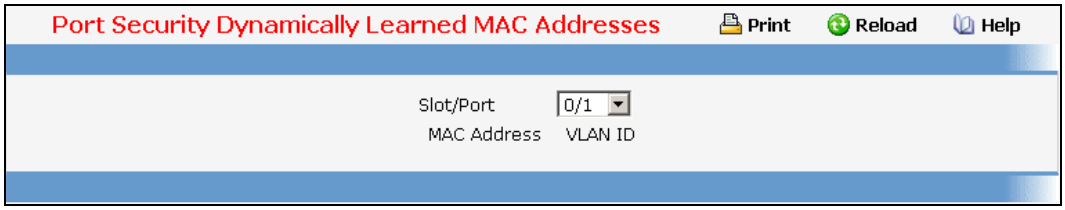
MAC Address - Displays the user specified statically locked MAC address.

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

11.3.21.4 Viewing Port Security Dynamically Learnt MAC Address Page



Selection Criteria

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

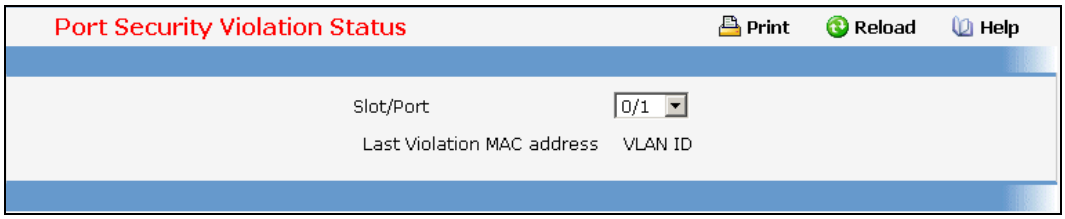
Non-configurable data

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.

11.3.21.5 Viewing Port Security Violation Status Page



Selection Criteria

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

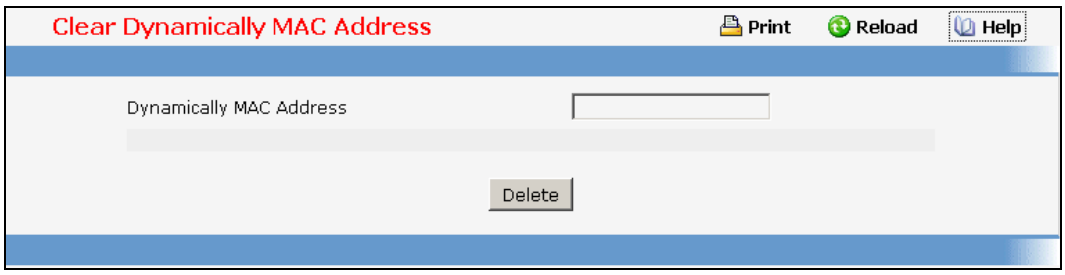
Non-configurable data

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.

11.3.21.6 Clearing Port Security Dynamically Learned MAC Addresses Page

Use this menu to clear a Dynamic MAC addresses of port security on switch.



Configurable Data

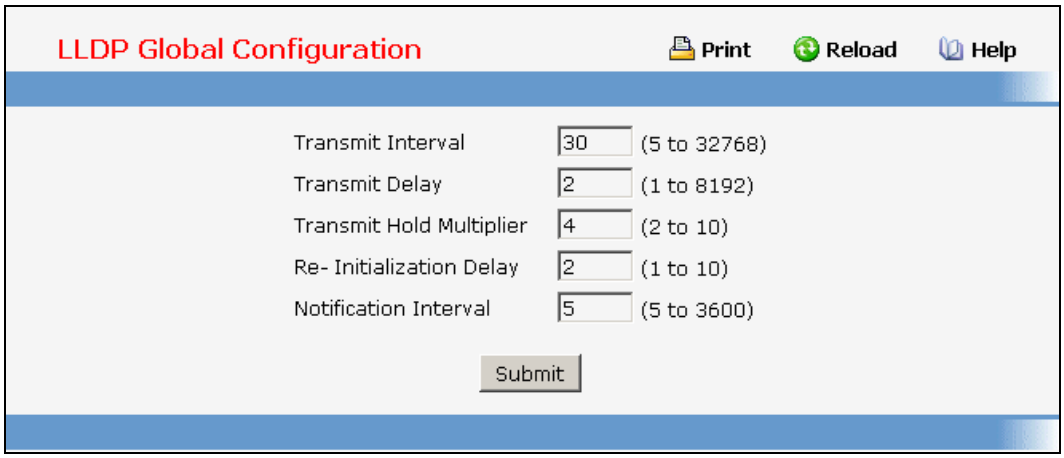
Dynamically MAC Address - Accepts user input for the MAC address to be deleted. The factory default is blank

Command Buttons

Delete - Send the updated screen to the switch perform the MAC clear

11.3.22 Managing LLDP

11.3.22.1 Configuring LLDP Global Configuration Page



Configurable Data

Transmit Interval - Specifies the interval in seconds to transmit LLDP frames. The range is from (1 to 32768) . Default value is 30 seconds.

Transmit Delay - Specifies the transmit delay in seconds. The range is from (1 to 8192) . Default value is 2 seconds.

Hold Multiplier - Specifies the multiplier on Transmit Interval to assign TTL. The range is from (2 to 10). Default value is 4.

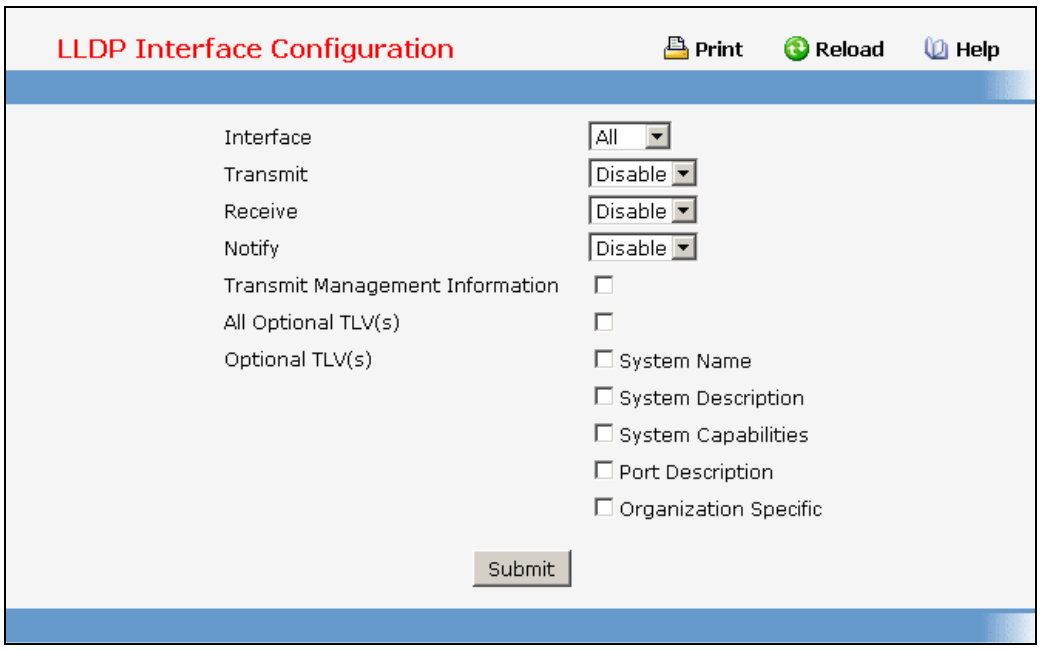
Re-Initialization Delay - Specifies the delay before re-initialization. The range is from (1 to 10) . Default value is 2 seconds.

Notification Interval - Specifies the interval in seconds for transmission of notifications. The range is from (5 to 3600) . Default value is 5 seconds.

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.

11.3.22.2 Configuring LLDP Interface Configuration Page



Selection Criteria

Interface - Specifies the list of ports on which LLDP - 802.1AB can be configured.

Transmit - Specifies the LLDP - 802.1AB transmit mode for the selected interface.

Receive - Specifies the LLDP - 802.1AB receive mode for the selected interface.

Notify - Specifies the LLDP - 802.1AB notification mode for the selected interface.

Configurable Data

Transmit Management Information - Specifies whether management address is transmitted in LLDP frames for the selected interface.

Optional TLV(s)

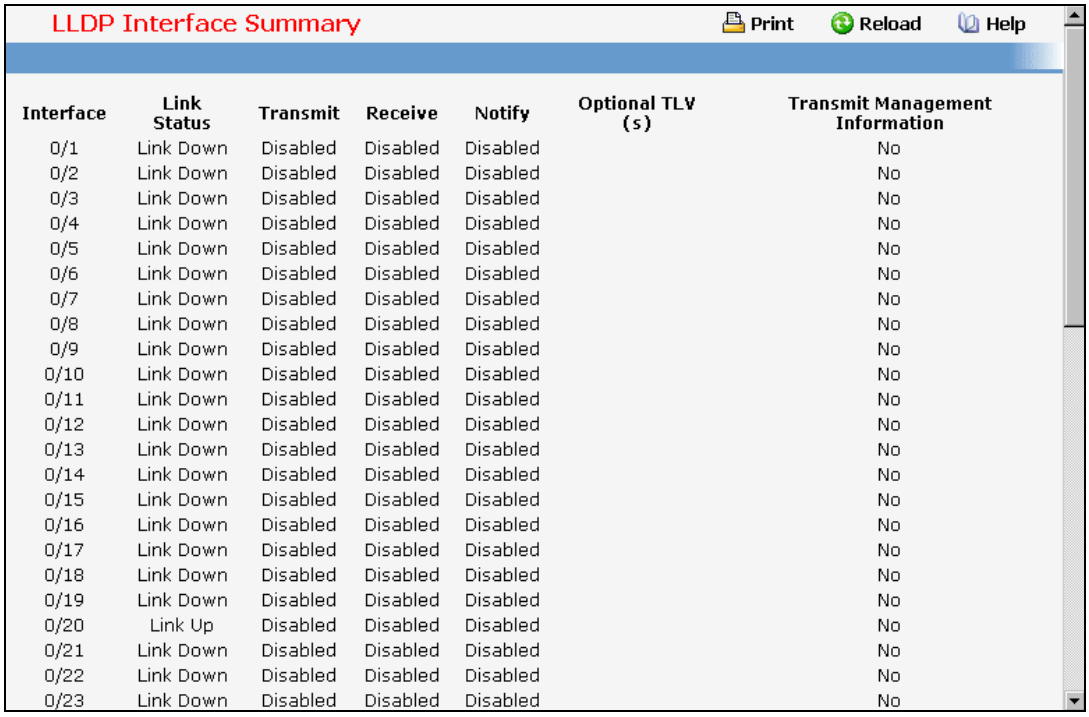
- **System Name** - To include system name TLV in LLDP frames.

- **System Description** - To include system description TLV in LLDP frames.
- **System Capabilities** - To include system capability TLV in LLDP frames.
- **Port Description** - To include port description TLV in LLDP frames.
- **Organization Specific** - To include organization specific TLV in LLDP frames.

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.

11.3.22.3 Viewing LLDP Interface Summary Page



Interface	Link Status	Transmit	Receive	Notify	Optional TLV (s)	Transmit Management Information
0/1	Link Down	Disabled	Disabled	Disabled		No
0/2	Link Down	Disabled	Disabled	Disabled		No
0/3	Link Down	Disabled	Disabled	Disabled		No
0/4	Link Down	Disabled	Disabled	Disabled		No
0/5	Link Down	Disabled	Disabled	Disabled		No
0/6	Link Down	Disabled	Disabled	Disabled		No
0/7	Link Down	Disabled	Disabled	Disabled		No
0/8	Link Down	Disabled	Disabled	Disabled		No
0/9	Link Down	Disabled	Disabled	Disabled		No
0/10	Link Down	Disabled	Disabled	Disabled		No
0/11	Link Down	Disabled	Disabled	Disabled		No
0/12	Link Down	Disabled	Disabled	Disabled		No
0/13	Link Down	Disabled	Disabled	Disabled		No
0/14	Link Down	Disabled	Disabled	Disabled		No
0/15	Link Down	Disabled	Disabled	Disabled		No
0/16	Link Down	Disabled	Disabled	Disabled		No
0/17	Link Down	Disabled	Disabled	Disabled		No
0/18	Link Down	Disabled	Disabled	Disabled		No
0/19	Link Down	Disabled	Disabled	Disabled		No
0/20	Link Up	Disabled	Disabled	Disabled		No
0/21	Link Down	Disabled	Disabled	Disabled		No
0/22	Link Down	Disabled	Disabled	Disabled		No
0/23	Link Down	Disabled	Disabled	Disabled		No

Non-Configurable Data

Interface - Specifies all the ports on which LLDP - 802.1AB can be configured.

Link Status - Specifies the Link Status of the ports whether it is Up/Down.

Transmit - Specifies the LLDP - 802.1AB transmit mode of the interface.

Receive - Specifies the LLDP - 802.1AB receive mode of the interface.

Notify - Specifies the LLDP - 802.1AB notification mode of the interface.

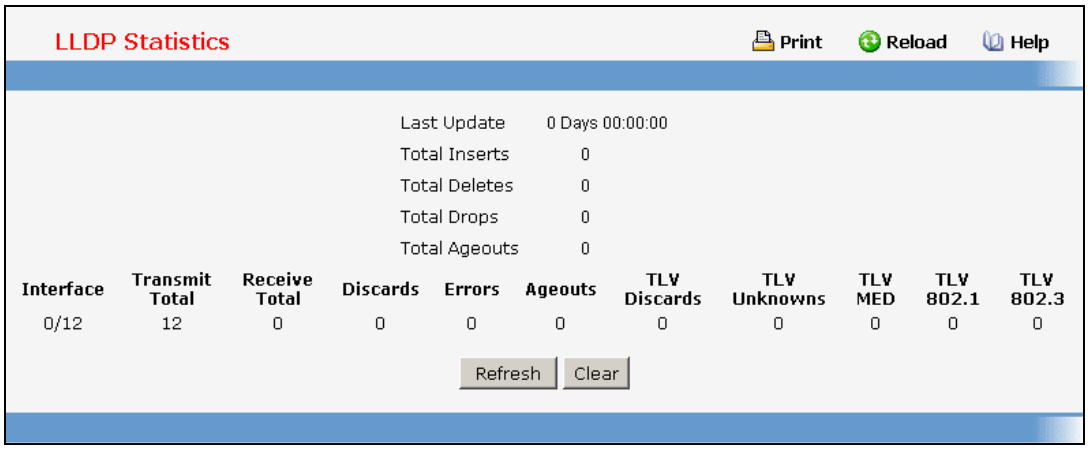
Optional TLV(s) - Specifies the LLDP - 802.1AB optional TLV(s) that are included.

Transmit Management Information - Specifies whether management address is transmitted in LLDP frames.

Command Buttons

Refresh - Updates the information on the page.

11.3.22.4 Viewing LLDP Statistics Page



Non-Configurable Data

Last Update - Specifies the time when an entry was created, modified or deleted in the tables associated with the remote system.

Total Inserts - Specifies the number of times the complete set of information advertised by a particular MAC Service Access Point (MSAP) has been inserted into tables associated with the remote systems.

Total Deletes - Specifies the number of times the complete set of information advertised by a particular MAC Service Access Point (MSAP) has been deleted from tables associated with the remote systems.

Total Drops - Specifies the number of times the complete set of information advertised by a particular MAC Service Access Point (MSAP) could not be entered into tables associated with the remote systems because of insufficient resources.

Total Age outs - Specifies the number of times the complete set of information advertised by a particular MAC Service Access Point (MSAP) has been deleted from tables associated with the remote systems because the information timeliness interval has expired.

Interface - Specifies the slot/port for the interfaces.

Transmit Total - Specifies the number of LLDP frames transmitted by the LLDP agent on the corresponding port.

Receive Total - Specifies the number of valid LLDP frames received by this LLDP agent on the corresponding port, while the LLDP agent is enabled.

Discards - Specifies the number of LLDP TLVs discarded for any reason by the LLDP agent on the corresponding port.

Errors - Specifies the number of invalid LLDP frames received by the LLDP agent on the corresponding port, while the LLDP agent is enabled.

Age outs - Specifies the number of age-outs that occurred on a given port. An age-out is the number of times the complete set of information advertised by a particular MAC Service Access Point (MSAP) has been deleted from tables associated with the remote entries because information timeliness interval had expired.

TLV Discards - Specifies the number of LLDP TLVs discarded for any reason by the LLDP agent on the corresponding port.

TLV Unknowns - Specifies the number of LLDP TLVs received on the local ports which were not recognized by the LLDP agent on the corresponding port.

TLV MED - Specifies the total number of LLDP-MED TLVs received on the local ports.

TLV 802.1 - Specifies the total number of LLDP TLVs received on the local ports which are of type 802.1.

TLV 802.3 - Specifies the total number of LLDP TLVs received on the local ports which are of type 802.3.

Command Buttons

Refresh - Updates the information on the page.

Clear - Clears LLDP Statistics of all the interfaces.

11.3.22.5 Viewing LLDP Local Device Information Page

Selection Criteria

Interface - Specifies the list of all the ports on which LLDP - 802.1AB frames can be transmitted.

Non-Configurable Data

Chassis ID Subtype - Specifies the string that describes the source of the chassis identifier.

Chassis ID - Specifies the string value used to identify the chassis component associated with the local system.

Port ID Subtype - Specifies the string describes the source of the port identifier.

Port ID - Specifies the string that describes the source of the port identifier.

System Name - Specifies the system name of the local system.

System Description - Specifies the description of the selected port associated with the local system.

Port Description - Specifies the description of the selected port associated with the local system.

System Capabilities Supported - Specifies the system capabilities of the local system.

System Capabilities Enabled - Specifies the system capabilities of the local system which are supported and enabled.

Management Address - Specifies the advertised management address of the local system.

Management Address Type - Specifies the type of the management address.

MAC/PHY Configuration/Status

- **Auto-Negotiation** - Specifies whether the auto-negotiation is supported and whether the auto-negotiation is enabled.
- **PMD Auto-Negoration Advertised Capabilities** - Specifies the auto-negotiation and speed capabilities of the PMD.
- **Operational MAU Type** - Specifies the current duplex and speed settings of the sending system.

Power Via MDI

- **MDI Power Support** - Specifies the MDI power support capabilities of the sending IEEE 802.3 LAN station.
- **PSE Power Pair** - Specifies which pair is powered.
- **Power Class** - Specifies the required power level required.

Link Aggregation Status - Specifies the capability and current aggregation status of the link.

Link Aggregation Port Id - Specifies the aggregated port identifier.

Maximum Frame Size - Specifies the maximum supported IEEE 802.3 frame size.

Port VLAN Identity - Specifies the VLAN ID of the port.

Protocol VLAN - Specifies the Protocol VLAN ID and status.

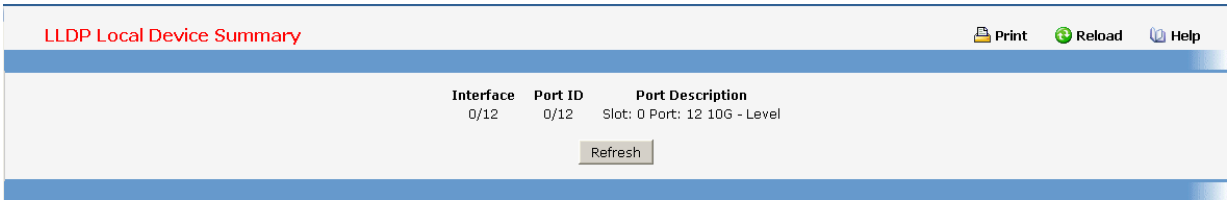
VLAN Name - Specifies the VLAN name.

Protocol Identity - Specifies the particular protocols that are accessible through the port.

Command Buttons

Refresh - Updates the information on the page.

11.3.22.6 Viewing LLDP Local Device Summary Page



Non-Configurable Data

Interface - Specifies the ports on which LLDP - 802.1AB frames can be transmitted.

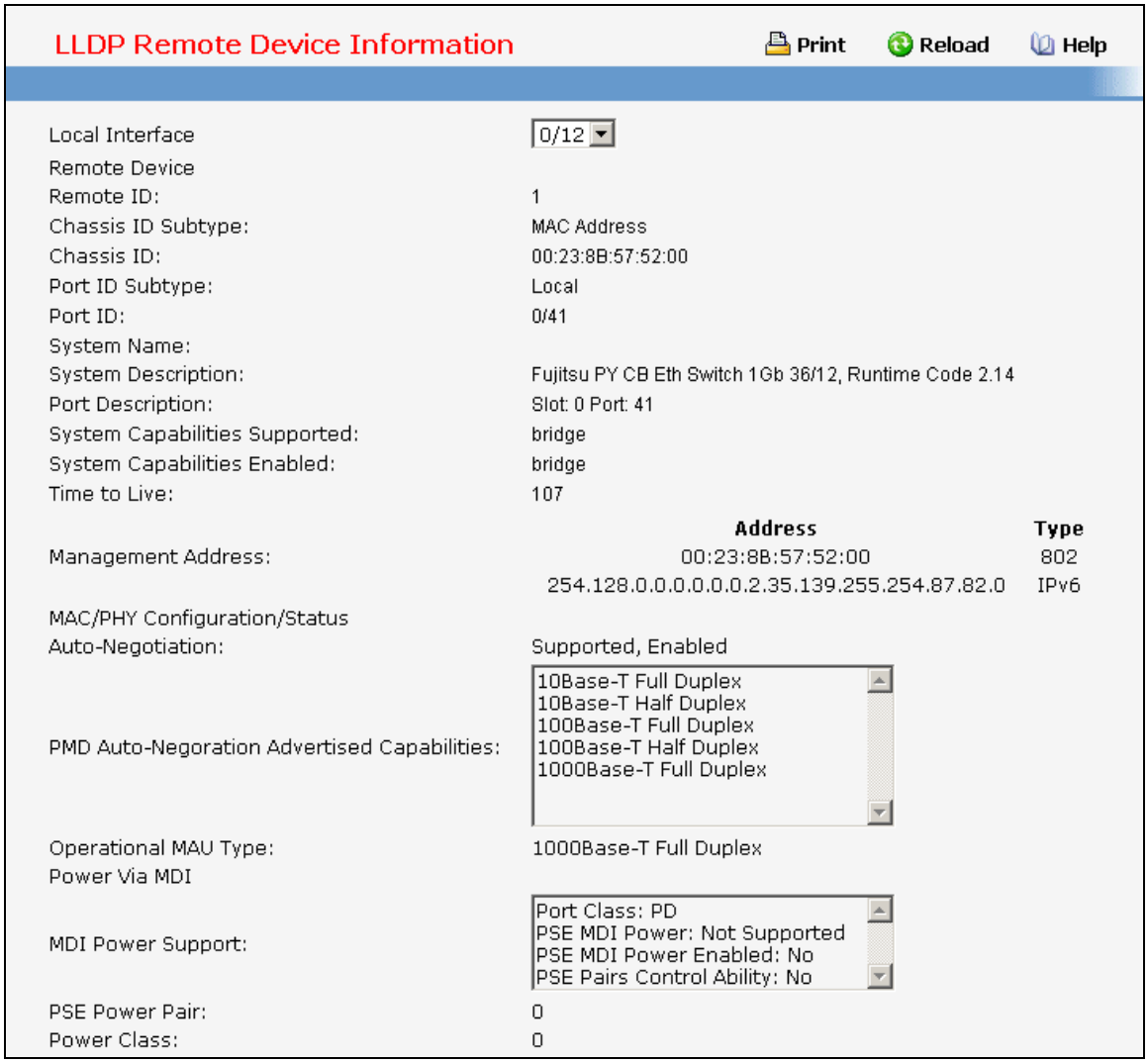
Port ID - Specifies the string describes the source of the port identifier.

Port Description - Specifies the description of the port associated with the local system.

Command Buttons

Refresh - Updates the information on the page.

11.3.22.7 Viewing LLDP Remote Device Information Page



Selection Criteria

Local Interface - Specifies all the local ports which can receive LLDP frames.

Non-Configurable Data

Remote ID - Specifies the remote client identifier assigned to the remote system.

Chassis ID Subtype - Specifies the source of the chassis identifier.

Chassis ID - Specifies the chassis component associated with the remote system.

Port ID Subtype - Specifies the source of port identifier.

Port ID - Specifies the port component associated with the remote system.

System Name - Specifies the system name of the remote system.

System Description - Specifies the description of the given port associated with the remote system.

Port Description - Specifies the description of the given port associated with the remote system.

System Capabilities Supported - Specifies the system capabilities of the remote system.

System Capabilities Enabled - Specifies the system capabilities of the remote system which are supported and enabled.

Time to Live - Specifies the Time To Live value in seconds of the received remote entry.

Management Address

- **Management Address** - Specifies the advertised management address of the remote system.
- **Type** - Specifies the type of the management address.

MAC/PHY Configuration/Status

- **Auto-Negotiation** - Specifies whether the auto-negotiation is supported and whether the auto-negotiation is enabled.
- **PMD Auto-Negoration Advertised Capabilities** - Specifies the auto-negotiation and speed capabilities of the PMD.
- **Operational MAU Type** - Specifies the current duplex and speed settings of the sending system.

Power Via MDI

- **MDI Power Support** - Specifies the MDI power support capabilities of the sending IEEE 802.3 LAN station.
- **PSE Power Pair** - Specifies which pair is powered.
- **Power Class** - Specifies the required power level required.

Link Aggregation Status - Specifies the capability and current aggregation status of the link.

Link Aggregation Port Id - Specifies the aggregated port identifier.

Maximum Frame Size - Specifies the maximum supported IEEE 802.3 frame size.

Port VLAN Identity - Specifies the VLAN ID of the port.

Protocol VLAN - Specifies the Protocol VLAN ID and status.

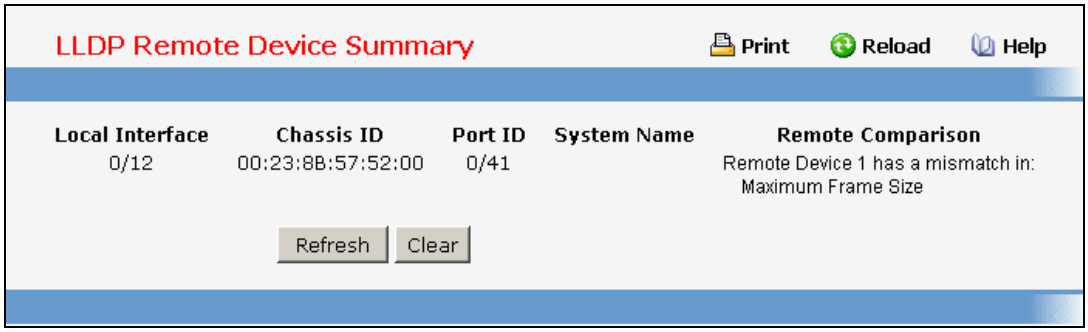
VLAN Name - Specifies the VLAN name.

Protocol Identity - Specifies the particular protocols that are accessible through the port.

Command Buttons

Refresh - Updates the information on the page.

11.3.22.8 Viewing LLDP Remote Device Summary Page



Non-Configurable Data

Local Interface - Specifies the local port which can receive LLDP frames advertised by a remote system.

Chassis ID - Specifies the chassis component associated with the remote system.

Port ID - Specifies the port component associated with the remote system.

System Name - Specifies the system name of the remote system.

Remote Comparison - Display the result of comparison between LLDP local and remote devices information.

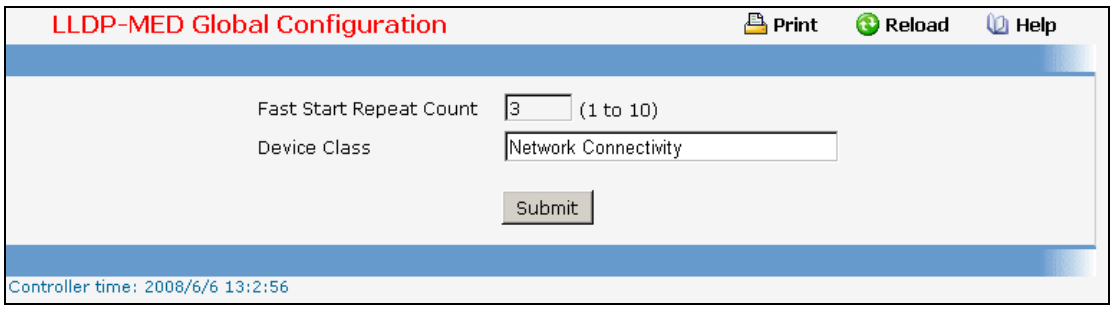
Command Buttons

Refresh - Updates the information on the page.

Clear - Clears LLDP Remote Device information received on all the interfaces.

11.3.23 Managing LLDP-MED

11.3.23.1 Configuring LLDP-MED Global Configuration Page



Configurable Data

Fast Start Repeat Count - Specifies the number of LLDP PDUs that will be transmitted when the protocol is enabled. The range is from (1 to 10). Default value of fast repeat count is 3.

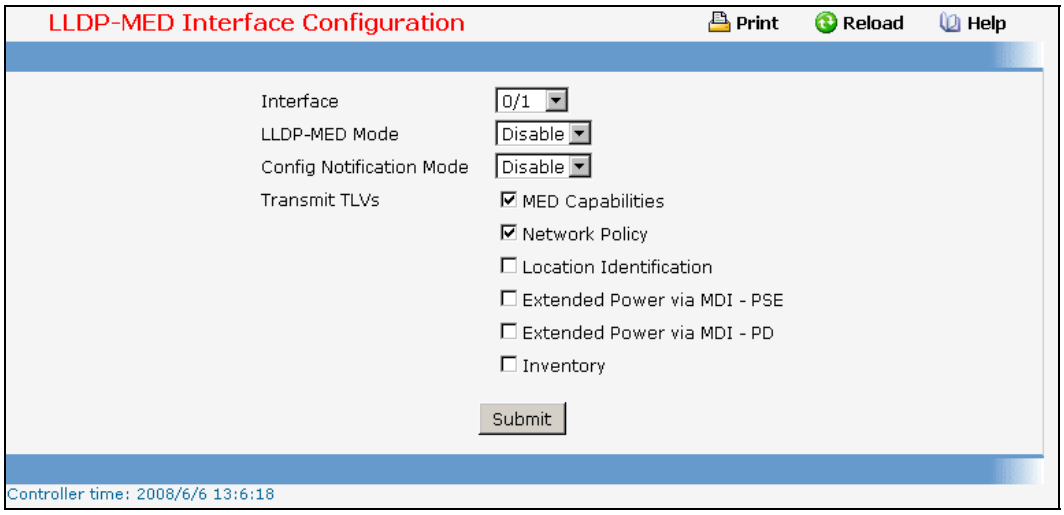
Non-Configurable Data

Device Class - Specifies local device's MED Classification. There are four different kinds of devices, three of them represent the actual end points (classified as Class I Generic [IP Communication Controller etc.], Class II Media [Conference Bridge etc.], Class III Communication [IP Telephone etc.]). The fourth device is Network Connectivity Device, which is typically a LAN Switch/Router, IEEE 802.1 Bridge, IEEE 802.11 Wireless Access Point etc.

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.

11.3.23.2 Configuring LLDP-MED Interface Configuration Page



Selection Criteria

Interface - Specifies the list of ports on which LLDP-MED - 802.1AB can be configured. 'All' option is provided to configure all interfaces on the DUT and to be consistent with CLI. To view the summary of all interfaces refer to 'Interface Summary' webpage. Interface configuration page will not be able to display summary of 'All' interfaces, summary of individual interfaces is visible from 'Interface Configuration' webpage. 'Interface Configuration' webpage for 'All' option will always display LLDP-MED mode and notification mode as 'disabled' and checkboxes for 'Transmit TLVs' will always be unchecked.

LLDP-MED Mode - Specifies the Link Layer Data Protocol-Media End Point (LLDP-MED) mode for the selected interface. By enabling MED, we will be effectively enabling the transmit and receive function of LLDP.

Config Notification Mode - Specifies the LLDP-MED topology notification mode for the selected interface.

Configurable Data

Transmit TLVs - Specifies which optional type length values (TLVs) in the LLDP-MED will be transmitted in the LLDP PDUs frames for the selected interface.

MED Capabilities - To transmit the capabilities TLV in LLDP frames

Network Policy - To transmit the network policy TLV in LLDP frames.

Location Identification - To transmit the location TLV in LLDP frames.

Extended Power via MDI - PSE - To transmit the extended PSE TLV in LLDP frames.

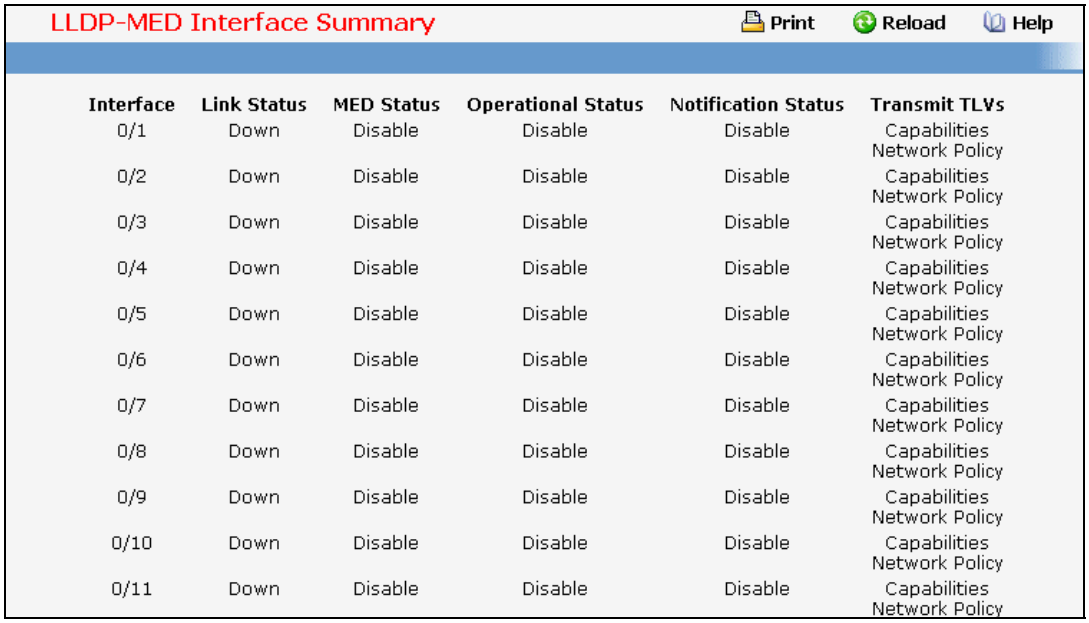
Extended Power via MDI - PD - To transmit the extended PD TLV in LLDP frames.

Inventory - To transmit the inventory TLV in LLDP frames.

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.

11.3.23.3 Configuring LLDP-MED Interface Summary Page



Non-Configurable Data

Interface - Specifies all the ports on which LLDP-MED can be configured.

Link Status - Specifies the link status of the ports whether it is Up/Down.

MED Status - Specifies the LLDP-MED mode is enabled or disabled on this interface.

Operational Status - Specifies the LLDP-MED TLVs are transmitted or not on this interface.

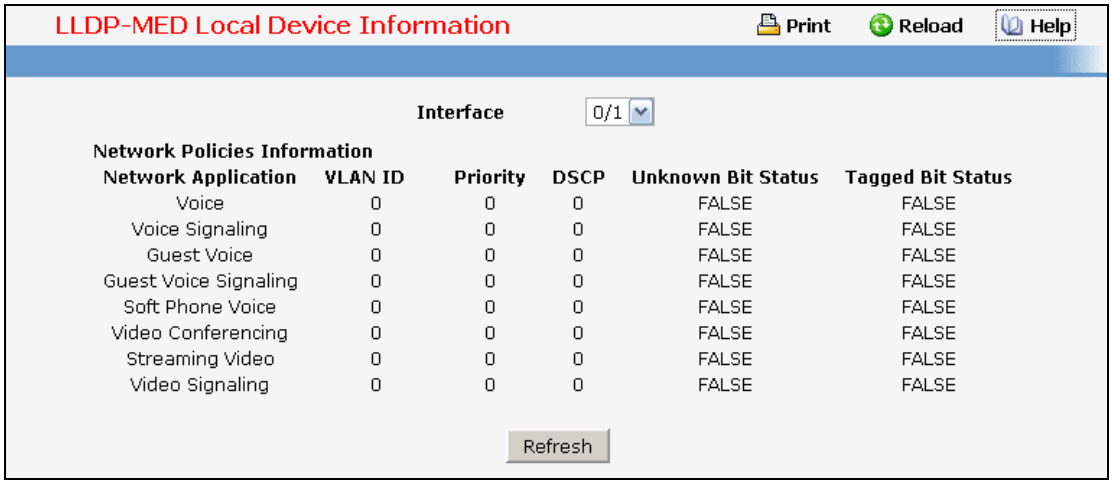
Notification Status - Specifies the LLDP-MED topology notification mode of the interface.

Transmit TLV(s) - Specifies the LLDP-MED transmit TLV(s) that are included.

Command Buttons

Refresh - Updates the information on the page.

11.3.23.4 Configuring LLDP-MED Local Device Information Page



Selection Criteria

Interface - Specifies the list of all the ports on which LLDP-MED frames can be transmitted.

Non-Configurable Data

Network Policy Information - Specifies if network policy TLV is present in the LLDP frames.

Media Application Type - Specifies the application type. Types of application types are unknown, voicesignaling, guestvoice, guestvoicesignalling, softphonevoice, videoconferencing, streammingvideo, vidoesignalling. Each application type that is received has the VLAN id, priority, DSCP, tagged bit status and unknown bit status. A port may receive one or many such application types. If a network policy TLV has been transmitted only then would this information be displayed.

Vlan Id - Specifies the VLAN id associated with a particular policy type.

Priority - Specifies the priority associated with a particular policy type.

DSCP - Specifies the DSCP associated with a particular policy type.

Unknown Bit Status - Specifies the unknown bit associated with a particular policy type.

Tagged Bit Status - Specifies the tagged bit associated with a particular policy type.

Inventory - Specifies if inventory TLV is present in LLDP frames.

Hardware Revisions - Specifies hardware version.

Firmware Revisions - Specifies Firmware version.

Software Revisions - Specifies Software version.

Serial Number - Specifies serial number.

Manufacturer Name - Specifies manufacturers name.

Model Name - Specifies model name.

Asset ID - Specifies asset id.

Location Information - Specifies if location TLV is present in LLDP frames.

Sub Type - Specifies type of location information.

Location Information - Specifies the location information as a string for given type of location id

Extended PoE - Specifies if local device is a PoE device.

Device Type - Specifies power device type.

Extended PoE PSE - Specifies if extended PSE TLV is present in LLDP frame.

Available - Specifies available power sourcing equipment's power value in tenths of watts on the port of local device.

Source - Specifies power source of this port.

Priority - Specifies PSE port power priority.

Extended PoE PD - Specifies if extended PD TLV is present in LLDP frame.

Required - Specifies required power device power value in tenths of watts on the port of local device.

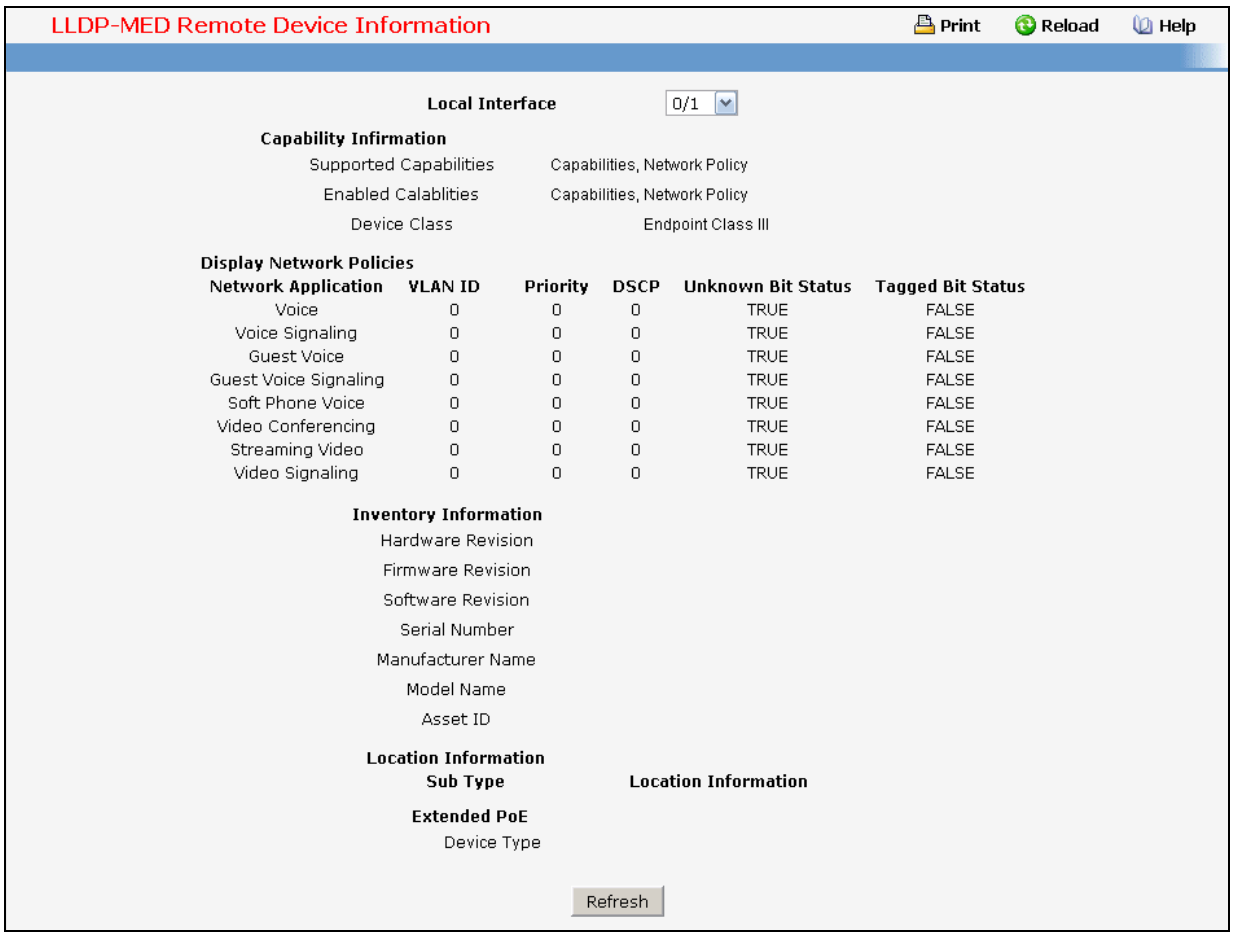
Source - Specifies power source of this port.

Priority - Specifies PD port power priority.

Command Buttons

Refresh - Updates the information on the page.

11.3.23.5 Configuring LLDP-MED Remote Device Information Page



Selection Criteria

Local Interface - Specifies the list of all the ports on which LLDP-MED is enabled.

Non-Configurable Data

Capability Information - Specifies the supported and enabled capabilities that was received in MED TLV on this port.

Supported Capabilities - Specifies supported capabilities that was received in MED TLV on this port.

Enabled Capabilities - Specifies enabled capabilities that was received in MED TLV on this port.

Device Class - Specifies device class as advertised by the device remotely connected to the port.

Network Policy Information - Specifies if network policy TLV is received in the LLDP frames on this port.

Media Application Type - Specifies the application type. Types of application types are unknown, voicesignaling, guestvoice, guestvoicesignalling, softphonevoice, videoconferencing, streammingvideo, vidoesignalling. Each application type that is received has the VLAN id, priority, DSCP, tagged bit status and unknown bit status. A port may receive one or many such application types. If a network policy TLV has been receive on this port only then would this information be displayed.

VLAN Id - Specifies the VLAN id associated with a particular policy type.

Priority - Specifies the priority associated with a particular policy type.

DSCP - Specifies the DSCP associated with a particular policy type.

Unknown Bit Status - Specifies the unknown bit associated with a particular policy type.

Tagged Bit Status - Specifies the tagged bit associated with a particular policy type.

Inventory Information - Specifies if location TLV is received in LLDP frames on this port.

Hardware Revision - Specifies hardware version of the remote device.

Firmware Revision - Specifies Firmware version of the remote device.

Software Revision - Specifies Software version of the remote device.

Serial Number - Specifies serial number of the remote device.

Manufacturer Name - Specifies manufacturers name of the remote device.

Model Name - Specifies model name of the remote device.

Asset ID - Specifies asset id of the remote device.

Location Information - Specifies if location TLV is received in LLDP frames on this port.

Sub Type - Specifies type of location information.

Location Information - Specifies the location information as a string for given type of location id.

Extended PoE - Specifies if remote device is a PoE device.

Device Type - Specifies remote device's PoE device type connected to this port.

Extended PoE PSE - Specifies if extended PSE TLV is received in LLDP frame on this port.

Available - Specifies the remote ports PSE power value in tenths of watts.

Source - Specifies the remote ports PSE power source.

Priority - Specifies the remote ports PSE power priority.

Extended PoE PD - Specifies if extended PD TLV is received in LLDP frame on this port.

Required - Specifies the remote port's PD power requirement.

Source - Specifies the remote port's PD power source.

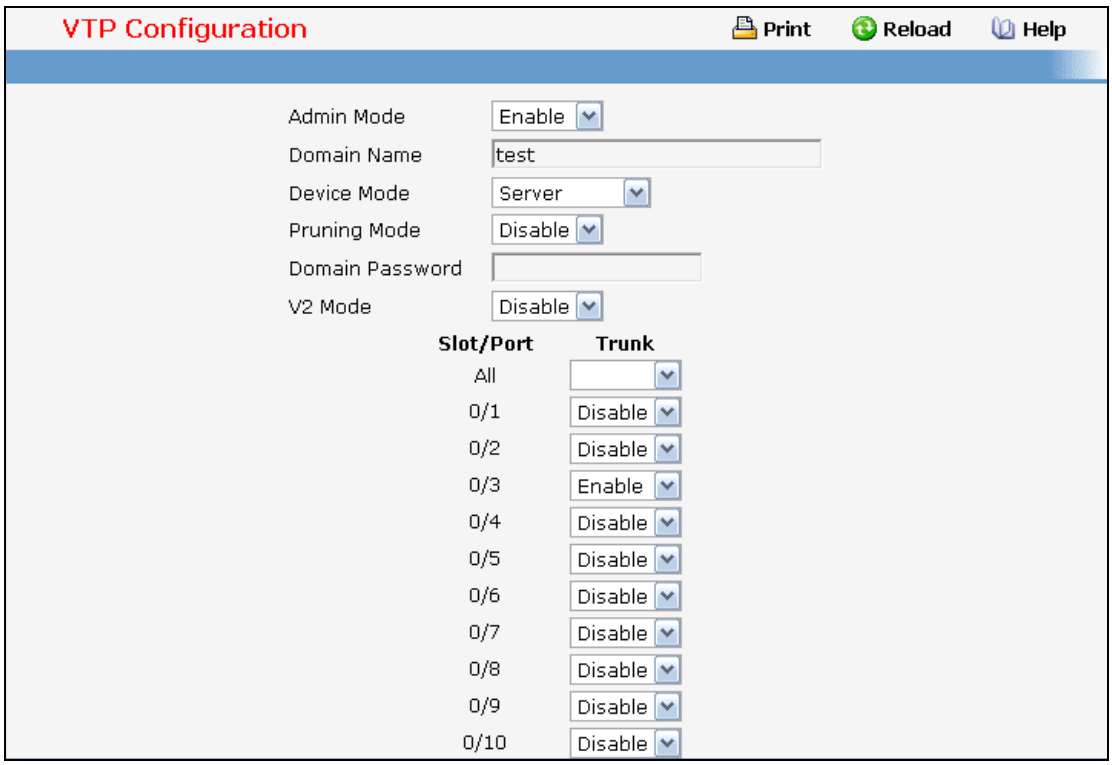
Priority - Specifies the remote port's PD power priority.

Command Buttons

Refresh - Updates the information on the page.

11.3.24 Managing VTP

11.3.24.1 Configuring VTP Configuration Page



Selection Criteria

Admin Mode - Enable or disable the VTP feature.

Device Mode - Use the pulldown menu to select the VTP device mode(client, server and transparent). The default operational mode of VTP device is "server".

Pruning Mode - Enable or disable the VTP pruning mode.

V2 Mode - Enable or disable the VTP version 2 mode.

Trunkport - Enable or disable the VTP trunkport for specified interface.

Configurable Data

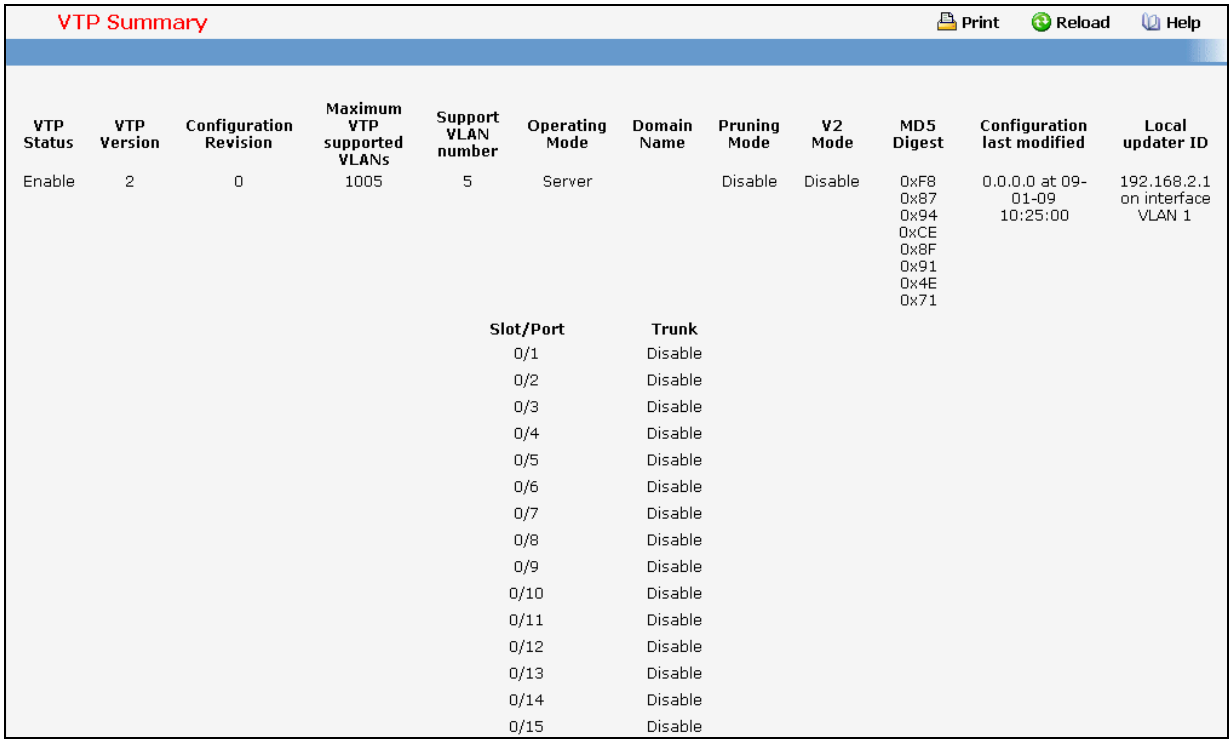
Domain Name - Set the name of the VTP administrative domain.

Domain Password - Set the password for the VTP administrative domain.

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.

11.3.24.2 Viewing VTP Status Page



Non-configurable data

VTP Status - Displays the VTP Status.

VTP Version - Displays the VTP version operating on the switch.

Configuration Revision - Displays the current configuration revision number on this switch.

Maximum VTP supported VLANs - Maximum number of VLANs supported locally.

Support VLAN number - Number of existing VLANs.

Operating mode - Displays VTP operating mode.

Domain Name - Displays the name that identifies the administrative domain for the switch.

Pruning mode - Displays VTP pruning mode.

V2 Mode - Displays VTP version 2 mode.

MD5 Digest - Displays the checksum values for the VTP domain status.

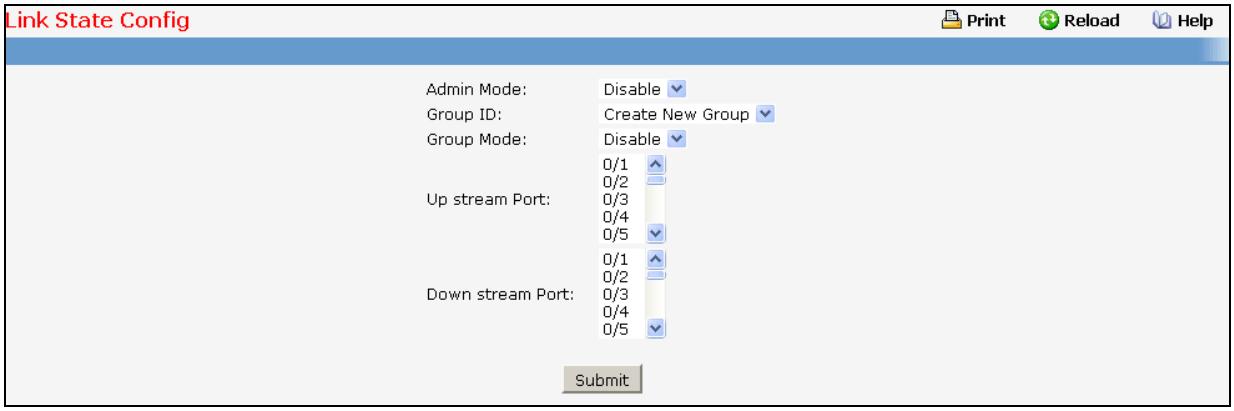
Configuration last modified - Displays the time stamp of the last configuration modification and the IP address of the switch that caused the configuration change to the database.

Local updater ID - Displays the Local updater ID for the VTP domain status.

Trunkport - Displays the VTP Trunkport.

11.3.25 Managing Link State

11.3.25.1 Configuring Link State Configuration Page



Selection Criteria

Admin Mode - Choose the link state administrative mode for the switch by selecting enable or disable from the pull-down menu. The factory default is disabled.

Group ID – You can use this screen to reconfigure an existing group or to create a new one. Use this pull-down menu to select one of the existing groups or select 'Create' to add a new one.

Group Mode - Choose the group administrative mode for the switch by selecting enable or disable from the pull-down menu. The factory default is disabled.

Upstream - Choose the upstream port for a group. Switch will monitor the link level of this port for rapidly fail-over of redundant LAN ports.

Configurable Data

Downstream - Choose downstream ports for a group. Switch will associate these downstream ports with upstream port. If the upstream port is link down, all downstream ports will be disabled. Otherwise, they will be enabled.

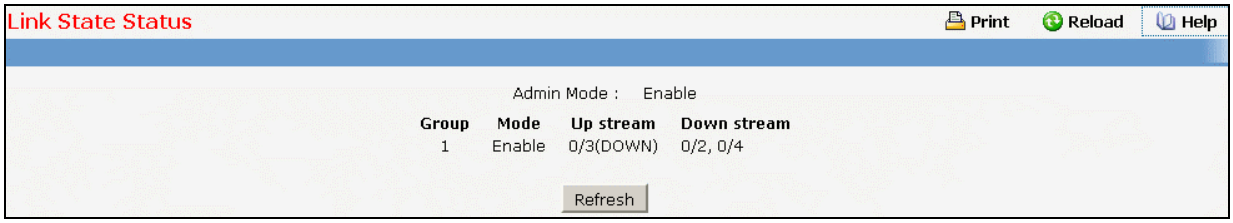
Command Buttons

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 this group.

11.3.25.2 Configuring Link State Status

This page displays the status of all currently configured link state.



Selection Criteria

Admin Mode - The administrative mode of the link state function.

Group ID - The group identify of the link state. The range of the group ID is 1 ~ 6.

Mode - The administrative mode of the group.

Upstream port - The monitored uplink port, and the link state of this uplink port.

Downstream ports - The downlink ports for link state.

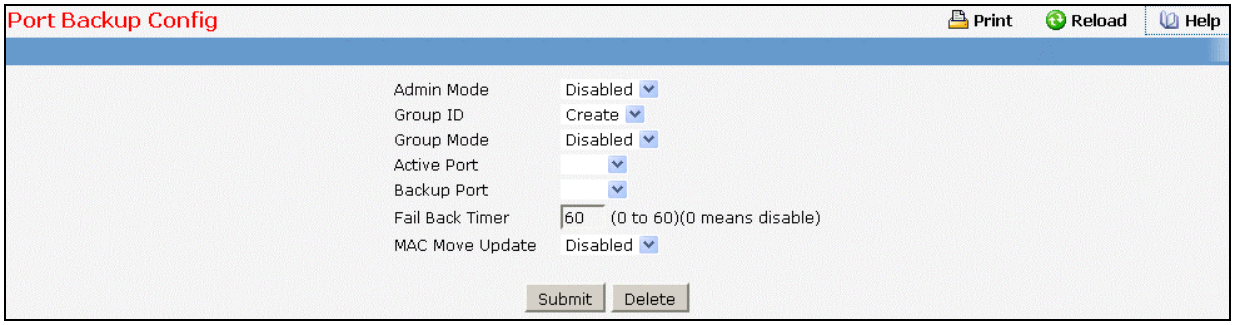
Command Buttons

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

11.3.26 Managing Port-Backup

11.3.26.1 Configuring Port-Backup Configuration

Two ports are associated for one group. Two ports are acted as active and backup ports. One of two ports will be active at a one time. As configured active port is linkup, the backup port will be disabled. Otherwise, if configured active port is link down, the configured backup port will be enabled. The configured active has higher priority to become 'active', as two ports of a group are all link up before group is enabled.



Selection Criteria

Admin Mode - Choose the port-backup administrative mode for the switch by selecting enable or disable from the pull-down menu. The factory default is disabled.

Group ID - You can use this screen to reconfigure an existing group or to create a new one. Use this pull-down menu to select one of the existing groups or select 'Create' to add a new one.

Group Mode - Choose the group administrative mode for the switch by selecting enable or disable from the pull-down menu. The factory default is disabled. You could enable this group as active port and backup port are configured.

Active port - Configure the active port for a group. 6 port pair for six 1Gbps are configurable for active port.

Backup port - Choose the backup port for a group. 6 port pair for six 1Gbps are configurable for backup port.

MAC Move Update - Choose the MAC Move Update mode for the switch by selecting enable or disable from the pull-down menu.

Configurable Data

Fail Back Timer - Configure the time delay for activating the active port.

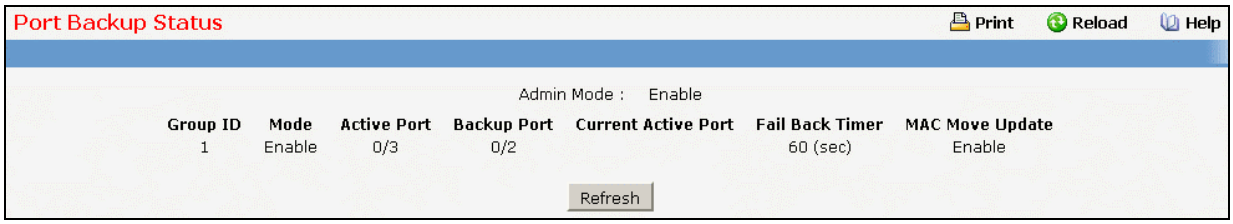
Command Buttons

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 this group.

11.3.26.2 Configuring Port-Backup Status

This page displays the status of all currently configured port-backup.



Non-Configurable Data

Admin Mode - The administrative mode of the port-backup function.

Group ID - The group identify of the port-backup. The range of the group ID is 1~6.

Mode - The administrative mode of this group.

Active port - The configured active port for this group.

Backup port - The configured backup port for this group.

Current Active port - Current active port for this group.

Failback Time - The Failback Time value for the group.

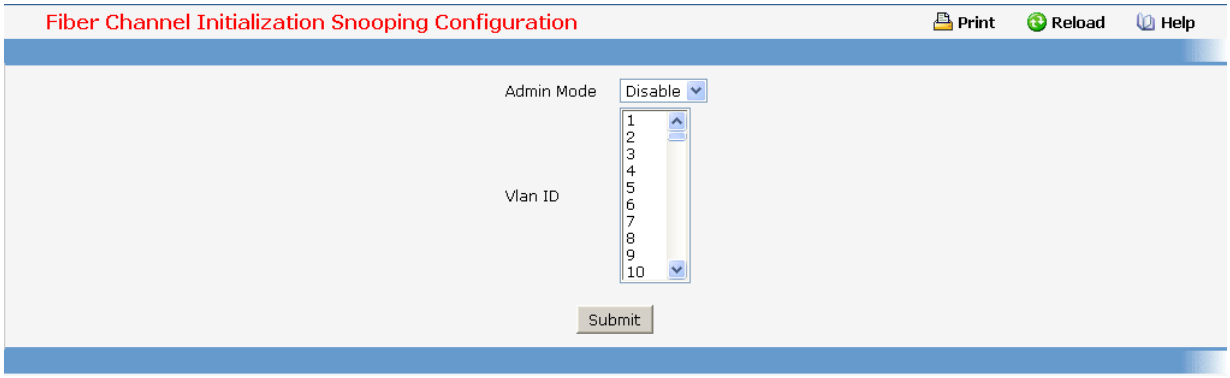
MAC Move Update - The MAC Move Update mode for the group.

Command Buttons

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

11.3.27 Managing FIP-Snooping

11.3.27.1 Configuring FIP-Snooping Configuration



Selection Criteria

Admin Mode - Enable/Disable FIP Snooping function.

- **Enable** - Enable FIP Snooping and start the FIP Snooping process.
- **Disable** - Disable ETS and stop the ETS process.

