XENYA

Xenya Layer 2/3/4 Managed Switch

User's Guide

Applicable Products

XS52HVS

XS52HVD

XS52EVD

XS48DVx

Edition November 2012

Comments… Suggestions… Corrections…

The User documentation Department would like to know your opinion on this manual. Your feedback helps us to optimize our documentation to suit your individual needs.

Fax forms for sending us your comments are included at the back of the manual.

There you will also find the addresses of the relevant User documentation Department.

Copyright and Trademarks

Copyright © 2012 Xenya d.o.o. All rights reserved.

Delivery subject to availability; right of technical modifications reserved.

All hardware and software names used are trademarks of their respective manufacturers.

Document History

Revision	Date	Editor	Remark
0.1	12/28/2011	Moore C. J. Lee	First Edition
0.2	10/19/2010	Switch Team	2nd Edition
0.3	11/25/2012	Moore C. J. Lee	3rd Edition - Modify port-channel commands & VLAN interface commnads - Add source IP configuration support - Add Policy-based routing commands - Add AAA accounting commands

CONTENTS

1 INTRODUCTION 12

1.1 SWITCH DESCRIPTION 12
1.2 FEATURES 12
1.3 FRONT-PANEL COMPONENTS 15
1.4 REAR PANEL DESCRIPTION 15
1.5 LED INDICATORS 15
1.6 MANAGEMENT OPTIONS 16
1.7 WEB-BASED MANAGEMENT INTERFACE 16
1.8 COMMAND LINE CONSOLE INTERFACE THROUGH THE SERIAL PORT OR TELNET 16
1.9 SNMP-BASED MANAGEMENT 17

2 INSTALLATION AND QUICK STARTUP 20

2.1 PACKAGE CONTENTS 20
2.2 SWITCH INSTALLATION 21
2.3 INSTALLING THE SWITCH IN A RACK 22
2.4 QUICK STARTING THE SWITCH 23
2.5 SYSTEM INFORMATION SETUP 24
2.5.1 Quick Start up Software Version Information 24
2.5.2 Quick Start up Physical Port Data 24
2.5.3 Quick Start up User Account Management 25
2.5.4 Quick Start up IP Address 26
2.5.5 Quick Start up Uploading from Switch to Out-of-Band PC 27
2.5.6 Quick Start up Downloading from Out-of-Band PC to Switch 27
2.5.7 Quick Start up Downloading from TFTP Server 27
2.5.8 Quick Start up Factory Defaults 28

3 CONSOLE AND TELNET ADMINISTRATION INTERFACE 29

3.1 LOCAL CONSOLE MANAGEMENT 29
3.2 SET UP YOUR SWITCH USING CONSOLE ACCESS 29
3.3 SET UP YOUR SWITCH USING TELNET ACCESS 31
3.3.1 Accessing the Switch CLI Through the Network 31
3.3.2 Using the Service Port or Netowrk Interface for Remote Management 31

4 WEB-BASED MANAGEMENT 33

4.1 OVERVIEW 33
4.2 HOW TO LOG IN 34
4.3 WEB-BASED MANAGEMENT MENU 35

5 COMMAND LINE INTERFACE STRUCTURE AND MODE-BASED CLI 41

5.1 CLI COMMAND FORMAT 41
5.2 CLI MODE-BASED TOPOLOGY 42

6 SWITCHING COMMANDS 44

6.1 SYSTEM INFORMATION AND STATISTICS COMMANDS 44
6.1.1 show arp 44
6.1.2 show calendar 45
6.1.3 show process cpu 46
6.1.4 show eventlog 48
6.1.5 show running-config 49

6.1.6 show sysinfo 50
6.1.7 show system 51
6.1.8 show tech-support 52
6.1.9 show hardware 53
6.1.10 show version 55
6.1.11 show loginsession 56
6.1.12 show command filter 57
6.2 DEVICE CONFIGURATION COMMANDS 58
6.2.1 Interface 58
6.2.2 L2 MAC Address and Multicast Forwarding Database Tables 77
6.2.3 VLAN Management 85
6.2.4 Double VLAN commands 108
6.2.5 GVRP and Bridge Extension 110
6.2.6 IGMP Snooping 121
6.2.7 IGMP Snooping Querier 132
6.2.8 MLD Snooping 139
6.2.9 MLD Snooping Querier 150
6.2.10 Port Channel 157
6.2.11 Storm Control 171
6.2.12 L2 Priority 180
6.2.13 Port Mirror 182
6.2.14 Link State 185
6.2.15 Port Backup 188
6.3 MANAGEMENT COMMANDS 190
6.3.1 Network Commands 190
6.3.2 Serial Interface Commands 195
6.3.3 Telnet Session Commands 199
6.3.4 SSH Client Session Commands 207
6.3.5 SNMP Server Commands 210
6.3.6 SNMP Trap Commands 222
6.3.7 SNMP Inform Commands 234
6.3.8 HTTP commands 238
6.3.9 Secure Shell (SSH) Commands 242
6.3.10 Management Security Commands 245
6.3.11 DHCP Client Commands 246
6.3.12 DHCPv6 Client Commands 247
6.3.13 DHCP Relay Commands 249
6.3.14 sFlow Commands 251
6.3.15 Service Port Commands 261
6.3.16 Time Range Commands 267
6.4 SPANNING TREE COMMANDS 271
6.4.1 Show Commands 271
6.4.2 Configuration Commands 281
6.5 SYSTEM LOG MANAGEMENT COMMANDS 295
6.5.1 Show Commands 295
6.5.2 Configuration Commands 298
6.6 SCRIPT MANAGEMENT COMMANDS 305
6.6.1 script apply 305
6.6.2 script delete 305
6.6.3 script show 306
6.6.4 script validate 307
6.7 USER ACCOUNT MANAGEMENT COMMANDS 308
6.7.1 Show Commands 308
6.7.2 Configuration Commands 311

6.8 SECURITY COMMANDS 318
6.8.1 Show Commands 318
6.8.2 Configuration Commands 352
6.8.3 Dot1x Configuration Commands 357
6.8.4 Captive Portal Commands 367
6.8.5 TACACS+ Configuration Commands 412
6.8.6 LDAP Configuration Commands 417
6.8.7 Port Security Configuration Commands 420
6.8.8 Denial Of Service Commands 423
6.9 CDP (CISCO DISCOVERY PROTOCOL) COMMANDS 434
6.9.1 Show Commands 434
6.9.2 Configuration Commands 438
6.10 SNTP (SIMPLE NETWORK TIME PROTOCOL) COMMANDS 441
6.10.1 Show Commands 441
6.10.2 Configuration Commands 444
6.11 MAC-BASED VOICE VLAN COMMANDS 452
6.11.1 Show Commands 452
6.11.2 Configuration Commands 454
6.12 LLDP (LINK LAYER DISCOVERY PROTOCOL) COMMANDS 457
6.12.1 Show Commands 457
6.12.2 Configuration Commands 472
6.13 VTP (VLAN TRUNKING PROTOCOL) COMMANDS 482
6.13.1 Show Commands 482
6.13.2 Configuration Commands 485
6.14 PROTECTED PORTS COMMANDS 490
6.14.1 Show Commands 490
6.14.2 Configuration Commands 492
6.15 STATIC MAC FILTERING COMMANDS 493
6.15.1 Show Commands 493
6.15.2 Configuration Commands 494
6.16 SYSTEM UTILITIES 497
6.16.1 clear 497
6.16.2 copy 511
6.16.3 delete 514
6.16.4 dir 515
6.16.5 whichboot 516
6.16.6 boot-system 516
6.16.7 ping 517
6.16.8 traceroute 520
6.16.9 logging cli-command 522
6.16.10 calendar set 523
6.16.11 reload 523
6.16.12 configure 524
6.16.13 disconnect 524
6.16.14 hostname 525
6.16.15 quit 525
6.16.16 cablestatus 526
6.16.17 AutoInstall Commands 527
6.16.18 Capture CPU packet commands 531
6.17 DHCP SNOOPING COMMANDS 536
6.17.1 Show Commands 537
6.17.2 Configuration Commands 544
6.18 IP SOURCE GUARD (IPSG) COMMANDS 554
6.18.1 Show Commands 555

6.18.2 Configuration Commands 557
6.19 DYNAMIC ARP INSPECTION (DAI) COMMAND 558
6.19.1 Show Commands 559
6.19.2 Configuration Commands 563
6.20 DIFFERENTIATED SERVICE COMMAND 568
6.20.1 General Commands 570
6.20.2 Class Commands 571
6.20.3 Policy Commands 589
6.20.4 Service Commands 601
6.20.5 Show Commands 604
6.21 ACL COMMAND 612
6.21.1 Show Commands 612
6.21.2 Configuration Commands 617
6.22 IPV6 ACL COMMAND 626
6.22.1 Show Commands 626
6.22.2 Configuration Commands 628
6.23 COS (CLASS OF SERVICE) COMMAND 632
6.23.1 Show Commands 632
6.23.2 Configuration Commands 636
6.24 AUTO-VOICE OVER IP COMMANDS 641
6.24.1 Show Commands 642
6.24.2 Configuration Commands 643
6.25 ISCSI OPTIMIZATION COMMANDS 644
6.25.1 Show Commands 644
6.25.2 Configuration Commands 646
6.26 DOMAIN NAME SERVER RELAY COMMANDS 650
6.26.1 Show Commands 650
6.26.2 Configuration Commands 653
6.27 UDLD COMMANDS 661
6.27.1 Show command 661
6.27.2 Configuration Commands 663
6.28 MULTI CHASSIS LINK AGGREGATION COMMANDS 666
6.28.1 Show Commands 666
6.28.2 Configuration Commands 669

7 ROUTING COMMANDS 672

7.1 ADDRESS RESOLUTION PROTOCOL (ARP) COMMANDS 672
7.1.1 Show Commands 672
7.1.2 Configuration Commands 675
7.2 IP ROUTING COMMANDS 680
7.2.1 Show Commands 680
7.2.2 Configuration Commands 693
7.3 OPEN SHORTEST PATH FIRST (OSPF) COMMANDS 699
7.3.1 Show Commands 699
7.3.2 Configuration Commands 717
7.4 BOOTP/DHCP RELAY COMMANDS 743
7.4.1 Show Commands 743
7.4.2 Configuration Commands 744
7.5 IP HELPER COMMANDS 747
7.5.1 Show Commands 747
7.5.2 Configuration Commands 749
7.6 ROUTING INFORMATION PROTOCOL (RIP) COMMANDS 752
7.6.1 Show Commands 752
7.6.2 Configuration Commands 755

7.7 ROUTER DISCOVERY PROTOCOL COMMANDS 764
7.7.1 Show Commands 764
7.7.2 Configuration Commands 765
7.8 VLAN ROUTING COMMANDS 768
7.8.1 Configuration Commands 768
7.9 VIRTUAL ROUTER REDUNDANCY PROTOCOL (VRRP) COMMANDS 769
7.9.1 Show Commands 769
7.9.2 Configuration Commands 774

8 IP MULTICAST COMMANDS 782

8.1 DISTANCE VECTOR MULTICAST ROUTING PROTOCOL (DVMRP) COMMANDS 782
8.1.1 Show Commands 782
8.1.2 Configuration Commands 788
8.2 INTERNET GROUP MANAGEMENT PROTOCOL (IGMP) COMMANDS 790
8.2.1 Show Commands 790
8.2.2 Configuration Commands 796
8.3 MLD COMMANDS 801
8.3.1 Show Commands 801
8.3.2 Configuration Commands 805
8.4 MULTICAST COMMANDS 809
8.4.1 Show Commands 809
8.4.2 Configuration Commands 815
8.5 IPV4 PROTOCOL INDEPENDENT MULTICAST (PIM) COMMANDS 818
8.5.1 Show Commands 818
8.5.2 Configuration Commands 824
8.6 IPV6 PROTOCOL INDEPENDENT MULTICAST COMMANDS 831
8.6.1 Show Commands 831
8.6.2 Configuration Commands 838
8.7 IGMP PROXY COMMANDS 846
8.7.1 Show Commands 846
8.7.2 Configuration Commands 850
8.8 MLD PROXY COMMANDS 852
8.8.1 Show Commands 852
8.8.2 Configuration Commands 856

9 IPV6 COMMANDS 858

9.1 TUNNEL INTERFACE COMMANDS 858
9.1.1 Show Commands 858
9.1.2 Configuration Commands 860
9.2 LOOPBACK INTERFACE COMMANDS 862
9.2.1 Show Commands 862
9.2.2 Configuration Commands 863
9.3 IPV6 ROUTING COMMANDS 864
9.3.1 Show Commands 864
9.3.2 Configuration Commands 877
9.4 OSPFV3 COMMANDS 890
9.4.1 Show Commands 890
9.4.2 Configuration Commands 908
9.5 RIPNG COMMANDS 932
9.5.1 Show Commands 932
9.5.2 Configuration Commands 934

10 DATA CENTER BRIDGING COMMANDS 941

10.1 FIP SNOOPING 941

10.1.1 show fip-snooping 941
10.1.2 show fip-snooping enode 941
10.1.3 show fip-snooping session 943
10.1.4 show fip-snooping fcf 944
10.1.5 show fip-snooping vlan 945
10.1.6 fip-snooping 945
10.1.7 fip-snooping vlan 946
10.2 PRIORITY-BASED FLOW CONTROL 947
10.2.1 show dcb priority-flow-control 947
10.2.2 priority-flow-control mode 947
10.2.3 priority-flow-control priority 948
10.2.4 clear priority-flow-control statistics 948
10.3 ENHANCED TRANSMISSION SELECTION (ETS) 949
10.3.1 show dcb ets interface 949
10.3.2 ets mode 950
10.3.3 ets scheduler-type 950
10.3.4 ets weight 951
10.3.5 ets pg-mapping 952
10.4 CONGESTION NOTIFICATION 953
10.4.1 show dcb congestion-notify 953
10.4.2 show dcb congestion-notify interface 954
10.4.3 congestion-notify priority 954
10.4.4 congestion-notify tag 956
10.4.5 congestion-notify enable 957
10.4.6 congestion-notify msg 957
10.4.7 congestion-notify CPID 958
10.4.8 congestion-notify outer 959
10.4.9 congestion-notify inner 960
10.4.10 congestion-notify no-generate 961
10.5 DATA CENTER BRIDGING EXCHANGE (DCBX) 962
10.5.1 show dcbx interface 962
10.5.2 show dcbx priority-flow-control interface 963
10.5.3 show dcbx priority-group interface 965
10.5.4 dcbx enable 967
10.5.5 dcbx priority-flow-control willing 967
10.5.6 dcbx priority-group willing 968
10.6 ETHERNET VIRTUAL BRIDGING 969
10.6.1 show evb status 969
10.6.2 show evb status 970
10.6.3 show evb vsi-profile 971
10.6.4 evb enable 971
10.6.5 evb rte 972
10.7 VM TRACER COMMANDS 973
10.7.1 Show Commands 973
10.7.2 Configuration Commands 977

11 WEB-BASED MANAGEMENT INTERFACE 982

11.1 OVERVIEW 982
11.2 MANAGEMENT MENU 984
11.2.1 Viewing Information 984
11.2.2 Configuring Management Session and Network Parameters 990
11.2.3 Managing System Utilities 1003
11.2.4 File Management 1010
11.2.5 User Management 1015

11.2.6 Viewing Logs....1029
11.2.7 Viewing Statistics....1037
11.2.8 Managing SNMP and Trap....1046
11.2.9 Managing SNTP....1059
11.2.10 Managing CDP Function....1066
11.2.11 Managing UDLD....1069
11.2.12 Managing LLDP....1071
11.2.13 Managing LLDP-MED....1081
11.2.14 Managing sFlow....1088
11.2.15 Managing DHCP Client....1094
11.2.16 Managing Time Ranges....1096
11.2.17 Managing DNS Relay Function....1100
11.2.18 Managing DDNS Function....1105
11.3 SWITCHING MENU....1106
11.3.1 Defining Forwarding Database....1106
11.3.2 Managing Switch Interface....1108
11.3.3 Managing DHCP Snooping....1115
11.3.4 DHCP Snooping Information Option 82....1121
11.3.5 Managing IP Source Guard (IPSG)....1125
11.3.6 Managing Port-Based VLAN....1128
11.3.7 Managing DVLAN....1134
11.3.8 Managing Protected Ports....1136
11.3.9 Managing Protocol-based VLAN....1138
11.3.10 Managing IP Subnet-based VLAN....1141
11.3.11 Managing MAC-based VLAN....1143
11.3.12 Managing MAC-based Voice VLAN....1145
11.3.13 Managing Voice VLAN....1147
11.3.14 Managing MAC Filters....1148
11.3.15 Managing GARP....1150
11.3.16 Managing VTP....1154
11.3.17 Managing Dynamic ARP Inspection (DAI)....1156
11.3.18 Managing IGMP Snooping....1162
11.3.19 Managing IGMP Snooping Querier....1171
11.3.20 Managing MLD Snooping....1175
11.3.21 Managing MLD Snooping Querier....1183
11.3.22 Viewing Multicast Forwarding Database....1187
11.3.23 Managing Port-Channel....1192
11.3.24 Managing Spanning Tree....1195
11.3.25 Managing MLAG....1207
11.3.26 Managing Link State....1212
11.3.27 Managing Port-Backup....1214
11.4 SECURITY MENU....1216
11.4.1 Managing Access Control (802.1x)....1216
11.4.2 Managing Port Security....1234
11.4.3 Managing Captive Portal....1239
11.4.4 Managing RADIUS....1261
11.4.5 Managing TACACS+ Configuration....1271
11.4.6 Managing LDAP Configuration....1273
11.4.7 Managing Access Control Lists....1274
11.4.8 Managing IP Filter Configuration....1296
11.4.9 Managing Secure HTTP Configuration....1298
11.4.10 Managing Secure Shell Configuration....1300
11.4.11 Managing Denial of Service Page....1302
11.5 QOS MENU....1304

11.5.1 Managing Differentiated Services 1304
11.5.2 Configuring Diffserv Wizard Page 1316
11.5.3 Managing Auto VoIP 1318
11.5.4 Managing iSCSI 1321
11.5.5 Managing Class of Service 1325
11.6 ROUTING MENU 1332
11.6.1 Managing ARP Table 1332
11.6.2 Managing IP Interfaces 1335
11.6.3 Managing OSPF 1342
11.6.4 Managing BOOTP/DHCP Relay Agent 1366
11.6.5 Managing IP Helper 1368
11.6.6 Managing Routing Information Protocol (RIP) 1374
11.6.7 Managing Router Discovery 1381
11.6.8 Managing Route Table 1383
11.6.9 Managing VLAN Routing 1388
11.6.10 Managing VRRP 1390
11.6.11 Managing Tunnels 1402
11.6.12 Managing Loopbacks 1404
11.7 IPV6 MENU 1406
11.7.1 Managing IPv6 Global Configuration Page 1406
11.7.2 Managing IPv6 Interface Configuration Page 1407
11.7.3 Viewing IPv6 Interface Summary Page 1410
11.7.4 Viewing IPv6 Interface Statistics Page 1411
11.7.5 Viewing IPv6 Neighbor Table Information Page 1416
11.7.6 Viewing DHCPv6 Client Parameters 1417
11.7.7 Managing OSPFv3 Protocol 1419
11.7.8 Managing IPv6 Routes 1438
11.7.9 Managing RIPv6 1442
11.8 IPV4 MULTICAST MENU 1445
11.8.1 Configuring IPv4 Multicast Global 1445
11.8.2 Configuring IPv4 Multicast Interface 1446
11.8.3 Configuring Multicast Admin Boundary 1447
11.8.4 Viewing IPv4 Multicast Admin Boundary Summary 1448
11.8.5 Managing DVMRP 1449
11.8.6 Managing IGMP 1455
11.8.7 Managing PIM Protocol 1465
11.8.8 Viewing IPv4 Multicast Mroute Table 1475
11.8.9 Configuring IPv4 Multicast Static MRoute Table Configuration 1476
11.8.10 Viewing IPv4 Multicast Static MRoute Table Summary 1477
11.9 IPV6 MULTICAST MENU 1478
11.9.1 Managing MLD 1478
11.9.2 Managing PIM Protocol 1490
11.9.3 Viewing IPv6 Multicast MRoute Table 1501
11.9.4 Configuring IPv6 Multicast Static MRoute Table Configuration 1502
11.9.5 Viewing IPv6 Multicast Static MRoute Table Summary 1503
11.10 DATA CENTER 1504
11.10.1 Managing Congestion Notification 1504
11.10.2 Managing Data Bridging Exchange 1507
11.10.3 Managing PFC 1510
11.10.4 Managing ETS 1512
11.10.5 Managing FIP-Snooping 1514
11.10.6 Managing EVB 1516
11.10.7 Managing VM Tracer 1519

1 Introduction

1.1 Switch Description

The XS52HVD is a 48 1Gigabit plus 4 SFP+ 10Gigabit 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 1Gigabit Ethernet ports to function as a central distribution hub for other switches, switch groups, or routers. The one built-in 1000/100/10 Ethernet port for out of band management service. It also supports hot-swappable redundant power system (RPS) to ensure system reliability.

1.2 Features

- Supports 48 10/100/1000BASE-T RJ45 Ethernet ports
- Supports 4 SFP+ 10Gigabit uplink ports
- 1 built-in 1000/100/10 Ethernet port for out of band switch mangement.
- Support at most two power supplies (Depend on customer how many power they need) 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 ethernet 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
- Link Agregation (802.1ad LACP)
- Multi-chassis Link Aggregation (MLAG)
- 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 access control and RADIUS client support
- TACACS+ support
- LDAP support
- UDLD support
- Administrator-definable port security

- AAA support
- 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
- 32-way ECMP support
- /31 subnets support
- Source IP configuration support
- Poilcy Based Routing (PBR)
- 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
- IP Helper (BOOTP/DHCP Relay)
- DNS Client and Relay support
- DDNS client support
- Per-port bandwidth control
- SNMP v1, v2, v3 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
- Auto Install 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)
- Data Center Bridge Exchange (DCBX, IEEE802.1Qaz) (*)
  CEE 1.01 support
  IEEE version support
- Ethenet Virtual Bridge (EVB) (*)
  VEB/VEPA bridge support
- VM Tracer (*)
  VMware vSphere support
  VM Auto Discovery
  VM Adaptive Segmentation
  VM Host View

(*) Only support on XS52EVD and XS48DVx.

1.3 Front-Panel Components

The front panel of the Switch consists of 48 1-Giga interfaces, 4 SFP+10-Giga interfaces, 2 LED indicators, one built-in 1000/100/10 RJ-45 Ethernet service ports, an RS-232 communication port.

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. The management port (RJ-45 port) has two LED indicators. The Left side represents speed and Right side represents activity. The speed light will has three different colors for connecting speed 10M (Color Green), 100M (Color Yellow), and 1G (Color Orange). The activity light will have a yellow blinking once the mgmt port has a receive/transmit data.

1.4 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.

1.5 LED Indicators

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

1.6 Management Options

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

1.7 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.

1.8 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.

1.9 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:

- RFC1493 Bridge
- RFC 2819 RMON-MIB
- RFC 2233 Interface MIB
- 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)
- Xenya Enterprise MIB
- ROUTING-MIB
- MGMD-MIB
- RFC 2934 PIM-MIB
- DVMRP-STD-MIB
- IANA-RTPROTO-MIB
- MULTICAST-MIB
- ROUTING6-MIB
- IEEE8021-PAE-MIB
- INVENTORY-MIB
- MGMT-SECURITY-MIB
- QOS-MIB
- QOS-ACL-MIB
- QOS-COS-MIB
- QOS-AUTOVOIP-MIB

- QOS-DIFFSERV-PRIVATE-MIB
- QOS-ISCSI-MIB
- RFC 1907 - SNMPv2-MIB
- RFC 2465 - IPV6-MIB
- RFC 2466 - IPV6-ICMP-MIB
- TACACS-MIB
- IGMP/MLD Snooping
- IGMP/MLD Layer2 Multicast
- QoS - IPv6 ACL
- Voice VLAN
- Guest VLAN
- LLDP-MIB
- LLDP MED
- RFC 2925 (DISMAN-TRACEROUTE-MIB)
- RFC 2080 (RIPng)
- OSPFV3-MIB
- RFC 2571 - SNMP-FRAMEWORK-MIB
- RFC 2572 - SNMP-MPD-MIB
- RFC 2573 - SNMP-NOTIFICATION-MIB
- RFC 2573 - SNMP-TARGET-MIB
- RFC 2574 - SNMP-USER-BASED-SM-MIB
- RFC 2576 - SNMP-COMMUNITY-MIB
- RFC 2263 - USM-TARGET-TAG-MIB
- RFC 3176 - SFLOW-MIB
- IEEE8023-LAG-MIB (IEEE Std 802.3ad)
- RFC 2674 - P-BRIDGE-MIB
- RFC 2674 - Q-BRIDGE-MIB
- RFC 2737 - ENTITY-MIB
- RFC 2863 - IF-MIB
- RFC 3635 - Etherlike-MIB
- PORTSECURITY-PRIVATE-MIB
- RADIUS-CLIENT-PRIVATE-MIB
- CAPTIVE-PORTAL-MIB
- RFC 5060 - PIM-STD-MIB
- RFC 5240 - PIM-BSR-MIB
- RFC 3419 - TRANSPORT-ADDRESS-MIB
- IANA-MAU-MIB

2 Installation and Quick Startup

2.1 Package Contents

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

One XS52HVD Layer 2/3/4 1-Gigabit Managed Switch

- Mounting kit: 2 mounting brackets and screws

Four rubber feet with adhesive backing

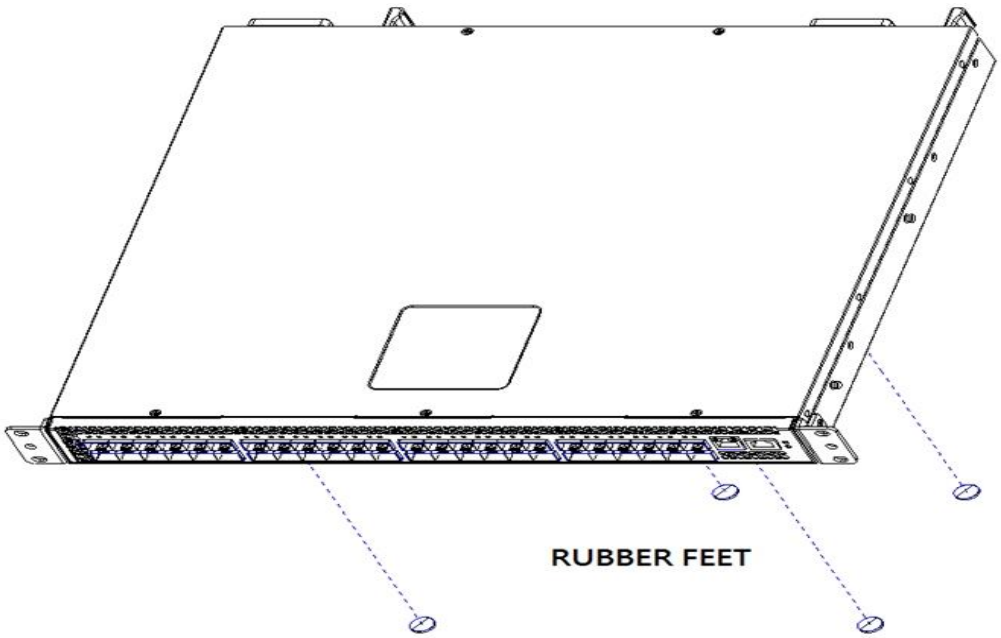
- Redundant AC power cord

2.2 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.

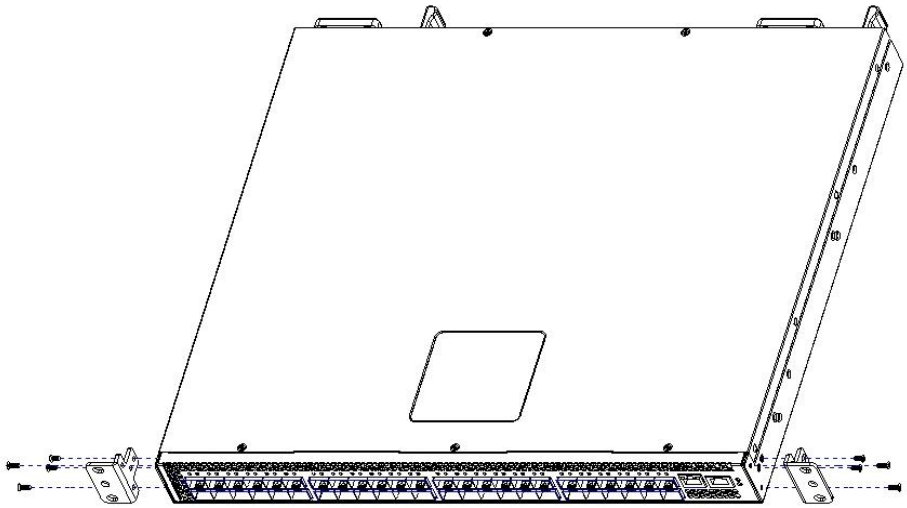
The rubber feet are recommended to keep the unit from slipping.



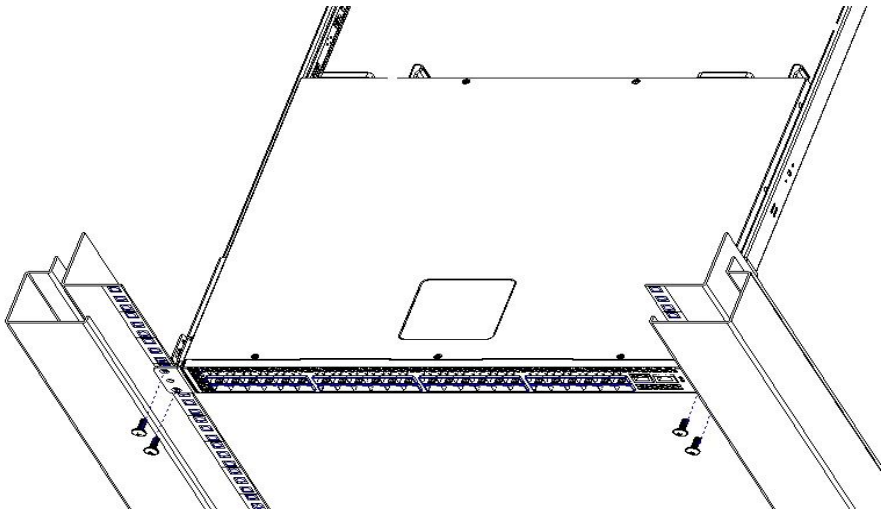
2.3 Installing the Switch in a Rack

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



2.4 Quick Starting the Switch

1. Read the device Installation Guide for the connectivity procedure. In-band connectivity allows access to the 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, suggesting 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.

2.5 System Information Setup

2.5.1 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

2.5.2 Quick Start up Physical Port Data

Table 2-2. Quick Start up Physical Port

Command	Details
show Interface status [<slot/port>]	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

2.5.3 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.

2.5.4 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 Interface Status - Indicates whether the interface is up or down. IP Address - IP Address of the interface Subnet Mask - IP Subnet Mask for the interface. MAC Address - The MAC Address used for this inband connectivity Network Configurations Protocol Current - Indicates which network protocol is being used. Default is none.
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

2.5.5 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.

2.5.6 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.

2.5.7 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.

2.5.8 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 [warm]	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. warm - indicates only switch application is restarted.

3 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.

The command-line interface (CLI) provides a text-based way to manage and monitor the switch features. You can access the CLI by using a direct connection to the console port or by using a Telnet or SSH client. To access the switch by using Telnet or Secure Shell (SSH), the switch must have an IP address configured on either the service port or the network interface, and the management station you use to access the device must be able to ping the switch IP address. DHCP is enabled by default on the service port. It is disabled on the network interface.

3.1 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.

3.2 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: 115,200
- Data width: 8 bits
- Parity: none
- Stop bits: 1
- Flow Control: none

A typical console connection is illustrated below:

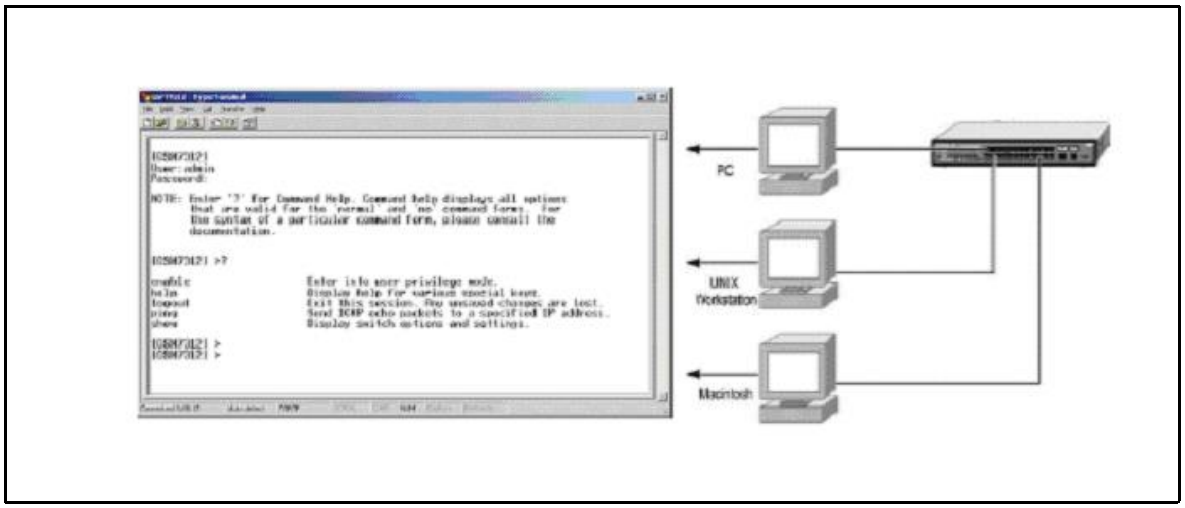


Figure 3-1: Console Setting Environment

3.3 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.

3.3.1 Accessing the Switch CLI Through the Network

Remote management of the switch is available through the service port or through the network interface. To use telnet, SSH, SNMP for swith management, the switch must be connected to the network, and you must know the IP or IPv6 address of the management interface. The switch has no IP address by default. The DHCP client on the service port is enabled, and the DHCP client on the network interface is disaled.

3.3.2 Using the Service Port or Netowrk Interface for Remote Management

The service port is a dedicated Ethernet port for out-of-band management. We recommend that you use the service port to manage the switch. Traffic on this port is segregated from operational network traffic on the switch ports and cannot be switched or routed to the operational network. Additonally, if the production network is experiencing problems, the service port still allows you to access the switch management interface and troubleshoot issues. Configuration options on the service port are limited, which makes it difficult to accidentally cut off management access to the switch.

Alternatively, you can choose to manage the switch through the production network, which is known as in-band management, Bacuse in-nbad management traffic is mixed in with production netowork traffic, it is subject to all of the filtering rules usually applied on a switched/routed port such as ACLs and VLAN tagging. You can access the in-band network management interface through a connection to any front-panel port.

3.3.2.1 Configuring Service Port Information

To disable DHCP/BootP and manually assign an IPv4 address, enter commands under Global Configuration mode:

serviceport protocol none

serviceport ip ipaddress netmask

For example, serviceport ip 192.168.2.22 255.255.255.0

To disable DHCP/BootP and manually assign an IPv6 address, enter commands under Global Configuration mode:

serviceport protocol none dhcp6

serviceport ipv6 enable

serviceport ipv6 address address/prefix-length

serviceport ipv6 gateway ipv6-address

To view the assigned or configured network address, use:

show serviceport

To enable the DHCP/DHCPv6 client on the service port, use:

serviceport protocol dhcp

serviceport protocol dhcp6

To enable the BootP client on service port, use:

serviceport protocol bootp

3.3.2.2 Configuring the In-Band Netowrk Interface

To use a DHCP server to obtain the IP address, subnet mask, and default gateway information, use:

interface vlan 1

ip address dhcp

ipv6 address dhcp

To manually configure the IPv4 address, subnet mask, use:

interface vlan 1

ip address ipaddress netmask

To manually configure the IPv6 address, subnet mask, use:

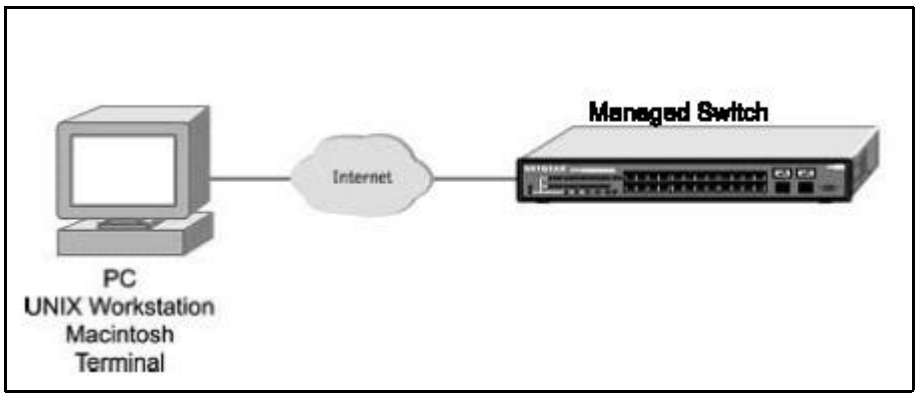
interface vlan 1

ipv6 address address/prefix-length

4 Web-Based Management

4.1 Overview

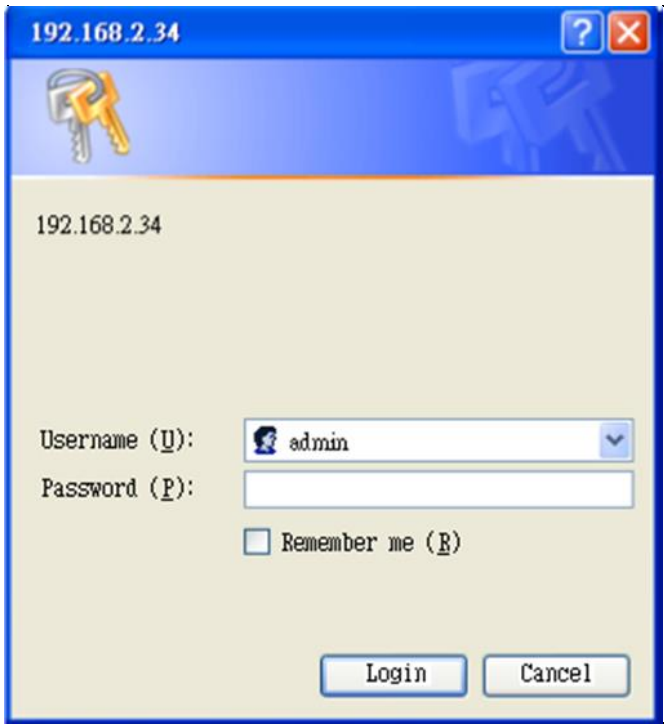
The Xenya Layer 2/3/4 Managed Switch provides a built-in browser interface that lets you configure and manage it remotely using a standard Web browser such as Microsoft Internet Explorer 5.0 or later or Netscape Navigator 6.0 or later. This interface also allows for system monitoring and management of 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.



4.2 How to log in

The Xenya Layer 2/3/4 Managed Switch can be configured remotely from Microsoft Internet Explorer (version 5.0 or above), or Mozilla FireFox (version 3.6 or above).

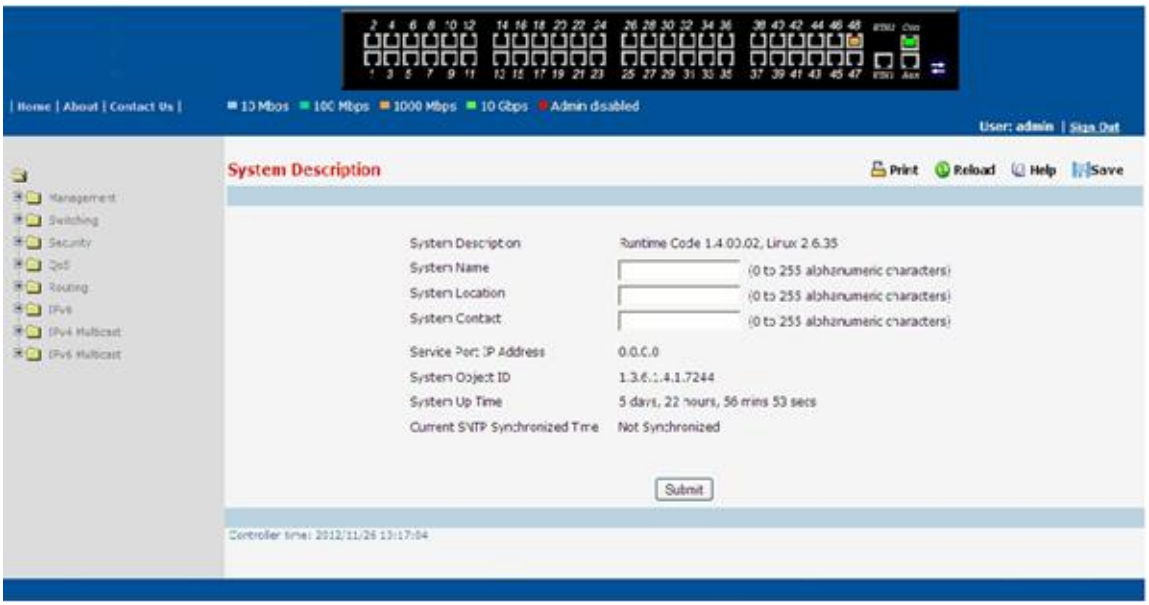
1. Determine the IP address of your managed switch.
2. Open your Web browser.
3. Log in to the managed switch using whatever IP address the unit is currently configured with.



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 XS52HVD Series Layer 2/3/4 Managed Switch and display the home page, as shown below.

4.3 Web-Based Management Menu



This above page displays system information, such as:

System Description

- System Name
- System Location
- System Contact
- Service Port IP Address
- System Object ID (OID)
- System Up Time
- Current SNTP Synchronized Time

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

- Management
- Switching
- Security

- QoS
- Routing
- IPv6
- IPv4 Multicast
- IPv6 Multicast
- Data Center (*)

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.

Management

- Information— see “show arp” and “show hardware”
- Configuration — see “Management Commands and Device Configuration Commands”
- System Utilities — see “System Utilities”
- File Management — see “Copy and Delete Commands”
- User Management — see “User Account and AAA Commands”
- Statistics — see “show interface counters”
- Logs — see “System Information and Statistics Commands”
- SNMP — see “SNMP Server Commands and SNMP Trap Commands”
- SNTP — see “SNTP Commands”
- CDP — see “CDP Commands”
- LLDP — see “LLDP Commands”
- UDLD — see “UDLD Commands”
- sFlow — see “sFlow Commands”
- DHCP Client — see “DHCP Client Commands”
- Time Ranges - see “Time Ranges Commands”
- DNS Relay — see “Domain Name Server Relay Commands”
- DDNS - see “DDNS Commands”

Switching

- Forwarding Database — see “Device Configuration Commands’ L2MAC Address”
- Port — see “Device Configuration Commands’ Interface”
- DHCP Snooping — see “DHCP snooping Commands”
- VLAN — see “VLAN Management Commands”
- DVLAN—see “DVLAN 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”
- VTP — see “VTP Commands”
- GARP — see “GVRP and Bridge Extension Commands”
- MAC Filters — see “MAC Filters 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”
- MLAG — see “Multi-Chassis Link Aggregation Commands”
- Link State — see “Link state Commands”
- Port Backup — see “Port backup Commands”

Security

- Port Access Control — see “Dot1x Configuration Commands”
- Port Security — see “Port Security Configuration Commands”
- Captive Portal — see “Captive Portal Commands” (Not support in XS48DSD and XS52HVx)
- RADIUS — see “Radius Configuration Commands”
- TACACS+ — see “TACACS+ Configuration Commands”
- LDAP - see “LDAP Configuration Commands”
- Access Control List — see “ACL Commands”
- IP Filter — see “Network Commands”
- Secure HTTP — see “HTTP Commands”
- Secure Shell — see “Secure Shell (SSH) Commands”
- Denial of Service — see “Denial of Service Commands”

QoS

- Differentiated Services — see “Differentiated Services Commands”
- Class of Service — see "Class of Service Commands" and “L2 Priority Commands”
- Auto VoIP — “Auto-Voice over IP Commands”
- iSCSI — “iSCSI Optimization 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”
- DHCP Client - see “DHCP Client Commands”
- IP Helper - see “IP Helper 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”

IPv6

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

Data Center (*)

- Congestion Notification — see “Congestion Notification Commands”
- Data Center Bridging Exchange — see “Data Center Bridging Exchange Commands”
- PFC — see “Priority-based Flow Control Commands”
- ETS — see “Enhanced Transmission Selection(ETS) Commands”
- FIP — see “FIP Snooping Commands”
- EVB — see “EVB Commands”
- VM Tracer — see “VM Trace commands”

5 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.

5.1 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.

5.2 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> (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
```

6 Switching Commands

6.1 System Information and Statistics commands

6.1.1 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.

6.1.2 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

6.1.3 show process cpu

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

Syntax

show process cpu

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 250978304

alloc 275599360

CPU Utilization:

PID	Name	5 Secs	60 Secs	300 Secs
1030	osapiTimer	0.00%	0.02%	0.02%
1032	_interrupt_thread	0.00%	0.02%	0.02%
1034	bcmL2X.0	1.99%	2.10%	1.81%
1035	bcmCNTR.0	1.59%	1.42%	1.19%
1038	bcmLINK.0	2.99%	2.84%	2.44%
1040	bcmL2X.1	1.99%	2.09%	1.81%
1041	bcmCNTR.1	1.39%	1.40%	1.19%
1042	bcmLINK.1	2.99%	2.87%	2.45%
1043	bcmRX	0.19%	0.19%	0.16%

1044	cpuUtilMonitorTask	0.19%	0.14%	0.11%
1046	tL7Timer0	0.00%	0.02%	0.01%
1054	simPts_task	0.00%	0.02%	0.01%
1058	Detecting SFP+ Modu	0.00%	0.02%	0.01%
1080	emWeb	0.00%	0.08%	0.06%
1085	StormCtrl Log Table	0.00%	0.03%	0.03%
1091	SNMPTask	1.79%	12.48%	37.44%
1101	dot1s_timer_task	0.19%	0.07%	0.04%
1118	sFlowTask	0.00%	0.09%	0.11%
1135	RMONTask	0.00%	0.12%	0.15%
1137	udldTask	0.00%	0.01%	0.01%
Total CPU Utilization		15.37%	26.14%	49.21%

6.1.4 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.

unit parameter is only support for stacking platform.

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.

Event log information is retained across a switch reset.

6.1.5 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

6.1.6 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 255 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 255 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 Synchronized Time: The time which is synchronized from SNTP server.

6.1.7 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 255 alpha-numeric characters. The factory default is blank.

System Contact: Text used to identify a contact person for this switch. May be up to 255 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.

6.1.8 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 interface status, show logging, show event log, show logging buffered, show trap log, show running config, … etc.

Syntax
show tech-support

Default Setting

None

Command Mode

Privileged Exec

This command is only support on console port.

6.1.9 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.

ADT7470_1: Sensor 1 Now Temperature: The temperature of sensor 1 of ADT7470.

ADT7470_1: Sensor 2 Now Temperature: The temperature of sensor 2 of ADT7470.

ADT7470_1: Sensor 3 Now Temperature: The temperature of sensor 3 of ADT7470.

ADT7470_1: Sensor 4 Now Temperature: The temperature of sensor 4 of ADT7470.

Depend on air flow FAN 1 - 4 connected ADT7470-1 or ADT7470-2: Front-

To-Back: (Connected ADT7470-1)

ADT7470_1: FAN 1 Status: Status of FAN1. It could be active or inactive.

ADT7470_1: FAN 2 Status: Status of FAN2. It could be active or inactive.

ADT7470_1: FAN 3 Status: Status of FAN3. It could be active or inactive.

Back-To-Front: (Connected ADT7470-2)

ADT7470_2: FAN 1 Status: Status of FAN1. It could be active or inactive.

ADT7470_2: FAN 2 Status: Status of FAN2. It could be active or inactive.

ADT7470_2: FAN 3 Status: Status of FAN3. It could be active or inactive.

Switch Power+ y……Active/Inactive (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 Number: 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: (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.

6.1.10 show version

This command displays inventory information for the switch.

Syntax

show version

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.

FRU Number: The field replaceable unit number.

Part Number: Manufacturing part number.

Maintenance Level: The identification of the hardware change level.

Manufacturer: The two-octet code that identifies the manufacturer.

Burned In MAC Address: The burned-in universally administered MAC address of this switch.

Software Version: The platform.function.release. maintenance number of the code currently running on the switch.

Operating System: The operating system currently running on the switch.

Network Processing Device: Identifies the network processor hardware.

Additional Packages: A list of the optional software packages installed on the switch, if any. For example, QOS, Routing, IPv6, IPv6 Management, Multicast or Data Center.

6.1.11 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 port, SSH or HTTP/HTTPS.

6.1.12 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

6.2 Device Configuration Commands

6.2.1 Interface

6.2.1.1 show interface status

This command displays the Port monitoring information for the system.

Syntax

show interface status [{<slot/port> | loopback <loopback-id> | port-channel <portchannel-id> | tunnel <tunnel-id> | vlan <vlan-id>}]

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

<loopback-id> - Disaplys information for the loopback interfaces. The range of the loopback ID is 0 to 7.

<portchannel-id> - Displays information for the port-channel interfaces. The range of the port-channel ID is 1 to 64.

<tunnel-id> - Displays information for the tunnel interfaces. The range of the tunnel ID is 0 to 7.

<vlan-id> - Displays information for the vlan interfaces. The range of the VLAN ID is 1 to 4093. no

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: Disable:

This port is disabled flow control.

Enable: This port is enabled flow control.

Capabilities Status: Displays interface capabilities.

6.2.1.2 show interface counters

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

Syntax

show interface counters [{<slot/port> | [port-channel <portchannel-id>]}]

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

<portchannel-id> - is the desired port-channel interface number. The range of the port-channel ID is 1 to 64.

no paramter - Displays statistics information for all interfaces.

Default Setting

None

Command Mode

Privileged Exec

Display Message

The display parameters when the argument is '<slot/port>' or port-channel 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 if no argument is used are as follows:

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

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.

Time Since Counters Last Cleared: The elapsed time, in days, hours, minutes, and seconds since the statistics for this port were last cleared.

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> | port-channel <portchannel-id> | switchport}
```

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

<portchannel-id> - is the desired port-channel interface number. The range of the port-channel ID is 1 to 64.

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>' or port-channel 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.

6.2.1.3 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.

6.2.1.4 interface

This command is used to enter Interface configuration mode.

Syntax

interface {<slot/port> | loopback <loopback-id> | port-channel <portchannel-id> | tunnel <tunnel-d> | vlan <vlan-id>}

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

<loopback-id> - is the desired loopback interface number. The range of loopback ID is 0 to 7.

<portchannel-id> - is the desired port-channel interface number. The range of port-channel ID is 1 to 64.

<tunnel-id> - is the desired tunnel interface number. The range of tunnel ID is 0 to 7.

<vlan-id> - is the desired vlan interface number. The range of VLAN ID is 1 to 4093.

Default Setting

None

Command Mode

Global Config

6.2.1.5 speed-duplex

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

i The 10-Giga interfaces could be configured to operate at 10-Giga or 1-Giga speed. Use 'speed-duplex 1000' to change the speed of 10-Giga port to 1G speed.

The speed of 40-Giga interfaces can not be changed by this command.

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 10G ports.

Default Setting

None

Command Mode

Global Config

6.2.1.6 negotiate

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

The 10-Giga and 40-Giga interfaces do not provide the following command.

Syntax

```
negotiate
no negotiate
```

no - This command disables automatic negotiation on a port.

Default Setting

Disable

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

Disable

Command Mode

Global Config

6.2.1.7 capabilities

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

The 10-Giga and 40-Giga interfaces do 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

10G full-duplex for 10G ports

40G full-duplex for 40G ports

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 full/half duplex, 100 full/half duplex and 1000 full duplex for 1G ports.

10G full-duplex for 10G ports

40G full-duplex for 40G ports

Command Mode

Global Config

6.2.1.8 storm-control flowcontrol

This command enables 802.3x flow control for the switch.

802.3x flow control only applies to full-duplex mode ports. If PFC feature is enabled on the same interface, 802.3x flow control will be disabled internally.

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. If PFC feature is enabled on the same interface, 802.3x flow control will be disabled internally.

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

6.2.1.9 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

6.2.1.10 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

6.2.1.11 mdi

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

This command is not provided for the 10-Giga SFP+ interface and 40G QSFP interface.

6.2.2 L2 MAC Address and Multicast Forwarding Database Tables

6.2.2.1 show mac-addr-table

This command displays the forwarding database entries. If the command is entered with no parameter, the entire table is displayed. 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> <vlan-id>}]

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

<vlan-id> - VLAN ID (Range: 1 - 4093)

no parameter - 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.

6.2.2.2 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.

6.2.2.3 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> | port-channel <portchannel-id> | vlan <vlan-id>}

<slot/port> - Specifies the desired interface.

<portchannel-id> - Specifies the desired port-channel interface. The range of port-channel ID is 1 to 64.

<vlan-id> - Specifies the desired VLAN interface. The range of VLAN ID is 1 to 4093.

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.

6.2.2.4 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:).

6.2.2.5 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:).

6.2.2.6 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> <vlan-id>]]

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

<vlan-id> - VLAN ID (Range: 1 - 4093)

no parameter - 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.

6.2.2.7 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.

6.2.2.8 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.

6.2.2.9 mac-addr-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

6.2.3 VLAN Management

6.2.3.1 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 4093.

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.

6.2.3.2 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 - 4093)

<vlanname> - vlan name (up to 32 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 4093.

VLAN Name: A string associated with this VLAN as a convenience. It can be up to 32 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.

6.2.3.3 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 4093.

Priority: There is a priority for each MAC-based.

6.2.3.4 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 4093.

Priority: There is a priority for each IPsubnet-based.

6.2.3.5 show vlan internal usage

This command displays the VLAN assigned to port-based routing interfaces.

Syntax
show vlan internal usage

Default Setting

None

Command Mode

Privileged Exec

Display Message

Base VLAN ID: This is the Base VLAN ID for Internal allocation of VLANs to the routing interface.

Allocation Policy: Allocation Policy for VLAN ID in ascending or descending order.

VLAN: This is the Used Internal VLAN ID for the Interface.

Usage: This is the switch interface.

6.2.3.6 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>]

<group-name> - The group name of an entry in the Protocol-based VLAN table. no

parameter - 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.

6.2.3.7 show interface switchport

This command displays VLAN port information.

Syntax

show interface switchport {[<slot/port>] | port-channel <portchannel-id>}

<slot/port> - Interface number.

<portchannel-id> - port-channel interface number. The range of port-channel ID is 1 to 64. no parameter - 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.

6.2.3.8 vlan database

This command is used to enter VLAN Interface configuration mode.

Syntax

```
vlan database
```

Default Setting

None

Command Mode

Global Config

6.2.3.9 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 2-4093.

Syntax

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

<vlan-list> - VLAN ID (Range: 2 - 4093) - 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 2-4093.

Default Setting

None

Command Mode

VLAN database

6.2.3.10 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- 4093.

Syntax

```
vlan name <vlan-id> <newname>
no vlan name <vlan-id>
```

<vlan-id> - VLAN ID (Range: 1 - 4093).

<newname> - Configure a new VLAN Name (up to 32 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 1-4093.

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

6.2.3.11 vlan association mac

This command associates a MAC address to a VLAN.

Syntax

```
vlan association mac <macaddr> <vlan-id> [<priority>]
no vlan association mac <macaddr>
```

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

<vland-id> - VLAN identification number. ID range is 1-4093.

< priority> - The priority value for untagged frames received. Valid priority value is 0 to 7. no -

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

Default Setting

None

Command Mode

VLAN database

6.2.3.12 vlan association subnet

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

Syntax

vlan association subnet <ipaddr> <netmask> <vlan-id> [<priority>] no
vlan association subnet <ipaddr> <netmask>

<ipaddr> - The IP address.

<netmask> - The subnet mask.

<vland-id> - VLAN identification number. ID range is 1-4093.

<priority> - The priority value for untagged frames received. Valid priority value is 0 to 7. no -

This command removes association of a specific IP-subnet to a VLAN.

Default Setting

None

Command Mode

VLAN database

6.2.3.13 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 2-4093.

Syntax

vlan makestatic <vlan-id>

<vlan-id> - VLAN ID (Range: 2 -4093).

Default Setting

None

Command Mode

VLAN database

6.2.3.14 protocol group

This command attaches a <vlan-id> 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> <vlan-id>
no protocol group <group-name> <vlan-id>
```

<vlan-id> - VLAN ID (Range: 1 - 4093).

<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

6.2.3.15 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

6.2.3.16 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

6.2.3.17 switchport native vlan

This command changes the VLAN ID which will be assigned to untagged or priority tagged frames per interface.

Syntax

```
switchport native vlan <vlan-id>
no switchport native vlan <vlan-id>
```

<vlan-id> - VLAN ID (Range: 1 - 4093).

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

Default Setting

1

Command Mode

Interface Config

This command changes the VLAN ID which will be assigned to untagged or priority tagged frames for all interfaces.

Syntax

```
switchport native vlan all <vlan-id>
```

<vlan-id> - VLAN ID (Range: 1 - 4093). all

- All interfaces.

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

Default Setting

1

Command Mode

Global Config

6.2.3.17 switchport native vlan

This command changes the VLAN ID which will be assigned to untagged or priority tagged frames per interface.

Syntax

```
switchport native vlan <vlan-id>
no switchport native vlan <vlan-id>
```

<vlan-id> - VLAN ID (Range: 1 - 4093).

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

Default Setting

1

Command Mode

Interface Config

This command changes the VLAN ID which will be assigned to untagged or priority tagged frames for all interfaces.

Syntax

```
switchport native vlan all <vlan-id>
```

<vlan-id> - VLAN ID (Range: 1 - 4093). all

- All interfaces.

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

Default Setting

1

Command Mode

Global Config

6.2.3.18 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 - 4093) - 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 <vlan-id>
```

<vlan-id> - VLAN ID (Range: 1 - 4093).

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

6.2.3.19 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 - 4093) - 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 <vlan-id>
```

<vlan-id> - VLAN ID (Range: 1 - 4093). 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

6.2.3.20 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 - 4093) - 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

6.2.3.21 switchport priority

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

Syntax

```
switchport priority <0-7>
no switchport priority
```

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

no - This command restore the priority configuration to default value.

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>
no switchport priority all
```

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

all - All interfaces

no - This command restores the priority value to default value for all interfaces.

Default Setting

0

Command Mode

Global Config

6.2.3.22 switchport protocol group

This command adds the physical 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

6.2.4 Double VLAN commands

6.2.4.1 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> | port-channel <portchannel-id>}]

<slot/port> - Specifies the desired interface.

<portchannel-id> - Specifies the desired port-channel interface. The range of port-channel ID is 1 to 64.

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.

6.2.4.2 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

6.2.4.3 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}] no
switchport {dvlan-tunnel | dot1q-tunnel} [ethertype]
```

Default Setting

802.1Q

Command Mode

Interface Config

6.2.5 GVRP and Bridge Extension

6.2.5.1 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.

6.2.5.2 show gvrp configuration

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

Syntax

show gvrp configuration [{<slot/port> | port-channel <portchannel-id>}]

<slot/port> - Specifies the desired interface.

<portchannel-id> - Specifies the port-channel interface. The range of port-channel ID is 1 to 64. no parameter - 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.

6.2.5.3 show gmrp configuration

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

Syntax

show gmrp configuration [{<slot/port> | port-channel <portchannel-id>}]

<slot/port> - Specifies the desired interface.

<portchannel-id> - Specifies the desired port-channel interface. The range of port-channel ID is 1 to 64.

no parameter - 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.

6.2.5.4 show garp configuration

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

Syntax

```
show garp configuration [{<slot/port> | port-channel <portchannel-id>}]
```

<slot/port> - Specifies the desired interface.

<portchannel-id> - Specifies the desired port-channel interface. The range of port-channel ID is 1 to 64.

no parameter - 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.

6.2.5.5 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

6.2.5.6 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

6.2.5.7 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

6.2.5.8 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 all interfaces.

Default Setting

Disabled

Command Mode

Global Config

6.2.5.9 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

6.2.6 IGMP Snooping

6.2.6.1 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

6.2.6.2 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

6.2.6.3 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

6.2.6.4 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

6.2.6.5 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

6.2.6.6 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|<vlaniid> interface configuration command. Use the no ip igmp snooping mrouter interface|<vlan-id> disable multicast router attached mode for the interface or a VLAN.

Syntax

```
ip igmp snooping mrouter interface|<vlan-id>
no ip igmp snooping mrouter interface|<vlan-id>
```

<vlan-id> - VLAN ID (Range: 1 - 4093).

Default Setting

None

Command Mode

Interface Config

6.2.6.7 set igmp

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

Syntax

```
set igmp <vlan-id>
no set igmp <vlan-id>
```

<vlan-id> - VLAN ID (Range: 1 - 4093).

Default Setting

Disabled

Command Mode

VLAN database

6.2.6.8 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 <vlan-id> vlan configuration command. Use the no set igmp fast-leave <vlan-id> disable IGMP Snooping fast-leave admin mode.

Syntax

```
set igmp fast-leave <vlan-id>
no set igmp fast-leave <vlan-id>
```

<vlan-id> - VLAN ID (Range: 1 - 4093).

Default Setting

Disabled

Command Mode

VLAN database

6.2.6.9 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 <vlan-id> <2-3600> vlan configuration command. Use the no set igmp groupmembership-interval <vlan-id> return to default value 260.

Syntax

```
set igmp groupmembership-interval <vlan-id> <2-3600>
no set igmp groupmembership-interval <vlan-id>
```

<vlan-id> - VLAN ID (Range: 1 - 4093).

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

Default Setting

260

Command Mode

VLAN database

6.2.6.10 set igmp maxresponse

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

Syntax

```
set igmp maxresponse <vlan-id> <1-25>
no set igmp maxresponse <vlan-id>
```

<vlan-id> - VLAN ID (Range: 1 - 4093).

<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 database

6.2.6.11 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 <vlan-id> <0-3600> vlan configuration command. Use the no set igmp mcrtrexpiretime <vlan-id> to return to default value 0.

Syntax

```
set igmp mcrtrexpiretime <vlan-id> <0-3600>
no set igmp mcrtrexpiretime <vlan-id>
```

<vlan-id> - VLAN ID (Range: 1 - 4093).

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

Default Setting

0

Command Mode

VLAN database

6.2.6.12 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 <vlan-id> interface {<slot/port> | port-channel
<portchannel-id>}
no ip igmp snooping static <macaddr> vlan <vlan-id> interface {<slot/port> | port-channel
<portchannel-id>}
```

<vlan-id> - VLAN ID (Range: 1 - 4093).

<macaddr> - Static MAC address.

<slot/port> - Interface number.

<portchannel-id> - Port-channel interface number. The range of port-channel ID is 1 to 64.

Default Setting

None

Command Mode

Global Config

6.2.6.13 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 [<slot/port> | vlan <vlan-id> | port-channel <portchannel-id>]

<slot/port> - Interface number.

<vlan-id> - VLAN ID (Range: 1 - 4093).

<portchannel-id> - Port-channel interface number. The range of port-channel ID is 1 to 64.

Default Setting

None

Command Mode

Privilege Exec

Display Message

When the optional arguments <slot/port>, <portchannel-id> or <vlan-id> 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> or <portchannel-id> 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.

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 <vlan-id>, 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.

6.2.6.14 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> | port-channel <portchannel-id>}
```

<slot/port> - Interface number.

<portchannel-id> - Port-channel interface number. The range of port-channel ID is 1 to 64.

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.

6.2.6.15 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> | port-channel <portchannel-id>}

<slot/port> - Interface number.

<portchannel-id> - Port-channel interface number. The range of port-channel ID is 1 to 64.

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.

6.2.6.16 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.

6.2.6.17 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:).

6.2.7 IGMP Snooping Querier

6.2.7.1 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

6.2.7.2 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.

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

6.2.7.3 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.

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

60

Command Mode

Global Config

6.2.7.4 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.

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

120 seconds

Command Mode

Global Config

6.2.7.5 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.

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

6.2.7.6 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 <vlan-id> global configuration command. Use the no ip igmp snooping querier vlan <vlan-id> return to disable.

Syntax

```
ip igmp snooping querier vlan <vlan-id>
no ip igmp snooping querier vlan <vlan-id>
```

<vlan-id> - VLAN ID (Range: 1 - 4093).

Default Setting

Disabled

Command Mode

Global Config

6.2.7.7 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 <vlan-id> address <ip-address> global configuration command. Use the no ip igmp snooping querier vlan <vlan-id> address return to default value zero.

Syntax

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

<vlan-id> - VLAN ID (Range: 1 - 4093).

<ip-address> - ip address

Default Setting

0.0.0.0

Command Mode

Global Config

6.2.7.8 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 <vlan-id> global configuration command. Use the no ip igmp snooping querier vlan election participate <vlan-id> return to disable.

Syntax

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

<vlan-id> - VLAN ID (Range: 1 - 4093).

Default Setting

Disabled

Command Mode

Global Config

6.2.7.9 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 120.

6.2.7.10 show ip igmp snooping querier vlan

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

Syntax

show ip igmp snooping querier vlan <vlan-id>

<vlan-id> - VLAN ID (Range: 1 - 4093).

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.

6.2.7.11 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 120.

6.2.8 MLD Snooping

6.2.8.1 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 [interface {<slot/port> | vlan <vlan-id> | port-channel <portchannel-id>}]

<slot/port> - Interface number.

<vlan-id> - VLAN ID (Range: 1 - 4093).

<portchannel-id> - Port-channel interface number. The range of port-channel ID is 1 to 64.

Default Setting

None

Command Mode

Privileged Exec

User Exec

Display Message

When the optional arguments <slot/port>, <portchannel-id> or <vlan-id> 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> or <portchannel-id> 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.

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 <vlan-id>, 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 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.

6.2.8.2 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> | port-channel <portchannel-id>}

<slot/port> - Interface number.

<portchannel-id> - Port-channel interface number. The range of port-channel ID is 1 to 64.

Default Setting

None

Command Mode

Privileged Exec

User 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.

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

6.2.8.3 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> | port-channel <portchannel-id>}

<slot/port> - Interface number.

<portchannel-id> - Port-channel interface number. The range of port-channel ID is 1 to 64.

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.

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

6.2.8.4 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.

6.2.8.5 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:).

6.2.8.6 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

6.2.8.7 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

6.2.8.8 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 to enable MLD snooping on global/interface. Use the no ipv6 mld snooping interfacemode to disable MLD Snooping on global/ interfaces.

Syntax

```
ipv6 mld snooping interfacemode [<all>]
no ipv6 mld snooping interfacemode [<all>]
```

Default Setting

Disabled

Command Mode

Global Config

Interface Config

6.2.8.9 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

6.2.8.10 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
```

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

Default Setting

260

Command Mode

Global Config

Interface Config

6.2.8.11 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
```

<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

6.2.8.12 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 | <vlan-id>} interface configuration command. Use the no ipv6 mld snooping mrouter {interface | <vlan-id>} disable multicast router attached mode for the interface or a VLAN.

Syntax

```
ipv6 mld snooping mrouter {interface |<vlan-id>}
no ipv6 mld snooping mrouter {interface|<vlan-id>}
```

<vlan-id> - VLAN ID (Range: 1 - 4093).

Default Setting

None

Command Mode

Interface Config

6.2.8.13 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> | port-channel
<portchannel-id>}
no ipv6 mld snooping static <macaddr> vlan <vlan-id> interface {<slot/port> | port-channel
<portchannel-id>}
```

<macaddr> - Static MAC address.

<vlan-id> - VLAN ID (Range: 1 - 4093).

<slot/port> - Interface number.

<portchannel-id> - Port-channel interface number. The range of port-channel ID is 1 to 64.

Default Setting

None

Command Mode

Global Config

6.2.8.14 set mld

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

Syntax

```
set mld <vlan-id>
no set mld <vlan-id>
```

<vlan-id> - VLAN ID (Range: 1 - 4093).

Default Setting

Disabled

Command Mode

VLAN database

6.2.8.15 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 <vlan-id> vlan configuration command. Use the no set mld fast-leave <vlan-id> disable MLD Snooping fast-leave admin mode.

Syntax

```
set mld fast-leave <vlan-id>
no set mld fast-leave <vlan-id>
```

<vlan-id> - VLAN ID (Range: 1 - 4093).

Default Setting

Disabled

Command Mode

VLAN database

6.2.8.16 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 <vlan-id> <2-3600> vlan configuration command. Use the no set mld groupmembership-interval <vlan-id> return to default value 260.

Syntax

```
set mld groupmembership-interval <vlan-id> <2-3600>
no set mld groupmembership-interval <vlan-id>
```

<vlan-id> - VLAN ID (Range: 1 - 4093).

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

Default Setting

260

Command Mode

VLAN database

6.2.8.17 set mld maxresponse

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

Syntax

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

<vlan-id> - VLAN ID (Range: 1 - 4093).

<1-65> - This value must be less than the MLD Query Interval time value. The range is 1 to 65 seconds.

Default Setting

10

Command Mode

VLAN database

6.2.8.18 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 <vlan-id> <0-3600> vlan configuration command. Use the no set mld mcrtrexpiretime <vlan-id> to return to default value 0.

Syntax

```
set mld mcrtrexpiretime <vlan-id> <0-3600>
no set mld mcrtrexpiretime <vlan-id>
```

<vlan-id> - VLAN ID (Range: 1 - 4093).

<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

VLAN database

6.2.9 MLD Snooping Querier

6.2.9.1 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 120.

6.2.9.2 show ipv6 mld snooping querier vlan

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

Syntax

show ipv6 mld snooping querier vlan <vlan-id>

<vlan-id> - VLAN ID (Range: 1 - 4093).

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.

6.2.9.3 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 120.

6.2.9.4 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

6.2.9.5 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>
```

<ipv6-address> - The IPv6 address of the MLD querier on the subnet the interface is associated with.

Default Setting

0

Command Mode

Global Config

6.2.9.6 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.

Syntax

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

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

Default Setting

60

Command Mode

Global Config

6.2.9.7 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.

Syntax

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

<60-300> - set igmp querier timer expiry

Default Setting

120

Command Mode

Global Config

6.2.9.8 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 <vlan-id> global configuration command. Use the no ipv6 mld snooping querier vlan <vlan-id> return to disable.

Syntax

```
ipv6 mld snooping querier vlan <vlan-id>
no ipv6 mld snooping querier vlan <vlan-id>
```

<vlan-id> - VLAN ID (Range: 1 - 4093).

Default Setting

Disabled

Command Mode

Global Config

6.2.9.9 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 <vlan-id> address <ip-address> global configuration command. Use the no ipv6 mld snooping querier vlan <vlan-id> address <ip-address> return to default value zero.

Syntax

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

<vlan-id> - VLAN ID (Range: 1 - 4093).

<ipv6-address> - The IPv6 address will be used in the IPv6 header while sending out MLD queries on this VLAN.

Default Setting

Disabled

Command Mode

Global Config

6.2.9.10 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 <vlan-id> global configuration command. Use the no ipv6 mld snooping querier vlan election participate <vlan-id> return to disable.

Syntax

ipv6 mld snooping querier vlan election participate <vlan-id>
no ipv6 mld snooping querier vlan election participate <vlan-id>

<vlan-id> - VLAN ID (Range: 1 - 4093).

Default Setting

Disabled

Command Mode

Global Config

6.2.10 Port Channel

6.2.10.1 show interface port-channel

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

Syntax
show interface port-channel brief

Default Setting

None

Command Mode

Privileged Exec

Display Message

For each port-channel the following information is displayed: Channel

ID: The field displays the port-channel's ID.

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 specified port-channel (LAG) on the switch.

Syntax

```
show interface port-channel <ID>
```

<ID> - The port-channel interface number. The range of port-channel ID is 1 to 64.

Default Setting

None

Command Mode

Privileged Exec

Display Message

Port Channel ID: The ID of this port-channel.

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 interface port-channel

Default Setting

None

Command Mode

Privileged Exec

Display Message

Channel ID: The ID of this port-channel.

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).

6.2.10.2 Interface port-channel

This command configures a new port-channel (LAG) with the specified ID. Display the information of this port-channel using the show interface port-channel <portchannel-id>.

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

Syntax

```
interface port-channel <portchannel-id>
no interface port-channel <portchannel-id>
```

<portchannel-id> - The port-channel interface number to be created. The range of the port-channel ID is 1 to 64.

no - This command delete the specified 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.

6.2.10.3 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

6.2.10.4 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

6.2.10.5 port-channel linktrap

This command enables link trap notifications for the port-channel (LAG). The interface is a ID for a configured port-channel. The option all sets every configured port-channel with the same administrative mode setting.

Syntax

```
port-channel linktrap {<ID> | all}
no port-channel linktrap {<ID> | all}
```

<ID> - The port-channel interface number. The range of the port-channel ID is 1 to 64. all

- all port-channel interfaces.

no - This command disables link trap notifications for the port-channel (LAG). The interface is a ID 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

6.2.10.6 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 { src-mac | dst-mac | dst-src-mac | src-ip | dst-ip | dst-src-ip } {<ID> | all} no port-channel load-balance {<ID> | 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.

<ID> - The ID of the port-channel to be configured.

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

6.2.10.7 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

6.2.10.8 adminmode

This command enables a port-channel (LAG) members. The interface is a ID 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

6.2.10.9 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

6.2.10.10 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 0-65535.

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

6.2.10.11 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.

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

Syntax

```
channel-group <ID>
```

<ID> - Port-Channel Interface number. The range of the port-channel ID is 1 to 64.

Default Setting

None

Command Mode

Interface Config

Command Usage

The maximum number of members for each port-channel is 8.

6.2.10.12 delete-channel-group

This command deletes the port from the port-channel (LAG). The interface is a ID of a configured port-channel.

Syntax

```
delete-channel-group <ID>
```

<ID> - Port-channel Interface number. The range of the port-channel ID is 1 to 64.

Default Setting

None

Command Mode

Interface Config

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

Syntax

```
delete-channel-group <ID> all
```

<ID> - Port-channel Interface number. The range of the port-channel ID is 1 to 64. all

- All members for specific Port-channel.

Default Setting

None

Command Mode

Global Config

6.2.11 Storm Control

6.2.11.1 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.

Rate: Displays rate in pps (packet per second) for storm control broadcast.

Action: Shutdown or send trap when storm is detected.

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.

Rate: Displays rate in pps (packet per second) for storm control multicast.

Action: Shutdown or send trap when storm is detected.

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.

Rate: Displays rate in pps (packet per second) for storm control unicast.

Action: Shutdown or send trap when storm is detected.

6.2.11.2 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

6.2.11.3 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

6.2.11.4 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

6.2.11.5 storm control action

This command configure what actions will be performed while the storm control is detected. The actions include shutdown the interfae and send a SNMP trap if the storm occurs.

Syntax

```
storm-control action {shutdown | trap}
no storm-control {shutdown | trap}
```

shutdown - To shutdown the interface if the storm occurs. trap

- To send SNMP trap if the storm occurs.

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

Default Setting

None

Command Mode

Interface Config

6.2.11.6 switchport broadcast rate

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

Syntax

```
switchport broadcast rate <1-14880000>
```

<1-14880000> - Specify the threshold for broadcast traffic.

Note: pps (packet per second)

Default Setting

4160 for 10G interfaces

512 for 1G interfaces

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 rate <1-14880000>
```

<1-14880000> - Specify the threshold for broadcast traffic. all

- This command represents all interfaces.

Note: pps (packet per second)

Default Setting

4160 for 10G interfaces

512 for 1G interfaces

Command Mode

Global Config

6.2.11.7 switchport multicast rate

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

Syntax

switchport multicast rate <1-14880000>

<1-14880000> - Specify the threshold for multicast traffic

Note: pps (packet per second)

Default Setting

4160 for 10G interfaces

512 for 1G interfaces

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 rate <1-14880000>

<1-14880000> - Specify the threshold for multicast traffic. all

- This command represents all interfaces.

Note: pps (packet per second)

Default Setting

4160 for 10G interfaces

512 for 1G interfaces

Command Mode

Global Config

6.2.11.8 switchport unicast rate

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

Syntax

```
switchport unicast rate <1-14880000>
```

<1-14880000> - Specify the threshold for unicast traffic

Note: pps (packet per second)

Default Setting

4160 for 10G interfaces

512 for 1G interfacces

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 rate <1-14880000>
```

<1-14880000> - Specify the threshold for unicast traffic. all

- This command represents all interfaces.

Note: pps (packet per second)

Default Setting

4160 for 10G interfaces

512 for 1G interfaces

Command Mode

Global Config

6.2.12 L2 Priority

6.2.12.1 show queue cos-map

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

Syntax

```
show queue cos-map {<slot/port> | port-channel <portchannel-id>}
```

<slot/port> - Interface number.

<portchannel-id> - Port-channel interface number. The range of port-channel ID is 1 to 64.

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.

6.2.12.2 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

6.2.13 Port Mirror

6.2.13.1 show port-monitor session

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

Syntax

```
show port-monitor session <session-id>
```

<session-id> - session ID. The range of session ID is 1 to 4.

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.

Source 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.

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

<slot/port> - Interface number.

<portchannel-id> - Port-channel interface number. The range of port-channel ID is 1 to 64. 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

6.2.13.3 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

6.2.14 Link State

6.2.14.1 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.

6.2.14.2 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

6.2.14.3 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

6.2.15 Port Backup

6.2.15.1 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.

6.2.15.2 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

6.2.15.3 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

6.3 Management Commands

6.3.1 Network Commands

6.3.1.1 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

VLAN ID: Indicates whether the VLAN ID is used for this vlan interface.

Interface: Indicates whether the interface number for this interface.

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

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

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

6.3.1.2 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.

6.3.1.3 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 <1518-12288> is a valid integer between 1518-12288.

Syntax

```
mtu    <1518-12288>
no mtu
```

<1518-12288> - Max frame size (Range: 1518 - 12288).

no - This command sets the default maximum transmission unit (MTU) size (in bytes) for the interface.

Default Setting

1518

Command Mode

Interface Config

6.3.1.4 interface vlan

This command is used to create a vlan interface and enter Interface-vlan configuration mode.

Syntax

```
interface vlan <vlan-id>
```

<vlan-id> - VLAN ID (Range: 1 - 4093).

Default Setting

None

Command Mode

Global Config

6.3.1.5 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.

6.3.1.6 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

6.3.1.7 ip address dhcp

This command specifies the network configuration protocol to be used. If you modify this value, the change is effective immediately.

Syntax

```
ip address dhcp [restart]
```

<dhcp> - Obtains IP address from DHCP.

<restart> - To restart the DHCP process.

Default Setting

None

Command Mode

Interface-Vlan Config

6.3.1.8 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 <name> {ipv4 | ipv6} <ipAddr> [<mask>]
no ip filter <name>
```

<name> - The name of the IP filter.

<ipAddr> - Configure a IP address to the filter.

<mask> - Specifies the mask for a range filter.

no - Remove this IP address from filter.

Default Setting

None

Command Mode

Global Config

6.3.2 Serial Interface Commands

6.3.2.1 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.

6.3.2.2 line console

This command is used to enter Line configuration mode

Syntax

line console

Default Setting

None

Command Mode

Global Config

6.3.2.3 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

6.3.2.4 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

6.3.2.5 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

6.3.2.6 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

6.3.2.7 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

6.3.3 Telnet Session Commands

6.3.3.1 telnet

This command establishes a new outbound telnet connection to a remote host.

Syntax

```
telnet <ip-address|hostname> [port] [debug] [line]
```

<ip-address|hostname> - 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'.

Default Setting

None

Command Mode

Privileged Exec

User Exec

6.3.3.2 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.

Telnet Server Admin Mode: The telnet server admin mode status. The factory default is enable.

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.

Terminal Length: The columns per page for terminal vty port.

6.3.3.3 line vty

This command is used to enter vty (Telnet) configuration mode.

Syntax
line vty

Default Setting

None

Command Mode

Global Config

6.3.3.4 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.

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

6.3.3.5 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

6.3.3.6 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

6.3.3.7 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

6.3.3.8 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

6.3.3.9 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

6.3.3.10 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

6.3.3.11 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

6.3.3.12 telnet exec-timeout

This command sets the outbound telnet session timeout value in minute.

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

6.3.3.13 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.

6.3.4 SSH Client Session Commands

6.3.4.1 ssh

This command establishes a new outbound ssh connection to a remote host.

Syntax

ssh <ip-address|hostname> <username> { [port <port-id>] [protocol <protocollevel>] | [protocol <protocollevel>] [port <port-id>]}

<ip-address|hostname> - A hostname or a valid IP address.

<username> - user account.

<port-id> - A valid decimal integer in the range of 1 to 65535, where the default value is 22.

<protocollevel> - SSH Protocol Level (Version) 1 or 2.

Default Setting

None

Command Mode

Privileged Exec

Display Message

Connected to 192.168.2.200, use ~. to terminate connection.

6.3.4.2 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

6.3.4.3 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

6.3.4.4 sshc exec-timeout

This command sets the outbound ssh session timeout value in minute.

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

6.3.4.5 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.