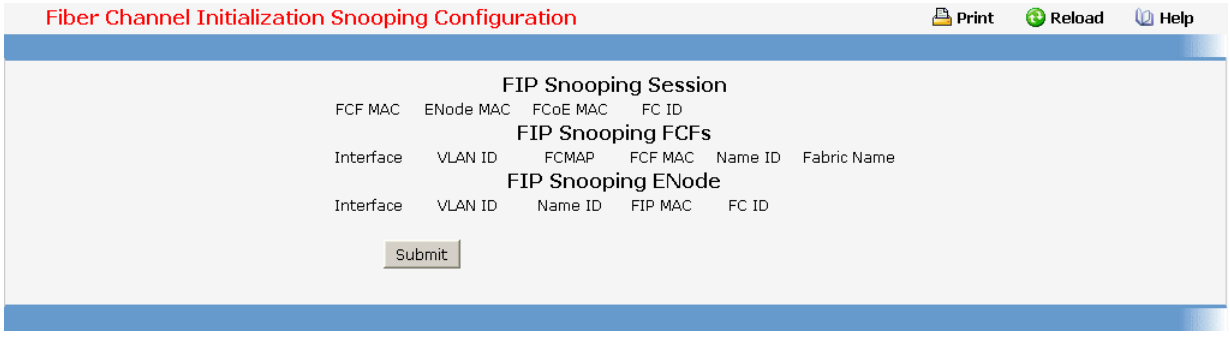
The system's default FIP Snooping admin mode is disabled.

Vlan ID - Configure Vlans the FIP packets will be snooped.

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.

11.3.27.2 Viewing FIP-Snooping Status



Non-Configurable Data

FIP Snooping Session

- **FCF MAC** - MAC address of the FCF.
- **ENode MAC** - MAC address of the ENode.
- **FCoE MAC** - FCoE MAC address that is used to send the FCoE packets.

- **FC ID** - ID number of the virtual port that was created by the FCF when the ENode logged into the network.

FIP Snooping FCFs

- **Interface** - Name of the interface to which the FCoE Forwarder (FCF) is connected.
- **VLAN** - ID number of the VLAN to which the FCF belongs.
- **FCMAP** - May FC-Map value used by the FCF. The default value is 0xEFC00.
- **FCF MAC** - MAC address of the FCF.
- **Name ID** - Name ID.
- **Fabric Name** - Name of the FCF.

FIP Snooping ENode

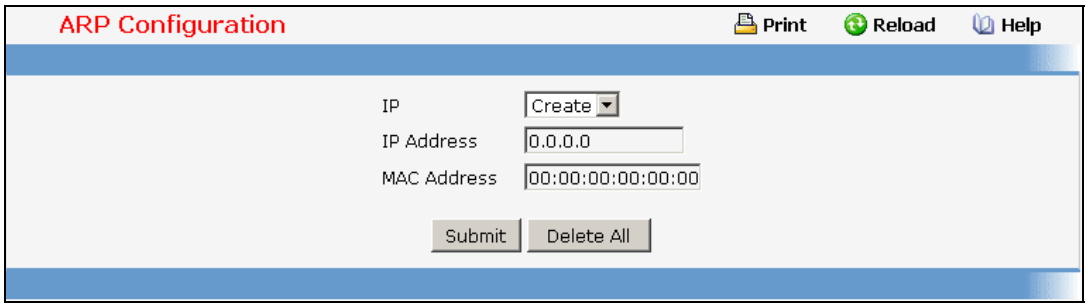
- **Interface** - Name of the interface to which the ENode is connected.
- **VLAN** - ID number of the VLAN to which the ENode belongs.
- **Name ID** - Name ID.
- **ENode MAC** - MAC address of the ENode.

11.4 Routing Menu

11.4.1 Managing ARP Table

11.4.1.1 Creating ARP entries

Use this panel to add an entry to the Address Resolution Protocol table.



Configurable Data

IP - Specifies all the existing static ARP along with an additional option "Create". When the user selects "Create" another text boxes " IP Address" and "MAC Address" appear where the user may enter IP address and MAC address to be configured.

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.

Command Buttons

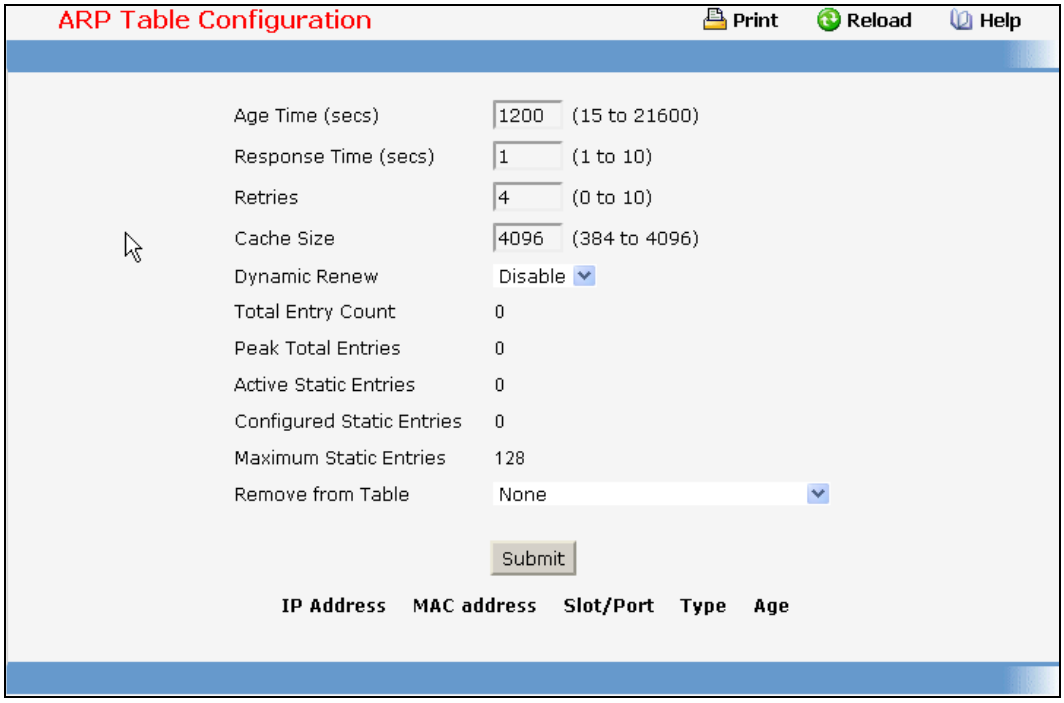
Submit - Update the switch with the values on this screen. If you want the switch to retain the new values across a power cycle, you must perform a save.

Delete - Allows the user to remove specified static entry from the ARP Table.

Delete All - Allows the user to remove all static entries from the ARP Table.

11.4.1.2 Configuring ARP Table

You can use this panel to change the configuration parameters for the Address Resolution Protocol Table. You can also use this screen to display the contents of the table.



Configurable Data

Age Time (secs)- 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 (secs) - 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.

Cache Size - Enter an integer which specifies the maximum number of entries for the ARP cache. The range for this field is 384 to 4096. The default value for Cache Size is 4096.

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.
- **Specific Interface** - Selecting this allows the user to specify the required interface.
- **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.

Slot/Port - The routing interface associated with the ARP entry.

Non-Configurable Data

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.

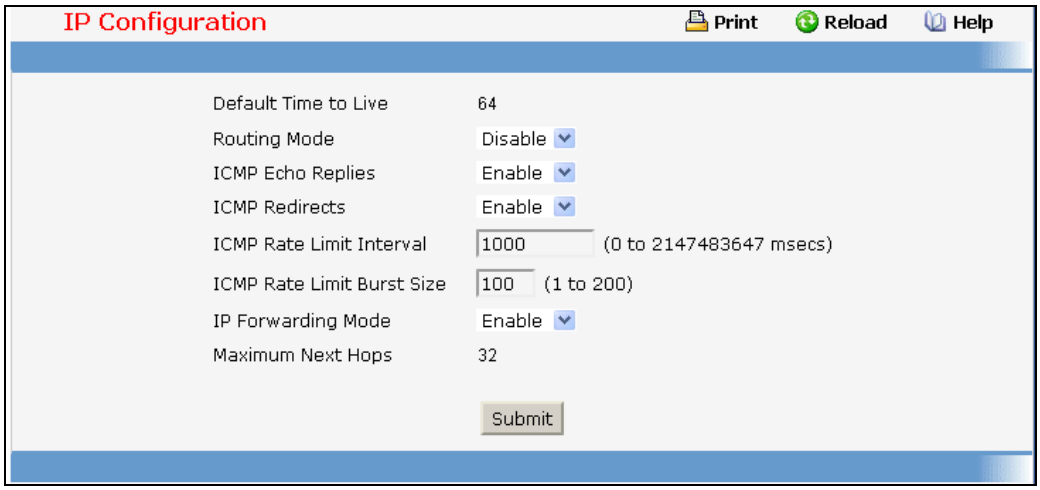
Command Buttons

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.

11.4.2 Managing IP Interfaces

11.4.2.1 Configuring IP

Use this menu to configure routing parameters for the switch as opposed to an interface.



Selection Criteria

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.

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.

11.4.2.2 Viewing IP Statistics

The statistics reported on this panel are as specified in RFC 1213.

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.

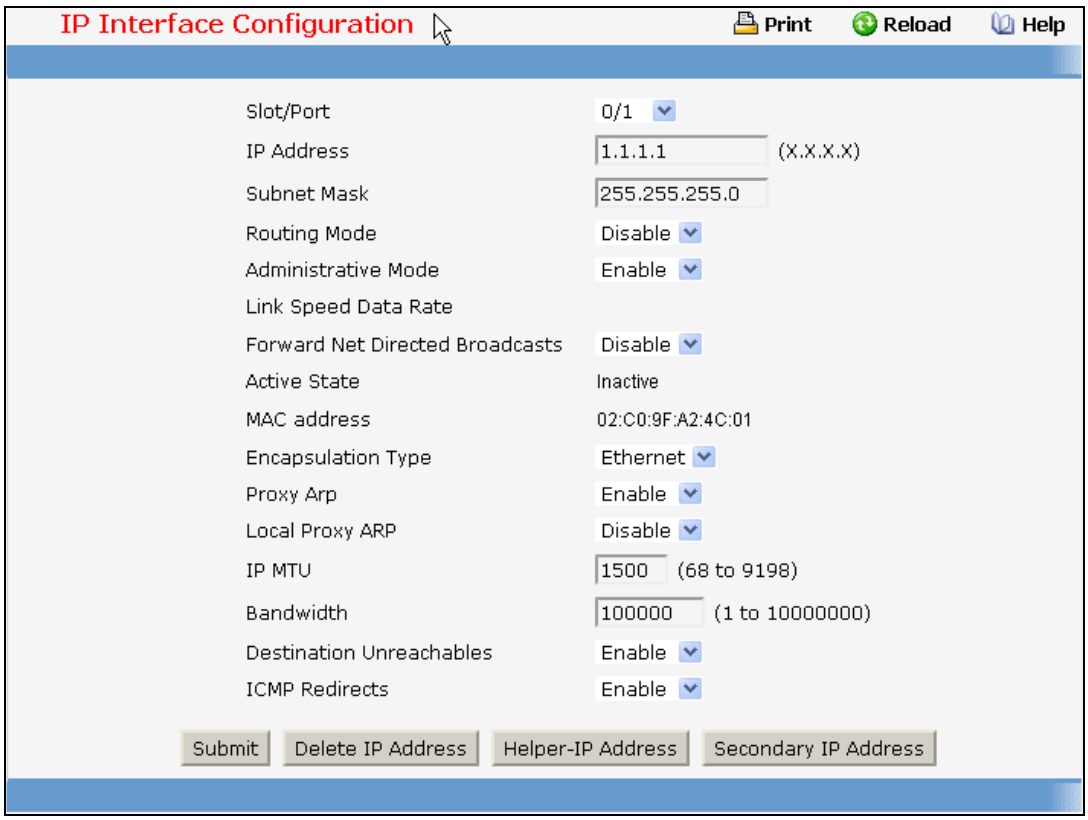
IcmpOutAddrMasks - The number of ICMP Address Mask Request messages sent.

IcmpOutAddrMaskReps - The number of ICMP Address Mask Reply messages sent.

Command Buttons

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

11.4.2.3 Configuring IP Interfaces



Selection Criteria

Slot/Port - Select the interface for which data is to be displayed or configured.

Routing Mode - Setting this enables or disables routing for an interface. The default value is enable.

Administrative Mode - The Administrative Mode of the 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.

Local Proxy Arp - Select to disable or enable Local Proxy ARP for the specified interface from the pulldown menu.

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.

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

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.

Link Speed Data Rate - An integer representing the physical link data rate of the specified interface. This data is valid only for physical interfaces and is measured in Megabits per second (Mbps).

Command Buttons

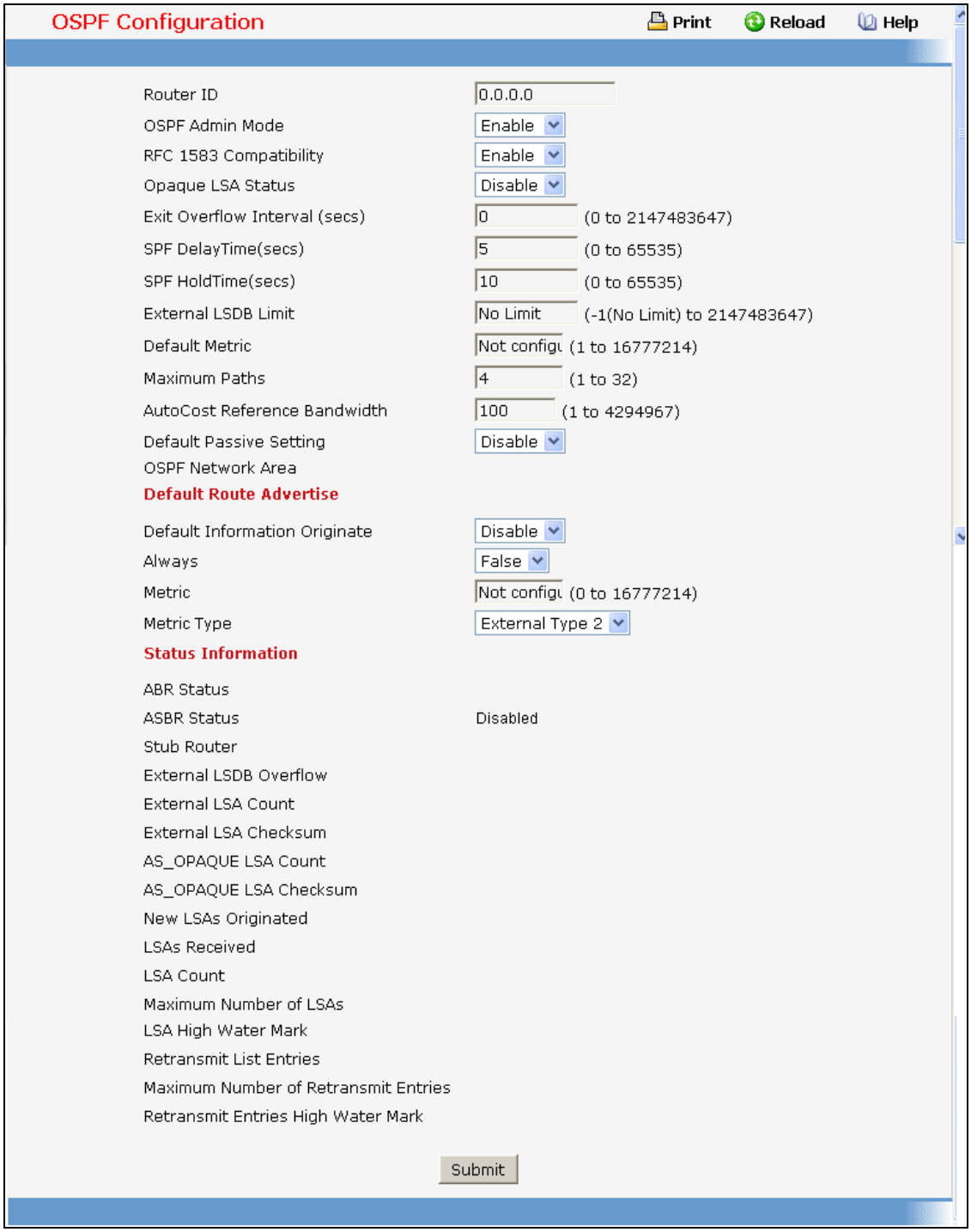
Submit - Update the switch with the values on this screen. If you want the switch to retain the new values across a power cycle, you must perform a save.

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.

11.4.3 Managing OSPF

11.4.3.1 Configuring OSPF



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.

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 (secs)- 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.

SPF DelayTime(secs) - Enter the number of seconds, Delay time (in seconds)is the time between when OSPF receives a topology change and when it starts an SPF calculation. It can be an integer from 0 to 65535. The default time is 5 seconds. A value of 0 means that there is no delay; that is, the SPF calculation is started immediately.

SPF HoldTime(secs) - Enter the number of seconds, minimum time (in seconds) between two consecutive SPF calculations.It can be an integer from 0 to 65535. The default time is 10 seconds. A value of 0 means that there is no delay; that is, two SPF calculations can be done, one immediately after the other.

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)

Maximum Paths - Sets the maximum number of paths that OSPF can report for a given destination. The valid values are (1 to 6).

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.

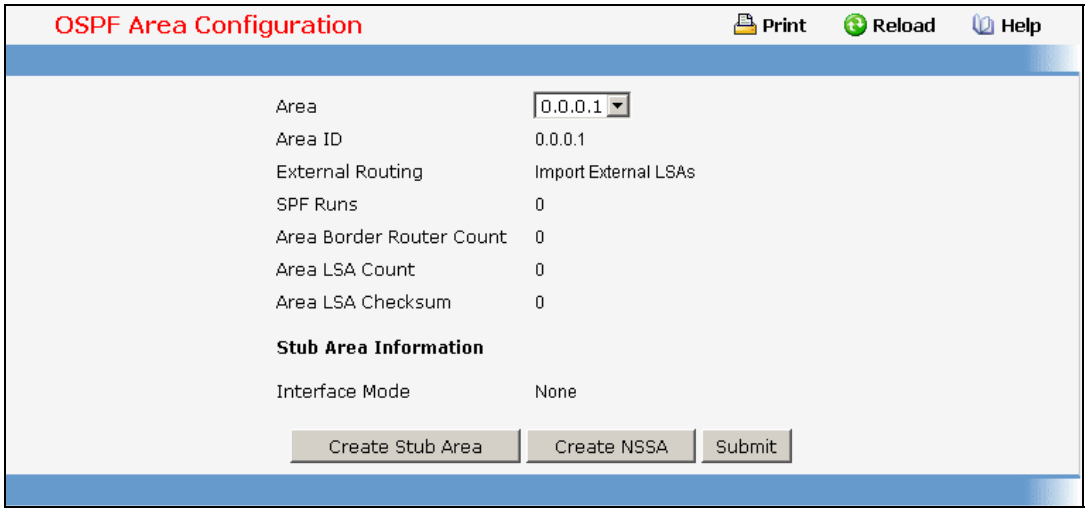
New LSAs Originated - In any given OSPF area, a router will originate several LSAs. Each router originates a router-LSA. If the router is also the Designated Router for any of the area's networks, it will originate network-LSAs for those networks. This value represents the number of LSAs originated by 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.

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.

11.4.3.2 Configuring Area



Configurable Data

Router ID - The 32 bit integer in dotted decimal format that uniquely identifies the router within the OSPF domain. 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 Enable. You must configure a Router ID before OSPF can become operational.

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 RFC 2328. The newer preference rules prevent routing loops when AS-external-LSAs for the same destination have been originated from different areas. The default value is Enable. All routers in the OSPF domain must be configured the same. If all OSPF routers are capable of operating according to RFC 2328, RFC 1583 Compatibility should be disabled.

Opaque LSA Status - Set this parameter to Enable to if OSPF should store and flood opaque LSAs. An opaque LSA is used for flooding user-defined information within an OSPF router domain.

Exit Overflow Interval - When the number of non-default external LSAs exceeds a configured limit, the router enters an overflow state as defined in RFC 1765. The Exit Overflow Interval specifies how long OSPF must wait before attempting to leave overflow state. In overflow state, OSPF cannot originate non-default external LSAs. If the Exit Overflow Interval is 0, OSPF will not leave overflow state until it is disabled and re-enabled. The range is 0 to 2,147,483,647 seconds.

SPF DelayTime(secs) - Delay time is the number of seconds from when OSPF receives a topology change to the start of the next SPF calculation. Delay Time is an integer from 0 to 65535 seconds. The default time is 5 seconds. A value of 0 means that there is no delay; that is, the SPF calculation is started upon a topology change.

SPF HoldTime(secs) - Hold Time is the minimum time in seconds between two consecutive SPF calculations. The range is 0 to 65,535 seconds. The default time is 10 seconds. A value of 0 means that there is no delay; that is, two SPF calculations can be done, one immediately after the other.

External LSDB Limit - The maximum number of External LSAs that can be stored in the database. A value of -1 indicates there is no limit. The valid range of values is (-1 to 2147483647).

Default Metric - Sets a default for the metric of redistributed routes. This field is blank if a default metric has not been configured. The range of valid values is (1 to 16777214)

Maximum Paths - Configure the maximum number of paths that OSPF can report to a given destination. The range of valid values is (1 to 32)

AutoCost Reference Bandwidth - Configure the auto-cost reference-bandwidth to control how OSPF calculates link cost. Specify the reference bandwidth in megabits per second. Unless a link cost is configured, the link cost is computed by dividing the reference bandwidth by the interface bandwidth. The range is (1 to 4294967)

Default Passive Setting - Configure the global passive mode setting for all OSPF interfaces. Configuring this field overwrites any present interface level passive mode setting. OSPF does not form adjacencies on passive interfaces, but does advertise attached networks as stub networks.

Default Route Advertise

Default Information Originate - When this parameter is enabled, OSPF originates an external LSA advertising a default route (0.0.0.0/0.0.0.0).

Always - If Default Information Originate is enabled, but the Always option is FALSE, OSPF will only originate a default route if the router already has a default route in its routing table. Set Always to TRUE to force OSPF to originate a default route regardless of whether the router has a default route.

Metric - Specifies the metric of the default route. The range of valid values is (0 to 16777214)

Metric Type - Sets the OSPF metric type of the default route.

Non-Configurable Data

ABR Status - The router is an Area Border Router if it has active non-virtual interfaces in two or more OSPF areas.

ASBR Status - The router is an Autonomous System Boundary Router if it is configured to redistribute routes from another protocol, or if it is configured to originate an external LSA advertising the default route.

Stub Router - When OSPF runs out of resources to store the entire link state database, or any other state information, OSPF goes into stub router mode. As a stub router, OSPF re-originates its own router LSAs, setting the cost of all non-stub interfaces to infinity. To restore OSPF to normal operation, disable and re-enable OSPF.

External LSDB Overflow - When the number of non-default external LSAs exceeds the configured limit, External LSDB Limit, OSPF goes into LSDB overflow state. In this state, OSPF withdraws all of its self-originated non-default external LSAs. After the Exit Overflow Interval, OSPF leaves the overflow state, if the number of external LSAs has been reduced.

External LSA Count - The number of external LSAs in the link state database.

External LSA Checksum - The sum of the LS checksums of the external LSAs 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. This value is in hexadecimal.

AS_OPAQUE LSA Count - The number of opaque LSAs with domain wide flooding scope.

AS_OPAQUE LSA Checksum - The sum of the LS checksums of the opaque LSAs with domain wide flooding scope. 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. This value is in hexadecimal.

New LSAs Originated - The number of LSAs originated by this router.

LSAs Received - The number of LSAs received.

LSA Count - The total number of link state advertisements currently in the link state database.

Maximum Number of LSAs - The maximum number of LSAs that OSPF can store.

LSA High Water Mark - The maximum size of the link state database since the system started.

Retransmit List Entries - The total number of LSAs waiting to be acknowledged by all neighbors. An LSA may be pending acknowledgment from more than one neighbor.

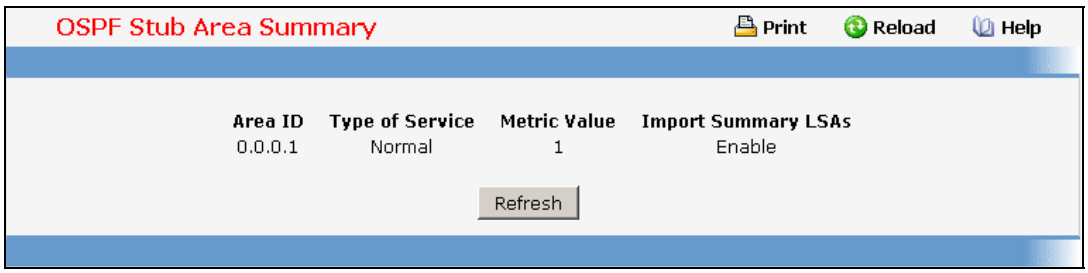
Maximum Number of Retransmit Entries - The maximum number of LSAs that can be waiting for acknowledgment at any given time.

Retransmit Entries High Water Mark - The highest number of LSAs that have been waiting for acknowledgment.

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.

11.4.3.3 Viewing Stub Area Summary Information



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.

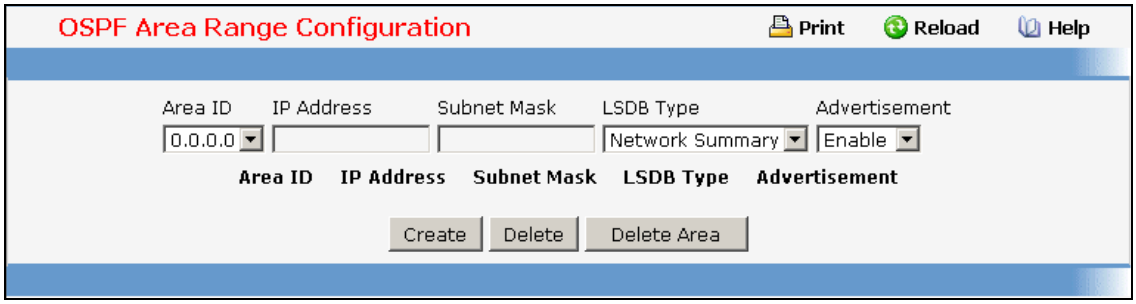
Metric Value - Set the metric value you want applied for the default route advertised into the area. Valid values range from 1 to 16,777,215.

Import Summary LSAs - Whether the import of Summary LSAs is enabled or disabled.

Command Buttons

Refresh - Refresh the data on the screen to the current values from the switch.

11.4.3.4 Configuring Area Range



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.

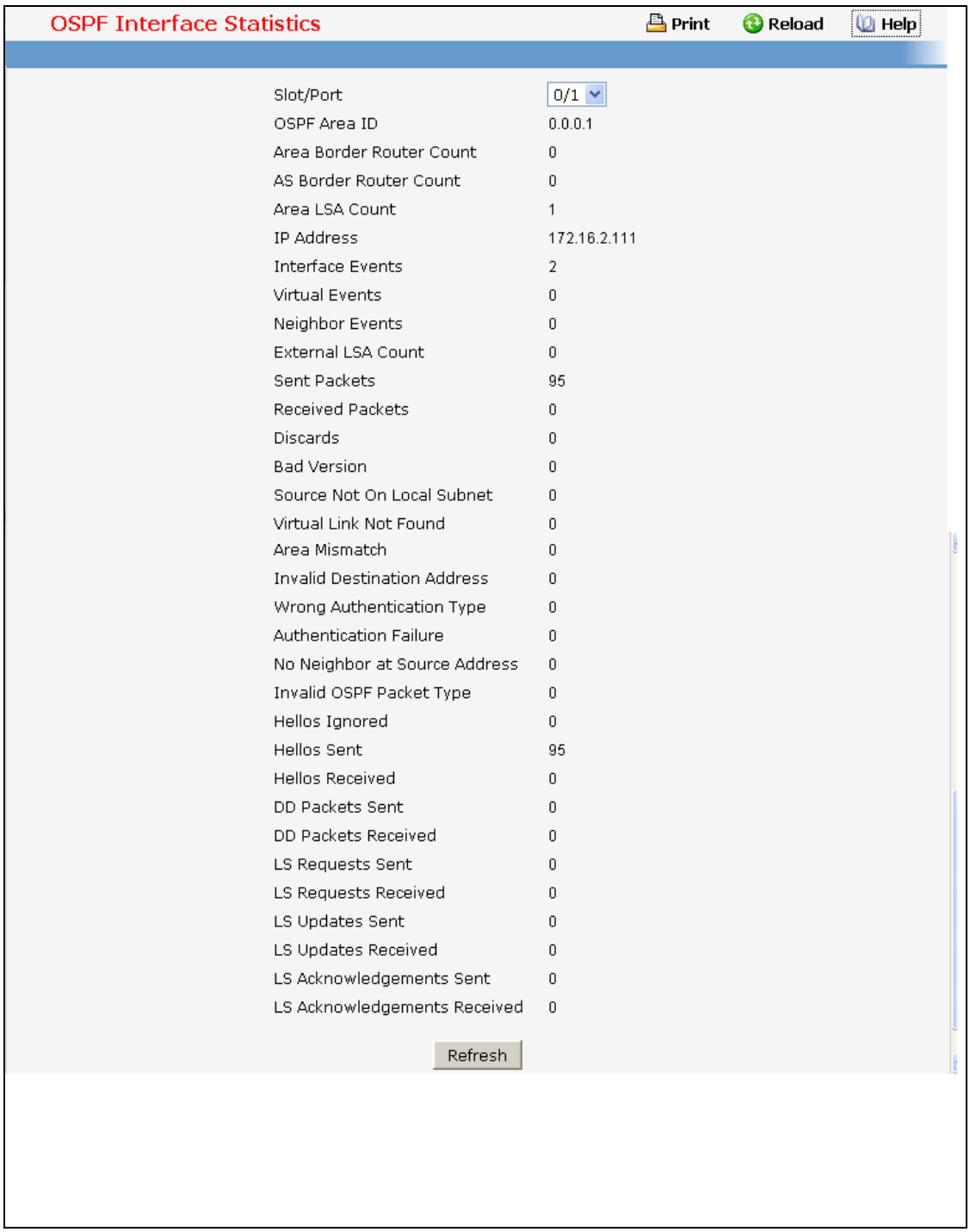
Command Buttons

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.

11.4.3.5 View Interface Statistics

This panel displays statistics for the selected interface. The information will be displayed only if OSPF is enabled.



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.

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.

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.

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.

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.

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.

Invalid OSPF Packet Type - The number of OSPF packets discarded because the packet type field in the OSPF header is not a known type.

Hellos Ignored - The number of received Hello packets that were ignored by this router from the new neighbors after the limit has been reached for the number of neighbors on an interface or on the system as a whole.

Hellos Sent - The number of Hello packets sent on this interface by this router.

Hellos Received - The number of Hello packets received on this interface by this router.

DD Packets Sent - The number of Database Description packets sent on this interface by this router.

DD Packets Received - The number of Database Description packets received on this interface by this router.

LS Requests Sent - The number of LS Requests sent on this interface by this router.

LS Requests Received - The number of LS Requests received on this interface by this router.

LS Updates Sent - The number of LS updates sent on this interface by this router.

LS Updates Received - The number of LS updates received on this interface by this router.

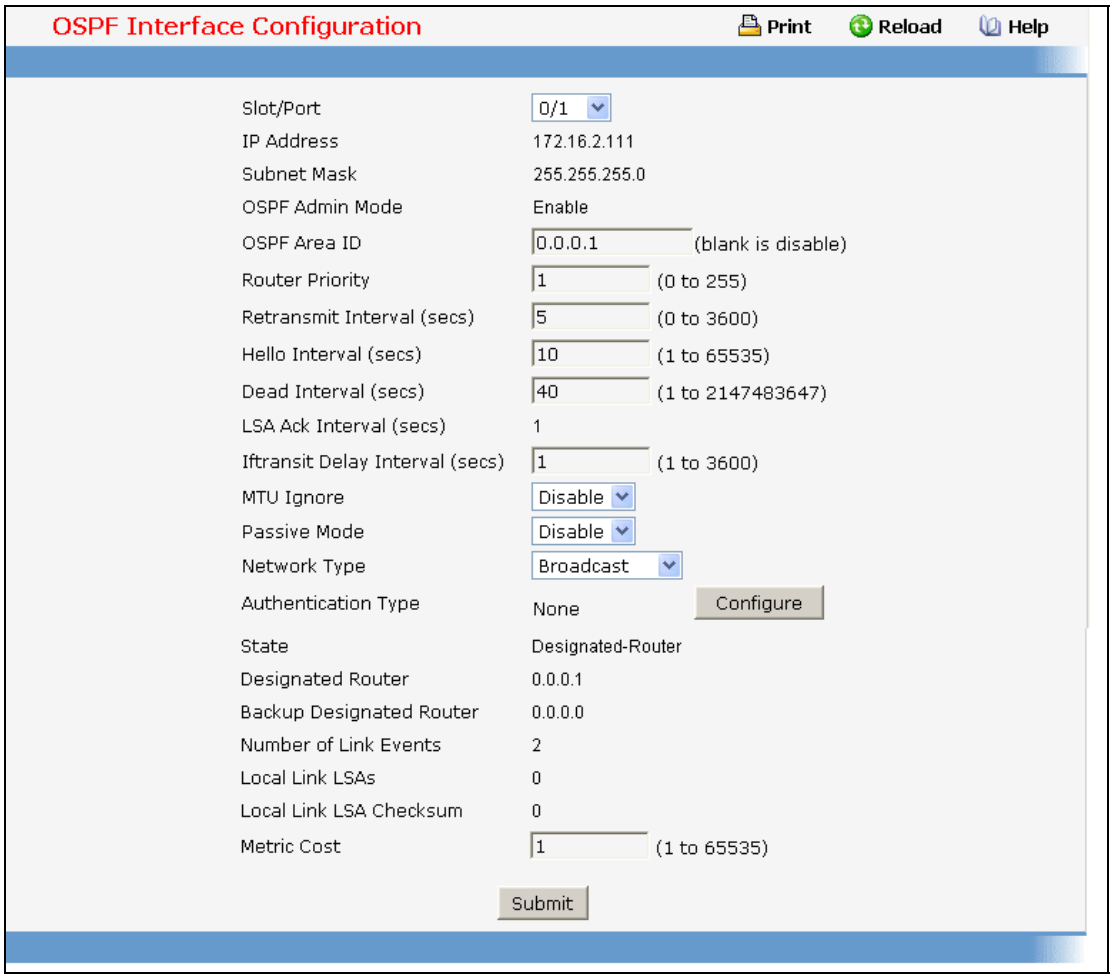
LS Acknowledgements Sent - The number of LS acknowledgements sent on this interface by this router.

LS Acknowledgements Received - The number of LS acknowledgements received on this interface by this router.

Command Buttons

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

11.4.3.6 Configuring OSPF Interface



Selection Criteria

Slot/Port - Select the interface for which data is to be displayed or configured.

Configurable Data

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. Leave blank to disable.

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 (secs)- 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 (secs)- 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 (secs)- 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 (secs)- 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. (MTU mismatch detection is enabled.)

Passive Mode - Make an interface passive to prevent OSPF from forming an adjacency on an interface. OSPF advertises networks attached to passive interfaces as stub networks. Interfaces are not passive by default.

Network Type - Sets the OSPF network type on the interface to broadcast or point-to-point. OSPF only selects a designated router and originates network LSAs for broadcast networks. No more than two OSPF routers may be present on a point-to-point link. The default network type for Ethernet interfaces is broadcast..

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:

- ***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.

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 Key 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

OSPF Admin Mode - 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 .

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.

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.

Local Link LSAs - The number of opaque LSAs whose flooding scope is the link on this interface.

Link Local LSA Checksums - The sum of the checksums of local link LSAs for this link.

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.

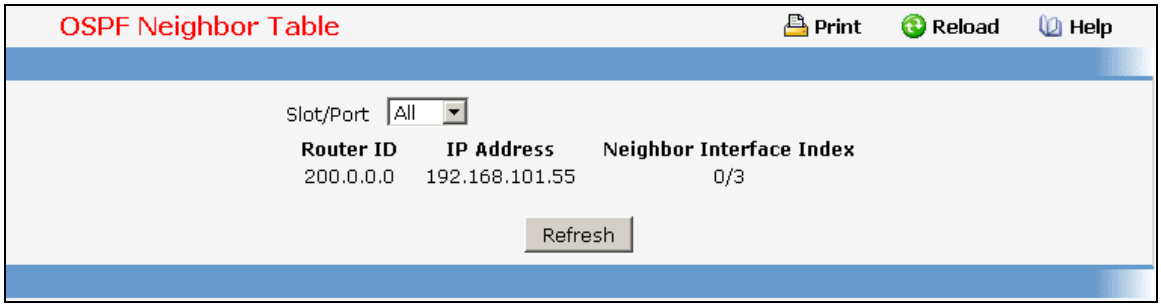
Command Buttons

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.

11.4.3.7 Viewing Neighbor Table Information

This panel 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.



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.

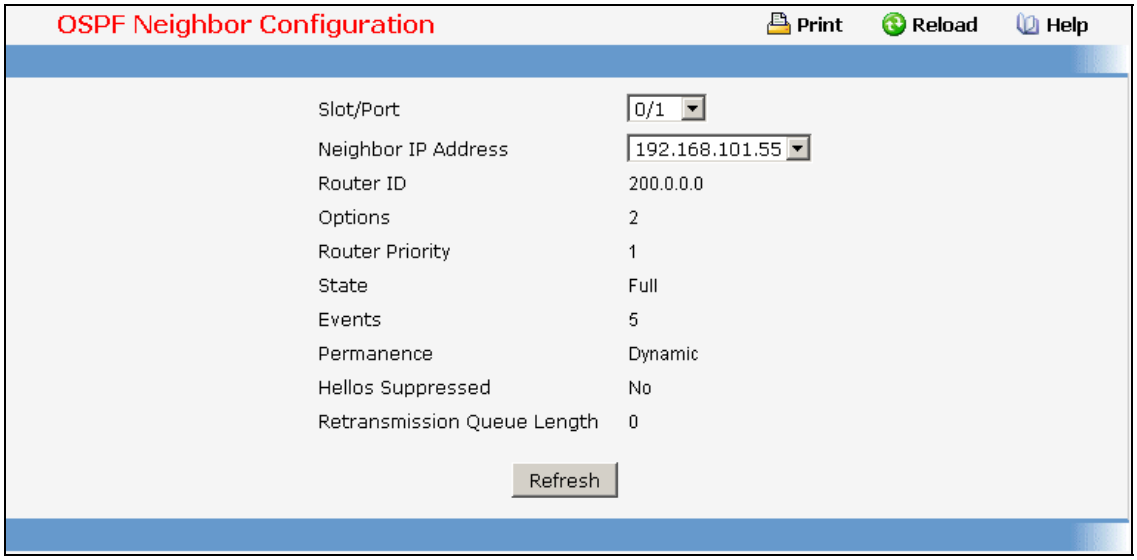
Neighbor Interface Index - A Slot/Port identifying the neighbor interface index.

Command Buttons

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

11.4.3.8 Configuring OSPF Neighbor

This panel 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.



Selection Criteria

Slot/Port - Selects the interface for which data is to be displayed or configured. Slot 0 is the base unit.

Neighbor IP Address - 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.

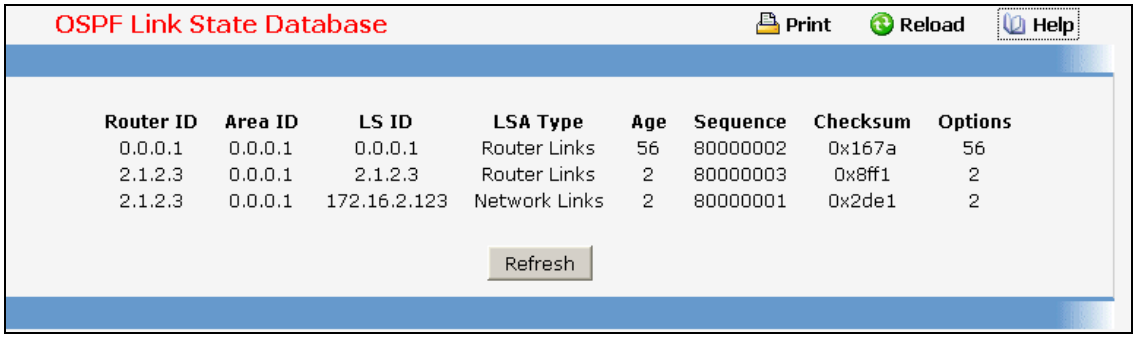
Hellos Suppressed - This indicates whether Hellos are being suppressed to the neighbor.

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.

11.4.3.9 Viewing 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.

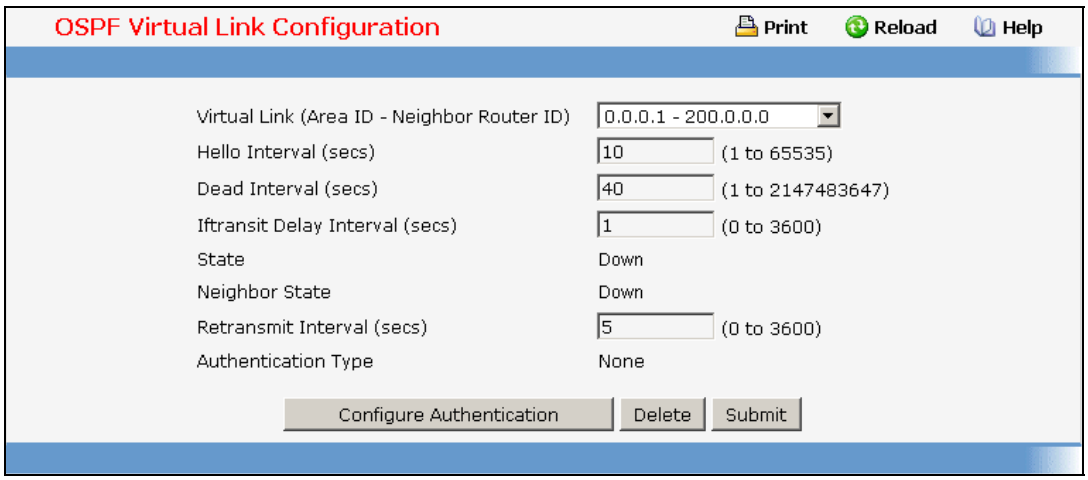
Options - The Options field in the link state advertisement header indicates which optional capabilities are associated with the advertisement. The options are:

- ***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.

Command Buttons

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

11.4.3.10 Configuring OSPF Virtual Link



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 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. 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.

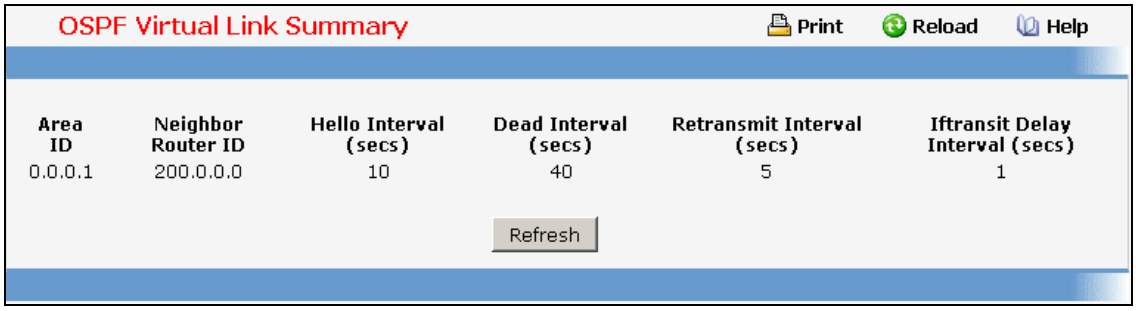
Command Buttons

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.

11.4.3.11 Viewing OSPF Virtual Link Summary Table



Non-Configurable Data

Area ID - The Area ID portion of the virtual link identification for which data is to be displayed. The Area ID and Neighbor Router ID together define a virtual link.

Neighbor Router ID - The neighbor portion of the virtual link identification. Virtual links may be configured between any pair of area border routers having interfaces to a common (non-backbone) area.

Hello Interval - The OSPF hello interval for the virtual link in units of seconds. The value for hello interval must be the same for all routers attached to a network.

Dead Interval - The OSPF dead interval for the virtual link in units of 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 common network, and should be a multiple of the Hello Interval (i.e. 4).

Retransmit Interval - The OSPF retransmit interval for the virtual link in units of seconds. This specifies the time 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.

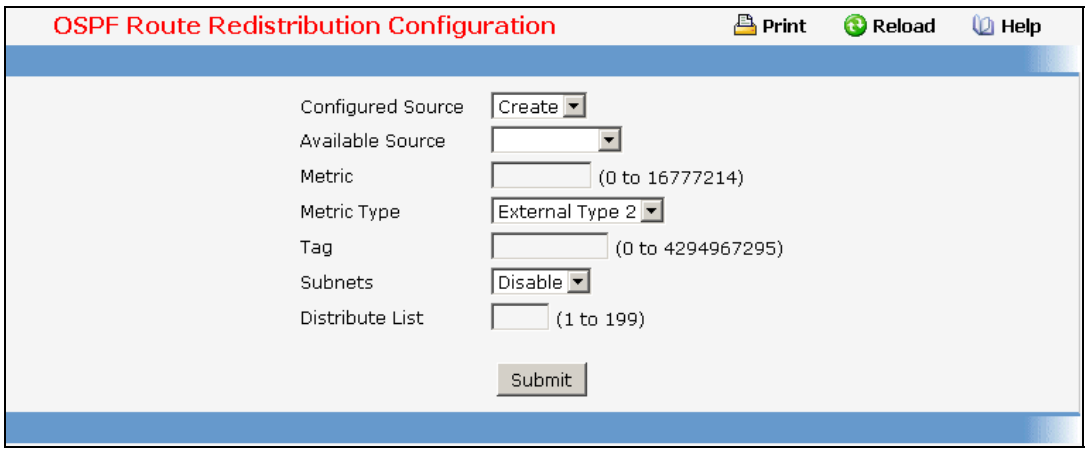
Iftransit Delay Interval - The OSPF Transit Delay for the virtual link in units of seconds. It specifies the estimated number of seconds it takes to transmit a link state update packet over this interface.

Command Buttons

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

11.4.3.12 Configuring OSPF Route Redistribution

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.



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' 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' and 'RIP'.

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.

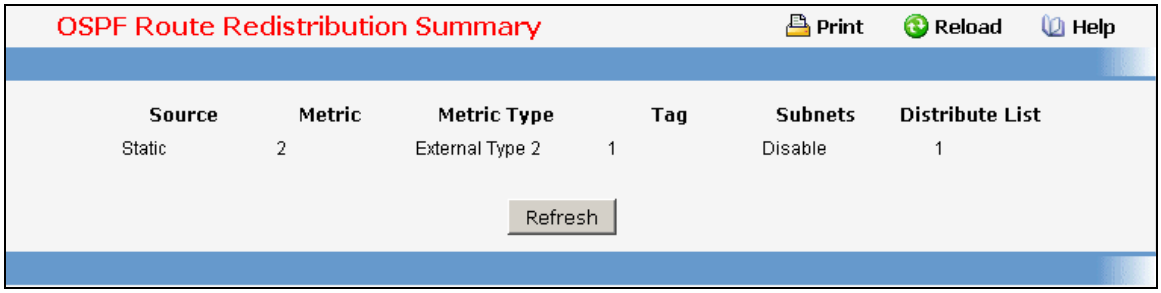
Command Buttons

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.

11.4.3.13 Viewing OSPF Route Redistribution Summary Information

This screen displays the OSPF Route Redistribution Configurations.



Non-Configurable Data

Source - The Source Route to be Redistributed by OSPF.

Metric- The Metric of redistributed routes for the given Source Route. Display "Unconfigured" when not configured.

Metric Type - The OSPF metric types 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 0 to 4294967295.

Subnets - Whether the subnetted routes should be redistributed or not.

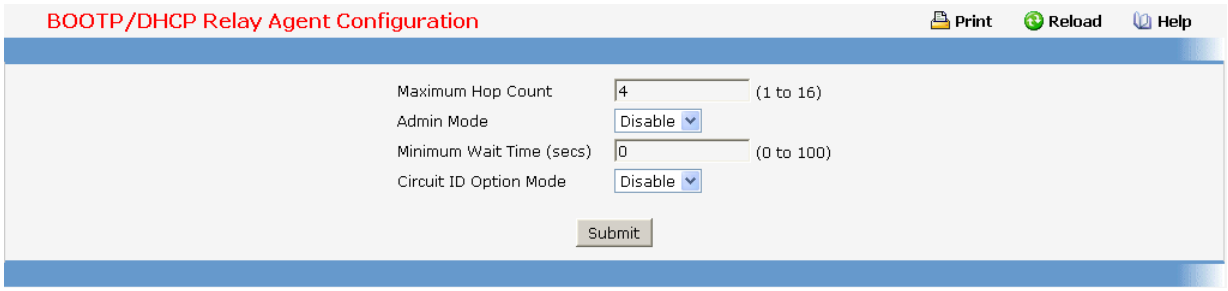
Distribute List - The Access List that filters the routes to be redistributed by the Destination Protocol. Display 0 when not configured.

Command Buttons

Refresh - Displays the latest OSPF Route Redistribution Configuration data.

11.4.4 Managing BOOTP/DHCP Relay Agent

11.4.4.1 Configuring BOOTP/DHCP Relay Agent



Configurable Data

Maximum Hop Count - Enter the maximum number of hops a client request can take before being discarded.

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.

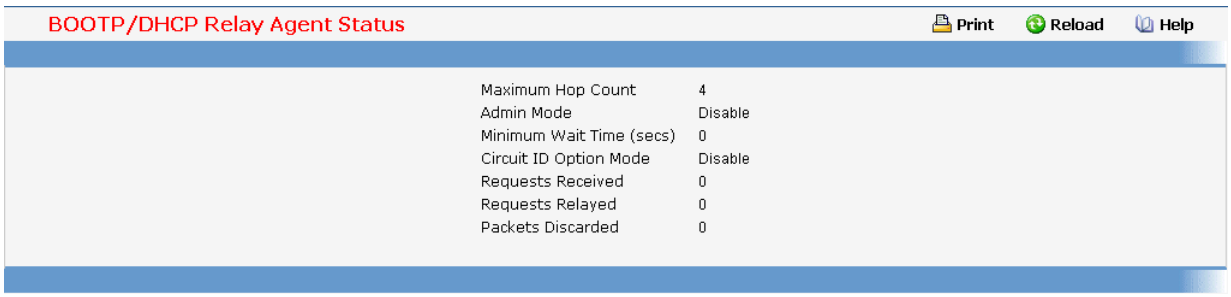
Minimum Wait Time (secs)- Enter a time in seconds. This value will be compared to the time stamp in the client's request packets, which should represent the time since the client was powered up. Packets will only be forwarded when the time stamp exceeds the minimum wait time.

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.

11.4.4.2 Viewing BOOTP/DHCP Relay Agent Status



Non-Configurable Data

Maximum Hop Count - The maximum number of Hops a client request can go without being discarded.

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 (secs) - 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.

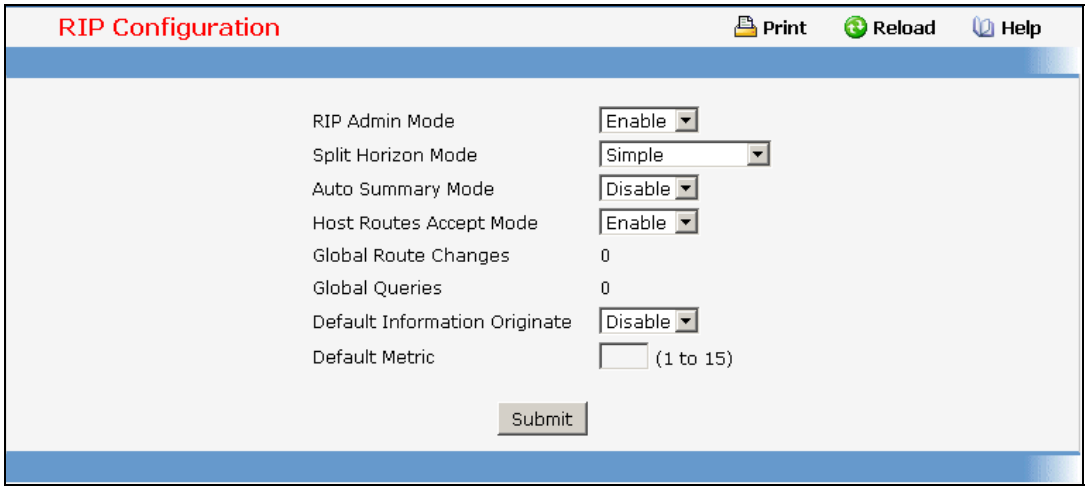
Requests Received - The total number of BOOTP/DHCP requests received from all clients since the last time the switch was reset.

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.

11.4.5 Managing Routing Information Protocol (RIP)

11.4.5.1 Configuring RIP Global Configuration Page



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 disabled.

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 disabled.

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 enabled.

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

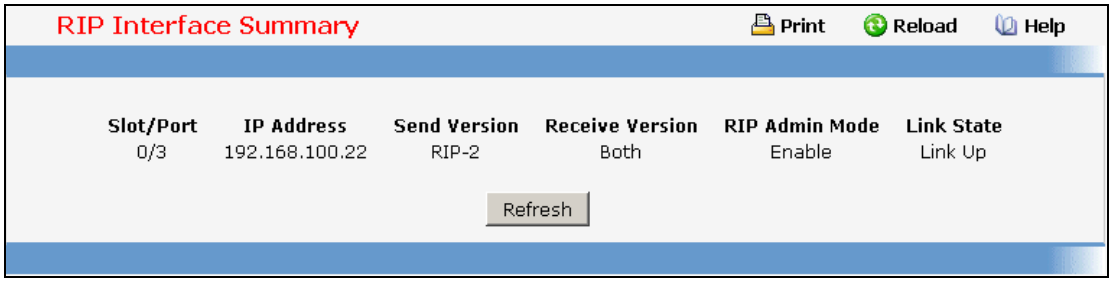
Global Route Changes - The number of route changes made to the IP Route Database by RIP. This does not include the refresh of a route's age.

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.

11.4.5.2 Viewing Each Routing Interface's RIP Configuration Page



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.

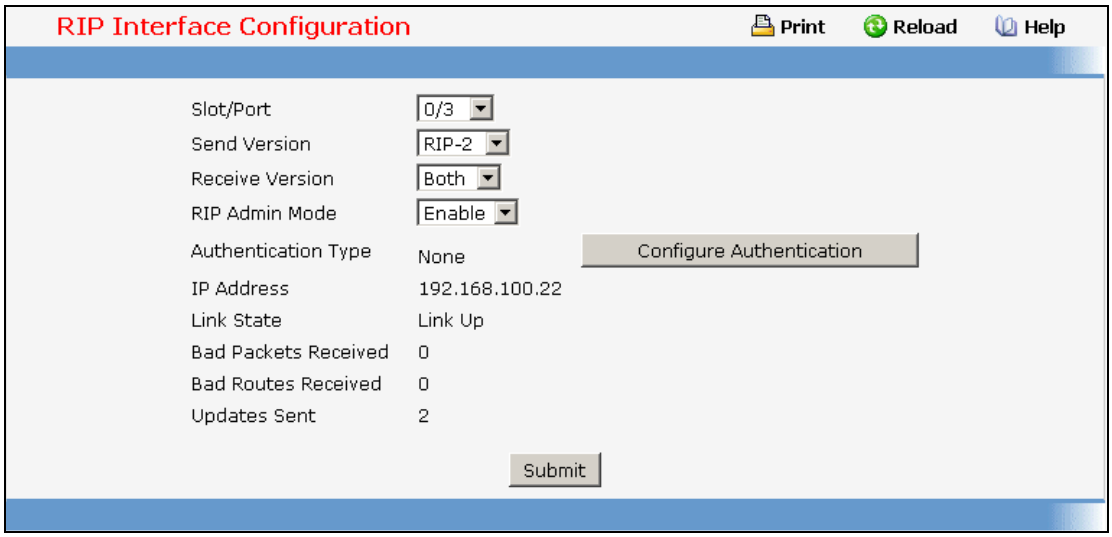
RIP Admin Mode - Whether RIP is enabled or disabled on the interface.

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.

11.4.5.3 Defining The Routing Interface's RIP Configuration Page



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 disabled.

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 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' 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.

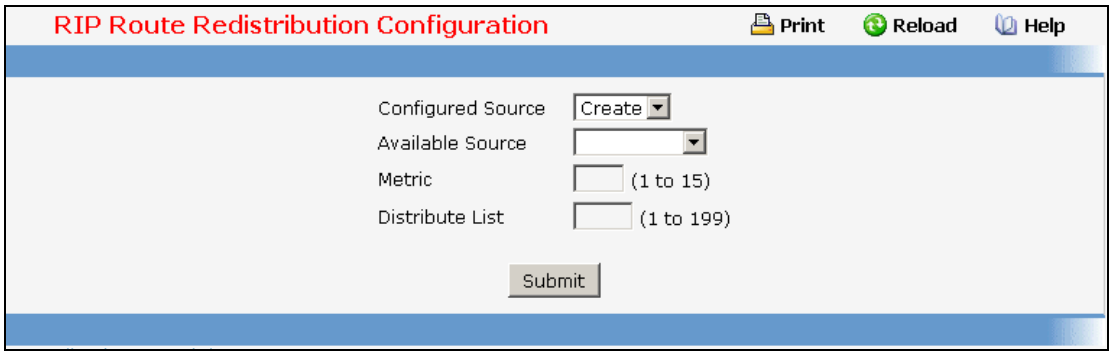
Command Buttons

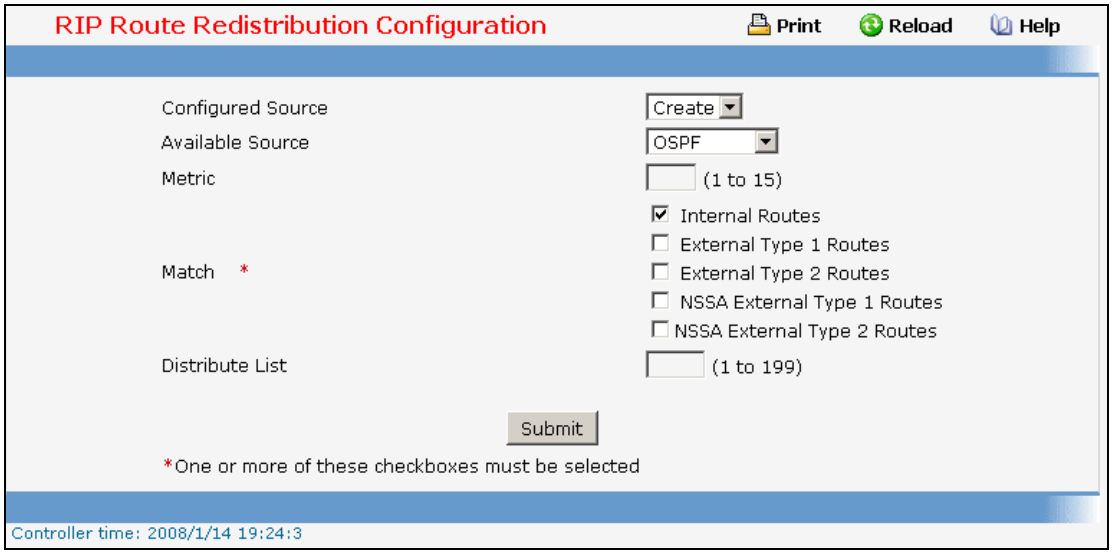
Configure Authentication - Display a new screen where you can select the authentication method for the virtual link.

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.

11.4.5.4 Configuring Route Redistribution Configuration

This screen can be used to configure the RIP Route Redistribution parameters. The allowable values for each field 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 'Static', 'Connected', 'OSPF' 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 RIP. This select box would appear only if the user selects "Create" option as Configured Source. The valid values are 'Static', 'Connected', and 'OSPF'.

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.

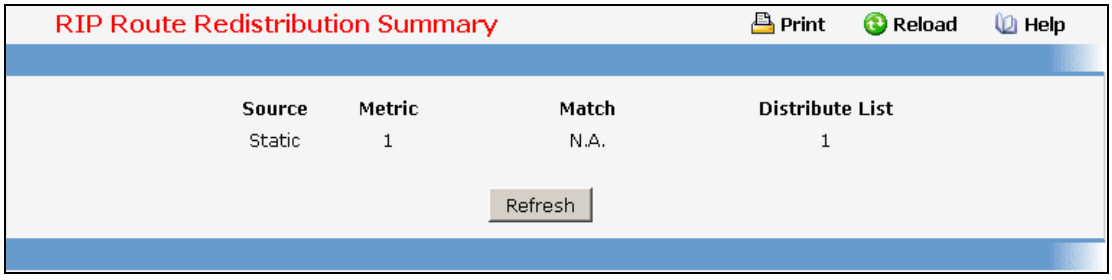
Command Buttons

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.

11.4.5.5 Viewing Route Redistribution Configuration

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

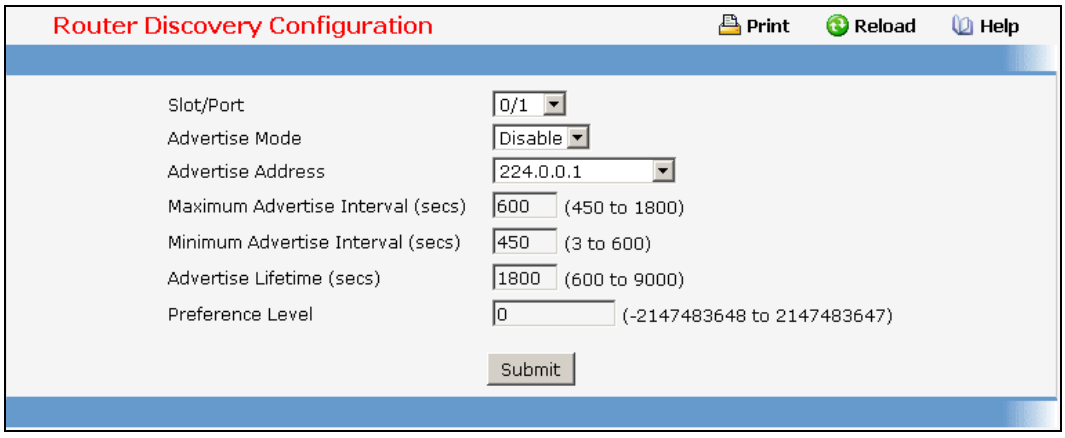
Distribute List - The Access List that filters the routes to be redistributed by the Destination Protocol. Displays 0 when not configured.