6.3.5 SNMP Server Commands

6.3.5.1 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.

6.3.5.2 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.

ACL Traps: May be enabled or disabled. The factory default is disabled. Indicates whether ACL traps will be sent.

Captive Portal Traps: May be enabled or disabled. The factory default is disabled. Indicates whether Captive Portal 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.

PIM Traps: May be enabled or disabled. The factory default is disabled. Indicates whether PIM traps will be sent.

6.3.5.3 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

6.3.5.4 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

6.3.5.5 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

6.3.5.6 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

6.3.5.7 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

6.3.5.8 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

Disabled

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 Captive Portal traps..

Syntax

```
snmp-server enable traps captive-portal
no snmp-server enable traps captive-portal
```

no - This command disables Captive Portal trap.

Default Setting

Disabled

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 | 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

6.3.6 SNMP Trap Commands

6.3.6.1 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/Hostname: The IP or IPv6 Address or domain name to receive SNMP Informs from this device.

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.

SNMP v3 - Uses SNMP v3 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.

Secure Level: The authentication and encryption level for snmpv3.

None - no authentication checksum and no encryption algorithm assigned.

Auth - md5 or sha authentication checksum assigned and no encryption algorithm assigned.

Priv - md5 or sha authentication checksum and des encryption algorithm assigned.

6.3.6.2 show snmptrap source-interface

This command displays the configured global source interface used for the SNMP client. The IP address of the selected interface is used as source IP for all communications with the server.

Syntax

```
show snmptrap source-interface
```

Default Setting

None

Command Mode

Privileged Exec

Display Message

SNMP trap Client Source Interface: The interface configured as the source interface for the SNMP trap/inform client.

SNMP trap Client IPv4 Address: The IP address configured on the SNMP client source interface.

6.3.6.3 snmptrap snmpversion

This command configures the version for snmp trap.

Syntax

snmptrap snmpversion <name> <ipAddr|ipv6Addr|hostname> <snmpversion>

<name> - SNMP trap name (Range: up to 16 case-sensitive alphanumeric characters).

< ipAddr|ipv6Addr|hostname> - an IPv4 or IPv6 address or hostname of the trap receiver.

<snmpversion> - SNMP trap version.

Default Setting

Snmpv2

Command Mode

Global Config

6.3.6.4 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

6.3.6.5 snmptrap <name> <ipAddr|ipv6Addr|hostname>

This command adds an SNMP trap name. The maximum length of the name is 16 case-sensitive alphanumeric characters.

Syntax

snmptrap <name> <ipAddr|ipv6Addr|hostname> { port <port> | snmpversion <snmpversion> } no snmptrap <name> <ipAddr|ipv6Addr|hostname>

<name> - SNMP trap name (Range: up to 16 case-sensitive alphanumeric characters).

<ipAddr|ipv6Addr|hostname> - an IPv4 or IPv6 address or hostname of the trap receiver.

<port> - SNMP trap port number.

<snmpversion> - SNMP trap version.

no - This command deletes trap receivers.

Default Setting

None

Command Mode

Global Config

6.3.6.6 snmptrap ipaddr <name> <ipAddr|ipv6Addr|hostname> <new ipAddr|ipv6Addr|hostname>

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.

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|ipv6Addr|hostname> <new ipAddr|ipv6Addr|hostname>

<name> - SNMP trap name.

<ipAddr|ipv6Addr|hostname> - an original IPv4 or IPv6 address or hostname.

<new ipAddr|ipv6Addr|hostname> - a new IPv4 or IPv6 address or hostname.

Default Setting

None

Command Mode

Global Config

6.3.6.7 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|ipv6Addr|hostname>
no snmptrap mode <name> <ipAddr|ipv6Addr|hostname>
```

<name> - SNMP trap name.

<ipAddr|ipv6Addr|hostname> - an IPv4 or IPv6 address or hostname.

no - This command deactivates an SNMP trap. Trap receivers are inactive (not able to receive traps).

Default Setting

None

Command Mode

Global Config

6.3.6.8 snmptrap port

This command configures an SNMP trap port.

Syntax

```
snmptrap port <name> <ipAddr|ipv6Addr|hostname> <port>
no snmptrap port <name> <ipAddr|ipv6Addr|hostname>
```

<name> - SNMP trap name.

<ipAddr|ipv6Addr|hostname> - an IPv4 or IPv6 address or hostname.

<port> - a port number between 1 and 65535.

no - This command resets an SNMP trap port number to default port 162.

Default Setting

None

Command Mode

Global Config

6.3.6.9 snmptrap source-interface

Use this command in Global configuration mode to configure the global source-interface (Source IP address) for all SNMP communications between the SNMP client and the server. This command takes effect for both SNMP trap and inform client.

Syntax

snmptrap source-interface {<slot/port> | loopback <loopback-id> | tunnel <tunnel-id> | vlan <vlan-id>} no snmptrap source-interface

<slot/port> - Specifies the interface to use as the source interface.

<loopback-id> - Specifies the loopback interface to use as the source interface. The range of the loopback ID is 0 to 7.

<tunnel-id> - Specifies the tunnel interface to use as the source interface. The range of the tunnel ID is 0 to 7.

<vlan-id> - Specifies the VLAN interface to use as the source interface. The range of VLAN ID is 1 to 4093.

no - This command removes the global source-interface for all SNMP communication between the SNMP client and the server.

Default Setting

None

Command Mode

Global Config

This feature is only support with L3 feature enabled.

6.3.6.10 snmp-server enable informs

This command enables snmp inform.

Syntax

```
snmp-server enable informs
no snmp-server enable informs
```

no - This command disables snmp inform.

Default Setting

Enabled

Command Mode

Global Config

6.3.6.11 snmp-server inform

This command configures snmp inform retries.

Syntax

```
snmp-server inform retries <retries>
no snmp-server informs retries
```

<retries> - Number of times to retry an Inform request. The range is between 0 and 100. no - This command resets snmp inform retries.

Default Setting

3

Command Mode

Global Config

This command configures snmp inform timeout.

Syntax

```
snmp-server inform timeout <timeout>
no snmp-server informs timeout
```

<timeout> - Timeout value, in seconds. The range is between 0 and 1000. no - This command resets snmp inform timeout.

Default Setting

15

Command Mode

Global Config

6.3.6.12 snmp-server engineID

This command configures snmp engineID.

Syntax

```
snmp-server engineID remote <ipAddr|ipv6Addr> <engineid-string>
no snmp-server engineID remote <ipAddr|ipv6Addr> <engineid-string>
```

<ipAddr|ipv6Addr> - Enter IP or IPv6 address of the remote device.

<engineid-string> - Enter the name of a copy of SNMP. The maximum length of the name is 24 characters.

no - This command removes snmp engineID.

Default Setting

None

Command Mode

Global Config

6.3.6.13 snmp-server user

This command configures snmp server user for SNMPv3.

Syntax

```
snmp-server user <username> auth { noauth | { md5 <passtype> <pass> [ priv des <passtype>
<pass> ] } | { sha <passtype> <pass> [ priv des <passtype> <pass> ] } }
no snmp-server user <username>
```

<username> - Username of SNMPv3.

<auth> - auth types include noauth, md5, and sha, when use md5 or sha as the auth type, one should have a pass.

<passtype> - 0 specifies password in plain text, 7 specifies password in encrypted form.

<pass> - password string in plain text or encrypted format.

no - This command removes snmp user.

Default Setting

None

Command Mode

Global Config

6.3.7 SNMP Inform Commands

6.3.7.1 show snmpinform

This command displays SNMP inform receivers. SNMP Inform 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 inform receivers are simultaneously supported.

Syntax
show snmpinform

Default Setting

None

Command Mode

Privileged Exec

Display Message

SNMP Inform Flags: Shows SNMP Inform is Enable or Disable.

SNMP Inform Retries: Shows how many times should SNMP Inform retry when not success.

SNMP Inform Timeout: Shows how long should SNMP Inform wait when not success.

SNMP Inform 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/Hostname: The IP or IPv6 Address or domain name to receive SNMP Informs from this device.

SNMP Version: The trap version to be used by the receiver.

SNMP v2 - Uses SNMP v2 to send traps to the receiver.

SNMP v3 - Uses SNMP v3 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.

Secure Level: The authentication and encryption level for snmpv3.

None - no authentication checksum and no encryption algorithm assigned.

Auth - md5 or sha authentication checksum assigned and no encryption algorithm assigned.

Priv - md5 or sha authentication checksum and des encryption algorithm assigned.

6.3.7.2 snmpinform version

This command configures the version for snmp inform.

Syntax

```
snmpinform version <name> <ipAddr|ipv6Addr|hostname> <version>
```

<name> - SNMP trap name (Range: up to 16 case-sensitive alphanumeric characters).

<ipAddr|ipv6Addr|hostname> - an IPv4 or IPv6 address or hostname of the inform receiver.

<version> - SNMP inform version, SNMPv2 or SNMPv3.

Default Setting

SNMPv2

Command Mode

Global Config

6.3.7.3 snmpinform <name> <ipAddr|ipv6Addr|hostname> version <snmpversion>

This command adds an SNMP inform name. The maximum length of the name is 16 case-sensitive alphanumeric characters.

Syntax

```
snmpinform <name> <ipAddr|ipv6Addr|hostname> version <version> no
snmpinform <name> <ipAddr|ipv6Addr|hostname>
```

<name> - SNMP trap name (Range: up to 16 case-sensitive alphanumeric characters).

<ipAddr|ipv6Addr|hostname> - an IP or IPv6 address or hostname of the inform receiver.

<version> - SNMP inform version, SNMPv2 or SNMPv3.

no - This command deletes trap receivers for a community.

Default Setting

None

Command Mode

Global Config

6.3.7.4 snmpinform ipaddr <name> <ipAddr|ipv6Addr|hostname> <new ipAddr|ipv6Addr|hostname>

This command changes the IP address of the inform receiver for the specified community name. The maximum length of name is 16 case-sensitive alphanumeric characters.

IP addresses in the SNMP inform receiver table must be unique for the same community name or user name. If you make multiple entries using the same IP address and community name or user name, the first entry is retained and processed. All duplicate entries are ignored.

Syntax

snmpinform ipaddr <name> <ipAddr|ipv6Addr|hostname> <new ipAddr|ipv6Addr|hostname>

<name> - SNMPv2 community name or SNMPv3 user name.

<ipAddr|ipv6Addr|hostname> - an original IPv4 or IPv6 address or hostname.

<new ipAddr|ipv6Addr|hostname> - a new IPv4 or IPv6 address or hostname.

Default Setting

None

Command Mode

Global Config

6.3.7.5 snmpinform mode

This command activates or deactivates an SNMP inform. Enabled inform receivers are active (able to receive informs). Disabled inform receivers are inactive (not able to receive informs).

Syntax

```
snmpinform mode <name> <ipAddr|ipv6Addr|hostname>
no snmpinform mode <name> <ipAddr|ipv6Addr|hostname>
```

<name> - SNMPv2 community name or SNMPv3 user name.

<ipAddr|ipv6Addr|hostname> - an original IPv4 or IPv6 address or hostname.

no - This command deactivates an SNMP inform. Inform receivers are inactive (not able to receive traps).

Default Setting

None

Command Mode

Global Config

6.3.8 HTTP commands

6.3.8.1 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.

6.3.8.2 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

6.3.8.3 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

6.3.8.4 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

6.3.8.5 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

6.3.8.6 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

6.3.8.7 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

6.3.9 Secure Shell (SSH) Commands

6.3.9.1 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.

6.3.9.2 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

Enabled

Command Mode

Global Config

6.3.9.3 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

6.3.9.4 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

5

Command Mode

Global Config

6.3.9.5 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

6.3.10 Management Security Commands

6.3.10.1 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

6.3.10.2 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

6.3.11 DHCP Client Commands

6.3.11.1 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

6.3.11.2 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

A text string : “Default”

Command Mode

Global Config

6.3.12 DHCPv6 Client Commands

6.3.12.1 ipv6 address dhcp

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 dhcp [restart]
```

<dhcp> - Obtains IPv6 address from DHCPv6.

<restart> - To restart the DHCPv6 process.

Default Setting

None

Command Mode

Interface-Vlan Config

Interface Config

6.3.12.2 serviceport protocol

This command specifies the service port 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

6.3.12.3 serviceport protocol dhcp6 restart

This command is used to initiate a DHCPv6 client request by service port interface.

Syntax

```
serviceport protocol dhcp6 restart
```

Default Setting

None

Command Mode

Global Config

6.3.13 DHCP Relay Commands

6.3.13.1 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.

6.3.13.2 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

6.3.14 sFlow Commands

6.3.14.1 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.

6.3.14.2 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.

6.3.14.3 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.

6.3.14.4 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.

6.3.14.5 show sflow rate

Use this command to display the sFlow traffic rate summary on the switch.

Syntax

show sflow rate interface [<slot/port>]

<slot/port> - An interface number.

no parameter - All interfaces.

Command Mode

Privilege Exec

Display Message

Octets Received Rate	The number of octets rate received on the interface including framing characters.
Unicast Packets Received Rate	The number of unicast packets rate delivered by this sub-layer to a higher sub-layer.
Multicast Packets Received Rate	The number of multicast packets rate delivered by this sub-layer to a higher sub-layer.
Broadcast Packets Received Rate	The number of broadcast packets rate delivered by this sub-layer to a higher sub-layer.
Discarded Packets Received Rate	The number of inbound packets rate which were chosen to be discarded.
Errors Received Rate	The number of the counter rate IfInErrors.
Unknown Protocols Packets Received Rate	The number of packets rate received via the interface which were discarded because of an unknown or unsupported protocol.
Octets Transmitted Rate	The total number of octets rate transmitted out of the interface, including framing characters.
Unicast Packets Transmitted Rate	The total number of unicast packets rate that higher-level protocols requested be transmitted.
Multicast Packets Transmitted Rate	The total number of multicast packets rate that higher-level protocols requested be transmitted.
Broadcast Packets Transmitted Rate	The total number of broadcast packets rate that higher-level protocols requested be transmitted.

6.3.14.6 show sflow source-interface

The user can go to the CLI Privilege Exec to get the configured source interface for sFlow, use the show sflow source-interface Privilege command.

Syntax

```
show sflow source-interface
```

Default Setting

None

Command Mode

Privilege Exec

Display Message

sFlow Client Source interface: The interface ID of the physical or logical interface configured as the sFlow client source interface.

sFlow Client Source IPv4 Address: The IP address of the interface configured as the sFlow client source interface.

6.3.14.7 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

6.3.14.8 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

6.3.14.9 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

6.3.14.10 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

6.3.14.11 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

6.3.14.12 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

6.3.14.13 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

6.3.14.14 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

6.3.14.15 Set sflow source-interface

Use this command to specify the physical or logical routing interface to use as the sFlow client source interface. If configured, the address of source interface is used for all sFlow communications between the sFlow receiver and the sFlow client. Otherwise there is no change in behavior. If the configured interface is down, the sFlow client falls back to normal behavior. User can go to the CLI Interface Configuration Mode to configure a new sFlow source interface, use the sflow source-interface global configuration command. Use the no sflow source-interface remove the source interface setting

Syntax

sflow source-interface {<slot/port> | loopback <loopback-id> | tunnel <tunnel-id> | vlan <vland-id>} no sflow source-interface

<slot/port> - Specifies the interface to use as the source interface.

<loopback-id> - Specifies the loopback interface to use as the source interface. The range of the loopback ID is 0 to 7.

<tunnel-id> - Specifies the tunnel interface to use as the source interface. The range of the tunnel ID is 0 to 7.

<vlan-id> - Specifies the VLAN interface to use as the source interface. The range of the VLAN ID is 1 to 4093.

Default Setting

None

Command Mode

Global Config

6.3.15 Service Port Commands

6.3.15.1 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 Prefix is: 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.Configured IPv4 Protocol: Indicate what IPv4 network protocol was used on the last, or current power-up cycle, if any.

Configured IPv6 Protocol: Indicate what IPv6 network protocol was used on the last, or current power-up cycle, if any.

IPv6 AutoConfig Mode: Whether enabled or disabled. Default value is disabled. IPv6

Link-local Scope ID: The scope ID for this interface

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

6.3.15.2 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. isRtr:.

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.

6.3.15.3 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

6.3.15.4 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

6.3.15.5 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

6.3.15.6 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.

Multiple IPv6 prefixes can be configured for the service port.

Default Setting

None

Command Mode

Global Config

6.3.15.7 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.

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

6.3.16 Time Range Commands

Time-based ACLs allow one or more rules within an ACL to be based on time. Each ACL rule within an ACL except for the implicit deny all rule can be configured to be active and operational only during a specific time period. The time range commands allow you to define specific times of the day and week in order to implement time-based ACLs. The time range is identified by a name and can then be referenced by an ACL rule defined with in an ACL.

6.3.16.1 Show Commands

6.3.16.1.1 show time-range

Use this command to display a time range and all the absolute/periodic time entries that are defined for the time range. Use the name parameter to identify a specific time range to display. When name is not specified, all the time ranges defined in the system are displayed.

Syntax

```
show time-range [<name>]
```

<name> - time-range name.

Default Setting

None

Command Mode

Privileged Exec

Display Message

Number of Time Ranges: Number of time ranges configured in the system.

Time Range Name: Name of the time range.

Time Range Status: Status of the time range (active/inactive).

Absolute start: Start time and day for absolute time entry.

Absolute end: End time and day for absolute time entry.

Periodic Entries: Number of periodic entries in a time-range.

Periodic start: Start time and day for periodic entry.

Periodic end: End time and day for periodic entry.

6.3.16.2 Configuration Commands

6.3.16.2.1 time-range

Use this command to create a time range identified by name, consisting of one absolute time entry and/or one or more periodic time entries. The name parameter is a case-sensitive, alphanumeric string from 1 to 31 characters that uniquely identifies the time range. An alpha-numeric string is defined as consisting of only alphabetic, numeric, dash, underscore, or space characters.

If a time range by this name already exists, this command enters Time-Range config mode to allow updating the time range entries

Syntax

```
time-range <name>
no time-range <name>
```

<name> - The time range name.

no - This command deletes a time-range identified by name.

Default Setting

None

Command Mode

Global Config

6.3.16.2.2 absolute

Use this command to add an absolute time entry to a time range. Only one absolute time entry is allowed per time-range. The time parameter is based on the currently configured time zone.

The [start time date] parameters indicate the time and date at which the configuration that referenced the time range starts going into effect. The time is expressed in a 24-hour clock, in the form of hours:minutes. For example, 8:00 is 8:00 am and 20:00 is 8:00 pm. The date is expressed in the format day month year. If no start time and date are specified, the configuration statement is in effect immediately.

The [end time date] parameters indicate the time and date at which the configuration that referenced the time range is no longer in effect. The end time and date must be after the start time and date. If no end time and date are specified, the configuration statement is in effect indefinitely.

Syntax

```
absolute { [start time date] [end time date] }
no absolute
```

no - This command deletes the absolute time entry in the time range.

Default Setting

None

Command Mode

Time-Range Config

6.3.16.2.3 periodic

Use this command to add a periodic time entry to a time range. The time parameter is based off of the currently configured time zone.

The first occurrence of the days-of-the-week argument is the starting day(s) from which the configuration that referenced the time range starts going into effect. The second occurrence is the ending day or days from which the configuration that referenced the time range is no longer in effect. If the end days-of-the-week are the same as the start, they can be omitted

This argument can be any single day or combinations of days: Monday, Tuesday, Wednesday, Thursday, Friday, Saturday, Sunday. Other possible values are:

- daily — Monday through Sunday
- weekdays — Monday through Friday
- weekend — Saturday and Sunday

If the ending days of the week are the same as the starting days of the week, they can be omitted. The first occurrence of the time argument is the starting hours:minutes which the configuration that referenced the time range starts going into effect. The second occurrence is the ending hours:minutes at which the configuration that referenced the time range is no longer in effect.

The hours:minutes are expressed in a 24-hour clock. For example, 8:00 is 8:00 am and 20:00 is 8:00 pm.

Syntax

```
periodic {days-of-the-week time} to {[days-of-the-week] time}
no periodic {days-of-the-week time} to {[days-of-the-week] time}
```

no - This command deletes a periodic time entry from a time range.

Default Setting

None

Command Mode

Time-Range Config

6.4 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.

6.4.1 Show Commands

6.4.1.1 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.

6.4.1.2 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> | port-channel <portchannel-id>}

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

<portchannel-id> - is the desired port-channel interface number. The range of port-channel ID is 1 to 64.

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.

6.4.1.3 show spanning-tree vlan

This command displays the association between a VLAN and a multiple spanning tree instance. The <vlan-id> corresponds to an existing VLAN ID.

Syntax

show spanning-tree vlan <vlan-id>

<vlan-id> - VLAN ID (Range: 1 - 4093).

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.

6.4.1.4 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> | port-channel <portchannel-id>}
```

<0-4094> - multiple spanning tree instance ID.

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

<portchannel-id> - is the desired port-channel interface number. The range of port-channel ID is 1 to 64.

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>} indicates the desired switch port.

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> | active | port-channel <portchannel-id>}]
```

<0-4094> - multiple spanning tree instance ID.

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

active - All active interfaces.

<portchannel-id> - is the desired port-channel interface number. The range of port-channel ID is 1 to 64.

no parameter - 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”.

6.4.1.5 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.

6.4.1.6 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).

6.4.2 Configuration Commands

6.4.2.1 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

6.4.2.2 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> | port-channel <portchannel-id> | all}
no spanning-tree protocol-migration {<slot/port> | port-channel <portchannel-id> | all}
```

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

<portchannel-id> - is the desired interface number. The range of port-channel ID is 1 to 4. 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

6.4.2.3 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

6.4.2.4 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

6.4.2.5 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

6.4.2.6 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

6.4.2.7 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 6 to 40.

Syntax

```
spanning-tree max-hops <6-40>
no spanning-tree max-hops
```

<6-40> - the Maximum hops value (Range: 6-40).

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

6.4.2.8 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

6.4.2.9 spanning-tree mst

This command adds a multiple spanning tree instance to the switch. The instance <1-4094> is a number within a range of 1 to 4094 that corresponds to the new instance ID to be added. The maximum number of multiple instances supported 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 <1-4093> corresponds to an existing VLAN ID.

Syntax

```
spanning-tree mst vlan <0-4094> <vlan-list>
no spanning-tree mst vlan <0-4094> <vlan-list>
```

<0-4094> - multiple spanning tree instance ID.

<vlan-list> - VLAN ID (Range: 1 - 4093).

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 <1-4093> 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

6.4.2.10 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

6.4.2.11 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

6.4.2.12 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

6.4.2.13 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

6.4.2.14 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

6.4.2.15 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

6.5 System Log Management Commands

6.5.1 Show Commands

6.5.1.1 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.

Logging Client Source Interface The interface configured as the source interface for the syslog client.

Logging Client Source IPv4 Address The IP address configured on the syslog client source interface.

6.5.1.2 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.

Message log information is not retained across a switch reset.

6.5.1.3 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.

6.5.1.4 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.

6.5.2 Configuration Commands

6.5.2.1 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

6.5.2.2 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

6.5.2.3 logging monitor

This command enables logging to the terminal monitor.

Syntax

```
logging monitor [<severitylevel> | <0-7>]
no logging monitor
```

[<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

6.5.2.4 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

6.5.2.5 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

6.5.2.6 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

Use this command to specify the physical or logical interface to use as the Syslog client source interface. If configured, the address of source interface is used for all Syslog communications between the Syslog server and the Syslog client. Otherwise there is no change in behavior. If the configured interface is down, the Syslog client falls back to normal behavior.

Syntax

```
logging syslog source-interface {<slot/port> | loopback <loopback-id> | tunnel <tunnel-id> | vlan <vlan-id>}
no logging syslog source-interface
```

<slot/port> - Specifies the interface to use as the source interface.

<loopback-id> - Specifies the loopback interface to use as the source interface. The range of the loopback ID is 0 to 7.

<tunnel-id> - Specifies the tunnel interface to use as the source interface. The range of the tunnel ID is 0 to 7.

<vlan-id> - Specifies the VLAN interface to use as the source interface. The range of VLAN ID is 1 to 4093.

no - To remove the configured source interface for all Syslog communications between the Syslog client and the server.

Default Setting

None

Command Mode

Globla Config

6.5.2.7 clear logging buffered

This command clears all in-memory log.

Syntax
clear logging buffered

Default Setting

None

Command Mode

Privileged Exec

6.6 Script Management Commands

6.6.1 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

6.6.2 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

6.6.2.1 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.

6.6.3 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

6.6.4 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

6.7 User Account Management Commands

6.7.1 Show Commands

6.7.1.1 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 ReadWrite, 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.

6.7.1.2 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.

Privilege: The user's privilege level. The range of privilege level is 1 to 15. Access mode for privilege level 15 is read/write, the others is read-only.

Password Aging: Indicates number of days, since the password was configured, until the password expires.

Password Expiration Date: The current password expiration date in date format.

Lockout: Indicates whether the user account is locked out (true or false).

6.7.1.3 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.

Password Strength Check: The user to configure passwords that comply with the strong password configuration.

Minimum Password Uppercase Letters: Minimum number of uppercase characters required when changing passwords.

Minimum Password Lowercase Letters: Minimum number of lowercase characters required when changing passwords.

Minimum Password Numeric Characters: Minimum number of numeric characters required when changing passwords.

Minimum Password Special Characters: Minimum number of special characters required when changing passwords.

Maximum Password Repeated Characters: Maximum number of characters cannot repeated when changing passwords.

Maximum Password Consecutive Characters: Maximum number of characters cannot consecutive when changing passwords.

Minimum Password Character Classes: Valid range for user passwords.

Password Exclude Keywords: The password to be configured should not contain the keyword mentioned in this field.

6.7.1.4 Show password result

Use this command to display the last password set result information.

Syntax
show passwords result

Default Setting

None

Command Mode

Privileged Exec

Display Message

Last User Whose Password Is Set: Shows the name of the user with the most recently set password.

Password Strength Check: Shows whether password strength checking is enabled.

Last Password Set Result: Shows whether the attempt to set a password was successful. If the attempt failed, the reason for the failure is include.

6.7.2 Configuration Commands

6.7.2.1 username

This command adds a new user (account) if space permits. The default privilege level is 1. 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> {passwd <0|7> <password> | nopasswd | level <level>} 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. When 7 is used, the password must be exactly 128 hexadeciaml characters in length. Maximum plain-text password length is 64 characters.

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.

<level> - The user level. Level 0 can be assigned by a level 15 user to another user to suspend that user’s access. Range 0-15. Enter access level 1 for Read Access or 15 for Read/Write Access. If not specified where it is optional, the privilege level is 1.

i

The admin user account cannot be deleted.

The special characters allowed in the password include ! # $ % & ‘ ( ) * + , - / ; < = > @ [\ ] ^ _ ` { | } ~

Default Setting

No password

Command Mode

Global Config

6.7.2.2 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

6.7.2.3 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

6.7.2.4 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.

<key> - A key 128 alphanumeric characters in length.

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

6.7.2.5 Set the password aging

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.

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.

Syntax

```
passwords aging <1-365>
no passwords aging
```

<1-365> - Number of days until password expires.

Default Setting

0, no aging

Command Mode

Global Config

6.7.2.6 Set the password history

Use this command to set the number of previous passwords that shall be stored for each user account. 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.

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.

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

6.7.2.7 Set the password lock-out count

Use this command to strengthen the security of the switch by locking user accounts that have failed login due to wrong passwords. When a lockout count is configured, a user that is logged in must enter the correct password within that count. Otherwise the user will be locked out from further switch access. Only a user with read/write access can re-activate a locked user account. 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

6.7.2.8 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

6.7.2.9 Set the password strength policy enforcement.

The user can go to the CLI Global Configuration Mode to set the password strength policy enforcement, use the passwords strength-check Global configuration command. Use the no passwords strength-check return to default disable.

Syntax

```
passwords strength-check
no passwords strength-check
```

Default Setting

Disable

Command Mode

Global Config

6.7.2.10 Set the password strength maximum.

The user can go to the CLI Global Configuration Mode to set the password strength, use the passwords strength maximum {consecutive-characters | repeated} [<0-15>] Global configuration command. Use the no passwords strength maximum {consecutive-characters | repeated} return to default value 0.

Syntax

```
passwords strength maximum {consecutive-characters | repeated} [<0-15>] no
passwords strength maximum {consecutive-characters | repeated}
```

Default Setting

0

Command Mode

Global Config

6.7.2.11 Set the password strength minimum.

The user can go to the CLI Global Configuration Mode to set the password strength, use the passwords strength minimum {character-classes | lowercase-letters | numeric-characters | special-characters | uppercase-letters} [<0-15>] Global configuration command. Use the no passwords strength minimum {character-classes | lowercase-letters | numeric-characters | special-characters | uppercase-letters} return to default value 2.

Syntax

passwords strength minimum {character-classes | lowercase-letters | numeric-characters | special-characters | uppercase-letters} [<0-15>]
no passwords strength minimum {character-classes | lowercase-letters | numeric-characters | special-characters | uppercase-letters}

Default Setting

2

Command Mode

Global Config

6.7.2.12 Set the password strength exclude-keyword.

The user can go to the CLI Global Configuration Mode to set the password strength, use the passwords strength exclude-keyword <keyword> Global configuration command. Use the no passwords strength exclude-keyword <keyword> return to default none.

Syntax

passwords strength exclude-keyword <keyword>
no passwords strength exclude-keyword <keyword>

Default Setting

None

Command Mode

Global Config

6.8 Security Commands

6.8.1 Show Commands

6.8.1.1 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.

6.8.1.2 show authentication methods

This command displays the ordered authentication methods for all authentication login lists.

Syntax

```
show authentication methods
```

Default Setting

None

Command Mode

Privileged Exec

Display Message

Login Authentication Method Lists: This displays the authentication login listname.

Enable Authentication Method Lists: This displays the authentication enable listname.

6.8.1.3 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.

6.8.1.4 show accounting

Use this command to display ordered methods for accounting lists.

Syntax

show accounting

Default Setting

None

Command Mode

Privileged Exec

Display Message

Number of Accounting Notifications sent at beginning of an EXEC session: 0

Errors when sending Accounting Notifications beginning of an EXEC session: 0

Number of Accounting Notifications at end of an EXEC session: 0

Errors when sending Accounting Notifications at end of an EXEC session: 0

Number of Accounting Notifications sent at beginning of a command execution: 0

Errors when sending Accounting Notifications at beginning of a command execution: 0

Number of Accounting Notifications sent at end of a command execution: 0

Errors when sending Accounting Notifications at end of a command execution: 0

6.8.1.5 show accounting methods

Use this command to display configured accounting method lists.

Syntax

show accounting methods

Default Setting

None

Command Mode

Privileged Exec

6.8.1.6 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).

Dynamic VLAN Creation Mode: Indicates whether the switch can dynamically create a RADIUS-assigned VLAN if it does not currently exist on the switch.

Monitor Mode: Indicates whether the Dot1x Monitor mode on the switch is enabled or disabled.

6.8.1.7 show dot1x authentication-history

This command is used to display the Dot1x Authentication History Log for the specified port or all ports.

Syntax

show dot1x authentication-history <all | <slot/port>>

Default Setting

None

Command Mode

Privileged Exec

Display Message

Time Stamp: The exact time at which the event occurs.

Interface: Physical Port on which the event occurs.

MAC-Address: The supplicant/client MAC address.

VLANID: The VLAN assigned to the client/port on authentication.

Auth Status: The authentication status.

6.8.1.8 show dot1x client

This command is used to display client information.

Syntax

show dot1x clients [<slot/port>]

<slot/port> - is the desired interface number. no

parameter - All interfaces.

Default Setting

None

Command Mode

Privileged Exec

Display Message

Clients Authenticated using Monitor Mode: Indicates the number of the Dot1x clients authenticated using Monitor mode.

Clients Authenticated using Dot1x: Indicates the number of Dot1x clients authenticated using 802.1x authentication process.

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.

Supp MAC Address: The supplicant device MAC address.

Session Time: The time since the supplicant is logged on.

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, Monitor Mode, or Default. When the VLAN Assigned reason is Default, it means that the VLAN was assigned to the port because the P-VID 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. This value is valid for the port only when the port-control mode is not MAC-based.

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.

6.8.1.9 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.

6.8.1.10 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.

PAE Capabilities: The port access entity (PAE) functionality of this port. Possible values are Authenticator or Supplicant.

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.

6.8.1.11 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>]
```

<slot/port> - is the desired interface number. no

parameter - 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.

6.8.1.12 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.

6.8.1.13 show captive-portal

This command reports status of the captive portal feature.

Syntax

```
show captive-portal
```

Default Setting

None

Command Mode

Privileged Exec

Display Message

Administrative Mode: Shows whether the CP is enabled.

Operational Status: Indicates whether the CP operational status is enabled or disabled.

Disable Reason: If CP is disabled, this field displays the reason, which can be None, Administratively Disabled, No IPv4 Address, or Routing Enabled, but no IPv4 routing interface.

Captive Portal IPAddress: Shows the IP address that the captive portal feature uses.

6.8.1.14 show captive-portal client <macaddr> statistics

This command displays client connection details or a connection summary for connected captive portal users. Use the optional [macaddr] keyword, which is the MAC address of a client, to view additional information about that client.

Syntax

```
show captive-portal client <macaddr> statistics
```

Default Setting

None

Command Mode

Privileged Exec

Display Message

Administrative Mode: Shows whether the CP is enabled.

6.8.1.15 show captive-portal client [macaddr] status

This command reports status of the captive portal feature.

Syntax

show captive-portal client [macaddr] status

Default Setting

None

Command Mode

Privileged Exec

Display Message

Client MAC Address: Identifies the MAC address of the client (if applicable).

Client IP Address: Identifies the IP address of the client (if applicable).

Protocol Mode: Shows the current connection protocol, which is either HTTP or HTTPS.

Verification Mode: Shows the current account type, which is Guest, Local, or RADIUS.

Failure Count: The number of times that user login failed.

Session Time: Shows the amount of time that has passed since the client was authorized.

If you specify a client MAC address, the following additional information displays:

CP ID: Shows the captive portal ID the connected client is using.

CP Name: Shows the name of the captive portal the connected client is using.

Interface: Valid slot and port number separated by a forward slash.

Interface Description: Describes the interface.

User Name: Displays the user name (or Guest ID) of the connected client.

6.8.1.16 show captive-portal configuration <cp-id>

This command displays the operational status of each captive portal configuration. The <cp-id> variable is the captive portal ID, which ranges from 1-10.

Syntax

show captive-portal configuration <1-10>

Default Setting

None

Command Mode

Privileged Exec

Display Message

CP ID: Shows the captive portal ID.

CP Name: Shows the captive portal name.

Operational Status: Shows whether the captive portal is enabled or disabled.

Disable Reason: If the captive portal is disabled, this field indicates the reason.

Blocked Status: Shows the blocked status, which is Blocked or Not Blocked.

Authenticated Users: Shows the number of authenticated users connected to the network through this captive portal.

Configured Locales: Shows the number of locales defined for this captive portal.

6.8.1.17 show captive-portal configuration [cp-id] client status This command reports status of the captive portal feature.

Syntax

show captive-portal configuration [cp-id] client status

Default Setting

None

Command Mode

Privileged Exec

Display Message

CP ID: Shows the captive portal ID the connected client is using.

CP Name: Shows the name of the captive portal the connected client is using.

Client MAC Address: Identifies the MAC address of the wireless client (if applicable).

If you use the optional [cp-id] information, the following additional information appears:

Client IP Address: Identifies the IP address of the wireless client (if applicable).

Interface: Valid slot and port number separated by a forward slash.

Interface Description: Describes the interface.

6.8.1.18 show captive-portal configuration <cp-id> interface [interface]

This command displays information for all interfaces assigned to a captive portal configuration or a specific interface assigned to a captive portal configuration.

Syntax

show captive-portal configuration <1-10> interface [<slot/port>]

Default Setting

None

Command Mode

Privileged Exec

Display Message

CP ID: Shows the captive portal ID.

CP Name: Shows the captive portal name.

Interface: Valid slot and port number separated by a forward slash.

Interface Description: Describes the interface.

Operational Status: Shows whether the captive portal is enabled or disabled.

Block Status: Shows the blocked status, which is Blocked or Not Blocked.

If you include the optional slot/port information, the following additional information appears:

Disable Reason: If the captive portal is disabled, this field indicates the reason.

Authenticated Users: Shows the number of authenticated users connected to the network through this captive portal.

6.8.1.19 show captive-portal configuration <cp-id> locales

This command displays locales associated with a specific captive portal configuration.

Syntax

show captive-portal configuration <1-10> locales

Default Setting

None

Command Mode

Privileged Exec

Display Message

Locale Code: Two-letter abbreviation for languages.

Locale Link: The names of the languages.

6.8.1.20 show captive-portal configuration <cp-id> status

This command displays information of all configured captive portal configurations or a specific captive portal configuration.

Syntax

show captive-portal configuration <1-10> status

Default Setting

None

Command Mode

Privileged Exec

Display Message

CP ID: Shows the captive portal ID.

CP Name: Shows the captive portal name.

CP Mode: Shows whether the CP is enabled or disabled.

Protocol Mode: Shows the current connection protocol, which is either HTTP or HTTPS.

Verification Mode: Shows the current account type, which is Guest, Local, or RADIUS.

If you include the optional [cp-id] status keywords, the following additional information appears:

URL Redirect Mode: Indicates whether the Redirect URL Mode is enabled or disabled.

Max Bandwidth Up(bytes/sec): The maximum rate in bytes per second (bps) at which a client can send data into the network.

Max Bandwidth Down (bytes/sec): The maximum rate in bps at which a client can receive data from the network.

Max Input Octets (bytes): The maximum number of octets the user is allowed to transmit.

Max Output Octets (bytes): The maximum number of octets the user is allowed to receive.

Max Total Octets (bytes): The maximum number of octets the user is allowed to transfer, i.e., the sum of octets transmitted and received.

Session Timeout (seconds): Shows the number of seconds a user is permitted to remain connected to the network. Once the Session Timeout value is reached, the user is logged out automatically. A value of 0 means that the user does not have a session Timeout limit.

Idle Timeout(seconds): Shows the number of seconds the user can remain idle before the switch automatically logs the user out. A value of 0 means that the user will not be logged out automatically.

6.8.1.21 show captive-portal interface [slot/port] client status

This command displays information about clients authenticated on all interfaces or a specific interface.

Syntax
show captive-portal interface [<slot/port>] client status

Default Setting

None

Command Mode

Privileged Exec

Display Message

Interface: Valid slot and port number separated by a forward slash.

Interface Description: Describes the interface.

Client MAC Address: Identifies the MAC address of the wireless client (if applicable).

If you use the optional [slot/port] information, the following additional information appears:

Client IP Address: Identifies the IP address of the wireless client (if applicable).

CP ID: Shows the captive portal ID the connected client is using.

CP Name: Shows the name of the captive portal the connected client is using.

Protocol: Shows the current connection protocol, which is either HTTP or HTTPS.

Verification: Shows the current account type, which is Guest, Local, or RADIUS.

User Name: Displays the user name (or Guest ID) of the connected client.

6.8.1.22 show captive-portal interface capability [slot/port]

This command displays all the captive portal eligible interfaces or the interface capabilities for a specific captive portal interface.

Syntax
show captive-portal interface capability [slot/port]

Default Setting

None

Command Mode

Privileged Exec

Display Message

Interface: Valid slot and port number separated by a forward slash.

Interface Description: Describes the interface.

Type: Shows the type of interface.

If you use the optional [slot/port] information, the following additional information appears:

Session Timeout: Indicates whether or not this field is supported by the specified captive portal interface.

Idle Timeout: Indicates whether or not this field is supported by the specified captive portal interface.

Bytes Received Counter: Indicates whether or not this field is supported by the specified captive portal interface.

Bytes Transmitted Counter: Indicates whether or not this field is supported by the specified captive portal interface.

Packets Received Counter: Indicates whether or not this field is supported by the specified captive portal interface.

6.8.1.23 show captive-portal interface configuration [cp-id] status

This command displays the interface to configuration assignments for all captive portal configurations or a specific configuration.

Syntax

```
show captive-portal interface configuration [1-10] status
```

Default Setting

None

Command Mode

Privileged Exec

Display Message

CP ID: Shows the captive portal ID the connected client is using.

CP Name: Shows the name of the captive portal the connected client is using.

Interface: Valid slot and port number separated by a forward slash.

Interface Description: Describes the interface.

Type: Shows the type of interface.

6.8.1.24 show captive-portal status

This command reports status of all captive portal instances in the system.

Syntax
show captive-portal status

Default Setting

None

Command Mode

Privileged Exec

Display Message

Additional HTTP Port: Displays the port number of the additional HTTP port configured for traffic. A value of 0 indicates that only port 80 is configured for HTTP traffic.

Additional HTTP Secure Port: Displays the port number of the additional HTTPS secure port. A value of 0 indicates no additional port and the default port (443) is used.