Command Buttons

Refresh - Displays the latest RIP Route Redistribution Configuration data.

11.4.6 Managing Router Discovery

11.4.6.1 Configuring Router Discovery



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 (secs) - Enter the maximum time (in seconds) allowed between router advertisements sent from the interface.

Minimum Advertise Interval (secs) - Enter the minimum time (in seconds) allowed between router advertisements sent from the interface.

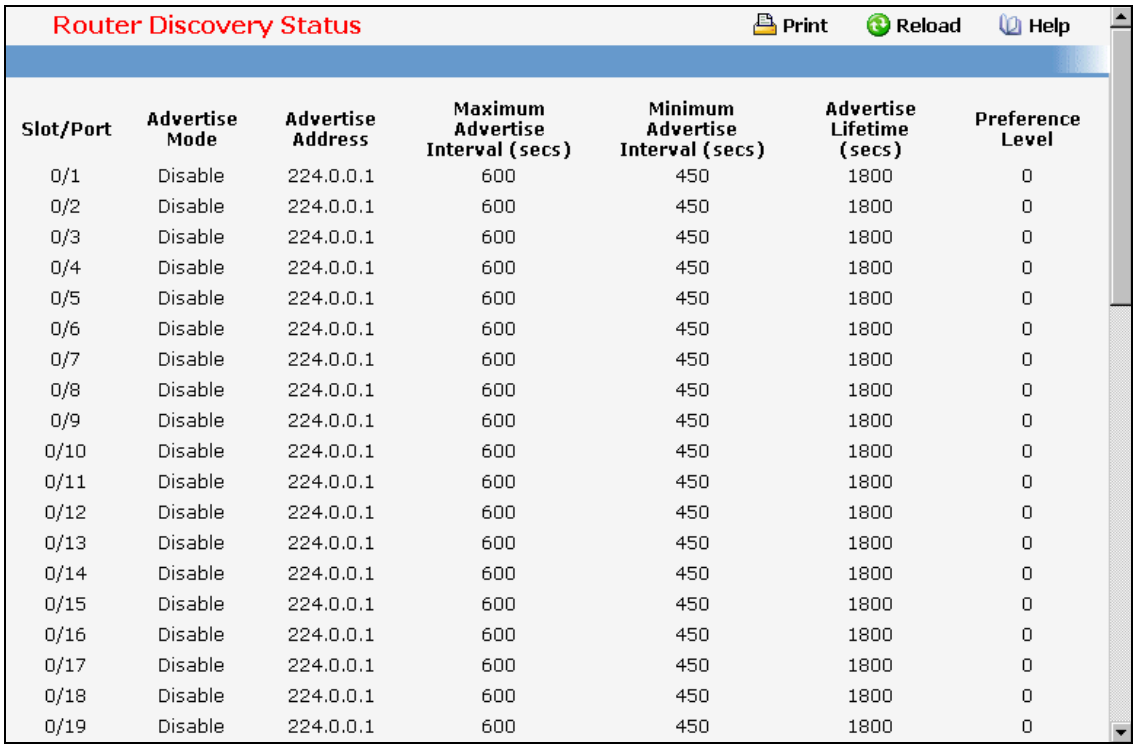
Advertise Lifetime (secs) - Enter the value (in seconds) to be used as the lifetime field in router advertisements sent from the interface. This is the maximum length of time that the advertised addresses are to be considered as valid router addresses by hosts.

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.

11.4.6.2 Viewing Router Discovery Status



Router Discovery Status

Print Reload Help

Slot/Port	Advertise Mode	Advertise Address	Maximum Advertise Interval (secs)	Minimum Advertise Interval (secs)	Advertise Lifetime (secs)	Preference Level
0/1	Disable	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
0/10	Disable	224.0.0.1	600	450	1800	0
0/11	Disable	224.0.0.1	600	450	1800	0
0/12	Disable	224.0.0.1	600	450	1800	0
0/13	Disable	224.0.0.1	600	450	1800	0
0/14	Disable	224.0.0.1	600	450	1800	0
0/15	Disable	224.0.0.1	600	450	1800	0
0/16	Disable	224.0.0.1	600	450	1800	0
0/17	Disable	224.0.0.1	600	450	1800	0
0/18	Disable	224.0.0.1	600	450	1800	0
0/19	Disable	224.0.0.1	600	450	1800	0

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 (secs) - The maximum time (in seconds) allowed between router advertisements sent from the interface.

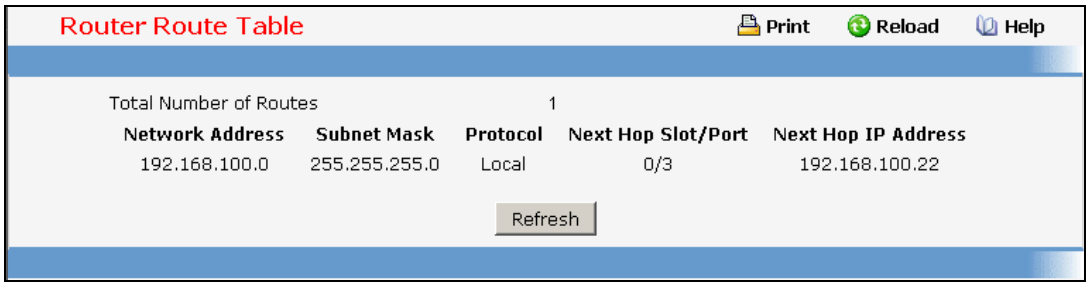
Minimum Advertise Interval (secs) - The minimum time (in seconds) allowed between router advertisements sent from the interface.

Advertise Lifetime (secs) - 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.

11.4.7 Managing Route Table

11.4.7.1 Viewing 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

Next Hop Slot/Port - The outgoing router interface to use when forwarding traffic to the destination.

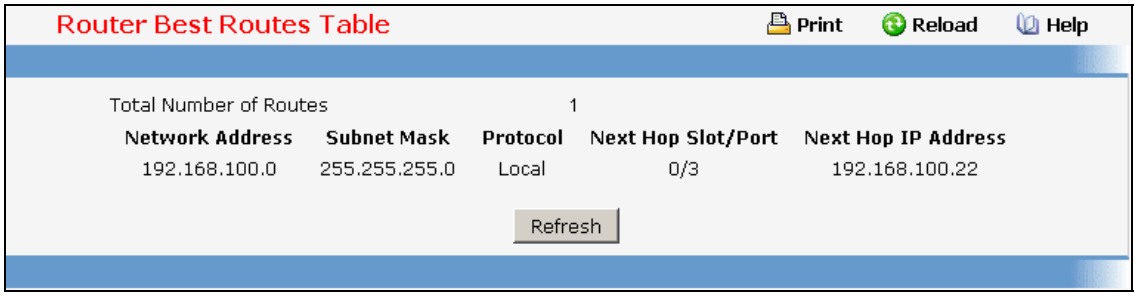
Next Hop IP Address - The outgoing router IP address to use when forwarding traffic to the next router (if any) in the path towards the destination. The next router will always be one of the adjacent neighbors or the IP address of the local interface for a directly attached network.

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.

11.4.7.2 Viewing Router Best 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

Next Hop Slot/Port - The outgoing router interface to use when forwarding traffic to the destination.

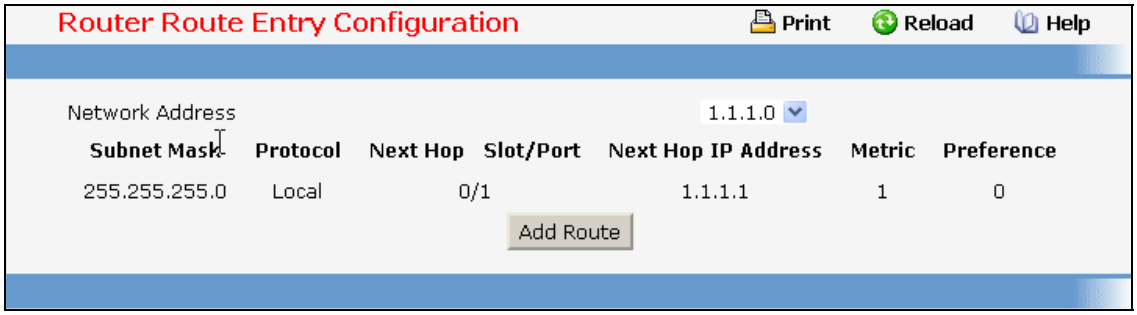
Next Hop IP Address - The outgoing router IP address to use when forwarding traffic to the next router (if any) in the path towards the destination. The next router will always be one of the adjacent neighbors or the IP address of the local interface for a directly attached network.

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.

11.4.7.3 Configuring Router Static Route Entry



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.

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

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.

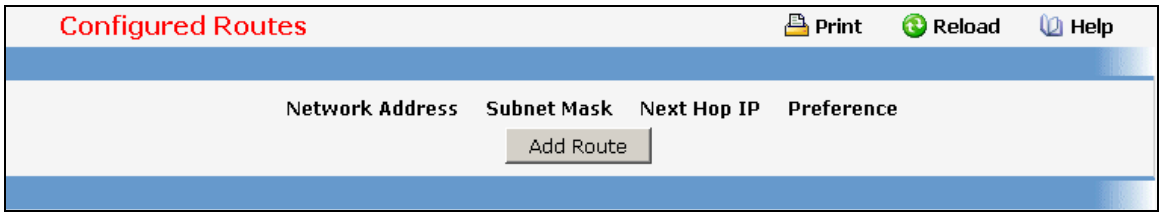
Metric - Administrative cost of the path to the destination. If no value is entered, default is 1. The range is 0 - 255.

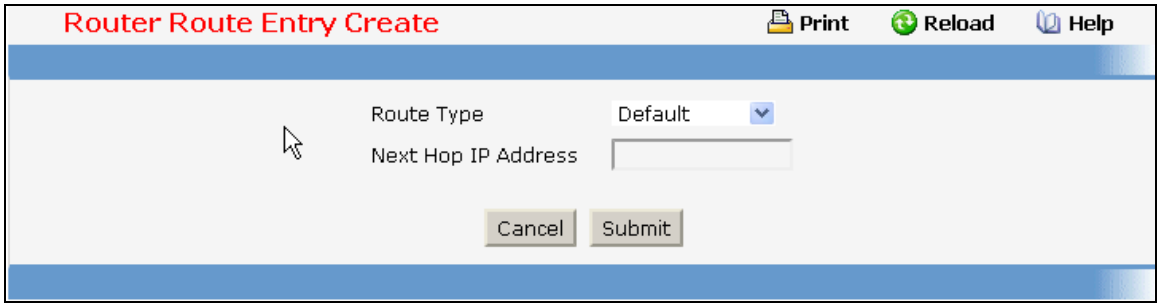
Preference – Specifies a preference value for the configured next hop.

Command Buttons

Add Route - Go to a separate page where a route can be created.

11.4.7.4 Configuring (Static) Routes Entry





Selection Criteria

Route Type - This field can be either default or static or static reject. 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

Network Address - The IP route prefix for the destination.

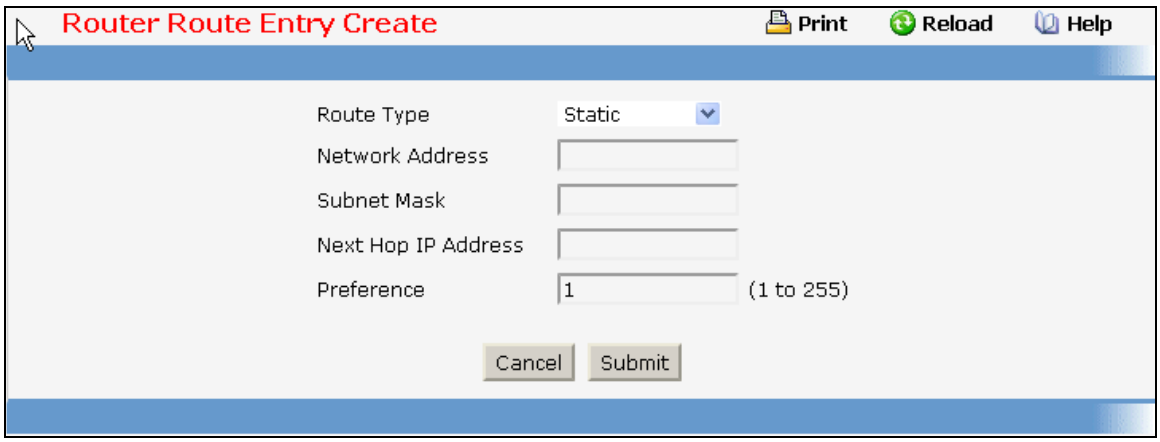
Subnet Mask - Also referred to as the subnet/network mask, this indicates the portion of the IP interface address that identifies the attached network.

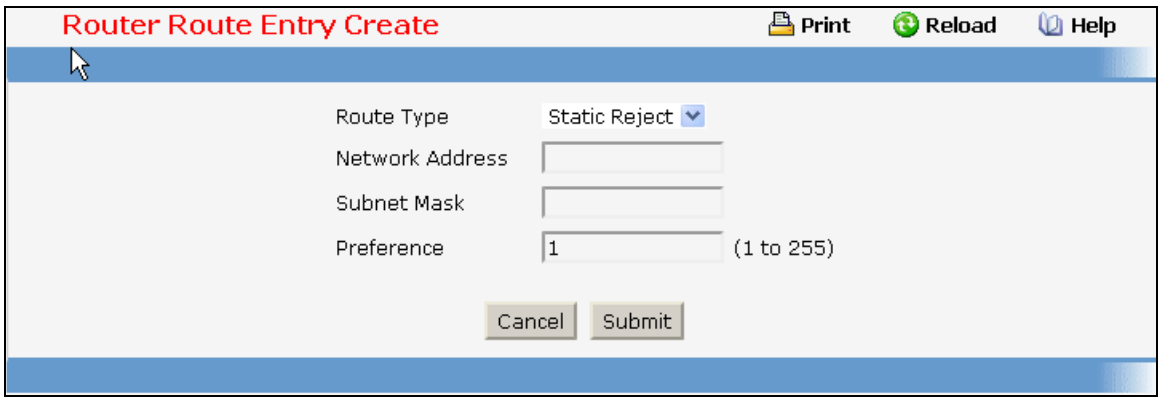
Next Hop IP Address - The outgoing router IP address to use when forwarding traffic to the next router (if any) in the path towards the destination. The next router will always be one of the adjacent neighbors or the IP address of the local interface for a directly attached network.

Preference - Specifies a preference value for the configured next hop.

Command Buttons

Add Route - Go to a separate page where a route can be created.

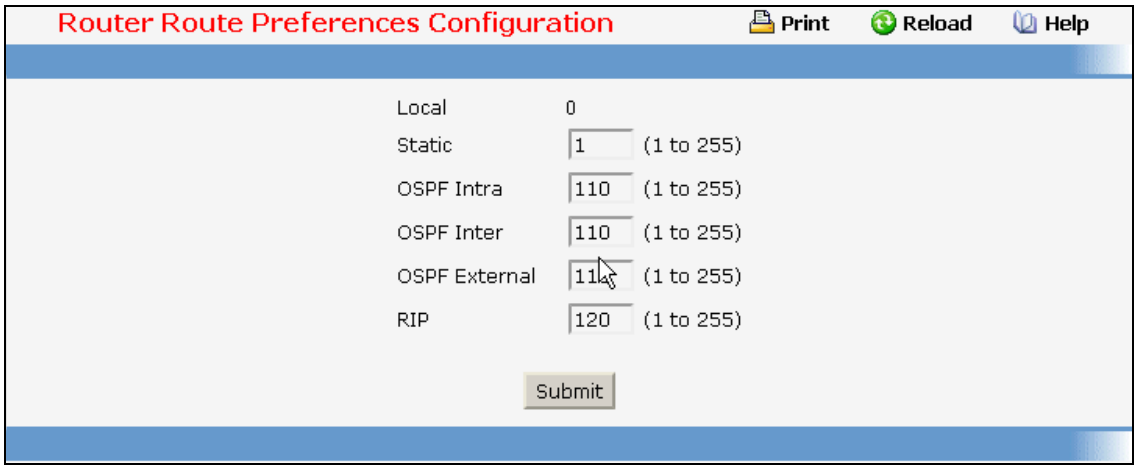




11.4.7.5 Configuring Router Route Preference

Use the Route Preferences Configuration page to configure the default preference for each protocol. These values arearbitrary values that range from 1 to 255, and are independent of route metrics. Most routing protocols use a route metric todetermine the shortest path known to the protocol, independent of any other protocol. Routes with a preference of 255 arenot used for forwarding.

The best route to a destination is chosen by selecting the route with the lowest preference value. When there are multipleroutes to a destination, the preference values are used to determine the preferred route.



Configurable Data

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 110. 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 110. 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 External - The OSPF External route preference value in the router. The default value is 110. 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 120. The range is 1 to 255.

Non-Configurable Data

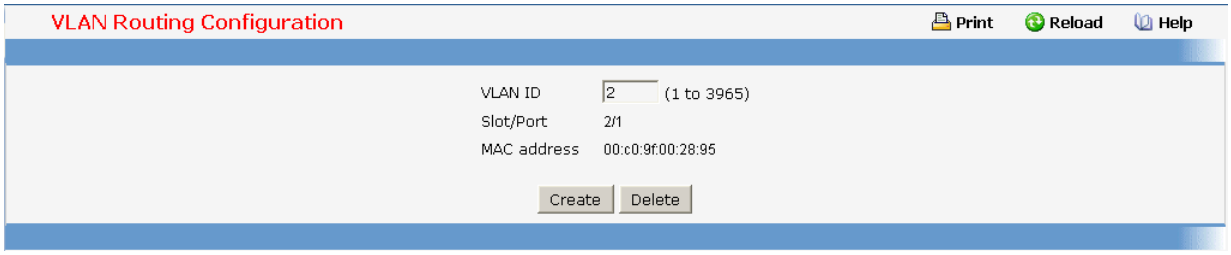
Local - This field displays the local route preference value.

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.

11.4.8 Managing VLAN Routing

11.4.8.1 Configuring VLAN Routing



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.

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.

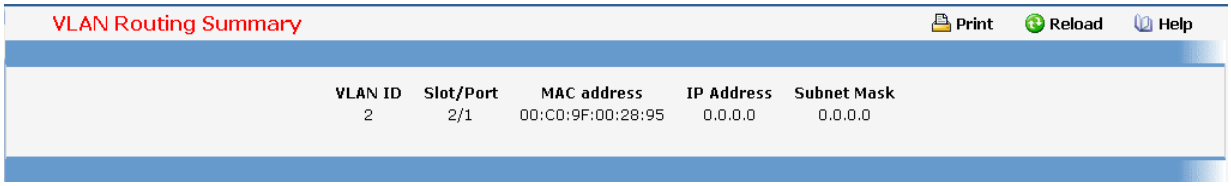
Delete - Remove the VLAN Routing Interface specified in the *VLAN ID input field* from the router configuration.

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.

11.4.8.2 Viewing VLAN Routing Summary Information



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

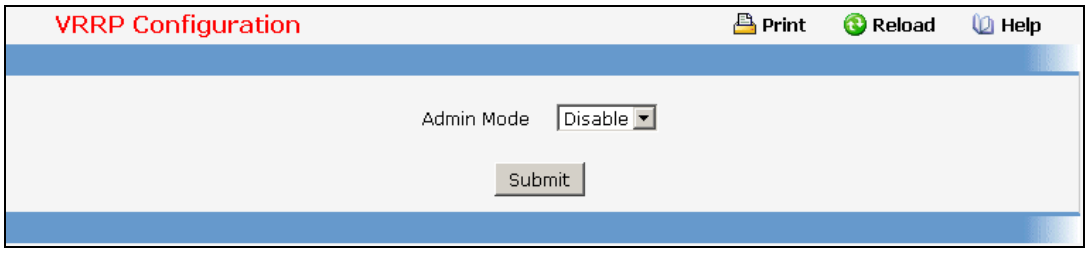
MAC Address - The MAC Address assigned to the VLAN Routing Interface

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.

11.4.9 Managing VRRP

11.4.9.1 Configuring VRRP



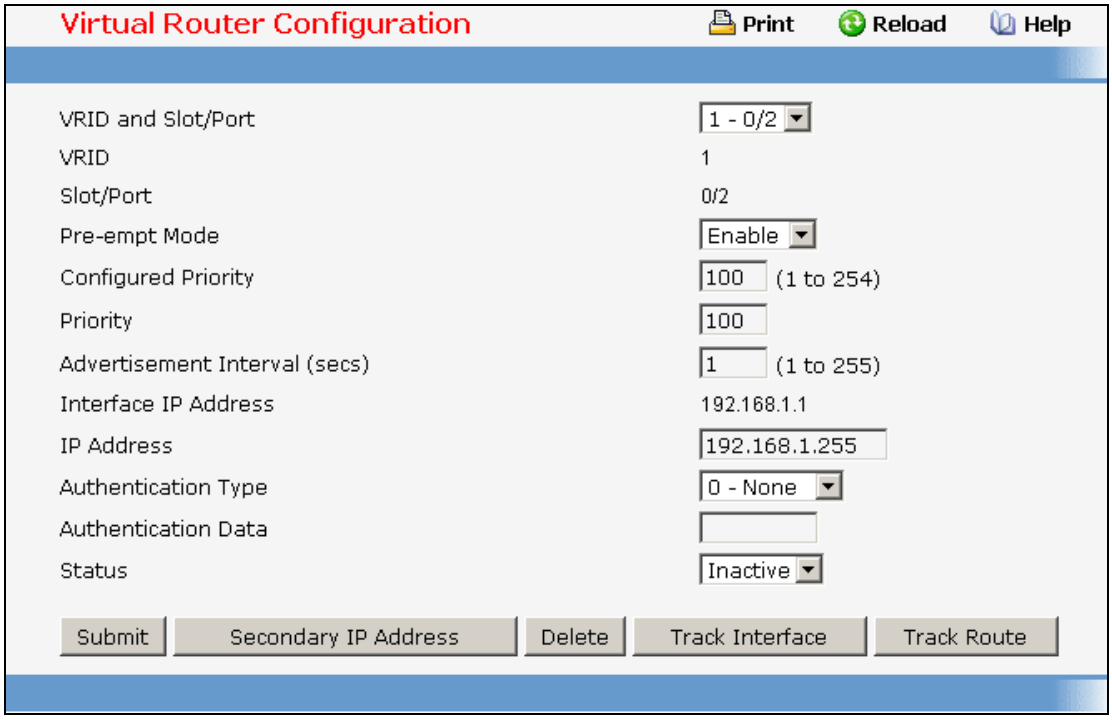
Configurable Data

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.

11.4.9.2 Configuring Virtual Router



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 (secs) - 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-Key - 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.

Priority - This is the operational priority of the VRRP router. This is relative to the configured priority. The operational priority is depending upon the configured priority and the priority decrements configured through tracking procss.

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.

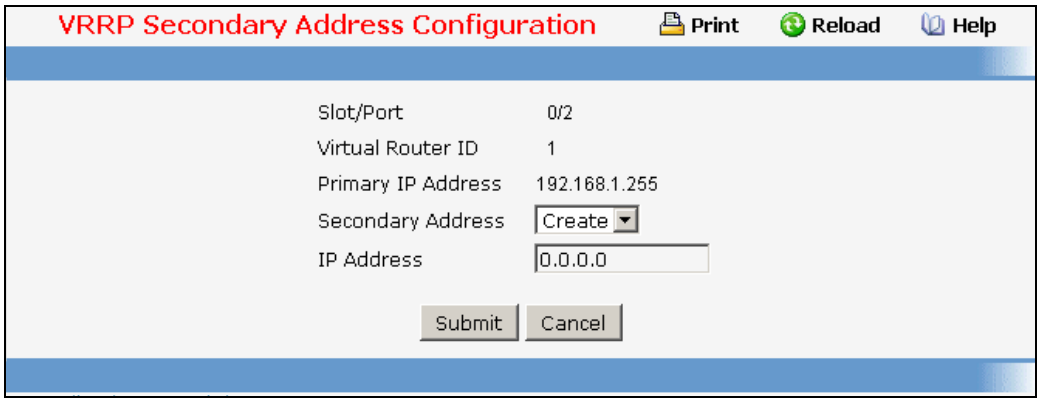
Delete - Delete the selected Virtual Router. Note that the router can not be deleted if there are secondary addresses configured.

Secondary IP Address - Proceed to the Secondary IP Address configuration screen.

Track Interface - Proceed to the VRRP Track interface configuration screen.

Track Route - Proceed to the VRRP Track Route configuration screen.

11.4.9.3 Configuring VRRP Secondary Address



Selection Criteria

Secondary Address - he 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.

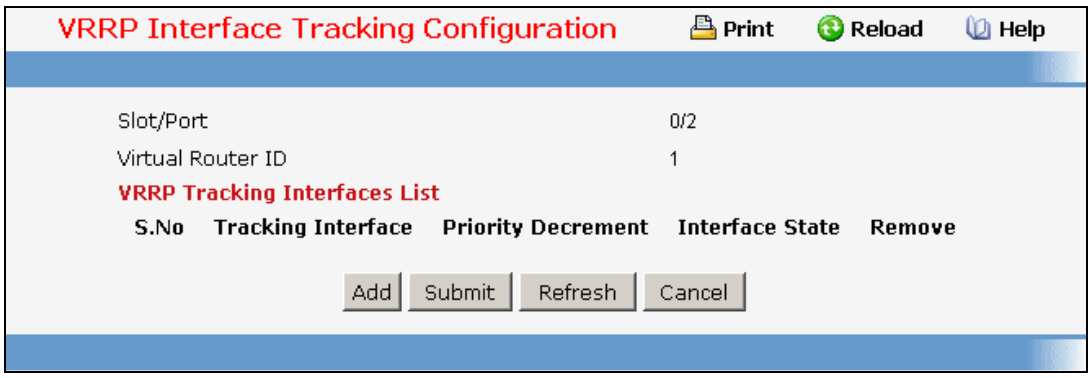
Command Buttons

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.

11.4.9.4 Configuring VRRP Interface Tracking



Configurable Data

Priority Decrement - The priority decrement for the tracked interface. The valid range is 1 -254. default value is 10.

Remove - Removes the selected Tracking interface from the VRRP tracked list.

Non-Configurable Data

Slot/Port - The interface for which data is to be displayed.

Virtual Router ID - The Virtual Router ID for which data is to be displayed.

S.No - The serial number for this row.

Tracking Interface - The Tracked interface for which data is to be displayed or configured.

Interface State - The IP state of the tracked interface.

Command Buttons

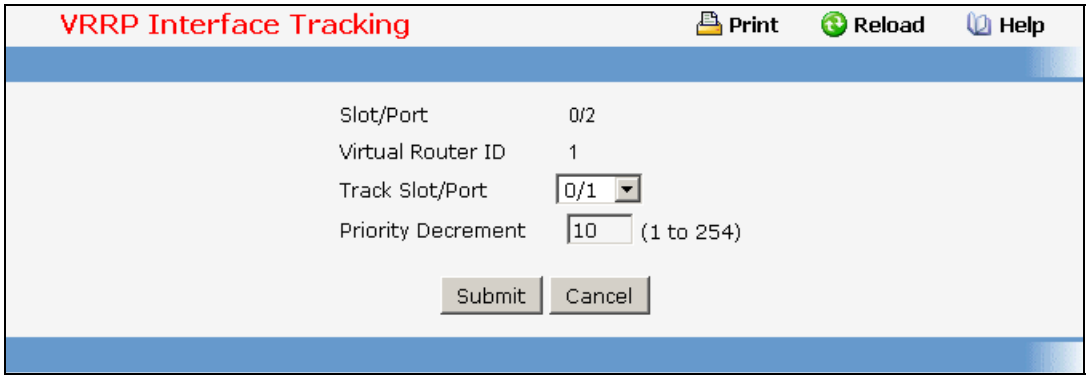
Add - Proceed to the VRRP Track interface screen.

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.

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

Cancel - Return to the Virtual Router Configuration screen.

11.4.9.5 Configuring VRRP Track Interface



Selection Criteria

Track Slot/Port - Displays all routing interface which are not yet tracked for this vrid and interface configuration. Exception to this loopback and tunnels could not be tracked.

Configurable Data

Priority Decrement - The priority decrement for the tracked interface. The valid range is 1 -254. default value is 10.

Non-Configurable Data

Slot/Port - The interface for which data is to be displayed.

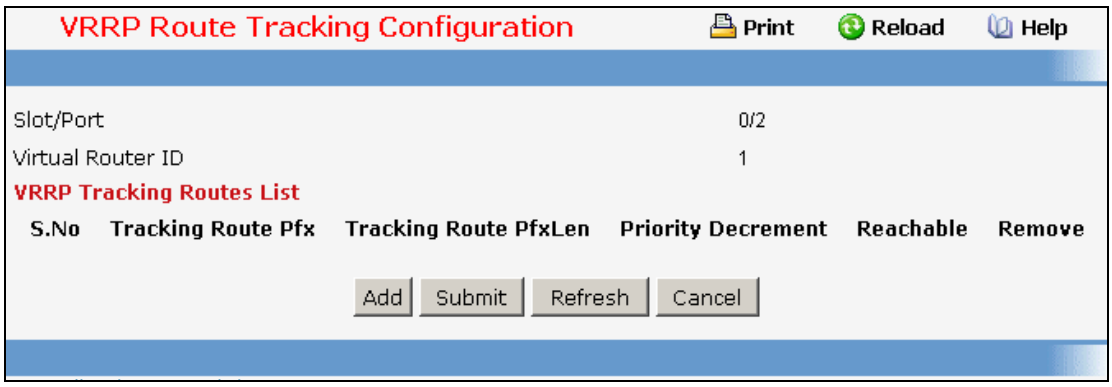
Virtual Router ID - The Virtual Router ID for which data is to be displayed.

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.

Cancel - Return to the VRRP Interface Tracking Configuration screen.

11.4.9.6 Configuring VRRP Route Tracking



Configurable Data

Priority Decrement - Enter the priority decrement for the tracked Route. The valid range is 1 -254. default value is 10.

Remove - Removes the selected Tracking Routes from the VRRP tracked list.

Non-Configurable Data

Slot/Port - The VRRP interface for which Tracking data is to be displayed.

Virtual Router ID - he Virtual Router ID for which Tracking data is to be displayed.

S.No - The serial number for this row.

Tracking Route Pfx - The Prefix of the tracked route.

Tracking Route PfxLen - The prefix length of the tracked route.

Reachable - The reachability of the tracked Route.

Command Buttons

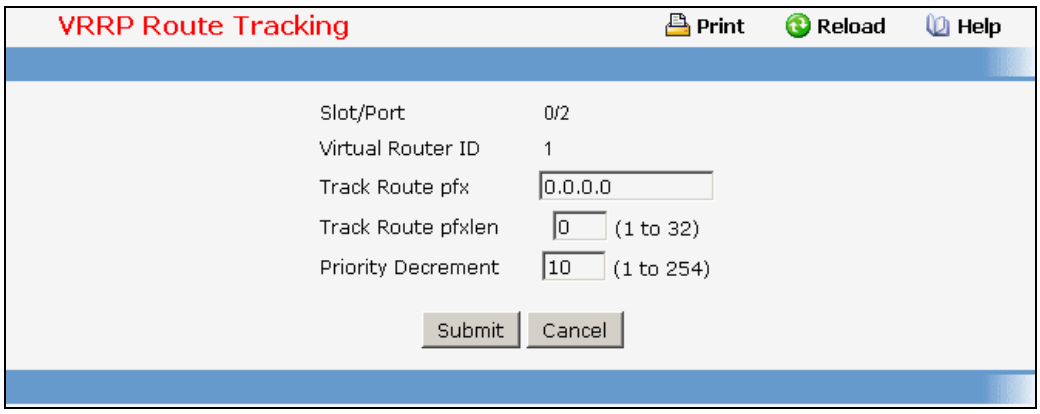
Add - Proceed to the VRRP Track Route screen.

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.

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

Cancel - Return to the Virtual Router Configuration screen.

11.4.9.7 Configuring VRRP Track Route



Configurable Data

Track Route Pfx - The Prefix of the route.

Track Route PfxLen - The prefix length of the route.

Priority Decrement - The priority decrement for the Route. The valid range is 1 -254. Default value is 10.

Non-Configurable Data

Slot/Port - The interface for which data is to be displayed.

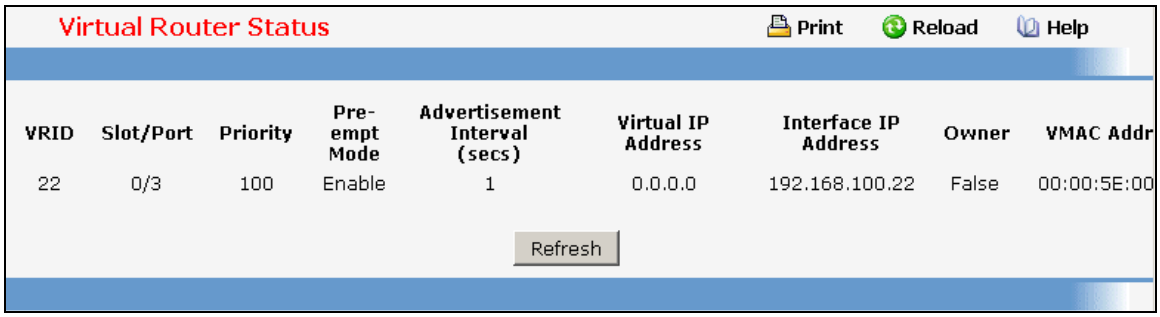
Virtual Router ID - The Virtual Router ID for which data is to be displayed.

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.

Cancel - Return to the VRRP Route Tracking Configuration screen.

11.4.9.8 Viewing Virtual Router 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 (secs) - 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:

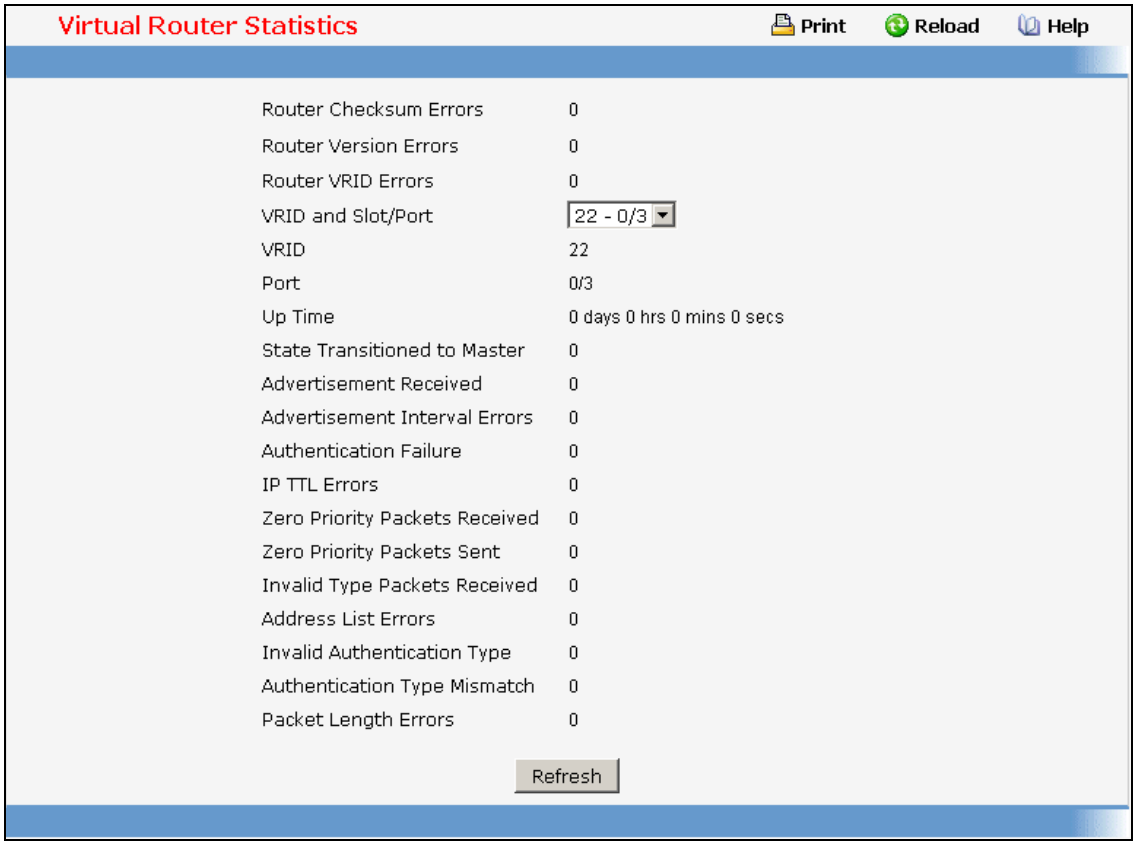
- Inactive
- Active

Secondary IP Address - The secondary IP address.

Command Buttons

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

11.4.9.9 Viewing 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.

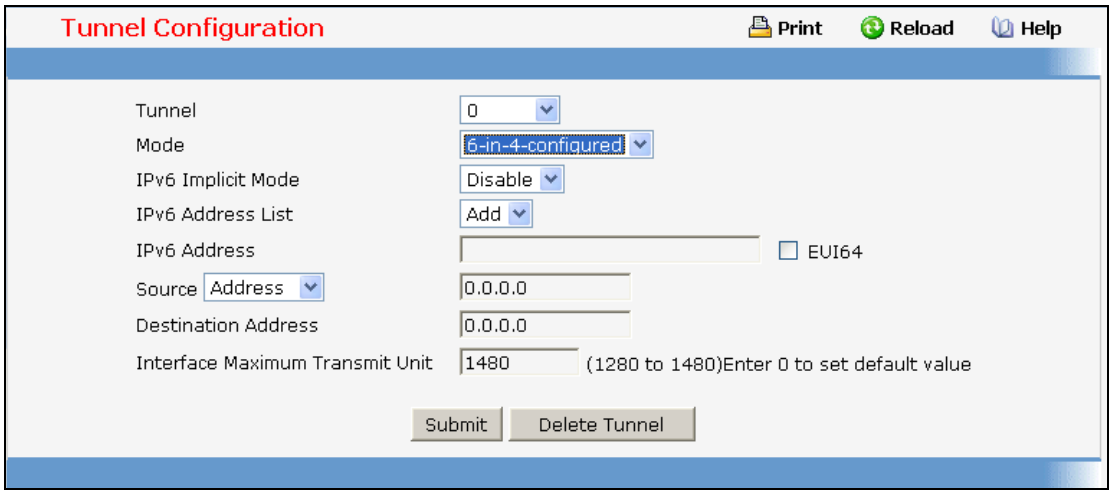
Command Buttons

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

11.4.10 Managing Tunnels

11.4.10.1 Configuring Tunnels Configuration Page

Tunnels can be created, configured and deleted from this page.



Configurable Data

Tunnel - Select list of currently configured tunnel interfaces. Create is also a valid choice if the maximum number of tunnel interfaces has not been created.

Tunnel ID - When 'Create' is chosen from the tunnel selector this list of available tunnel ID's becomes visible.

Mode - Selector for the Tunnel mode. The supported modes are 6-in-4-configured and 6-to-4.

IPv6 Implicit Mode - Enable IPv6 on this interface using the IPv6 address. This option is only configurable prior to specifying an explicit IPv6 address.

IPv6 Address - Select list of configured IPv6 addresses for the selected Loopback interface. Add is also a valid choice if the maximum number of addresses has not been configured.

IPv6 Address - When 'Add' is chosen from the IPv6 Address selector this IPv6 address input field becomes visible. Address must be entered in the format prefix/length.
The user also has the option to specify the 64-bit extended unique identifier (EUI-64).

Source - Select the desired source, Address or Interface. If Address is selected the the source address for this tunnel must be entered in dotted decimal notation. If Interface is selected the source interface for this tunnel must be selected. The address associated with the selected interface will be used as the source address.

Destination Address - The destination address for this tunnel in dotted decimal notation.

Interface Maximum Transmit Unit - Specifies maximum trasmit unit on an interface. It is not valid to set this value to 0 if routing is enabled. If the value set to 0 that will be changed to default value 1480. Range of MTU is (1280 to 1480)

Command Buttons

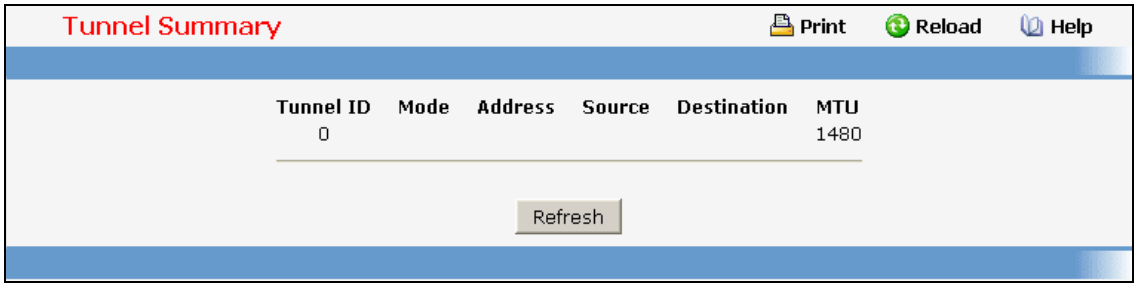
Submit - Update the system with the values on this screen.

Delete Tunnel - Remove the selected interface.

Delete Selected Address - Remove the selected IPv6 Address.

11.4.10.2 Viewing Tunnels Summary Page

This page displays a summary of the configured tunnels.



Non-Configurable Data

Tunnel ID - The Tunnel ID.

Mode - The corresponding mode of the Tunnel.

Address - The IPv6 Address(es) of the Tunnel.

Source - The corresponding Tunnel Source Address. In the case where an interface has been configured both the interface and the address are displayed. If the source interface has no address configured the text 'unconfigured' is displayed in place of the address.

Destination - The corresponding Tunnel Destination Address.

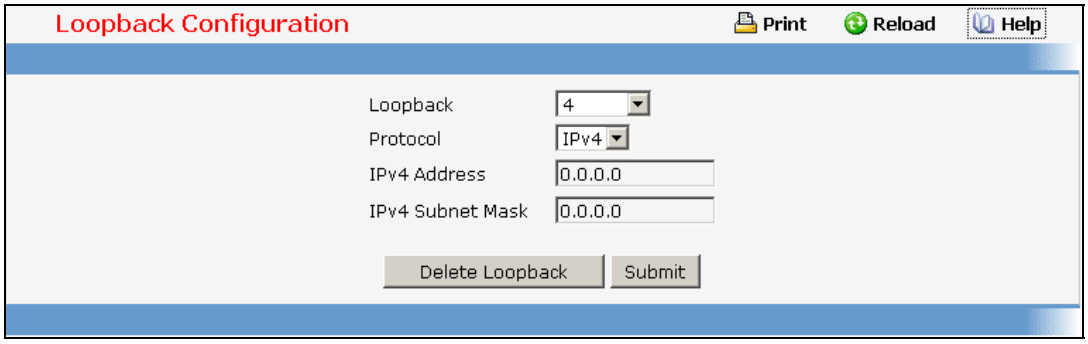
Command Buttons

Refresh - Refresh the page with the latest Tunnel entries.

11.4.11 Managing Loopbacks

11.4.11.1 Configuring Loopbacks Configuration Page

Loopback interfaces can be created, configured and removed on this page.



Configurable Data

Loopback - Select list of currently configured loopback interfaces. Create is also a valid choice if the maximum number of loopback interfaces has not been created.

Loopback ID - When 'Create' is chosen from the Loopback selector this list of available loopback ID's becomes visible.

Protocol - Select IPv4 or IPv6 to configure the corresponding attributes on the loopback interface.

IPv6 Mode - Enable IPv6 on this interface using the IPv6 address. This option is only configurable prior to specifying an explicit IPv6 address.

IPv6 Address - Select list of configured IPv6 addresses for the selected Loopback interface. Add is also a valid choice if the maximum number of addresses has not been configured.

IPv6 Address - When 'Add' is chosen from the IPv6 Address selector this IPv6 address input field becomes visible. Address must be entered in the format prefix/length.
The user also has the option to specify the 64-bit extended unique identifier (EUI-64).

IPv4 Address - The primary IPv4 address for this interface in dotted decimal notation.

IPv4 Subnet Mask - The primary IPv4 subnet mask for this interface in dotted decimal notation.

Secondary Address - Select list of configured IPv4 secondary addresses for the selected Loopback interface. Add Secondary is also a valid choice if the maximum number of secondary addresses has not been configured. A primary address must be configured before secondary addresses can be added.

Secondary IP Address - The secondary ip address for this interface in dotted decimal notation. This input field is visible only when 'Add Secondary' is selected.

Secondary Subnet Mask - The secondary subnet mask for this interface in dotted decimal notation. This input field is visible only when 'Add Secondary' is selected.

Command Buttons

Submit - Update the system with the values on this screen.

Delete Loopback - Remove the selected loopback interface.

Delete Primary - Remove the configured Primary IPv4 Address.

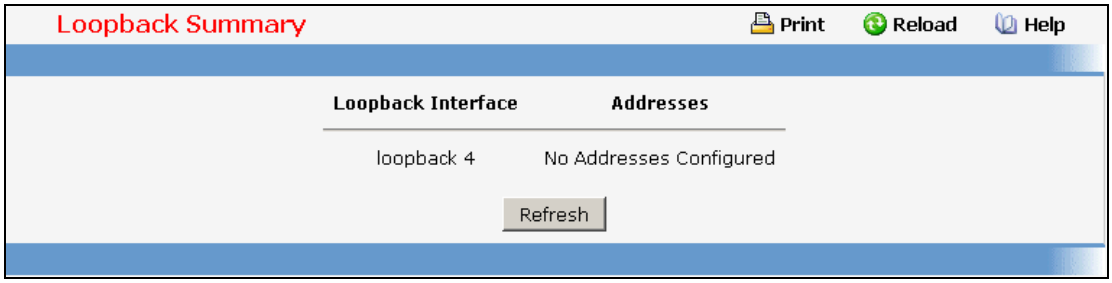
Add Secondary - Add the user specified Secondary IPv4 Address.

Delete Selected Secondary - Remove the selected Secondary IPv4 Address.

Delete Selected Address - Remove the selected IPv6 Address.

11.4.11.2 Viewing Loopbacks Summary Page

This page displays a summary of the configured Loopback interfaces.



Non-Configurable Data

Loopback Interface - The ID of the configured loopback interface.

Addresses - A list of the addresses configured on the loopback interface.

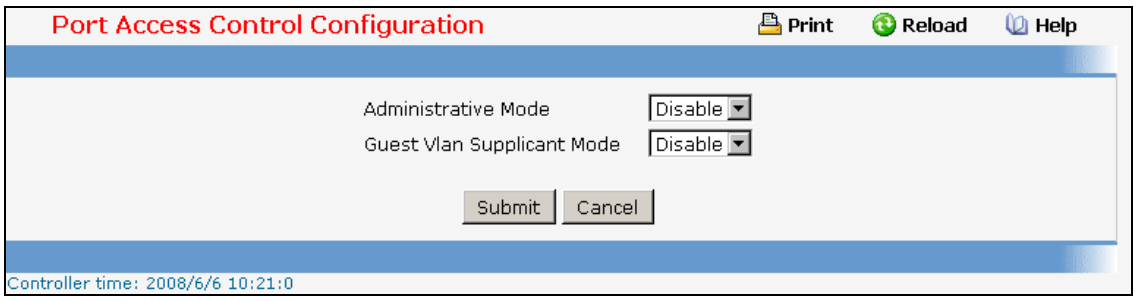
Command Buttons

Refresh - Refresh the page.

11.5 Security Menu

11.5.1 Managing Access Control (802.1x)

11.5.1.1 Defining Access Control Page



Configurable Data

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

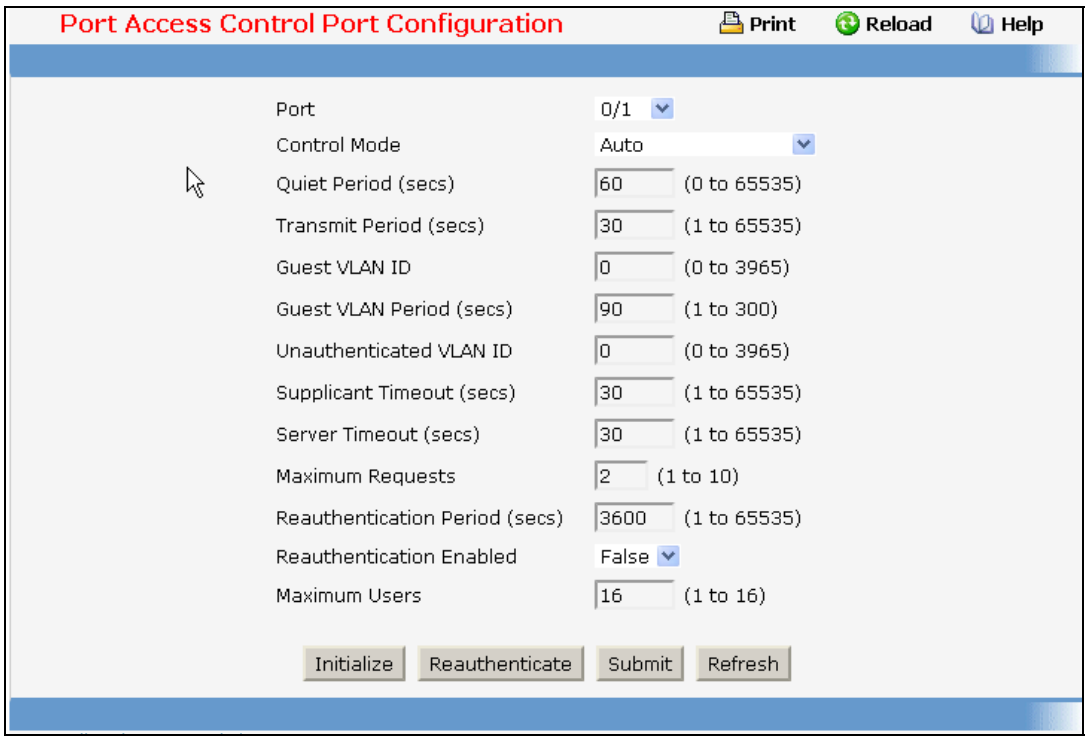
Guest Vlan Supplicant Mode - This selector lists the two options for Guest VLAN Supplicant mode: enable and disable. The default value is disabled.

Command Buttons

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

Cancel - This resets the page to display the administrative mode that is currently configured by the selected unit.

11.5.1.2 Configuring each Port Access Control Configuration Page



Selection Criteria

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.
- *mac based*: The authenticator PAE sets the controlled port mode to reflect the outcome of the authentication exchanges between the supplicant, authenticator, and the authentication server on a per supplicant basis.

Reauthentication Enabled - This 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.

Configurable Data

Quiet Period (secs)- 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 (secs)- 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 to 65535. The default value is 30. Changing the value will not change the configuration until the Submit button is pressed.

Guest VLAN Id (secs) - This field allows the user to configure Guest Vlan Id on the interface. The valid range is 0 - L7_PLATFORM_MAX_VLAN_ID.The default value is 0. Changing the value will not change the configuration until the Submit button is pressed. *Enter 0 to reset the Guest Vlan Id on the interface.*

Guest VLAN Period (secs) - This input field allows the user to enter the guest Vlan period for the selected port. The guest Vlan period is the value, in seconds, of the timer used by the GuestVlan Authentication. The guest Vlan timeout must be a value in the range of 1 and 300. The default value is 90. Changing the value will not change the configuration until the Submit button is pressed.

Supplicant Timeout (secs)- 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 to 65535. The default value is 30. Changing the value will not change the configuration until the Submit button is pressed.

Server Timeout (secs)- 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 to 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 to 10. The default value is 2. Changing the value will not change the configuration until the Submit button is pressed.

Reauthentication Period (secs)- 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 to 65535. The default value is 3600. Changing the value will not change the configuration until the Submit button is pressed.

Maximum Users - Defines the maximum number of clients that can get authenticated on the port in the MAC-based dot1x authentication mode. The range is 1 to 16. The default value is 16. Changing the value will not change the configuration until you click the Submit button.

Command Buttons

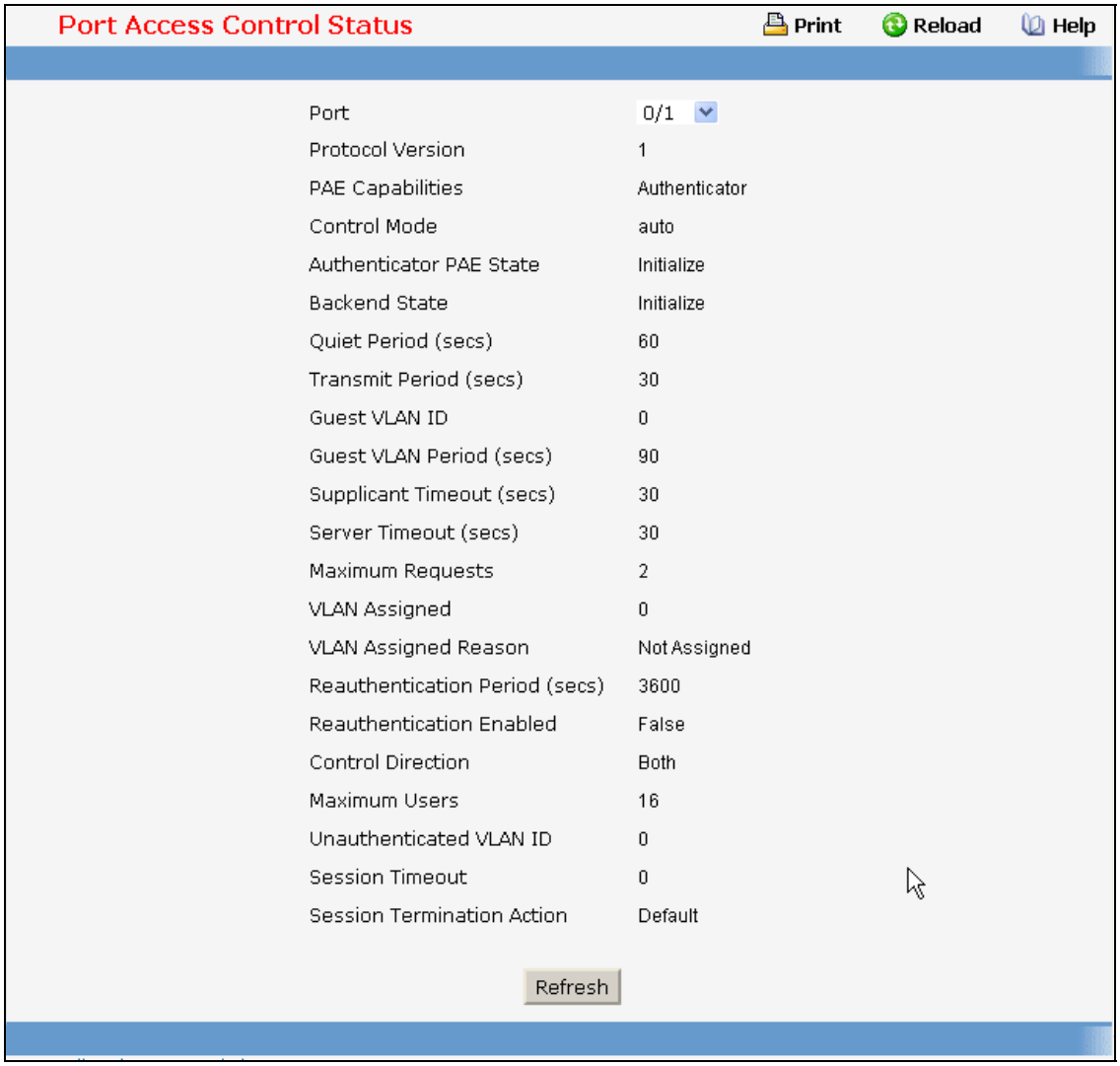
Initialize - This button begins the initialization sequence on the selected port. This button is only selectable if the control mode is 'auto'. If the button is not selectable, it will be grayed out. Once this button is pressed, the action is immediate. It is not required to press the Submit button for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

11.5.1.3 Viewing each Port Access Control Configuration Information Page



Selection Criteria

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.

Non-Configurable Data

Control Mode - Displays the configured control mode for the specified port. 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.

mac based: The authenticator PAE sets the controlled port mode to reflect the outcome of the authentication exchanges between the supplicant, authenticator, and the authentication server on a per supplicant basis.

Quiet Period(secs) - This field displays the configured quiet period for the selected port. This quiet period is 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 is a number in the range of 0 and 65535.

Transmit Period(secs) - This field displays the configured 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 is a number in the range of 1 to 65535.

Guest VLAN ID(secs) - This field displays the configured guest Vlan ID for the selected port. The guest Vlan ID is a value of 0 to 3965.

Guest VLAN Period(secs) - This field displays the configured guest Vlan period for the selected port. The guest Vlan period is the value, in seconds, of the timer used by the GuestVlan Authentication. The guest Vlan period is a number in the range of 1 and 300.

Supplicant Timeout(secs) - This field displays the configured 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 is a value in the range of 1 to 65535.

Server Timeout(secs) - This field displays the configured 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 is a value in the range of 1 to 65535.

Maximum Requests - This field displays the configured 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 is in the range of 1 to 10.

Reauthentication Period(secs) - This field displays the configured 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 is a value in the range of 1 to 65535.

Reauthentication Enabled - This field displays if reauthentication is enabled on the selected port. This is a configurable field. The possible values are 'true' and 'false'. If the value is 'true' reauthentication will occur. Otherwise, reauthentication will not be allowed.

Control Direction - This displays the control direction for the specified port. The control direction dictates the degree to which protocol exchanges take place between Supplicant and Authenticator. This affects whether the unauthorized controlled port exerts control over communication in both directions (disabling both incoming and outgoing frames) or just in the incoming direction (disabling only the reception of incoming frames). This field is not configurable on some platforms.

Protocol Version - This field displays the protocol version associated with the selected port. The only possible value is 1, corresponding to the first version of the 802.1x specification. This field is not configurable.

PAE Capabilities - This field displays the port access entity (PAE) functionality of the selected port. Possible values are "Authenticator" or "Supplicant". This field is not configurable.

Authenticator PAE State - This field displays the current state of the authenticator PAE state machine. Possible values are:

"Initialize"

"Disconnected"

"Connecting"

"Authenticating"

"Authenticated"

"Aborting"

"Held"

"ForceAuthorized"

"ForceUnauthorized".

Backend State - This field displays the current state of the backend authentication state machine. Possible values are:

"Request"

"Response"

"Success"

"Fail"

"Timeout"

"Initialize"

"Idle"

VLAN Assigned - Displays the VLAN ID assigned to the selected interface by the Authenticator. Note: This field is displayed only when the port control mode of the selected interface is not MAC-based.

VLAN Assigned Reason - Displays the reason for the VLAN ID assigned by the authenticator to the selected interface. Possible values are:

- Radius
- Unauth
- Default
- Not Assigned

Maximum Users - Displays the maximum number of clients that can get authenticated on the port in the MAC-based dot1x authentication mode. This field is configurable. The maximum users value is in range of 1 to 16.

Maximum Users - Displays the maximum number of clients that can get authenticated on the port in the MAC-based dot1x authentication mode. This field is configurable. The maximum users value is in range of 1 to 16.

Unauthenticated VLAN ID - Displays the Unauthenticated VLAN ID for the selected port. The valid range is 0 to 3965.

Session Timeout - Displays the Session Timeout set by the RADIUS Server for the selected port. Note: This field is displayed only when the port control mode of the selected port is not MAC-based.

Session Termination Action - Displays the Termination Action set by the RADIUS Server for the selected port. Possible values are:

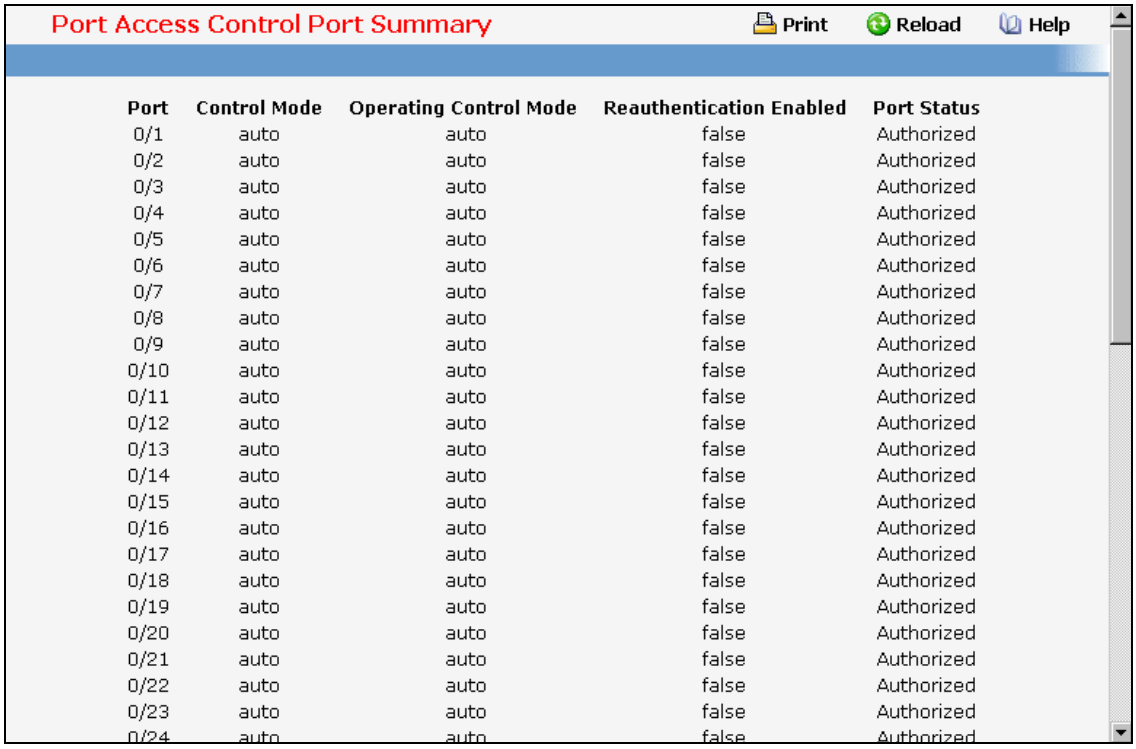
- Default
- Reauthenticate

If the termination action is Default then, at the end of the session, the client details are initialized. Otherwise, re-authentication is attempted. Note: This field is displayed only when the port control mode of the selected port is not MAC-based.

Command Buttons

Refresh - Update the information on the page.

11.5.1.4 Viewing Access Control Summary Page



Port	Control Mode	Operating Control Mode	Reauthentication Enabled	Port Status
0/1	auto	auto	false	Authorized
0/2	auto	auto	false	Authorized
0/3	auto	auto	false	Authorized
0/4	auto	auto	false	Authorized
0/5	auto	auto	false	Authorized
0/6	auto	auto	false	Authorized
0/7	auto	auto	false	Authorized
0/8	auto	auto	false	Authorized
0/9	auto	auto	false	Authorized
0/10	auto	auto	false	Authorized
0/11	auto	auto	false	Authorized
0/12	auto	auto	false	Authorized
0/13	auto	auto	false	Authorized
0/14	auto	auto	false	Authorized
0/15	auto	auto	false	Authorized
0/16	auto	auto	false	Authorized
0/17	auto	auto	false	Authorized
0/18	auto	auto	false	Authorized
0/19	auto	auto	false	Authorized
0/20	auto	auto	false	Authorized
0/21	auto	auto	false	Authorized
0/22	auto	auto	false	Authorized
0/23	auto	auto	false	Authorized
0/24	auto	auto	false	Authorized

Non-Configurable Data

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 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.
- *mac based*: The authenticator PAE sets the controlled port mode to reflect the outcome of the authentication exchanges between the supplicant, authenticator, and the authentication server on a per supplicant basis.

Operating Control Mode - This field indicates the control mode under which the port is actually operating. Possible values are:

- ForceUnauthorized
- ForceAuthorized
- Auto
- mac based

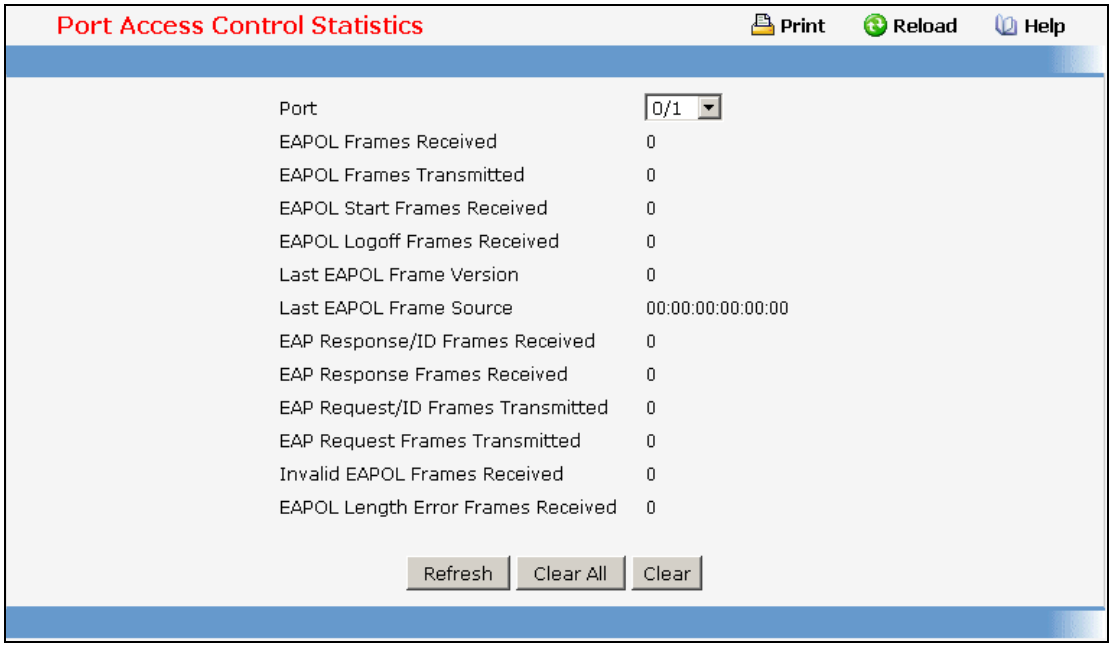
Reauthentication Enabled - This field shows whether reauthentication of the supplicant for the specified port is allowed. The possible values are 'true' and 'false'. If the value is 'true' reauthentication will occur. Otherwise, reauthentication will not be allowed.

Port Status - This field shows the authorization status of the specified port. The possible values are 'Authorized' and 'Unauthorized'.

Command Buttons

Refresh - Update the information on the page.

11.5.1.5 Viewing each Port Access Control Statistics Page



Selection Criteria

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.

Non-Configurable Data

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.

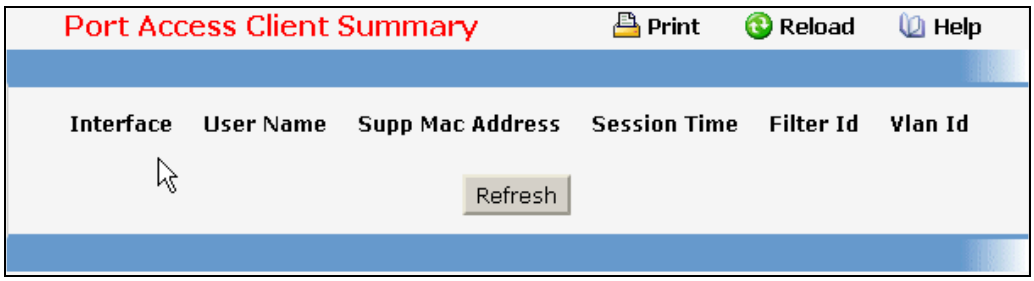
Command Buttons

Refresh - Update the information on the page.

Clear All - This button resets all statistics for all ports to 0. There is no confirmation prompt. When this button is pressed, the stats are immediately cleared.

Clear - This button resets the statistics for the selected port. There is no confirmation prompt. When this button is pressed, the stats are immediately cleared.

11.5.1.6 Defining Port Access Client Summary Page



Non-Configurable Data

Interface Displays - the interface address of the supplicant device.

User Name - Displays the user name representing the supplicant device.

Supp Mac Address - Displays the supplicant device's MAC address.

Session Time - Displays the time since the supplicant logged in. The value is in seconds.

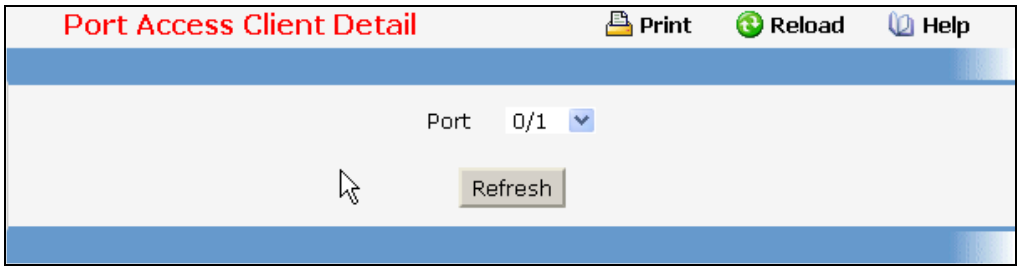
Filter ID - The policy filter ID assigned by the authenticator to the supplicant device.

VLAN ID - The VLAN ID assigned by the authenticator to the supplicant device.

Command Buttons

Refresh - Update the information on the page.

11.5.1.7 Defining Port Access Client Summary Page



Selection Criteria

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.

Non-Configurable Data

User Name - Displays the user name representing the supplicant device.

Supp Mac Address - Displays the supplicant device's MAC address.

Session Time - Displays the time since the supplicant logged in. The value is in seconds.

Filter ID - The policy filter ID assigned by the authenticator to the supplicant device.

VLAN ID - The VLAN ID assigned by the authenticator to the supplicant device.

VLAN Assigned Displays the reason for the VLAN ID assigned by the authenticator to the supplicant device.

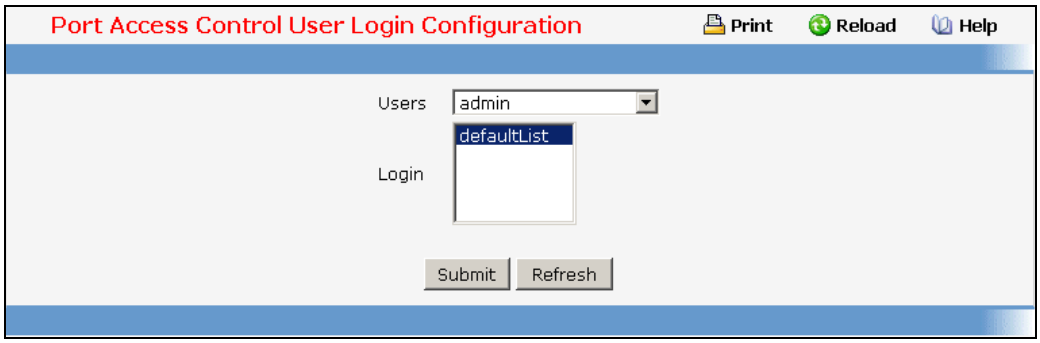
Session Timeout Displays the session timeout set by the radius server to the supplicant device.

Termination Action Displays the termination action set by the radius server to the supplicant device.

Command Buttons

Refresh - Update the information on the page.

11.5.1.8 Defining Access Control User Login Page



Selection Criteria

Users - Selects the user name that will use the selected login list for 802.1x port security.

Configurable Data

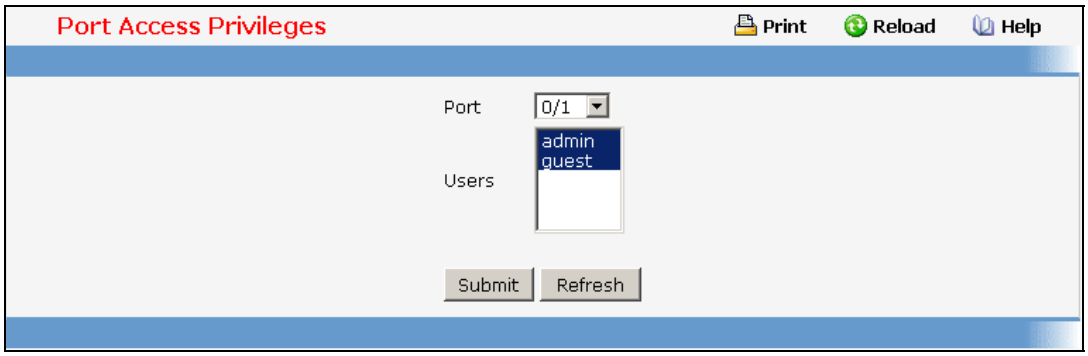
Login - Selects the login to apply to the specified user. All configured logins are displayed.

Command Buttons

Submit - Sends the updated screen to the switch and causes 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.

11.5.1.9 Defining each Port Access Privileges Page



Selection Criteria

Port - Selects the port to configure.

Configurable Data

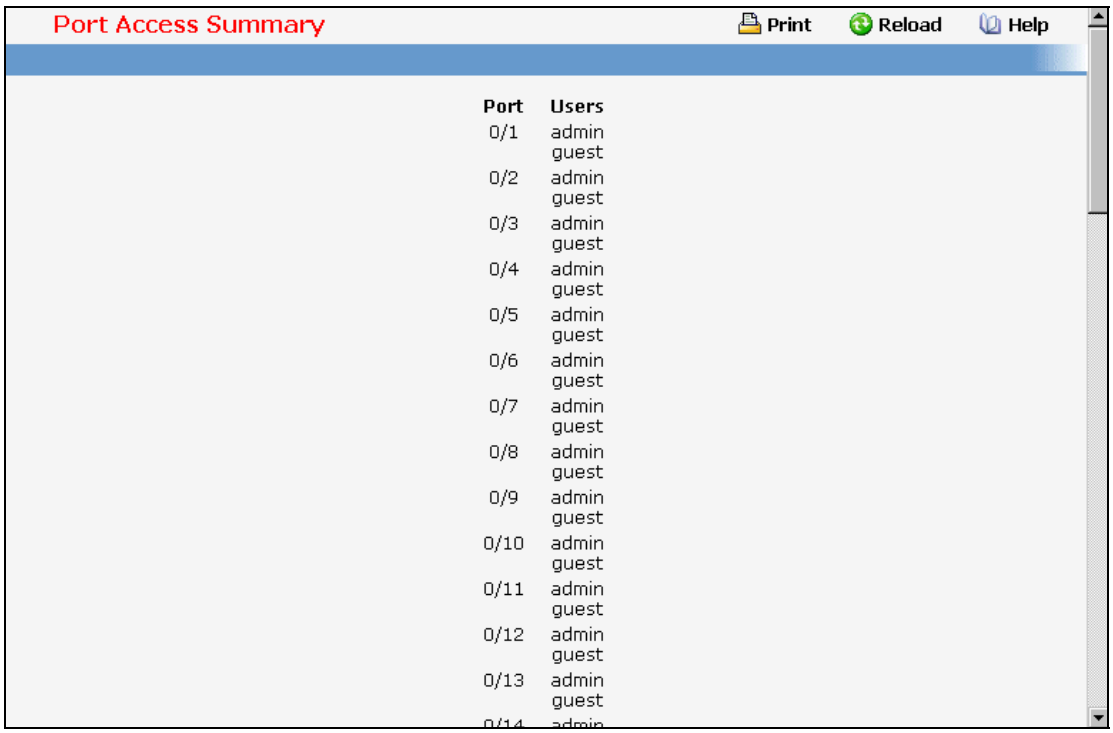
Users - Selects the users that have access to the specified port or ports.

Command Buttons

Submit - Sends the updated screen to the switch and causes 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.

11.5.1.10 Viewing each Port Access Privileges Summary Page



Non-Configurable Data

Port - Displays the port in Slot/Port format.

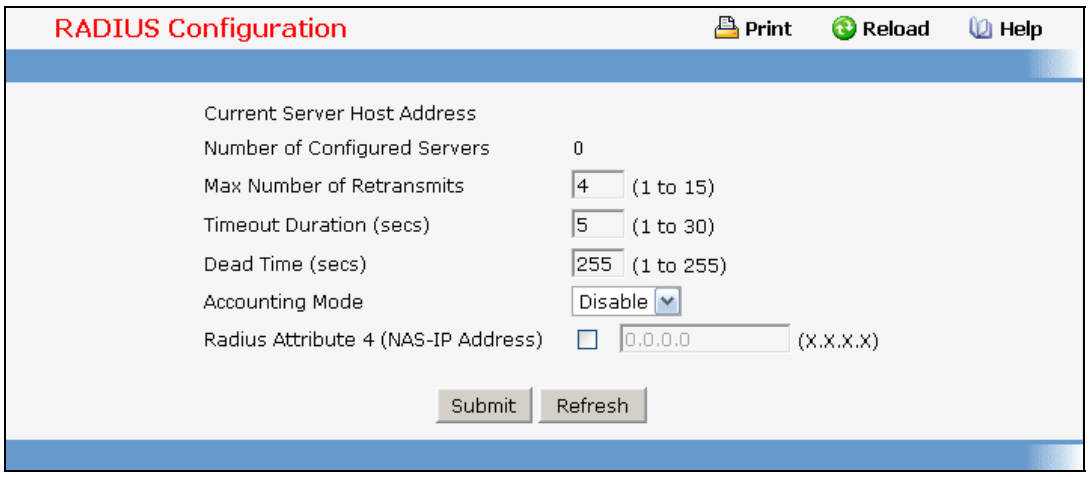
Users - Displays the users that have access to the port.

Command Buttons

Refresh - Update the information on the page.

11.5.2 Managing RADIUS

11.5.2.1 Configuring RADIUS Configuration Page



Selection Criteria

Accounting Mode - Selects if the RADIUS accounting mode is enabled or disabled.

Configurable Data

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.

Dead Time - The dead time value, in seconds. The valid range is 1 - 255. - Selects if the RADIUS accounting mode is enabled or disabled.

Radius Attribute 4 (NAS-IP Address) - Select if the Radius Attribute 4 (NAS-IP Address) inclusion in Radius Requests is enabled or disabled. Mention explicitly the IP address to be sent as NAS-IP Address to the Radius servers. If not mentioned, then the outgoing interface IP address that is used to send the packet to the Radius server is added as NAS-IP Address.

Non-Configurable Data

Current Server IP Address - The IP address of the current server. This field is blank if no servers are configured.

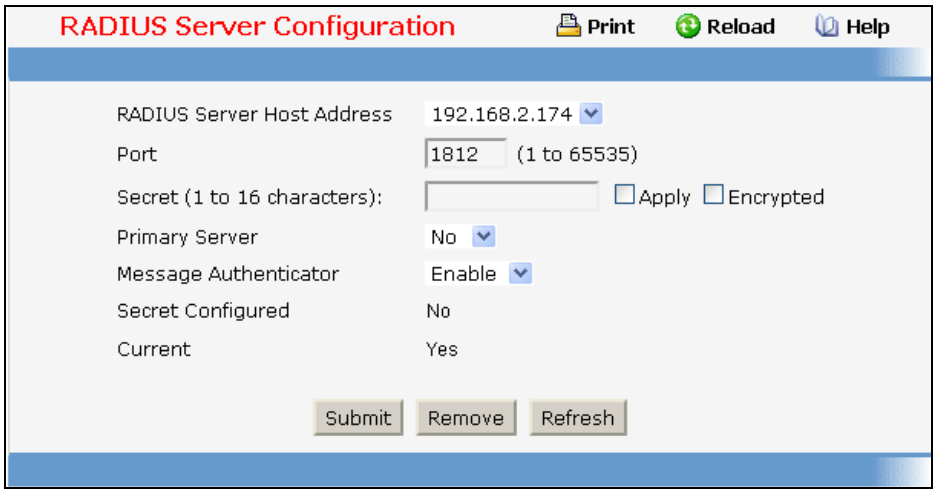
Number of Configured Servers - The number of RADIUS servers that have been configured. This value will be in the range of 0 and 3.

Command Buttons

Submit - Sends the updated screen to the switch and causes 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.

11.5.2.2 Configuring RADIUS Server Configuration Page



Selection Criteria

RADIUS Server IP Address - Selects the RADIUS server to be configured. Select add to add a server.

Primary Server - Sets the selected server to thePrimary or Secondary server.

Message Authenticator - Enable or disable the message authenticator attribute for the selected server.

Configurable Data

IP Address - The IP address of the server being added.

You cannot define these IP addresses:

0.0.0.0

255.255.255.255

224.xxx.xxx.xxx

127.0.0.1

Host Name -The host name 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.

Encrypted - When the secret string is encrypted, this box need to be checked. This field is only displayed if the user has READWRITE access.

Non-Configurable Data

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.

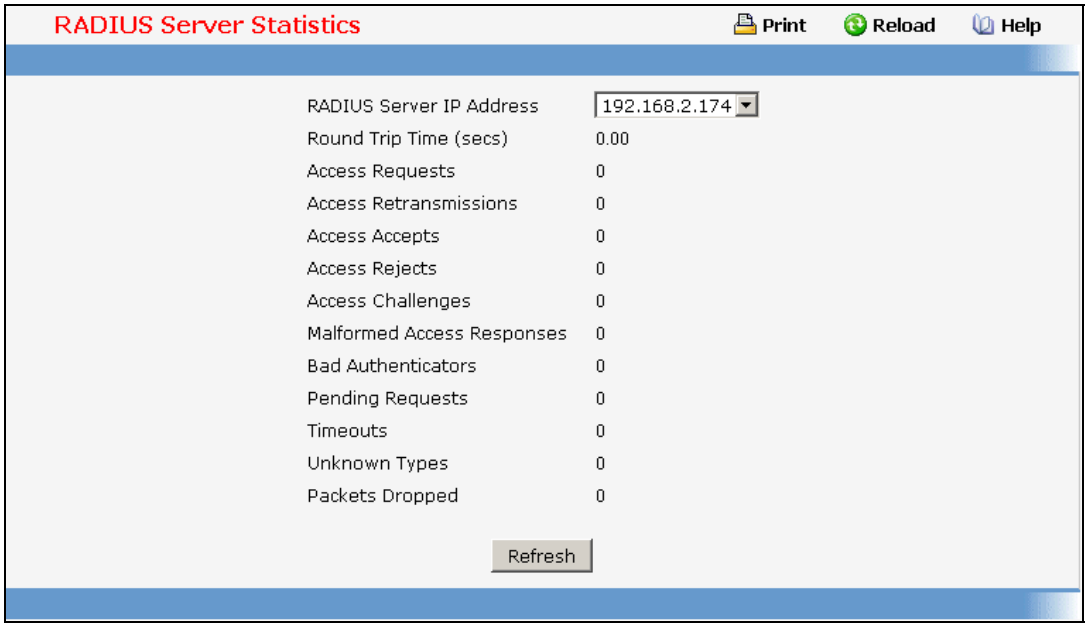
Command Buttons

Submit - Sends the updated screen to the switch and causes 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.

11.5.2.3 Viewing RADIUS Server Statistics Page



Selection Criteria

RADIUS Server IP Address - Selects the IP address of the RADIUS server for which to display statistics.

Non-Configurable Data

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.

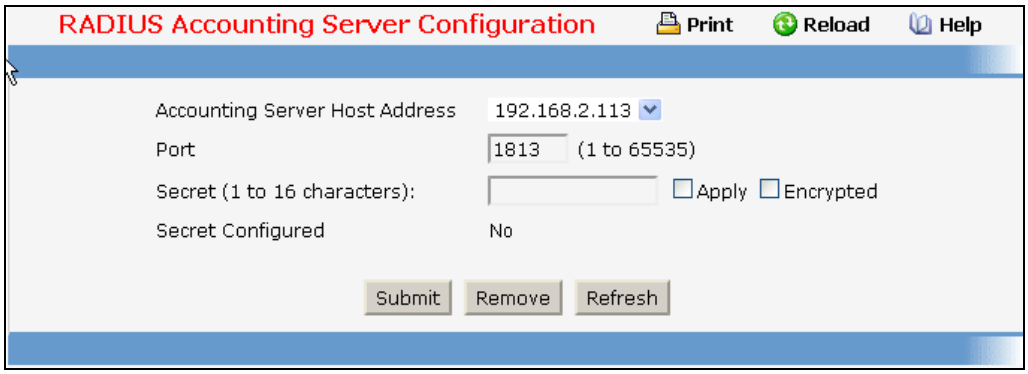
Unknown Types - The number of RADIUS packets of unknown type which were received from this server on the authentication port.

Packets Dropped - The number of RADIUS packets received from this server on the authentication port and dropped for some other reason.

Command Buttons

Refresh - Update the information on the page.

11.5.2.4 Defining RADIUS Accounting Server Configuration Page



Selection Criteria

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.

Configurable Data

IP Address - The IP address of the accounting server to add. This field is only configurable if the add item is selected.

You cannot define these IP addresses:

0.0.0.0

255.255.255.255

224.xxx.xxx.xxx

127.0.0.1

Host name - Enter the host name of the station.

Port - Specifies 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 specified 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.

Encrypted - When the secret string is encrypted, this box need to be checked. This field is only displayed if the user has READWRITE access.

Non-Configurable Data

Secret Configured - Indicates if the secret has been configured for this accounting server.

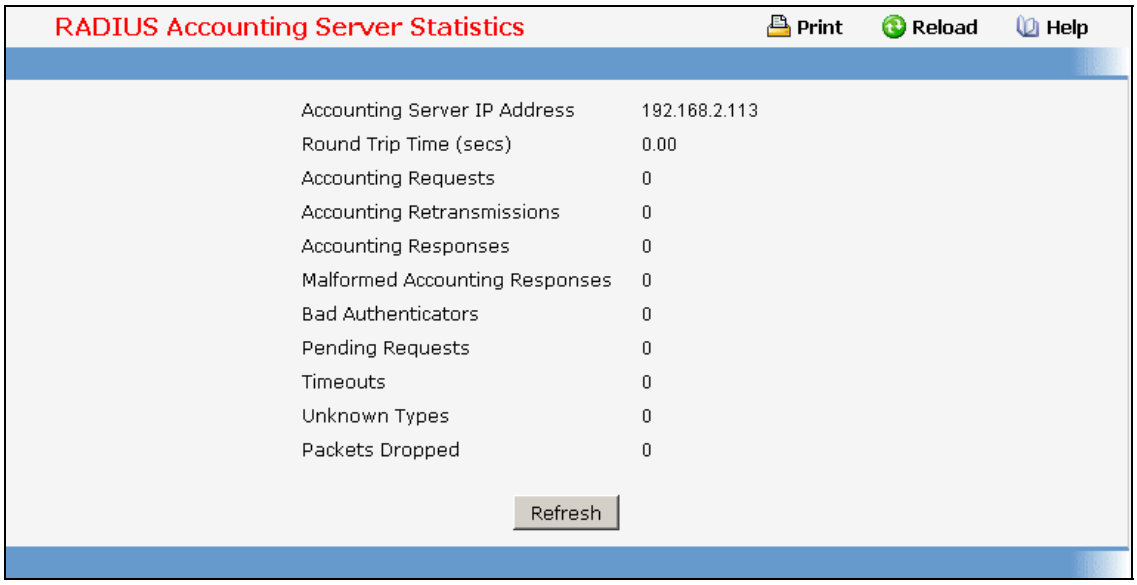
Command Buttons

Submit - Sends the updated screen to the switch and causes 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.

11.5.2.5 Viewing RADIUS Accounting Server Statistics Page



Non-Configurable Statistics

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.

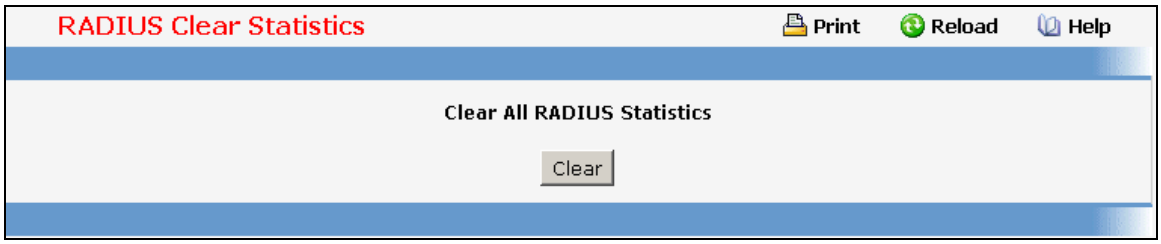
Unknown Types - Displays the number of RADIUS packets of unknown type that were received from this server on the accounting port.

Packets Dropped - Displays the number of RADIUS packets that were received from this server on the accounting port and dropped for some other reason.

Command Buttons

Refresh - Update the information on the page.

11.5.2.6 Resetting All RADIUS Statistics Page

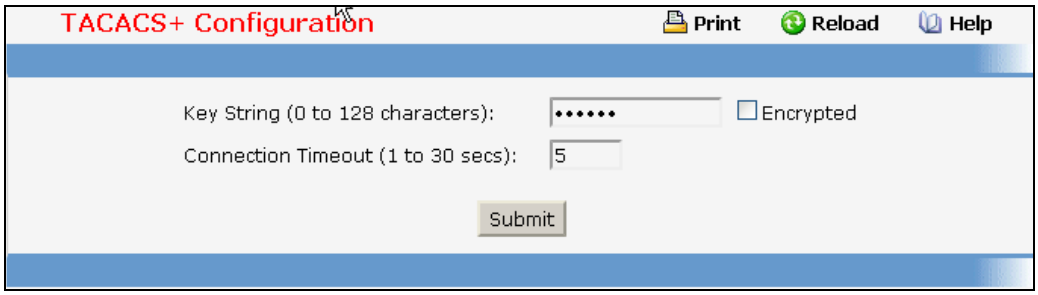


Command Buttons

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

11.5.3 Defining TACACS+ Configuration

11.5.3.1 Configuring TACACS Configuration Page



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.

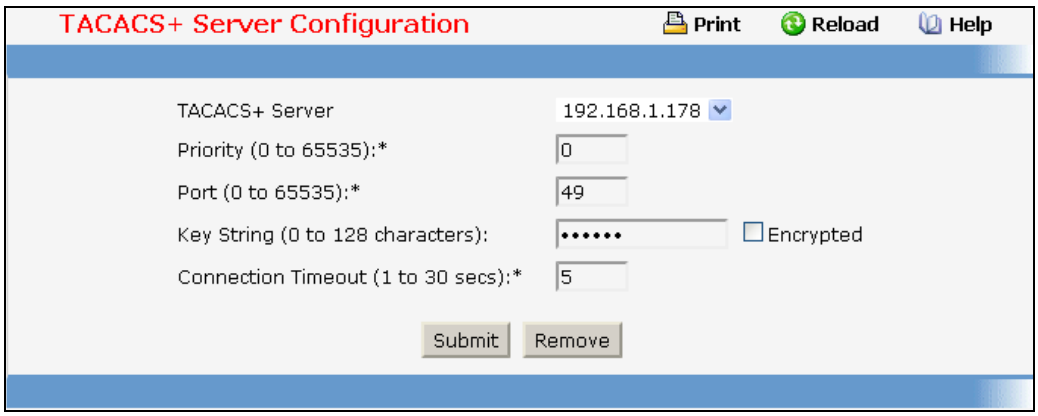
Connection Timeout - The maximum number of seconds allowed to establish a TCP connection between the device and the TACACS+ server.

Encrypted - When the secret string is encrypted, this box need to be checked. This field is only displayed if the user has READWRITE access.

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.

11.5.3.2 Configuring TACACS+ Server Configuration Page



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.

You cannot define these IP addresses:

0.0.0.0

255.255.255.255

224.xxx.xxx.xxx

127.0.0.1

Host name - The host name of the server being added.

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.

Encrypted - When the secret string is encrypted, this box need to be checked. This field is only displayed if the user has READWRITE access.

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.

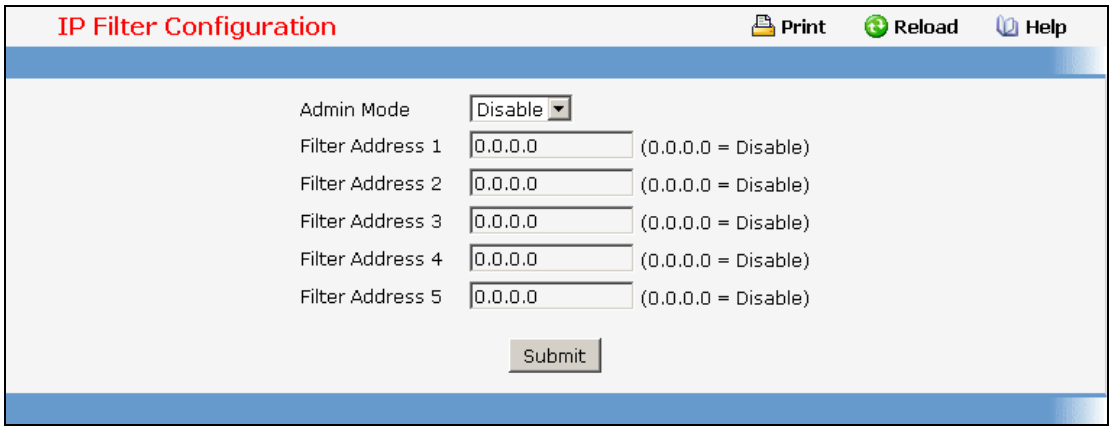
Remove - Remove the selected server from the configuration.

11.5.4 Defining IP Filter Configuration

11.5.4.1 IP Filter Configuration Page

Management IP filter designates stations that are allowed to make configuration changes to the Switch. Select up to five management stations used to manage the Switch. If you choose to define one or more

designated management stations, only the chosen stations, as defined by IP address, will be allowed management privilege through the web manager, Telnet session, Secure Shell (SSH) or Secure Socket Layer (SSL) for secure HTTP.



Selection Criteria

Admin Mode - Selects the IP Filter admin mode for enable or disable.

Configurable Data

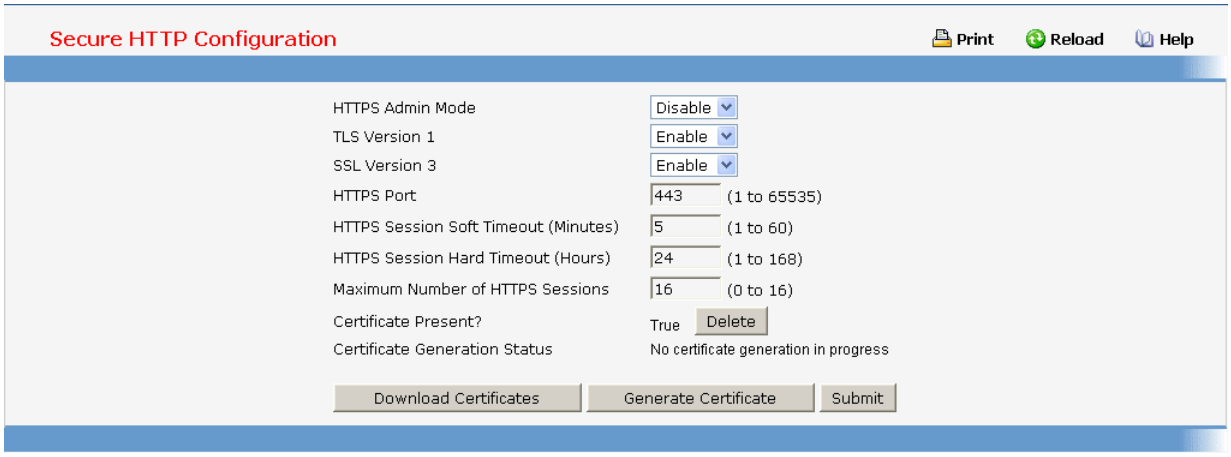
Filter Address 1~5 - Stations that are allowed to make configuration changes to the Switch.

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.

11.5.5 Defining Secure Http Configuration

11.5.5.1 Secure HTTP Configuration Page



Selection Criteria

HTTPS Admin Mode - This 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 disabled.

TLS Version 1 - This 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 enabled.

SSL Version 3 - This 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 enabled.

Configurable Data

HTTPS Port Number - This 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.

HTTPS Session Soft Timeout - This field is used to set the inactivity timeout for HTTPS sessions. The value must be in the range of (1 to 60) minutes. The default value is 5 minutes. The currently configured value is shown when the web page is displayed.

HTTPS Session Hard Timeout - This field is used to set the hard timeout for HTTPS sessions. This timeout is unaffected by the activity level of the session. The value must be in the range of (1 to 168) hours. The default value is 24 hours. The currently configured value is shown when the web page is displayed.

Maximum Number of HTTPS Sessions - This field is used to set the maximum allowable number of HTTPS sessions. The value must be in the range of (0 to 16). The default value is 16. The currently configured value is shown when the web page is displayed.

Non-Configurable Data

Certificate Present? - Displays whether there is a certificate present on the device.

Certificate Generation Status - Displays whether SSL certificate generation is in progress.

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.

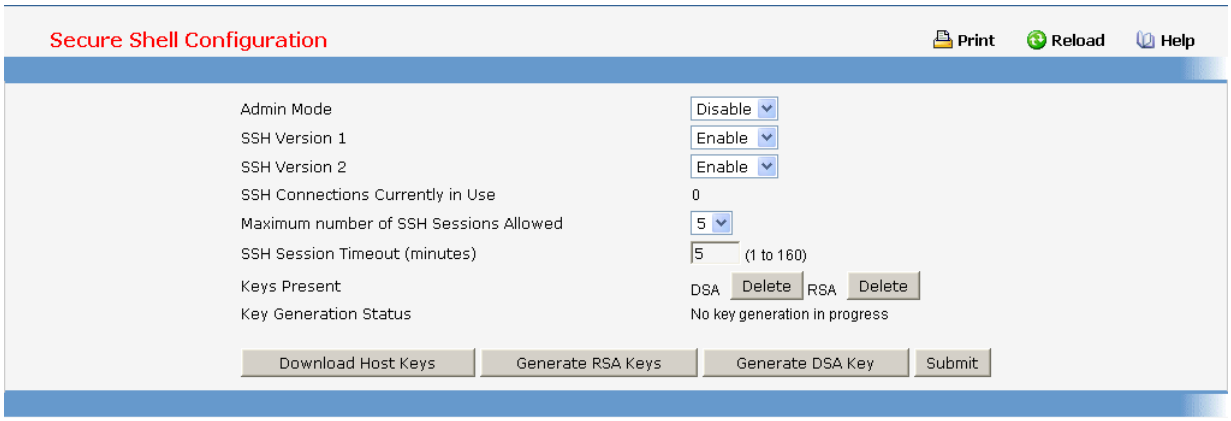
Download Certificates - Link to the File Transfer page for the SSL Certificate download. Note that to download SSL Certificate files SSL must be administratively disabled.

Generate Certificate - Begin generating the Certificate. Note that to generate SSL Certificate files SSL must be administratively disabled.

Delete - Used to delete the corresponding certificate, if it is present.

11.5.6 Defining Secure Shell Configuration

11.5.6.1 Configuring Secure Shell Configuration Page



Selection Criteria

Admin Mode - This select field is used to Enable or Disable the administrative 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.

Maximum Number of SSH Sessions Allowed - This select field is used to configure the maximum number of inbound SSH sessions allowed on the switch. The currently configured value is shown when the web page is displayed. The range of acceptable values for this field is (0-5).

Configurable Data

SSH Session Timeout (Minutes) - This text field is used to configure the inactivity timeout value for incoming SSH sessions to the switch. The acceptable range for this value is (1-160) minutes.

Non-Configurable Data

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

Keys Present - Displays which keys, RSA, DSA or both, are present (if any).

Key Generation Status - Displays which keys, RSA or DSA, are being generated.

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 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.

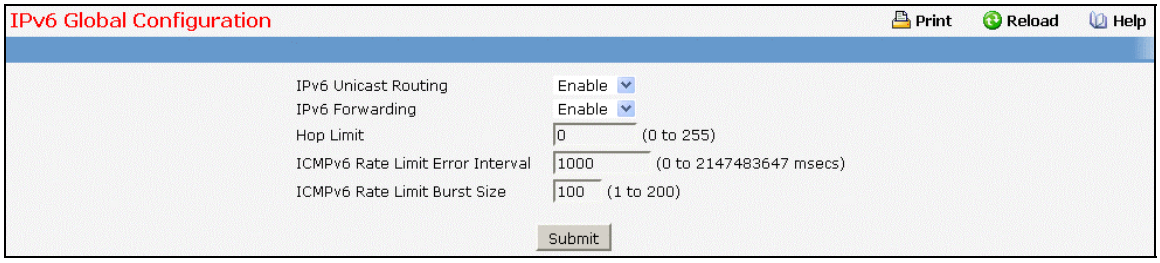
Generate RSA Host Keys - Begin generating the RSA host keys. Note that to generate SSH key files SSH must be administratively disabled and there can be no active SSH sessions.

Generate DSA Host Key - Begin generating the DSA host keys. Note that to generate SSH key files SSH must be administratively disabled and there can be no active SSH sessions.

Delete - Use to delete the corresponding key file (RSA or DSA), if it is present.

11.6 IPv6 Menu

11.6.1 Configuring IPv6 Global Configuration Page



Configurable Data

IPv6 Unicast Routing - Globally enable or disable IPv6 unicast routing on the entity.

IPv6 Forwarding - Enable or disable forwarding of IPv6 frames on the router.

Hop Limit - Specifies the TTL value for the router.The valid range is (1 to 255). The Value '0' is used to set the TTL to deafult value.

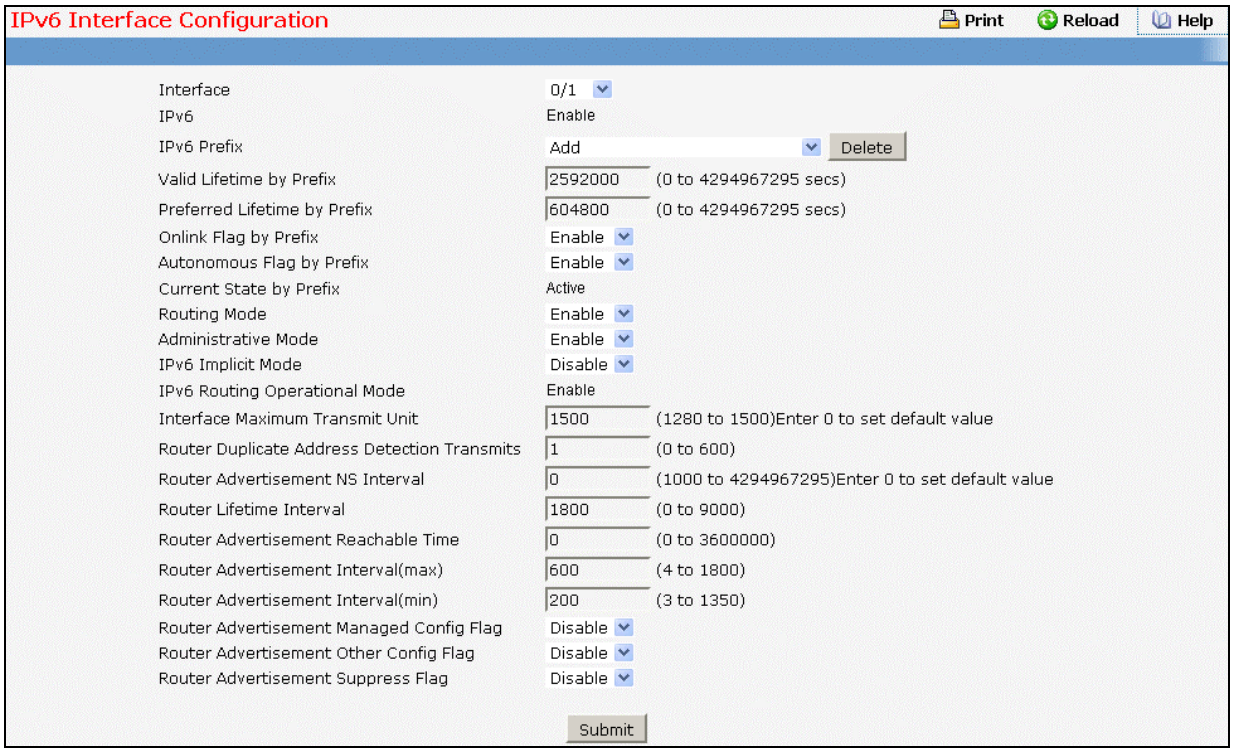
ICMPv6 Rate Limit Error Interval - To control the ICMPv6 error packets user can specify the number of ICMP error packets are allowed per burst interval. By Default Ratelimit is 100 packets/sec i.e burst interval is 1000 msec. To disable ICMP Ratelimiting set this field to '0'.Valid Rate Interval must be in the range (0 to 2147483647)

ICMPv6 Rate Limit Burst Size -To control the ICMP error packets user can specify the number of ICMP error packets are allowed per burst interval. Default burstsize is 100 packets. When burst interval is 0 then configuring this field is not a valid operation. Valid Burst Size must be in the range (1 to 200)

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.

11.6.2 Configuring IPv6 Interface Configuration Page



Selection Criteria

Interface - Selects the interface 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.

IPv6 Prefix - Specifies IPv6 prefix with prefix length for an interface. When the selection is changed screen is refreshed and valid lifetime, preferred lifetime, on-link flag and autonomous flag will be updated for selected IPv6 address.

Configurable Data

IPv6 - Specifies IPv6 protocol stack is Enable or Disable on this routing interface.

IPv6 Prefix - Specifies IPv6 prefix with prefix length for an interface.

EUI-64 - Specifies 64 bit unicast prefix.

Valid Lifetime by Prefix - Specifies router advertisement per prefix time to consider prefix valid for purposes of on link determination. Valid lifetime must be in the range (0 to 4294967295)

Preferred Lifetime by Prefix - Specifies router advertisement per prefix time. An autoconfigured address generated from this prefix is preferred. Preferred lifetime must be in range (0 to -1)

OnLink Flag by Prefix - Specifies selected prefix can be used for on-link determination. Default value is enable. This selector lists the two options for on-link flag: enable and disable.

Autonomous Flag by Prefix - Specifies selected prefix can be used for autonomous address configuration. Default value is disable. This selector lists the two options for autonomous flag: enable and disable.

Routing Mode - Specifies routing mode of an interface. This selector lists the two options for routing mode: enable and disable. Default value is disable.

Administrative Mode - Specifies administrative mode of an interface. This selector lists the two options for administrative mode: enable and disable. Default value is enable.

IPv6 Implicit Mode - When ipv6 implicit mode is enabled, interface is capable of ipv6 operation without a global address. In this case, an eui-64 based link-local address is used. This selector lists the two options for ipv6 mode: enable and disable. Default value is disable.

IPv6 Routing Operational Mode - Specifies operational state of an interface. Default value is disable.

Interface Maximum Transmit Unit - Specifies maximum trasmit unit on an interface. It is not valid to set this value to 0 if routing is enabled. If the value set to 0 that will be changed to default value 1500. Range of MTU is (1280 to 1500)

Router Duplicate Address Detection Transmits - Specifies number of duplicate address detections transmits on an interface. DAD transmits values must be in range (0 to 600)

Router Advertisement NS Interval - Specifies retransmission time field of router advertsisement sent from the interface. A value of 0 means interval is not specified for router. Range of neighbor solicit interval is (1000 to 4294967295)

Router Lifetime Interval - Specifies router advertisement lifetime field sent from the interface. This value must be greater than or equal to maximum advertisement interval. 0 means do not use router as default router. Range of router lifetime is (0 to 9000)

Router Advertisement Reachable Time - Specifies router advertisement time to consider neighbor reachable after ND confirmation. Range of reachable time is (0 to 3600000)

Router Advertisement Interval - Specifies maximum time allowed between sending router advertisements from the interface. Default value is 600. Range of maximum advertisement interval is (4 to 1800)

Router Advertisement Managed Config Flag - Specifies router advertisement managed address configuration flag. When true, end nodes use DHCPV6. When false end nodes autoconfigure addresses. Default value of managed flag is disable.

Router Advertisement Other Config Flag - Specifies router advertisement other stateful configuration flag. Default value of other config flag is disable.

Router Advertisement Suppress Flag - Specifies router advertisement suppression on an interface. Default value of suppress flag is disable.

Non-Configurable Data

Current State by Prefix - Indicates the state of the IPV6 address. The state is TENT if routing is disabled or DAD fails . The state is Active if interface is active and DAD is successful.

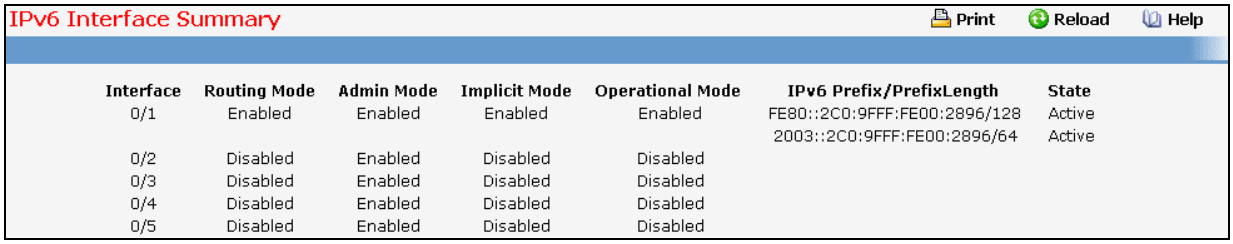
IPv6 Routing Operational Mode - Specifies operational state of an interface. Default value is disable.

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.

Delete - Delete the IPv6 Address configured on an interface.

11.6.3 Viewing IPv6 Interface Summary Page



Non-Configurable Data

Interface - Specifies the interface whose settings are displayed in the current table row.

Routing Mode - Specifies routing mode of an interface.

Admin Mode - Specifies administrative mode of an interface.

Implicit Mode - When ipv6 implicit mode is enabled, interface is capable of ipv6 operation without a global address. In this case, an eui-64 based link-local address is used. This selector lists the two options for ipv6 mode: enable and disable. Default value is disable.

Operational Mode - Specifies operational mode of an interface.

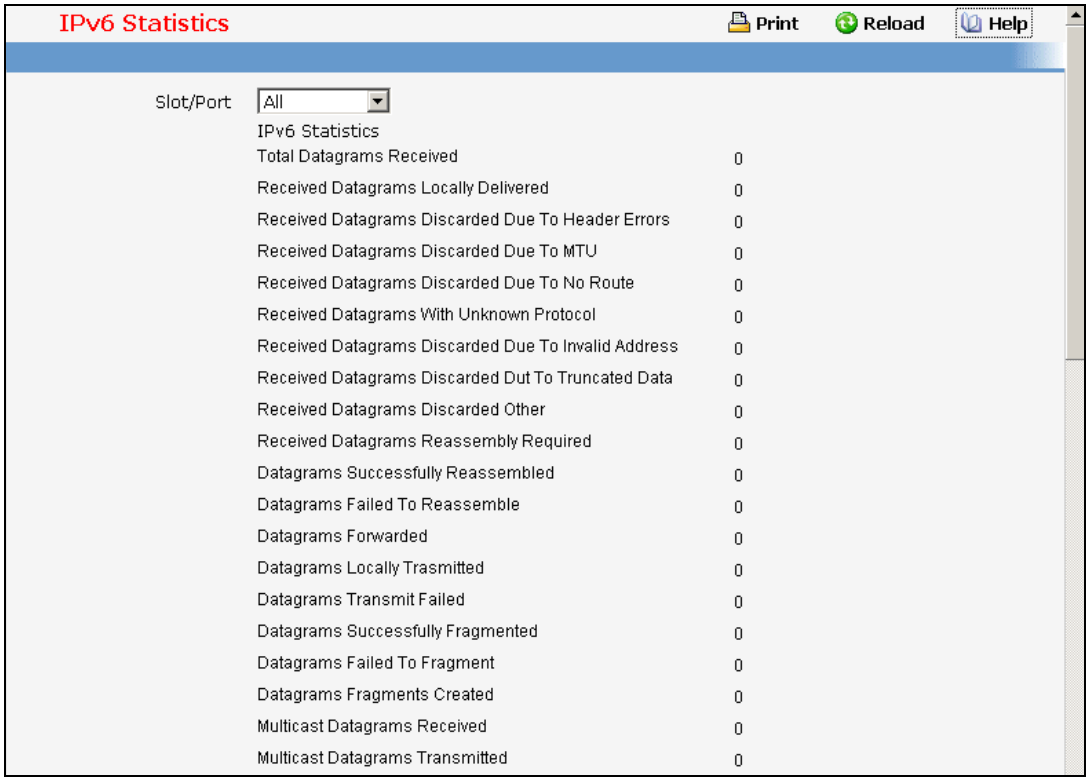
IPv6 Prefix/PrefixLength - Specifies configured IPv6 addresses on an interface.

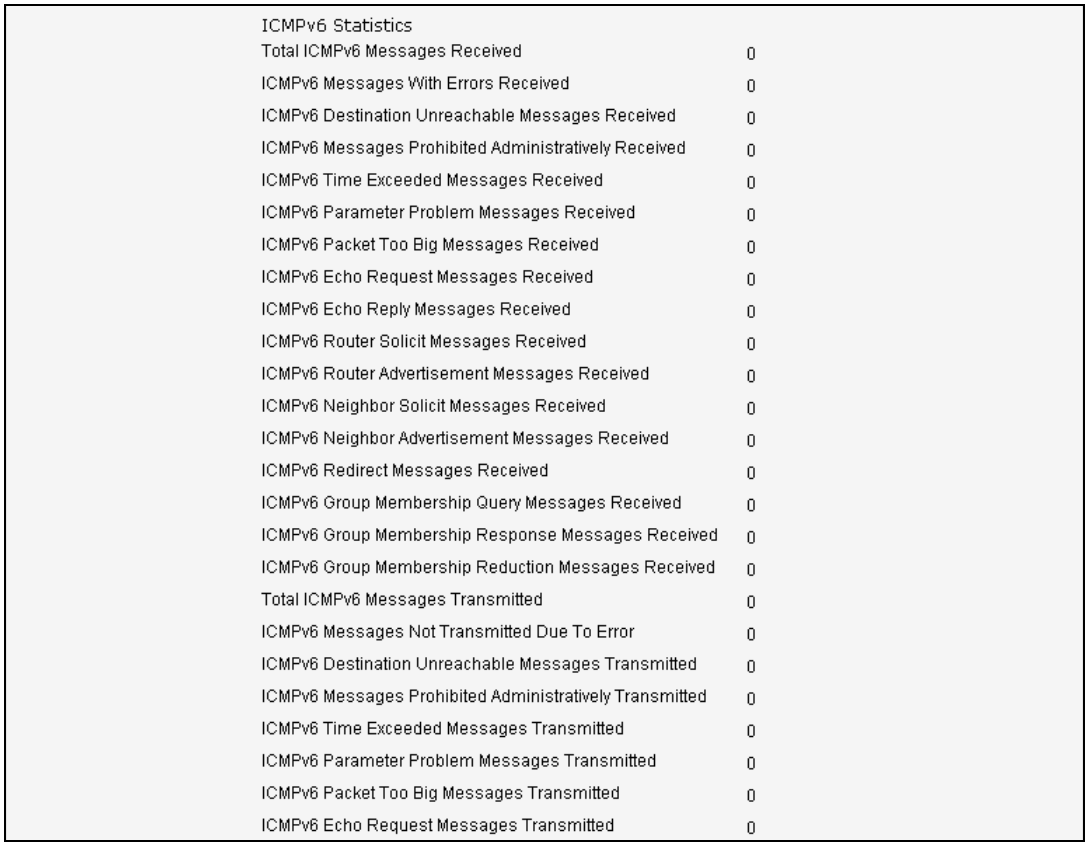
State - Specifies whether an interface is active or not.

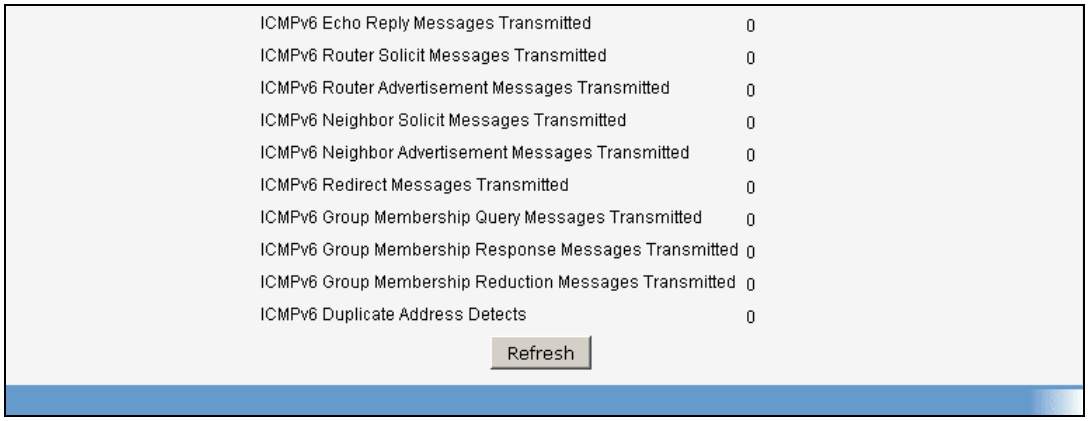
Command Buttons

Refresh - Refreshes the screen with most recent data.

11.6.4 Viewing IPv6 Interface Statistics Page


IPv6 Statistics
Print
Reload
Help
Slot/Port
All
IPv6 Statistics
Total Datagrams Received 0
Received Datagrams Locally Delivered 0
Received Datagrams Discarded Due To Header Errors 0
Received Datagrams Discarded Due To MTU 0
Received Datagrams Discarded Due To No Route 0
Received Datagrams With Unknown Protocol 0
Received Datagrams Discarded Due To Invalid Address 0
Received Datagrams Discarded Dut To Truncated Data 0
Received Datagrams Discarded Other 0
Received Datagrams Reassembly Required 0
Datagrams Successfully Reassembled 0
Datagrams Failed To Reassemble 0
Datagrams Forwarded 0
Datagrams Locally Trasmitted 0
Datagrams Transmit Failed 0
Datagrams Successfully Fragmented 0
Datagrams Failed To Fragment 0
Datagrams Fragments Created 0
Multicast Datagrams Received 0
Multicast Datagrams Transmitted 0


ICMPv6 Statistics
Total ICMPv6 Messages Received 0
ICMPv6 Messages With Errors Received 0
ICMPv6 Destination Unreachable Messages Received 0
ICMPv6 Messages Prohibited Administratively Received 0
ICMPv6 Time Exceeded Messages Received 0
ICMPv6 Parameter Problem Messages Received 0
ICMPv6 Packet Too Big Messages Received 0
ICMPv6 Echo Request Messages Received 0
ICMPv6 Echo Reply Messages Received 0
ICMPv6 Router Solicit Messages Received 0
ICMPv6 Router Advertisement Messages Received 0
ICMPv6 Neighbor Solicit Messages Received 0
ICMPv6 Neighbor Advertisement Messages Received 0
ICMPv6 Redirect Messages Received 0
ICMPv6 Group Membership Query Messages Received 0
ICMPv6 Group Membership Response Messages Received 0
ICMPv6 Group Membership Reduction Messages Received 0
Total ICMPv6 Messages Transmitted 0
ICMPv6 Messages Not Transmitted Due To Error 0
ICMPv6 Destination Unreachable Messages Transmitted 0
ICMPv6 Messages Prohibited Administratively Transmitted 0
ICMPv6 Time Exceeded Messages Transmitted 0
ICMPv6 Parameter Problem Messages Transmitted 0
ICMPv6 Packet Too Big Messages Transmitted 0
ICMPv6 Echo Request Messages Transmitted 0



Selection Criteria

Interface - Selects the interface to be configured. When the selection is changed, a screen refresh will occur causing all fields to be updated for the newly selected port.

Non-Configurable Data

IPv6 Statistics

Total Datagrams Received - The total number of input datagrams received by the interface, including those received in error.

Received Datagrams Locally Delivered - The total number of datagrams successfully delivered to IPv6 user-protocols (including ICMP). This counter is incremented at the interface to which these datagrams were addressed which might not be necessarily the input interface for some of the datagrams.

Received Datagrams Discarded Due To Header Errors - The number of input datagrams discarded due to errors in their IPv6 headers, including version number mismatch, other format errors, hop count exceeded, errors discovered in processing their IPv6 options, etc.

Received Datagrams Discarded Due To MTU - The number of input datagrams that could not be forwarded because their size exceeded the link MTU of outgoing interface.

Received Datagrams Discarded Due To No Route - The number of input datagrams discarded because no route could be found to transmit them to their destination.

Received Datagrams With Unknown Protocol - The number of locally-addressed datagrams received successfully but discarded because of an unknown or unsupported protocol. This counter is incremented at the interface to which these datagrams were addressed which might not be necessarily the input interface for some of the datagrams.

Received Datagrams Discarded Due To Invalid Address - The number of input datagrams discarded because the IPv6 address in their IPv6 header's destination field was not a valid address to be received at this entity. This count includes invalid addresses (e.g., ::0) and unsupported addresses(e.g., addresses with unallocated prefixes). For entities which are not IPv6 routers and therefore do not forward datagrams, this counter includes datagrams discarded because the destination address was not a local address.

Received Datagrams Discarded Dut To Truncated Data - The number of input datagrams discarded because datagram frame didn't carry enough data.

Received Datagrams Discarded Other - The number of input IPv6 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.

Received Datagrams Reassembly Required - The number of IPv6 fragments received which needed to be reassembled at this interface. Note that this counter is incremented at the interface to

which these fragments were addressed which might not be necessarily the input interface for some of the fragments.

Datagrams Successfully Reassembled - The number of IPv6 datagrams successfully reassembled. Note that this counter is incremented at the interface to which these datagrams were addressed which might not be necessarily the input interface for some of the fragments.

Datagrams Failed To Reassemble - The number of failures detected by the IPv6 reassembly algorithm (for whatever reason: timed out, errors, etc.). Note that this is not necessarily a count of discarded IPv6 fragments since some algorithms (notably the algorithm in RFC 815) can lose track of the number of fragments by combining them as they are received. This counter is incremented at the interface to which these fragments were addressed which might not be necessarily the input interface for some of the fragments.

Datagrams Forwarded - The number of output datagrams which this entity received and forwarded to their final destinations. In entities which do not act as IPv6 routers, this counter will include only those packets which were Source-Routed via this entity, and the Source-Route processing was successful. Note that for a successfully forwarded datagram the counter of the outgoing interface is incremented.

Datagrams Locally Trasmitted - The number of datagrams which this entity has successfully transmitted from this output interface.

Datagrams Transmit Failed - The number of datagrams which this entity failed to transmit successfully.

Datagrams Successfully Fragmented - The number of IPv6 datagrams that have been successfully fragmented at this output interface.

Datagrams Failed To Fragment - The number of output datagrams that could not be fragmented at this interface.

Datagrams Fragments Created - The number of output datagram fragments that have been generated as a result of fragmentation at this output interface.

Multicast Datagrams Received - The number of multicast packets received by the interface.

Multicast Datagrams Transmitted - The number of multicast packets transmitted by the interface.

ICMPv6 Statistics

Total ICMPv6 Messages Received - The total number of ICMP messages received by the interface which includes all those counted by ipv6IfIcmpInErrors. Note that this interface is the interface to which the ICMP messages were addressed which may not be necessarily the input interface for the messages.

ICMPv6 Messages With Errors Received - The number of ICMP messages which the interface received but determined as having ICMP-specific errors (bad ICMP checksums, bad length, etc.)

ICMPv6 Destination Unreachable Messages Received - The number of ICMP Destination Unreachable messages received by the interface.