Peer Switch Statistics Reporting Interval: Displays the interval at which statistics are reported in the Cluster Controller. The reporting interval is in the range of 0, 15-3600 seconds where 0 disables statistical reporting.

Authentication Timeout: Displays the number of seconds to keep the authentication session open with the client. When the timeout expires, the switch disconnects any active TCP or SSL connection with the client.

Supported Captive Portals: Shows the number of supported captive portals in the system.

Configured Captive Portals: Shows the number of captive portals configured on the switch.

Active Captive Portals: Shows the number of captive portal instances that are operationally enabled.

Local Supported Users: Shows the number of users that can be added and configured using the local user database.

Configured Local Users: Shows the number of users that are configured from the local user database.

System Supported Users: Shows the total number of authenticated users that the system can support.

Authenticated Users: Show the number of users currently authenticated to all captive portal instances on this switch.

6.8.1.25 show captive-portal trapflags

This command shows which captive portal SNMP traps are enabled.

Syntax

```
show captive-portal trapflags
```

Default Setting

None

Command Mode

Privileged Exec

Display Message

Client Authentication Failure Traps: Shows whether the SNMP agent sends a trap when a client attempts to authenticate with a captive portal but is unsuccessful.

Client Connection Traps: Shows whether the SNMP agent sends a trap when a client authenticates with and connects to a captive portal.

Client Database Full Traps: Shows whether the SNMP agent sends a trap each time an entry cannot be added to the client database because it is full.

Client Disconnection Traps: Shows whether the SNMP agent sends a trap when a client disconnects from a captive portal.

6.8.1.26 show captive-portal user [user-id] [group [<group-id>]]

This command displays all configured users or a specific user in the captive portal local user database. Enter the optional user ID to view information about the specified user. The [user-id] variable is a valid user configured in the local database. Enter the group keyword or the group keyword and group ID variable to view the user information organized by groups.

Syntax

show captive-portal user [user-id] [group [<group-id>]]

Default Setting

None

Command Mode

Privileged Exec

Display Message

User ID: Displays the ID of the user.

User Name: Displays the user name.

Session Timeout: Displays the number of seconds the user can remain in a session before being disconnected from the Captive Portal.

Idle Timeout: Displays the number of seconds the user can remain idle before being disconnected from the Captive Portal.

Group ID: Displays the group identifier for the group to which the user belongs.

When you include the [user-id] variable, the following information also displays:

Password Configured: Indicates whether a password has been configured for the user.

Max Bandwidth Up(bps): The maximum rate in bytes per second (bps) at which a client can send data into the network.

Max BandwidthDown (bps): The maximum rate in bps at which a client can receive data from the network.

Max Bandwidth Input Octets(bytes): Max Bandwidth Input Octets(bytes)

Max Bandwidth Output Octets(bytes): The maximum number of octets the user is allowed to receive.

Max Bandwidth Total Octets(bytes): The maximum number of octets the user is allowed to transfer, i.e., the sum of octets transmitted and received.

6.8.1.27 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

Number of Configured 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 Authentication server groups.

Number of Named Accounting Server Groups: The number of configured named RADIUS Accounting server groups.

Number of Retransmits: The configured value of the maximum number of times a request packet is retransmitted.

Timeout Duration: The configured timeout value, in seconds, for request re-transmissions.

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.

RADIUS Attribute 95 Mode: A global parameter to indicate whether the NAS-IPv6-Address attribute has been enabled to use in RADIUS requests.

RADIUS Attribute 95 Value: A global parameter that specifies the IPv6 address to be used in the NAS-IP-Address attribute to be used in RADIUS requests.

6.8.1.28 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 [{<ipaddr | ipv6addr | hostname> | name <servername> | statistics {<ipaddr| ipv6addr | hostname> | name <servername>}}]

<ipaddr | ipv6addr| hostname> - is an IPv4/v6 Address or hostname.

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

Host 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 ' ipaddr| ipv6addr| hostname ' is included.

RADIUS Accounting Server IP Address: IP Address of the configured RADIUS accounting server.

RADIUS Accounting Server Name: The name of the configured RADIUS accounting server.

Port: The port in use by the RADIUS accounting server.

Secret Configured: Yes or No Boolean value indicating whether this server is configured with a secret.

If the optional token 'statistics <ipaddr| ipv6addr | hostname>' 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 Host 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.

6.8.1.29 show radius servers

This command is used to display items of the configured RADIUS servers.

Syntax

show radius servers [{<ipaddr | ipv6addr | hostname> | name <servername>}]

Default Setting

None

Command Mode

Privileged Exec

Display Message

RADIUS Server Name: The Name of the authenticating server.

RADIUS Server IP Address: The IP address or host name of the authenticating server.

Current Server IP Address: The '*' symbol preceeding the server host address specifies that the server is currently active.

Number of Retransmits: The configured value of the maximum number of times a request packet is retransmitted.

Timeout Duration: The configured timeout value, in seconds, for request re-transmissions.

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.

RADIUS Attribute 95 Mode: A global parameter to indicate whether the NAS-IPv6-Address attribute has been enabled to use in RADIUS requests.

RADIUS Attribute 95 Value: A global parameter that specifies the IPv6 address to be used in the NAS-IP-Address attribute to be used in RADIUS requests.

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.

6.8.1.30 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|ipv6addr|hostname> | name <servername> }

<ipaddr|ipv6addr|hostname> - is an IPv4/v6 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.

RADIUS Server Name: The Name of the authenticating server.

Server Host Address - 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.

6.8.1.31 show radius source-interface

This command is used to display the configured global source interface details used for a RADIUS client. The IP address of the selected interface is used as source IP for all communications with the server.

Syntax

```
show radius source-interface
```

Default Setting

None

Command Mode

Privileged Exec

Display Message

RADIUS Client Source Interface: The interface to use as the source interface for RADIUS client.

RADIUS Client Source IPv4 Address: The IP address of the interface configured as the RADIUS client source interface.

6.8.1.32 show tacacs

This command display configured information and statistics of a TACACS+ server.

Syntax

```
show tacacs [<ipaddr|ipv6Addr|hostname>]
```

<ipaddr|ipv6Addr|hostname> - is an IPv4/v6 Address or a hostname.

Default Setting

None

Command Mode

Privileged Exec

Display Message

Host address - 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.

6.8.1.33 show tacacs-server source-interface

This command is used to display the configured global source interface details used for a RADIUS client. The IP address of the selected interface is used as source IP for all communications with the server.

Syntax

```
show tacacs-server source-interface
```

Default Setting

None

Command Mode

Privileged Exec

Display Message

TACACS Client Source Interface: The interface to use as the source interface for TACACS client.

TACACS Client Source IPv4 Address: The IP address of the interface configured as the TACACS client source interface.

6.8.1.34 show ldap

Use this command to display LDAP configuration.

Syntax

show ldap

Default Setting

None

Command Mode

Privileged Exec

User Exec

Display Message

Server Ip: The IP address of LDAP server.

Server Port: The port number that LDAP server is listening.

BaseDn: The base DN.

RacName: The attribute that presents user name.

RacDomain: The path of the user name node.

6.8.1.35 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.

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

Number of static MAC addresses configured: Number of static MAC addresses configured.

Statically configured MAC Address: Statically locked MAC address.

VLAN ID: Vlan ID of the Statically configured 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.

6.8.2 Configuration Commands

6.8.2.1 aaa authentication login <method>

This command creates an authentication login list. The <listname> is up to 12 alphanumeric characters and is not case sensitive. Up to 5 authentication login lists can be configured on the switch.

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 possible method values are enable, ldap, line, local, radius, noneand 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 none 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. The value of ldap indicates that the user's ID and password will be authenticated using the LDAP.

To authenticate a user, the authentication methods in the user's login will be attempted in order until an authentication attempt succeeds or fails.

The default login list included with the default configuration cannot be changed.

Syntax

```
aaa authentication login <listname> { enable | ldap | line | local | none | radius | tacacs} no
aaa authentication login <listname>
```

<listname> - creates an authentication login list (Range: up to 12 characters).

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

6.8.2.2 aaa accounting

Use this command in Global config mode to create an accounting method list for either user EXEC sessions or for user-executed commands. This list is identified by default or a user-specified list_name. Accounting records, when enabled for a line-mode, can be sent at both the beginning and at the end (start-stop) or only at the end (stop-only). If none is specified, then accounting is disabled for the specified list. If tacacs is specified as the accounting method, accounting records are notified to a TACACS+ server. If radius is the specified accounting method, accounting records are notified to a RADIUS server.

- A maximum of five Accounting Method lists can be created for each exec and commands type.
- The same list-name can be used for both exec and commands accounting type.
- AAA Accounting for commands with RADIUS as the accounting method is not supported.

Syntax

aaa accounting {exec | commands} {default | <list_name>} { start-stop | stop-only | none} method1 [method2...]
no aaa accounting {exec | commands} {default | <list_name>}

exec - Provide accounting for a user EXEC terminal sessions.

commands - Provide accounting for all user executed commands.

default - The default list of methods for accounting services.

<listname> - Character string used to name the list of accounting methods.

start-stop - Send a start accounting notice at the beginning of a process and a stop accounting notice at the end of a process.

stop-only - Sends a stop accounting notice at the end of the requested user process.

none - Disables accounting services on this line.

method - Use either TACACS or RADIUS server for accounting purposes. no

- This command deletes the accounting method list.

Default Setting

None

Command Mode

Global Config

6.8.2.3 accounting

Use this command in Line Configuration mode to apply the accounting method list to a line config (console/telnet/ssh).

Syntax

accounting {exec | commands} {default | <list_name>}
no accounting

exec - Causes accounting for an EXEC session.

commands - This causes accounting for each command execution attempt. If a user is enabling accounting for exec mode for the current line-configuration type, the user will be logged out..

default - The default Accounting List.

<listname> - Enter a string of not more than 15 characters.

no - This command removes accounting from a Line Configuration mode.

Default Setting

None

Command Mode

Line Configuration Mode

6.8.2.4 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

6.8.2.5 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.

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

6.8.3 Dot1x Configuration Commands

6.8.3.1 dynamic-vlan

This command enable dot1x dynamic vlan creation configuration.

Syntax

```
dot1x dynamic-vlan enable
no dot1x dynamic-vlan enable
```

Default Setting

None

Command Mode

Global Config

6.8.3.2 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

6.8.3.3 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 [monitor]
no dot1x system-auth-control [monitor]
```

no - This command is used to disable the dot1x authentication support on the switch.

Default Setting

Disabled

Command Mode

Global Config

6.8.3.4 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

6.8.3.5 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

6.8.3.6 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

6.8.3.7 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

6.8.3.8 dot1x pae

This command set the PAE capability mode on the specified port.

Syntax

```
dot1x pae <authenticator| supplicant>
```

Default Setting

authenticator

Command Mode

Interface Config

6.8.3.9 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

6.8.3.10 dot1x supplicant max-start

This command configure the maximum number of Start EAPOL messages to be sent in the absence of Authenticator.

Syntax

```
dot1x supplicant max-start <1-10>
no dot1x supplicant max-start
```

Default Setting

3

Command Mode

Interface Config

6.8.3.11 dot1x supplicant port-control

This command set the authentication mode on the specified port.

Syntax

dot1x supplicant port-control < auto| force-authorized|force-unauthorized> no
dot1x supplicant port-control

Default Setting

auto

Command Mode

Interface Config

6.8.3.12 dot1x supplicant timeout auth-period

This command configure the auth period value.

Syntax

dot1x supplicant timeout auth-period <seconds>
no dot1x supplicant timeout auth-period

<seconds> - Range: 1-65535.

Default Setting

30

Command Mode

Interface Config

6.8.3.13 dot1x supplicant timeout held-period

This command configure the held period value.

Syntax

```
dot1x supplicant timeout held-period <seconds>
no dot1x supplicant timeout held -period
```

<seconds> - Range: 1-65535.

Default Setting

60

Command Mode

Interface Config

6.8.3.14 dot1x supplicant timeout start-period

This command configure the start period value.

Syntax

```
dot1x supplicant timeout start-period <seconds>
no dot1x supplicant timeout start-period
```

<seconds> - Range: 1-65535.

Default Setting

60

Command Mode

Interface Config

6.8.3.15 dot1x supplicant user

This command configure Supplicant user.

Syntax

```
dot1x supplicant user <user>
no dot1x supplicant user <user>
```

Default Setting

None

Command Mode

Interface Config

6.8.3.16 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

6.8.3.17 dot1x unauthenticated-vlan

This command configure Unauthenticated VLAN for the port.

Syntax

```
dot1x unauthenticated-vlan <vlan-id>
no dot1x unauthenticated-vlan
```

Default Setting

0

Command Mode

Interface Config

6.8.4 Captive Portal Commands

6.8.4.1 captive-portal mode

Use this command to enter the Captive Portal Configuration Mode.

Syntax

captive-portal

Default Setting

Command Mode

Global Config

6.8.4.2 captive-portal authentication timeout

This command configures the authentication timeout. If the captive portal user does not enter valid credentials within this time limit, the authentication page needs to be served again in order for the client to gain access to the network. The <timeout> variable is the authentication timeout and is a number in the range of 60-600 seconds.

Syntax

authentication timeout <60-600>
no authentication timeout

Default Setting

300

Command Mode

Captive Portal Config

6.8.4.3 captive-portal configuration mode

Use this command to enter the Captive Portal Instance Mode.

The captive portal configuration, identified by CP ID 1, is the default CP configuration. You can create up to nine additional captive portal configurations. The system supports a total of ten CP configurations. The Captive Portal ID <cp-id> variable is a number in the range of 1-10.

Syntax

```
configuration <1-10>
```

Default Setting

None

Command Mode

Captive Portal Config

6.8.4.4 Enable/Disable captive-portal

This command globally enables the captive portal feature on the switch.

Syntax

```
enable
no enable
```

Default Setting

Disable

Command Mode

Captive Portal Config

6.8.4.5 Captive-portal http port

This command configures an additional HTTP port. Valid port numbers are in the range of 0-65535, excluding port numbers 80 and 443 which are reserved. The HTTP port default is 0 which denotes no additional port and the default port (80) is used.

Syntax

```
http port <0-65535>
no http port
```

Default Setting

0

Command Mode

Captive Portal Config

6.8.4.6 Captive-portal https port

This command configures an additional HTTPS secure port. The HTTPS secure port default is 0 which denotes no additional port and the default port (443) is used.

Syntax

```
https port <0-65535>
no http port
```

Default Setting

0

Command Mode

Captive Portal Config

6.8.4.7 Captive-portal trapflags

This command enables captive portal SNMP traps. If no parameters are specified, then all traps are enabled. SNMP traps can also be enabled individually by supplying the optional parameters.

Syntax

```
trapflags [client-auth-failure| client-connect | client-db-full | client-disconnect]
no trapflags [client-auth-failure | client-connect | client-db-full | client-disconnect]
```

Default Setting

Disable

Command Mode

Captive Portal Config

6.8.4.8 Captive Portal local user parameters

This command assigns/modifies the group name for the associated captive portal user. The <user-id> variable is the user ID, which is a number in the range of 1 to 128. The <group-name> variable is a name up to 32 characters.

Syntax

```
user <1-128> group <1-10>
no user <1-128> [group <1-10>]
```

Default Setting

None

Command Mode

Captive Portal Config

6.8.4.9 Captive Portal user idle timeout

This command sets the session idle timeout value for the associated captive portal user. The <user-id> variable is the ID of a user configured in the local database, and is a number in the range of 1 to 128. The <timeout> variable is a number that represents the idle timeout in seconds. Use 0 to indicate that the timeout is not enforced.

Syntax

```
user <1-128> idle-timeout <0-900>
no user <1-128> idle-timeout
```

Default Setting

0

Command Mode

Captive Portal Config

6.8.4.10 Captive Portal max down/receive bandwidth

This command is used configure the bandwidth in bytes per second (bps) at which the client can receive data from the network. 0 denotes using the default value configured for the captive portal.

Syntax

```
user <1-128> max-bandwidth-down <0-536870911>
no user <1-128> max-bandwidth-down
```

Default Setting

0

Command Mode

Captive Portal Config

6.8.4.11 Captive Portal max up/transmit bandwidth

This command is used to configure the bandwidth in bytes per second (bps) at which the client can send data into the network. 0 denotes using the default value configured for the captive portal.

Syntax

```
user <1-128> max-bandwidth-up <0-536870911>
no user <1-128> max-bandwidth-up
```

Default Setting

0

Command Mode

Captive Portal Config

6.8.4.12 Captive Portal max bytes allowed to input/transmit

This command is used to limit the number of octets in bytes that the user is allowed to transmit. After this limit has been reached, the user will be disconnected. 0 octets denote unlimited transmission.

Syntax

```
user <1-128> max-input-octets <0-4294967295>
no user <1-128> max-input-octets
```

Default Setting

0

Command Mode

Captive Portal Config

6.8.4.13 Captive Portal max bytes allowed to output/transmit

This command is used to limit the number of octets in bytes that the user is allowed to receive. After this limit has been reached, the user will be disconnected. 0 octets denote unlimited transmission.

Syntax

user <1-128> max-output-octets <0-4294967295>

no user <1-128> max-output-octets

Default Setting

0

Command Mode

Captive Portal Config

6.8.4.14 Captive Portal max total allowed to transmit and receive

This command is used to limit the number of octets in bytes that the user is allowed to transmit and receive. The maximum number of octets is the sum of octets transmitted and received. After this limit has been reached, the user will be disconnected. 0 octets denote unlimited transmission.

Syntax

user <1-128> max-total-octets <0-4294967295>

no user <1-128> max-total-octets

Default Setting

0

Command Mode

Captive Portal Config

6.8.4.15 Captive Portal user name

This command assigns a name to the User ID. This name is used at the client station for authentication. The <user-id> variable is the local user ID created with the user command and can be from 1 to 128 characters. The <username> variable is the name of the user and can have up to 32 alphanumeric characters.

Syntax

```
user <1-128> name <name>
```

Default Setting

None

Command Mode

Captive Portal Config

6.8.4.16 Captive Portal user by specifying a password string

This command sets or modifies the password for the associated captive portal user. The <user-id> variable is the local user ID created with the user command and can be from 1 to 128 characters. The <password> variable is the user id's password and can have from 8 to 64 alphanumeric characters.

Syntax

```
user <1-128> password [encrypted <encrypted-password>]
```

Default Setting

None

Command Mode

Captive Portal Config

6.8.4.17 Captive Portal user session timeout

This command configures the session timeout for a captive portal configuration. The <timeout> variable is a number that represents the session timeout in seconds. Use 0 to indicate that the timeout is not enforced.

Syntax

user <1-128> session-timeout <0-86400>

no user <1-128> session-timeout

Default Setting

0

Command Mode

Captive Portal Config

6.8.4.18 Captive Portal user groups

Use this command to create a user group. The <group-id> variable is a number in the range of 1-10.

Syntax

user group <1-10>

no user group <1-10>

Default Setting

None

Command Mode

Captive Portal Config

6.8.4.19 Captive Portal Move users between existing user groups

This command moves existing users from one user group to another. Note that the destination group must already exist before a move is successful. The <group-id> and <destination-group-id> variables are each a number in the range of 1-10.

Syntax

```
user group <1-10> moveusers <destination-group-id>
```

Default Setting

None

Command Mode

Captive Portal Config

6.8.4.20 Captive Portal user group name

Use this command to configure a group name. The <group-id> variable is a number in the range of 1-10. The <name> variable can be up to 32 alphanumeric characters.

Syntax

```
user group <1-10> name <name>
```

Default Setting

None

Command Mode

Captive Portal Config

6.8.4.21 Captive Portal configuration background color

Use this command to customize the background color of the Captive Portal authentication page using a wellknown color name or RGB value. For example, red or RGB hex-code, i.e. #FF0000.The range of <colorcode> is 1-32 characters.

Syntax

background-color <color-code>

no background-color

Default Setting

#BFBFBF

Command Mode

Captive Portal Instance

6.8.4.22 Captive Portal configuration Block/Unblock traffic

This command blocks all traffic for a captive portal configuration.

Syntax

captive-portal configuration <1-10> block

no captive-portal configuration <1-10> block

Default Setting

None

Command Mode

Privileged Exec

6.8.4.23 Captive Portal clear configuration

This command sets the configuration for this instance to the default values.

Syntax

clear

Default Setting

None

Command Mode

Captive Portal Instance

6.8.4.24 Captive Portal Enable/Disable configuration

This command enables a captive portal configuration.

Syntax

enable

no enable

Default Setting

Enable

Command Mode

Captive Portal Instance

6.8.4.25 Captive Portal configuration foreground color

Use this command to customize the foreground color of the Captive Portal authentication page using a wellknown color name or RGB value. For example, red or RGB hex-code, i.e. #FF0000.The range of <colorcode> is 1-32 characters.

Syntax

foreground-color <color-code>

no foreground-color

Default Setting

#999999

Command Mode

Captive Portal Instance

6.8.4.26 Captive Portal configuration associate to a group

This command assigns a group ID to a captive portal configuration. Each Captive Portal configuration must contain at least one group ID. The group-ID has a 1-1024 range. Group ID 1 is the default.

Syntax

group <1-10>

no group

Default Setting

group-ID 1

Command Mode

Captive Portal Instance

6.8.4.27 Captive Portal configuration idle timeout

This command configures the idle timeout for a captive portal configuration. The <timeout> variable is a number that represents the idle timeout in seconds. Use 0 to indicate that the timeout is not enforced.

Syntax

idle-timeout <0-900>

no idle-timeout

Default Setting

0

Command Mode

Captive Portal Instance

6.8.4.28 Captive Portal configuration associate an interface

This command associates an interface to a captive portal configuration or removes the interface captive portal association.

Syntax

interface <slot/port>

no interface <slot/port>

Default Setting

None

Command Mode

Captive Portal Instance

6.8.4.29 Captive Portal configuration enter locale mode

This command is not intended to be a user command. The administrator must use the WEB user interface to create and customize captive portal web content. The command is primarily used by the FASTPATH show running config command and process as it provides the ability to save and restore configurations using a textbased format.

Syntax

```
locale <1-5>
no locale <1-5>
```

Default Setting

None

Command Mode

Captive Portal Instance

6.8.4.30 Captive Portal configuration max down/receive bandwidth

This command configures the maximum rate at which a client can receive data from the network.

Syntax

```
max-bandwidth-down      <0-536870911>
no max-bandwidth-down
```

Default Setting

0

Command Mode

Captive Portal Instance

6.8.4.31 Captive Portal configuration max up/transmit bandwidth

This command configures the maximum rate at which a client can send data into the network.

Syntax

max-bandwidth-up <0-536870911>

no max-bandwidth-up

Default Setting

0

Command Mode

Captive Portal Instance

6.8.4.32 Captive Portal configuration max bytes allowed to input/transmit

This command configures the maximum number of octets the user is allowed to transmit. After this limit has been reached the user will be disconnected. If the value is set to 0 then the limit is not enforced.

Syntax

max-input-octets <0-4294967295>

no max-input-octets

Default Setting

0

Command Mode

Captive Portal Instance

6.8.4.33 Captive Portal configuration max bytes allowed to output/receive

This command configures the maximum number of octets the user is allowed to receive. After this limit has been reached the user will be disconnected. If the value is set to 0 then the limit is not enforced.

Syntax

max-output-octets <0-4294967295>

no max-output-octets

Default Setting

0

Command Mode

Captive Portal Instance

6.8.4.34 Captive Portal configuration max total allowed to transmit and receive

This command configures the maximum number of octets the user is allowed to transfer, i.e., the sum of octets transmitted and received. After this limit has been reached the user will be disconnected. If the value is set to 0, then the limit is not enforced.

Syntax

max-total-octets <0-4294967295>

no max-total-octets

Default Setting

0

Command Mode

Captive Portal Instance

6.8.4.35 Captive Portal configuration name

This command configures the name for a captive portal configuration. The name can contain up to 32 alphanumeric characters.

Syntax

```
name    <cp-name>
no name
```

Default Setting

None

Command Mode

Captive Portal Instance

6.8.4.36 Captive Portal configuration protocol

This command configures the protocol mode for a captive portal configuration. The CP can use HTTP or HTTPS protocols.

Syntax

```
protocol <http|https>
```

Default Setting

http

Command Mode

Captive Portal Instance

6.8.4.37 Captive Portal configuration RADIUS authentication server

Use this command to configure a captive portal configuration RADIUS authentication server.

Syntax

radius-auth-server <server-name>

no radius-auth-server

Default Setting

Disable

Command Mode

Captive Portal Instance

6.8.4.38 Enable/Disable Captive Portal configuration redirect mode

This command enables the redirect mode for a captive portal configuration.

Syntax

redirect

no redirect

Default Setting

Disable

Command Mode

Captive Portal Instance

6.8.4.39 Captive Portal configuration redirect mode redirect URL

Use this command to specify the URL to which the newly authenticated client is redirected if the URL Redirect Mode is enabled. This command is only available if the redirect mode is enabled.

Syntax

redirect-url <url>

Default Setting

None

Command Mode

Captive Portal Instance

6.8.4.40 Captive Portal configuration separator color

Use this command to customize the separator bar color of the Captive Portal authentication page using a wellknown color name or RGB value. For example, red or RGB hex-code; i.e. #FF0000.The range of <colorcode> is 1-32 characters.

Syntax

separator-color <color-code>

no separator-color

Default Setting

#BFBFBF

Command Mode

Captive Portal Instance

6.8.4.41 Captive Portal configuration session timeout

This command configures the session timeout for a captive portal configuration. The <timeout> variable is a number that represents the session timeout in seconds. Use 0 to indicate that the timeout is not enforced.

Syntax
session-timeout
no session-timeout

Default Setting

0

Command Mode

Captive Portal Instance

6.8.4.42 Captive Portal configuration user-logout mode

This command enables the ability for an authenticated user to de-authenticate from the network. This command is configurable for a captive portal configuration.

Syntax
user-logout
no user-logout

Default Setting

Disable

Command Mode

Captive Portal Instance

6.8.4.43 Captive Portal configuration verification mode

This command configures the verification mode for a captive portal configuration. The type of user verification to perform can be one of the following:

· Guest: The user does not need to be authenticated by a database.

· Local: The switch uses a local database to authenticated users.

· RADIUS: The switch uses a database on a remote RADIUS server to authenticate users.

Syntax

verification <guest| local | radius>

Default Setting

guest

Command Mode

Captive Portal Instance

6.8.4.44 Captive Portal configuration error message indicating user must accept

This command is to Captive Portal configuration error message indicating user must accept.

Syntax

accept-msg <UTF-16>

no accept-msg

Default Setting

None

Command Mode

Captive Portal Locale Mode

6.8.4.45 Captive Portal configuration user acceptance text

This command is to Captive Portal configuration user acceptance text.

Syntax

accept-text <UTF-16>

no accept-text

Default Setting

None

Command Mode

Captive Portal Locale Mode

6.8.4.46 Captive Portal configuration image name for accounting identification

This command is to Captive Portal configuration image name for accounting identification.

Syntax

account-image <image-name>

no account-image

Default Setting

None

Command Mode

Captive Portal Locale Mode

6.8.4.47 Captive Portal configuration label name for accounting identification

This command is to Captive Portal configuration label name for accounting identification.

Syntax

account-label <UTF-16>

no account-label

Default Setting

None

Command Mode

Captive Portal Locale Mode

6.8.4.48 Captive Portal configuration Acceptance Use Policy

This command is to Captive Portal configuration Acceptance Use Policy.

Syntax

aup-text <UTF-16>

no aup-text

Default Setting

None

Command Mode

Captive Portal Locale Mode

6.8.4.49 Captive Portal image name for background appearence

This command is to Captive Portal configuration image name for background appearence.

Syntax

background-image <image-name>

no background-image

Default Setting

None

Command Mode

Captive Portal Locale Mode

6.8.4.50 Captive Portal image name for branding appearence

This command is to Captive Portal configuration image name for branding appearence.

Syntax

branding-image <image-name>

no branding-image

Default Setting

None

Command Mode

Captive Portal Locale Mode

6.8.4.51 Captive Portal text intended for browser title

This command is to Captive Portal configuration text intended for browser title.

Syntax

browser-title <UTF-16>

no browser-title

Default Setting

None

Command Mode

Captive Portal Locale Mode

6.8.4.52 Captive Portal button label

This command is to Captive Portal configuration button label.

Syntax

button-label <UTF-16>

no button-label

Default Setting

None

Command Mode

Captive Portal Locale Mode

6.8.4.53 Captive Portal locale code

This command is to Captive Portal configuration locale code.

Syntax

code <locale-code>

no code

Default Setting

None

Command Mode

Captive Portal Locale Mode

6.8.4.54 Captive Portal denied error message

This command is to Captive Portal configuration denied error message.

Syntax

denied-msg <UTF-16>

no denied-msg

Default Setting

None

Command Mode

Captive Portal Locale Mode

6.8.4.55 Captive Portal preferred fonts for this locale

This command is to Captive Portal configuration preferred fonts for this locale.

Syntax

font-list <font,font>

no font-list

Default Setting

None

Command Mode

Captive Portal Locale Mode

6.8.4.56 Captive Portal instructional-text

This command is to Captive Portal configuration instructional-text.

Syntax

instructional-text <UTF-16>

no instructional-text

Default Setting

None

Command Mode

Captive Portal Locale Mode

6.8.4.57 Captive Portal locale link text for user identification

This command is to Captive Portal configuration locale link text for user identification.

Syntax

link <UTF-16>

no link

Default Setting

None

Command Mode

Captive Portal Locale Mode

6.8.4.58 Captive Portal locale logout text intended for internet browser title

This command is to Captive Portal configuration logout text intended for internet browser title.

Syntax

logout-browser-title <UTF-16>

no logout-browser-title

Default Setting

None

Command Mode

Captive Portal Locale Mode

6.8.4.59 Captive Portal text for logout button

This command is to Captive Portal configuration text for logout button.

Syntax

logout-button-label <UTF-16>

no logout-button-label

Default Setting

None

Command Mode

Captive Portal Locale Mode

6.8.4.60 Captive Portal text for logout confirmation text

This command is to Captive Portal configuration text for logout confirmation text.

Syntax

logout-confirmation-text <UTF-16>

no logout-confirmation-text

Default Setting

None

Command Mode

Captive Portal Locale Mode

6.8.4.61 Captive Portal image name for background appearence

This command is to Captive Portal configuration image name for background appearence.

Syntax

logout-success-background-image <image-name>

no logout-success-background-image

Default Setting

None

Command Mode

Captive Portal Locale Mode

6.8.4.62 Captive Portal logout success text intended for internet browser title

This command is to Captive Portal configuration logout success text intended for internet browser title.

Syntax

logout-success-browser-title <UTF-16>

no logout-success-browser-title

Default Setting

None

Command Mode

Captive Portal Locale Mode

6.8.4.63 Captive Portal text for logout success content

This command is to Captive Portal configuration text for logout success content.

Syntax

logout-success-text <UTF-16>

no logout-success-text

Default Setting

None

Command Mode

Captive Portal Locale Mode

6.8.4.64 Captive Portal text for logout success title

This command is to Captive Portal configuration text for logout success title.

Syntax

logout-success-title <UTF-16>

no logout-success-title

Default Setting

None

Command Mode

Captive Portal Locale Mode

6.8.4.65 Captive Portal text for logout instructions

This command is to Captive Portal configuration text for logout instructions.

Syntax

logout-text <UTF-16>

no logout-text

Default Setting

None

Command Mode

Captive Portal Locale Mode

6.8.4.66 Captive Portal text for logout title

This command is to Captive Portal configuration text for logout title.

Syntax

logout-title <UTF-16>

no logout-title

Default Setting

None

Command Mode

Captive Portal Locale Mode

6.8.4.67 Captive Portal text to remind user to allow popups from our web site

This command is to Captive Portal configuration text to remind user to allow popups from our web site.

Syntax

popup-text <UTF-16>

no popup-text

Default Setting

None

Command Mode

Captive Portal Locale Mode

6.8.4.68 Captive Portal text to notify user if their browser has javascript disabled

This command is to Captive Portal configuration text to notify user if their browser has javascript disabled.

Syntax

script-text <UTF-16>

no script-text

Default Setting

None

Command Mode

Captive Portal Locale Mode

6.8.4.69 Captive Portal error message indicating authentication timeout

This command is to Captive Portal configuration error message indicating authentication timeout.

Syntax

timeout-msg <UTF-16>

no timeout-msg

Default Setting

None

Command Mode

Captive Portal Locale Mode

6.8.4.70 Captive Portal text for main title

This command is to Captive Portal configuration text for main title.

Syntax

title-text <UTF-16>

no title-text

Default Setting

None

Command Mode

Captive Portal Locale Mode

6.8.4.71 Captive Portal user input label

This command is to Captive Portal configuration user input label.

Syntax

user-label <UTF-16>

no user-label

Default Setting

None

Command Mode

Captive Portal Locale Mode

6.8.4.72 Captive Portal greeting description

This command is to Captive Portal configuration greeting description.

Syntax

welcome-text <UTF-16>

no welcome-text

Default Setting

None

Command Mode

Captive Portal Locale Mode

6.8.4.73 Captive Portal main title used to greet user

This command is to Captive Portal configuration main title used to greet user.

Syntax

welcome-title <UTF-16>

no welcome-title

Default Setting

None

Command Mode

Captive Portal Locale Mode

6.8.4.74 Captive Portal message indicating authentication in progress

This command is to Captive Portal configuration message indicating authentication in progress.

Syntax

wip-msg <UTF-16>

no wip-msg

Default Setting

None

Command Mode

Captive Portal Locale Mode

6.8.4.75 Radius Configuration Commands

6.8.4.76 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

6.8.4.77 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

6.8.4.78 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

6.8.4.79 radius server attribute 95

This command to set the NAS-IPv6 address for the radius server.

Syntax

radius server attribute 95 [ipv6 address]
no radius server attribute 95

no - use this command to reset the NAS-IPv6 address for the radius server.

Default Setting

None

Command Mode

Global Config

6.8.4.80 radius server dead-time

This command cnfiguresradius server dead time.

Syntax

```
radius server dead-time <minutes>
no radius server dead-time
```

minutes - Set radius server dead time (sec). Range 0 - 2000.

no - This command is used to set dead time to the default value.

Default Setting

0

Command Mode

Global Config

6.8.4.81 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| ipv6addr|hostname> [name <servername>] [port <port>] no
radius server host {acct | auth} <ipaddr| ipv6addr|hostname>
```

<ipaddr| ipv6addr|hostname > - is a IPv4/IPv6 address or a hostname.

<servername> - Server name

<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

6.8.4.82 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|ipv6addr|hostname> [encrypted <password>]
```

<ipaddr|ipv6addr| hostname > - is a IPv4/IPv6 address or hostname.

<password> is the password in encrypted format.

Default Setting

None

Command Mode

Global Config

6.8.4.83 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 retransmit 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, 4.

Default Setting

4

Command Mode

Global Config

6.8.4.84 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, 5.

Default Setting

5

Command Mode

Global Config

6.8.4.85 radius server msgauth

This command enables the message authenticator attribute for a specified server.

Syntax

radius server msgauth <ipaddr| ipv6addr| hostname >

<ipaddr| ipv6addr| hostname > - is a IPv4/v6 address or hostname.

Default Setting

None

Command Mode

Global Config

6.8.4.86 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| ipv6addr| hostname>

<ipaddr|hostname > - is a IPv4/v6 address or a hostname.

Default Setting

None

Command Mode

Global Config

6.8.4.87 radius source-interface

Use this command to specify the physical or logical interface to use as the RADIUS client source interface (Source IP address). If configured, the address of source interface is used for all RADIUS

communications between the RADIUS server and the RADIUS client. The selected source-interface IP address is used for filling the IP header of RADIUS management protocol packets. This allows security device (firewalls) to identify the source packets coming from the specific switch.

If a source-interface is not specified, the primary IP address of the originating (outbound) interface is used as the source address. If the configured interface is down, the RADIUS client falls back to its default behavior.

Syntax

radius source-interface {<slot/port> | loopback <loopback-id> | tunnel <tunnel-id> | vlan <vlan-id>}

<slot/port> - Specifies the interface to use as the source interface.

<loopback-id> - Specifies the loopback interface to use as the source interface. The range of the loopback ID is 0 to 7.

<tunnel-id> - Specifies the tunnel interface to use as the source interface. The range of the tunnel ID is 0 to 7.

<vlan-id> - Specifies the VLAN interface to use as the source interface. The range of VLAN ID is 1 to 4093.

Default Setting

None

Command Mode

Global Config

6.8.5 TACACS+ Configuration Commands

6.8.5.1 tacacs-server 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-server host <ipAddr | ipv6Addr | hostname>
no tacacs-server host <ipAddr | ipv6Addr | hostname>
```

<ipAddr|ipv6Addr|hostname> - The IPv4/v6 address or hostname of the TACACS+ server. no -

This command is used to remove all of configuration.

Default Setting

None

Command Mode

Global Config

6.8.5.2 tacacs-server key

This command is used to configure the TACACS+ authentication and encryption key.

Syntax

```
tacacs-server key [<key-string>|encrypted <key-string>]
no tacacs-server 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

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

6.8.5.3 tacacs-server timeout

This command is used to configure the TACACS+ connection timeout value.

Syntax

```
tacacs-server timeout [<timeout>]
no tacacs-server 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

6.8.5.4 tacacs-server source-interface

Use this command in Global config mode to configure the source interface (Source IP address) for TACACS+ server configuration. The selected source-interface IP address is used for filling the IP header of management protocol packets. This allows security devices (firewalls) to identify the source packets coming from the specific switch.

If a source-interface is not specified, the primary IP address of the originating (outbound) interface is used as the source address.

Syntax

```
tacacs-server source-interface {<slot/port> | loopback <loopback-id> | tunnel <tunnel-id> | vlan <vlan-id>}
no tacacs-server source-interface
```

<slot/port> - Specifies the interface to use as the source interface.

<loopback-id> - Specifies the loopback interface to use as the source interface. The range of the loopback ID is 0 to 7.

<tunnel-id> - Specifies the tunnel interface to use as the source interface. The range of the tunnel ID is 0 to 7.

<vlan-id> - Specifies the VLAN interface to use as the source interface. The range of VLAN ID is 1 to 4093.

no - Use this command to remove the global source interface for all TACACS+ communications between the TACACS+ client and the server.

Default Setting

None

Command Mode

Global Config

6.8.6 LDAP Configuration Commands

6.8.6.1 ldap baseDN

Use this command to indicate the base DN.

Syntax

```
ldap baseDN <baseDN>
no ldap baseDN
```

<baseDN> - The top level of the LDAP directory tree.

no - This command is used to remove base DN setting.

Default Setting

None

Command Mode

Global Config

6.8.6.2 ldap ip

Use this command indicate the IP of LDAP server you want to connect.

Syntax

```
ldap baseDN <ipaddr>
no ldap ip
```

<ipaddr> - The LDAP server's IP address.

no - This command is used to remove LDAP server setting.

Default Setting

None

Command Mode

Global Config

6.8.6.3 ldap port

Use this command to indicate the port number that server are listening.

Syntax

```
ldap baseDN <port>
no ldap port
```

<port> - Range from 1 to 65535.

no - Use no command to default value.

Default Setting

None

Command Mode

Global Config

6.8.6.4 ldap racDomain

Use this command to indicate the full path of parent node of user name.

Syntax

```
ldap racDomain < racDomain>
no ldap racDomain
```

<racDomain> - The full path of parent node of user name. no

- Use no command to default value.

Default Setting

None

Command Mode

Global Config

6.8.6.5 ldap racName

Use this command to indicate which attribute that store the user name.

Syntax

```
ldap racName < racName>
no ldap racName
```

<racName> - The attribute that store the user name. no

- Use no command to default value.