ICMPv6 Messages Prohibited Administratively Received - The number of ICMP destination unreachable/communication administratively prohibited messages received by the interface.

ICMPv6 Time Exceeded Messages Received - The number of ICMP Time Exceeded messages received by the interface.

ICMPv6 Parameter Problem Messages Received - The number of ICMP Parameter Problem messages received by the interface.

ICMPv6 Packet Too Big Messages Received - The number of ICMP Packet Too Big messages received by the interface.

ICMPv6 Echo Request Messages Received - The number of ICMP Echo (request) messages received by the interface.

ICMPv6 Echo Reply Messages Received - The number of ICMP Echo Reply messages received by the interface.

ICMPv6 Router Solicit Messages Received - The number of ICMP Router Solicit messages received by the interface.

ICMPv6 Router Advertisement Messages Received - The number of ICMP Router Advertisement messages received by the interface.

ICMPv6 Neighbor Solicit Messages Received - The number of ICMP Neighbor Solicit messages received by the interface.

ICMPv6 Neighbor Advertisement Messages Received - The number of ICMP Neighbor Advertisement messages received by the interface.

ICMPv6 Redirect Messages Received - The number of ICMPv6 Redirect messaged received by the interface.

ICMPv6 Group Membership Query Messages Received - The number of ICMPv6 Group Membership Query messages received by the interface.

ICMPv6 Group Membership Response Messages Received - The number of ICMPv6 Group Membership Response messages received by the interface.

ICMPv6 Group Membership Reduction Messages Received - The number of ICMPv6 Group Membership Reduction messages received by the interface

Total ICMPv6 Messages Transmitted - The total number of ICMP messages which this interface attempted to send. Note that this counter includes all those counted by icmpOutErrors.

ICMPv6 Messages Not Transmitted Due To Error - The number of ICMP messages which this interface 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 IPv6 to route the resultant datagram. In some implementations there may be no types of error which contribute to this counter's value.

ICMPv6 Destination Unreachable Messages Transmitted - The number of ICMP Destination Unreachable Messages sent by the interface.

ICMPv6 Messages Prohibited Administratively Transmitted - Number of ICMP destination unreachable/communication administratively prohibited messages sent.

ICMPv6 Time Exceeded Messages Transmitted - The number of ICMP Time Exceeded messages sent by the interface.

ICMPv6 Parameter Problem Messages Transmitted - The number of ICMP Parameter Problem messages sent by the interface.

ICMPv6 Packet Too Big Messages Transmitted - The number of ICMP Packet Too Big messages sent by the interface.

ICMPv6 Echo Request Messages Transmitted - The number of ICMP Echo (request) messages sent by the interface.

ICMPv6 Echo Reply Messages Transmitted - The number of ICMP Echo Reply messages sent by the interface.

ICMPv6 Router Solicit Messages Transmitted - The number of ICMP Neighbor Solicitation messages sent by the interface.

ICMPv6 Router Advertisement Messages Transmitted - The number of ICMP Router Advertisement messages sent by the interface.

ICMPv6 Neighbor Solicit Messages Transmitted - The number of ICMP Neighbor Solicitation messages sent by the interface.

ICMPv6 Neighbor Advertisement Messages Transmitted - The number of ICMP Neighbor Advertisement messages sent by the interface.

ICMPv6 Redirect Messages Transmitted - The number of Redirect messages sent.

ICMPv6 Group Membership Query Messages Transmitted - The number of ICMPv6 Group Membership Query messages sent.

ICMPv6 Group Membership Response Messages Transmitted - The number of ICMPv6 Group Membership Response messages sent.

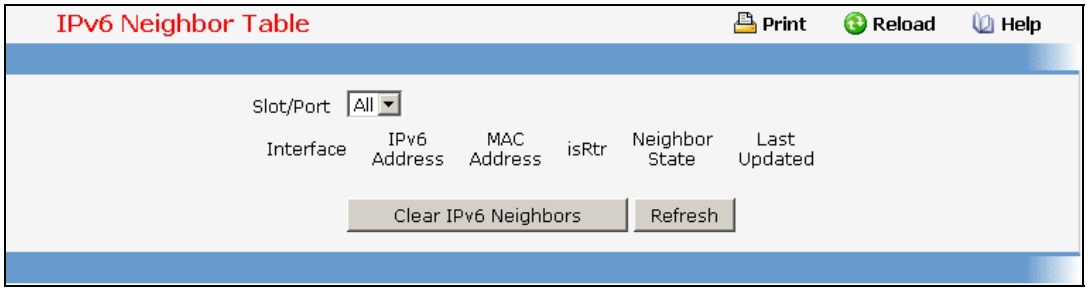
ICMPv6 Group Membership Reduction Messages Transmitted - The number of ICMPv6 Group Membership Reduction messages sent.

ICMPv6 Duplicate Address Detects - The number of duplicate Addresesses detected by the interface.

Command Buttons

Refresh - Refreshes the screen with most recent data.

11.6.5 Viewing IPv6 Neighbor Table Information Page



Selection Criteria

Slot/Port - Selects the interface whose information has to be displayed.

Non-Configurable Data

Interface - Specifies the interface whose settings are displayed in the current table row.

IPv6 Address - Specifies the IPv6 address of neighbor or interface.

MAC Address - Specifies MAC address associated with an interface.

IsRtr - Specifies router flag.

Neighbor State - Specifies the state of the neighbor cache entry. Following are the states for dynamic entries in the IPv6 neighbor discovery cache:

- ***Incmp*** - Address resolution is being performed on the entry. A neighbor solicitation message has been sent to the solicited-node multicast address of the target, but the corresponding neighbor advertisement message has not yet been received.
- ***Reach*** - Positive confirmation was received within the last Reachable Time milliseconds that the forward path to the neighbor was functioning properly. While in REACH state, the device takes no special action as packets are sent.

- ***Stale*** - More than ReachableTime milliseconds have elapsed since the last positive confirmation was received that the forward path was functioning properly. While in STALE state, the device takes no action until a packet is sent.
- ***Delay*** - More than ReachableTime milliseconds have elapsed since the last positive confirmation was received that the forward path was functioning properly. A packet was sent within the last DELAY_FIRST_PROBE_TIME seconds. If no reachability confirmation is received within DELAY_FIRST_PROBE_TIME seconds of entering the DELAY state, send a neighbor solicitation message and change the state to PROBE.
- ***Probe*** - A reachability confirmation is actively sought by resending neighbor solicitation messages every RetransTimer milliseconds until a reachability confirmation is received.

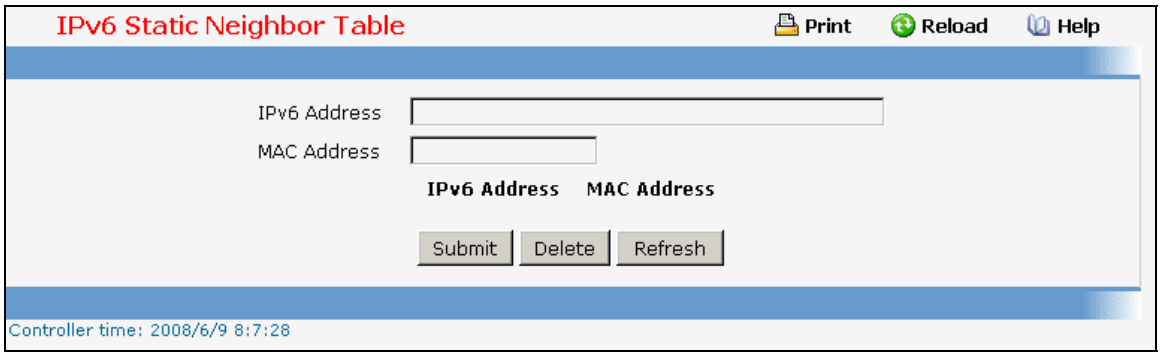
Last Updated - Time since the address was confirmed to be reachable.

Command Buttons

Refresh - Refreshes the screen with most recent data.

Clear IPv6 Neighbors - Clear IPv6 neighbors on selected interface or all interfaces.

11.6.6 Viewing IPv6 Static Neighbor Table Information Page



Configurable Data

IPv6 Address - Specifies the IPv6 address of neighbor.

MAC Address - Specifies the IPv6 address of neighbor.

Non-Configurable Data

IPv6 Address - Display the IPv6 address of current IPv6 neighbor table.

MAC Address - Display the MAC address of current IPv6 neighbor table.

Command Buttons

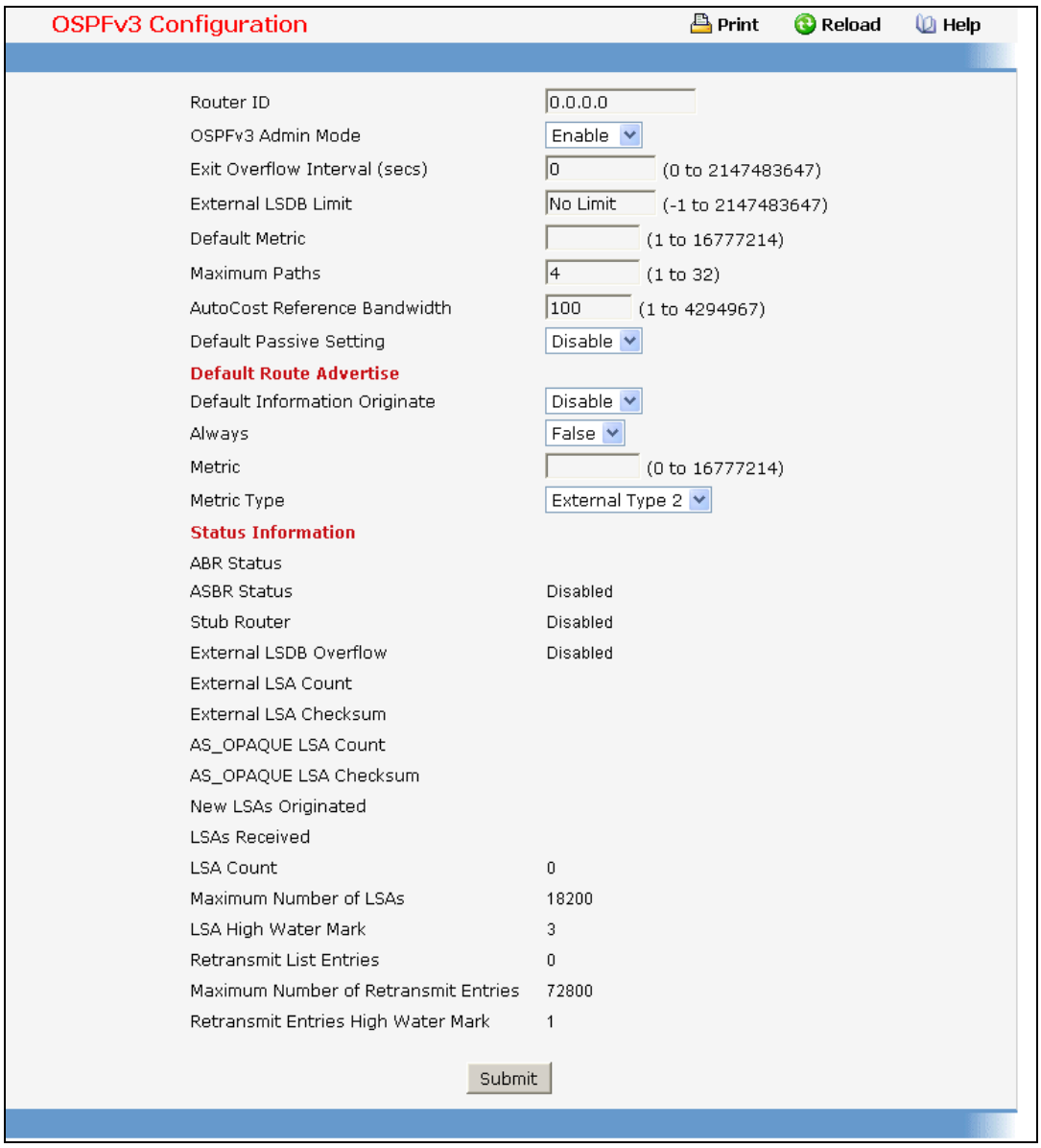
Add - Add the IPv6 neighbor.

Delete - Delete the IPv6 neighbor.

Refresh - Refreshes the screen with most recent data.

11.6.7 Managing OSPFv3 Protocol

11.6.7.1 Configuring OSPFv3 Configuration Page



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 OSPFv3. After you set the new Router ID, you must re-enable OSPFv3 to have the change take effect. The default value is 0.0.0.0, although this is not a valid Router ID.

OSPFv3 Admin Mode* - Select enable or disable from the pull down menu. If you select enable OSPFv3 will be activated for the switch. The default value is enable. You must configure a Router ID before OSPFv3 can become operational. This can also be done by issuing the CLI command router-id, in the ipv6 router ospf mode.

***NOTE: once OSPFv3 is initialized on the router, it will remain initialized until the router is reset.**

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.

External LSDB Limit - The maximum number of AS-External-LSAs that can be stored in the database. A value of -1 implies there is no limit on the number that can be saved. The valid range of values is (-1 to 2147483647).

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 16777214)

Maximum Paths - Configure the maximum number of paths that OSPFv3 can report to a given destination. The valid values are 1 to 32.

AutoCost Reference Bandwidth - Configure the auto-cost reference-bandwidth to control how OSPF calculates default metrics for the interface. The valid values are (1 to 4294967)

Default Passive Setting - Configure the global passive mode setting for all OSPF interfaces. Configuring this field overwrites any present interface level passive mode setting. OSPF does not form adjacencies on passive interfaces, but does advertise attached networks as stub networks.

Default Route Advertise

Default Information Originate - Enable or Disable Default Route Advertise. Note that the values for 'Always', 'Metric' and 'Metric Type' can only be configured after Default Information Originate is set to enable. If Default Information Originate is set to enable and values for 'Always', 'Metric' and 'Metric Type' are already configured, then setting Default Information Originate back to disable will set the 'Always', 'Metric' and 'Metric Type' values to default.

Always - Sets the router advertise ::/0 when set to "True".

Metric - Specifies the metric of the default route. The valid values are (0 to 16777214)

Metric Type - Sets the metric type of the default route. Valid values are External Type 1 and External Type 2.

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.

Stub Router - When OSPF runs out of resources to store the entire link state database, or any other state information, OSPF goes into stub router mode. As a stub router, OSPF re-originates its own router LSAs, setting the cost of all non-stub interfaces to infinity. To restore OSPF to normal operation, disable and re-enable OSPF.

External LSDB Overflow - When the number of non-default external LSAs exceeds the configured limit, External LSDB Limit, OSPF goes into LSDB overflow state. In this state, OSPF withdraws all of its self-originated non-default external LSAs. After the Exit Overflow Interval, OSPF leaves the overflow state, if the number of external LSAs has been reduced.

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.

AS_OPAQUE LSA Count - The number of opaque LSAs with domain wide flooding scope.

AS_OPAQUE LSA Checksum - The sum of the LS checksums of the opaque LSAs with domain wide flooding scope. 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. This value is in hexadecimal.

New LSAs Originated - In any given OSPFv3 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.

LSA Count - The total number of link state advertisements currently in the link state database.

Maximum Number of LSAs - The maximum number of LSAs that OSPF can store.

LSA High Water Mark - The maximum size of the link state database since the system started.

Retransmit List Entries - The total number of LSAs waiting to be acknowledged by all neighbors. An LSA may be pending acknowledgment from more than one neighbor.

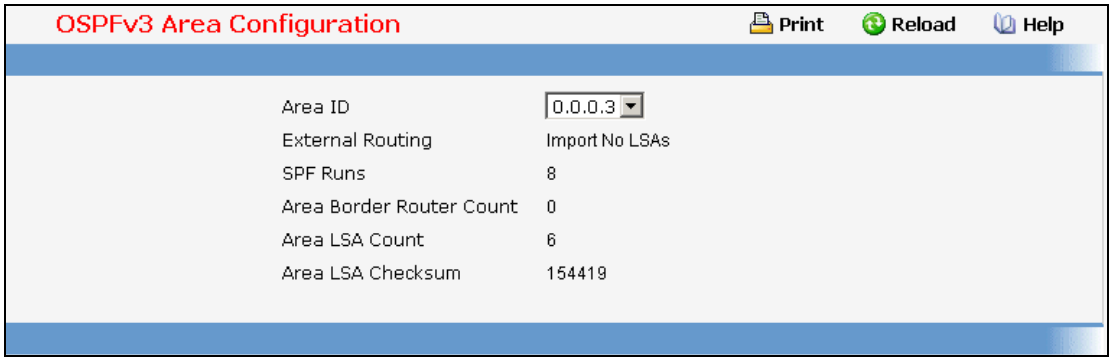
Maximum Number of Retransmit Entries - The maximum number of LSAs that can be waiting for acknowledgment at any given time.

Retransmit Entries High Water Mark - The highest number of LSAs that have been waiting for acknowledgment.

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.

11.6.7.2 Configuring OSPFv3 Area Configuration Page



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 areas. Defaults to Enable.

Stub Area Specific Parameters.

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. This value is applicable only to Stub areas.

NSSA Specific Parameters.

Default Information Originate - The default Route Information. This can also be applied by the CLI command 'area (area-id) nssa default-info-originate' in the ipv6 router ospf config mode. Valid values are True or False.

Default Metric - Set the Default Metric value for NSSA. The valid range of values is (1 to 16777214).

Metric Type Type - Select the type of metric specified in the Metric Value field.

- ***Default*** - The default metric value. On CLI this value shows up as "-------"
- ***Comparable Cost*** - External Type 1 metrics that are comparable to the OSPFv3 metric
- ***Non-comparable Cost*** - External Type 2 metrics that are assumed to be larger than the cost of the OSPFv3 metric

Translator Role - NSSA Border router's ability to perform NSSA translation of type-7 LSAs into type-5 LSAs. The valid values are 'Always' and 'Candidate'.

Translator Stability Interval - The number of seconds after an elected translator determines its services are no longer required, that it should continue to perform its translation duties. The valid range of values is (0 to 3600).

No-Redistribute Mode - Enable or Disable the No-Redistribute Mode.

Non-Configurable Data

Area ID - The OSPFv3 area. An Area ID is a 32 bit integer in dotted decimal format that uniquely identifies the area to which a router interface connects.

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.

SPF Runs - The number of times that the intra-area route table has been calculated using this area's link-state database. This is 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.

Stub Area Specific Parameters.

Metric Value - The Configured Metric value for the Stub. This can be modified using the CLI command 'area (area-id) default-cost' in the ipv6 router ospf config mode. The valid range is (1 to 16777215).

NSSA Specific Parameters.

Translator State - Translator State 'Enabled' means that the NSSA router OSPFv3 Area NssA Translator Role has been set to always. Translator State of 'Elected' means a candidate NSSA Border router is translating type-7 LSAs into type-5.' Disabled' implies tha a candidate NSSA Border router is NOT translating type-7 LSAs into type-5.

Command Buttons

Create Stub Area - Configure the area as a stub area.

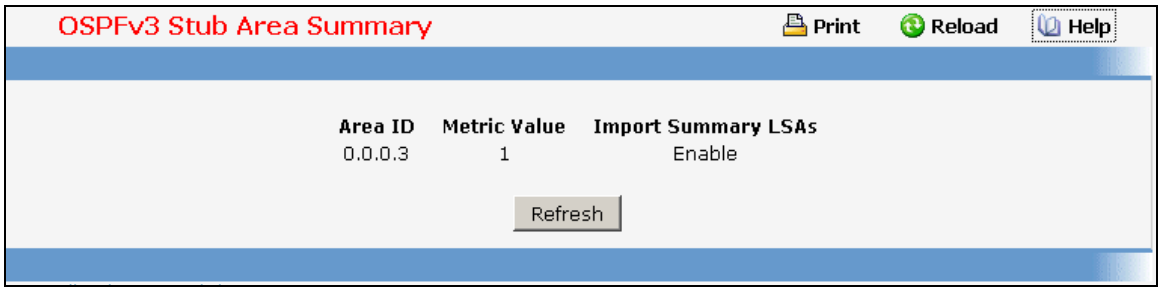
Delete Stub Area - Delete the stub area designation. The area will be returned to normal state.

Create NSSA - Configure the area as NSSA.

Delete NSSA - Delete the NSSA 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.

11.6.7.3 Viewing OSPFv3 Stub Area Summary Page



Non-Configurable Data

Area ID - The Area ID of the Stub area

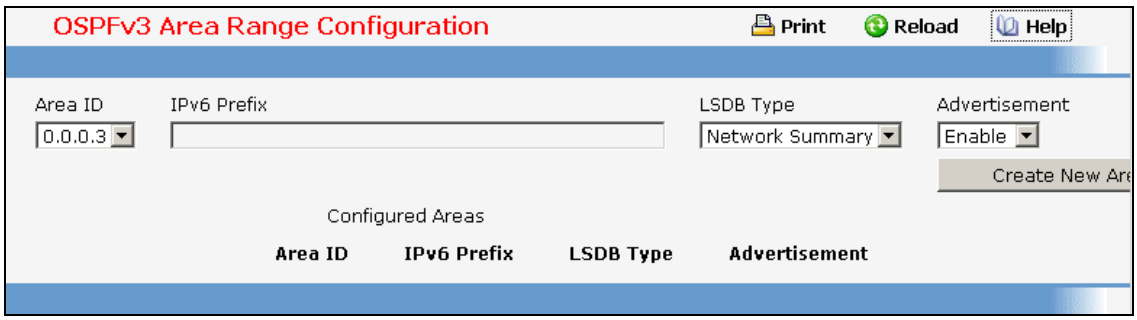
Metric Value - The metric value applied to the default route advertised into the area.

Import Summary LSAs - Whether the import of Summary LSAs is enabled or disabled.

Command Buttons

Refresh - Refresh the data on the screen to the current values from the switch.

11.6.7.4 Configuring OSPFv3 Area Range Configuration Page



Selection Criteria

Area ID - Selects the area for which data is to be configured.

Configurable Data

IPv6 Prefix - Enter the IPv6 Prefix/Prefix Length 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 OSPFv3 area.

IPv6 Prefix - The IPv6 Prefix of an address range for the area.

LSDB Type - The Link Advertisement type for the address range and area.

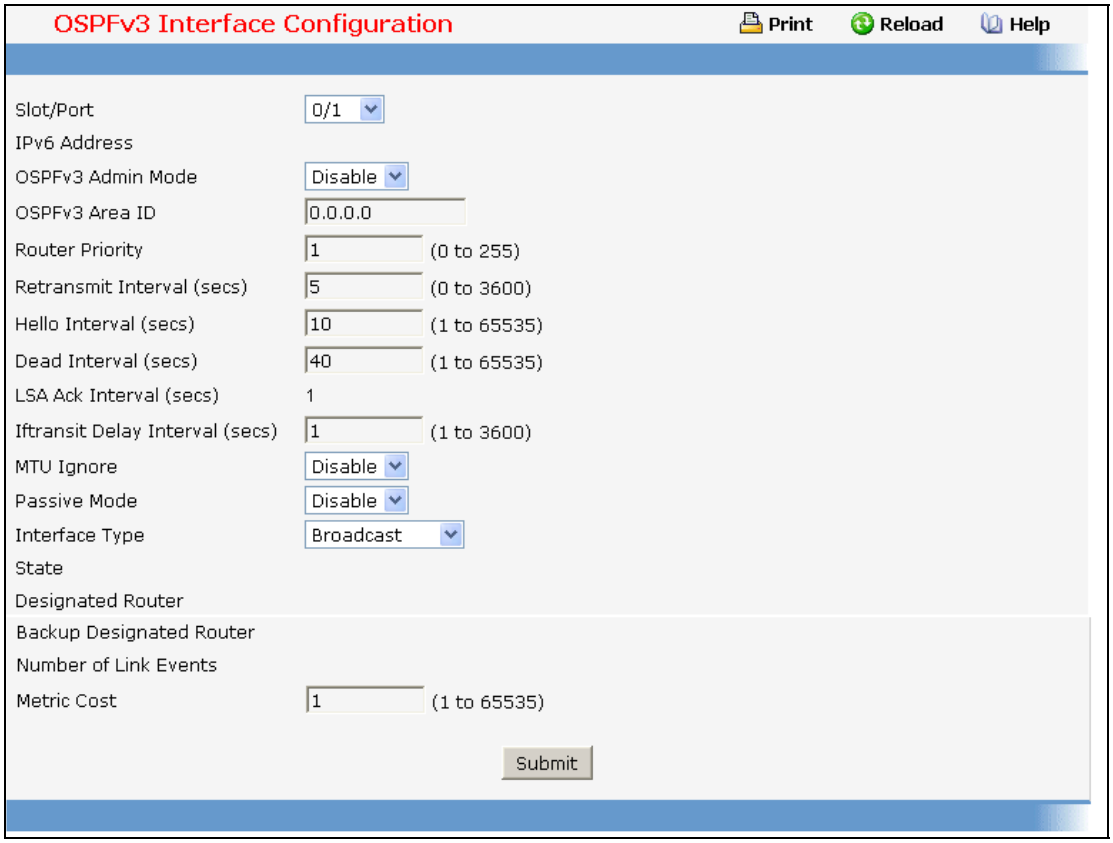
Advertisement - The Advertisement mode for the address range and area.

Command Buttons

Create New Area Range - 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.

11.6.7.5 Configuring OSPFv3 Interface Configuration Page



Selection Criteria

Slot/Port - Select the interface for which data is to be displayed or configured.

Configurable Data

OSPFv3 Admin Mode* - You may select enable or disable from the pulldown menu. The default value is 'disable.' You can configure OSPFv3 parameters without enabling OSPFv3 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 OSPFv3 to be fully functional, the interface must have a valid IPv6 Prefix/Prefix Length. This can be done through the CLI using the ipv6 address command in the interface configuration mode.

Once OSPFv3 is initialized on the router, it will remain initialized until the router is reset.

OSPFv3 Area ID - Enter the 32 bit integer in dotted decimal format that uniquely identifies the OSPFv3 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 OSPFv3 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 OSPFv3 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 0 to 3600 seconds (1 hour). The default is 5 seconds.

Hello Interval - Enter the OSPFv3 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 OSPFv3 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 OSPFv3 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 OSPFv3 MTU mismatch detection on receiving packets. Default value is Disable.

Passive Mode - Make an interface passive to prevent OSPF from forming an adjacency on an interface. OSPF advertises networks attached to passive interfaces as stub networks. Interfaces are not passive by default.

Interface Type - The interface type, which can either be set to broadcast mode or point to point mode. The default interface type is broadcast.

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 if OSPFv3 is initialized on the interface.

Non-Configurable Data

IPv6 Address - The IPv6 address of the interface.

LSA Ack Interval - The number of seconds between LSA Acknowledgment packet transmissions, which must be less than the Retransmit Interval.

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 OSPFv3 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 OSPFv3 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 OSPFv3 admin mode is enabled.

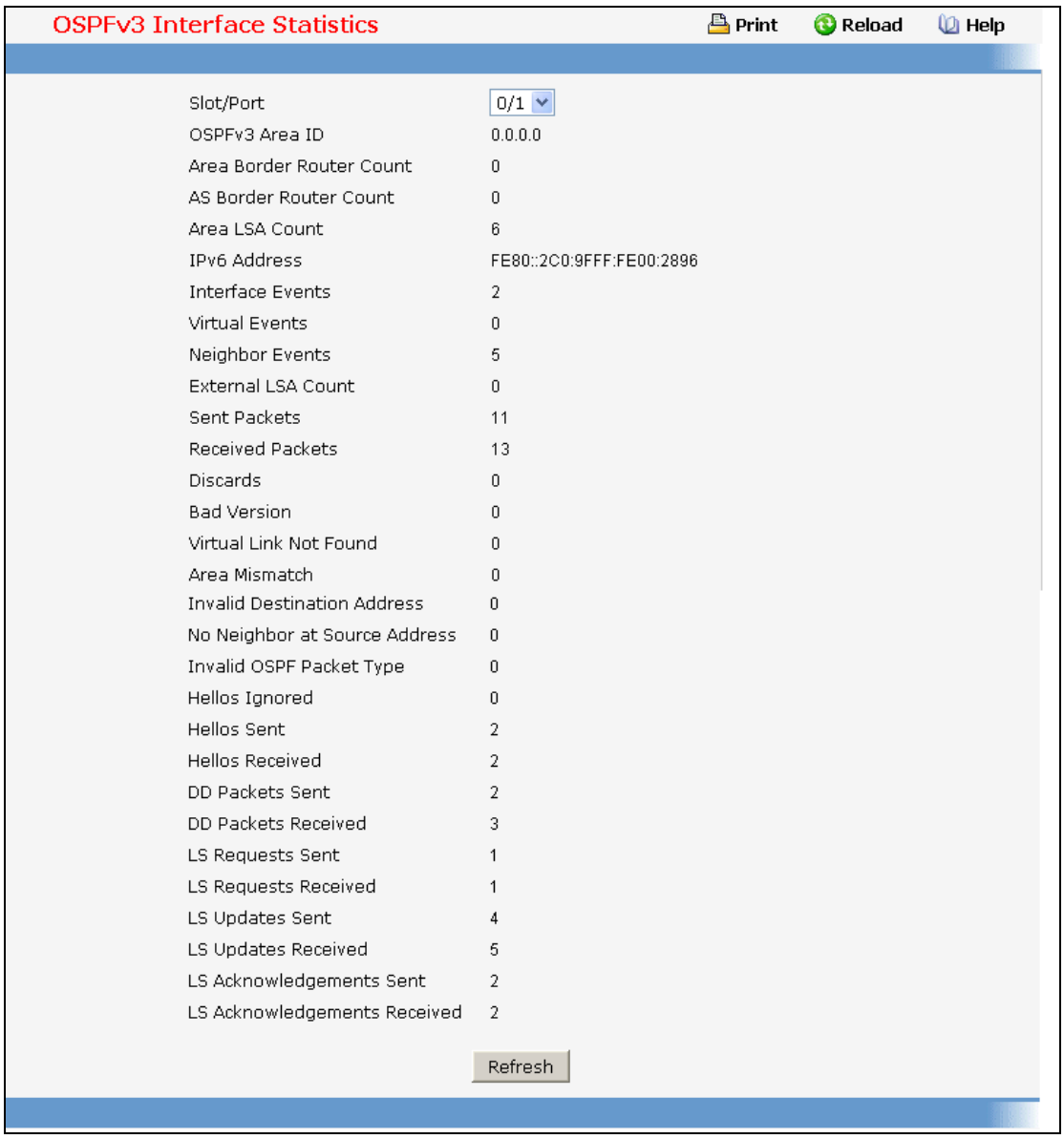
Number of Link Events - This is the number of times the specified OSPFv3 interface has changed its state. This field is only displayed if the OSPFv3 admin mode is enabled.

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.

11.6.7.6 Viewing OSPFv3 Interface Statistics Page

This screen displays statistics for the selected interface. The information will be displayed only if OSPFv3 is enabled.



Selection Criteria

Slot/Port - Select the interface for which data is to be displayed.

Non-Configurable Data

OSPFv3 Area ID - The OSPFv3 area to which the selected router interface belongs. An OSPFv3 Area ID is a 32 bit integer in dotted decimal format that uniquely identifies the area to which the interface connects.

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.

IPv6 Address - The IPv6 address of the interface.

Interface Events - The number of times the specified OSPFv3 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.

Sent packets - The number of OSPFv3 packets transmitted on the interface.

Received packets - The number of valid OSPFv3 packets received on the interface.

Discards - The number of received OSPFv3 packets discarded because of an error in the packet or an error in processing the packet.

Bad Version - The number of received OSPFv3 packets whose version field in the OSPFv3 header does not match the version of the OSPFv3 process handling the packet.

Virtual Link Not Found - The number of received OSPFv3 packets discarded where the ingress interface is in a non-backbone area and the OSPFv3 header identifies the packet as belonging to the backbone, but OSPFv3 does not have a virtual link to the packet's sender.

Area Mismatch - The number of OSPFv3 packets discarded because the area ID in the OSPFv3 header is not the area ID configured on the ingress interface.

Invalid Destination Address - The number of OSPFv3 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.

No Neighbor at Source Address - The number of OSPFv3 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.

Invalid OSPF Packet Type - The number of OSPFv3 packets discarded because the packet type field in the OSPFv3 header is not a known type.

Hellos Ignored - The number of received Hello packets that were ignored by this router from the new neighbors after the limit has been reached for the number of neighbors on an interface or on the system as a whole.

Hellos Sent - The number of Hello packets sent on this interface by this router.

Hellos Received - The number of Hello packets received on this interface by this router.

DD Packets Sent - The number of Database Description packets sent on this interface by this router.

DD Packets Received - The number of Database Description packets received on this interface by this router.

LS Requests Sent - The number of LS Requests sent on this interface by this router.

LS Requests Received - The number of LS Requests received on this interface by this router.

LS Updates Sent - The number of LS updates sent on this interface by this router.

LS Updates Received - The number of LS updates received on this interface by this router.

LS Acknowledgements Sent - The number of LS acknowledgements sent on this interface by this router.

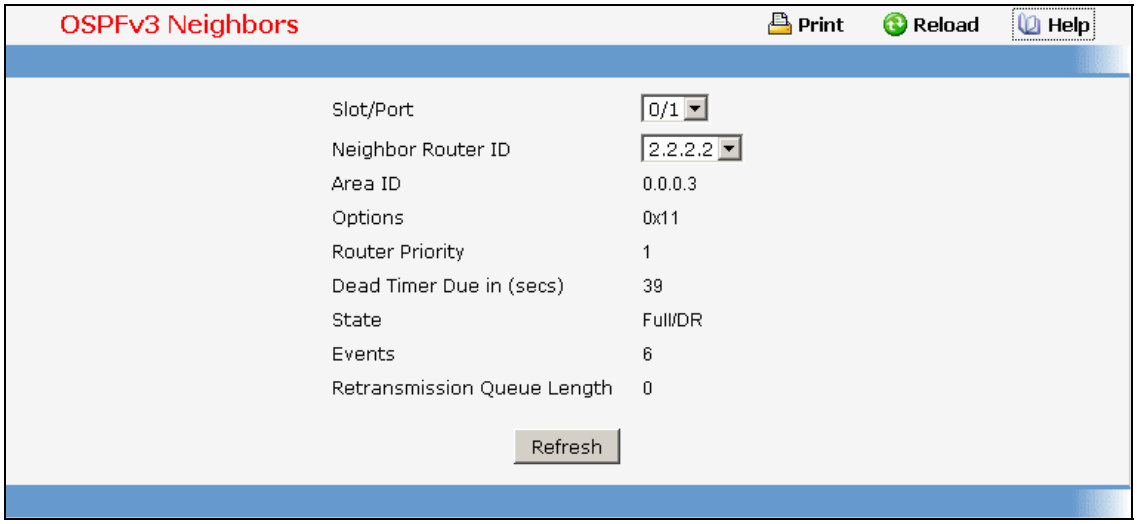
LS Acknowledgements Received - The number of LS acknowledgements received on this interface by this router.

Command Buttons

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

11.6.7.7 Viewing OSPFv3 Neighbor Information Page

This screen shows the OSPFv3 Neighbor information for a selected neighbor Router ID on the selected interface. When a particular Neighbor Router ID is selected, it shows detailed information about the neighbor. This information is displayed only is OSPFv3 is enabled and there is at least one OSPFv3 enabled interface with a valid neighbor present.



Selection Criteria

Slot/Port - Select the Interface for which the data needs to be displayed.

Neighbor Router ID - Selects a specific neighbor router ID on the interface selected in the Slot/Port selector.

Non-Configurable Data

Area ID - A 32-bit integer in dotted decimal format representing the area common to the neighbor selected.

Options - A Bit Mask corresponding to the neighbor's options field.

Priority - The priority of this neighbor in the designated router election algorithm. A value of 0 signifies that the neighbor is not eligible to become the designated router on this particular network.

Dead Timer Due in (secs) - Number of seconds since last Hello was received from Adjacent Neighbors. Set to 0 for neighbors in a state less than or equal to Init.

State - State of the relationship with this neighbor.

Events - The number of times this neighbor relationship has changed state, or an error has occurred.

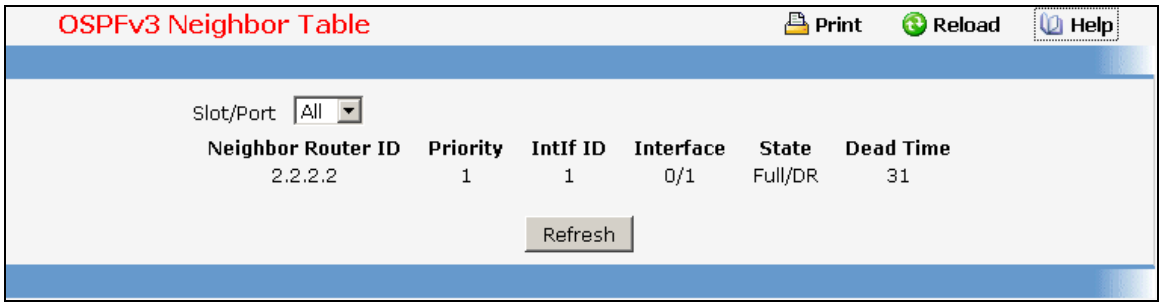
Retransmission Queue Length - Length of the selected neighbor's retransmit queue.

Command Buttons

Refresh - Refreshes the page with the latest OSPFv3 neighbor information for the selected interface and Neighbor Router ID.

11.6.7.8 Viewing OSPFv3 Neighbor Table Information Page

This screen shows the OSPFv3 Neighbor Table, either for all interfaces on which valid OSPFv3 Neighbors are present or the neighbors specific to a given interface on which OSPFv3 Neighbors exist. This information is displayed only if OSPFv3 is enabled and there exists at least on OSPFv3 enabled interface having a valid neighbor.



Selection Criteria

Slot/Port - Select the Interface for which the data needs to be displayed. Selecting 'All' will display all valid interfaces.

Non-Configurable Data

Neighbor Router ID - A 32-bit integer in dotted decimal format representing the Router ID of the neighbor on the selected Interface.

Priority - The priority of this neighbor in the designated router election algorithm. A value of 0 signifies that the neighbor is not eligible to become the designated router on this particular network.

IntIf ID - The interface ID that the neighbor advertises in its Hello packets on this link.

Interface - A Slot/Port identifying the neighbor interface index.

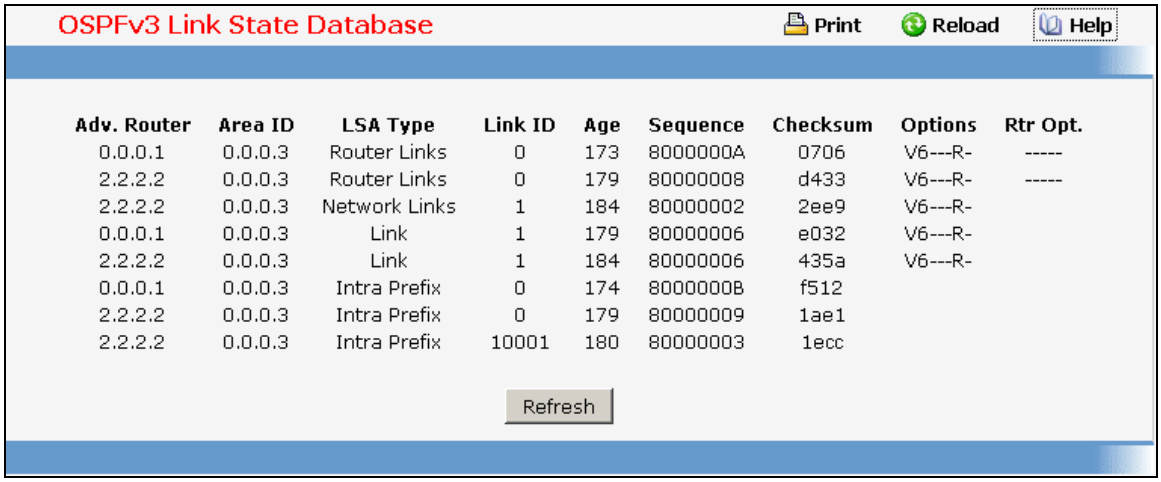
State - State of the relationship with this neighbor.

Dead Time - Number of seconds since last Hello was received from Adjacent Neighbors. Set to 0 for neighbors in a state less than or equal to Init.

Command Buttons

Refresh - Refreshes the page with the latest OSPFv3 neighbor information for the selected interface.

11.6.7.9 Viewing OSPFv3 Link State Database Information Page



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 OSPFv3 Interface Configuration page. If you want to change the Router ID you must first disable OSPFv3. After you set the new Router ID, you must re-enable OSPFv3 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 OSPFv3 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.

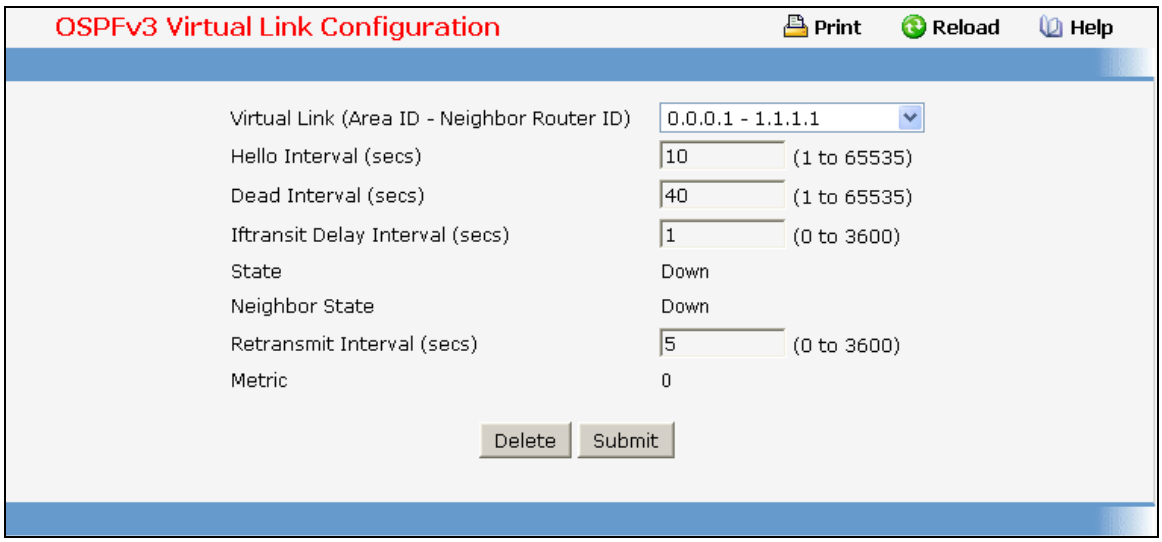
Options - The Options field in the link state advertisement header indicates which optional capabilities are associated with the advertisement.

Rtr Options - The router specific options.

Command Buttons

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

11.6.7.10 Configuring OSPFv3 Virtual Link Configuration Page



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

Hello Interval - The OSPFv3 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 - The OSPFv3 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 - The OSPFv3 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 - The OSPFv3 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.

Non-Configurable Data

State - The state of the interface.

- ***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.

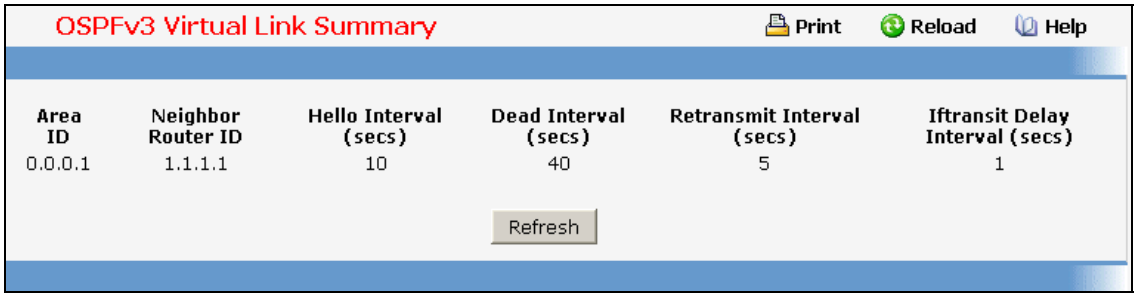
Metric - The metric value used by the Virtual Link.

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 - Removes the specified virtual link from the router configuration.

11.6.7.11 Viewing OSPFv3 Virtual Link Summary Page



Non-Configurable Data

Area ID - The Area ID portion of the virtual link identification for which data is to be displayed. The Area ID and Neighbor Router ID together define the virtual link.

Neighbor Router ID - The neighbor portion of the virtual link identification. Virtual links may be configured between any pair of area border routers having interfaces to a common (non-backbone) area.

Hello Interval - The OSPFv3 hello interval for the virtual link in units of seconds.

Dead Interval - The OSPFv3 dead interval for the virtual link in units of seconds. This determiness how long a router will wait to see a neighbor router's Hello packets before declaring that the router is down.

Retransmit Interval - The OSPFv3 retransmit interval for the virtual link in units of seconds. This specifies the time 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.

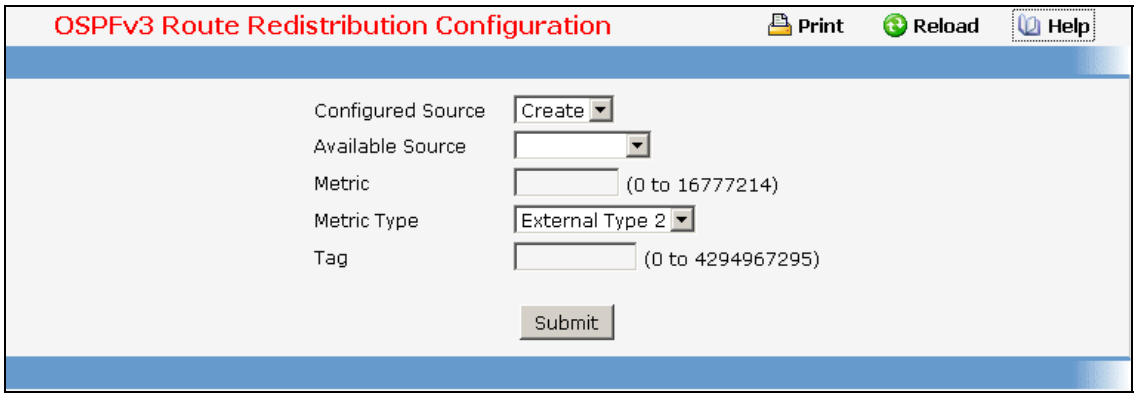
Iftransit Delay Interval - The OSPFv3 Transit Delay for the virtual link in units of seconds. It specifies the estimated number of seconds it takes to transmit a link state update packet over this interface.

Command Buttons

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

11.6.7.12 Configuring OSPFv3 Route Redistribution Configuration Page

This screen can be used to configure the OSPFv3 Route Redistribution parameters. The allowable range for each field is displayed next to it. If an invalid value is entered in one or multiple fields, an alert message will be displayed with the list of all the valid values.



Configurable Data

Configured Source - This dynamic select list is populated by only those Source Protocols that have already been configured for redistribution by OSPFv3. However, the topmost option in the select box is "Create", and this allows the user to configure another, among the Available Source Protocols. The valid values are 'Static' and 'Connected'. An additional 'Create' option is also available.

Available Source - This dynamic select list is populated by only those Source Protocols that have not previously been configured for redistribution by OSPFv3. This select box would appear only if the user selects "Create" option as Configured Source. The valid values are 'Static' or 'Connected'.

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 16777214)

Metric Type - Sets the OSPFv3 metric type of redistributed routes.

Tag - Sets the tag field in routes redistributed. This field displays the tag if the source was pre-configured, else a default tag value of 0 is displayed. The valid values are (0 to 4294967295)

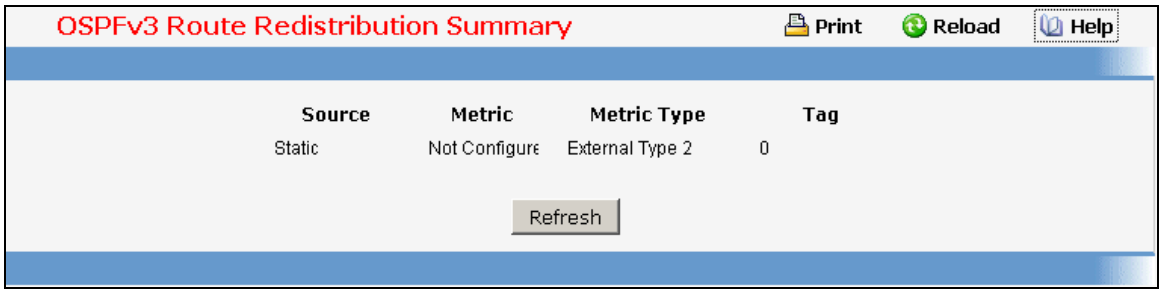
Command Buttons

Submit - Send the updated configuration to the router. Configuration changes take effect immediately.

Delete - Delete the entry of the Source Protocol selected as Configured Source from the list of Sources configured for OSPFv3 Route Redistribution.

11.6.7.13 Viewing OSPFv3 Route Redistribution Summary Page

This screen displays the OSPFv3 Route Redistribution Configuration Summary.



Non-Configurable Data

Source - The Source Protocol to be Redistributed by OSPFv3.

Metric- The Metric of redistributed routes for the given Source Protocol.

Metric Type - The OSPFv3 metric type of redistributed routes.

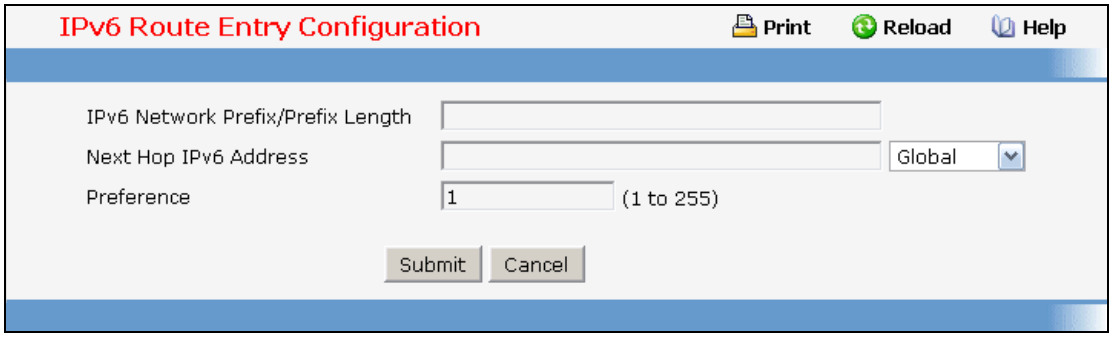
Tag - The tag field in routes redistributed.

Command Buttons

Refresh - Displays the latest OSPFv3 Route Redistribution Configuration data.

11.6.8 Managing IPv6 Routes

11.6.8.1 Configuring IPv6 Route Entry Configuration Page



Selection Criteria

Global or Link-local Next-hop - Specify if the Next Hop IPv6 Address is a Global IPv6 Address or a Link-local IPv6 Address.

Slot/Port - Enter the unit, slot and port number for the Link-local IPv6 Next Hop Address. This field is displayed only if the Global or Link-local Next-hop Selector is selected as Link-local.

Configurable Data

IPv6 Network Prefix/PrefixLength - Enter an IPv6 Network Address with Prefix Length.

Next Hop IPv6 Address - Enter an IPv6 Next Hop Address. If the Next Hop IPv6 Address specified is a Link-local IPv6 Address, specify the Slot/Port for the Link-local IPv6 Next Hop Address.

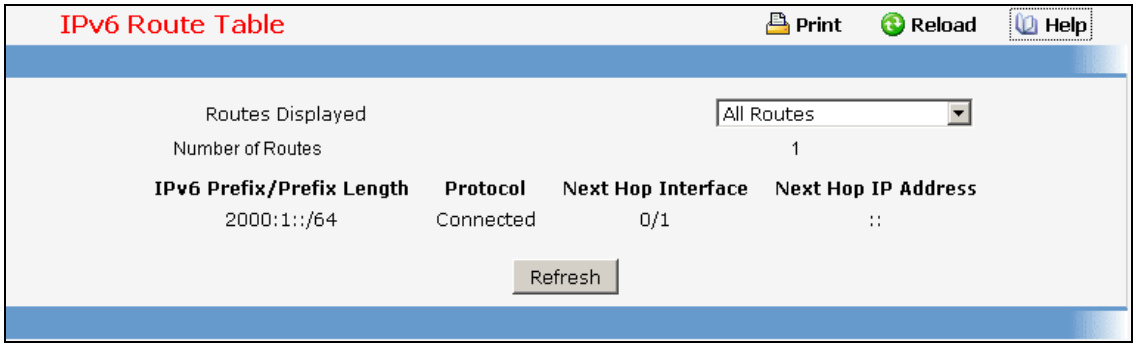
Preference - Enter a Preference Value for the given route.

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.

Cancel - Discards the changes made on the page and navigates back to the referring page.

11.6.8.2 Viewing IPv6 Route Table Information Page



Selection Criteria

Routes Displayed -

- Configured Routes - Shows the routes configured by the user
- Best Routes - Shows only the best active routes

- All Routes - Shows all active IPv6 routes

Non-Configurable Data

Number of Routes/Best Routes - Displays the total number of active routes/best routes in the route table.

IPv6 Prefix/Prefix Length - Displays the Network Prefix and Prefix Length for the Active Route.

Protocol - Displays the Type of Protocol for the Active Route.

Next Hop Slot/Port - Displays the Interface over which the Route is Active.

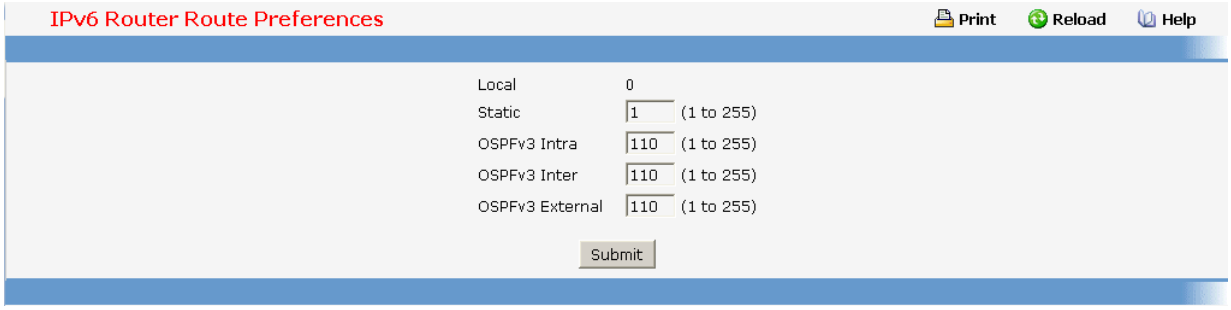
Next Hop IP - Displays the Next Hop IPv6 Address for the Active Route.

Command Buttons

Refresh - Reloads the data on the page.

11.6.8.3 Configuring IPv6 Router Route Preference Page

Use this panel to configure the default preference for each protocol. 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 you must configure different preference values for each of the protocols.



Configurable Data

Static - The Static Route preference value for the router. The default value is 1. The range is 1 to 255.

OSPFv3 Intra - The OSPFv3 intra route preference value in the router. The default value is 110. The range is 1 to 255.

OSPFv3 Inter - The OSPFv3 inter route preference value in the router. The default value is 110. The range is 1 to 255.

OSPFv3 External - The OSPFv3 External route preference value in the router. The default value is 110. The range is 1 to 255.

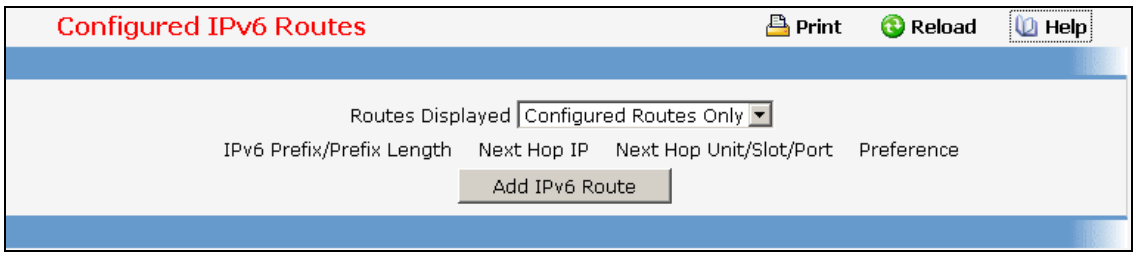
Non-Configurable Data

Local - Local preference.

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.

11.6.8.4 Configuring IPv6 Routes Configuration Page



Selection Criteria

Routes Displayed -

- Configured Routes - Shows the routes configured by the user
- Best Routes - Shows only the best active routes
- All Routes - Shows all active IPv6 routes

Non-Configurable Data

IPv6 Prefix/Prefix Length - Displays the Network Prefix and Prefix Length for the Configured Route.

Next Hop IP - Displays the Next Hop IPv6 Address for the Configured Route.

Preference - Displays the Route Preference of the Configured Route.

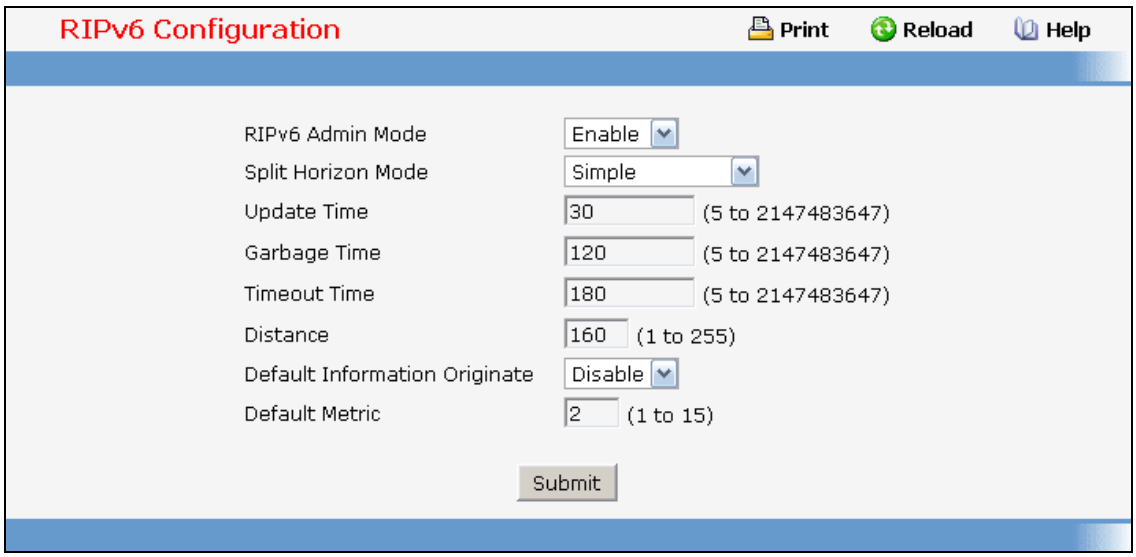
Command Buttons

Add IPv6 Route - Allows the user to configure a new route.

Delete - Deletes the corresponding route.

11.6.9 Managing RIPv6

11.6.9.1 Configuring RIPv6 Configuration Page



Configurable Data

RIPv6 Admin Mode - Select enable or disable from the pulldown menu. If you select enable RIPv6 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.

Update Time - Configure the Ripng update time.

Garbage Time - Configure the Ripng garbage time.

Timeout Time - Configure the Ripng timeout time.

Distance - Configure the Ripng distance.

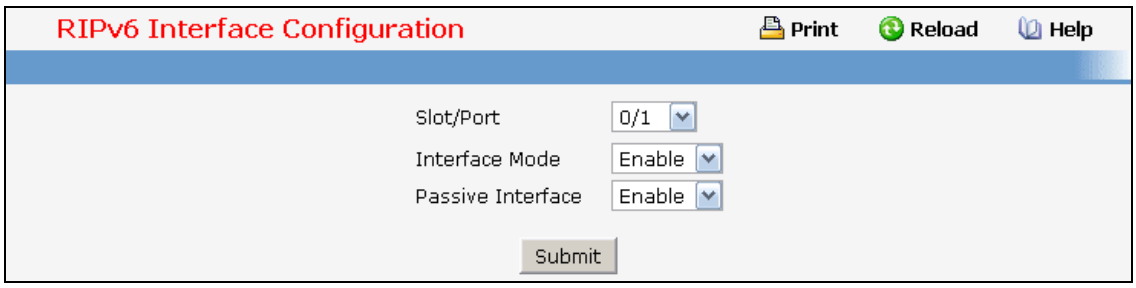
Default Information Originate - Enable or Disable Default Route Advertise.

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.

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.

11.6.9.2 Configuring RIPv6 Interface Configuration Page



Selection Criteria

Slot/Port - Select the interface for which data is to be configured.

Configurable Data

Interface Mode - Select enable or disable from the pulldown menu. Before you enable RIPv6 version 1 or version 1c on an interface, you must first enable network directed broadcast mode on the corresponding interface. The default value is disabled.

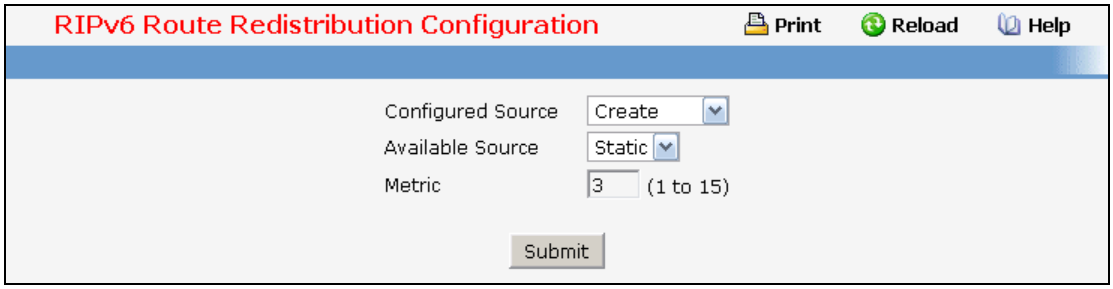
Passive Interface - Select enable or disable from the pulldown menu. The default value is disabled.

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.

11.6.9.3 Configuring RIPv6 Redistribution Configuration Page

This screen can be used to configure the RIPv6 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 RIPv6. 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

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 RIPv6. This select box would appear only if the user selects "Create" option as Configured Source. The valid values are

Static

Connected

OSPF

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.

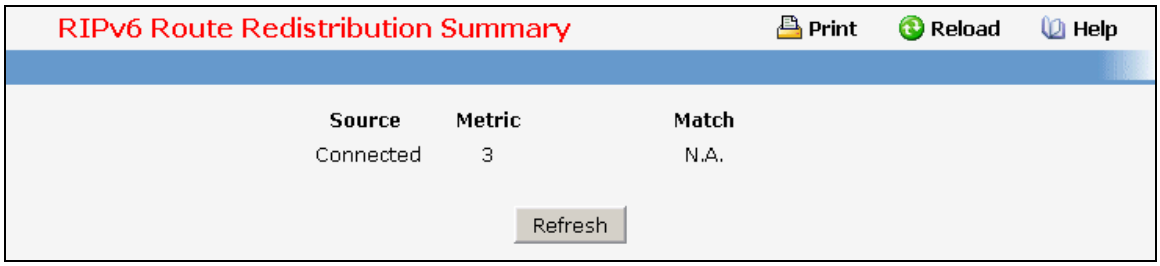
Command Buttons

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 RIPv6 Route Redistribution.

11.6.9.4 Configuring RIPv6 Route Redistribution Summary Page

This screen displays the RIPv6 Route Redistribution Configurations.



Non-Configurable Data

Source - The Source Route to be Redistributed by RIPv6.

Metric - The Metric of redistributed routes for the given Source Route. Displays "Unconfigured" when not configured.

Command Buttons

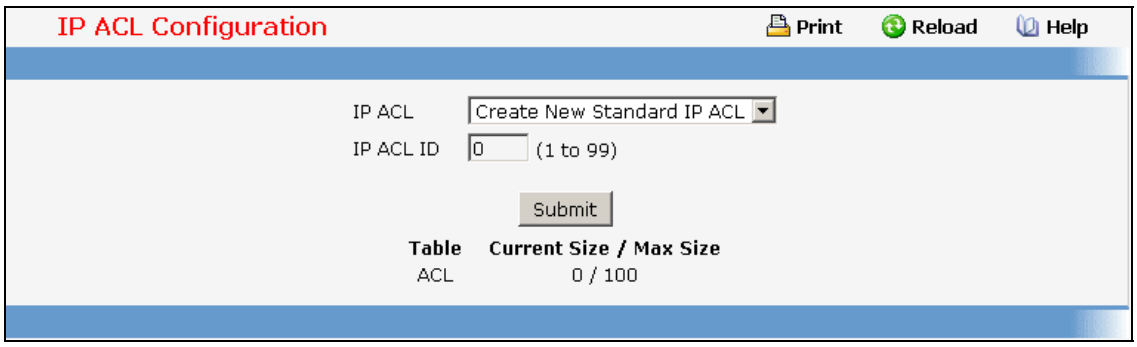
Refresh - Displays the latest RIPv6 Route Redistribution Configuration data.

11.7 QOS Menu

11.7.1 Managing Access Control Lists

11.7.1.1.1 Configuring IP Access Control List Configuration Page

An IP 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 IP ACL applies must be specified, as well as whether it applies to inbound traffic. Rules for the IP ACL are specified/created using the IP ACL Rule Configuration menu.



Selection Criteria

IP ACL - Make a selection from the pulldown menu. A new IP Access Control List may be created or the configuration of an existing IP ACL can be updated.

Configurable Data

IP ACL ID - IP ACL ID must be a whole number in the range of 1 to 99 for IP Standard Access Lists and 100 to 199 for IP Extended Access Lists.

IP ACL Name - Specifies IP ACL Name string which includes alphanumeric characters only. The name must start with an alphabetic character. This field displays the name of the currently selected IP ACL if the ACL has already been created.

Non-Configurable Data

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

Current Size - The current number of IP ACLs.

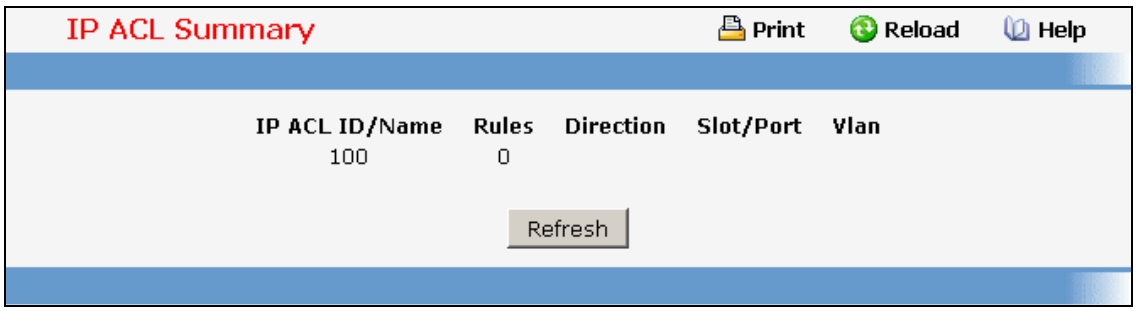
Max Size - The maximum number of IP ACLs.

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 - Removes the currently selected IP ACL from the switch configuration.

11.7.1.2 Viewing IP Access Control List Summary Page



Non-Configurable Data

IP ACL ID - The IP ACL identifier.

Rules - The number of rules currently configured for the IP ACL.

Direction - The direction of packet traffic affected by the IP ACL.
Direction can only be:

- Inbound

Slot/Port(s) - The interfaces to which the IP ACL applies.

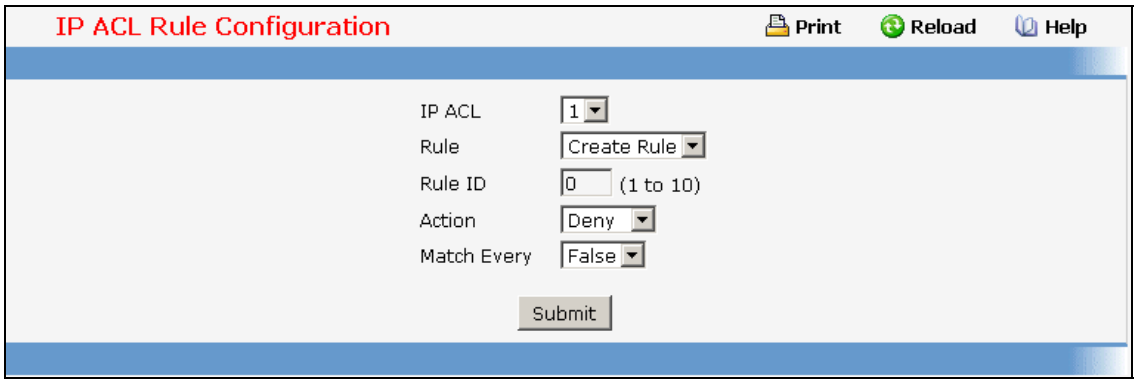
VLAN(s) - VLAN(s) to which the IP ACL applies.

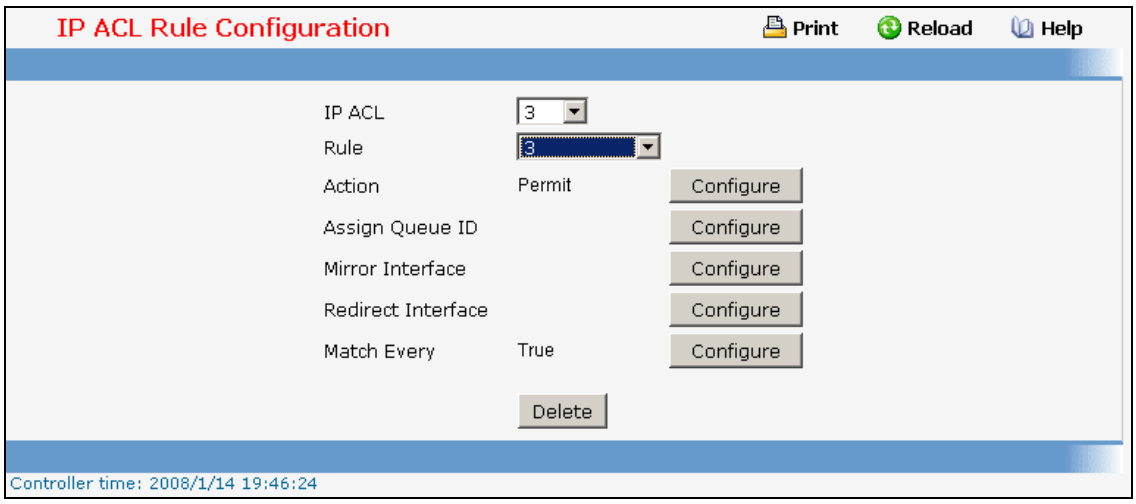
Command Buttons

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

11.7.1.3 Configuring IP Access Control List Rule Configuration Page

Use these screens to configure the rules for the IP Access Control Lists created using the IP Access Control List Configuration screen. What is shown on this screen varies depending on the current step in the rule configuration process. A Standard/Extended IP 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.





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 8 that will be used to identify the rule. An IP ACL may have up to 8 rules.

Action - Specify what action should be taken if a packet matches the rule's criteria. The choices are permit or deny.

Logging - When set to 'True', logging is enabled for this ACL rule (subject to resource availability in the device). If the Access List Trap Flag is also enabled, this will cause periodic traps to be generated indicating the number of times this rule was 'hit' during the current report interval. A fixed 5 minute report interval is used for the entire system. A trap is not issued if the ACL rule hit count is zero for the current interval. This field is visible for a 'Deny' Action.

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 6). This field is visible when 'Permit' is chosen as 'Action'.

Mirror Interface - Specifies the specific egress interface where the matching traffic stream is copied in addition to being forwarded normally by the device. This field cannot be set if a Redirect Interface is already configured for the ACL rule. This field is visible for a 'Permit' 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 Wildcard 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.

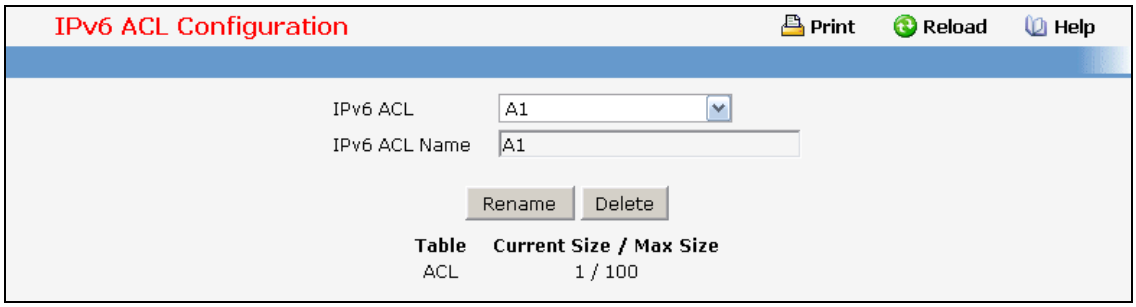
Command Buttons

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.

11.7.1.4 Configuring IPv6 Access Control List Configuration Page

An IPv6 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 IPv6 ACL applies must be specified, as well as whether it applies to inbound or outbound traffic. Rules for the IPv6 ACL are specified/created using the IPv6 ACL Rule Configuration menu.



Selection Criteria

IPv6 ACL - A new IPv6 ACL may be created or the configuration of an existing IPv6 ACL can be updated by selecting right option from the pull down menu.

Configurable Data

IPv6 ACL Name - Specifies IPv6 ACL Name string which includes alphanumeric characters only. The name must start with an alphabetic character. This field displays the name of the currently selected IPv6 ACL if the ACL has already been created.

Non-Configurable Data

Table - Displays the current and maximum number of ACLs.

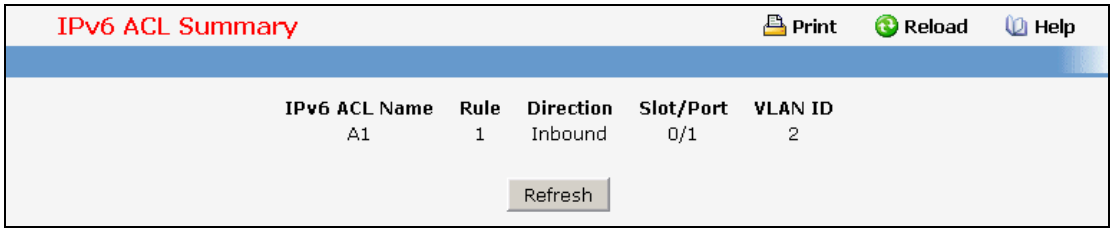
Command Buttons

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.

Rename - Rename the currently selected IPv6 ACL.

Delete - Removes the currently selected IPv6 ACL from the switch configuration.

11.7.1.5 IPv6 Access Control List Summary Page



Non-Configurable Data

IPv6 ACL Name - Exiting IPv6 ACL identifier.

Rules - The number of rules currently configured for the IPv6 ACL.

Direction - The direction of packet traffic affected by the IPv6 ACL.
Direction can only be one of the following:

Inbound

Slot/Port(s) - The interfaces to which the IPv6 ACL applies.

VLAN(s) - VLAN(s) to which the IPv6 ACL applies.

Command Buttons

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

11.7.1.6 IPv6 Access Control List Rule Configuration Page

Use these screens to configure the rules for the IPv6 Access Control Lists, which is created using the IPv6 Access Control List Configuration screen. By default, no specific value is in effect for any of the IPv6 ACL rules.

Selection Criteria

IPv6 ACL Name - Use the pull down menu to select the IPv6 ACL for which to create or update a rule.

Rule - Select an existing rule from the pull down menu, or select 'Create 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 10) 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.

Logging - When set to 'True', logging is enabled for this ACL rule (subject to resource availability in the device). If the Access List Trap Flag is also enabled, this will cause periodic traps to be generated indicating the number of times this rule was 'hit' during the current report interval. A fixed 5 minute report interval is used for the entire system. A trap is not issued if the ACL rule hit count is zero for the current interval. This field is visible for a 'Deny' Action.

Assign Queue ID - Specifies the hardware egress queue identifier used to handle all packets matching this IPv6 ACL rule. Valid range of Queue Ids is (0 to 7). This field is visible for a 'Permit' Action.

Mirror Interface - Specifies the specific egress interface where the matching traffic stream is copied in addition to being forwarded normally by the device. This field cannot be set if a Redirect Interface is already configured for the ACL rule. This field is visible for a 'Permit' 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 cannot be set if a Mirror Interface is already configured for the ACL rule. This field is visible for a 'Permit' Action.

Match Every - Select true or false from the pull down menu. True signifies that all packets will match the selected IPv6 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 - There are two ways to configure IPv6 protocol.

Specify an integer ranging from 0 to 255 after selecting protocol keyword "other". This number represents the IP protocol

Select name of a protocol from the existing list of Internet Protocol (IP), Transmission Control Protocol (TCP), User Datagram Protocol (UDP), Internet Control Message Protocol (ICMPv6).

Source Prefix / PrefixLength - Specify IPv6 Prefix combined with IPv6 Prefix length of the network or host from which the packet is being sent. Prefix length can be in the range (0 to 128).

Source L4 Port - Specify a packet's source layer 4 port as a match condition for the selected IPv6 ACL rule. Source port information is optional. Source port information can be specified in two ways:

Select keyword "other" from the drop down menu and specify the number of the port in the range from 0 to 65535.

Select one of the keyword from the list: 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.

Destination Prefix / PrefixLength - Enter up to 128-bit prefix combined with prefix length to be compared to a packet's destination IP Address as a match criteria for the selected IPv6 ACL rule. Prefix length can be in the range (0 to 128).

Destination L4 Port Keyword - Specify the destination layer 4 port match conditions for the selected IPv6 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 IPv6 ACL rule. This is an optional configuration.

Flow Label - Flow label is 20-bit number that is unique to an IPv6 packet, used by end stations to signify quality-of-service handling in routers. Flow label can specified within the range (0 to 1048575).

IPv6 DSCP Service - 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 IPv6 header. This is an optional configuration. Enter an integer from 0 to 63. The IPv6 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.

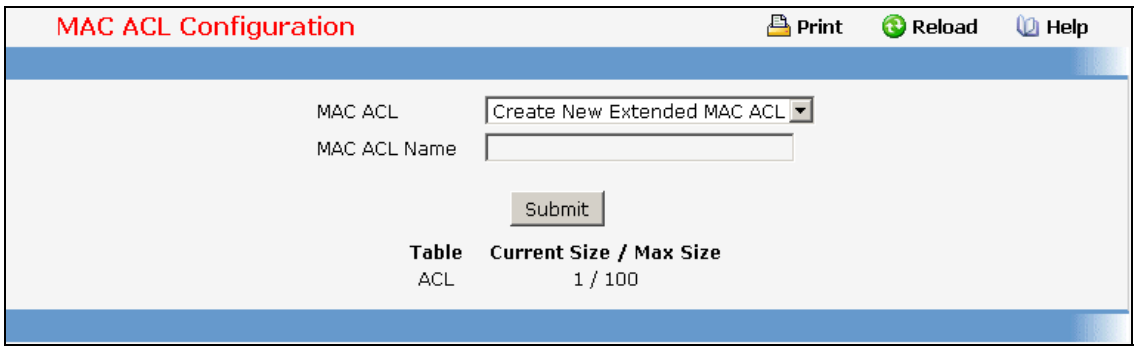
Command Buttons

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.

11.7.1.7 Configuring MAC Access Control List Configuration Page

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.



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.

Non-Configurable Data

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

Current Size - The current number of MAC ACLs.

Max Size - The maximum number of MAC 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.

Rename - Renames the currently selected MAC ACL.

Delete - Removes the currently selected MAC ACL from the switch configuration.

11.7.1.8 Viewing MAC Access Control List Summary Page

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

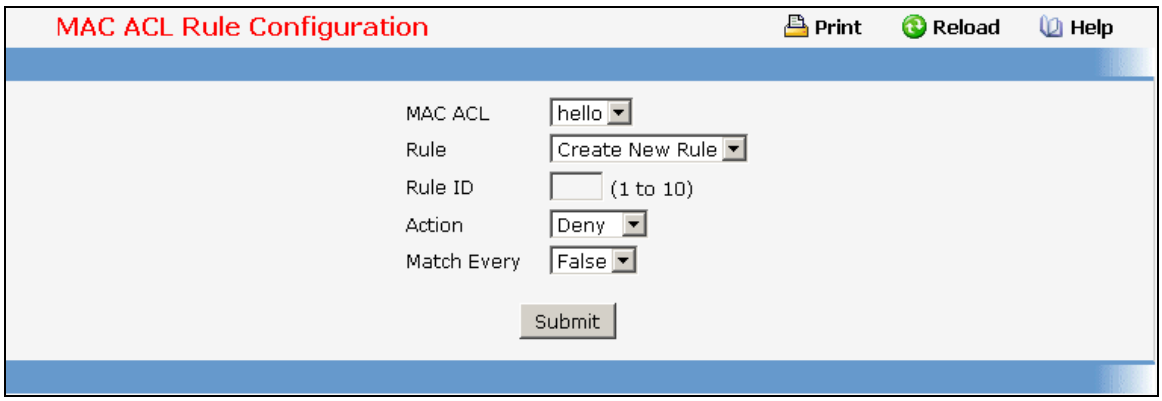
Slot/Port(s) - The interfaces to which the MAC ACL applies.

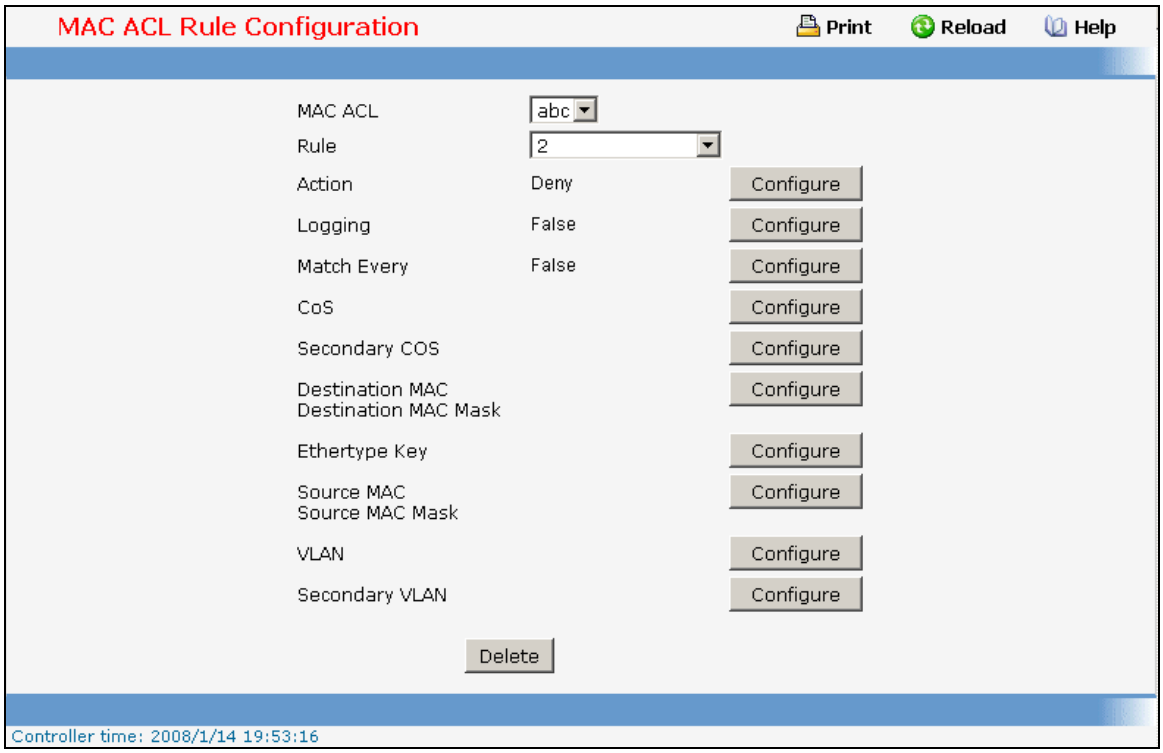
VLAN(s) - VLAN(s) to which the MAC ACL applies.

Command Buttons

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

11.7.1.9 Configuring MAC Access Control List Rule Configuration Page





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 8) 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.

Logging - When set to 'True', logging is enabled for this ACL rule (subject to resource availability in the device). If the Access List Trap Flag is also enabled, this will cause periodic traps to be generated indicating the number of times this rule was 'hit' during the current report interval. A fixed 5 minute report interval is used for the entire system. A trap is not issued if the ACL rule hit count is zero for the current interval. This field is visible for a 'Deny' Action.

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 6).

Mirror Interface - Specifies the specific egress interface where the matching traffic stream is copied in addition to being forwarded normally by the device. This field cannot be set if a Redirect Interface is already configured for the ACL rule. This field is visible for a 'Permit' Action.

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.

Destination MAC Mask - Specifies the destination MAC address mask specifying which bits in the destination MAC 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 mask of 00:00:00:ff:ff:ff.

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).

Source MAC Mask - Specifies the Source MAC address mask specifying which bits in the Source MAC 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 (1 to 3965). 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.

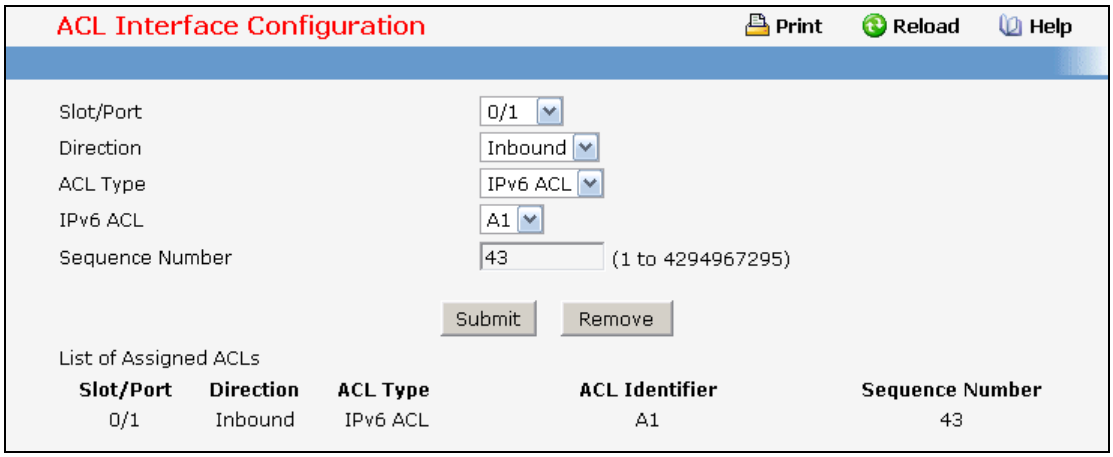
Command Buttons

Configure - Configure the corresponding match criteria for the selected rule.

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.

11.7.1.10 Configuring Access Control List Interface Configuration Page



Selection Criteria

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
- IPv6 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".

IPv6 ACL - Specifies list of all IPv6 ACLs. This field is visible only if the user has selected "IPv6 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".

Configurable Data

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.

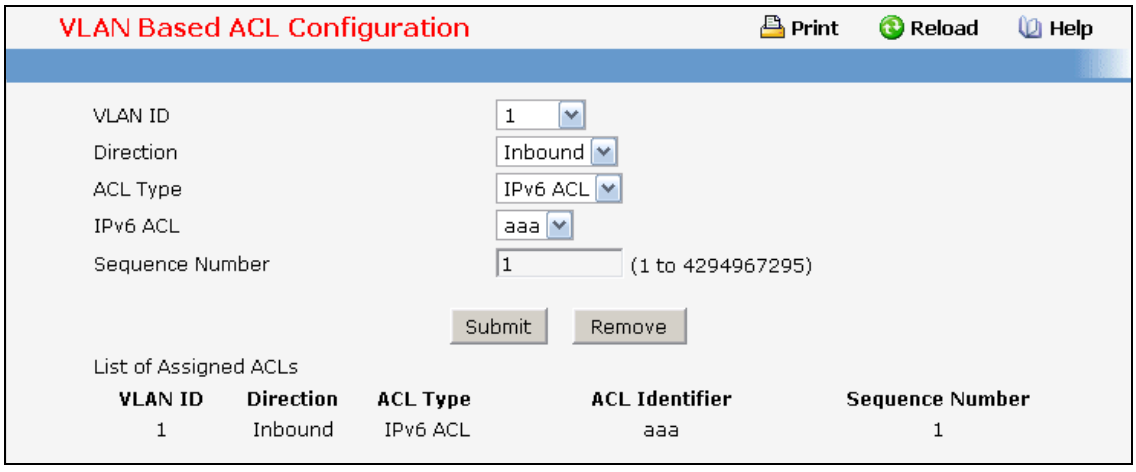
Sequence Number - Displays the Sequence Number signifying the order of specified ACL relative to other ACLs assigned to selected interface and direction.

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.

11.7.1.11 Configuring Access Control List VLAN ACL Configuration Page



Configurable Data

VLAN ID - Specifies list of all configured VLAN Id(s) for ACL mapping.

Direction - Specifies the packet filtering direction for ACL. Valid Directions:

- Inbound

ACL Type - Specifies the type of ACL. Valid ACL Types:

- IP ACL
- IPv6 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".

IPv6 ACL - Specifies list of all IPv6 ACLs. This field is visible only if the user has selected "IPv6 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 VLAN and direction. A lower number indicates higher precedence order. If a sequence number is already in use for this VLAN 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 VLAN and direction will be used. Valid range is (1 to 4294967295).

Non-Configurable Data

Slot/Port - Displays selected interface

VLAN ID(s) - Displays selected VLAN Id.

Direction - Displays selected packet filtering direction for ACL.

ACL Type - Displays the type of ACL assigned to selected VLAN and direction.

ACL Identifier - Displays the ACL Number(in case of IP ACL) or ACL Name(in case of IPv6 ACL and MAC ACL) identifying the ACL assigned to selected VLAN and direction.

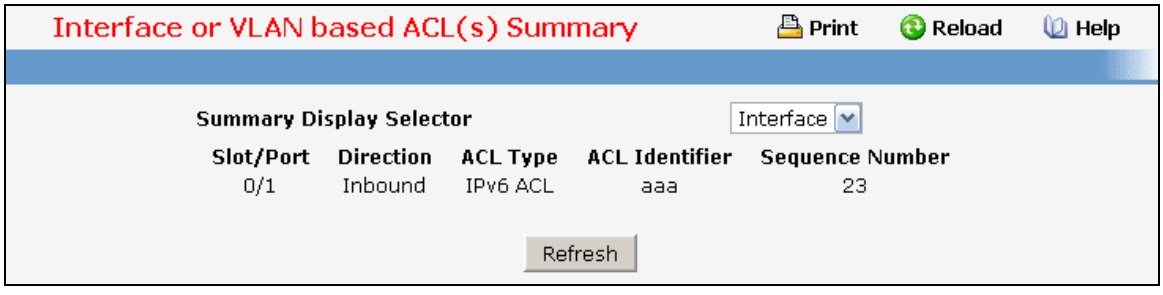
Sequence Number - Displays the Sequence Number signifying the order of specified ACL relative to other ACLs assigned to selected VLAN and direction.

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 VLAN Direction Mapping from the switch configuration.

11.7.1.12 Access Control List VLAN ACL Summary Page



Non-Configurable Data

Summary Display Selector - Select interface or VLAN to display summary. By default summary of Interface-based ACL(s) is displayed.

Slot/Port(s) - The interfaces to which the IP ACL applies.

VLAN(s) - VLAN(s) to which the IP ACL applies.

Direction - The direction of packet traffic affected by the IP ACL.

Direction can only be one of the following:

- Inbound

ACL Type - Displays the type of ACL assigned to selected VLAN and direction.

ACL Identifier - Displays the ACL Number(in case of IP ACL) or ACL Name(in case of IPv6 ACL and MAC ACL) identifying the ACL assigned to selected VLAN and direction.

Sequence Number - Displays the Sequence Number signifying the order of specified ACL relative to other ACLs assigned to selected VLAN and direction.

Command Buttons

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

11.7.2 Managing Differentiated Services

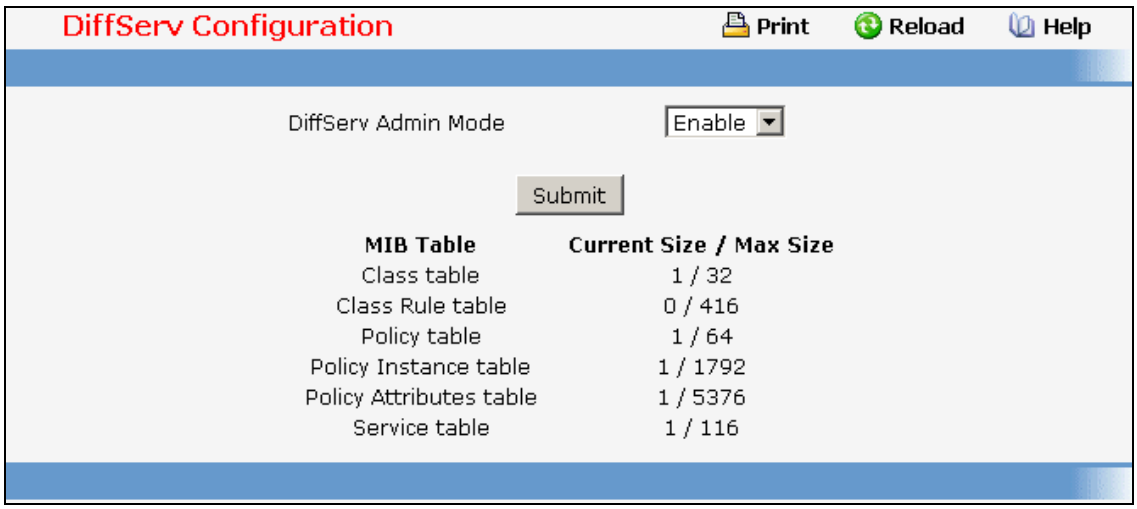
11.7.2.1 Defining DiffServ Configuration Page

Operation

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.



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.

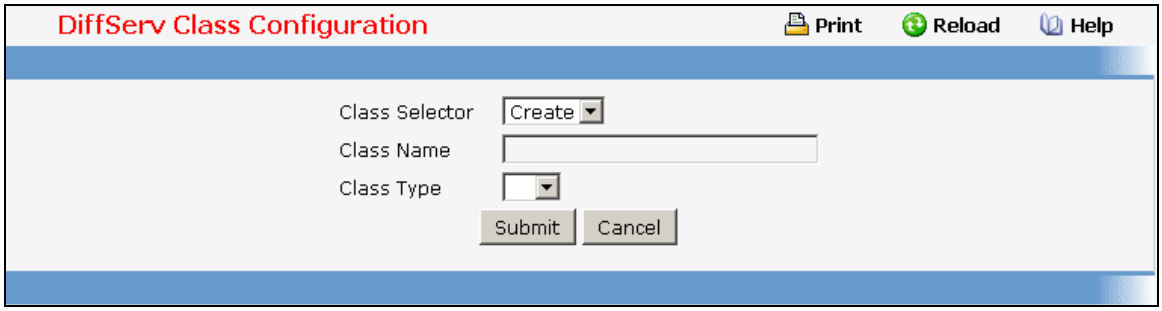
Policy Attributes table - Displays the number of configured policy attributes (attached to the policy class instances) out of the total allowed on the switch.

Service table - Displays the number of configured services (attached to the policies on specified interfaces) out of the total allowed on the switch.

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.

11.7.2.2 Configuring DiffServ Class Configuration Page



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. Options:

- All

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 Layer 3 Protocol - Indicates how to interpret the any layer 3. This lists types of packets supported by Diffserv. Layer 3 Protocol option is available only when user selects class type as 'All' . Options:

- IPv4
- IPv6

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, is this field 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.

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.

Cancel - Cancel the currently selected filter.

Delete - Delete the currently selected filter.

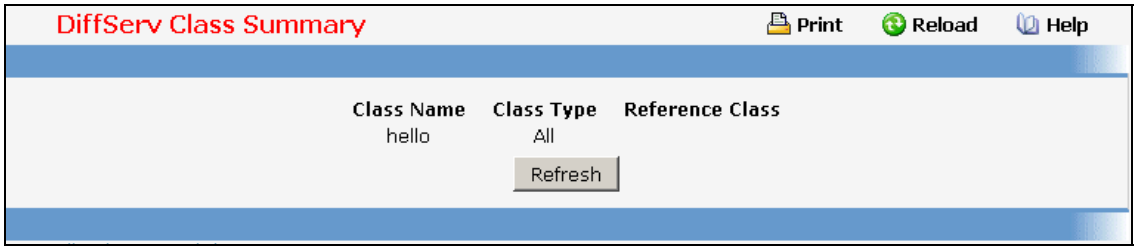
Rename - Allows to rename a specified class.

Add Match Criteria - Only one match criterion can be specified each time this button is invoked. Based on the selected match criterion, an individual match criterion screen is provided to configure its value.

Match criteria cannot be deleted from a class. The class must be deleted in order to remove the match criteria.

Remove Class Reference - This button appears on the screen only if a specified class references another class. The current class reference, of the specified class, is removed by invoking this button.

11.7.2.3 Viewing DiffServ Class Summary Page



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 - Displays name of the configured class of type

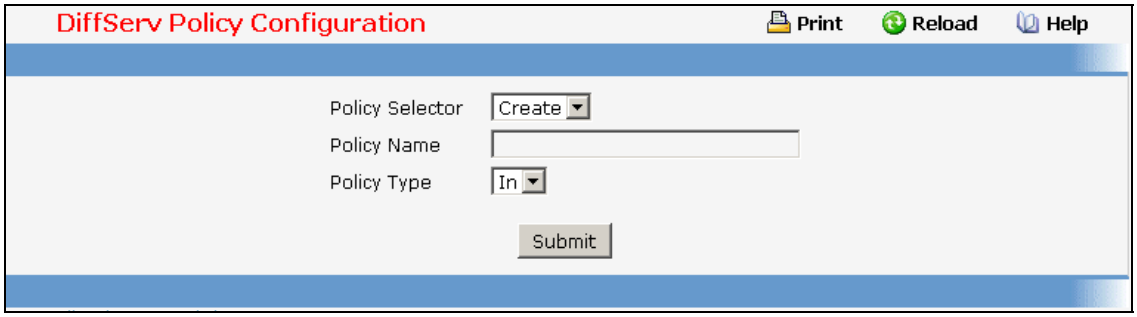
- All

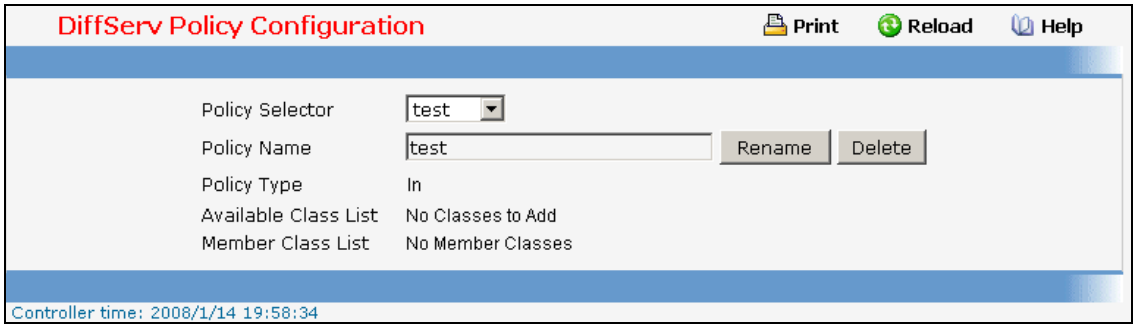
referenced by the specified class of the same type.

Command Buttons

Refresh - Refresh the currently selected filter.

11.7.2.4 DiffServ Policy Configuration Page





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 - *In* indicates the type is specific to inbound 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 - *In* indicates the type is specific to inbound 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.

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, is this field 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 is this field a selector field. After creation of the policy class instance this becomes a non-configurable field.

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.

Delete - Delete the currently selected filter.

Rename - Allows to rename a specified policy.

Add Selected Class - Creates a policy class instance by attaching the policy to the specified class.

Remove Selected Class - Removes a policy class instance by detaching the policy from the specified class.

11.7.2.5 Viewing DiffServ Policy Summary Page

Non-Configurable Data

Policy Name - Displays name of the DiffServ policy.

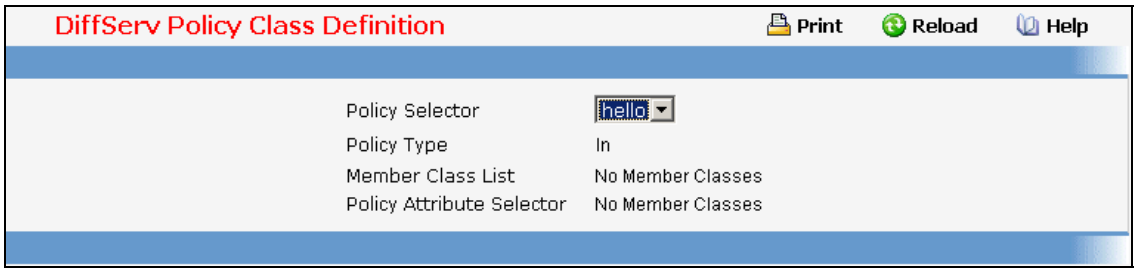
Policy Type - Displays type of the policy as 'In'.

Member Classes - Displays name of each class instance within the policy.

Command Buttons

Refresh – Refresh the currently selected filter.

11.7.2.6 Configuring DiffServ Policy Class Definition Page



Selection Criteria

Policy Selector - This lists all the existing DiffServ policy names, from which one can be selected.

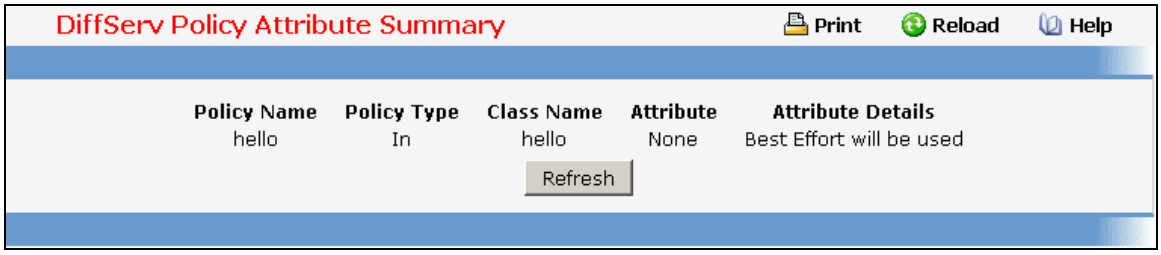
Member Class List - This lists all existing DiffServ classes currently defined as members of the specified Policy, from which one can be selected. This list is automatically updated as a new class is added to or removed from the policy.

Policy Attribute Selector - This lists all attributes supported for this type of policy, from which one can be selected.

Non-Configurable Data

Policy Type - Displays type of the configured policy as 'In'.

11.7.2.7 Viewing DiffServ Policy Attribute Summary Page



Non-Configurable Data

Policy Name - Displays name of the specified DiffServ policy.

Policy Type - Displays type of the specified policy as 'In'.

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.

Command Buttons

Refresh - Refresh the displayed data.

11.7.2.8 Configuring DiffServ Service Configuration Page

Selection Criteria

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.

Direction - Select the traffic direction of this service interface. This selection is only available to Read/Write users when Slot/Port is specified as 'All'.

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.

Non-Configurable Data

This information is only displayed when Slot/Port is specified as 'All'.

Slot/Port - Shows the Slot/Port that uniquely specifies an interface.

Direction - Shows that the traffic direction of this service interface is In.

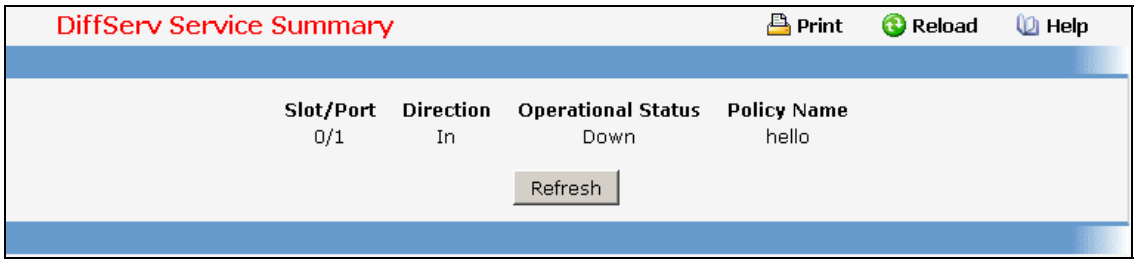
Operational Status - Shows the operational status of this service interface, either Up or Down.

Policy Name - Shows the name of the attached policy.

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.

11.7.2.9 Viewing DiffServ Service Summary Page



Non-Configurable Data

Slot/Port - Shows the Slot/Port that uniquely specifies an interface.

Direction - Shows that the traffic direction of this service interface is In.

Operational Status - Shows the operational status of this service interface, either Up or Down.

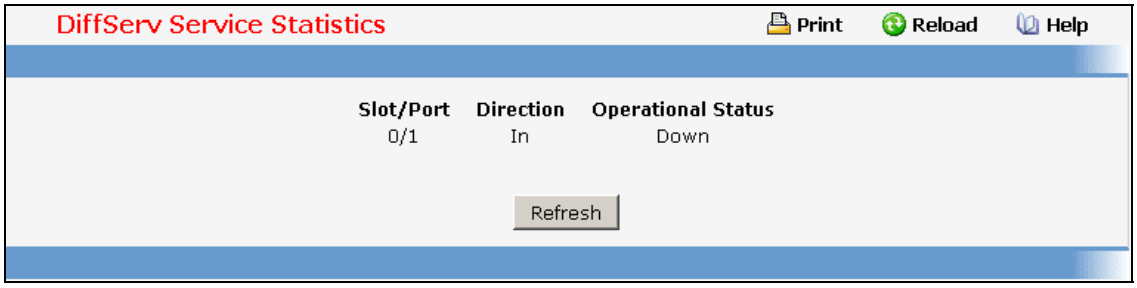
Policy Name - Shows the name of the attached policy.

Command Buttons

Refresh - Refresh the displayed data.

11.7.2.10 Viewing DiffServ Service Statistics Page

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).



Non-Configurable Data

Slot/Port - Shows the Slot/Port that uniquely specifies an interface.

Direction - Shows that the traffic direction of this service interface is In.

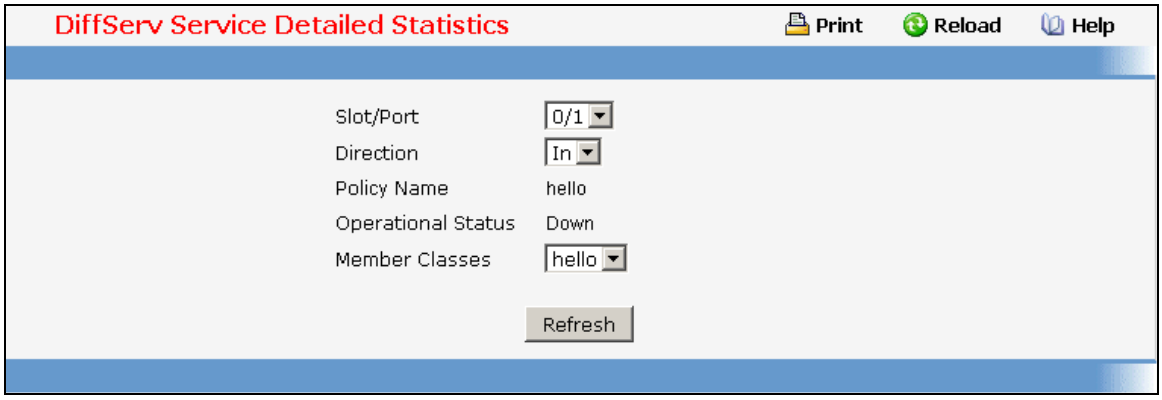
Operational Status - Shows the operational status of this service interface, either Up or Down.

Command Buttons

Refresh - Refresh the displayed data.

11.7.2.11 Viewing DiffServ Service Detailed Statistics Page

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

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. 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.

Command Buttons

Refresh - Refresh the displayed data.

11.7.3 Configuring Diffserv Wizard Page

Operation

The DiffServ Wizard enables DiffServ on the switch by creating a traffic class, adding the traffic class to a policy, and then adding the policy to the ports selected on DiffServ Wizard page. The DiffServ Wizard will:

Create a DiffServ Class and define match criteria used as a filter to determine if incoming traffic meets the requirements to be a member of the class.

Set the DiffServ Class match criteria based on Traffic Type selection as below:

VOIP - sets match criteria to UDP protocol.

HTTP - sets match criteria to HTTP destination port.

FTP - sets match criteria to FTP destination port.

Telnet - sets match criteria to Telnet destination port.

Any - sets match criteria to all traffic.

Create a DiffServ Policy and adds the DiffServ Policy to the DiffServ Class created.

If Policing is set to YES, then DiffServ Policy style is set to Simple. Traffic which conforms to the Class Match criteria will be processed according to the Outbound Priority selection. Outbound Priority configures the handling of conforming traffic as below:

High - sets policing action to markdscp ef.

Med - sets policing action to markdscp af31.

Low - sets policing action to send.

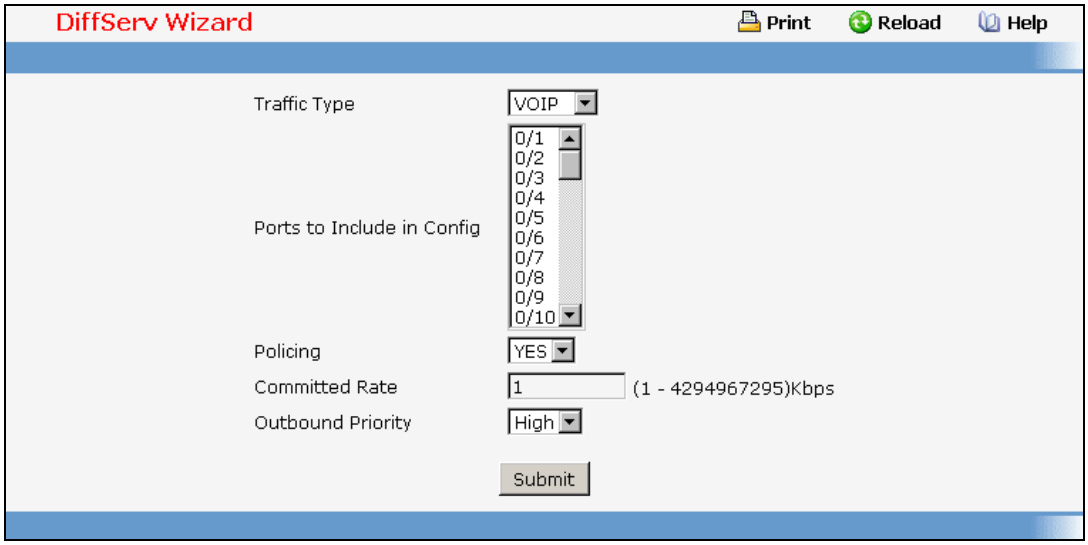
If Policing is set to NO, then all traffic will be marked as specified below:

High - sets policy mark ipdscp ef.

Med - sets policy mark ipdscp af31.

Low - sets policy mark ipdscp be.

Each port selected will be added to the policy created.



Selection Criteria

Traffic Type - Traffic type is used to define the DiffServ Class. Traffic type options: VOIP, HTTP, FTP, Telnet, and Any.

Policing - Enabling policing will add policing to the DiffServ Policy and the policing rate will be applied.

Outbound Priority - When Policing is enabled, Outbound Priority defines the type of policing conform action where: High sets action to markdscp ef, Med sets action to markdscp af31, and Low sets action to send. When Policing is disabled, Outbound Priority defines the policy where: High sets policy to mark ipdscp ef, Med sets policy to mark ipdscp af31, Low set policy to mark ipdscp be.

Configurable Data

Ports to Include in Config - List the ports which can be configured to support a DiffServ policy. The DiffServ policy will be added to selected ports.

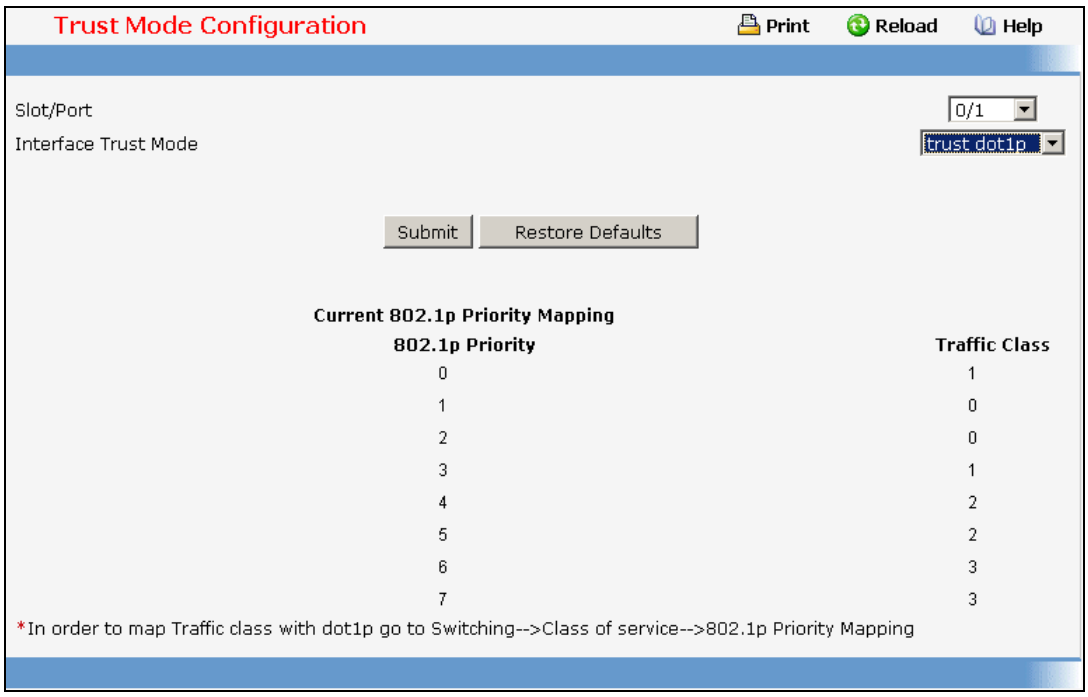
Committed Rate - When Policing is enabled, the committed rate will be applied to the policy and the policing action is set to conform. When Policing is disabled, the committed rate is not applied and the policy is set to markdscp.

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 operation is performed.

11.7.4 Managing Class of Service

11.7.4.1 Configuring Trust Mode Configuration Page



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.

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-dscp

Default value is trust dot1p.

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).

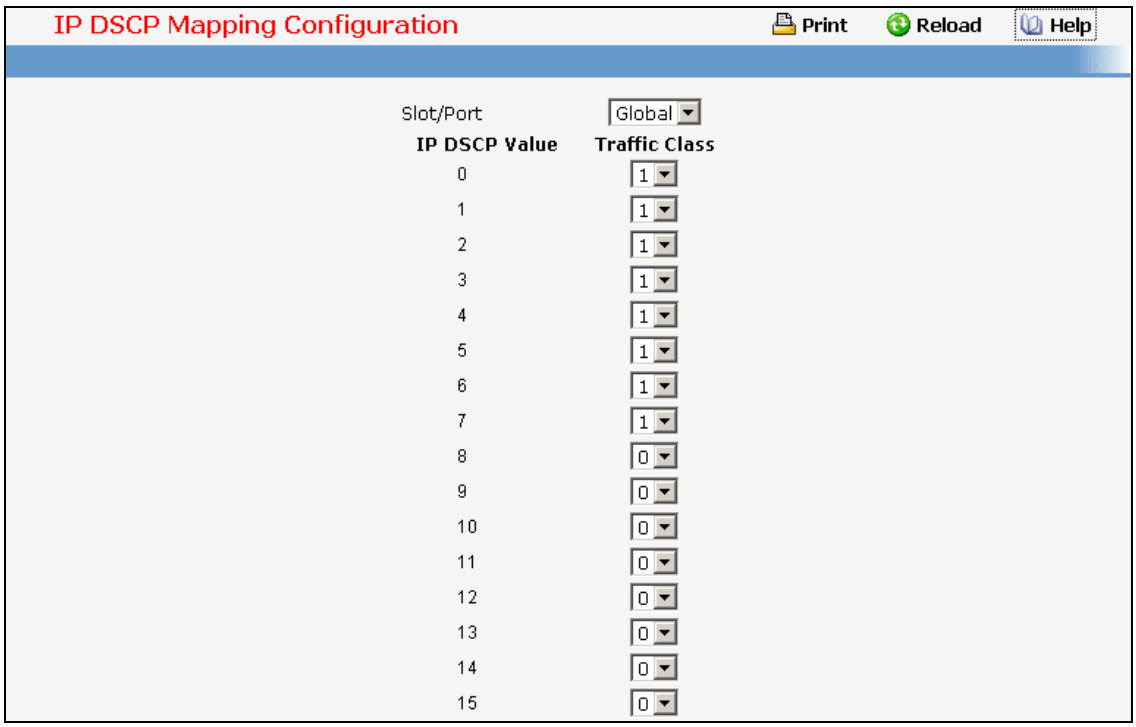
Current 802.1p Priority Mapping - Displays the current 802.1p priority mapping configuration.

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.

11.7.4.2 Managing DSCP Mapping Configuration Page



Selection Criteria

Slot/Port - Specifies all CoS configurable interfaces. The option "Global" represents the most recent global configuration settings.

Configurable Data

IP DSCP Value Traffic Class - Specify which internal traffic class to map the corresponding IP DSCP value. Valid Range is (0 to 7) .

Non-Configurable Data

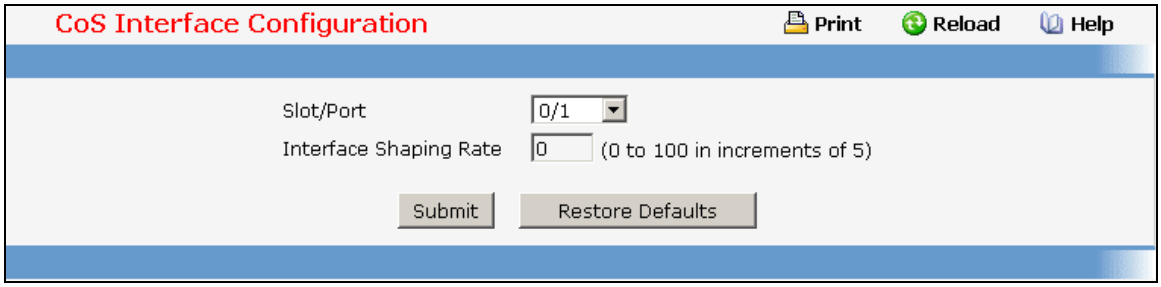
IP DSCP Value - Specify the IP DiffServ Code Point (DSCP) Value.

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.

Restore Defaults - Restores default settings.

11.7.4.3 Configuring CoS interface



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

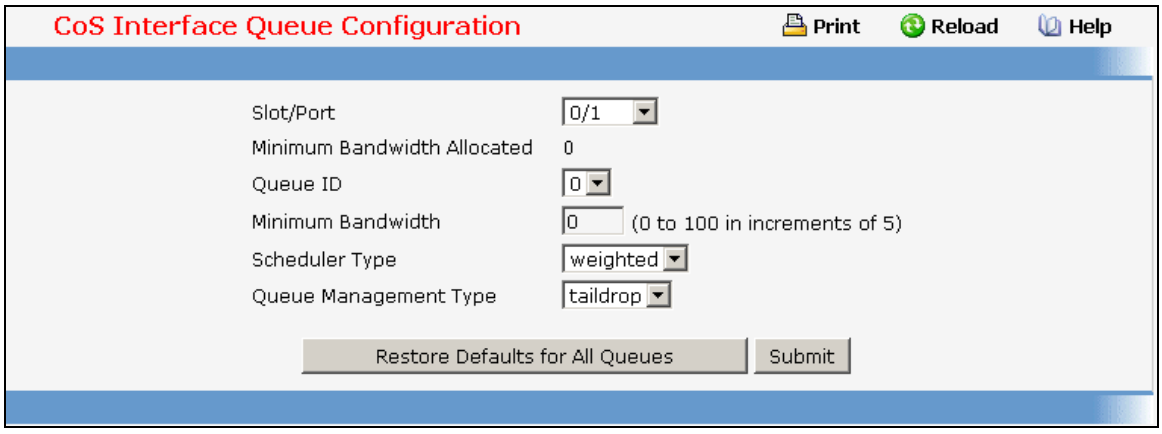
Interface Shaping Rate - Specifies the maximum bandwidth allowed, typically used to shape the outbound transmission rate. This value is controlled independently of any per-queue maximum bandwidth configuration. It is effectively a second-level shaping mechanism. Default value is 0. Valid Range is (0 to 100) in increments of 5 . 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.

11.7.4.4 Configuring CoS interface queue



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).

Scheduler Type - Specifies the type of scheduling used for this queue.
Scheduler Type can only be one of the following:

- strict
- weighted

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:

- taildrop

Default value is taildrop.

Configurable Data

Minimum Bandwidth Allocated - Specifies the sum of individual Minimum Bandwidth values for all queues in the interface. The sum cannot exceed the defined maximum (100). This value is considered while configuring the Minimum Bandwidth for a queue in the selected interface.

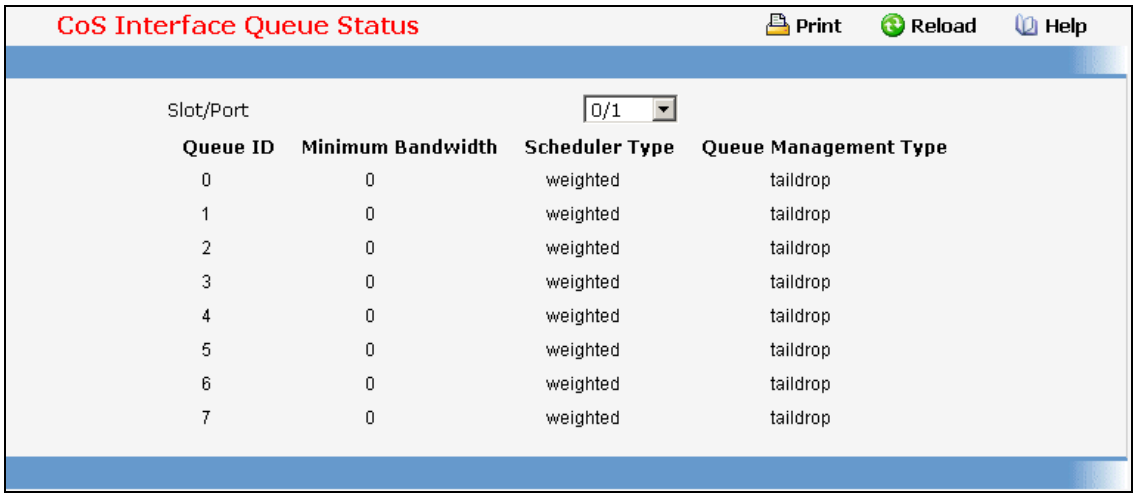
Minimum Bandwidth - Specifies the minimum guaranteed bandwidth allotted to this queue. Setting this value higher than its corresponding Maximum Bandwidth automatically increases the maximum to the same value. Default value is 0. Valid Range is (0 to 100) in increments of 5 . The value 0 means no guaranteed minimum. Sum of individual Minimum Bandwidth values for all queues in the selected interface cannot exceed defined maximum (100).

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.

11.7.4.5 Viewing 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.

Minimum Bandwidth - Specifies the minimum guaranteed bandwidth allotted to this queue. The value 0 means no guaranteed minimum. Sum of individual Minimum Bandwidth values for all queues in the selected interface cannot exceed defined maximum (100).