Default Setting

None

Command Mode

Global Config

6.8.7 Port Security Configuration Commands

6.8.7.1 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

6.8.7.2 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

6.8.7.3 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

6.8.7.4 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> <1-4093>
no port-security mac-address <mac-addr> <1-4093>
```

<1-4093> - 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

6.8.7.5 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

6.8.7.6 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

6.8.8 Denial Of Service Commands

6.8.8.1 Show Commands

6.8.8.1.1 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.

ICMPv4 Mode: May be enabled or disabled. The factory default is disabled.

Max ICMPv4 Payload Size: The range is 0-16376. The factory default is 512.

ICMPv6 Mode: May be enabled or disabled. The factory default is disabled.

Max ICMPv6 Payload Size: The range is 0-16376. 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.

6.8.8.2 Configuration Commands

6.8.8.2.1 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

6.8.8.2.2 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

6.8.8.2.3 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 More Fragments(MF) equal to 1 and coorperate with other DoS options, 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

6.8.8.2.4 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

6.8.8.2.5 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

6.8.8.2.6 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

6.8.8.2.7 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

6.8.8.2.8 dos-control icmpv4

This command enables Maximum ICMPv4 Payload 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 payload size greater than the configured value, the packets will be dropped if the mode is enabled.

Syntax

```
dos-control icmpv4
no dos-control icmpv4
```

no - This command disables Maximum ICMPv4 Payload Size Denial of Service protections.

Default Setting

Disabled

Command Mode

Global Config

6.8.8.2.9 dos-control icmpv6

This command enables Maximum ICMPv6 Payload 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 payload size greater than the configured value, the packets will be dropped if the mode is enabled.

Syntax

```
dos-control icmpv6
no dos-control icmpv6
```

no - This command disables Maximum ICMPv6 Payload Size Denial of Service protections.

Default Setting

Disabled

Command Mode

Global Config

6.8.8.2.10 dos-control icmpv4

This command enables Maximum ICMPv4 Payload 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 payload size greater than the configured value, the packets will be dropped if the mode is enabled.

Syntax

```
dos-control icmpv4 [<0-16376>]
no dos-control icmpv4
```

<0-16376> - This command sets maximum ICMPv4 payload size.

no - This command resets the Maximum ICMPv4 Payload Size Denial of Service protections to its default value.

Default Setting

512

Command Mode

Global Config

6.8.8.2.11 dos-control icmpv6

This command enables Maximum ICMPV6 Payload 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 payload size greater than the configured value, the packets will be dropped if the mode is enabled.

Syntax

```
dos-control icmpv6 [<0-16376>]
no dos-control icmpv6
```

<0-16376> - This command sets maximum ICMPV6 payload size.

no - This command resets the Maximum ICMPV6 Payload Size Denial of Service protections to its default value.

Default Setting

512

Command Mode

Global Config

6.8.8.2.12 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

6.8.8.2.13 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

6.8.8.2.14 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

6.8.8.2.15 dos-control tcpflagseq

This command enables the TCP Control Flags=0 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 Control Flags set to 0 and TCP Sequence Number set to 0, the packets will be dropped if the mode is enabled.

Syntax

```
dos-control tcpflagseq
no dos-control tcpflagseq
```

no - This command disables the TCP Control Flags=0 and SEQ=0 checking Denial of Service protections.

Default Setting

Disabled

Command Mode

Global Config

6.8.8.2.16 dos-control tcpsyn

This command enables the TCP SYN and L4 source port = 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 port = 0-1023 Denial of Service protection.

Default Setting

Disabled

Command Mode

Global Config

6.8.8.2.17 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

6.8.8.2.18 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

6.8.8.2.19 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

6.9 CDP (Cisco Discovery Protocol) Commands

6.9.1 Show Commands

6.9.1.1 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

6.9.1.2 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 Intf: 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, Xenya the L2 Network Switch.

Port Id: Identifies the port on which the CDP packet is sent.

6.9.1.3 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, Xenya 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.

6.9.1.4 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.

6.9.2 Configuration Commands

6.9.2.1 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

6.9.2.2 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

6.9.2.3 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

6.9.2.4 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

6.10 SNTP (Simple Network Time Protocol) Commands

6.10.1 Show Commands

6.10.1.1 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.

Multicast Count Current number of unsolicited multicast 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.

Broadcast Poll Interval Poll interval value for SNTP clients in seconds as a power of two.

Multicast Poll Interval Poll interval value for SNTP clients in seconds as a power of two.

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 Maximum 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.

6.10.1.2 show sntp source-interface

Use this command to display the SNTP client source interface configured on the switch.

Syntax
show sntp source-interface

Default Setting

None

Command Mode

Privileged Exec

Display Message

SNTP Client source Interface The interface ID of the physical or logical interface configured as the SNTP client source interface.

SNTP Client Source IPv4 Address The IP address of the interface configured as the SNTP client source interface.

6.10.2 Configuration Commands

6.10.2.1 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

6.10.2.2 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

6.10.2.3 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

6.10.2.4 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

6.10.2.5 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

6.10.2.6 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

6.10.2.7 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

6.10.2.8 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

6.10.2.9 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

6.10.2.10 sntp source-interface

Use this command to specify the physical or logical interface to use as the SNTP client source interface. If configured, the address of source interface is used for all SNTP communications between the SNTP server and the SNTP client. Otherwise, there is no change in behavior. If the configured interface is down, the SNTP client falls back to its default behavior.

Syntax

sntp source-interface {<slot/port> | loopback <loopback-id> | tunnel <tunnel-id> | vlan <vlan-id>} no sntp source-interface

<slot/port> - Specifies the port to use as the source interface.

<loopback-id> - Specifies the loopback interface to use as the source interface. The range of the loopback ID is 0 to 7.

<tunnel-id> - Specifies the tunnel interface to use as the source interface. The range of the tunnel ID is 0 to 7.

<vlan-id> - Specifies the VLAN interface to use as the source interface. The range of the VLAN ID is 1 to 4093.

no - This command will reset the SNTP source interface to its default settings.

Default Setting

None

Command Mode

Global Config

6.11 MAC-Based Voice VLAN Commands

6.11.1 Show Commands

6.11.1.1 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.

6.11.1.2 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 [<slot/port>]]

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.

6.11.2 Configuration Commands

6.11.2.1 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

6.11.2.2 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

6.11.2.3 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

6.11.2.4 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

6.11.2.5 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

6.12 LLDP (Link Layer Discovery Protocol) Commands

6.12.1 Show Commands

6.12.1.1 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.

Reinit Delay: Shows the delay before re-initialization, in seconds.

Notification Interval: Shows how frequently the system sends remote data change notifications, in seconds.

6.12.1.2 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>]
```

<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.

6.12.1.3 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>]

<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.

Tx Total: Total number of LLDP packets transmitted on the port.

Rx 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.

Ageout: Total number of times a complete remote data entry was deleted for the port because the Time to Live interval expired.

TLV Discards: Shows the number of TLVs discarded

TLV Unknowns: Total number of LLDP TLVs received on the port where the type value is in the reserved range, and not recognized.

TLV MED: Total number of LLDP TLVs received on the port where the type value is 127 and OUI type is 00-12-BB.

TLV 802.1: Total number of LLDP TLVs received on the port where the type value is 127 and OUI type is 00-80-C2.

TLV 802.3: Total number of LLDP TLVs received on the port where the type value is 127 and OUI type is 00-12-0F.

TLV EVB: Total number of LLDP TLVs received on the port where the type value is 127 and OUI type is 00-1B-3F.

TLV DCBX: Total number of LLDP TLVs received on the port where the type value is 127 and OUI type is 00-1B-21.

6.12.1.4 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>]
```

<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.

6.12.1.5 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.

MAC/PHY Configuration/Status

Auto-Negetitation: Identifies the auto-negotiation support and current status of the remote device.

PMD Auto-Negetitation: The duplex and bit-rate capability of the port of the remote device.

Operational MAU Type: Displays the MAU type. The MAU performs physical layer functions, including digital data conversion from the Ethernet interfaces' collision detection and bit injection into the network.

Power Via MDI

MDI Power Support: The MDI power capabilities and status.

PSE Power Pair: Indicates the way of feeding the voltage to the data cable.

Power Class: PoE power class.

Link Aggregation

Aggregation Status: Indicates the link aggregation capabilities and the current aggregation status.

Aggregation Port Id: Aggregated port identifier.

Maximum Frame Size: Shows the maximum frame size capability of the implemented MAC and PHY of the remote device.

Port VLAN Identity: Shows the PVID of the connected port of the remote device.

Protocol VLAN

Status: Indicates the port and protocol VLAN capability and status.

ID: The PPVID number for the port of the remote device.

VLAN Name: Shows the name of the VLAN which the connected port is in.

Protocol Identity: Shows the particular protocols that are accessible through the port of the remote device.

6.12.1.6 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>]
```

<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.

6.12.1.7 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.

MAC/PHY Configuration/Status

Auto-Negetitation: Identifies the auto-negotiation support and current status of the local device. PMD

Auto-Negetitation: The duplex and bit-rate capability of the port of the local device.

Operational MAU Type: Displays the MAU type. The MAU performs physical layer functions, including digital data conversion from the Ethernet interfaces' collision detection and bit injection into the network.

Power Via MDI

MDI Power Support: The MDI power capabilities and status.

PSE Power Pair: Indicates the way of feeding the voltage to the data cable.

Power Class: PoE power class.

Link Aggregation

Aggregation Status: Indicates the link aggregation capabilities and the current aggregation status.

Aggregation Port Id: Aggregated port identifier.

Maximum Frame Size: Shows the maximum frame size capability of the implemented MAC and PHY of the remote device.

Port VLAN Identity: Shows the PVID of the connected port of the local device.

VLAN Name: Shows the name of the VLAN which the connected port is in.

Protocol Identity: Shows the particular protocols that are accessible through the port of the local device.

6.12.1.8 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.

6.12.1.9 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 [</slot/port>] Privilege command.

Syntax

show lldp med interface [<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

6.12.1.10 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 <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

Interface: Identifies the interface.

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.

6.12.1.11 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>] Privilege command.

Syntax

show lldp med remote-device [<slot/port>]

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.

6.12.1.12 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.

6.12.2 Configuration Commands

6.12.2.1 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

6.12.2.2 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

6.12.2.3 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

6.12.2.4 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

6.12.2.5 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

6.12.2.6 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

6.12.2.7 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

6.12.2.8 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

6.12.2.9 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

6.12.2.10 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

6.12.2.11 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

6.12.2.12 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

6.12.2.13 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

6.12.2.14 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

6.12.2.15 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

6.13 VTP (VLAN Trunking Protocol) Commands

6.13.1 Show Commands

6.13.1.1 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.

6.13.1.2 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.

6.13.1.3 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.

6.13.1.4 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.

6.13.2 Configuration Commands

6.13.2.1 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

6.13.2.2 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

6.13.2.3 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

6.13.2.4 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

6.13.2.5 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

6.13.2.6 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

6.13.2.7 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

6.14 Protected Ports Commands

6.14.1 Show Commands

6.14.1.1 show switchport protected

This command displays the status of all the interfaces, including protected and unprotected interfaces.

Syntax

show switchport protected [<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.

6.14.1.2 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>.

6.14.2 Configuration Commands

6.14.2.1 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

6.15 Static MAC Filtering Commands

6.15.1 Show Commands

6.15.1.1 show mac-addr-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 <vlan-id>, and the system displays Static MAC Filter information only for that MAC address and VLAN.

Syntax

```
show mac-addr-table static [<macaddr> <vlan-id>]
```

<macaddr> - Static MAC address.

<vlan-id> - VLAN ID. The range of VLAN ID is 1 to 4093.

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).

6.15.2 Configuration Commands

6.15.2.1 macfilter

This command adds a static MAC filter entry for the MAC address <macaddr> on the VLAN <vlan-id>. 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 <vlan-id> parameter must identify a valid VLAN. You can create up to 100 static MAC filters.

Syntax

```
macfilter <macaddr> <vlan-id>
no macfilter <macaddr> <vlan-id>
```

<macaddr> - Specified a 6-byte hexadecimal number in the format of b1:b2:b3:b4:b5:b6.

<vlan-id> - VLAN ID. The range of VLAN ID is 1 to 4093.

no - This command removes all filtering restrictions and the static MAC filter entry for the MAC address <macaddr> on the VLAN <vlan-id>.

Default Setting

None

Command Mode

Global Config

6.15.2.2 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 <vlan-id>. The <macaddr> parameter must be specified as a 6-byte hexadecimal number in the format of b1:b2:b3:b4:b5:b6. The <vlan-id> parameter must identify a valid VLAN.

Syntax

```
macfilter addsrc <macaddr> <vlan-id>
no macfilter addsrc <macaddr> <vlan-id>
```

<macaddr> - Specified a 6-byte hexadecimal number in the format of b1:b2:b3:b4:b5:b6.

<vlan-id> - VLAN ID. The range of VLAN ID is 1 to 4093.

no - This command removes a port from the source filter set for the MAC filter with the MAC address of <macaddr> and VLAN of <vlan-id>.

Default Setting

None

Command Mode

Interface Config

6.15.2.3 macfilter addsrc all

This command adds all interfaces to the source filter set for the MAC filter with the MAC address of <macaddr> and <vlan-id>. You must specify the <macaddr> parameter as a 6-byte hexadecimal number in the format of b1:b2:b3:b4:b5:b6. The <vlan-id> parameter must identify a valid VLAN.

Syntax

```
macfilter addsrc all <macaddr> <vlan-id>
no macfilter addsrc all <macaddr> <vlan-id>
```

<macaddr> - Specified a 6-byte hexadecimal number in the format of b1:b2:b3:b4:b5:b6.

<vlan-id> - VLAN ID. The range of VLAN ID is 1 to 4093.

no - This command removes all interfaces to the source filter set for the MAC filter with the MAC address of <macaddr> and VLAN of <vlan-id>.

Default Setting

None

Command Mode

Global Config

6.16 System Utilities

6.16.1 clear

6.16.1.1 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

6.16.1.2 clear traplog

This command clears the trap log.

Syntax

```
clear traplog
```

Default Setting

None

Command Mode

Privileged Exec

6.16.1.3 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

6.16.1.4 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

6.16.1.5 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

6.16.1.6 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

6.16.1.7 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> | port-channel <portchannel-id> | all]

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

<portchannel-id> - is the desired port-channel ID. The port-channel ID is range from 1 to 64. all - All interfaces.

Default Setting

None

Command Mode

Privileged Exec

6.16.1.8 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

6.16.1.9 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

6.16.1.10 clear vlan

This command resets VLAN configuration parameters to the factory defaults.

Syntax

```
clear vlan
```

Default Setting

None

Command Mode

Privileged Exec

6.16.1.11 clear igmp snooping

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 igmp snooping
```

Default Setting

None

Command Mode

Privileged Exec

6.16.1.12 clear port-channel

This command clears all port-channels (LAGs).

Syntax

```
clear port-channel
```

Default Setting

None

Command Mode

Privileged Exec

6.16.1.13 clear ip filter

This command is used to clear all ip filter entries.

Syntax

```
clear ip filter
```

Default Setting

None

Command Mode

Privileged Exec

6.16.1.14 clear dot1x authentication-history

This command resets the 802.1x authenticaiton-history.

Syntax

```
clear dot1x authentication-history [<slot/port>]
```

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

Default Setting

None

Command Mode

Privileged Exec

6.16.1.15 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

6.16.1.16 clear radius statistics

This command is used to clear all RADIUS statistics.

Syntax

```
clear radius statistics
```

Default Setting

None

Command Mode

Privileged Exec

6.16.1.17 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

6.16.1.18 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

6.16.1.19 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

6.16.1.20 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> | vlan <vlan-id>}]

<slot/port> - Interface number.

<vlan-id> - The VLAN interface number. The range of VLAN ID is 1 to 4093.

Default Setting

None

Command Mode

Privileged Exec

6.16.1.21 clear lldp statistics

This command will use to reset all LLDP statistics.

Syntax

```
clear lldp statistics
```

Default Setting

None

Command Mode

Privileged Exec

6.16.1.22 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

6.16.1.23 enable passwd

This command changes Privileged EXEC password.

Syntax

```
enable passwd 0 <password>
```

0 - Plain text password

Default Setting

None

Command Mode

Global Config.

6.16.1.24 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 7 <password>
```

7 - entrypted password

Default Setting

None

Command Mode

Global Config.

6.16.1.25 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> | vlan <vlan-id>]
```

<slot/port> - Specify the interface.

<vlan-id> - Specifies the VLAN interface. The range of the VLAN ID is 1 to 4093.

Default Setting

None

Command Mode

Privileged Exec

6.16.1.26 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> | vlan <vlan-id>}]
```

<slot/port> - Specify the interface.

<loopback-id > - Specify loopback Interface ID. Range 0 -7.

<tunnel-id > - Specify the Tunnel ID. Range 0 -7.

<vlan-id> - Specifies the VLAN interface. The range of the VLAN ID is 1 to 4093.

Default Setting

None

Command Mode

Privileged Exec

6.16.1.27 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> | vlan <vlan-id>} statistics}

<slot/port> - Specify the interface.

<vlan-id> - Specifies the VLAN interface. The range of the VLAN ID is 1 to 4093.

Default Setting

None

Command Mode

Privileged Exec

6.16.2 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.

6.16.2.1 Upload file from switch

Syntax

```
copy startup-config <url> <sourcefilename>
copy {errorlog | log | traplog | cpu-pkt-capture} <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 -

error crash dump Log file.

log - message Log file.

traplog - trap Log file.

cpu-pkt-capture - The CPU packets capture file.

<filename> - Operation code file name.

Default Setting

None

Command Mode

Privileged Exec

6.16.2.2 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

6.16.2.3 Write running configuration file into flash or remote server

Syntax

```
copy running-config startup-config [filename]
copy running-config <url>
```

<filename> - name of the configuration file.

<url> - xmodem, tftp://ipaddr/path/file or ftp://user:pass@ipaddr/path/file.

Default Setting

None

Command Mode

Privileged Exec

6.16.2.4 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

6.16.3 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

6.16.4 dir

This command is used to display a list of files in Flash memory.

Syntax

```
dir [config | opcode [<filename>] ]
```

<filename> - name of the configuration or image file.

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.

6.16.5 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

6.16.6 boot-system

This command is used to specify the file or image used to start up the system.

Syntax

```
boot-system {config | opcode} <filename>
```

<filename> - name of the configuration or image file.

config - configuration file.

opcode - run time operation code.

Default Setting

None

Command Mode

Privileged Exec

6.16.7 ping

6.16.7.1 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

6.16.7.2 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

6.16.7.3 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

6.16.8 traceroute

6.16.8.1 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

6.16.8.2 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

6.16.9 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

6.16.10 calendar set

This command is used to set the system clock.

Syntax

calendar set <mm/dd/yyy> <hh:mm:ss>

<mm/dd/yyyy> - Date Time <mm/dd/yyyy> format. (Month <1-12>. Day <1-31>. Year <2000-2037>

<hh:mm:ss> - hh in 24-hour format (Range: 0 - 23), mm (Range: 0 - 59), ss (Range: 0 - 59)

Default Setting

None

Command Mode

Privileged Exec

6.16.11 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 [<warm>]

<warm> - To only restart the runtime code without rebooting whole system.

Default Setting

None

Command Mode

Privileged Exec

6.16.12 configure

This command is used to activate global configuration mode.

Syntax

```
configure
```

Default Setting

None

Command Mode

Privileged Exec

6.16.13 disconnect

This command is used to close a telnet session.

Syntax

```
disconnect {<0-58> | all}
```

<0-58> - telnet session ID.

all - all telnet sessions.

Default Setting

None

Command Mode

Privileged Exec

6.16.14 hostname

This command is used to set the prompt string.

Syntax

```
hostname <prompt_string>
```

<prompt_string> - Prompt string.

Default Setting

Xenya

Command Mode

Global Config

6.16.15 quit

This command is used to exit a CLI session.

Syntax

```
quit
```

Default Setting

None

Command Mode

Privileged Exec

6.16.16 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.

6.16.17 AutoInstall Commands

The AutoInstall feature enables the automatic update of the image and configuration of the switch. This feature enables touchless or low-touch provisioning to simplify switch configuration and imaging.

AutoInstall includes the following support:

- Downloading an image from TFTP server using DHCP option 125. The image update can result in a downgrade or upgrade of the firmware on the switch.
- Automatically downloading a configuration file from a TFTP server when the switch is booted with no saved configuration file.

When the switch boots, it attempts to obtain an IP address from a network DHCP server. The response from the DHCP server includes the IP address of the TFTP server where the image and configuration flies are located.

After acquiring an IP address and the additional relevant information from the DHCP server, the switch downloads the image file or configuration file from the TFTP server. A downloaded image is utomatically installed. A downloaded configuration file is saved to non-volatile memory

6.16.17.1 Show Commands

6.16.17.1.1 show autoinstall

This command displays the current status of the AutoInstall process.

Syntax
show autoinstall

Default Setting

None

Command Mode

Privileged Exec

Display Message

AutoInstall Operation: Displays the autoinstall operation is started or stoped.

AutoInstall Persistent Mode: Displays the autoinstall persistently for next reboot cycle.

AutoSave Mode: Displays the autoinstall persistently for next reboot cycle.

AutoReboot Mode: Displays the auto-save of downloaded configuration.

AutoUpgrade Mode: Displays the upgrade mode, which is used to allow to download the newer image.

AutoInstall Retry Count: Retry Count The number of times the switch has attempted to contact the TFTP server during the current AutoInstall session.

6.16.17.2 AutoInstall State: The status of the current or most recently completed AutoInstall session.Configuration Commands

6.16.17.2.1 boot-system autoinstall

Use this command to operationally start or stop the AutoInstall process on the switch. The command is non-persistent and is not saved in the startup or running configuration file.

Syntax

```
boot-system autoinstall { start | stop }
```

Default Setting

None

Command Mode

Privileged Exec

Display Message

None

6.16.17.2.2 boot-system host autoinstall

Use this command to enable AutoInstall on the switch for the next reboot cycle. The command does not change the current behavior of AutoInstall and saves the command to NVRAM.

Syntax

```
boot-system host autoinstall
no boot-system host autoinstall
```

no - Use this command to disable AutoInstall for the next reboot cycle.

Default Setting

None

Command Mode

Privileged Exec

Display Message

None

6.16.17.2.3 boot-system host autosave

Use this command to automatically save the downloaded configuration file to the startup-config file on the switch. When autosave is disabled, you must explicitly save the downloaded configuration to non-volatile memory. If the switch reboots and the downloaded configuration has not been saved, the AutoInstall process begins, if the feature is enabled.

Syntax

```
boot-system host autosave
no boot-system host autosave
```

no - Use this command to disable automatically saving the downloaded configuration on the switch.

Default Setting

None

Command Mode

Privileged Exec

Display Message

None

6.16.17.2.4 boot-system host autoreboot

Use this command to allow the switch to automatically reboot after successfully downloading an image. When auto reboot is enabled, no administrative action is required to activate the image and reload the switch.

This command only work on the autoupgrade is enable.

Syntax

```
boot-system host autoreboot
no boot-system host autoreboot
```

no - Use this command to prevent the switch from automatically rebooting after the image is downloaded by using the AutoInstall feature.

Default Setting

None

Command Mode

Privileged Exec

Display Message

None

6.16.17.2.5 boot-system host upgrade

Use this command to allow the switch only to upgrade the newer image version.

Syntax

```
boot-system host upgrade
no boot-system host upgrade
```

no - Use this command to disable this function.

Default Setting

None

Command Mode

Privileged Exec

Display Message

None

6.16.17.2.6 boot-system host retrycount

Use this command to set the number of attempts to download a configuration file from the TFTP server.

Syntax

```
boot-system host retrycount <1-3>
```

Default Setting

3

Command Mode

Privileged Exec

Display Message

None

6.16.18 Capture CPU packet commands

6.16.18.1 Show commands

6.16.18.1.1 show capture

Use this command to display packets captured and save to RAM, It is possible to capture and save into RAM, packets that are received or transmitted throuph the CPU. A maximum 128 packets can be saved into RAM per capturing session. A maximum 128 bytes per packet can be saved into the RAM. If a packet holds more than 128 bytes, only the first 128 bytes are saved; data more than 128 bytes is skipped and cannot be displayed in the CLI.

Capturing packets is stopped automatically when 128 packets are captured and have not yet been displayed during a capture session. Captured packets are not retained after a reload cycle.

Syntax
show capture [packets]

<packets> - Specifies this parameter to display the captured packets on the CLI.

Default Setting

None

Command Mode

Privileged Exec

Display Message

Operational Status: Displays capture status.

Current Capturing Type: Displays the current capturing type. Possible types are Line, File, and Remote.

Capturing Traffic Mode: Displays the capturing traffic mode. Possible modes are Rx, Tx, or Tx/Rx. Line

Wrap Mode: Displays the line wrap mode for Line capturing type. Default is disabled.

RPCAP Listening Port: Displays the pcap listening port number. Default listening port number is 2002.

RPCAP dump file size (KB): Disaply the capture packet file size. Default file size is 512KB.

Capturing Interface: Display the capturing interface.

6.16.18.2 Configuration Command

6.16.18.2.1 capture start

Use this command to manually start capturing CPU packets for packets for trace. The packet capture operates in three modes: capture file, remote capture and capture line.

This command is not persistent across a reboot cycle.

Syntax

```
capture start [{all | received | transmit}]
```

<all> - Specifies all to capture packets for both transmitted and received packets.

<received> - Specifies received to capture only received packets.

<transmit> - Specifies transmit to capture only transmitted packets.

Default Setting

None

Command Mode

Privileged Exec

6.16.18.2.2 capture stop

Use this command to manually stop capturing CPU packets for packets for trace.

Syntax

```
capture stop
```

Default Setting

None

Command Mode

Privileged Exec

6.16.18.2.3 Capture packet to file, remote or line

Use this command to configure packet capture options. This command is persistent across a reboot cycle.

Syntax

```
capture {file | remote | line}
```

file - In the capture file mode, the captured packets are stored in a file on Flash. The maximum file size defaults to 512KB. The switch can transfer the file to a TFTP server via TFTP, FTP via CLI. The file is formatted in pcap format, is name cpu-pkt-capture.pcap, and can be examined using network analyzer tools such as Wireshark or Ethereal. Starting a file capture automatically terminates any remote capture sessions and line captureing. After the packet capture is activated, the capture proceeds until the capture file reaches its maimum size, or until the capture is stopped manually using CLI command „capture stop“.

Remote - In the remote capture mode, the captured packets are redirected in real time to an external PC running the wireshark tool for Microsoft Windows. A packet capture server runs on the switch side and sends the captured packets via a TCP connection to the Wireshark tool. The remote capture can be enabled or disable using the CLI. There should be a Windows PC with the Wireshark tool to display the captured file. When using the remote capture mode, the switch does not sotre any captured data locally on its file system.

You can configure the IP port number for connecting Wireshark to the switch. The default port number is 2002. If a firewall is installed between the Wireshark PC and the switch, then these ports must be allowed to pass through the firewall.

If the client successfully connects to the switch, the CPU packets are sent to the client PC, then Wireshark receives the packets and displays them. This continues until the session is terminated by either end.

line - In the capture line mode, the captured packets are saved into the RAM and can be displayed on the CLI. Starting a line capture automatically terminates any remote capture dession and capturing into a file. There is a maximum 128 packets of maximum 128 btes that can be captured and displayed in Line mode.

Default Setting

Remote

Command Mode

Global Config

6.16.18.2.4 capture remote port

Use this command to configure file capture options. This command is persistent across a reboot cycle.

Syntax

capture remote [port <port-id>]

<port-id> - Configure the listening port for remote Wireshark tool. The range of port ID is 1024 to 49151.

Default Setting

2002

Command Mode

Global Config

6.16.18.2.5 capture file size

Use this command to configure file capture options. This command is persistent across a reboot cycle.

Syntax

capture file [size <file-size>]

<file-size> - Configure the file size in KB. The range of file size is 2 to 512KB.

Default Setting

512

Command Mode

Global Config

6.16.18.2.6 capture line warp

This command enables wrapping of captured packets in line mode when the captured packets reaches full capacity. This command is persistent across a reboot cycle.

Syntax

```
capture line [wrap]
no capture line wrap
```

Default Setting

Disable

Command Mode

Global Config

6.17 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.

You can enable the switch to operate as a DHCP Layer 2 relay agent to relay DHCP requests from clients to a Layer 3 relay agent or server. The Circuit ID and Remote ID can be added to DHCP requests relayed from clients to a DHCP server. This information is included in DHCP Option 82, as specified in sections 3.1 and 3.2 of RFC3046.

6.17.1 Show Commands

6.17.1.1 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.

6.17.1.2 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.

6.17.1.3 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.

6.17.1.4 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.

6.17.1.5 show ip dhcp snooping information all

This command display the summary of DHCP Option-82 configuration.

Syntax

```
show ip dhcp snooping information all
```

Default Setting

None

Command Mode

Privileged Exec

6.17.1.6 show ip dhcp snooping information stats interface

This command display statistics specific to DHCP Option-82 configuration interface.

Syntax

show ip dhcp snooping information stats interface [<slot/port>]

<slot/port> - Interface number.

Default Setting

None

Command Mode

Privileged Exec

6.17.1.7 show ip dhcp snooping information agent-option vlan

This command display the DHCP Option-82 configuration specific to VLAN.

Syntax

show ip dhcp snooping information agent-option vlan <vlan-list>

<vlan-list> - Specifies VLAN ID in a list. The range of VLAN ID is 1 to 4093.

Default Setting

None

Command Mode

Privileged Exec

6.17.1.8 show ip dhcp snooping information vlan

This command display the DHCP Option-82 configuration specific to VLAN.

Syntax

show ip dhcp snooping information vlan <vlan-list>

<vlan-list> - Specifies VLAN ID in a list. The range of VLAN ID is 1 to 4093.

Default Setting

None

Command Mode

Privileged Exec

6.17.1.9 show ip dhcp snooping information circuit-id vlan

This command display the DHCP Option-82 circuit-id configuration specific to VLAN.

Syntax

show ip dhcp snooping information circuit-id vlan <vlan-list>

<vlan-list> - Specifies VLAN ID in a list. The range of VLAN ID is 1 to 4093.

Default Setting

None

Command Mode

Privileged Exec

6.17.1.10 show ip dhcp snooping information remote-id vlan

This command display the DHCP Option-82 remote-id configuration specific to VLAN.

Syntax

```
show ip dhcp snooping information remote-id vlan <vlan-list>
```

<vlan-list> - Specifies VLAN ID in a list. The range of VLAN ID is 1 to 4093.

Default Setting

None

Command Mode

Privileged Exec

6.17.1.11 show ip dhcp snooping information interface

This command display DHCP Option-82 configuration interface.

Syntax

```
show ip dhcp snooping information interface [<slot/port>]
```

<slot/port> - Specifies the interface number.

Default Setting

None

Command Mode

Privileged Exec

6.17.2 Configuration Commands

6.17.2.1 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

6.17.2.2 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>
```

<vlan-list> - Specifies VLAN ID in a list. The range of VLAN ID is 1 to 4093. no -

This command disables the DHCP Snooping on VLANs.

Default Setting

Disabled

Command Mode

Global Config

6.17.2.3 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

6.17.2.4 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

6.17.2.5 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

6.17.2.6 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

6.17.2.7 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

6.17.2.8 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

6.17.2.9 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

6.17.2.10 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

6.17.2.11 clear ip dhcp snooping binding

Use this command to clear all DHCP Snooping bindings on all interfaces or on a specific interface.

Syntax

```
clear ip dhcp snooping binding [interface <slot/port>]
```

<slot/port> - Specifies the interface number.

Command Mode

Privileged EXEC

6.17.2.12 clear ip dhcp snooping statistics

Use this command to clear all DHCP Snooping statistics.

Syntax

```
clear ip dhcp snooping statistics
```

Command Mode

Privileged EXEC

6.17.2.13 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

6.17.2.14 ip dhcp snooping information option

This command ip dhcp snooping information option enables the DHCP L2 option mode on the interface.

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

Interface Config

6.17.2.15 ip dhcp snooping information option circuit-id

Use this command to enable the DHCP Snooping information option circuit-id on a range of VLANs.When enabled, the circuit ID is added in DHCP Option-82.

Use this command with no argument to disable the DHCP Snooping information option circuit-id on a range of VLANs. Clear the DHCP Option-82 circuit ID for a VLAN.

The circuit ID format should be in the form of LLLLVVVVXXYYZZ (LLLL: is the length from V to Z, VVVV: VLAN ID, XX is the Unit ID, YY is the function/module ID and ZZ is the Port number)

Syntax

ip dhcp snooping information option circuit-id vlan <vlan-list>

no ip dhcp snooping information option circuit-id vlan <vlan-list>

<vlan-list> - Specifies VLAN ID in a list. The range of VLAN ID is 1 to 4093. no -

Clear the DHCP Option-82 circuit ID for a VLAN..

Default Setting

Disabled

Command Mode

Global Config

6.17.2.16 ip dhcp snooping information option remote-id

Use this command to enable the DHCP Snooping information option remote-id on a range of VLANs. When remote-id string is set using this command, all Client DHCP requests that fall under this service subscription are added with Option-82 Remote-id as the configured remote-id string.

Use this command with no argument to disable the DHCP Snooping information option remote-id on a range of VLANs. When remote-id string is reset using this command, the Client DHCP requests that fall under this service subscription are not added with Option-82 Remote-id.

The remote ID format should be in the form of LLLLXXXXX (LLLL: is the length from remote-id strings)

Syntax

ip dhcp snooping information option remote-id <remoteId string> vlan <vlan-list> no

ip dhcp snooping information option remote-id vlan <vlan-list>

<vlan-list> - Specifies VLAN ID in a list. The range of VLAN ID is 1 to 4093. no -

Clear the DHCP Option-82 remoteId ID for a VLAN..

Default Setting

Disabled

Command Mode

Global Config

6.17.2.17 ip dhcp snooping information option vlan

Use this command to enable the DHCP Snooping information option on a range of VLANs.

Syntax

ip dhcp snooping information option vlan <vlan-list>

no ip dhcp snooping information option vlan <vlan-list>

<vlan-list> - Specifies VLAN ID in a list. The range of VLAN ID is 1 to 4093.

no - This command with no argument to disable the DHCP Snooping information option on a range of VLANs..

Default Setting

Disabled

Command Mode

Global Config

6.17.2.18 ip dhcp snooping information option trust

Use this command to configure an interface as trusted for Option-82 reception.

Syntax

ip dhcp snooping information option trust

no ip dhcp snooping information option trust

no - This command with no argument to configure an interface to default untrusted for Option-82 reception..

Default Setting

Disabled

Command Mode

Global Config

6.18 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.

6.18.1 Show Commands

6.18.1.1 show ip verify

This command displays the IPSG interface configurations on all ports.

Syntax

```
show ip verify [interface <slot/port>]
```

<slot/port> - Specifies the interface number.

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.

6.18.1.2 show ip verify source

This command displays the IPSG interface and binding configurations on all ports.

Syntax

```
show ip verify source [interface <slot/port>]
```

<slot/port> - Specifies the interface number.

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.

6.18.1.3 show ip source binding

This command displays the IPSG bindings.

Syntax

```
show ip source binding [{static | dhcp-snooping}] [interface <slot/port>] [vlan <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.

6.18.2 Configuration Commands

6.18.2.1 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

6.18.2.2 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

6.19 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.

6.19.1 Show Commands

6.19.1.1 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>]
```

<vlan-list> - Specifies VLAN ID in a list. The range of VLAN ID is 1 to 4093.

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.

6.19.1.2 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>]

<vlan-list> - Specifies VLAN ID in a list. The range of VLAN ID is 1 to 4093.

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.

6.19.1.3 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.

6.19.1.4 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

6.19.2 Configuration Commands

6.19.2.1 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

6.19.2.2 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

6.19.2.3 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

6.19.2.4 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

6.19.2.5 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

6.19.2.6 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

6.19.2.7 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

6.19.2.8 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

6.19.2.9 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

6.20 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 XS48DSD 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.

6.20.1 General Commands

The following characteristics are configurable for the platform as a whole.

6.20.1.1 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

6.20.1.2 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

6.20.2 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.

6.20.2.1 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

6.20.2.2 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

6.20.2.3 class-map rename

This command changes the name of a DiffServ class.

Syntax

class-map rename <new-class-map-name>

<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

Class-Map Config / Ipv6-Class-Map Config

6.20.2.4 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

6.20.2.5 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.

6.20.2.6 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

6.20.2.7 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

6.20.2.8 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).

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

6.20.2.9 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

6.20.2.10 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

6.20.2.11 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.

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

6.20.2.12 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.

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

6.20.2.13 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>

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

6.20.2.14 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

6.20.2.15 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

6.20.2.16 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).

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

6.20.2.17 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

6.20.2.18 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

6.20.2.19 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

6.20.2.20 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

6.20.2.21 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

6.20.2.22 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

6.20.3 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.

6.20.3.1 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

6.20.3.2 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

6.20.3.3 mirror

This command specifies that all incoming packets for the associated traffic stream are copied to a specific egress interface (physical port or LAG).

This command is not available on the Broadcom 5630x platform.

Syntax

mirror {<slot/port> | port-channel <portchannel-id>}

<slot/port> - Specifies the physical interface where the mirrored packet send to.

<portchannel-id> - Specifies the port-channel interface where the mirrorred packet send to. The range of the port-channel ID is 1 to 64.

Default Setting

None

Command Mode

Policy-Class-Map Config

Incompatibilities

Drop, Redirect

6.20.3.4 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> | port-channel <portchannel-id>}

<slot/port> - Specifies which physical interface that traffic stream are redirected to.

<portchannel-id> - Specifies which port-channel interface that traffic stream are directed to. The range of the port-channel ID is 1 to 64.

Command Mode

Policy-Class-Map Config

Incompatibilities

Drop, Mirror

6.20.3.5 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

6.20.3.6 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

Incompatibilities

Drop, Mark IP DSCP, IP Precedence, Police

6.20.3.7 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

6.20.3.8 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

6.20.3.9 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

Incompatibilities

Drop, Mark CoS, Mark IP Precedence, Police

6.20.3.10 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

Incompatibilities

Drop, Mark (all forms)

6.20.3.11 ip next-hop

Policy Based Routing (PBR) is an alternative to routing protocols and allows you to configure a policy for unicast traffic flows, which provides more control over routing than a routing protocols does and avoids the need to configure interface-level traffic classification.

PBR applies a route policy to all ingress unicast traffic received on a PBR-enabled interface. PBR cannot be applied to egress traffic or to multicast traffic.

If the ingress unicast traffic does not match any route policy statements, the route policy applies all the configured set clauses. Routing protocols forward traffic that does not match any route-policy permit statement.

Use this command to configure where to route the IPv4 unicast packets.

Syntax

ip next-hop <ipAddr>

<ipAddr> - Set next hop to which to route the packets.

Command Mode

Policy-Class-Map Config

6.20.3.12 ipv6 next-hop

Policy Based Routing (PBR) is an alternative to routing protocols and allows you to configure a policy for unicast traffic flows, which provides more control over routing than a routing protocols does and avoids the need to configure interface-level traffic classification.

PBR applies a route policy to all ingress unicast traffic received on a PBR-enabled interface. PBR cannot be applied to egress traffic or to multicast traffic.

If the ingress unicast traffic does not match any route policy statements, the route policy applies all the configured set clauses. Routing protocols forward traffic that does not match any route-policy permit statement.

Use this command to configure where to route the IPv6 unicast packets.

Syntax
Ipv6 next-hop <link-local-address> interface {<slot/port> | vlan <vlan-id>}

<link-local-address> - Set next hop to which to route the packets.

Command Mode

Policy-Class-Map Config

6.20.3.13 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)

6.20.3.14 police-two-rate

This command is the two-rate form of the police command and is used to establish the traffic policing style for the specified class. For each outcome, the only possible actions are drop, set-cos-as-sec-cos, set-cos-transmit, set-sec-cos-transmit, set-dscp-transmit, set-prec-transmit, or transmit. In this two-rate form of the police command, the conform action defaults to send, the exceed action defaults to drop, and the violate action defaults to drop. These actions can be set with this command once the style has been configured.

Syntax

police-two-rate {1-4294967295 1-4294967295 1-128 1-128 conform-action {drop | setcos-as-sec-cos | set-cos-transmit 0-7 | set-sec-cos-transmit 0-7 | set-prec-transmit 0-7 | set-dscp-transmit 0-63 | transmit} exceed-action {drop | set-cos-as-sec-cos | set-cos-transmit 0-7 | set-sec-cos-transmit 0-7 | set-prec-transmit 0-7 | set-dscp-transmit 0-63 | transmit} [violate-action {drop | set-cos-as-sec-cos | set-cos-transmit 0-7 | set-sec-cos-transmit 0-7 | set-prec-transmit 0-7 | set-dscp-transmit 0-63 | transmit}]}

<conform-action & violate-action & exceed-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

6.20.3.15 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 | out} ]
no policy-map <policyname>
```

no - this command is to delete this policy.

in|out - The direction value is either in or out

Command Mode

Global Config

6.20.3.16 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

6.20.4 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

6.20.4.1 service-policy

This command attaches a policy to an interface in a particular direction.

Syntax

service-policy {in | out} <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.

6.20.4.2 no service-policy

This command detaches a policy from an interface in a particular direction.

Syntax

```
no service-policy {in | out} <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)

6.20.5 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.

6.20.5.1 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.

6.20.5.2 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.

6.20.5.3 show diffserv service

This command displays policy service information for the specified interface and direction.

Syntax

show diffserv service {<slot/port> | port-channel <portchannel-id>} in

<slot/port> - specifies a valid slot number and port number for the system. The direction parameter indicates the interface direction of interest.

<portchannel-id> - Specifies the port-channel interface. The range of the port-channel ID is 1 to 64.

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).

6.20.5.4 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.

6.20.5.5 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.

6.20.5.6 show policy-map interface

This command displays policy-oriented statistics information for the specified interface and direction.

Syntax

show policy-map interface {<slot/port> | port-channel <portchannel-id>} in

<slot/port> - specifies a valid slot number and port number for the system. The direction parameter indicates the interface direction of interest.

<portchannel-id> - Specifies the port-channel interface. The range of port-channel ID is 1 to 64.

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.

6.20.5.7 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.

6.21 ACL Command

6.21.1 Show Commands

6.21.1.1 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.

Time Range Name: Displays the name of the time-range if the MAC ACL rule has referenced a time range.

6.21.1.2 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 or Outbound.

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.

6.21.1.3 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.

IPv4 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.

Time Range Name: Displays the name of the time-range if the IP ACL rule has referenced a time range.

Direction: Shows whether the ACL is applied to traffic coming into the interface (ingress) or leaving the interface (egress).

6.21.1.4 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> | port-channel <portchannel-id> } {in | out}

<slot/port> - is the interface number.

<portchannel-id> - is the port-channel ID. The port-channel ID is range from 1 to 64. in |

out - The direction value is either in or out

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).

6.21.2 Configuration Commands

6.21.2.1 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

6.21.2.2 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

6.21.2.3 mac access-group

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 |out} [<1-4294967295>] no mac access-group <name> [vlan <vlan-id>] {in | out}

<no> - This command removes a MAC ACL identified by <name> from the interface or vlan in a given direction.

in|out - The direction value is either in or out

Default Setting

None

Command Mode

Global Config

Interface Config

6.21.2.4 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.

The time-range parameter allows imposing time limitation on the MAC ACL rule as defined by the parameter time-range-name. If a time range with the specified name does not exist and the MAC ACL containing this ACL rule is applied to an interface or bound to a VLAN, then the ACL rule is applied immediately. If a time range with specified name exists and the MAC ACL containing this ACL rule is applied to an interface or bound to a VLAN, then the ACL rule is applied when the time-range with specified name becomes active. The ACL rule is removed when the time-range with specified name becomes inactive.

Syntax

{del-rule-id | deny | permit} {{<srcmac> <srcmask>} | any} {{<dstmac> <dstmask>} | any | bpdu} [<ethertypekey> | <0x0600-0xFFFF>] [vlan {{eq <0-4095>}} [cos <0-7>] [log] [time-range time-range-name] [assign-queue <queue-id>] [{mirror | redirect} {<slot/port> | port-channel <portchannel-id>}] [<rule-id>]

Default Setting

None

Command Mode

Mac Access-list Config

6.21.2.5 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] [time-range time-range-name] [assign-queue <queue-id>] [{mirror | redirect} {<slot/port> | port-channel <portchannel-id>}] [<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 icmp ,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 parameter.

<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.

[time-range time-range-name] - Allows imposing time limitation on the ACL rule as defined by the parameter time-range-name. If a time range with the specified name does not exist and the ACL containing this ACL rule is applied to an interface or bound to a VLAN, then the ACL rule is applied immediately. If a time range with specified name exists and the ACL containing this ACL rule is applied to an interface or bound to a VLAN, then the ACL rule is applied when the time-range with specified name becomes active. The ACL rule is removed when the time-range with specified name becomes inactive.

Default Setting

None

Command Mode

Global Config

6.21.2.6 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

6.21.2.7 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|out} [<1-4294967295>] no
ip access-group {<1-199> | <name>} [vlan <vlan-id>] {in|out}
```

<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.

in|out - The direction value is either in or out

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

6.21.2.8 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

6.21.2.9 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

6.22 IPv6 ACL Command

6.22.1 Show Commands

6.22.1.1 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.

IPv6 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.

Time Range Name: Displays the name of the time-range if the Ipv6 ACL rule has referenced a time range.

Direction: Shows whether the ACL is applied to traffic coming into the interface (ingress) or leaving the interface (egress).

6.22.2 Configuration Commands

6.22.2.1 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.

The CLI mode changes to IPv6-Access-List Config mode when you successfully execute this command.

Default Setting

None

Command Mode

Global Config

6.22.2.2 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

6.22.2.3 {deny | permit}

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.

The time-range parameter allows imposing time limitation on the IPv6 ACL rule as defined by the parameter time-range-name . If a time range with the specified name does not exist and the IPv6 ACL containing this ACL rule is applied to an interface or bound to a VLAN, then the ACL rule is applied immediately. If a time range with specified name exists and the IPv6 ACL containing this ACL rule is applied to an interface or bound to a VLAN, then the ACL rule is applied when the time-range with specified name becomes active. The ACL rule is removed when the time-range with specified name becomes inactive.

Syntax

{del-rule-id | deny | permit} {every | {{icmpv6 | ipv6 | tcp | udp | <number>} [log] [time-range time-range-name] [assign-queue <queue-id>] [{mirror | redirect} {<slot/port> | port-channel <portchannel-id>}] [rule-id]

Default Setting

None

Command Mode

IPv6-Access-List Config

6.22.2.4 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|out} [<1-4294967295>]
no ipv6 traffic-filter <name> [vlan <vlan-id>] {in|out} [<1-4294967295>]
```

in|out - The direction value is either in or out

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

6.23 CoS (Class of Service) Command

6.23.1 Show Commands

6.23.1.1 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> | port-channel <portchannel-id>}

< slot/port > - The interface number.

<portchannel-id> - The port-channel interface number. The range of the ID is 1 to 64.

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.

6.23.1.2 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.

6.23.1.3 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> | port-channel <portchannel-id>}
```

< slot/port > - The interface number.

<portchannel-id> - The port-channel interface number. The range of port-channel ID is 1 to 64.

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'.

6.23.1.4 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> | port-channel <portchannel-id>}

< slot/port > The interface number.

<portchannel-id> - The port-channel interface number. The range of port-channel ID is 1 to 64.

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.

6.23.2 Configuration Commands

6.23.2.1 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.

6.23.2.2 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

dot1p

Command Mode

Global Config.

Syntax

```
queue trust {dot1p | ip-dscp | untrusted }
no queue trust
```

no - This command sets the class of service trust mode to untrusted for all interfaces.

Default Setting

dot1p

Command Mode

Interface Config.

6.23.2.3 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 1 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.

6.23.2.4 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.

6.23.2.5 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 1.

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 1.

no - This command restores the default shaping rate value for all interfaces.

Default Setting

None

Command Mode

Global Config.

6.24 Auto-Voice over IP Commands

This section describes the commands you use to configure Auto-Voice over IP (VoIP) commands. The Auto-VoIP feature explicitly matches VoIP streams in Ethernet switches and provides them with a better class-of-service than ordinary traffic. When you enable the Auto-VoIP feature on an interface, the interface scans incoming traffic for the following call-control protocols:

- Session Initiation Protocol (SIP)
- H.323
- Skinny Client Control Protocol (SCCP)

When a call-control protocol is detected, the switch assigns the traffic in that session to the highest CoS queue, which is generally used for time-sensitive traffic.

6.24.1 Show Commands

6.24.1.1 show auto-voip interface

Use this command to display the VoIP Profile settings on the interface or interfaces of the switch.

Syntax

show auto-voip interface [{< slot/port > | port-channel <portchannel-id>}]

< slot/port > - The interface number.

<portchannel-id> - The port-channel interface number. The range of port-channel ID is 1 to 64.

Default Setting

None

Command Mode

Privileged EXEC

Display Message

AutoVoIP Mode: The Auto VoIP mode on the interface.

Traffic Class: The CoS Queue or Traffic Class to which all VoIP traffic is mapped to. This is not configurable and defaults to the highest CoS queue available in the system for data traffic.

6.24.2 Configuration Commands

6.24.2.1 auto-voip all

Use this command to enable VoIP Profile on the interfaces of the switch.

Syntax

```
auto-voip all
no auto-voip all
```

no - Use this command to disable VoIP Profile on the interfaces of the switch.

Default Setting

Disable

Command Mode

Global Config.

6.24.2.2 auto-voip

Use this command to enable VoIP Profile on an interface or range of interfaces.

Syntax

```
auto-voip
no auto-voip
```

no - Use this command to disable VoIP Profile on the interface.

Default Setting

Disable

Command Mode

Interface Config.

6.25 iSCSI Optimization Commands

This section describes commands you use to monitor iSCSI sessions and prioritize iSCSI packets. iSCSI Optimzation provides a means of giving traffic between iSCSI initiator and target systems special Quality of Service (QoS) treatment. This is accomplished by monitoring traffic to detect packets used by iSCSI stations to establish iSCSI sessions and connections. Data from these exchanges is used to create classification rules that assign the traffic between the stations to a configured traffic class. Packets in the flow are queued and scheduled for egress on the destination port based on these rules.

6.25.1 Show Commands

6.25.1.1 show iscsi

This command displays the iSCSI settings.

Syntax

```
show iscsi
```

Default Setting

None

Command Mode

Privileged EXEC

Display Message

```
Example : show iscsi
iSCSI enabled
iSCSI vpt is 5
Session aging time: 10 min
Maximum number of sessions is 192
-------------------------------------------------
iSCSI Targets and TCP Ports:
-------------------------------------------------
TCP Port       Target IP Address       Name
860                    -                        -
3260                   -                        -
```

6.25.1.2 show iscsi sessions

This command displays the iSCSI sessions.

Syntax

show iscsi sessions [detailed]

Default Setting

None

Command Mode

Privileged EXEC

Display Message

Example #1: show iscsi sessions

Session 0:

Target: iqn.2006-03.com.kernsafe:q97041406.ImageDisk0

Initiator: iqn.2003-06.com.starwindsoftware.starport:ap111111

ISID: 801234567890

Example #2: show iscsi sessions detailed

Session 0:

Target: iqn.2006-03.com.kernsafe:q97041406.ImageDisk0

Initiator: iqn.2003-06.com.starwindsoftware.starport:ap111111

Up Time: 00:00:11:00 (DD:HH:MM:SS)

Time for aging out: 598 secs

ISID: 801234567890

Initiator IP Address	Initiator TCP Port	Target IP Address	Target TCP Port
172.16.2.147	1090	172.16.2.151	3260
172.16.2.147	1092	172.16.2.151	3260

6.25.2 Configuration Commands

6.25.2.1 iscsi enable

This command globally enables iSCSI awareness.

Syntax

```
iscsi enable
no iscsi enable
```

no - This command disables iSCSI awareness. When you use the no iscsi enable command, iSCSI resources will be released.

Default Setting

Disable

Command Mode

Global Config.

6.25.2.2 iscsi cos

This command sets the quality of service profile that will be applied to iSCSI flows. iSCSI flows are assigned by default to the highest VPT/DSCP mapped to the highest queue not used for stack management. The user should also take care of configuring the relevant Class of Service parameters for the queue in order to complete the setting.

Setting the VPT/DSCP sets the QoS profile which determines the egress queue to which the frame is mapped. The switch default setting for egress queues scheduling is Weighted Round Robin (WRR).

You may complete the QoS setting by configuring the relevant ports to work in other scheduling and queue management modes via the Class of Service settings. Depending on the platform, these choices may include strict priority for the queue used for iSCSI traffic. The downside of strict priority is that, in certain circumstances (under heavy high priority traffic), other lower priority traffic may get starved. In WRR the queue to which the flow is assigned to can be set to get the required percentage.

Syntax

```
iscsi cos { dscp <dscp> [remark] | vpt <vpt> } no
iscsi cos
```

vpt/dscp - The VLAN Priority Tag or DSCP to assign iSCSI session packets.

remark - Mark the iSCSI frames with the configured VPT/DSCP when egressing the switch. no

- Use this command to disable VoIP Profile on the interface.

Default Setting

5 (vpt)

Command Mode

Global Config.

6.25.2.3 iscsi aging time

This command sets the aging time for iSCSI sessions. Behavior when changing aging time:

- When aging time is increased, current sessions will be timed out according to the new value.
- When aging time is decreased, any sessions that have been dormant for a time exceeding the new setting will be immediately deleted from the table. All other sessions will continue to be monitored against the new time out value.

Syntax

```
iscsi aging time <time>
no iscsi aging time
```

time - The number of minutes a session must be inactive prior to its removal. Range: 1-43,200.

no - Use the no form of the command to reset the aging time value to the default value.

Default Setting

10 minutes

Command Mode

Global Config.

6.25.2.4 iscsi target port

This command configures an iSCSI target port and, optionally, a target system's IP address and IQN name. When working with private iSCSI ports (not IANA-assigned ports 3260/860), it is recommended to specify the target IP address as well, so that the switch will only snoop frames with which the TCP destination port is one of the configured TCP ports, and the destination IP is the target's IP address. This way the CPU will not be falsely loaded by non-iSCSI flows (if by chance other applications also choose to use these un-reserved ports.

When a port is already defined and not bound to an IP address, and you want to bind it to an IP address, you should first remove it by using the no form of the command and then add it again, this time together with the relevant IP address.

Target names are only for display when using the show iscsi command. These names are not used to match with the iSCSI session information acquired by snooping.

A maximum of 16 TCP ports can be configured either bound to IP or not.

Syntax

```
iscsi target port tcp-port-1 [tcp-port-2...tcp-port-16] [address ip-address] [name targetname] no
iscsi target port tcp-port-1 [tcp-port-2...tcp-port-16] [address ip-address]
```

tcp-port-n - TCP port number or list of TCP port numbers on which the iSCSI target listens to requests. Up to 16 TCP ports can be defined in the system in one command or by using multiple commands.

ip-address - IP address of the iSCSI target. When the no form of this command is used, and the tcp port to be deleted is one bound to a specific IP address, the address field must be present.

Targetname - iSCSI name of the iSCSI target. The name can be statically configured; however, it can be obtained from iSNS or from sendTargets response. The initiator must present both its iSCSI Initiator Name and the iSCSI Target Name to which it wishes to connect in the first login request of a new session or connection.

no - Use the no form of the command to delete an iSCSI target port, address, and name.

Default Setting

iSCSI well-known ports 3260 and 860 are configured as default but can be removed as any other configured target.

Command Mode

Global Config.

6.26 Domain Name Server Relay Commands

6.26.1 Show Commands

6.26.1.1 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.

6.26.1.2 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.

Domain Relay Status: Enable or disable the IP Domain Naming System (DNS)-based host name-to-address relay function.

Default Domain Name: The default domain name that will be used for querying the IP address of a host.

DNS Client Source Interface: The interface to use as the source interface.

DNS Client Source IPv4 Address: The IPv4 address used for the DNS client to send packets.

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.

6.26.1.3 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.

6.26.2 Configuration Commands

6.26.2.1 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

6.26.2.2 clear hosts

This command clears the entire static host name-to-address mapping table.

Syntax

```
clear hosts
```

Default Setting

None

Command Mode

Privileged Exec

6.26.2.3 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

6.26.2.4 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

6.26.2.5 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

6.26.2.6 ip name-server source-interface

This command specifies the source address of dns client to use for name-to-address resolution.

Syntax

```
ip name-server source-interface {<slot/port> | loopback <loopback-id> | tunnel <tunnel-id> | vlan <vlan-id>}
no ip name-server source-interface
```

<slot/port> - Specifies the interface to use as the source interface.

<loopback-id> - Specifies the loopback interface to use as the source interface. The range of the loopback ID is 0 to 7.

<tunnel-id> - Specifies the tunnel interface to use as the source interface. The range of the tunnel ID is 0 to 7.

<vlan-id> - Specifies the VLAN interface to use as the source interface. The range of the VLAN ID is 1 to 4093.

<no> - Remove the corresponding Domain Name Server entry from the table.

Default Setting

None

Command Mode

Global Config

6.26.2.7 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

Enabled

Command Mode

Global Config

6.26.2.8 ip domain-lookup relay

This command enables the IP Domain Naming System (DNS)-based host name-to-address relay translation.

Syntax

```
ip domain-lookup relay
no ip domain-lookup realy
```

<no> - This command disables the IP Domain Naming System (DNS)-based host name-to-address relay translation.

Default Setting

Disabled

Command Mode

Global Config

6.26.2.9 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

6.26.2.10 clear dns

This command sets the DNS configuration to default value.

Syntax

```
clear dns
```

Default Setting

None

Command Mode

Privileged Exec

6.26.2.11 clear dns cache

This command clears all entries in the DNS cache table.

Syntax

```
clear dns cache
```

Default Setting

None

Command Mode

Privileged Exec

6.26.2.12 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

6.27 UDLD Commands

6.27.1 Show command

6.27.1.1 show udld

Show UDLD information in all interfaces or specific interface

Syntax

```
show udld {< slot/port>}
```

<slot/port> - The interface number.

Default Setting

None

Command Mode

Privileged Exec

Display Message

Port enable operational state: Specifies the Port Enable Operational State of the selected port.

Current bidirectional state: Specifies the Bidirectional State of the selected port.

Current operational state: Specifies the runtime Operational State of the selected port. This section will be hidden if the port doesn't enable udld.

Message interval: Specifies the runtime Message Interval of the selected port. This section will be hidden if the port doesn't enable udld.

Timeout interval: Specifies the runtime Timeout Interval of the selected port. This section will be hidden if the port doesn't enable udld.

Remote Entry: Display all the remote entry information if received.

Expiration time: Specifies the runtime Expiration Time of the remote entry.

Device ID: Specifies the Device Id associated with the remote system.

Device Name: Specifies the Device Name associated with the remote system.

Port ID: Specifies the Port Id associated with the remote system.

Neighbor echo device: Specifies the Device Id included in Echo TLV associated with the remote system.

Neighbor echo port: Specifies the port Id included in Echo TLV associated with the remote system.

Message interval: Specifies the Message Interval associated with the remote system.

Timeout interval: Specifies the Message Interval associated with the remote system.

CDP Device Name: Specifies the CDP Device Name associated with the remote system.

6.27.2 Configuration Commands

6.27.2.1 udld aggressive

Enable/Disable UDLD protocol in aggressive mode on fiber ports except where locally configured

Syntax
udld aggressive no udld aggressive

Default Setting

Disabled

Command Mode

Global Config.

6.27.2.2 udld enable

Enable/Disable UDLD protocol on fiber ports except where locally configured

Syntax
udld enable no udld enable

Default Setting

Disabled

Command Mode

Global Config.

6.27.2.3 udld message time

Set UDLD message time period in <7-90> range. The message time is to use between sending of messages in steady. Default value of UDLD message time is 15.

Syntax

udld message time <7-90>

no udld message time

Default Setting

15 sec

Command Mode

Global Config.

6.27.2.4 udld port

Enable/Disable UDLD protocol on the interface.

Syntax

udld port

no udld port

Default Setting

Disable

Command Mode

Interface Config.

6.27.2.5 udld port aggressive

Enable/Disable UDLD protocol in aggressive mode on the interface

Syntax

udld port aggressive

no udld port aggressive

Default Setting

Disable

Command Mode

Interface Config.

6.28 Multi Chassis Link Aggregation Commands

6.28.1 Show Commands

6.28.1.1 show mlag

This command displays detailed information about the Multi-chassis Link Aggregation (MLAG) configured on the switch.

Syntax
show mlag <mlag-number>

Default Setting

None

Command Mode

Privileged Exec

Display Message

Admin Mode: Displays the administrative mode for MLAG functionality on the switch.

Domain Id: Represents the domain identify number of MLAG peer devices.

MLAG Status: Represents the operation status of MLAG.

Configuration Consistency Status: Represents the configuration consistency status of MLAG peer devices.

MLAG Role: Represents the role of MLAG peer device.

MLAG System-Mac: Represents the operation system MAC address of MLAG peer devices.

MLAG Local Syatem-Mac: Represents the statically defined system MAC address of MLAG peer devices.

Number of MLAG Configured: Represents the number of MLAG port-channel member.

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

Status: Represents the link status of MLAG peer link port or port-channel member.

ID: Represents the identify number of MLAG port-channel member.

Consistency: Represents the configuration consistency status of MLAG port-channel member.

Active Vlan: Represents the VLAN which MLAG peer link port or port-channel member belong to.

6.28.1.2 show mlag consistency-parameters

This command displays the consistency of parameters that must be compatible across the Multi-chassis Link Aggregation (MLAG).

Syntax

show mlag consistency-parameters <mlag-number>

Default Setting

None

Command Mode

Privileged Exec

Display Message

Spanning Tree Admin Mode: Indicates whether administrative mode is enabled or disabled of MLAG peer devices.

Spanning Tree Version: Represents the version of 802.1 currently supported (IEEE 802.1s, IEEE 802.1w, or IEEE 802.1d) based upon the Force Protocol Version parameter of MLAG peer devices.

Spanning Tree Configuration Name: Represents the configured name of MLAG peer devices.

Spanning Tree BPDU Guard Mode: Indicates whether BPDU guard mode is enabled or disabled of MLAG peer devices.

Spanning Tree BPDU Filter Mode: Indicates whether BPDU filter mode is enabled or disabled of MLAG peer devices.

Spanning Tree Peer-Link Port Mode: Indicates whether port mode on peer link port is enabled or disabled of MLAG peer devices.

Spanning Tree Peer-Link Root Guard: Indicates whether root guard mode on peer link port is enabled or disabled of MLAG peer devices.

Spanning Tree Peer-Link Loop Guard: Indicates whether loop guard mode on peer link port is enabled or disabled of MLAG peer devices.

Spanning Tree Peer-Link BPDU Guard: Indicates whether BPDU guard mode on peer link port is enabled or disabled of MLAG peer devices.

Spanning Tree Peer-Link BPDU Filter Mode: Indicates whether BPDU filter mode on peer link port is enabled or disabled of MLAG peer devices.

Spanning Tree Peer-Link BPDU Flood Mode: Indicates whether BPDU flood mode on peer link port is enabled or disabled of MLAG peer devices.

VTP Admin Status: Indicates whether administrative mode is enabled or disabled of MLAG peer devices.

VTP Operating Mode: Displays the VTP operating mode of MLAG peer devices, which can be server, client, or transparent.

VTP Pruning Mode: Displays whether pruning is enabled or disabled of MLAG peer devices.

VTP V2 Mode: Displays if VTP version 2 mode is enabled of MLAG peer devices.

VTP Domain Name: Displays the name that identifies the administrative domain of MLAG peer devices.

VTP Password: Displays the VTP domain password of MLAG peer devices.

IGMP Snooping Admin Mode: Indicates whether or not IGMP Snooping is active on the switch of MLAG peer devices.

MLD Snooping Admin Mode: Indicates whether or not MLD Snooping is active on the switch of MLAG peer devices.

GMRP Admin Mode: This displays the administrative mode of GARP VLAN Registration Protocol (GVRP) for the system of MLAG peer devices..

GVRP Admin Mode: This displays the administrative mode of GARP Multicast Registration Protocol (GMRP) for the system of MLAG peer devices..

When you specify a value for <mlag-number>, the following information appears.

Spanning Tree Port Mode: Indicates whether port mode on MLAG member is enabled or disabled of MLAG peer devices.

Spanning Tree Root Guard: Indicates whether root guard mode on MLAG member is enabled or disabled of MLAG peer devices.

Spanning Tree Loop Guard: Indicates whether loop guard mode on MLAG member is enabled or disabled of MLAG peer devices.

Spanning Tree BPDU Guard: Indicates whether BPDU guard mode on MLAG member is enabled or disabled of MLAG peer devices.

Spanning Tree BPDU Filter Mode: Indicates whether BPDU filter mode on MLAG member is enabled or disabled of MLAG peer devices.

Spanning Tree BPDU Flood Mode: Indicates whether BPDU flood mode on MLAG member is enabled or disabled of MLAG peer devices.

VTP Port Trunk Mode: Indicates whether trunk mode is enabled or disabled on MLAG member of MLAG peer devices.

IGMP Snooping Mode: Indicates whether or not IGMP Snooping is active on MLAG member of MLAG peer devices.

MLD Snooping Mode: Indicates whether or not MLD Snooping is active on MLAG member of MLAG peer devices.

GMRP Mode: This displays the administrative mode of GARP VLAN Registration Protocol (GVRP) for MLAG member of MLAG peer devices..

GVRP Mode: This displays the administrative mode of GARP Multicast Registration Protocol (GMRP) for MLAG member of MLAG peer devices..

6.28.2 Configuration Commands

6.28.2.1 mlag

This command enables a Multi-chassis Link Aggregation (MLAG), which allows links that are physically connected to two different devices to appear as a single port channel to a third device.

To disable MLAG on the switch, use the no form of this command.

Syntax
mlag no mlag

Default Setting

Disabled

Command Mode

Global Config

6.28.2.2 mlag domain

This command creates a Multi-chassis Link Aggregation (MLAG) domain and assign a domain ID. The range is from 1 and 1000.

To revert to the default mlag configuration, use the no form of this command

Syntax
mlag domain <domain-id> no mlag domain

<domain-id> - Domain identify number of MLAG (Range: 1 - 1000).

Default Setting

1

Command Mode

Global Config

6.28.2.3 mlag system-mac

This command manually configures the Multi-chassis Link Aggregation (MLAG) domain MAC address. To restore the default system MAC address, use the no form of this command.

Syntax

```
mlag system-mac <mac-address>
no mlag system-mac
```

<mac-address> - Syatem MAC adress.

Default Setting

None

Command Mode

Global Config

6.28.2.4 mlag peer-link

This command creates a Multi-chassis Link Aggregation (MLAG) peer link by designating the port channel that you want on each device as the peer link for the specified MLAG domain.

To remove the peer link, use the no form of this command.

Syntax

```
mlag peer-link
no mlag peer-link
```

Default Setting

Disabled

Command Mode

Interface Config

6.28.2.5 mlag <mlag-number>

This command moves other port channels into a Multi-chassis Link Aggregation (MLAG) to connect to the downstream device. The range is from 1 and 4096.

To remove the port channels from the mlag, use the no form of this command.

Syntax

```
mlag    <mlag-number>
no mlag
```

<mlag-number> - Domain identify number of MLAG port-channel member (Range: 1 - 4096).

Default Setting

Disabled

Command Mode

Interface Config

7 Routing Commands

7.1 Address Resolution Protocol (ARP) Commands

7.1.1 Show Commands

7.1.1.1 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).

7.1.1.2 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.

7.1.1.3 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.

7.1.2 Configuration Commands

7.1.2.1 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

7.1.2.2 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

7.1.2.3 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

7.1.2.4 arp cachesize

This command configures the maximum number of entries in the ARP cache.

Syntax

```
arp cachesize <767-4096>
no arp cachesize
```

<767-3968> - The range of cache size is 767 to 4096.

no - This command configures the default ARP cache size.

Default Setting

The default cache size is 4096.

Command Mode

Global Config

7.1.2.5 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

7.1.2.6 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

7.1.2.7 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

7.1.2.8 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

7.1.2.9 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

7.1.2.10 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> | vlan <vlan-id>}]
```

Default Setting

None

Command Mode

Privileged Exec

7.2 IP Routing Commands

7.2.1 Show Commands

7.2.1.1 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.

Maximum Next Hops: The maximum number of hops supported by this switch.

Maximum Routes: The maximum number of routes the packet can travel.

ICMP Rate Limit Interval: Shows how often the token bucket is initialized with burst-size tokens. Burst-interval is from 0 to 2147483647 milliseconds. The default burst-interval is 1000 msec.

ICMP Rate Limit Burst Size: Shows the number of ICMPv4 error messages that can be sent during one burst-interval. The range is from 1 to 200 messages. The default value is 100 messages.

ICMP Echo Replies: Shows whether ICMP Echo Replies are enabled or disabled.

ICMP Redirects: Shows whether ICMP Redirects are enabled or disabled.

7.2.1.2 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

Routing Interface Status: Determine the operational status of IPv4 routing Interface. The possible values are Up or Down.

Primary IP Address: The primary IP address and subnet masks for the interface. This value appears only if you configure it.

Method: Shows whether the IP address was configured manually or acquired from a DHCP server.

Secondary IP Address: One or more secondary IP addresses and subnet masks for the interface. This value appears only if you configure it.

Helper IP Address: The helper IP addresses configured by the command “ip helper-address (Interface Config)”.

Routing Mode: The administrative mode of router interface participation. The possible values are enable or disable. This value is configurable.

Administrative Mode: The administrative mode of the specified interface. The possible values of this field are enable or disable. This value is configurable.

Forward Net Directed Broadcasts: Displays whether forwarding of network-directed broadcasts is enabled or disabled. This value is configurable.

Proxy ARP: Displays whether Proxy ARP is enabled or disabled on the system.

Local Proxy ARP: Displays whether Local Proxy ARP is enabled or disabled on the interface.

Active State Displays whether the interface is active or inactive. An interface is considered active if its link is up and it is in forwarding state.

Link Speed Data Rate: An integer representing the physical link data rate of the specified interface. This is measured in Megabits per second (Mbps).

MAC Address: The burned in physical address of the specified interface. The format is 6 two-digit hexadecimal numbers that are separated by colons.

Encapsulation Type: The encapsulation type for the specified interface. The types are: Ethernet or SNAP.

IP MTU: The maximum transmission unit (MTU) size of a frame, in bytes.

Bandwidth: Shows the bandwidth of the interface.

Destination Unreachables: Displays whether ICMP Destination Unreachables may be sent (enabled or disabled).

ICMP Redirects: Displays whether ICMP Redirects may be sent (enabled or disabled).

7.2.1.3 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 or VLAN routing interface.

State: Indicate the operational state of the routing interface.

IP Address: The IP address of the routing interface. IP

Mask: The IP mask of the routing interface.

Method: Is the way to get the IP Address. The possible value is “Manual”, “DHCP” or “None”.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.

7.2.1.4 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

7.2.1.5 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.

7.2.1.6 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.

Metric: Specifies the metric for this route entry.

Pref: The preference value that is used for this route entry.

7.2.1.7 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.

7.2.1.8 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.

7.2.1.9 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.

7.2.1.10 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.

7.2.1.11 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.

Reject Routes: Total number of reject routes installed by all protocols.

Total Routes: Total number of routes in the routing table.

7.2.1.12 show ip route preferences

This command displays detailed information about the route preferences. Route preferences are used in determining the best route. Lower router preference values are preferred over higher router preference values.

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 External: The OSPF External route preference value.

RIP: This field displays the RIP route preference value.

Configured Default Gateway: The route preference value of the statically-configured default gateway

DHCP Default Gateway: The route preference value of the default gateway learned from the DHCP server.

7.2.1.13 show ip stats

This command displays IP statistical information. Refer to RFC 1213 for more information about the fields that are displayed.

Syntax

```
show ip stats
```

Default Setting

None

Command Mode

Privileged Exec

7.2.2 Configuration Commands

7.2.2.1 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

7.2.2.2 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

7.2.2.3 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

7.2.2.4 ip address dhcp

This command enables the DHCPv4 client on an in-band interface so that it can acquire network information, such as the IP address, subnet mask, and default gateway, from a network DHCP server. When DHCP is enabled on the interface, the system automatically deletes all manually configured IPv4 addresses on the interface.

Syntax

```
ip address dhcp [restart]
no ip address <ipaddr> <subnet-mask> [secondary]
```

[secondary] - To restart IP Address given by DHCP server.

no - This command releases a leased address and disables DHCPv4 on an interface.

Default Setting

Disabled

Command Mode

Interface Config

7.2.2.5 ip route

This command configures a static route.

Syntax

```
ip route <networkaddr> <subnetmask> [ {<nexthopip>|Null0} [<1-255 >] ]
no ip route <networkaddr> <subnetmask> [ { <nexthopip> | <1-255 > | Null0 } ]
```

<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.

Null0 - Null interface.

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

7.2.2.6 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

7.2.2.7 ip route distance

This command sets the default distance (preference) for static routes. Lower route distance values are preferred when determining the best route. The ip route and ip route default commands allow you to optionally set the distance (preference) of an individual static route. The default distance is used when no distance is specified in these commands. Changing the default distance does not update the distance of existing static routes, even if they were assigned the original default distance. The new default distance will only be applied to static routes created after invoking the ip route distance command.

Syntax

```
ip route distance <1-255>
```

<1-255> - Default the Distance value of static routes. The range is 1 to 255.

Default Setting

The default preference value is 1.

Command Mode

Global Config

7.2.2.8 ip mtu

This command sets the IP Maximum Transmission Unit (MTU) on a routing interface or range of interfaces. The IP MTU is the size of the largest IP packet that can be transmitted on the interface without fragmentation. Forwarded packets are dropped if they exceed the IP MTU of the outgoing interface.

Packets originated on the router, such as OSPF packets, may be fragmented by the IP stack.

OSPF advertises the IP MTU in the Database Description packets it sends to its neighbors during database exchange. If two OSPF neighbors advertise different IP MTUs, they will not form an adjacency. (unless OSPF has been instructed to ignore differences in IP MTU with the ip ospf mtu-ignore command.)

Syntax
ip mtu <68-12270> no ip mtu <68-12270>

<68-12270> - The IP MTU on a routing interface. The range is 68 to 12270. no

- Reset the ip mtu to the default value.

Default Setting

The default value is 1500.

Command Mode

Interface Config

7.2.2.9 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.

7.3 Open Shortest Path First (OSPF) Commands

7.3.1 Show Commands

7.3.1.1 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.

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.

Default Passive Setting: Shows whether the interfaces are passive by default.

Maximum Paths: The maximum number of paths that OSPF can report for a given destination.

Default Metric: Default value for redistributed routes.

Network Area: Shows area for the Network Area setting.

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.

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.

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.

AS Scope LSA Flood List Length: Length of global flood list for LSAs with AS scope.

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.NSF Helper Support: Configure graceful restart.

NSF Helper Strict LSA Checking: Terminate graceful restart helper on topology change.

7.3.1.2 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.

7.3.1.3 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.

Flood List Length: Length of the area's LSA flood list.

Import Summary LSAs: Shows whether to import summary LSAs.

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.

No-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.

7.3.1.4 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.

7.3.1.5 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

show 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

Ls 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.

Chksm: 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.

7.3.1.6 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.

Opaque Link: Number of opaque link LSAs in the database.

Opaque Area: Number of opaque area LSAs in the database.

Type-5 Ext: Total number of Type-5 external LSAs in the database.

Self-Originated Type-5 Ext: Total number of self originated Type-5 external 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.

7.3.1.7 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> | vlan <vlan-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.

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.

7.3.1.8 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.

7.3.1.9 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> | loopback <loopback-id> | vlan <vlan-id>}

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.

7.3.1.10 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> | vlan <vlan-id>}] [<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.

7.3.1.11 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.

7.3.1.12 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

7.3.1.13 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.

7.3.1.14 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.

7.3.1.15 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.

7.3.2 Configuration Commands

7.3.2.1 router ospf

Use this command to enter Router OSPF mode.

Syntax
router ospf

Default Setting

None

Command Mode

Global Config

7.3.2.2 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

7.3.2.3 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

7.3.2.4 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

7.3.2.5 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

7.3.2.6 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

7.3.2.7 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

7.3.2.8 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

7.3.2.9 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

7.3.2.10 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

7.3.2.11 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

7.3.2.12 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

7.3.2.13 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

7.3.2.14 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

7.3.2.15 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

7.3.2.16 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

7.3.2.17 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

7.3.2.18 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

7.3.2.19 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

7.3.2.20 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

7.3.2.21 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

7.3.2.22 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

7.3.2.23 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

7.3.2.24 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

7.3.2.25 clear ip ospf

Use this command to disable and re-enable OSPF.

Syntax

```
clear ip ospf
```

Default Setting

None

Command Mode

Privileged Exec

7.3.2.26 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

7.3.2.27 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

7.3.2.28 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

7.3.2.29 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 [ipaddr].

Syntax

clear ip ospf neighbor [interface {{<slot/port> | vlan <vlan-id>} [ipAddr] | <ipaddr>}]

Default Setting

None

Command Mode

Privileged Exec

7.3.2.30 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

7.3.2.31 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

7.3.2.32 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

7.3.2.33 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

7.3.2.34 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

7.3.2.35 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

7.3.2.36 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

7.3.2.37 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

7.3.2.38 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

7.3.2.39 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

7.3.2.40 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

7.3.2.41 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

7.3.2.42 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

7.3.2.43 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

7.3.2.44 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

7.3.2.45 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

7.3.2.46 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

7.3.2.47 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

7.3.2.48 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

7.3.2.49 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

7.3.2.50 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> | vlan <vlan-id>}
no passive-interface {<slot/port> | vlan <vlan-id>}
```

Default Setting

Disabled

Command Mode

Router OSPF Config Mode

7.3.2.51 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

7.4 BOOTP/DHCP Relay Commands

7.4.1 Show Commands

7.4.1.1 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.

7.4.2 Configuration Commands

7.4.2.1 bootpdhcprelay cidoptmode

This command enables the circuit ID option mode for BootP/DHCP Relay on the system.

Syntax

```
bootpdhcprelay cidoptmode
no bootpdhcprelay cidoptmode
```

no - This command is used to disable the circuit ID option mode for BootP/DHCP Relay on the system.

Default Setting

Disabled

Command Mode

Global Config

7.4.2.2 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

7.4.2.3 bootpdhcprelay maxhopcount

This command configures the maximum allowable relay agent hops for BootP/DHCP Relay on the system.

Syntax

```
bootpdhcprelay maxhopcount <hops>
no bootpdhcprelay maxhopcount
```

<hops> - 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

7.4.2.4 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 <minwaittime>
no bootpdhcprelay minwaittime
```

<minwaittime> - 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

7.4.2.5 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

7.5 IP Helper Commands

7.5.1 Show Commands

7.5.1.1 show ip helper-address

Use this command to display the IP helper address configuration.

Syntax

show ip helper-address

Default Setting

None

Command Mode

Privileged Exec

User Exec

Display Message

Interface: The relay configuration is applied to packets that arrive on this interface. This field is set to ‘any’ for global IP helper entries.

UDP Port: The relay configuration is applied to packets whose destination UDP port is this port.

Discard: Indicate discard the UDP packets or not.

Hit Count: The number of times the IP helper entry has been used to relay or discard a packet.

Server Address: The IPv4 address of the server to which packets are relayed.

7.5.1.2 show ip helper statistics

Use this command to display the number of UDP packets processed and relayed.

Syntax
show ip helper statistics

Default Setting

None

Command Mode

Privileged Exec

User Exec

Display Message

DHCP client messages received: The number of valid messages received form a DHCP client

DHCP client messages relayed: The number of DHCP client messages relayed to a server. DHCP server messages received The number of DHCP responses received from the server. DHCP server messages relayed The number of DHCP server messages relayed to a client. UDP client messages received The number of valid UDP messages received.

UDP client messages relayed The number of valid UDP messages relayed

DHCP messages hop count exceeded max The number of DHCP client messages received whose hop count is larger than the maximum allowed.

DHCP messages with secs field below min The number of DHCP client messages received whose Second field is less than the minimum value.

DHCP message with giaddr set to local address The number of DHCP client messages received whose gateway address, giaddr, is already set to an IP address configured on one of the relay agent's own IP address.

Packets with expired TTL The number of packets received with TTL of 0 or 1 that otherwise have been relayed.

Packets that matched a discard entry The number of packets ignored by the relay agent because they match a discard entry.

7.5.2 Configuration Commands

7.5.2.1 ip helper-address

Use this command to configure the relay of certain UDP broadcast packets received on a specific interface or range of interfaces. This command can be invoked multiple times on a routing interface, either to specify multiple server addresses for a given port number or to specify multiple port numbers handled by a specific server.

Syntax

```
ip helper-address <ipaddr> [ <udp-port> | dhcp | domain | isakmp | mobile-ip | nameserver |
netbios-dgm | netbios-ns | ntp | pim-auto-rp | rip | tacacs | tftp | time ]
no ip helper-address <ipaddr> [ <udp-port> | dhcp | domain | isakmp | mobile-ip | nameserver |
netbios-dgm | netbios-ns | ntp | pim-auto-rp | rip | tacacs | tftp | time ]
```

no - This command is used to delete the address.

Default Setting

None

Command Mode

Interface Config

7.5.2.2 ip helper-address discard

Use this command to configure the discard of certain UDP broadcast packets received on a specific interface or range of interfaces. This command can be invoked multiple times on a routing interface for a given port number or to specify multiple port numbers handled by a specific server.

Syntax

```
ip helper-address discard { <udp-port> | dhcp | domain | isakmp | mobile-ip | nameserver | netbios-dgm |
netbios-ns | ntp | pim-auto-rp | rip | tacacs | tftp | time }
no ip helper-address discard { <udp-port> | dhcp | domain | isakmp | mobile-ip | nameserver |
netbios-dgm | netbios-ns | ntp | pim-auto-rp | rip | tacacs | tftp | time }
```

no - This command is used to delete the address.

Default Setting

None

Command Mode

Interface Config

7.5.2.3 ip helper-address

Use this command to configure the relay of certain UDP broadcast packets received on any interface. If the interface that receives a UDP packet has been configured with an address, this global address value will be ignored. This command can be invoked multiple times, either to specify multiple server addresses for a given UDP port number or to specify multiple UDP port numbers handled by a specific server.

Syntax

```
ip helper-address <ipaddr> { <udp-port> | dhcp | domain | isakmp | mobile-ip | nameserver |
netbios-dgm | netbios-ns | ntp | pim-auto-rp | rip | tacacs | tftp | time }
no ip helper-address <ipaddr> { <udp-port> | dhcp | domain | isakmp | mobile-ip | nameserver |
netbios-dgm | netbios-ns | ntp | pim-auto-rp | rip | tacacs | tftp | time }
```

no - This command is used to delete the address.