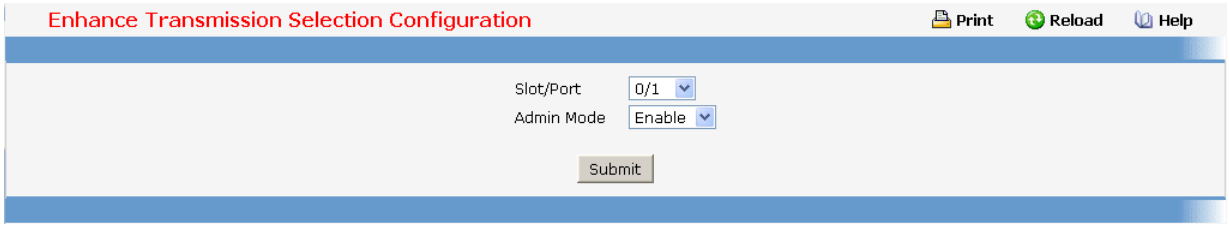
Scheduler Type - Specifies the type of scheduling used for this queue.
Scheduler Type can only be one of the following:

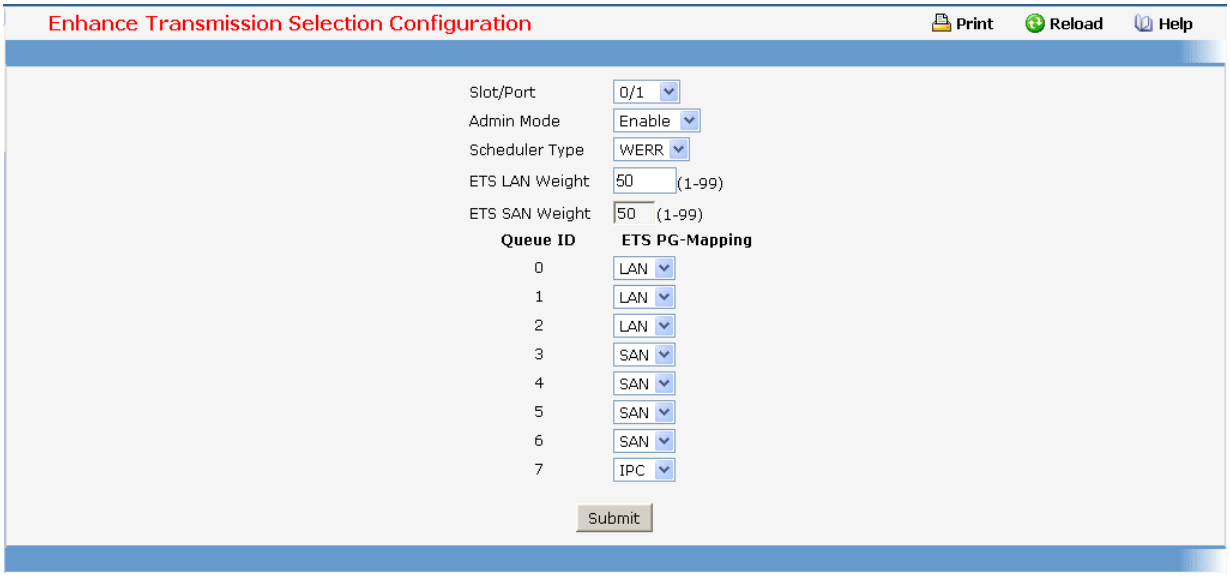
- strict
- weighted

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

11.7.4.6 Configuring Enhanced Transmission Selection (ETS) interface





Selection Criteria

Slot/Port - Choose a ETS configurable interfaces for setting.

Admin Mode - Enable/Disable Enhanced Transmission Selection function.

- **Enable** - Enable ETS, start the ETS process and enable other configuration options.

- **Disable** - Disable ETS and stop the ETS process. Other configuration will not be change if you disable ETS.

The system's default ETS admin mode is disabled

***Scheduler Type** - Configures the scheduler type for an interface.*

- **WERR** - Set scheduler type to WERR.
- **WRR** - Set the scheduler type to WRR.

When the ETS is enabled, the default scheduler type is WERR.

***ETS PG-Mapping** - This command configures the mapping list of priority to priority groups. Choose the CNM generation behavior when congestion notification threshold is reached but the incoming sampled packet does not have CN-TAG.*

- **LAN** - assign specific priority id to LAN priority group.
- **SAN** - assign specific priority id to SAN priority group.
- **IPC** - assign specific priority id to IPC priority group.

When the ETS is enabled, priority id 0 to 2 are assigned to LAN, priority 3 to 6 are assigned to SAN, and priority 7 is assigned to IPC.

Configurable Data

ETS LAN Weight - Set ETS LAN Weight. The system's default ETS LAN Weight is 50. The valid ETS LAN Weight range is 1 to 99, and ETS LAN Weight plus ETS SAN Weight must equal to 100.

ETS SAN Weight - Set ETS SAN Weight. The system's default ETS SAN Weight is 50. The valid ETS SAN Weight range is 1 to 99, and ETS LAN Weight plus ETS SAN Weight must equal to 100.

Non-Configurable Data

Queue ID - Specifies the queue priority ID.

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.

11.7.4.7 Viewing Enhanced Transmission Selection (ETS) interface status

Non-Configurable Data

Interface - The list of ETS configurable interfaces.

Admin Mode - admin mode of specific interface.

Scheduler Type - scheduler type of specific interface.

ETS LAN Weight - LAN Weight of specific interface.

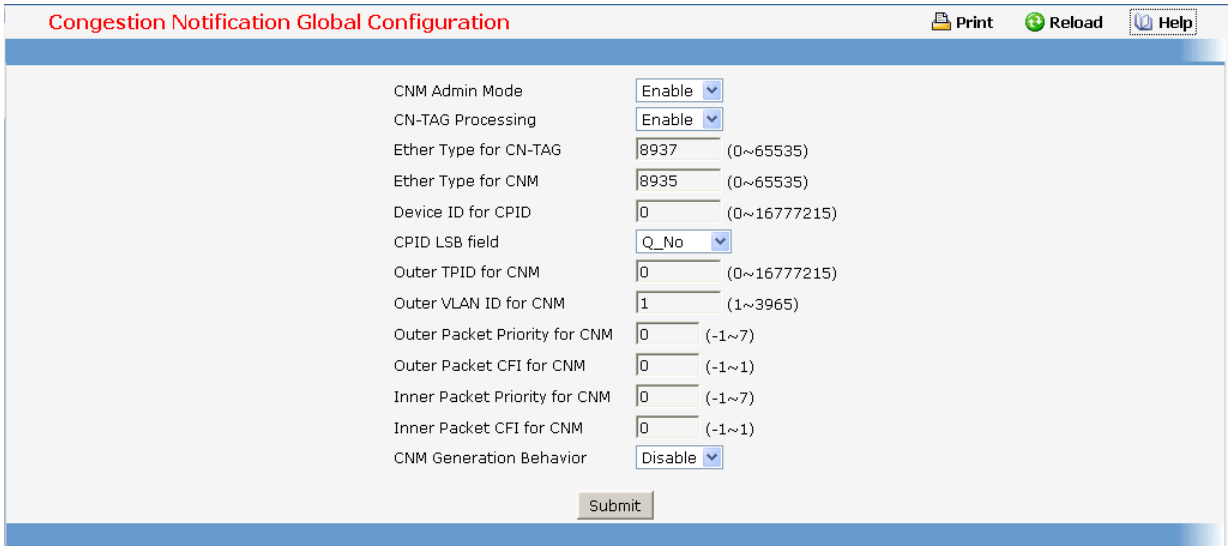
ETS SAN Weight - SAN Weight of specific interface.

Queue in LAN Priority Group - List of queues in LAN priority group.

Queue in SAN Priority Group - List of queues in SAN priority group.

Queue in IPC Priority Group - List of queues in IPC priority group.

11.7.4.8 Configuring Congestion Notification (CN)) Global configuration



Selection Criteria

CNM Admin Mode - Enable/Disable congestion notification message(CNM) handling.

- **Enable** - to enable handling congestion notification message.
- **Disable** - to disable handling congestion notification message.

The system's default CNM handling is Enabled.

CN-TAG Processing *- Enable/Disable CN-TAG processing.*

- **Enable** - configure the CNTAG Ether Type is recognized by parsing stages.
- **Disable** - configure CNTAG Ether Type is unrecognized.

CN-Tag Ether Type can be recognized by default.

CPID LSB Field *- Control the LSB field of Congestion Point Identifier of CNM payload.*

- **CPIndex** - Configure device identifier to use congestion point index.
- **Q_No** - Set the CPID mode to use queue number of sampled packet.

The system's default LSB field of CPID is using queue number of sampled packet.

CNM Generation Behavior *- Set Congestion Notification Message Generation Behavior. Choose the CNM generation behavior when congestion notification threshold is reached but the incoming sampled packet does not have CN-TAG.*

- **Enable** - Keep generate CNM.
- **Disable** - Not generate CNM

The system¡¦s default behavior of CNM generation is not generate.

Configurable Data

Ether Type for CN-TAG - Set Ether Type for CN-TAG. The system's default Ether Type of CN-TAG is 8937. The valid Ether Type range is 0 to 65535.

Ether Type for CNM - Set Ether Type for Congestion Notification Message (CNM). The system¡¦s default Ether Type of CNM is 8935. The valid Ether Type range is 0 to 65535.

Device ID for CPID - Set Device Identifier for Congestion Point Identifier (CPID). The system¡¦s default device identifier of CPID is 0. The valid device identifier range is 0 to16777215.

Outer TPID for CNM - Set Outer TPID for Congestion Notification Message (CNM). The system's default Outer TPID for CNM is 0. The valid TPID range is 0 to 16777215.

Outer VLAN ID for CNM - Set Outer VLAN ID for Congestion Notification Message (CNM). The system's default Outer VLAN ID for CNM is 1. The valid VLAN ID range is 1 to 3965.

Outer Packet Priority for CNM - Set Outer Packet Priority for Congestion Notification Message (CNM). The system's default Outer Packet Priority for CNM is 0. The valid dot1p range is -1 to 7.

Outer Packet CFI for CNM - Set Outer Packet CFI for Congestion Notification Message (CNM). The system's default Outer Packet CFI for CNM is 0. The valid CFI range is -1 to 1.

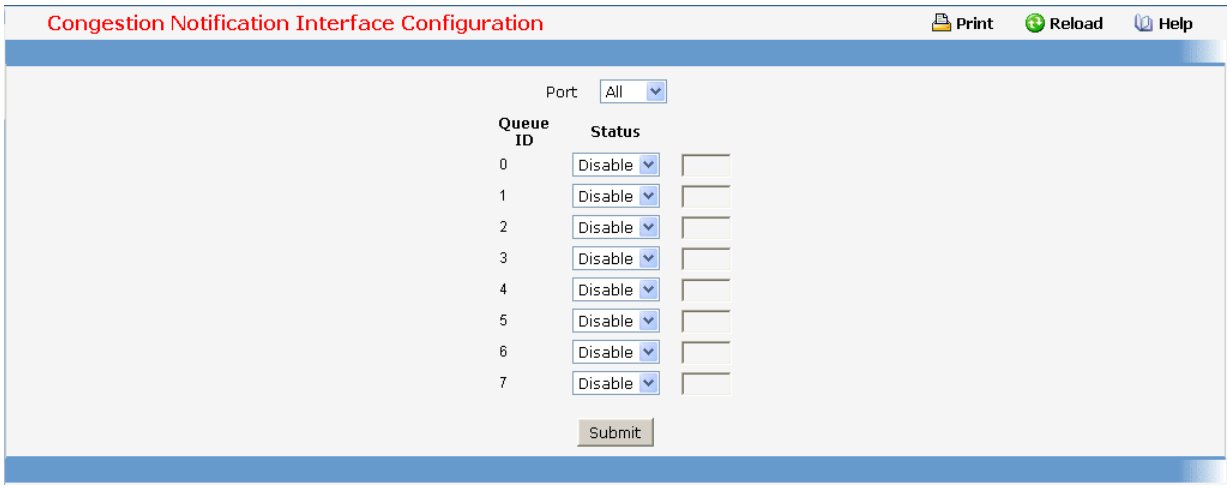
Inner Packet Priority for CNM - Set Inner Packet Priority for Congestion Notification Message (CNM). The system's default Inner Packet Priority for CNM is 0. The valid dot1p range is -1 to 7.

Inner Packet CFI for CNM - Set Inner Packet CFI for Congestion Notification Message (CNM). The system's default Inner Packet CFI for CNM is 0. The valid CFI range is -1 to 1.

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.

11.7.4.9 Configuring Congestion Notification (CN) Interface configuration



Selection Criteria

Port - Choose a CN configurable interfaces for setting.

Status - Enable or Disable specific priority queue. The CN function is disabled by default on all priorities for each port.

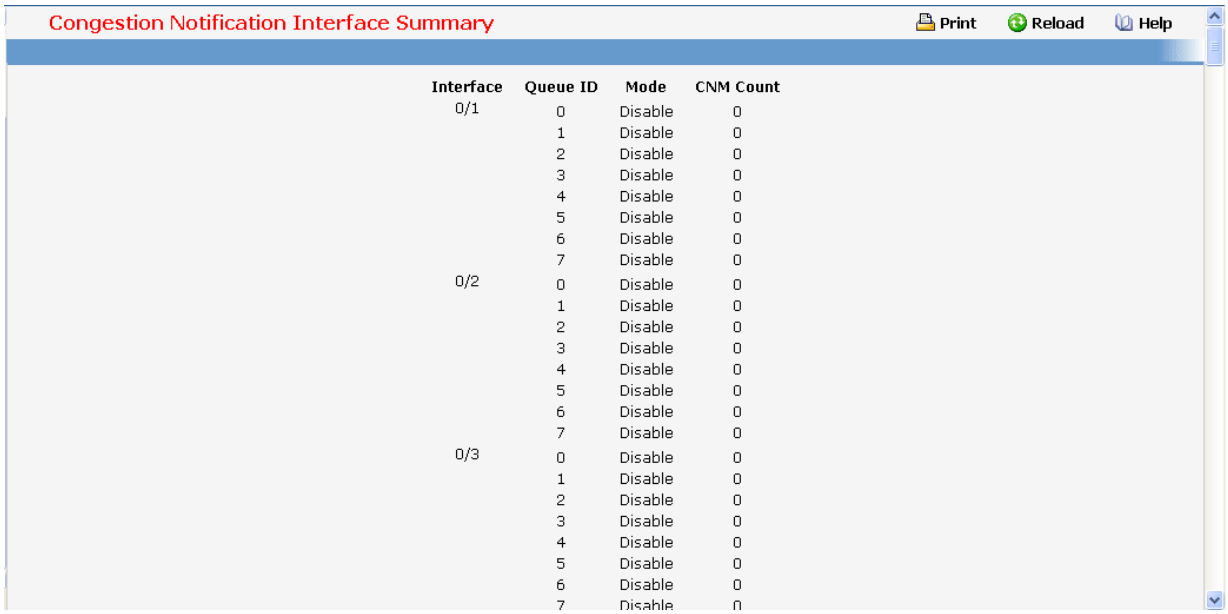
Non-Configurable Data

Queue ID - Specifies the queue ID.

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.

11.7.4.10 Viewing Congestion Notification (CN) interface summary



Interface	Queue ID	Mode	CNM Count
0/1	0	Disable	0
	1	Disable	0
	2	Disable	0
	3	Disable	0
	4	Disable	0
	5	Disable	0
	6	Disable	0
	7	Disable	0
0/2	0	Disable	0
	1	Disable	0
	2	Disable	0
	3	Disable	0
	4	Disable	0
	5	Disable	0
	6	Disable	0
	7	Disable	0
0/3	0	Disable	0
	1	Disable	0
	2	Disable	0
	3	Disable	0
	4	Disable	0
	5	Disable	0
	6	Disable	0
	7	Disable	0

Non-Configurable Data

Interface - The list of CN configurable interfaces.

Queue ID - Specifies the ID of priority queues.

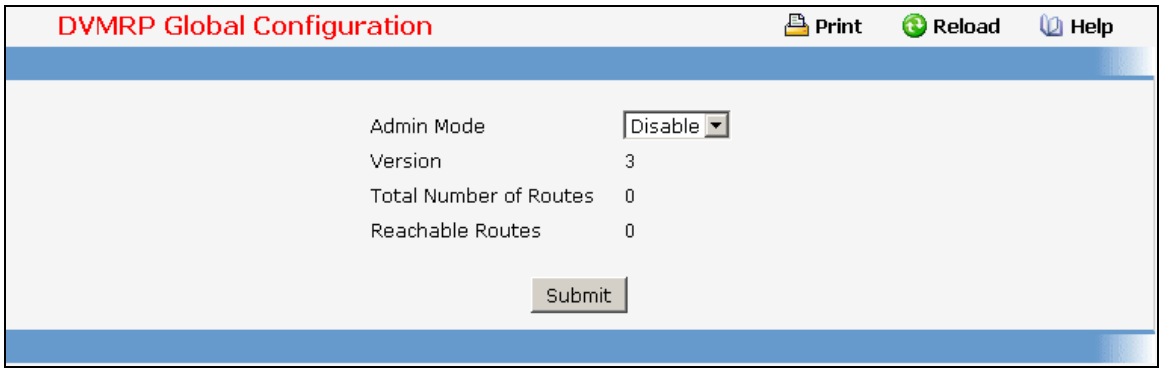
Mode - Specifies the mode of priority queues.

CNM Count - Counts the number of CN message generated by the congestion messaged queue.

11.8 IPv4 Multicast Menu

11.8.1 Managing DVMRP Protocol

11.8.1.1 Configuring DVMRP Global Configuration Page



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.

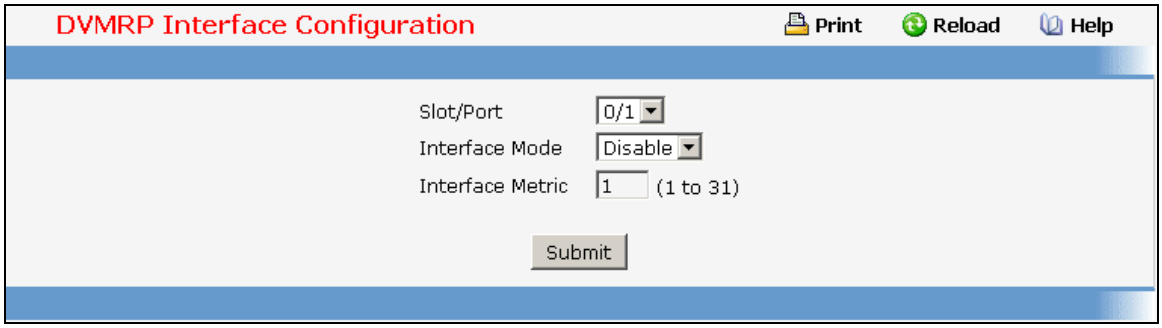
Total Number of Routes - The number of routes in the DVMRP routing table.

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.

11.8.1.2 Configuring DVMRP Interface Configuration Page



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

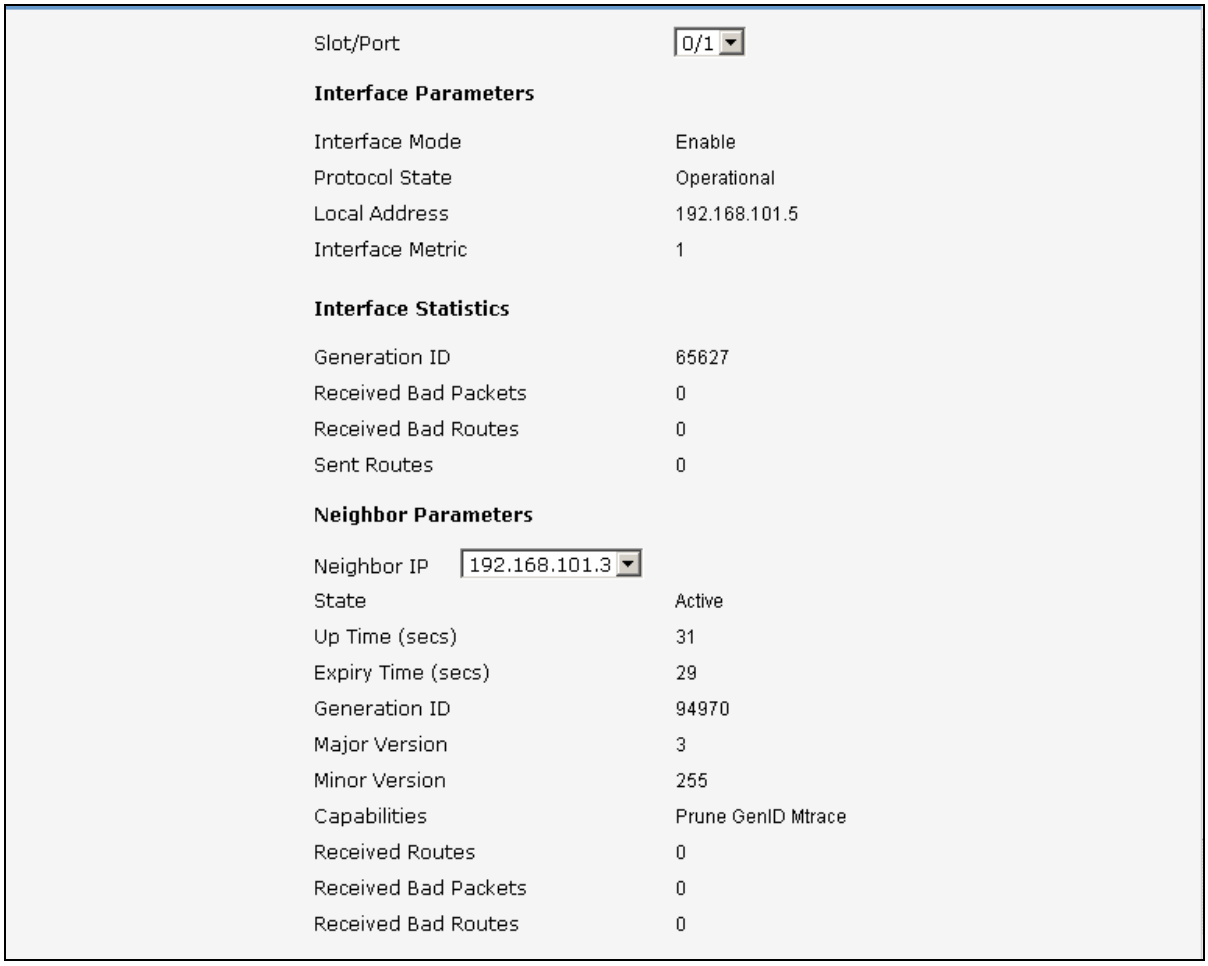
Interface Mode - Select enable or disable from the pull-down menu to set the administrative mode of the selected DVMRP routing interface.

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.

11.8.1.3 Viewing 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.

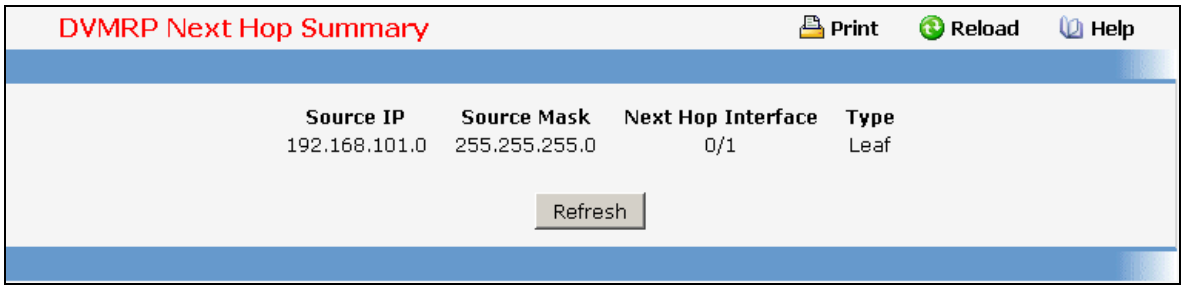
Received Bad Packets - The number of invalid packets received for the specified neighbor on the selected interface.

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.

11.8.1.4 Viewing DVMRP Next Hop Configuration 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.

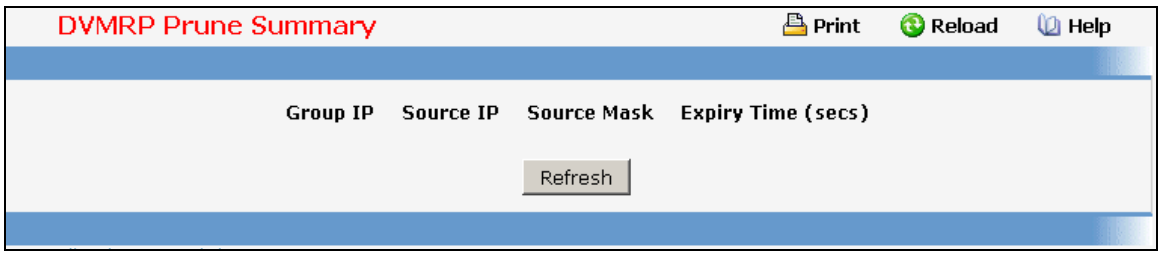
Next Hop Interface - The outgoing interface for this next hop.

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

11.8.1.5 Viewing 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.

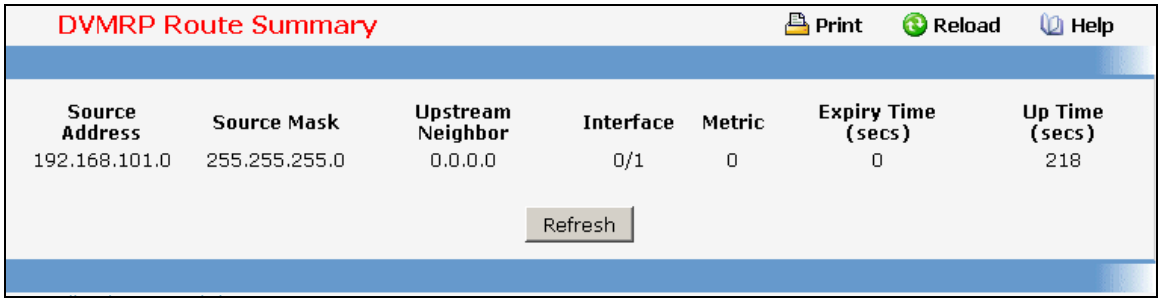
Source Mask - The subnet mask to be combined with the source IP address to identify the source or source network which has been pruned.

Expiry Time (secs) - 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

11.8.1.6 Viewing 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 (secs)- The minimum amount of time remaining before this entry will be aged out.

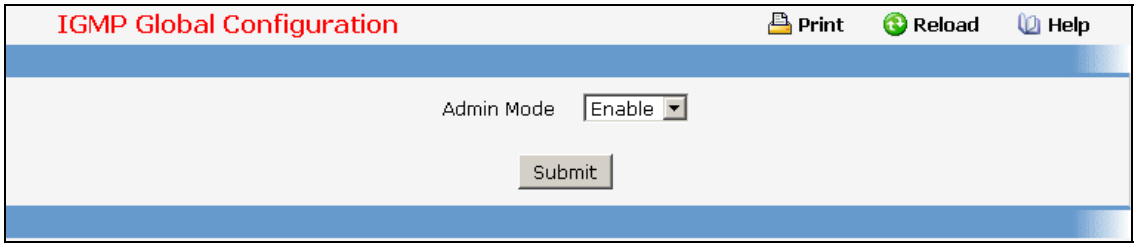
Up Time (secs)- The time since the route represented by this entry was learned by the router.

Command Buttons

Refresh - Refresh the screen with the new data.

11.8.2 Managing IGMP Protocol

11.8.2.1 Configuring IGMP Global Configuration Page



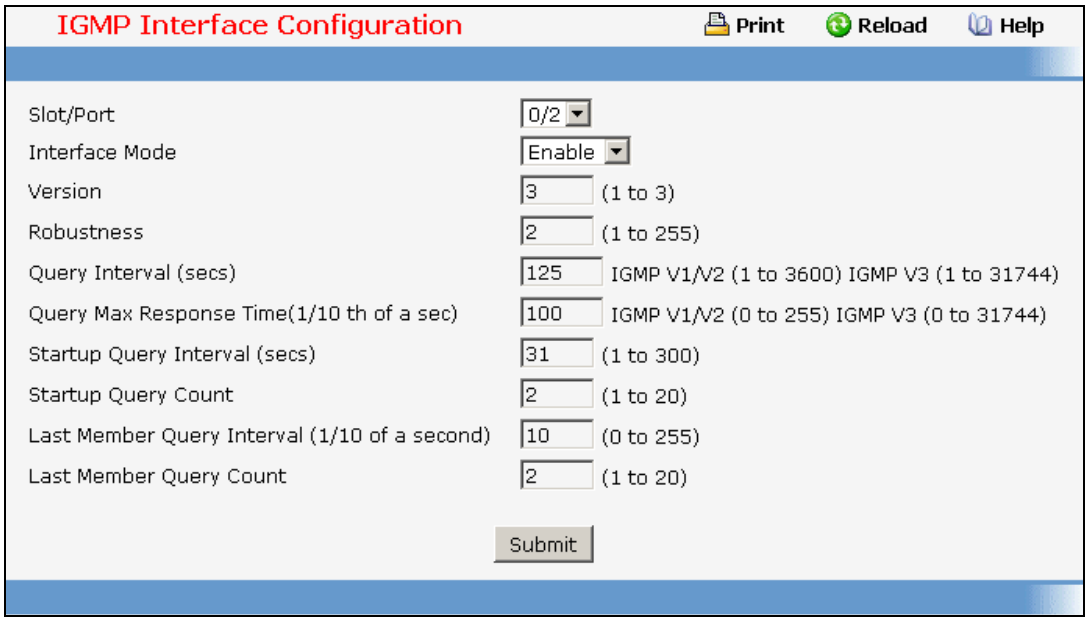
Configurable Data

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.

11.8.2.2 Configuring IGMP Interface Configuration Page



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 3 and the default value is 3. This field is configurable only when IGMP interface mode is enabled.

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 100. 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.

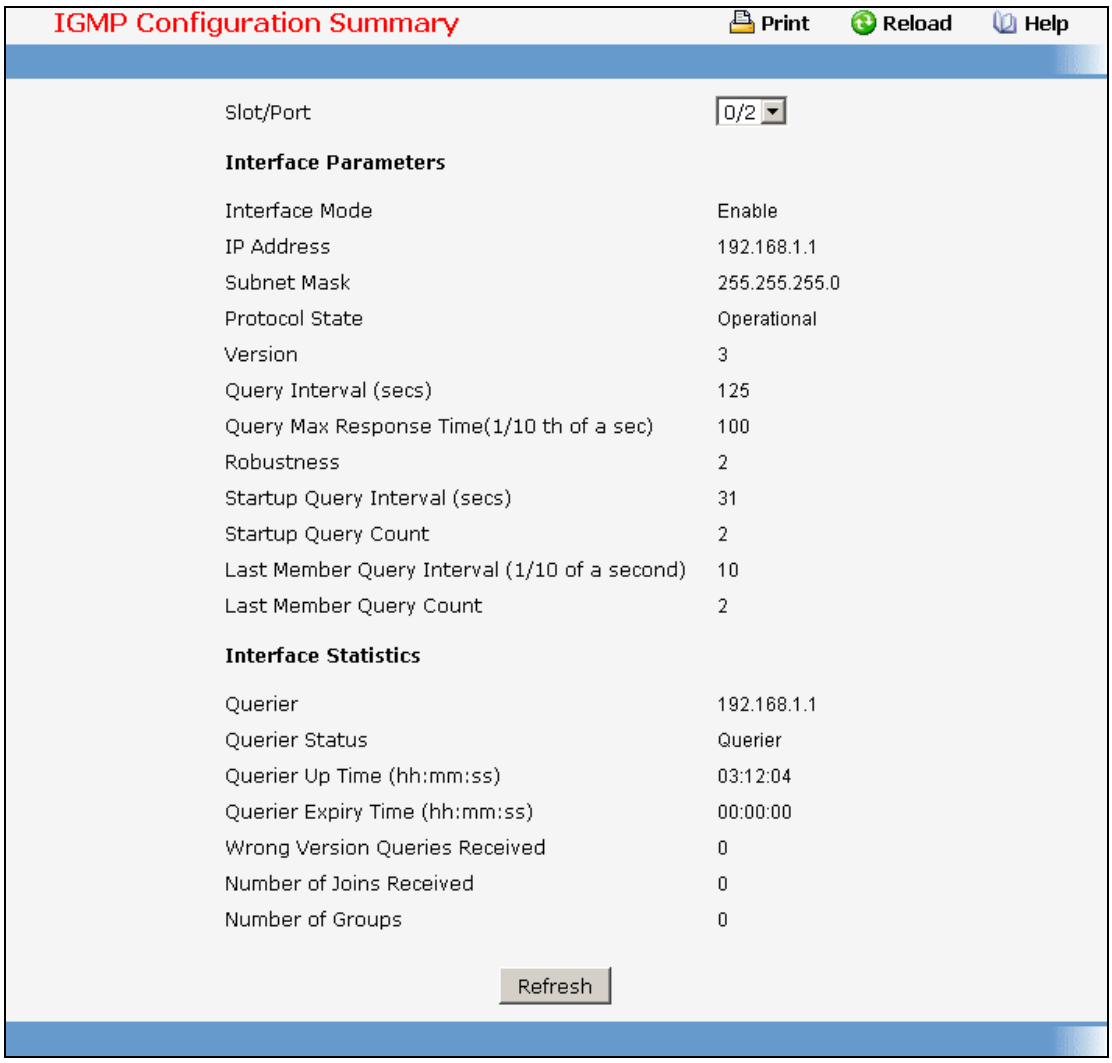
Last Member Query Interval - Enter the last member query interval in tenths of a second. This the maximum response time to be inserted into group-specific queries sent in response to leave group messages, and is also the amount of time between group-specific query messages. Valid values are from 0 to 255. The default value is 10. 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.

11.8.2.3 Viewing IGMP Configuration Summary Page



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

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.

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.

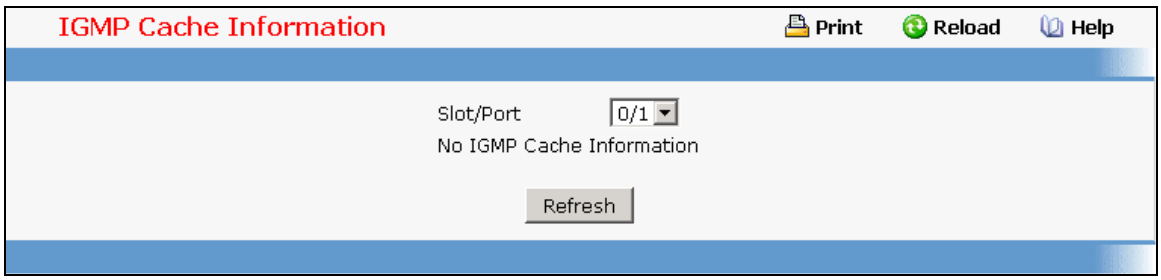
Number of Joins - The number of times a group membership has been added on the selected interface; that is, the number of times an entry for this interface has been added to the cache table. This gives an indication of the amount of IGMP activity on the interface.

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.

11.8.2.4 Viewing IGMP Cache Information Page



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.

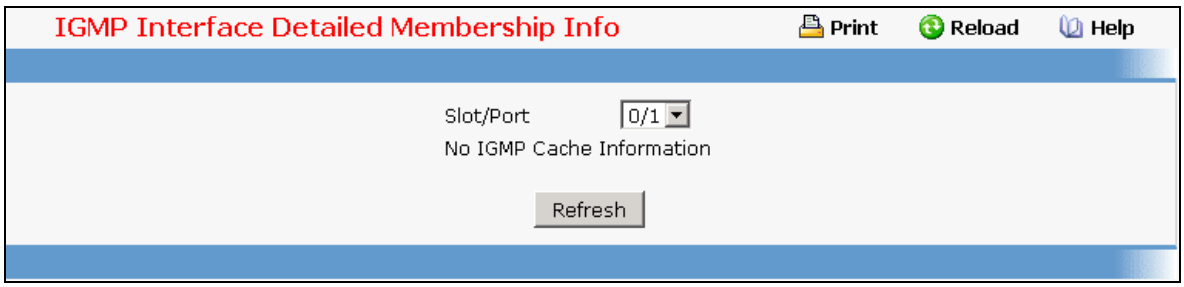
Compatibility - This parameter shows group compatibility mode (v1, v2 and v3) for this group on the specified interface.

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.

11.8.2.5 Viewing IGMP Interface Membership Details Information Page



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.

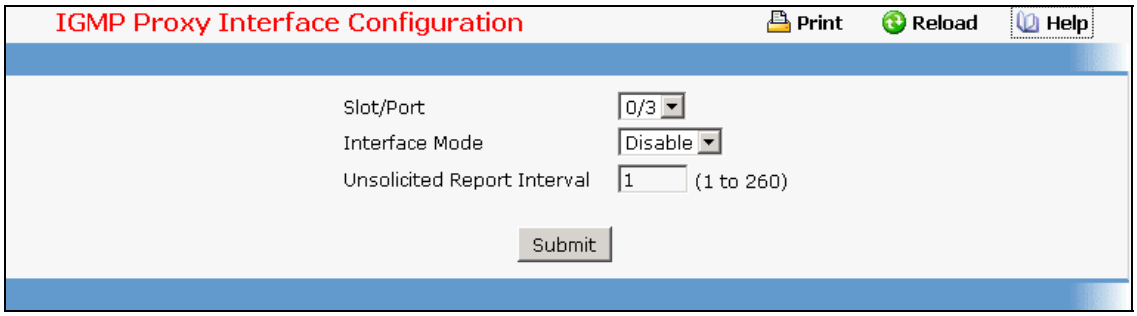
Source Hosts - This parameter shows source addresses which are members of this multicast address.

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.

Command Buttons

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

11.8.2.6 Configuring IGMP Proxy Interface Congiuration Page



Selection Criteria

Slot/Port - Select the port for which data is to be displayed or configured from the pulldown menu. You must have configured at least one router interface before configuring or displaying data for an IGMP Proxy interface and it should not be a IGMP routing interface. This field is configurable only when interface mode is disabled.

Configurable Data

Interface Mode - Select enable or disable from the pulldown menu to set the administrative status of IGMP Proxy on the selected interface. The default is disable. Routing, IGMP and Multicast global admin modes should be enabled to enable IGMP Proxy interface mode.

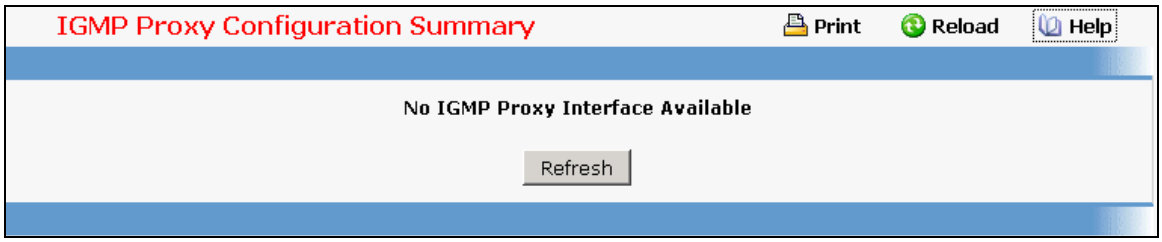
Version - Enter the version of IGMP you want to configure on the selected interface. Valid values are 1 to 3 and the default value is 3. This field is configurable only when IGMP Proxy interface mode is enabled.

Unsolicited Report Interval - Enter the unsolicited time interval value in seconds. The Unsolicited Report Interval is the time between repetitions of a host's initial report of membership in a group. Valid values are from 1 to 260. The default value is 1.

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.

11.8.2.7 Viewing IGMP Proxy Configration Summary Page



Non-Configurable Data

Slot/Port - Displays the interface on which IGMP proxy is enabled.

IP Address - The IP address of the IGMP Proxy interface.

Subnet Mask - The subnet mask for the IP address of the IGMP Proxy interface.

Admin Mode - The administrative status of IGMP Proxy on the selected interface.

Operational Mode - The operational state of IGMP Proxy interface.

Number of Groups - The current number of multicast group entries for the IGMP Proxy interface in the cache table.

Version - The version of IGMP configured on the IGMP Proxy interface.

Unsolicited Report Interval - The Unsolicited Report Interval is the time between repetitions of a host's initial report of membership in a group. Default: 1 second.

Version 1 Querier Timeout - The older IGMP version 1 querier timeout value in seconds. The Older Version Querier Interval is the time-out for transitioning a host back to IGMPv3 mode once an older version query is heard. When an older version query is received, hosts set their Older Version Querier Present Timer to Older Version Querier Interval.

Version 2 Querier Timeout - The older IGMP version 2 querier timeout value in seconds.

Proxy Start Frequency - The number of times the proxy was brought up.

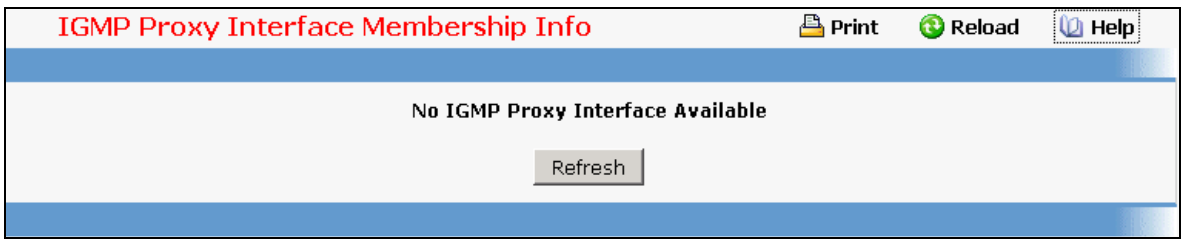
Proxy Interface Statistics - The Queries Received, Reports Received/Sent, Leaves Received/Sent are displayed in the form a table for each IGMP version.

Command Buttons

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

Clear Statistics - Clear the IGMP Proxy interface statistics.

11.8.2.8 Viewing IGMP Proxy Interface Membership Information Page



Selection Criteria

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

Slot/Port - Displays the interface on which IGMP proxy is enabled.

Last Reporter - The IP address of the source of the last membership report received for the IP Multicast group address on the IGMP Proxy interface.

Uptime - The time elapsed since this entry was created.

State - The state of the host entry. A Host can be in one of the state. Non-member state - does not belong to the group on the interface. Delaying member state - host belongs to the group on the interface and report timer running. The report timer is used to send out the reports. Idle member state - host belongs to the group on the interface and no report timer running.

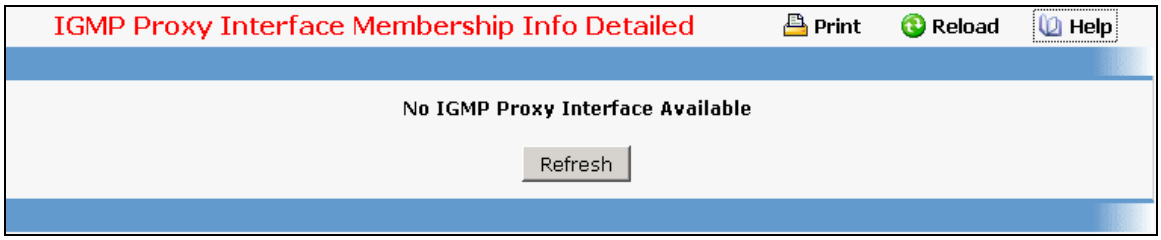
Filter Mode - The group filter mode (Include/Exclude/None) for the specified group on the IGMP Proxy interface.

Number of Sources - The number of source hosts present in the selected multicast group.

Command Buttons

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

11.8.2.9 Viewing IGMP Proxy Interface Membership Details Information Page



Selection Criteria

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 IGMP Proxy interface you will not be able to make this selection, and none of the non-configurable data will be displayed.

Non-Configurable Data

Slot/Port - Displays the interface on which IGMP proxy is enabled.

Source IP - 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 is a member of this multicast group. This is the amount of time after which the specified source entry is aged out.

Last Reporter - The IP address of the source of the last membership report received for the IP Multicast group address on the selected interface.

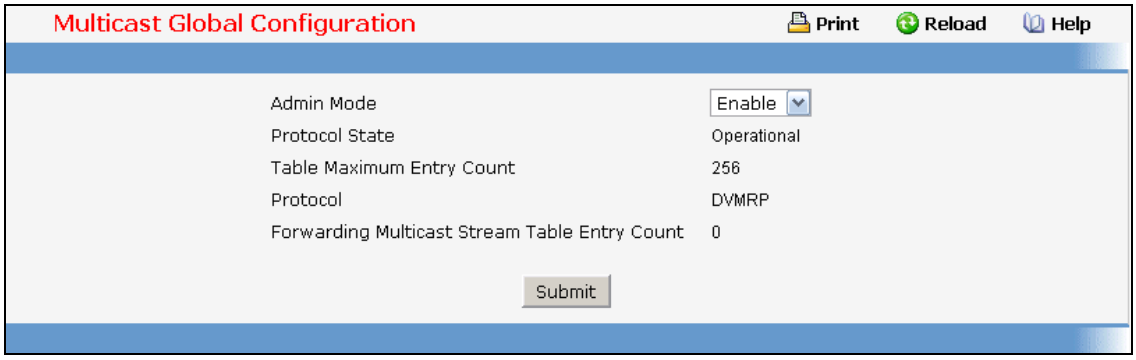
Up Time - Displays the up time since the entry was created in cache table.

State - The state of the host entry. A Host can be in one of the state. Non-member state - does not belong to the group on the interface. Delaying member state - host belongs to the group on the interface and report timer running. The report timer is used to send out the reports. Idle member state - host belongs to the group on the interface and no report timer running.

Filter Mode - The group filter mode (Include/Exclude/None) for the specified group on the IGMP Proxy interface.

11.8.3 Defining Multicast Configuration

11.8.3.1 Configuring Multicast Global Configuration Page



Selection Criteria

Admin Mode - Select enable or disable to set the administrative status of Multicast Forwarding in the router. The default is disabled.

Non-Configurable Data

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.

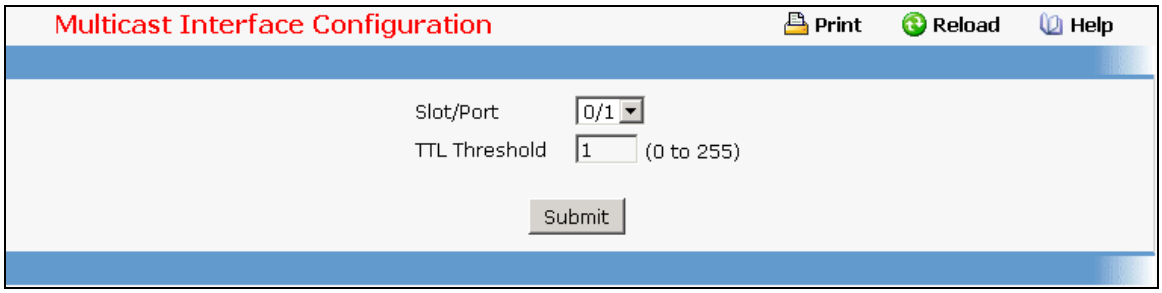
Protocol - The multicast routing protocol presently activated on the router, if any.

Forwarding Multicast Stream Table Entry Count - The number of multicast route entries currently 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.

11.8.3.2 Configuring Interface's Multicast Configuration Page



Selection Criteria

Slot/Port - Select the routing interface you want to configure from the dropdown menu.

Configurable Data

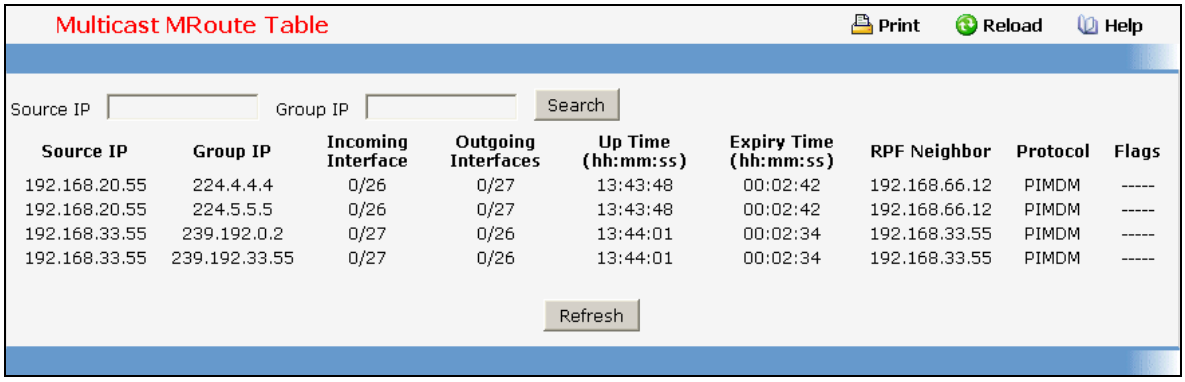
TTL Threshold - Enter the TTL threshold below which a multicast data packet will not be forwarded from the selected interface. You should enter a number between 0 and 255. If you enter 0 all multicast packets for the selected interface will be forwarded. You must configure at least one router interface 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.

11.8.3.3 Viewing Multicast MRoute Summary Page

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.



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 (secs)- The time in seconds since the entry was created.

Expiry Time (secs)- 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

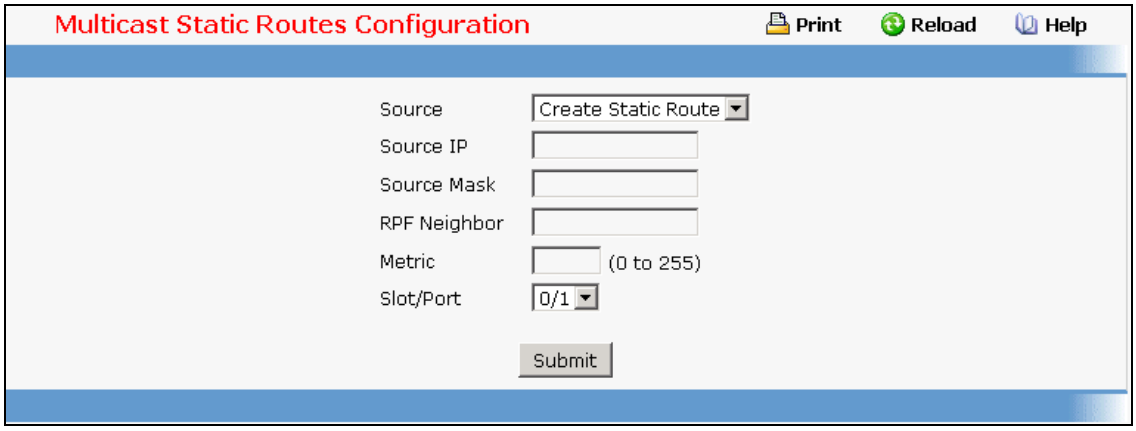
Flags - The value displayed in this field is valid if the multicast routing protocol running is PIMSM. The possible values are RPT or SPT. For other protocols a "------" is displayed.

Command Buttons

Search - Search the Mroute table for an entry matching the Source IP (if entered) and Group IP address.

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

11.8.3.4 Configuring Multicast Static Routes Configuration Page



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.

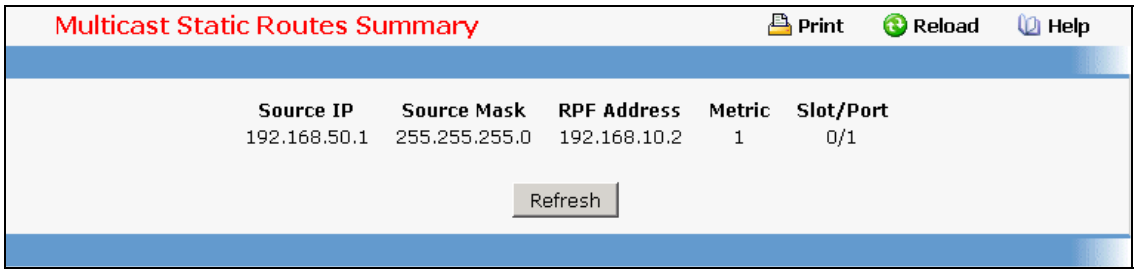
Slot/Port - Select the interface number from the dropdown menu. This is the interface that connects to the neighbor router for the given source IP address.

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.

11.8.3.5 Viewing Multicast Static Routes Configuration Page



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 Address - The IP address of the RPF neighbor.

Metric - The link state cost of the path to the multicast source. The range is 0 - 255.

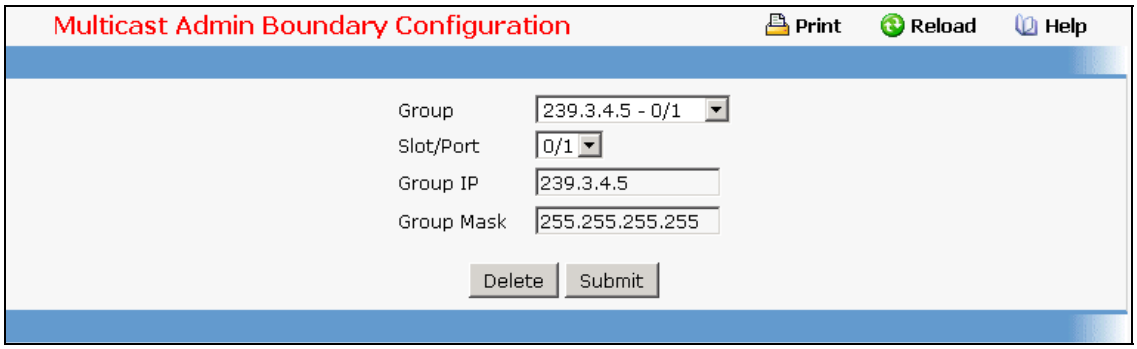
Slot/Port - The number of the incoming interface whose IP address is used as RPF for the given source IP address.

Command Buttons

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

11.8.3.6 Configuring Multicast Admin Boundary Configuration Page

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.



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.

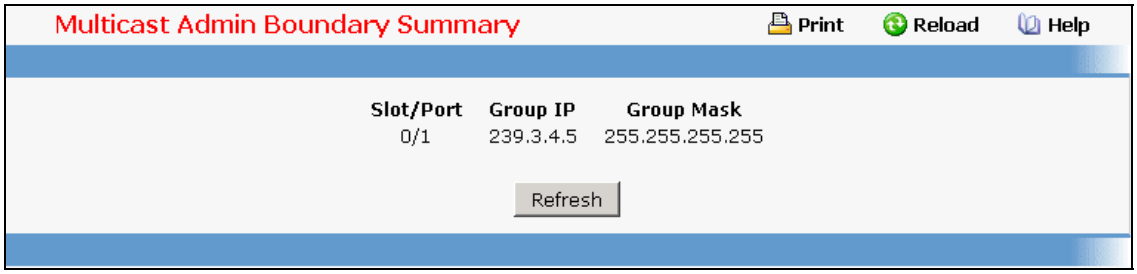
Group Mask - Enter the mask to be applied to the multicast group address. The combination of the mask and the Group IP gives the range of administratively scoped addresses for the selected interface.

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.

11.8.3.7 Viewing Multicast Admin Boundary Configuration Page



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.

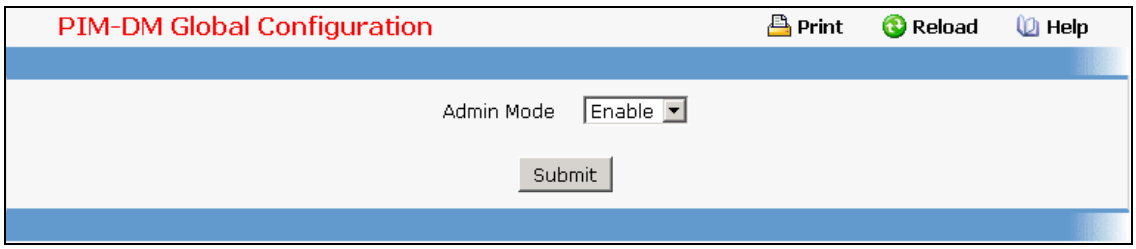
Group Mask - The mask that is applied to the multicast group address. The combination of the mask and the Group IP gives the range of administratively scoped addresses for the selected interface.

Command Buttons

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

11.8.4 Managing PIM-DM Protocol

11.8.4.1 Configuring PIM-DM Global Admin Configuration Page



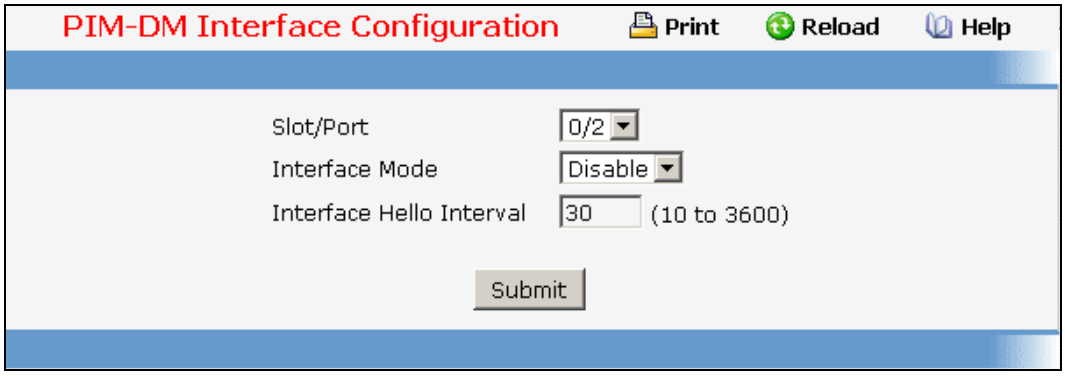
Configurable Data

Admin Mode - Select enable or disable from the pulldown menu to set the administrative status of PIM-DM in the router. The default is disabled.

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.

11.8.4.2 Configuring Interface's PIM-DM Configuration Page



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

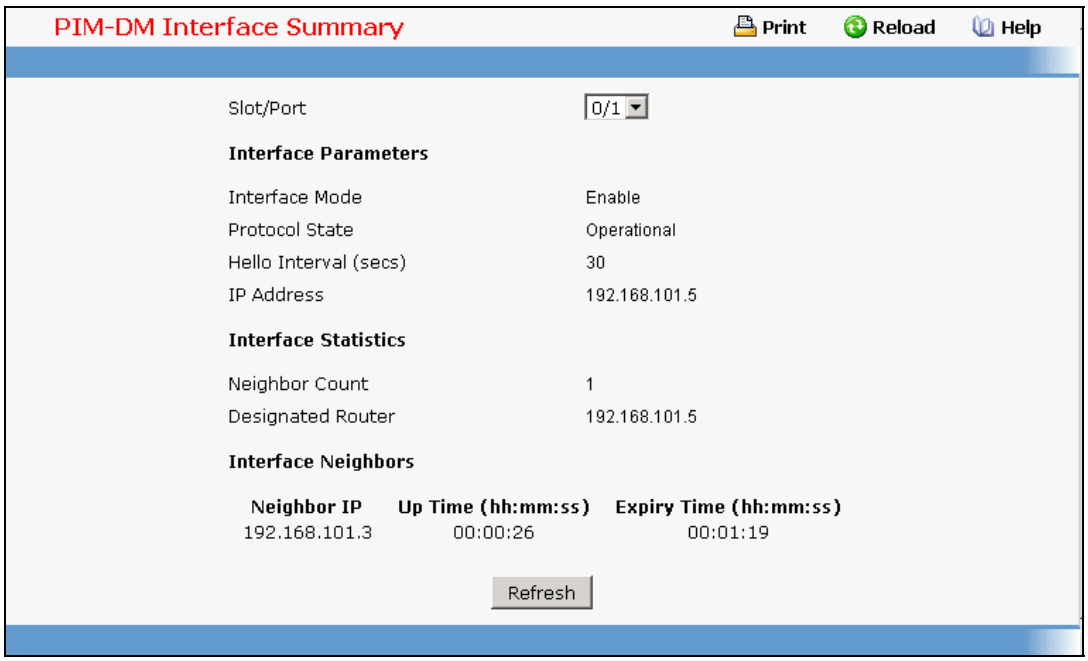
Interface Mode - Select enable or disable from the pulldown menu to set the administrative status of PIM-DM for the selected interface. The default is disabled.

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.

11.8.4.3 Viewing Interface's PIM-DM Configuration Page



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 disabled.

Protocol State - The operational state of the PIM-DM protocol on this interface.

Hello Interval (secs)- 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.

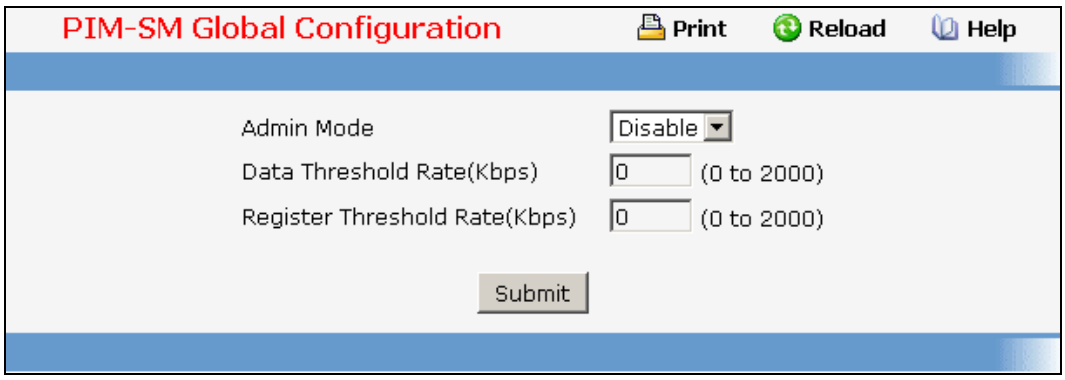
Expiry Time - The minimum time remaining before this PIM neighbor will be aged out.