Default Setting

None

Command Mode

Global Config

7.5.2.4 ip helper enable

This command enable the relay of UDP packets.

Syntax

```
ip helper enable
no ip helper enable
```

no - disable the relay of UDP packets.

Default Setting

Disabled.

Command Mode

Global Config

7.5.2.5 clear ip helper statistics

This command is used this command to clear the information of UDP packets processed and relayed by IP helper.

Syntax
clear ip helper statistics

Default Setting

None

Command Mode

Privileged Exec

User Exec

7.6 Routing Information Protocol (RIP) Commands

7.6.1 Show Commands

7.6.1.1 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.

7.6.1.2 show ip rip interface

This command displays information related to a particular RIP interface.

Syntax

show ip rip interface {<slot/port> | loopback <loopback-id> | vlan <vlan-id>}

< 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.

7.6.1.3 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).

7.6.2 Configuration Commands

7.6.2.1 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

7.6.2.2 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

7.6.2.3 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

7.6.2.4 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

7.6.2.5 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

7.6.2.6 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

7.6.2.7 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

7.6.2.8 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

7.6.2.9 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

7.6.2.10 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

7.6.2.11 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

7.6.2.12 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

7.6.2.13 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

7.7 Router Discovery Protocol Commands

7.7.1 Show Commands

7.7.1.1 show ip irdp

This commands displays the router discovery information for all interfaces, or a specified interface.

Syntax

show ip irdp [{<slot/port> | vlan <vlan-id>}]

<slot/port> - Show router discovery information for the specified interface. no

parameter - 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.

7.7.2 Configuration Commands

7.7.2.1 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

7.7.2.2 ip irdp address

This command configures the address to be used to advertise the router for the interface.

Syntax

```
ip irdp address <address>
no ip irdp address
```

<address> - The address used is 224.0.0.1 or 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

7.7.2.3 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

7.7.2.4 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

7.7.2.5 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

7.7.2.6 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

7.8 VLAN Routing Commands

7.8.1 Configuration Commands

7.8.1.1 vlan routing

This command creates a VLAN routing interface.

Syntax

```
interface vlan <vlan-id>
no interface vlan <vlan-id>
```

<vlan-id> - The VLAN ID used for this interface. The range of VLAN ID is 1 to 4093.

no - Delete a VLAN routing interface.

Default Setting

None

Command Mode

Global Config

7.9 Virtual Router Redundancy Protocol (VRRP) Commands

7.9.1 Show Commands

7.9.1.1 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.

7.9.1.2 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.

7.9.1.3 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> | vlan <vlan-id>} [<vrid>]

<slot/port> - Valid slot and port number separated by forward slashes.

<vrid> - Virtual router ID.

<vlan-id> - VLAN ID. The range of VLAN ID is 1 to 4093.

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.

Configured Priority: The priority configured through the ip vrrp vrid priority 1-254 command.

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.

Accept Mode: When enabled, the VRRP Master can accept ping packets sent to one of the virtual router's IP addresses.

State: Represents the state (Master/backup) of the specific virtual router

7.9.1.4 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> | vlan <vlan-id>} [<vrid>]

<slot/port> - Valid slot and port number separated by forward slashes.

<vrid> - Virtual router ID.

<vlan-id> - VLAN ID. The range of VLAN ID is 1 to 4093.

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.

7.9.2 Configuration Commands

7.9.2.1 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

7.9.2.2 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

7.9.2.3 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

7.9.2.4 ip vrrp accept-mode

Use this command to allow the VRRP Master to accept ping packets sent to one of the virtual router's IP addresses.

Syntax

```
ip vrrp <1-255> accept-mode
no ip vrrp <1-255> accept-mode
```

<1-255> - The range of virtual router ID is 1 to 255.

<no> - Use this command to prevent the VRRP Master from accepting ping packets sent to one of the virtual router's IP addresses.

Default Setting

Disabled

Command Mode

Interface Config

7.9.2.5 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

7.9.2.6 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

7.9.2.7 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

7.9.2.8 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

7.9.2.9 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> | vlan <vlan-id>} [decrement <1-254>] no
ip vrrp <1-255> track interface {<slot/port> | vlan <vlan-id>} [decrement]
```

<1-255> - The range of virtual router ID is 1 to 255.

< 1-254 > - The range of decrement is 1 to 254.

<vlan-id> - VLAN ID. The range of VLAN ID is 1 to 4093.

<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

7.9.2.10 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

8 IP Multicast Commands

8.1 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.

8.1.1 Show Commands

8.1.1.1 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.

8.1.1.2 show ip dvmrp interface

This command displays the interface information for DVMRP on the specified interface.

Syntax

show ip dvmrp interface {<slot/port> | vlan <vlan-id>}

<slot/port> - Valid slot and port number separated by forward slashes.

<vlan-id> - VLAN ID. The range of VLAN ID is 1 to 4093.

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.

8.1.1.3 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.

8.1.1.4 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.

8.1.1.5 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.

8.1.1.6 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.

8.1.2 Configuration Commands

8.1.2.1 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

8.1.2.2 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

8.2 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.

8.2.1 Show Commands

8.2.1.1 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.

8.2.1.2 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> | vlan <vlan-id>} [detail]

<slot/port> - Valid slot and port number separated by forward slashes.

<vlan-id> - VLAN ID. The range of VLAN ID is 1 to 4093.

[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.

8.2.1.3 show ip igmp interface

This command displays the IGMP information for the interface.

Syntax

show ip igmp interface {<slot/port> | vlan <vlan-id>}

<slot/port> - Valid slot and port number separated by forward slashes.

<vlan-id> - VLAN ID. The range of VLAN ID is 1 to 4093.

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.

8.2.1.4 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.

8.2.1.5 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> | vlan <vlan-id>}

<slot/port> - Valid slot and port number separated by forward slashes.

<vlan-id> - VLAN ID. The range of VLAN ID is 1 to 4093.

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.

8.2.2 Configuration Commands

8.2.2.1 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

8.2.2.2 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

8.2.2.3 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

8.2.2.4 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

8.2.2.5 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

8.2.2.6 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

8.2.2.7 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

8.2.2.8 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

8.2.2.9 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

8.3 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.

8.3.1 Show Commands

8.3.1.1 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> | vlan <vlan-id> | <group-address>}

<slot/port> - Valid slot and port number separated by forward slashes.

<vlan-id> - VLAN ID. The range of VLAN ID is 1 to 4093.

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

The following table is displayed to indicate all the sources associated with this group.

Source Address: The IP address of the source.

Uptime: Time elapsed in hours, minutes, and seconds since the source has been known.

Expiry Time: Time left in hours, minutes, and seconds before the entry is removed.

8.3.1.2 show ipv6 mld interface

Use this command to display MLD-related information for the interface.

Syntax

show ipv6 mld interface [{<slot/port> | vlan <vlan-id>}]

<slot/port> - Valid slot and port number separated by forward slashes.

<vlan-id> - VLAN ID. The range of VLAN ID is 1 to 4093.

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 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.

8.3.1.3 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.

8.3.2 Configuration Commands

8.3.2.1 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

8.3.2.2 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 <0-8387584>
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

10000 milliseconds

Command Mode

Interface Config

8.3.2.3 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 <0-65535>
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

8.3.2.4 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

8.3.2.5 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

8.3.2.6 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> vlan <vlan-id>}]
```

<slot/port> - Specify the interface.

<vlan-id> - Specifies the VLAN interface. The range of the VLAN ID is 1 to 4093.

Default Setting

None

Command Mode

Privilege Exec

8.3.2.7 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

8.3.2.8 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

8.4 Multicast Commands

8.4.1 Show Commands

8.4.1.1 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.

IPv4 Protocol State: This field indicates the current state of the IPv4 multicast protocol. Possible values are Operational or Non-Operational.

IPv6 Protocol State: This field indicates the current state of the IPv6 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.

IPv4 Protocol: This field displays the multicast protocol running on the router. Possible values are PIMDM, PIMSM, or DVMRP.

IPv6 Protocol: This field displays the multicast protocol running on the router. Possible values are PIMDM or PIMSM,

Multicast Forwarding Cache Entry Count: This field displays the number of entries in the multicast table.

8.4.1.2 show ip mcast boundary

This command displays all the configured administrative scoped multicast boundaries.

Syntax

show ip mcast boundary [{<slot/port> | vlan <vlan-id>}]

<slot/port > - Interface number.

<vlan-id> - VLAN ID. The range of VLAN ID is 1 to 4093. no

parameter - 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.

8.4.1.3 show ip mcast interface

This command displays the multicast information for the specified interface.

Syntax

```
show ip mcast interface {<slot/port> | vlan <vlan-id>}
```

<slot/port > - Interface number.

<vlan-id> - VLAN ID. The range of VLAN ID is 1 to 4093.

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.

8.4.1.4 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.

8.4.2 Configuration Commands

8.4.2.1 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

8.4.2.2 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

8.4.2.3 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

8.5 IPv4 Protocol Independent Multicast (PIM) Commands

8.5.1 Show Commands

8.5.1.1 show ip pim

This command displays the system-wide information for PIM-DM or PIM-SM.

Syntax
show ip pim

Default Setting

None

Command Mode

Privileged Exec, User Exec

Display Message

PIM Mode: Indicates whether the PIM mode is dense (PIM-DM) or sparse (PIM-SM)

Data Threshold: Rate (in kbps) of SPT Threshold

Register Rate-limit: Rate (in kbps) of the Register Threshold

Interface: slot/port

Interface Mode: Indicates whether PIM is enabled or disabled on this interface

Operational Status: The current state of PIM on this interface: Operational or Non-Operational.

8.5.1.2 show ip pim bsr-router

This command displays the bootstrap router (BSR) information.

Syntax

show ip pim bsr-router {candidate | elected}

Default Setting

None

Command Mode

Privileged Exec, User Exec

Display Message

BSR Address: IP address of the BSR

BSR Priority: Priority as configured in the „ip pim bsr-candidate“ command

BSR 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 pim bsrcandidate command

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

8.5.1.3 show ip pim interface

This command displays the interface information for PIM on the specified interface. If no interface is specified, the command displays the status parameters for all PIM-enabled interfaces.

Syntax

```
show ip pim interface [{<slot/port> | vlan <vlan-id>}]
```

<slot/port> - Interface number.

<vlan-id> - VLAN ID. The range of VLAN ID is 1 to 4093.

Default Setting

None

Command Mode

Privileged Exec, User Exec

Display Message

Interface: slot/port

Mode: Indicates whether the PIM mode enabled on the interface is dense or sparse

Hello Interval: The frequency at which PIM hello messages are transmitted on this interface. By default, the value is 30 seconds

Join Prune Interval: The join/prune interval for the PIM router. The interval is in seconds

DR Priority: The priority of the Designated Router configured on the interface. This field is not applicable if the interface mode is Dense

BSR Border: Identifies whether this interface is configured as a bootstrap router border interface

Neighbor Count: The number of PIM neighbors learned on this interface. This is a dynamic value and is shown only when a PIM interface is operational

Designated Router: The IP address of the elected Designated Router for this interface. This is a dynamic value and will only be shown when a PIM interface is operational. This field is not applicable if the interface mode is Dense

8.5.1.4 show ip pim neighbor

This command displays PIM neighbors discovered by PIMv2 Hello messages. If the interface number is not specified, this command displays the neighbors discovered on all the PIM enabled interfaces.

Syntax

```
show ip pim neighbor [{<slot/port> | vlan <vlan-id>}]
```

<slot/port > - Interface number.

<vlan-id> - VLAN ID. The range of VLAN ID is 1 to 4093.

Default Setting

None

Command Mode

Privileged Exec, User Exec

Display Message

Neighbor Address: The IP address of the neighbor on an interface

Interface: slot/port

Up Time: The time since this neighbor has become active on this interface

Expiry Time: The expiry time of the neighbor on this interface

DR Priority: The DR Priority configured on this Interface (PIM-SM only)

DR Priority is applicable only when sparse-mode configured routers areneighbors. Otherwise, NA is displayed in this field

8.5.1.5 show ip pim rp mapping

Use this command to display all active group-to-RP mappings of which the router is a aware (either configured or learned from the bootstrap router (BSR)). Use the optional parameters to limit the display to a specific RP address or to view group-to-candidate RP or group to Static RP mapping information.

Syntax

show ip pim rp mapping [{rp-address | candidate | static}]

Default Setting

None

Command Mode

Privileged Exec, User Exec

Display Message

RP Address: The IP address of the RP for the group specified

Group Address: The IP address and prefix length of the multicast group

Group Mask: The subnet mask associated with the group

Origin: Indicates the mechanism (BSR or static) by which the RP was selected

Expiry Time: The expiry time of the RP mapping

8.5.1.6 show ip pim rp-hash group-address

This command displays which rendezvous point (RP) is being used for a specified group.

Syntax

show ip pim rp-hash group-address

Default Setting

None

Command Mode

Privileged Exec, User Exec

Display Message

RP Address: The IP address of the RP for the group specified

Type: Indicates the mechanism (BSR or static) by which the RP was selected

8.5.1.7 show ip pim ssm

This command displays the configured source specific IP multicast addresses. If no SSM Group range is configured, this command output is No SSM address range is configured.

Syntax

show ip pim ssm

Default Setting

None

Command Mode

Privileged Exec, User Exec

Display Message

Group Address: The IP multicast address of the SSM group

Prefix Length: The network prefix length

8.5.2 Configuration Commands

8.5.2.1 ip pim bsr-candidate

This command is used to configure the router to announce its candidacy as a bootstrap router (BSR).

Syntax

```
ip pim bsr-candidate interface {<slot/port> | vlan <vlan-id>} <hash-mask-length> [<priority>]
no ip pim bsr-candidate interface {<slot/port> | vlan <vlan-id>} <hash-mask-length> [<priority>]
```

<slot/port> - Valid slot and port number separated by forward slashes.

<vlan-id> - VLAN ID. The range of VLAN ID is 1 to 4093.

<hash-mask-length> - BSR hash-mask length. The range of the mask is 0 to 32.

<priority> - BSR priority. The range of the priority is 0 to 255.

no - This command is used to disable the router to announce its candidacy as a bootstrap router (BSR).

Default Setting

Disabled

Command Mode

Global Config

Parameters

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.

This command takes effect only when PIM-SM is configured as the PIM mode

8.5.2.2 ip pim dense

This command enables the administrative mode of PIM-DM in the router.

Syntax

```
ip pim dense
no ip pim dense
```

no - This command disables the administrative mode of PIM-DM in the router.

Default Setting

Disabled

Command Mode

Global Config

8.5.2.3 ip pim rp-address

This command is used to statically configure the RP address for one or more multicast groups. The parameter rp-address 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

```
ip pim rp-address rp-address group-address/prefix-length [override] no
ip pim rp-address rp-address group-address/prefix-length
```

no - This command is used to statically remove the RP address for one or more multicast groups.

Default Setting

0

Command Mode

Global Config

This command takes effect only when PIM-SM is configured as the PIM mode

8.5.2.4 ip pim 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 pim rp-candidate interface {<slot/port> | vlan <vlan-id>} <group-address> <group-mask>
no ip pim rp-candidate interface {<slot/port> | vlan <vlan-id>} <group-address> <group-mask>
```

<slot/port> - Valid slot and port number separated by forward slashes.

<vlan-id> - VLAN ID. The range of VLAN ID is 1 to 4093.

<group-address> - Specifies the group address.

<group-mask> - Specifies the 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

This command takes effect only when PIM-SM is configured as the PIM mode

8.5.2.5 ip pim sparse

This command enables the administrative mode of PIM-SM in the router.

Syntax

```
ip pim sparse
no ip pim sparse
```

no - This command disables the administrative mode of PIM-SM in the router.

Default Setting

Disabled

Command Mode

Global Config

8.5.2.6 ip pim spt-threshold

Use this command to configure the Data Threshold rate for the last-hop router to switch to the shortest path. The possible values are 0 or Infinity.

Syntax

```
ip pim spt-threshold {0 | Infinity}
no ip pim 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

This command takes effect only when PIM-SM is configured as the PIM mode

8.5.2.7 ip pim ssm

Use this command to define the Source Specific Multicast (SSM) range of IP multicast addresses.

Syntax

```
ip pim ssm {default | <group-address> <group-mask>}
no ip pim ssm {default | <group-address> <group-mask>}
```

<group-address> - Specifies the group address.

<group-mask> - Specifies the group-mask.

no - This command is used to disable the specified Source Specific Multicast (SSM) range.

Default Setting

Disabled

Command Mode

Global Config

Parameters

default - Defines the SSM range access list to 232/8.

8.5.2.8 ip pim

This command administratively enables PIM on an interface or range of interfaces.

Syntax

```
ip pim
no ip pim
```

no - This command sets the administrative mode of PIM on an interface to disabled.

Default Setting

Disabled

Command Mode

Interface Config

8.5.2.9 ip pim bsr-border

Use this command to prevent bootstrap router (BSR) messages from being sent or received through an interface or range of interfaces.

Syntax

```
ip pim bsr-border
no ip pim bsr-border
```

no - Use this command to disable the interface from being the BSR border.

Default Setting

Disabled

Command Mode

Interface Config

This command takes effect only when PIM-SM is configured as the PIM mode

8.5.2.10 ip pim dr-priority

Use this command to set the priority value for which a router is elected as the designated router (DR). This command can be configured on a single interface or a range of interfaces.

Syntax

```
ip pim dr-priority <0-2147483647>
no ip pim dr-priority
```

no - Use this command to reset the priority value for which a router is elected as the designated router (DR).

Default Setting

1

Command Mode

Interface Config

This command takes effect only when PIM-SM is configured as the PIM mode

8.5.2.11 ip pim hello-interval

Use this command to configure the PIM hello interval for the specified router interface or range of interfaces. The hello-interval is specified in seconds and is in the range 10-18000.

Syntax

```
ip pim hello-interval <10-18000>
no ip pim hello-interval
```

no - Use this command to set the PIM hello interval to the default value.

Default Setting

30

Command Mode

Interface Config

8.5.2.12 ip pim join-prune-interval

This command is used to configure the join/prune interval for the PIM-SM router on an interface or range of interfaces. The join/prune interval is specified in seconds. This parameter can be configured to a value from 0 to 18000.

Syntax

```
ip pim join-prune-interval <0-18000>
no ip pim join-prune-interval
```

no - Use this command to set the join/prune interval to the default value.

Default Setting

60

Command Mode

Interface Config

This command takes effect only when PIM-SM is configured as the PIM mode

8.5.2.13 ip pim-trapflags

This command enables the PIM trap mode for both Sparse Mode (SM) and Dense Mode. (DM).

Syntax

```
ip pim-trapflags
no ip pim-trapflags
```

no - This command sets the PIM trap mode to the default

Default Setting

Disabled

Command Mode

Global Config

8.6 IPv6 Protocol Independent Multicast Commands

8.6.1 Show Commands

8.6.1.1 show ipv6 pim

Use this command to display the system-wide information for PIM-DM or PIM-SM.

Syntax

show ipv6 pim

Default Setting

None

Command Mode

Privileged Exec

User Exec

Display Message

PIM Mode: Indicates whether the PIM mode is dense (PIM-DM) or sparse (PIM-SM)

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

Interface-Mode: Indicates whether PIM is enabled or disabled on this interface.

Operational-State: The current state of PIM on this interface. Possible values are Operational or Non-Operational.

8.6.1.2 show ipv6 pim ssm

Use this command to displays the configured source specific IPv6 multicast addresses. If no SSM Group range is configured, this command output is No SSM address range is configured.

Syntax

show ipv6 pim ssm

Default Setting

None

Command Mode

Privileged Exec

User Exec

Display Message

Group Address: The IPv6 multicast address of the SSM group.

Prefix Length: The network prefix length.

8.6.1.3 show ipv6 pim interface

Use this command to displays the interface information for PIM on the specified interface. If no interface is specified, the command displays the status parameters for all PIM-enabled interfaces.

Syntax

show ipv6 pim interface [{<slot/port> | vlan <vlan-id>}]

<slot/port> - Valid slot and port number separated by forward slashes.

<vlan-id> - VLAN ID. The range of VLAN ID is 1 to 4093.

Default Setting

None

Command Mode

Privileged Exec

User Exec

Display Message

Interface: slot/port.

Mode: Indicate whether the PIM mode enabled on the interface is dense or sparse.

Hello Interval: The frequency at which PIM hello messages are transmitted on this interface. By default, the value is 30 seconds.

Join Prune Interval: The join/prune interval for the PIM router. The interval is in seconds. By default, the value is 60 seconds.

DR Priority: The priority of the Designated Router configured on the interface. This field is not applicable if the interface mode is Dense.

BSR Border: Identifies whether this interface is configured as a bootstrap router border interface.

Neighbor Count: The number of PIM neighbors learned on this interface. This is a dynamic value and is shown only when a PIM interface is operational.

Designated Router: The IP address of the elected Designated Router for this interface. This is a dynamic value and will only be shown when a PIM interface is operational. This field is not applicable if the interface mode is Dense.

8.6.1.4 show ipv6 pim neighbor

Use this command to display PIM neighbors discovered by PIMv2 Hello messages. If the interface number is not specified, this command displays the neighbors discovered on all the PIM-enabled interfaces.

Syntax

show ipv6 pim neighbor [{<slot/port> | vlan <vlan-id>}]

<slot/port> - Valid slot and port number separated by forward slashes.

<vlan-id> - VLAN ID. The range of VLAN ID is 1 to 4093.

Default Setting

None

Command Mode

Privileged Exec

User Exec

Display Message

Interface: 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.

DR Priority: The DR Priority configured on this interface (PIM-SM only).

8.6.1.5 show ipv6 pim bsr-router

This command displays the bootstrap router (BSR) information.

Syntax

show ipv6 pim bsr-router {candidate | elected}

Default Setting

None

Command Mode

Privileged Exec

User Exec

Display Message

BSR Address: IPv6 address of the BSR.

BSR Priority: Priority as configured in the ipv6 pim bsr-candidate command.

BSR 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 ipv6 pim bsr-candidate command.

Next Bootstrap Message: 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.

8.6.1.6 show ipv6 pim rp-hash

This command displays which rendezvous point (RP) is being used for a specified group.

Syntax

show ipv6 pim rp-hash <group-address>

<group-address> - The IPv6 address of the RP for the group specified.

Default Setting

None

Command Mode

Privileged Exec

User Exec

Display Message

RP Address: The IPv6 address of the RP for the group specified.

Type: Indicates the mechanism (BSR or static) by which the RP was selected.

8.6.1.7 show ipv6 pim rp mapping

Use this command to display all active group-to-RP mappings of which the router is a aware (either configured or learned from the bootstrap router (BSR)). Use the optional parameters to limit the display to a specific RPaddress or to view group-to-candidate RP or group to Static RP mapping information.

Syntax

show ipv6 pim rp mapping [{rp-address | candidate | static}]

Default Setting

None

Command Mode

Privileged Exec

User Exec

Display Message

RP Address: The IPv6 address of the RP for the group specified.

Group Address: The IPv6 address and prefix length of the multicast group.

Origin: Indicates the mechanism (BSR or static) by which the RP was selected.

Expiry Time: The expiry time of the RP mapping.

8.6.2 Configuration Commands

8.6.2.1 ipv6 pim dense

This command enables the administrative mode of PIM-DM in the router.

Syntax

```
ipv6 pim dense
no ipv6 pim dense
```

no - This command disables the administrative mode of PIM-DM in the router.

Default Setting

Disabled

Command Mode

Global Config

8.6.2.2 ipv6 pim sparse

This command enables the administrative mode of PIM-SM in the router.

Syntax

```
ipv6 pim sparse
no ipv6 pim sparse
```

no - This command disables the administrative mode of PIM-SM in the router.

Default Setting

Disbaled

Command Mode

Global Config

8.6.2.3 ipv6 pim

This command administratively enables PIM on an interface or range of interfaces.

Syntax

```
ipv6 pim
no ipv6 pim
```

no - This command sets the administrative mode of PIM on an interface to disabled.

Default Setting

Disbaled

Command Mode

Interface Config

8.6.2.4 ipv6 pim hello-interval

Use this command to configure the PIM hello interval for the specified router interface or range of interfaces. The hello-interval is specified in seconds and is in the range 0-18000.

Syntax

```
ipv6 pim hello-interval <0-18000>
no ipv6 pim hello-interval
```

no - Use this command to set the PIM hello interval to the default value.

Default Setting

30

Command Mode

Interface Config

8.6.2.5 ipv6 pim bsr-border

Use this command to prevent bootstrap router (BSR) messages from being sent or received through an interface or range of interfaces. Note that this command takes effect only when PIM-SM is enabled in the Global mode.

Syntax

```
ipv6 pim bsr-border
no ipv6 pim bsr-border
```

no - Use this command to disable the interface from being the BSR border.

Default Setting

Disbaled

Command Mode

Interface Config

8.6.2.6 ipv6 pim bsr-candidate

This command is used to configure the router to announce its candidacy as a bootstrap router (BSR). The argument <slot/port> corresponds to a physical routing interface or VLAN routing interface.

Syntax

```
ipv6 pim bsr-candidate interface {<slot/port> | vlan <vlan-id>} <hash-mask-length> [<priority>]
no ipv6 pim bsr-candidate interface {<slot/port> | vlan <vlan-id>} <hash-mask-length> [<priority>]
```

<slot/port> - Interface number on this router from which the BSR address is derived, to make it a candidate. This interface must be enabled with PIM..

<vlan-id> - VLAN ID. The range of VLAN ID is 1 to 4093.

<hash-mask-length> - BSR hash-mask length. The range of the mask is 0 to 128. The length of a mask that is to be ANDed with the group address before the hash function is called. All groups with the saem 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 of the priority is 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 remove the configured PIM candidate BSR router.

Default Setting

None

Command Mode

Global Config

8.6.2.7 ipv6 pim dr-priority

Use this command to set the priority value for which a router is elected as the designated router (DR). This command can be configured on a single interface or a range of interfaces.

Syntax

```
ipv6 pim dr-priority <0-4294967294>
no ipv6 pim dr-priority
```

no - Use this command to disable the interface from being the BSR border.

Default Setting

1

Command Mode

Interface Config

8.6.2.8 ipv6 pim join-prune-interval

This command is used to configure the interface join/prune interval for the PIM-SM router on an interface or range of interfaces. The join/prune interval is specified in seconds. This parameter can be configured to a value from 0 to 18000.

Syntax

```
ipv6 pim join-prune-interval <0-18000>
no ipv6 pim join-prune-interval
```

no - Use this command to set the join/prune interval to the default value.

Default Setting

60

Command Mode

Interface Config

8.6.2.9 ipv6 pim register-rate-limit

This command sets a limit on the maximum number of PIM-SM register messages sent, in kilobits per second,for each (S,G) entry. The valid values are from (0 to 2000 kilobits/sec).

Syntax

```
ipv6 pim register-rate-limit <0-2000>
no ipv6 pim register-rate-limit
```

no - This command resets the register rate limit to the default value.

Default Setting

0

Command Mode

Global Config

8.6.2.10 ipv6 pim rp-address

This command is used to define the address of a PIM Rendezvous point (RP) for a specific multicast group range. The parameter <rp-address> is the IPv6 address of the RP. The parameter <group-address> is the group address supported by the RP. The parameter <prefix-length> 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 pim rp-address <rp-address> <group-address/prefix-length> [override] no
ipv6 pim rp-address <rp-address> <group-address/prefix-length>
```

<rp-address> - The IPv6 address of the RP.

<group-address> - The group address supported by the RP.

<prefix-length> - The group mask for the group address.

override - Indicates that if there is a conflict, the RP configured with this command prevails over the RP learned by BSR.

no - This command is used to remove the address of the configured PIM Rendezvous point (RP) for the specified multicast group range.

Default Setting

None

Command Mode

Global Config

8.6.2.11 ipv6 pim 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) for a specific multicast group range.

Syntax

```
ipv6 pim rp-candidate interface {<slot/port> | vlan <vlan-id>} <group-address/prefix-length>
no ipv6 pim rp-candidate interface {<slot/port> | vlan <vlan-id>} <group-address/prefix-length>
```

<slot/port> - The IP address associated with this interface type and number is advertised as a candidate RP address. This interface must be enabled with PIM.

<vlan-id> - VLAN ID. The range of VLAN ID is 1 to 4093.<group-address> - The multicast group address that is advertised in association with the RP address.

<prefix-length> - The multicast group prefix that is advertised in association with the RP address.

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

8.6.2.12 ipv6 pim spt-threshold

This command is used to configure the Data Threshold rate for the last-hop router to switch to the shortest path. Now support to enable (0) or disable(Infinity).

Syntax

```
iipv6 pim spt-threshold <0 | Infinity>
no ipv6 pim spt-threshold
```

<0> - This is 0 kilobits per seconds.

<Infinity> - This command will disable the function.

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

8.6.2.13 ipv6 pim ssm

Use this command to define the Source Specific Multicast (SSM) range of IPv6 multicast addresses on the router. Note that this command takes effect only when PIM-SM is configured as the PIM mode.

Syntax

ipv6 pim ssm {default | <group-address>/<prefix-length>} no
ipv6 pim ssm

default - Defines the SSM range access list FF3x::/32.

no - This command is used to disable the Source Specific Multicast (SSM) range.

Default Setting

Disbaled

Command Mode

Global Config

8.7 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.

8.7.1 Show Commands

8.7.1.1 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.

8.7.1.2 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.

8.7.1.3 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.

8.7.1.4 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.

8.7.2 Configuration Commands

8.7.2.1 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

8.7.2.2 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

8.7.2.3 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

8.8 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.

8.8.1 Show Commands

8.8.1.1 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.

8.8.1.2 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.

8.8.1.3 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.

8.8.1.4 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.

8.8.2 Configuration Commands

8.8.2.1 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

8.8.2.2 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

8.8.2.3 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

9 IPv6 Commands

9.1 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.

9.1.1 Show Commands

9.1.1.1 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.

9.1.2 Configuration Commands

9.1.2.1 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

9.1.2.2 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> | vlan <vlan-id>}}
```

<slot/port> - The Interface number.

<vlan-id> - VLAN ID. The range of VLAN ID is 1 to 4093.

<ipv4-address> - A valid IP Address.

Default Setting

None

Command Mode

Interfacel Tunnel Mode

9.1.2.3 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

9.1.2.4 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

9.2 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.

9.2.1 Show Commands

9.2.1.1 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.

9.2.2 Configuration Commands

9.2.2.1 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

9.3 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.

9.3.1 Show Commands

9.3.1.1 show ipv6 brief

This command displays the IPv6 status and IPv6 unicast routing mode.

Syntax

show ipv6 brief

Default Setting

None

Command Mode

Privileged Exec

User Exec

Display Message

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.

9.3.1.2 show ipv6 interface port

This command displays the usability status of IPv6 interfaces and whether ICMPv6 Destination Unreachable messages may be sent.

Syntax

show ipv6 interface [{ brief | {port <slot/port> | vlan <vlan-id>} [prefix] }]

<slot/port> - Valid slot and port number separated by forward slashes.

<vlan-id> - VLAN ID. The range of VLAN ID is 1 to 4093.

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.

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).

Router Advertisement Router Preference: Shows router preference value in IPv6 router advertisements.

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.

9.3.1.3 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): The time in seconds that has elapsed since an entry was added to the cache.

9.3.1.4 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.

9.3.1.5 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, 6to4. 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> | vlan <vlan-id>} [<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, 6To4 - 6to4 Route, RG - RIPng

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.

9.3.1.6 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.

RIPng: Preference of RIPng routes.

9.3.1.7 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.

RIPng Routes: Total number of routes installed by RIPng protocol.

6to4 Routes: Total number of 6to4 routes in the routing table.

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.

9.3.1.8

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> | vlan <vlan-id>}]

Default Setting

None

Command Mode

Privileged Exec

Display Message

IPv6 STATISTICS

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.

ICMPv6 STATISTICS

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 Received: 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: Number of ICMP Destination Unreachable messages received by the interface.

ICMPv6 Messages Prohibited Administratively Received: Number of ICMP destination unreachable/communication administratively prohibited messages received by the interface.

ICMPv6 Time Exceeded Messages Received: Number of ICMP Time Exceeded messages received by the interface.

ICMPv6 Parameter Problem Messages Received: Number of ICMP Parameter Problem messages received by the interface.

ICMPv6 Packet Too Big Messages Received: 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.

ICMPv6 Group Membership Query Messages Received: Number of ICMPv6 Group Membership Query messages received by the interface.

ICMPv6 Group Membership Response Messages Received: Number of ICMPv6 Group Membership Response messages received by the interface.

ICMPv6 Group Membership Reduction Messages Received: Number of ICMPv6 Group Membership Reduction 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 Transmitted: 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 Transmitted: Number of ICMPv6 Group Membership Query messages sent.

ICMPv6 Group Membership Response Messages Transmitted: Number of ICMPv6 Group Membership Response messages sent.

ICMPv6 Group Membership Reduction Messages Transmitted: Number of ICMPv6 Group Membership Reduction messages sent.

ICMPv6 Duplicate Address Detects: Number of duplicate addresses detected by interface.

9.3.2 Configuration Commands

9.3.2.1 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

9.3.2.2 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

9.3.2.3 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

9.3.2.4 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

9.3.2.5 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

9.3.2.6 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> | tunnel <tunnel-id> | vlan <vlan-id>} <next-hop-address> [<preference>]}
no ipv6 route <ipv6-prefix>/<prefix_length> [{<next-hopaddress> | interface {<slot/port> | tunnel <tunnel-id> | vlan <vlan-id>} <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

9.3.2.7 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

9.3.2.8 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

9.3.2.9 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

9.3.2.10 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

9.3.2.11 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

9.3.2.12 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

9.3.2.13 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

9.3.2.14 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

9.3.2.15 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 - 3600000>
no ipv6 nd reachable-time
```

no - This command means reachable time is unspecified for the router.

Default Setting

0

Command Mode

Interface Config

9.3.2.16 ipv6 nd router-preference

This command sets the router preference for Default Router.

Syntax

```
ipv6 nd router-preference <high | low | medium>
no ipv6 nd router-preference
```

no - This command resets router preference to default.

Default Setting

Medium

Command Mode

Interface Config

9.3.2.17 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

9.3.2.18 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 -2592000

Preferred-lifetime -604800

Autoconfig - enabled

On-link - enabled

Command Mode

Interface Config

9.3.2.19 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

9.3.2.20 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

9.4 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.

9.4.1 Show Commands

9.4.1.1 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.

External LSDB Limit: Shows the maximum number of non-default AS-external-LSAs entries that can be stored in the link-state database.

Exit Overflow Interval: Shows the number of seconds that, after entering Overflow State, a router will attempt to leave Overflow State.

Autocost Ref BW: Shows the value of auto-cost reference bandwidth configured on the router.

Default Passive Setting: Shows whether the interfaces are passive by default.

Maximum Paths: The maximum number of paths that OSPF can report for a given destination.

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: 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

Number of Active Areas: The number of active OSPF areas. An “active” OSPF area is an area with at least one interface up.

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.

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: 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.

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.

NSF Helper Support: Configure graceful restart.

NSF Helper Strict LSA Checking: Terminate graceful restart helper on topology change.

9.4.1.2 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.

9.4.1.3 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).

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.

No-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.

9.4.1.4 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.

9.4.1.5 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

Ls 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.

Csum: 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.

9.4.1.6 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.

Subtotal: Number of entries for the identified area.Self-Originated Type-7 Ext: Total number of self originated Type-7 external LSAs in the database.

Type-5 Ext: Total number of Type-5 external LSAs in the database.

Self-Originated Type-5 Ext: Total number of self originated Type-5 external LSAs in the database.

Total: Total number of router LSAs in the OSPFv3 link state database.

9.4.1.7 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> | vlan <vlan-id>}

<slot/port> - Interface number.

<0-7> - Loopback/Tunnel Interface ID.

Default Setting

None

Command Mode

Privileged Exec

User Exec

Display Messages

IPv6 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.

Transmit Delay Interval: A number representing the OSPF Transmit Delay for the specified interface.

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.

9.4.1.8 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.

9.4.1.9 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> | loopback <loopback-id> | tunnel <tunnel-id> | vlan <vlan-id>}

<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.

9.4.1.10 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> | vlan <vlan-id>} | <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.

9.4.1.11 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.

9.4.1.12 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.

9.4.1.13 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.

9.4.1.14 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.

9.4.2 Configuration Commands

9.4.2.1 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

9.4.2.2 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

9.4.2.3 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

9.4.2.4 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

9.4.2.5 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

9.4.2.6 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

9.4.2.7 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

9.4.2.8 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

9.4.2.9 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

9.4.2.10 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

9.4.2.11 ipv6 router ospf

Use this command to enter Router OSPFv3 Config mode.

Syntax

```
ipv6 router ospf
```

Default Setting

None

Command Mode

Global Config

9.4.2.12 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

9.4.2.13 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

9.4.2.14 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

9.4.2.15 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

9.4.2.16 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

9.4.2.17 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

9.4.2.18 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

9.4.2.19 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

9.4.2.20 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

9.4.2.21 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

9.4.2.22 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

9.4.2.23 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

9.4.2.24 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

9.4.2.25 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

9.4.2.26 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

9.4.2.27 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

9.4.2.28 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

9.4.2.29 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

9.4.2.30 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

9.4.2.31 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

9.4.2.32 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

9.4.2.33 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

9.4.2.34 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.

9.4.2.35 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.

9.4.2.36 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 {< slot/port> | default | tunnel <tunnel-id> | vlan <vlan-id>}
no passive-interface {< slot/port> | default | tunnel <tunnel-id> | vlan <vlan-id>}
```

Default Setting

Disabled

Command Mode

Router OSPFv3 Config.

9.4.2.37 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

9.4.2.38 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

9.5 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.

9.5.1 Show Commands

9.5.1.1 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.

9.5.2 Configuration Commands

9.5.2.1 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

9.5.2.2 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

9.5.2.3 ipv6 router rip

Use this command to enter Router RIPng mode.

Syntax

```
ipv6 router rip
```

Default Setting

Disabled

Command Mode

Global Config

9.5.2.4 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

9.5.2.5 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

9.5.2.6 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

9.5.2.7 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

9.5.2.8 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

9.5.2.9 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

9.5.2.10 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 Data Center Bridging Commands

10.1 FIP Snooping

10.1.1 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.

10.1.2 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

ENode MAC: MAC address of the ENode.

ENode Interface Number: 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.

10.1.3 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

VN Port MAC: FCoE MAC address that is used to send the FCoE packets.

FCF Interface Number: The interface to which the FCF is connected

FCF MAC address: MAC address of the FCF..

ENode MAC address: MAC address of the ENode.

ENode Interface Number: The interface to which the ENode is connected

10.1.4 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

FCF MAC: MAC address of the FCF.

FCF Interface Number: 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.

Switch Name: Name ID.

Fabric Name: Name of the FCF.

10.1.5 show fip-snooping vlan

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

Syntax

```
show fip-snooping vlan {< 1-4093> | all}
```

<1 - 4093> - 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.

10.1.6 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

10.1.7 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 <1-4093>
no fip-snooping vlan <1-4093>
```

<1 - 4093> - VLAN ID.

no - This command disable snooping on a specific VLAN.

Default Setting

Disabled

Command Mode

Global Config

10.2 Priority-based Flow Control

10.2.1 show dcb priority-flow-control

Display the PFC information of a given interface or all interface.

Syntax

```
show dcb priority-flow-control {<interface> | all }
```

Default Setting

None

Command Mode

Privileged Exec

10.2.2 priority-flow-control mode

Set Priority-Flow-Control (PFC) to be enabled, disabled, or atuo on the interface.

Both PFC and 802.3x flow control are enabled, PFC will take effect.

Syntax

```
priority-flow-control mode { on | auto}
no priority-flow-control mode
```

no - This command auto the Priority-Flow-Control (PFC) on the interface.

Default Setting

Auto

Command Mode

DCB (Data Center Bridging) interface mode

10.2.3 priority-flow-control priority

Enable or disable the priority group for lossless (no-drop) or lossy (drop) behavior on the selected interface.

Syntax

priority-flow-control priority <priority_id> { drop | no-drop } no

priority-flow-control priority

Default Setting

The default behavior for priority(3,4,5,6) are no-drop

Command Mode

DCB (Data Center Bridging) interface mode

10.2.4 clear priority-flow-control statistics

Clear all global and interface PFC statistics

Syntax

clear priority-flow-control statistics

Command Mode

Privileged EXEC

10.3 Enhanced Transmission Selection (ETS)

10.3.1 show dcb ets interface

This command displays ETS mode on specific interface.

Syntax

show dcb ets interface [<slot/port>]

<slot/port> - Interface number.

Default Setting

None

Command Mode

Privileged Exec

Display Message

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

ETS: ETS admin mode.

Scheduler Type: ETS scheduler type.

LAN: ETS weight in percentage for LAN stream.

SAN: ETS weight in percentage for SAN stream.

Priority: ETS priority.

Priority Group: ETS priority to priority group mapping list.

10.3.2 ets mode

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

Syntax

```
ets mode {auto | on}
no ets mode
```

auto - This command enables the DCBX ETS function on

- This command enables ETS function.

no - This command disables ETS function.

Default Setting

Disabled

Command Mode

Data-Center-Bridging Interface Mode

10.3.3 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

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

Data-Center-Bridging Interface Mode

10.3.4 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

```
ets weight <1-99> <1-99>
no 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

Data-Center-Bridging Interface Mode

10.3.5 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

ets pg-mapping {lan|san|ipc} [<0-7> [<0-7> [<0-7> [<0-7> [<0-7> [<0-7> [<0-7>]]]]]]] no 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

Data-Center-Bridging Interface Mode

10.4 Congestion Notification

10.4.1 show dcb congestion-notify

This command displays CN function global parameter on system.