Command Buttons

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

11.8.5 Managing PIM-SM Protocol

11.8.5.1 Configuring PIM-SM Global Configuration Page



Configurable Data

Admin Mode - Select enable or disable from the pulldown menu to set the administrative status of PIM-SM in the router. The default is disable.

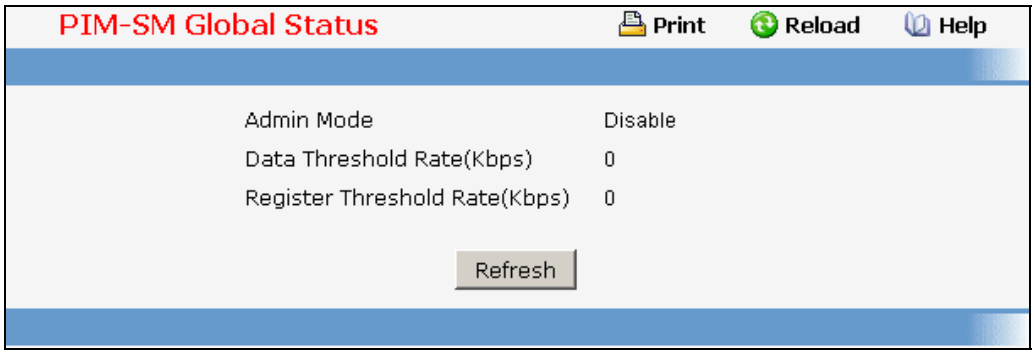
Data Threshold Rate - Enter the rate in K bits/second above which the last-hop router will switch to a source-specific shortest path tree. The valid values are from (0 to 2000) The default value is 0.

Register Threshold Rate - Enter 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) 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.

11.8.5.2 Viewing PIM-SM Global Configuration Page



Non-Configurable Data

Admin Mode - The administrative status of PIM-SM in the router: either enable or disable.

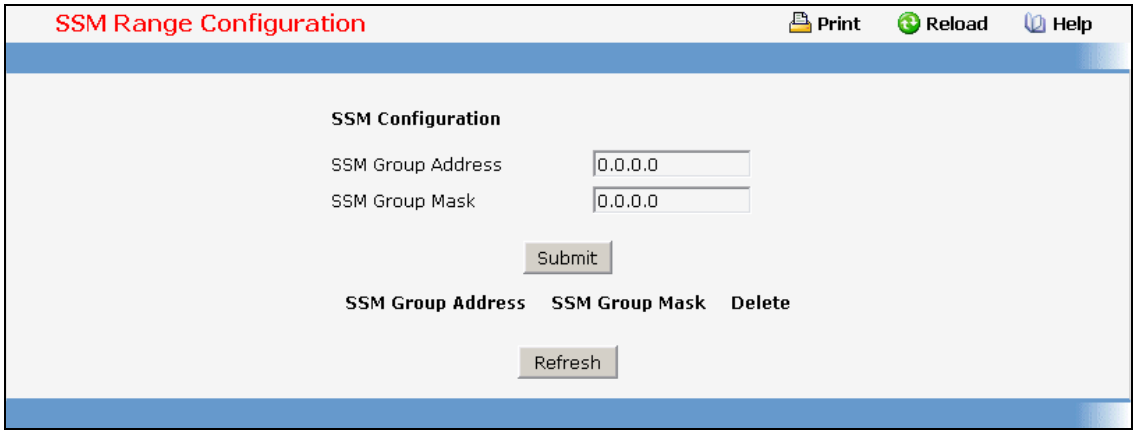
Data Threshold Rate - The minimum source data rate in K bits/second above which the last-hop router will switch to a source-specific shortest path tree.

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.

11.8.5.3 Configuring PIM-SM SSM Range Configuration Page



Configurable Data

SSM Group Address - Enter the source-specific multicast group ip-address.

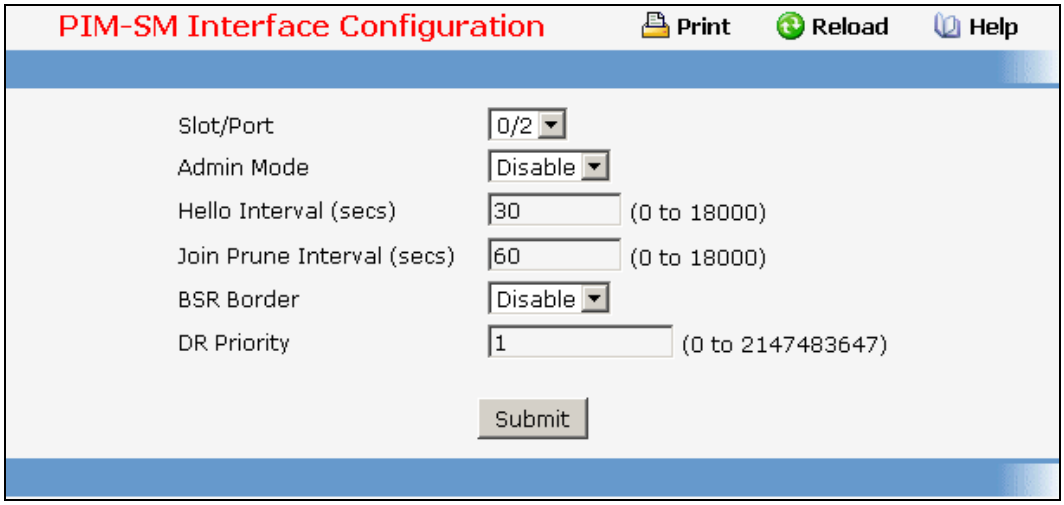
SSM Group Mask - Enter the source-specific multicast group ip-address mask.

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.

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

11.8.5.4 Configuring Interface's PIM-SM Configuration Page



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 (secs)- Enter the time in seconds between the transmission of which PIM Hello messages on this interface. The valid values are from (0 to 18000 secs) . The default value is 30.

Join/Prune Interval - Enter the frequency at which PIM Join/Prune messages are transmitted on this PIM interface. The valid values are from (0 to 18000) . The default value is 60.

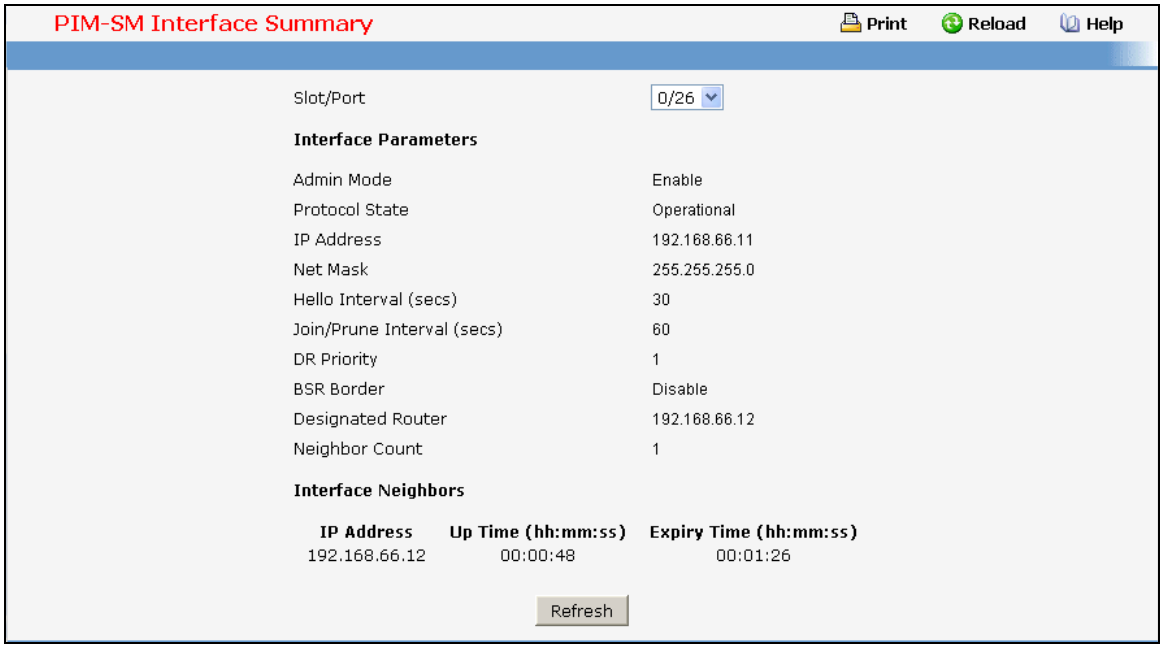
BSR Border - Select enable or disable to set BSR border status on the selected interface.

DR Priority - Enter the DR priority for the selected interface. The valid values are from (0 to 2147483647) The default value is 1.

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.

11.8.5.5 Viewing Interface's PIM-SM Configuration Page



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.

Protocol State - The operational state of the PIM-SM protocol on this interface.

IP Address - The IP address of the selected PIM interface.

Net Mask - The network mask for the IP address of the selected PIM interface.

Hello Interval (secs) - The frequency at which PIM Hello messages are transmitted on the selected interface.

Join/Prune Interval - The frequency at which PIM Join/Prune messages are transmitted on this PIM interface.

DR Priority - Indicates the DR priority on the PIM interface.

BSR Border - Specifies the BSR border mode on the PIM interface.

Designated Router - The Designated Router on the selected PIM interface

Neighbor Count - The number of PIM neighbors on the selected interface.

IP Address - The IP address of the PIM neighbor for this entry.

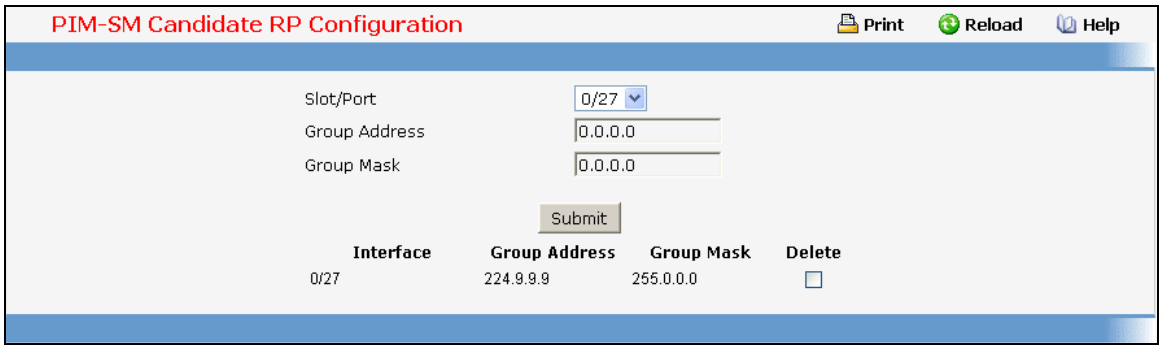
Up Time - The time since this PIM neighbor (last) became a neighbor of the local router.

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.

11.8.5.6 Configuring PIM-SM Candidate RP Configuration Page



Selection Criteria

Slot/Port - Select the slot and port for which data is to be displayed. Slot 0 is the base unit.

Configurable Data

Group Address - The group address transmitted in Candidate-RP-Advertisements.

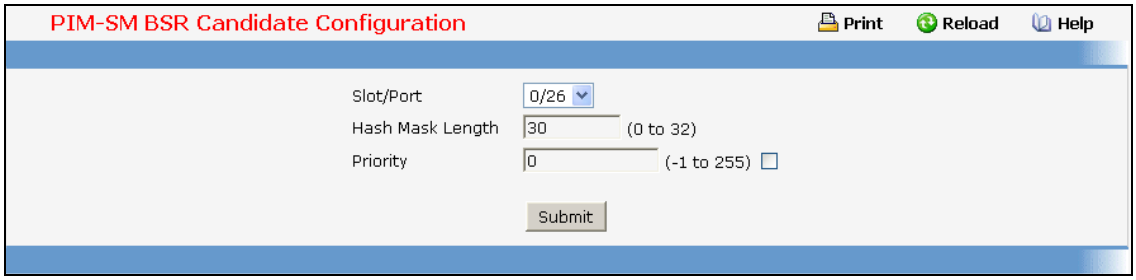
Group Mask - The group address mask transmitted in Candidate-RP-Advertisements.

Delete - Attempts to remove the specified Candidate RP 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.

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.

11.8.5.7 Configuring PIM-SM BSR Candidate Configuration Page



Selection Criteria

Slot/Port - Select the slot and port for which data is to be displayed. Slot 0 is the base unit.

Configurable Data

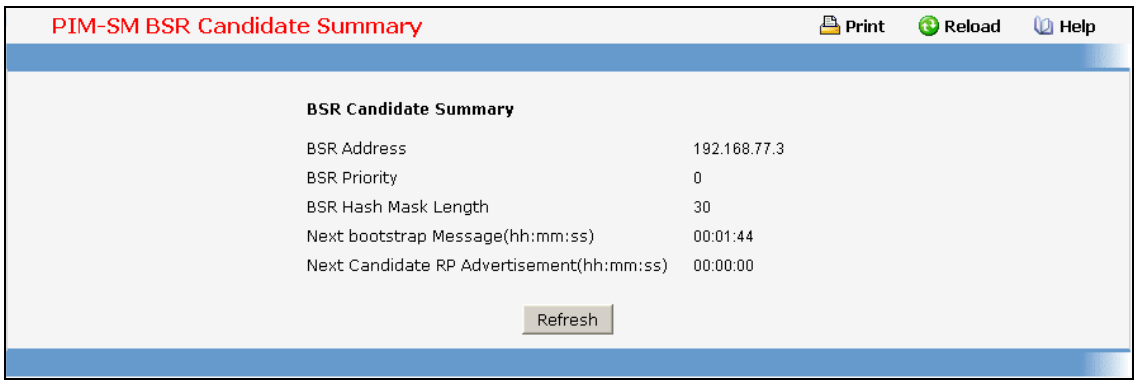
Hash Mask Length - Enter the C-BSR hash mask length to be advertised in bootstrap messages. This hash mask length will be used in the hash algorithm for selecting the RP for a particular group. The valid values are from (0 to 32). Default value is 30.

Priority - Enter the priority of C-BSR.

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.

11.8.5.8 Viewing PIM-SM BSR Candidate Summary Page



Non-Configurable Data

BSR Address - Displays the IP address of the Elected BSR.

BSR Priority - Displays the Priority of the Elected BSR.

BSR Hash Mask Length - Displays hash mask length of the Elected BSR.

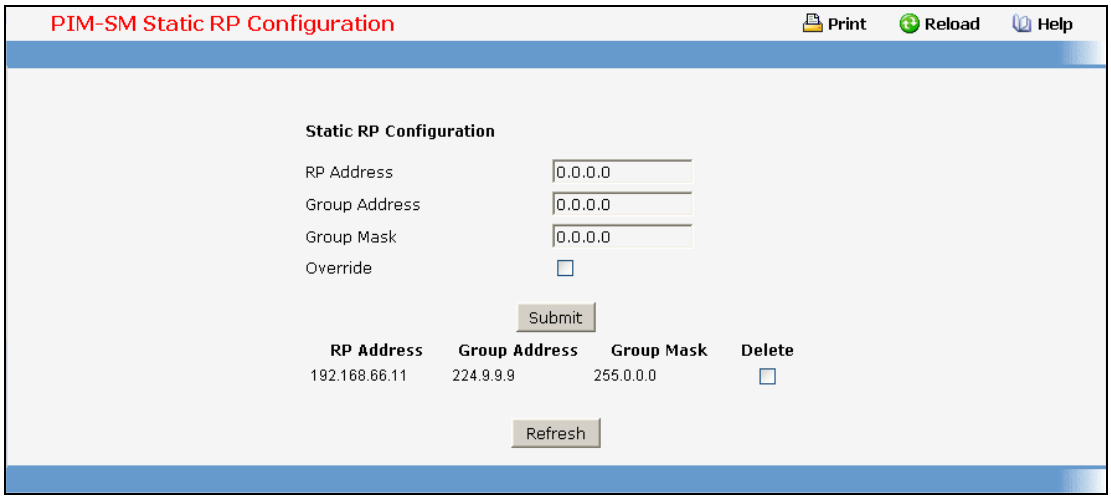
Next bootstrap Message - Time (in hours, minutes, and seconds) in which the next bootstrap message is due from this BSR.

Next Candidate RP Advertisement - Time (in hours, minutes, and seconds) in which the next candidate RP advertisement will be sent.

Command Buttons

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

11.8.5.9 Configuring PIM-SM Static RP Configuration Page



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

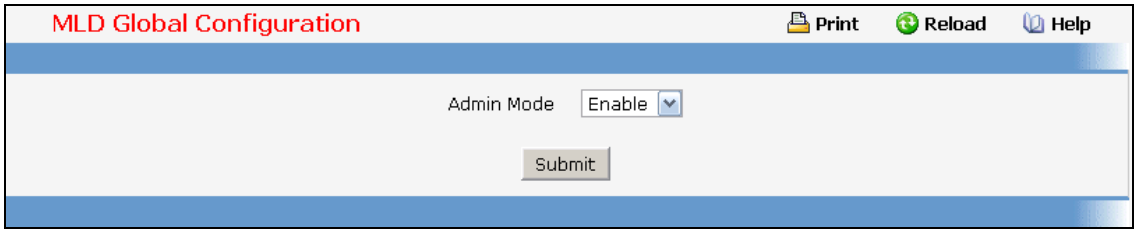
Submit - Attempts to create the specified static RP IP Address for the PIM-SM router. Configuration changes take effect immediately. These changes will not be retained across a power cycle unless a save is performed.

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.

11.9 IPv6 Multicast Menu

11.9.1 Managing MLD

11.9.1.1 Configuring MLD Global Configuration Page



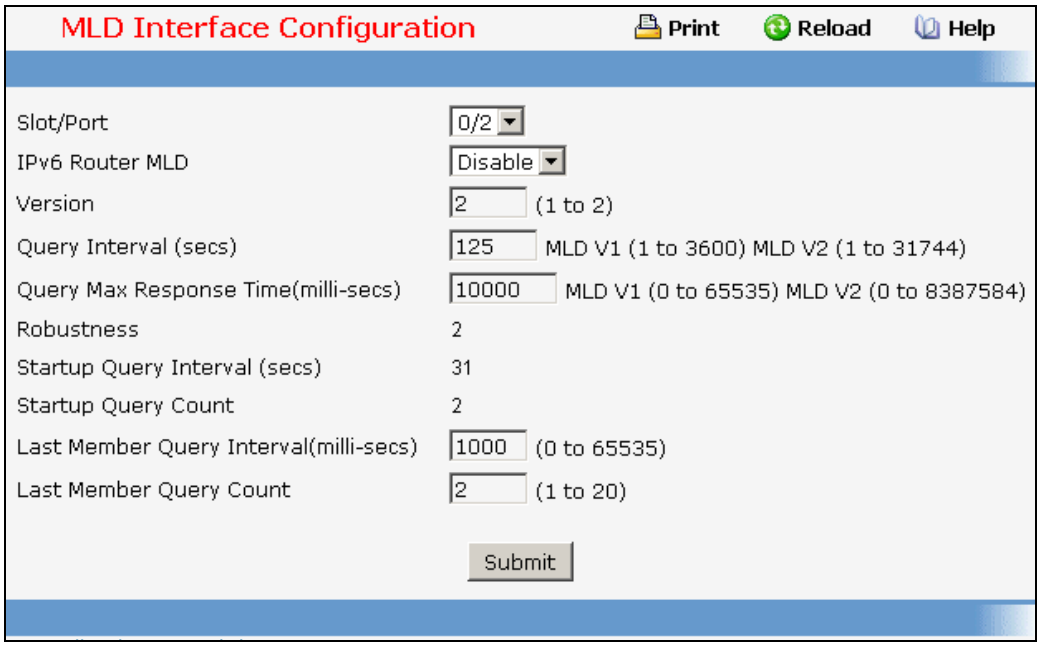
Selection Criteria

Admin Mode - Select enable or disable from the pulldown menu to set the administrative status of MLD in the router to active or inactive. The default is disabled.

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.

11.9.1.2 Configuring MLD Interface Configuration Page



Selection Criteria

Admin Mode - 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 MLD interface, otherwise an error message will be displayed.

Configurable Data

IPv6 Router MLD - Select enable or disable from the pull down menu to set the administrative status of MLD on the selected interface.The default value is disable.

Version - Enter the version to be configured on the selected interface. Valid values are (1 to 2) The default value is 2.

Query Interval - Enter the frequency in seconds at which MLD 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 MLDv2 queries on this interface, in milli-seconds.Valid values are from (0 to 65535) . The default value is 10000milliseconds.

Last Member Query Interval - Enter the last member query interval in milli-seconds. 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 65535) . The default value is 1000 milli seconds.

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.

Non-Configurable Data

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.

MLD is robust to (robustness variable-1) packet losses. Valid values are from (1 to 255) . The default value is 2

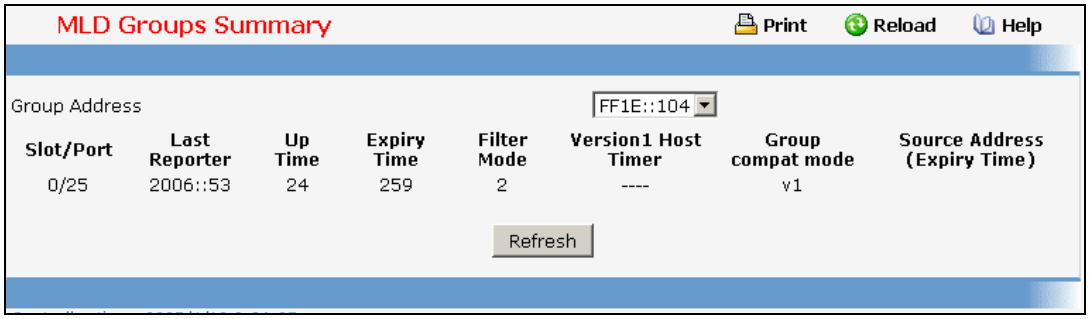
Startup Query Interval - Enter the number of seconds between the transmission of startup queries on the selected interface. The valid values are from (1 to 300) . The default value is 31.

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.

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.

11.9.1.3 Viewing MLD Groups Summary Page



Selection Criteria

Group Address - Indicates the address of the Mgmd members.

Non-Configurable Data

Slot/Port - Indicates the slot and port on which data is displayed.

Last Reporter - The IP Address of the source of the last membership report received for this multicast group address on the interface.

Up Time - Time elapsed in seconds since the multicast group has been known.

Expiry Time - Time left in seconds before the entry is removed from the MLD membership table of this interface.

Filter Mode - The filter mode of the multicast group on this interface. The values it can take are INCLUDE and EXCLUDE.

Version1 Host Timer - The time remaining until the router assumes there are no longer any MLD version-1 Hosts on the specified interface.

Group Compat Mode - The compatibility mode of the multicast group on the interface. The values it can take are MLDv1 and MLDv2.

11.9.1.4 Viewing MLD Interface Summary Page

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

MLD Global Admin Mode - The administrative status of MLD on the selected interface.

MLD Operational Mode- The operational status of MLD on the Interface.

Routing - The Routing mode for an interface.

MLD Version - The version of MLD configured on the selected interface.

Query Interval - This field indicates the configured query interval (in seconds) for the interface.

Query Max Response Time - This field indicates the configured maximum query response time (in milli-seconds) advertised in MLD queries on this 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. MLD is robust to (robustness variable-1) packet losses.

Startup Query Interval - This value indicates the configured interval (in seconds) between General Queries sent by a Querier on startup.

Startup Query Count - This value indicates the configured number of Queries sent out on startup, separated by the Startup Query Interval

Last Member Query Interval - This value indicates the configured Last Member Query Interval(in milli-seconds) inserted into Group-Specific Queries sent in response to Leave Group messages.

Last Member Query Count - This value indicates the configured number of Group-Specific Queries sent before the router assumes that there are no local members.

Querier Status - This value indicates whether the interface is a MLD querier or non-querier on the subnet it is associated with.

Querier Address - The address of the MLD querier on the IP subnet to which the selected interface is attached.

Querier Up Time - The time in seconds since the MLD 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 Received - Indicates the number of queries received whose MLD version does not match the MLD version of the interface.

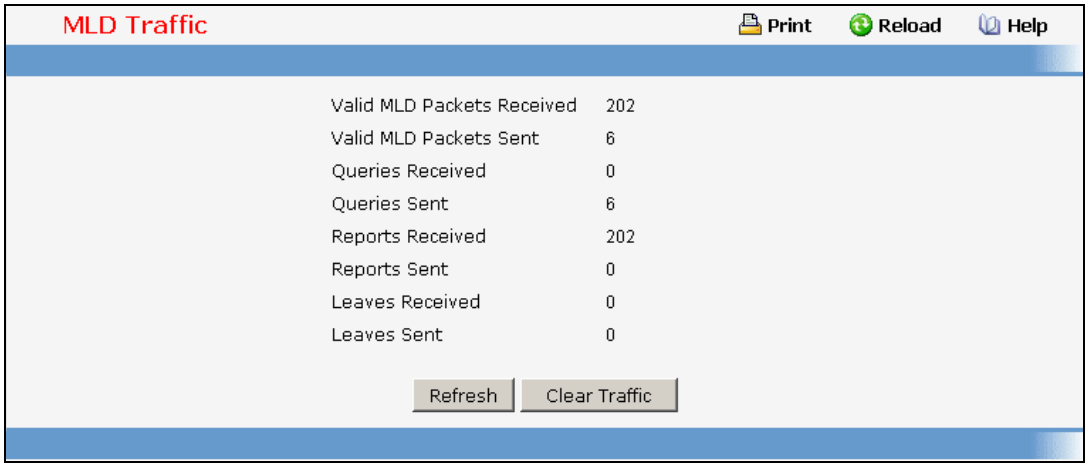
Number of Joins Received - The number of times a group membership has been added on this interface.

Number of Groups - The current number of membership entries for the selected interface in the cache table.

Common Button

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

11.9.1.5 Viewing MLD Traffic Page



Non-Configurable Data

Valid MLD Packets Received - The number of valid MLD packets received by the router.

Valid MLD Packets Sent - The number of valid MLD packets sent by the router.

Queries Received - The number of valid MLD queries received by the router.

Queries Sent - The number of valid MLD queries sent by the router.

Reports Received - The number of valid MLD reports received by the router.

Reports Sent - The number of valid MLD reports sent by the router.

Leaves Received - The number of valid MLD leaves received by the router.

Leaves Sent - The number of valid MLD leaves sent by the router.

Bad Checksum MLD Packets - The number of Bad Checksum MLD Packets received by the router.

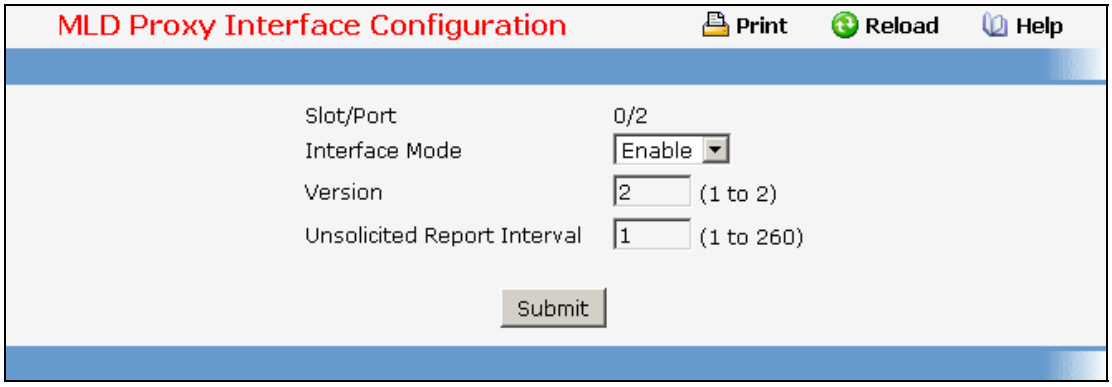
Malformed MLD Packets - The number of Malformed MLD Packets received by the router.

Common Button

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

Clear Traffic - Clears all the parameters for the selected interface.

11.9.1.6 Configuring MLD Proxy Interface Congiuration Page



Selection Criteria

Slot/Port - Select the port for which data is to be displayed or configured from the pulldown menu. You must have configured at least one router interface before configuring or displaying data for an MLD Proxy interface and it should not be a MLD routing interface. This field is configurable only when interface mode is disabled.

Configurable Data

Interface Mode - elect enable or disable from the pulldown menu to set the administrative status of MLD Proxy on the selected interface. The default is disable. Routing, MLD and Multicast global admin modes should be enabled to enable MLD Proxy interface mode.

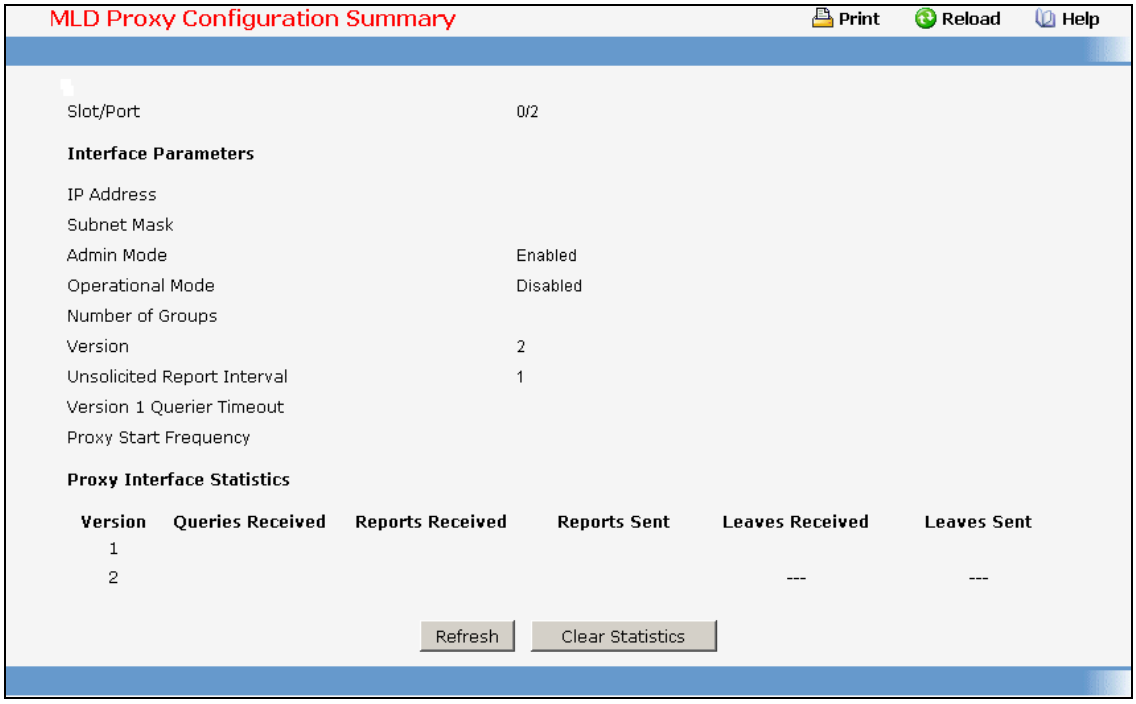
Version - nter the version of MLD you want to configure on the selected interface. Valid values are (1 to 2) and the default value is 2. This field is configurable only when MLD Proxy interface mode is enabled.

Unsolicited Report Interval - Enter the unsolicited time interval value in seconds. The Unsolicited Report Interval is the time between repetitions of a host's initial report of membership in a group. Valid values are from (1 to 260). The default value is 1.

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.

11.9.1.7 Viewing MLD Proxy Configration Summary Page



Non-Configurable Data

Slot/Port - Displays the interface on which MLD proxy is enabled.

IPv6 Address - The IPv6 address of the MLD Proxy interface.

Subnet Mask - The subnet mask for the IPv6 address of the MLD Proxy interface.

Admin Mode - The administrative status of MLD Proxy on the selected interface.

Operational Mode - The operational state of MLD Proxy interface.

Number of Groups - The current number of multicast group entries for the MLD Proxy interface in the cache table.

Version - The version of MLD configured on the MLD Proxy interface.

Unsolicited Report Interval - The Unsolicited Report Interval is the time between repetitions of a host's initial report of membership in a group. Default: 1 second.

Version 1 Querier Timeout - The older MLD version 1 querier timeout value in seconds. The Older Version Querier Interval is the time-out for transitioning a host back to MLDv2 mode once an older version query is heard. When an older version query is received, hosts set their Older Version Querier Present Timer to Older Version Querier Interval.

Proxy Start Frequency - The number of times the proxy was brought up.

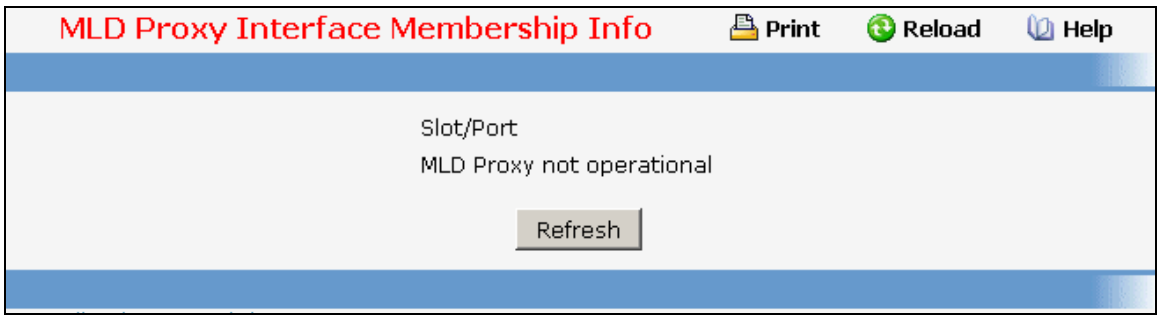
Proxy Interface Statistics - The Queries Received, Reports Received/Sent, Leaves Received/Sent are displayed in the form a table for each MLD version.

Command Buttons

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

Clear Statistics - Clear the MLD Proxy interface statistics.

11.9.1.8 Viewing MLD Proxy Interface Membership Information Page



Selection Criteria

Multicast Group IPv6 - Select the IPv6 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

Slot/Port - Displays the interface on which MLD proxy is enabled.

Last Reporter - The IPv6 address of the source of the last membership report received for the IPv6 Multicast group address on the MLD Proxy interface.

Uptime - The time elapsed since this entry was created.

State - The state of the host entry. A Host can be in one of the state. Non-member state - does not belong to the group on the interface. Delaying member state - host belongs to the group on the interface and report timer running. The report timer is used to send out the reports. Idle member state - host belongs to the group on the interface and no report timer running.

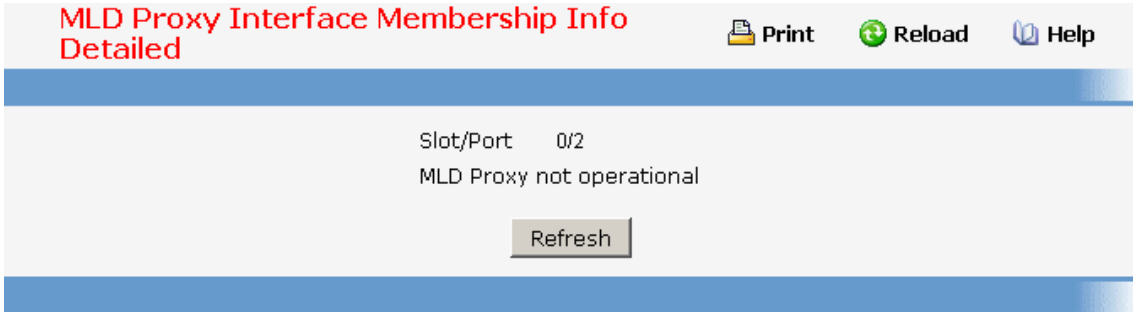
Filter Mode - The group filter mode (Include/Exclude/None) for the specified group on the MLD Proxy interface.

Number of Sources - The number of source hosts present in the selected multicast group.

Command Buttons

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

11.9.1.9 Viewing MLD Proxy Interface Membership Details Information Page



Selection Criteria

Multicast Group IPv6 - Select the IPv6 multicast group address for which data is to be displayed. If no group membership reports have been received on the MLD Proxy interface you will not be able to make this selection, and none of the non-configurable data will be displayed.

Non-Configurable Data

Slot/Port - Displays the interface on which MLD proxy is enabled.

Source IPv6 - 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 is a member of this multicast group. This is the amount of time after which the specified source entry is aged out.

Last Reporter - The IPv6 address of the source of the last membership report received for the IPv6 Multicast group address on the selected interface.

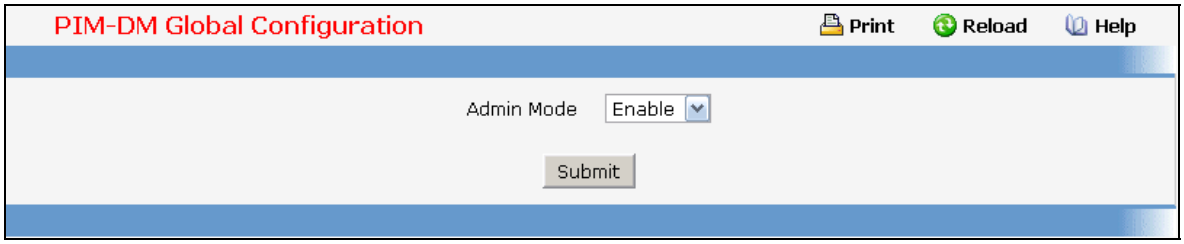
Up Time - Displays the up time since the entry was created in cache table.

State - The state of the host entry. A Host can be in one of the state. Non-member state - does not belong to the group on the interface. Delaying member state - host belongs to the group on the interface and report timer running. The report timer is used to send out the reports. Idle member state - host belongs to the group on the interface and no report timer running.

Filter Mode - The group filter mode (Include/Exclude/None) for the specified group on the MLD Proxy interface.

11.9.2 Managing PIM-DM

11.9.2.1 Configuring PIM-DM Global Configuration Page



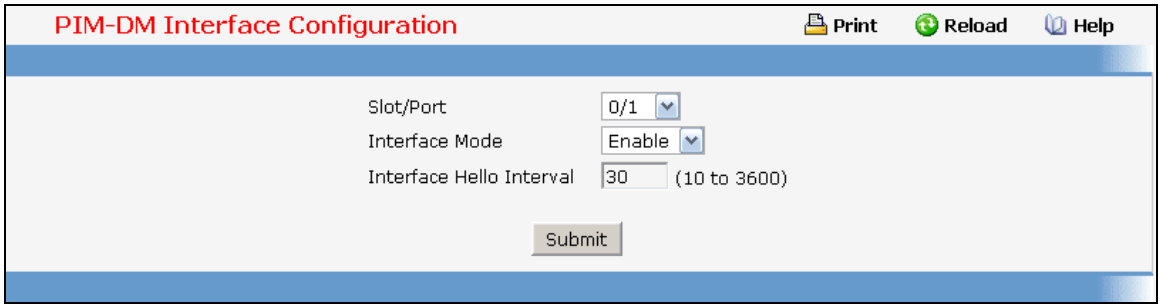
Selection Criteria

Admin Mode - Select enable or disable from the pulldown menu to set the administrative status of PIM-DM in the router to active or inactive. The default is disabled.

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.

11.9.2.2 Configuring PIM-DM Interface Configuration Page



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.

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.

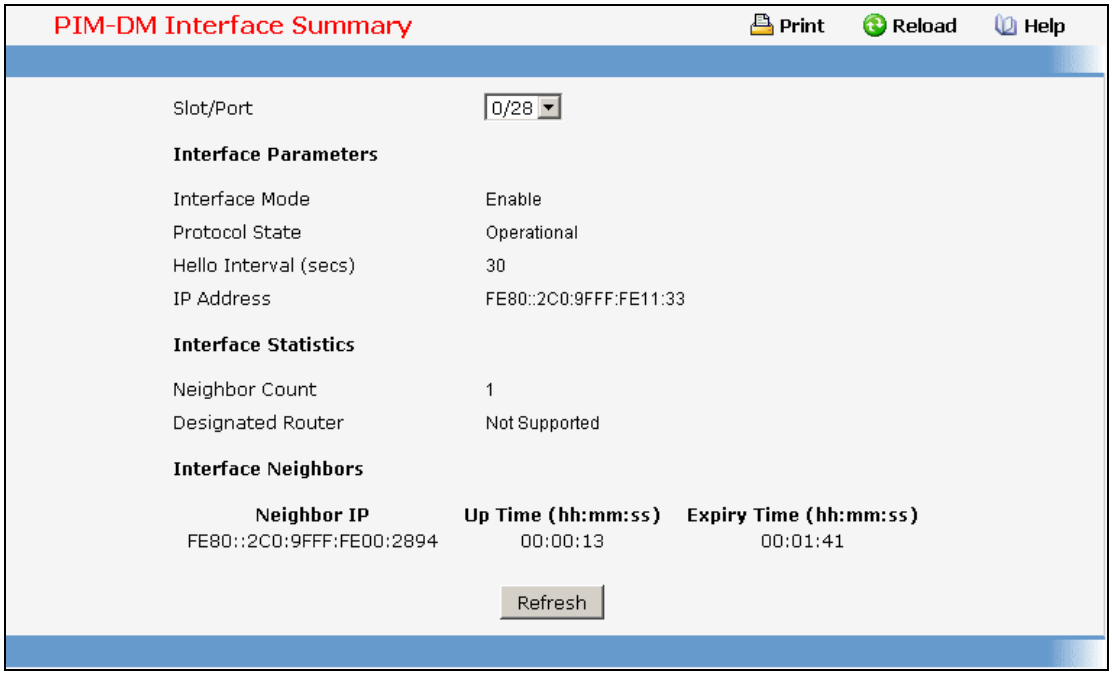
Configurable Data

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 switch. Configuration changes take effect immediately. These changes will not be retained across a power cycle unless a save is performed.

11.9.2.3 Viewing PIM-DM Interface Summary Page



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.

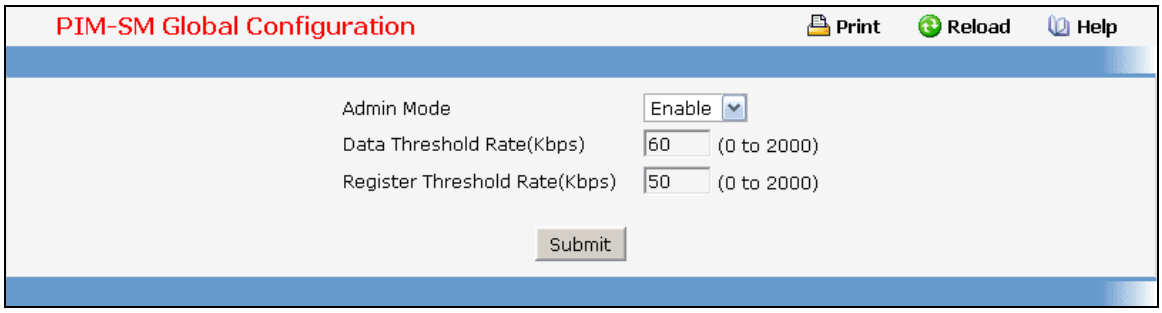
Expiry Time - The minimum time remaining before this PIM neighbor will be aged out.

Common Button

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

11.9.3 Managing PIM-SM Protocol

11.9.3.1 Configuring PIM-SM Global Configuration Page



Configurable Data

PIMSM Admin Mode - Select enable or disable from the pulldown menu to set the administrative status of PIM-SM in the router. The default is disable.

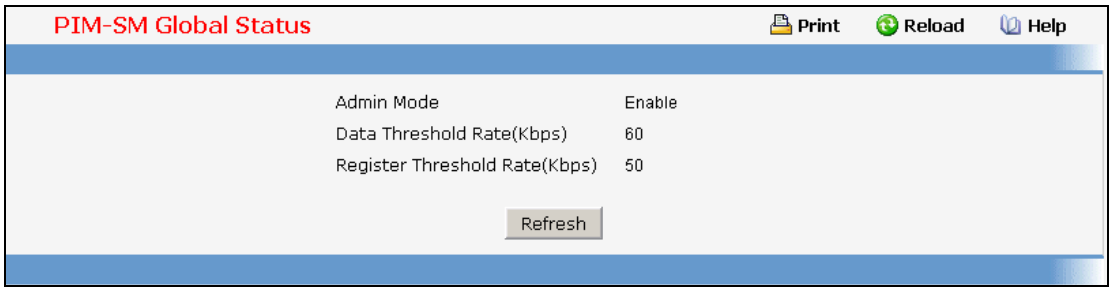
Data Threshold Rate - Enter the rate in K bits/second above which the last-hop router will switch to a source-specific shortest path tree. The valid values are from (0 to 2000) The default value is 0

Register Threshold Rate - Enter 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) 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.

11.9.3.2 Viewing PIM-SM Global Status Page



Non-Configurable Data

PIMSM Admin Mode - The administrative status of PIM-SM in the router: either enable or disable.

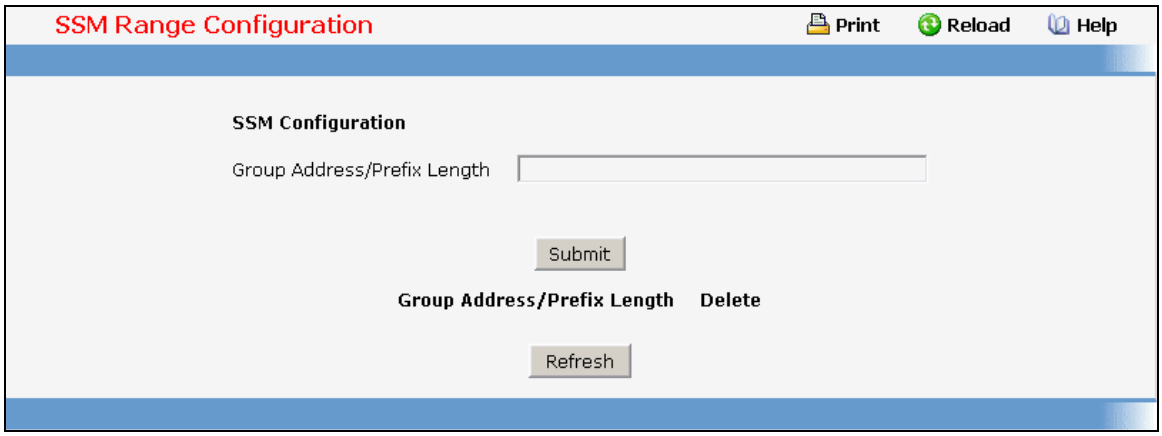
Data Threshold Rate - The minimum source data rate in K bits/second above which the last-hop router will switch to a source-specific shortest path tree.

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.

11.9.3.3 Configuring PIM-SM SSM Range Configuration Page



Configurable Data

Group Address/Prefix Length - Enter the source-specific multicast group ip-address / Prefix Length.

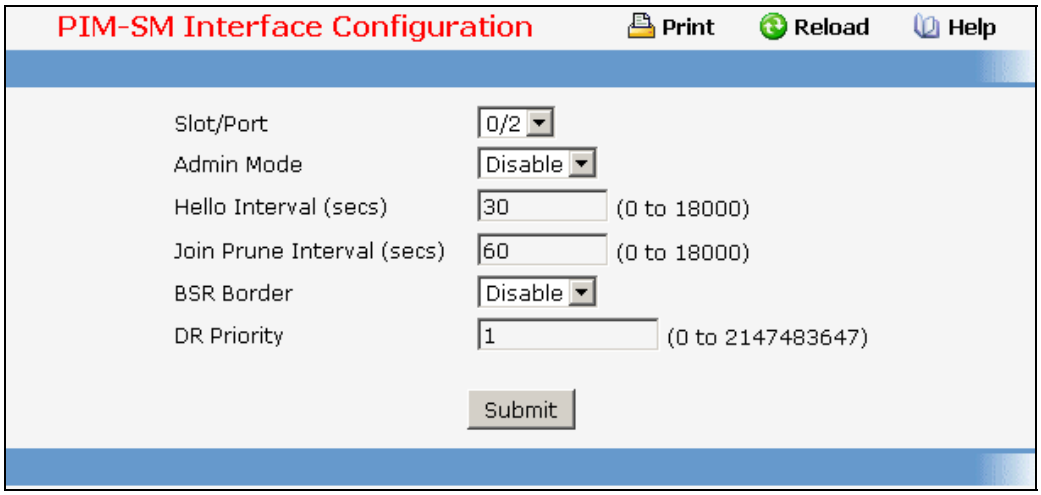
Delete - Attempts to remove the specified SSM Group Address for the PIM-SM router. Configuration changes take effect immediately. These changes will not be retained across a power cycle unless a save is performed.

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.

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

11.9.3.4 Configuring Interface's PIM-SM Configuration Page



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 (secs)- Enter the time in seconds between the transmission of which PIM Hello messages on this interface. The valid values are from (0 to 18000 secs) . The default value is 30.

Join/Prune Interval - Enter the frequency at which PIM Join/Prune messages are transmitted on this PIM interface. The valid values are from (0 to 18000) . The default value is 60.

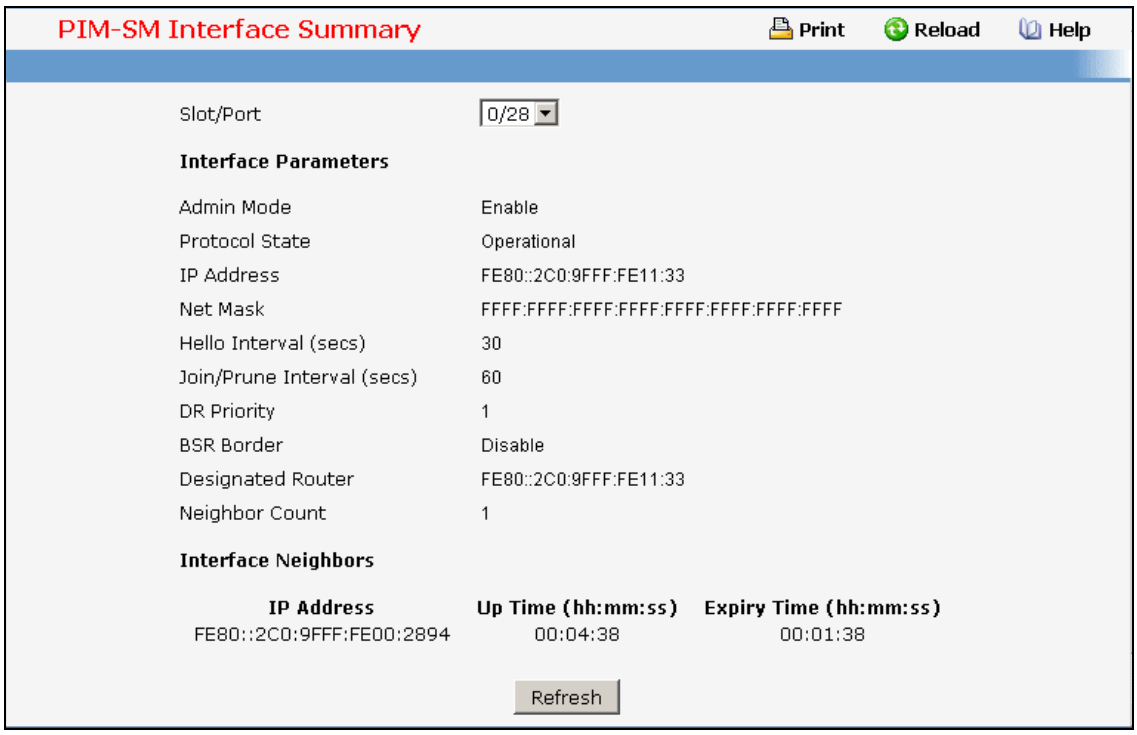
BSR Border - Select enable or disable to set BSR border status on the selected interface.

DR Priority - Enter the DR priority for the selected interface. The valid values are from (0 to 2147483647) The default value is 1.

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.

11.9.3.5 Viewing Interface's PIM-SM Summary Page



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

Admin Mode - The administrative status of PIM-SM in the router: either enable or disable.

Protocol State - The operational state of the PIM-SM protocol on this interface.

IP Address - The IP address of the selected PIM interface.

Net Mask - The network mask for the IP address of the selected PIM interface.

Hello Interval (secs) - The frequency at which PIM Hello messages are transmitted on the selected interface.

Join/Prune Interval - The frequency at which PIM Join/Prune messages are transmitted on this PIM interface.

DR Priority - Indicates the DR priority on the PIM interface.

BSR Border - Specifies the BSR border mode on the PIM interface.

Designated Router - The Designated Router on the selected PIM interface

Neighbor Count - The number of PIM neighbors on the selected interface.

IP Address - The IP address of the PIM neighbor for this entry.

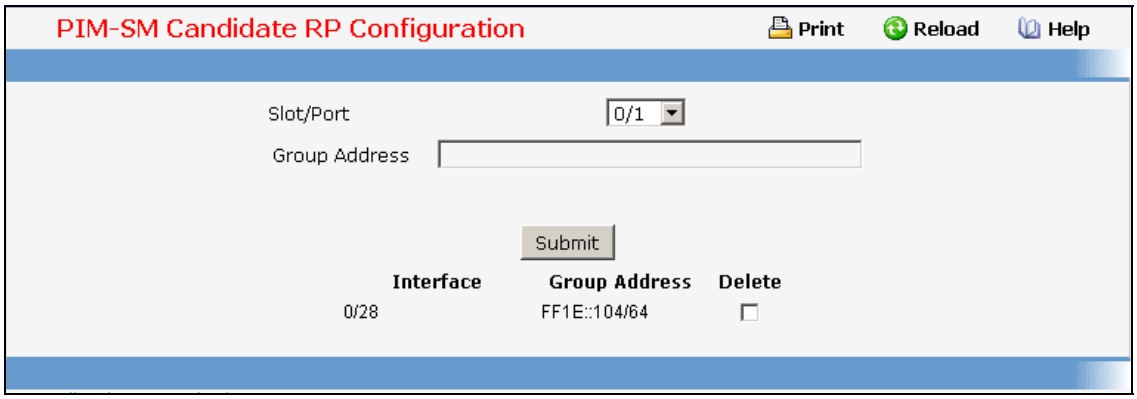
Up Time - The time since this PIM neighbor (last) became a neighbor of the local router.

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.

11.9.3.6 Configuring PIM-SM Candidate RP Configuration Page



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

Group Address - The group address transmitted in Candidate-RP-Advertisements.

Configurable Data

Interface - Display the interface.

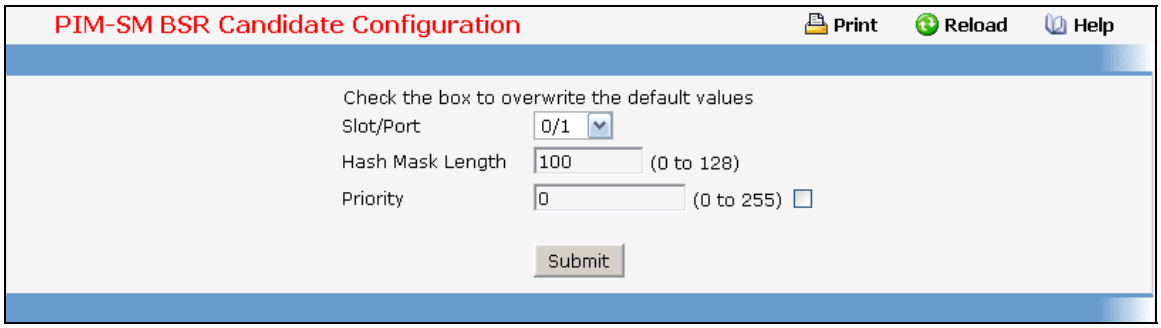
Group Address - Display the group address transmitted in Candidate – RP – Advertisements.

Delete - Attempts to remove the specified Candidate RP 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.

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.

11.9.3.7 Configuring PIM-SM BSR Candidate Configuration Page



Selection Criteria

Slot/Port - Select the slot and port for which data is to be displayed. Slot 0 is the base unit.

Configurable Data

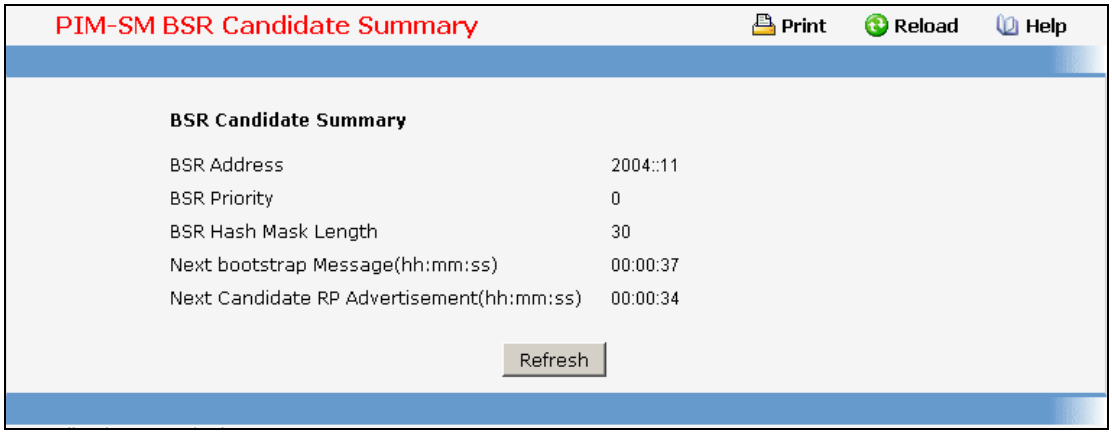
Hash Mask Length - Enter the C-BSR hash mask length to be advertised in bootstrap messages. This hash mask length will be used in the hash algorithm for selecting the RP for a particular group. The valid values are from (0 to 128). Default value is 30.

Priority - Enter the priority of C-BSR.

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.

11.9.3.8 Viewing PIM-SM BSR Candidate Summary Page



Non-Configurable Data

BSR Address - Displays the IP address of the Elected BSR.

BSR Priority - Displays the Priority of the Elected BSR.

BSR Hash Mask Length - Displays hash mask length of the Elected BSR.

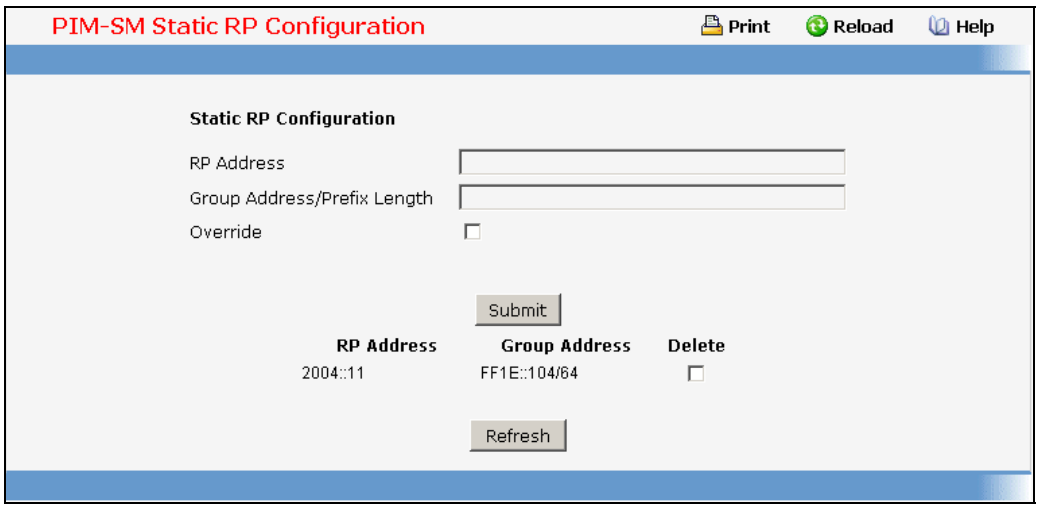
Next bootstrap Message - Time (in hours, minutes, and seconds) in which the next bootstrap message is due from this BSR.

Next Candidate RP Advertisement - Time (in hours, minutes, and seconds) in which the next candidate RP advertisement will be sent.

Command Buttons

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

11.9.3.9 Configuring PIM-SM Static RP Configuration Page



Configurable Data

RP Address - IP Address of the RP.

Group Address/Prefix Length - Enter the source-specific multicast group ip-address / Prefix Length.

Overide - To override the entry you need to check this box and then select the submit button.

Delete - Attempts to remove the specified Static RP 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.

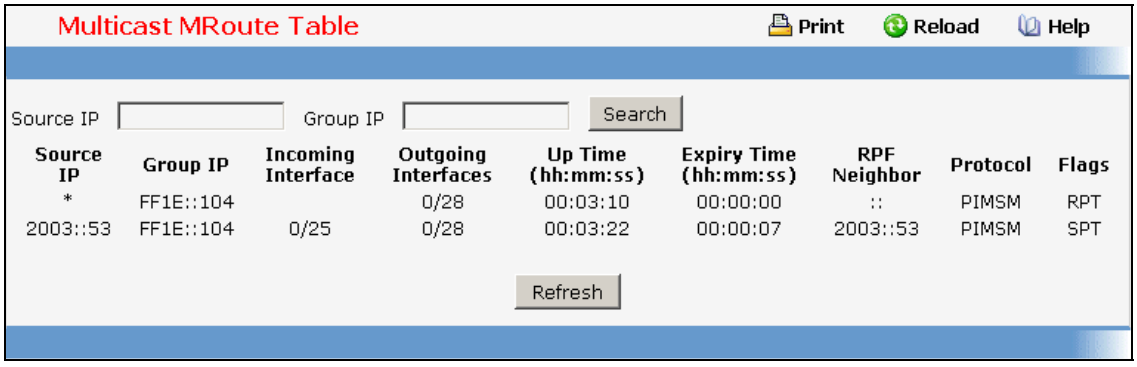
Command Buttons

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.

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

11.9.3.10 Viewing Multicast MRoute Table Page

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.



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 (secs)- The time in seconds since the entry was created.

Expiry Time (secs)- 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 a "------" is displayed.

Command Buttons

Search - Search the Mroute table for an entry matching the Source IP (if entered) and Group IP address.

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

www.fortinet.com