Syntax
show dcb 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.

10.4.2 show dcb congestion-notify interface

This command displays CN function global parameter on system.

Syntax

```
show dcb congestion-notify interface [<slot/port>]
```

<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.

10.4.3 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

Data-Center-Bridging Interface Mode

10.4.4 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

Enabled

Command Mode

Global Data-Center-Bridging Mode

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 Data-Center-Bridging Mode

10.4.5 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

Enabled

Command Mode

Global Data-Center-Bridging Mode

10.4.6 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 Data-Center-Bridging Mode

10.4.7 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 Data-Center-Bridging Mode

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

Q_No

Command Mode

Global Data-Center-Bridging Mode

10.4.8 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 <-1-65535> | vlan <-1-4093>} 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. <-1-65535> - This command sets value of CNM's outer VLAN tag's TPID. <-1-4095> - This command sets the CNM's outer VLAN ID.

no - This command restored default value.

Default Setting

CFI: -1

Dot1p: -1

TPID: -1

Vlan: -1

Command Mode

Global Data-Center-Bridging Mode

10.4.9 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

CFI: -1

Dot1p: -1

Command Mode

Global Data-Center-Bridging Mode

10.4.10 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 Data-Center-Bridging Mode

10.5 Data Center Bridging eXchange (DCBX)

10.5.1 show dcbx interface

This command displays DCBX interface paramters on system.

Syntax
show dcbx interface

Default Setting

None

Command Mode

Privileged Exec

Display Message

Interface: Displays the interface number.

DCBX Admin: Displays the administrative mode of DCBX.

PFC Willing: Displays the willing mode of PFC.

PG Willing: Displays the willing mode of PG

10.5.2 show dcbx priority-flow-control interface

This command displays DCBX priority flow control paramters for an interface.

Syntax

show dcbx priority-flow-control interface <slot/port>

<slot/port> - interface number

Default Setting

None

Command Mode

Privileged Exec

Display Message

Port: Displays the interface number.

Show Type: Displays the data type, including Admin Config, Oper Config, and Peer Config.

Feature: Displays the feature name.

Enable: Displays the enable mode of PFC

Advertise: Display the advertise mode of PFC

Willing: Display the willing mode of PFC

Priority Mask: Display the priority mask of PFC, priority is shown from 0 to 7 in sequence. 0 means the priority is disabled, and 1 means the priority is enabled.

Max Traffic Class: Displays the max. traffic class support.

Oper Version: Displays the operational version of PFC feature.

Max Version: Displays the maximum version of PFC feature. Error:

Displays the error code

Operational Mode: Displays the operational mode of PFC feature.

Syncd with Peer: Displays if feature is synchronized with peer.

(Xenya) #show dcbx priority-flow-control interface 0/1

Port..... 0/1

Show Type..... Admin Config

Feature ..... Priority Flow Control

Enable ..... true

Advertise..... true
Willing..... true
Priority Mask..... 0 0 0 1 1 1 1 0
Max Traffic Class 8

Show Type..... Oper Config
Feature ..... Priority Flow Control
Oper Version..... 0
Max Version..... 0
Error ..... 0x0 - None
Operational Mode ..... false
Syncd with Peer..... false
Priority Mask..... 0 0 0 1 1 1 1 0
Max Traffic Class 8

Show Type..... Peer Config
Feature ..... Priority Flow Control
Local Interface 0/1
Status ..... Not present
Enable ..... false
Willing..... false
Priority Mask..... 0 0 0 0 0 0 0 0
Max Traffic Class 8

10.5.3 show dcbx priority-group interface

This command displays DCBX priority group paramters for an interface.

Syntax

show dcbx priority-group interface <slot/port>

<slot/port> - interface number

Default Setting

None

Command Mode

Privileged Exec

Display Message

Port: Displays the interface number.

Show Type: Displays the data type, including Admin Config, Oper Config, and Peer Config.

Feature: Displays the feature name.

Enable: Displays the enable mode of PG

Advertise: Displays the advertise mode of PG

Willing: Displays the willing mode of PG

Group Bandwidth: Displays the bandwidth percentage for each group.

Priority Group ID: Displays the Priority and Group ID mapping.

Max Traffic Class: Displays the max. traffic class support.

Oper Version: Displays the operational version of PFC feature.

Max Version: Displays the maximum version of PFC feature.

Error: Displays the error code

Operational Mode: Displays the operational mode of PFC feature.

Syncd with Peer: Displays if feature is synchronized with peer.

(Xenya) #show dcbx priority-group interface 0/1

Port..... 0/1

Show Type..... Admin Config

Feature ..... Priority Group

Enable ..... true

Advertise..... true
Willing ..... false
Group Bandwidth 10% 90% 0% 0% 0% 0% 0% 0%
Priority Group ID 0 0 0 1 1 1 1 15
Max Traffic Class 8

Show Type..... Oper Config
Feature ..... Priority Group
Oper Version..... 0
Max Version..... 0
Error..... 0x0 - None
Operational Mode..... false
Syncd with Peer ..... false
Group Bandwidth 10% 90% 0% 0% 0% 0% 0% 0%
Priority Group ID 0 0 0 1 1 1 1 15
Max Traffic Class 8

Show Type..... Peer Config
Feature ..... Priority Group
Local Interface 0/1
Status ..... Not present
Enable ..... false
Willing ..... false
Group Bandwidth 0% 0% 0% 0% 0% 0% 0% 0%
Priority Group ID 0 0 0 0 0 0 0 0
Max Traffic Class 8

10.5.4 dcbx enable

This command sets DCBX administrative mode for an interface. Use no form of this command to disable the DCBX for an interface.

Syntax

```
dcbx enable
no dcbx enable
```

no - This command sets administrative mode to disable for the interface.

Default Setting

Disabled

Command Mode

Data Center Bridging Interface Mode

10.5.5 dcbx priority-flow-control willing

This command sets DCBX willing mode for priority-flow-control. Use no form of this command to disable it.

Syntax

```
dcbx priority-flow-control willing
no dcbx priority-flow-control willing
```

no - This command sets willing mode to disable for the interface.

Default Setting

Enabled

Command Mode

Data Center Bridging Interface Mode

10.5.6 dcbx priority-group willing

This command sets DCBX willing mode for priority-group. Use no form of this command to disable it.

Syntax

```
dcbx priority-group willing
no dcbx priority-group willing
```

no - This command sets willing mode to disable for the interface.

Default Setting

Disabled

Command Mode

Data Center Bridging Interface Mode

10.6 Ethernet Virtual Bridging

10.6.1 show evb status

This command displays EVB function global parameter on system.

Syntax

show evb status

Default Setting

None

Command Mode

Privileged Exec

Display Message

Interface: Displays the interface number.

Link: Displays the link status of this interface

Admin Mode: Displays the administrative mode of EVB on this interface.

10.6.2 show evb status

This command displays EVB function interface parameter on system.

Syntax

show evb status <slot/port>

Default Setting

None

Command Mode

Privileged Exec

Display Message

Admin Mode: Display the administrative mode of this interface

Remote Sync: Displays the synchronization status

Support Capability: Displays the support capabilities of EVB on this interface.

Configure Capability: Displays the configured capabilities of EVB on this interface.

Support Mode: Display the support mode of EVB on this interface.

Configure Mode: Display the configured mode of EVB on this interface.

Configure RTE: Display the configured RTE of EVB on this interface.

Current RTE: Display the current RTE of EVB on this interface.

10.6.3 show evb vsi-profile

This command displays VSI profile paramters on system.

Syntax

```
show evb vsi-profile [<slot/port> | detailed <slot/port>]
```

Default Setting

None

Command Mode

Privileged Exec

Display Message

Interface: Display the interface number.

Instance ID: Displays the instance ID of the VSI profile.

MAC address: Displays the MAC address of VSI profile.

VLAN: Displays the VLAN information of VSI profile.

10.6.4 evb enable

This command sets the administrative mode of EVB for an interface.

Syntax

```
evb enable
no evb enable
```

no - This command sets administrative mode to disable for the interface.

Default Setting

Disabled

Command Mode

Interface Config

10.6.5 evb rte

This command sets the Retransmission Timer Exponent of EVB for an interface.

Syntax

```
evb rte <16-31>
no evb rte
```

<16-31>: Retransmission timer Exponent (RTE) ranged from 16 to 31. no

- This command sets RTE to default setting.

Default Setting

16

Command Mode

Interface Config

10.7 VM Tracer Commands

10.7.1 Show Commands

10.7.1.1 show vmtracer interface

This command displays VM Tracer interface mode on all interfaces or the VM interface (Vnics) that are on the specific switch interface where the VM Tracer interface mode is enabled.

Syntax

```
show vmtracer interface <Interface_Name>
```

<Interface_Name>

- no parameter - show VM Tracer interface mode on all interfaces.
- <slot/port> - show the VM interface (Vnics) that are on the <slot/port> where the VMTracer interface mode is enabled.

Default Setting

None

Command Mode

Privileged Exec

Display Message

Port: the physical interface number of the device.

VM Tracer: the VM Tracer interface mode state. The value should be Enable or Disable. VM

Name: the name of attached VM.

VM Adapter: the adapter name of the VM interface.

VLAN: the VLAN value of the VM interface.

10.7.1.2 show vmtracer session

This command displays information about a specified VM Tracer session on the system.

Syntax

```
show vmtracer session <Session_Name>
```

<Session_Name>

- no parameter - displays all configured VM Tracer sessions.
- <session_name> - displays the specific configured VM Tracer session with the name.

Default Setting

None

Command Mode

Privileged Exec

Display Message

Session Name: the configured name of the VM Tracer session.

vCenter URL: the url address of vCenter. It should be start with https://.

Username: the login username of vCenter on the VM Tracer session

Password: the login password of vCenter on the VM Tracer session.

AutoVlan: the mode of AutoVlan. The value should be Enable of Disable.

Allow-Vlan: allow-vlan list of the VM Tracer session.

Session Status: the link state of the VM Tracer session.

10.7.1.3 show vmtracer vm

The command displays VMs interfaces (Vnics) that are accessible to the switch interfaces where the VM Tracer interface mode is enabled.

Syntax

show vmtracer vm <Info_Level> <Vm_Name>

<Info_Level>

- no parameter - displays VM name, VM adapter name, assoiated interface, and VLAN value.
- detail - displays VM name associated interface vnic, mac, portgroup, vlan, switch and host.

<Vm_Name>

- no parameter - displays information for all aooaciated VMs.
- <Vm_Name> - displays information for the specific VM.

Default Setting

None

Command Mode

Privileged Exec

Display Message

VM Name: the name of attached VM.

VM Adapter: the adapter name of the VM interface.

Interface: the associated switch interface of attached VM.

VLAN: the VLAN value of the VM interface.

Vnic: the adapter name of the VM interface.

Mac: the network mac address of vnic.

Portgroup: the portgroup of the VM.

Vlan: the vlan value of the VM interface.

Switch: the vSwitch of the VM.

Host: the host of the VM.

10.7.1.4 show vmtracer host

The command displays information about the hosts associated to the VM Tracer enabled interface.

Syntax
show vmtracer host

Default Setting

None

Command Mode

Privileged Exec

Display Message

Interface: the associated switch interface of the host device.

Host: the host name

Manufacturer: the manufacture vendor of the host device

Model: the model name of host device.

CPU Speed: the cpu speed of the host device.

CPUs: the number of cpu inside the host device.

CPU Cores: the cpu cores of the host device.

Memory: the memory size of the host device.

10.7.2 Configuration Commands

10.7.2.1 vmtracer session

This command places the switch in vmtracer mode for the specified session. The command creates a new session or loads an existing session for editing.

The switch supports total four VM Tracer sessions.

Syntax
vmtracer session <Session_Name> no vmtracer session <Session_Name>

no - This command removes a existed VM Tracer session.

<Session_Name> - The label assigned to the VM Tracer session.

Default Setting

None

Command Mode

Global Config

When the switch in vmtracer mode, it can configure the following commands: ●

allow-vlan

- autovlan disable
- exit (vmtracer mode)
- password (vmtracer mode)
- url
- username (vmtracer mode)

10.7.2.2 allow-vlan

The command specifies the VLANs that may be added when a VM is added or moved from the hypervisor connected to the session specified by the vmtracer mode. By default, all VLANs are allowed.

Syntax

allow-vlan <VLAN_Action> <VLAN_Range>

<VLAN_Action>

- no parameter - create a allow-vlan list by following <VLAN_Range>
- add - add <VLAN_Range> to current allow-vlan list
- remove - remove <VLAN_Range> from current allow-vlan list
- none - make allow-vlan to empty
- all - make allow-vlan to all vlan (1-4093)

<VLAN_Range> - hyphen is used to assign a continued numbers (ex. 1-1024) and comma is used to connect 2 different numbers (ex. 1,2,3,4)

Default Setting

all

Command Mode

VM Tracer Config

10.7.2.3 autovlan disable

This command disable vlan auto provisioning which allows the dynamic assignment and pruning of VLANs when a VM attached to the ESX connected to the switch is created, deleted, or moved to a different ESX host. The autovlan setting controls auto provisioning.

Syntax

```
autovlan disable
no autovlan disable
```

no - this command enables vlan auto provisioning.

Default Setting

no autovlan disable

Command Mode

VM Tracer Config

10.7.2.4 password

The command specifies the token that authorizes the username to the vCenter associated with the VM Tracer session.

Syntax

```
password <Encryption> <Password>
```

<Encryption> - This command sets encryption level of the password.

0 - the password is a clear text string.

7 - the password is an encrypted string.

<Encryption> - text that authenticates the username.

Default Setting

none

Command Mode

VM Tracer Config

10.7.2.5 username

The command identifies the switch's account name on the vCenter server. The switch uses this user name to access vCenter information.

Syntax

username <Name_String>

<Name_String> - vCenter account user name. Parameter must match the user name configured on the vCenter.

Default Setting

none

Command Mode

VM Tracer Config

10.7.2.6 url

The command specifies the vCenter server location that is monitored by the session being edited by the current vmtracer mode. The command must reference a fully formed secure url.

Syntax

url <URL_Name>

<URL_Name> - the location value of the vCenter server. Valid formats include IP address (dotted decimal notation) and fully qualified domain name.

Default Setting

none

Command Mode

VM Tracer Config

10.7.2.7 exit

This command returns the switch to Global Configuration mode and enables the VM Tracer session. Changes to the VM Tracer session that were made in vmtracer mode are stored when the mode is exited.

Syntax

exit

Default Setting

none

Command Mode

VM Tracer Config

10.7.2.8 vmtracer

The command enables vmtracer mode on the configuration mode interface. Interfaces with vmtracer mode enabled send discovery packets to the connected host device.

The no vmtracer command disables vmtracer mode on the configuration mode interface.

Syntax

vmtracer

no vmtracer

no - This command disables VM Tracer mode on the configuration mode interface

Default Setting

disable

Command Mode

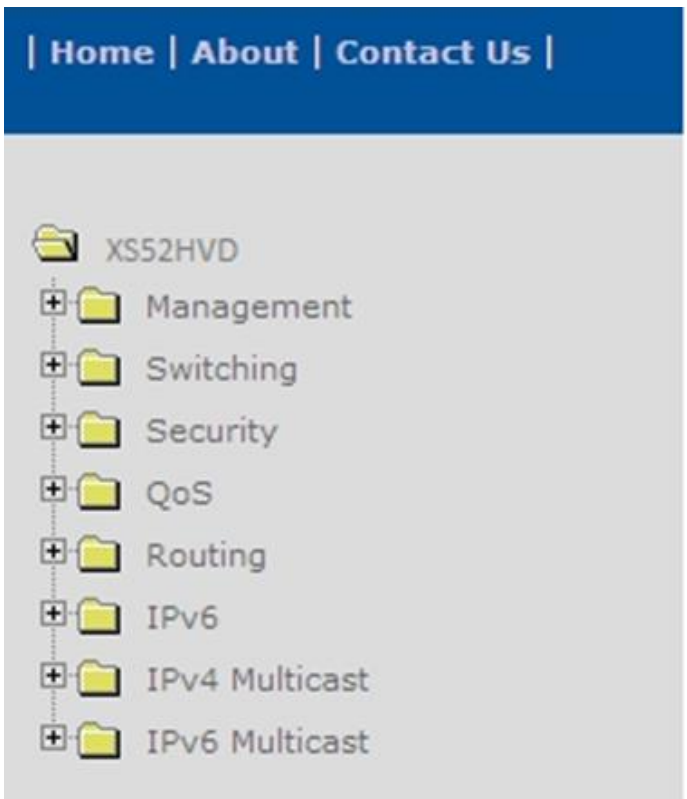
Interface Config

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: Management, Switching, Security, QOS, Routing, IPv6, IPv4 Multicast, IPv6 Multicast and Data Center.



1. Management Menu: This section provides information for SNMP and trap manager, User management, System utility including system time, defining system parameters including telnet session and console baud rate, etc, File management including downloading switch module software and configuration file, and resetting the switch module switch statistics, SNTP, LLDP, UDLD, CDP, DHCP client, DNS Relay and DDNS.

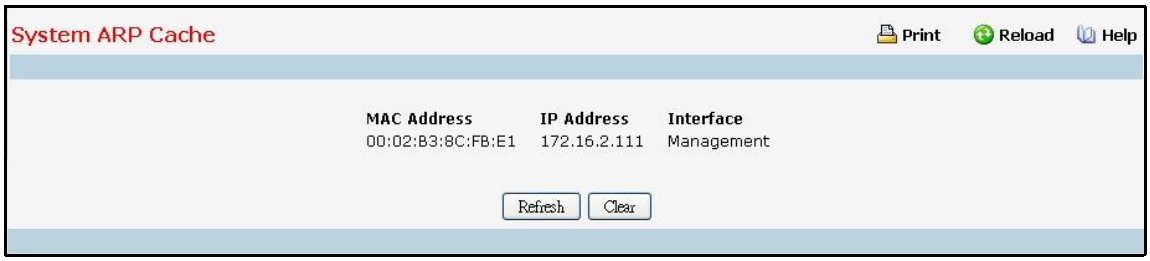
2. Switching Menu: This section provides users to configure switch interface (port), DHCP Snooping, VLAN, Protected Ports, Protocol-Based VLAN, IP Subnet-based VLAN, MAC-based VLAN, MAC-Based Voice VLAN, Voice VLAN, Filters, GARP, Dynamic Arp Inspection, IGMP Snooping, IGMP Snooping Querier, MLD Snooping, MLD Snooping Querier, Port Channel, Multicast Forwarding Database, Spanning Tree, MLAG, VTP, Link State, and Port Backup.
3. Security Menu: This section provides users to configure switch securities including Port Access Control, Port Security, Captive-portal, RADIUS, TACACS+, LDAP, Access Control Lists, IP Filter, Secure HTTP, Secure Shell and Denial of Service.
4. QOS Menu: This section provides users to configure Differentiated Service, DiffServ Wizard, Class of Service, Auto VoIP and iSCSI optimization.
5. 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.
6. IPv6 Menu: This section provides users to configure OSPFv3, RIPv6, and IPv6 Routing Interface.
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.
9. Data Center Menu: This section provides users to configure Congestion notification, Data Center Bridging Exchange, PFC, ETS ,FIP snooping, EVB and VM Tracer.

11.2 Management Menu

11.2.1 Viewing Information

11.2.1.1 Viewing 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.

11.2.1.2 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.

FRU Number - The field replaceable unit number.

Part Number - The manufacturing part number.

Maintenance Level - The identification of the hardware change level

Manufacturer - The two-octet code that indicates the manufacturer.

Burned in MAC Address - The burned-in universally administered MAC address of this switch.

Software Version - The platform.function.release.manintenance number of the code is currently running on the switch.

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

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

Operating System - The operating system currently running on the switch.

Network Processing Device - Identifies the network processor hardware.

PSOC_CY8C3245 Sensor - The temperature of sensor of PSOC_CY8C3245

Depend on air flow FAN 1 - 4 connected PSOC_CY8C3245-1 or PSOC_CY8C3245-2:

Front-To-Back: (Connected PSOC_CY8C3245-1 or ADT7470-1)

PSOC_CY8C3245_1/ADT7470-1: Fan 1 Status: Status of Fan1. It could be active or inactive.

PSOC_CY8C3245_1/ADT7470-1: Fan 2 Status: Status of Fan2. It could be active or inactive.

PSOC_CY8C3245_1/ADT7470-1: Fan 3 Status: Status of Fan3. It could be active or inactive.

PSOC_CY8C3245_1/ADT7470-1: Fan 4 Status: Status of Fan3. It could be active or inactive.

Back-To-Front: (Connected PSOC_CY8C3245-2 or ADT7470-2)

PSOC_CY8C3245_2/ADT7470-2: Fan 1 Status: Status of Fan1. It could be active or inactive.

PSOC_CY8C3245_2/ADT7470-2: Fan 2 Status: Status of Fan2. It could be active or inactive.

PSOC_CY8C3245_2/ADT7470-2: Fan 3 Status: Status of Fan3. It could be active or inactive.

PSOC_CY8C3245_2/ADT7470-2: Fan 4 Status: Status of Fan3. It could be active or inactive.

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

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 Number: 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).

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.

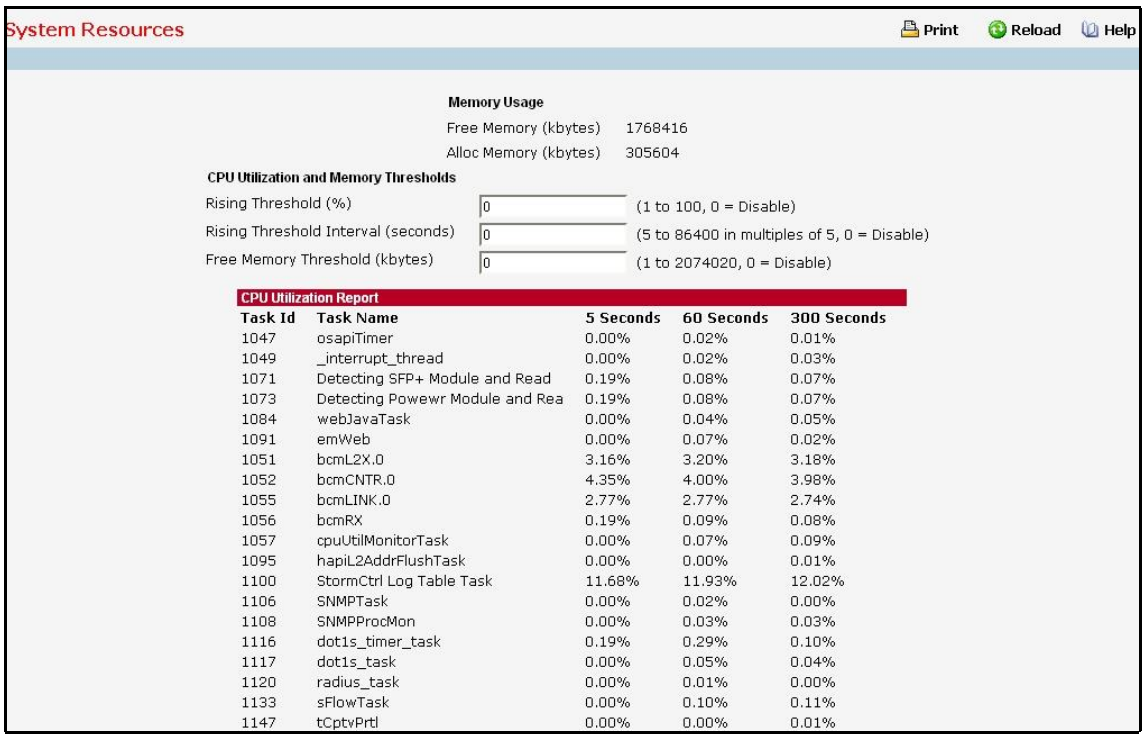
Vendor Manufacturing Date: The vendor's manufacturing date.

Additional Packages - A list of the optional software packages installed on the switch, if any.

Command Buttons

Refresh - Updates the information on the page.

11.2.1.3 System Resources



Use this panel to configure and display the Free Memory and Task CPU Utilization parameters

Configurable Data

Rising Threshold - The CPU Rising utilization threshold in percentage. A zero percent threshold indicates CPU Utilization Notification feature is disabled.

Rising Threshold Interval - The CPU Rising threshold interval in seconds. The time interval is configured in multiples of 5. A time interval of zero seconds indicates CPU Utilization Notification feature is disabled.

Free Memory Threshold - The CPU Free Memory threshold in kilobytes. A zero threshold value indicates CPU Free Memory Notification feature is disabled

Non- Configurable Data

Free Memory - Available Free Memory on system in kilobytes

Alloc Memory - Allocated Memory for the system in kilobytes

Task Id - Id of the Currently Running Tasks.

Task Name - Name of the Currently Running Tasks.

5 Seconds - Percentage of CPU utilized by the corresponding task in the last 5 seconds.

60 Seconds - Percentage of CPU utilized by the corresponding task in the last 60 seconds.

300 Seconds - Percentage of CPU utilized by the corresponding task in the last 300 seconds.

Total CPU Utilization - Total CPU Utilization in terms of Percentage over a period of 5, 60, 300 seconds, and the Rising threshold period also in seconds, if configured.

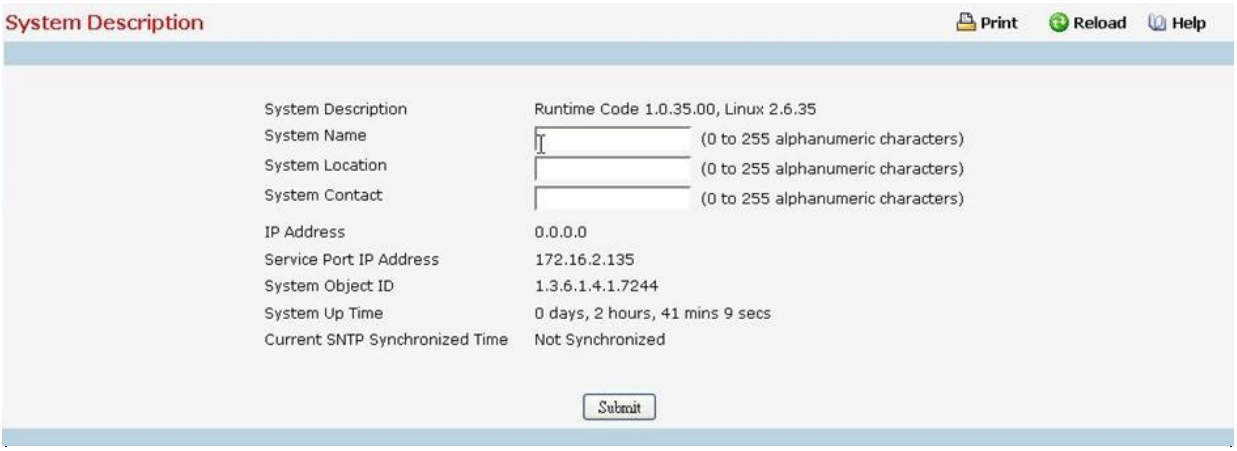
Command Buttons

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.

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

11.2.2 Configuring Management Session and Network Parameters

11.2.2.1 Viewing System Description Page



Configurable Data

System Name - Enter the name you want to use to identify this switch. You may use up to 255 alpha-numeric characters. The factory default is blank.

System Location - Enter the location of this switch. You may use up to 255 alpha-numeric characters. The factory default is blank.

System Contact - Enter the contact person for this switch. You may use up to 255 alpha-numeric characters. The factory default is blank.

Non-Configurable Data

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 Synchronized Time - Displays currently synchronized SNTP time in UTC. If time is not synchronized, it displays "Not Synchronized."

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.

11.2.2.2 IP Address Conflict Detection

Non- Configurable Data

Conflict Detection Status - Whether or not an address conflict has been detected since status was last reset.

Last Conflicting IP Address - The IP address of the interface that was last found to be conflicting.

Last Conflicting MAC Address - The MAC address of the remote host associated with the IP address that was last found to be conflicting.

Time Since Conflict Detected - The time elapsed (displayed in days, hours, mins, secs) since the last conflict was detected (provided a reset did not occur in the meantime).

Command Buttons

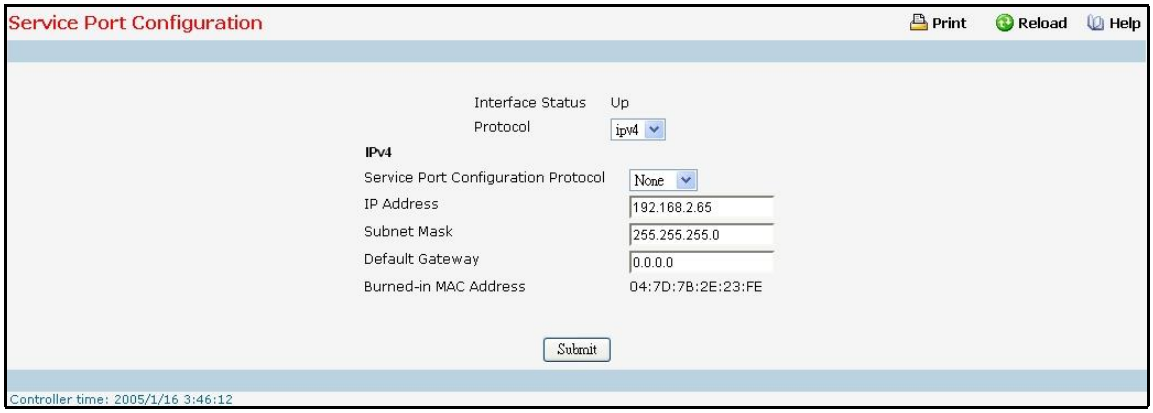
Reset Conflict Detection Status - Reset the last conflict detection status on the switch.

Run Conflict Detection - Triggers the active IP address conflict detection in the system.

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

11.2.2.3 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.



Configurable Data

Protocol - Choose IPv4 or IPv6 protocol.

Non-Configurable Data

Interface Status - Indicates whether the link status is up or down.

IPv4 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.

IPv6 Selection Critieria

IPv6 Mode - Enable/Disable IPv6.

Service Port Configuration Protocol - Enable or Disable DHCPv6 Client protocol on the management port. The factory default is None.

IPv6 Stateless Address AutoConfig Mode-Enable or Disable the IPv6 stateless address autoconfiguration on the management port. The factory default is Disable.

Add/Delete IPv6 Addresses - To Add or Delete the IPv6 Addresses, select Add or Remove from the drop-down menu. The fields "New IPv6 Address" and "EUI Flag" are visible when we select the "Add" from this menu.

Change IPv6 Gateway -Select the checkbox to configure/change/remove IPv6 Gateway Addresses. To configure / change the Ipv6 gateway, select the checkbox and enter the desired value in the "IPv6 Gateway" textbox. To remove, select the checkbox, the textbox "IPv6 Gateway" has to be empty and click submit button.

IPv4 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 Configurable Data

New IPv6 Address - To configure the field, select Add from the "Add/Delete IPv6 Addresses" drop down menu

EUI Flag -To set the EUI flag while configuring "New IPv6 Address" select True from the drop down menu. Default is False.

IPv6 Address to Delete - To configure the field to delete IPv6 address, select Delete from the "Add/Delete IPv6 Addresses" drop down menu.

IPv6 Gateway - The default gateway for the IPv6 interface. The factory default value is None

IPv4 Non-Configurable Data

Burned-in MAC Address - The burned-in MAC address used for in-band connectivity. IPv6

Non-Configurable Data

DHCPv6 Client DUID -Displays the Client Identifier used by DHCPv6 Client when sending messages to the DHCPv6 Server. This entry is visible to user only if IPv6 Service Port Configuration Protocol is set to DHCP

IPv6 Addresses -List of configured IPv6 addresses.

Default IPv6 Gateway Address -Default IPv6 Gateway addresses

IPv6 Link-local scope ID - Service Port's IPv6 Link-local address scope ID.

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

11.2.2.4 Configuring Service port 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.

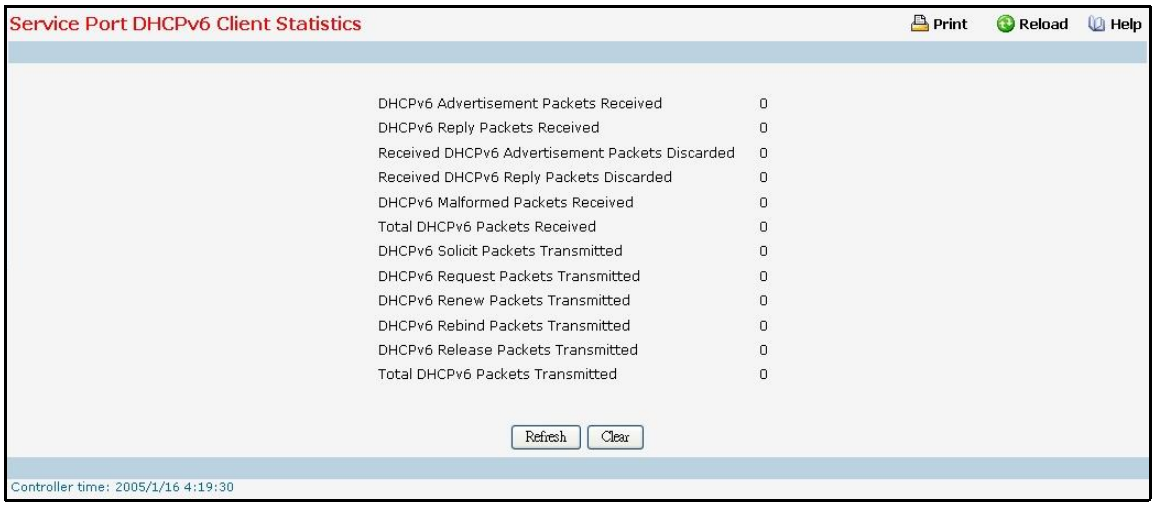
Neighbor State -The state of the neighboring switch: reachable (1) - The neighbor is reachable by this switch. Stale (2) - Information about the neighbor is scheduled for deletion. Delay (3) - No information has been received from neighbor during delay period. Probe (4) - Switch is attempting to probe 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.

11.2.2.5 Service Port DHCPv6 Client Statistics



Non-Configurable Data

DHCPv6 Advertisement Packets Received - Number of DHCPv6 Advertisement packets received on the service port.

DHCPv6 Reply Packets Received - Number of DHCPv6 Reply packets received on the service port.

Received DHCPv6 Advertisement Packets Discarded - Number of DHCPv6 Advertisement packets discarded on the service port

Received DHCPv6 Reply Packets Discarded - Number of DHCPv6 Reply packets discarded on the service port.

DHCPv6 Malformed Packets Received - Number of DHCPv6 packets that are received malformed on the service port.

Total DHCPv6 Packets Received - Total number of DHCPv6 packets received on the service port.

DHCPv6 Solicit Packets Transmitted - Number of DHCPv6 Solicit packets transmitted on the service port.

DHCPv6 Request Packets Transmitted - Number of DHCPv6 Request packets transmitted on the service port.

DHCPv6 Renew Packets Transmitted - Number of DHCPv6 Renew packets transmitted on the service port.

DHCPv6 Rebind Packets Transmitted - Number of DHCPv6 Rebind packets transmitted on the service port.

DHCPv6 Release Packets Transmitted - Number of DHCPv6 Release packets transmitted on the service port.

Total DHCPv6 Packets Transmitted - Total number of DHCPv6 packets transmitted on the service port.

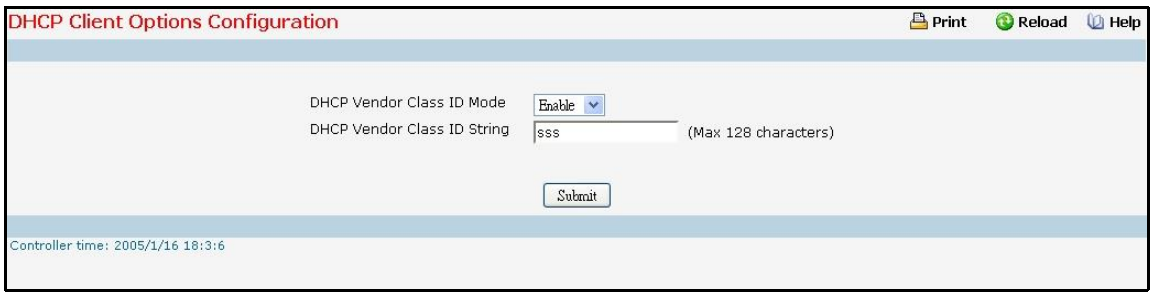
Command Buttons

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

Clear - Clears all the counters, resetting all statistics to defaults.

11.2.2.6

11.2.2.7 Configuring DHCP Client Options Configuration



Selection Criteria

DHCP Vendor Class ID Mode - Enable / Disable the vendor class identifier mode.

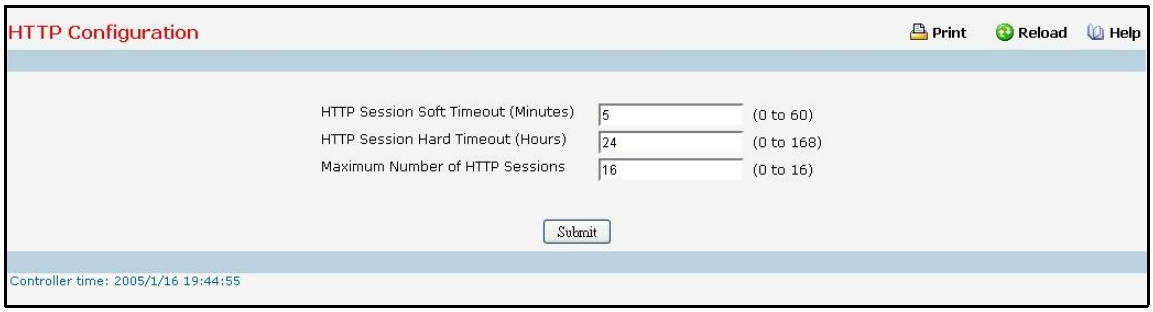
Configurable Data

DHCP Vendor Class ID String - The string that would be added to DHCP requests as Option-60. i.e. Vendor Class Identifier option. Range is up to 128 characters

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.

11.2.2.8 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.

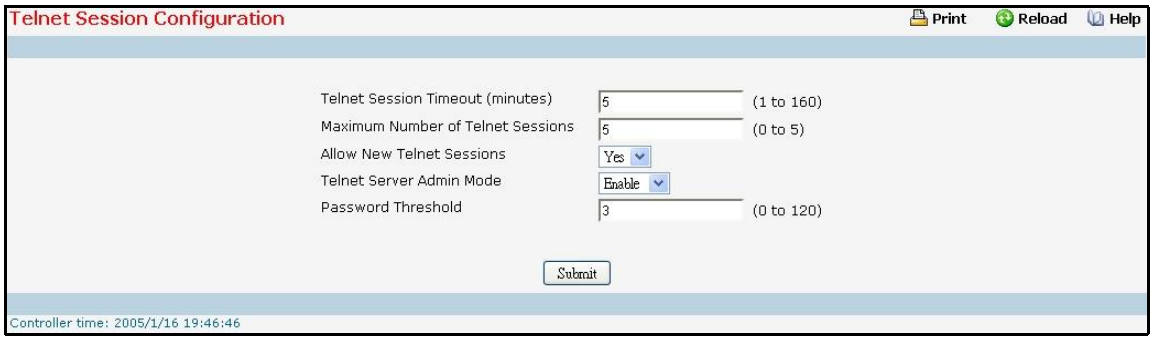
HTTP Session Hard Timeout - This field is used to set the hard timeout for HTTP sessions. This timeout is unaffected by the activity level of the session. The value must be in the range of (0 to 168) hours. A value of zero corresponds to an infinite timeout. The default value is 24 hours. The currently 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.

11.2.2.9 Configuring Telnet Session Page



Selection Criteria

Maximum Number of Telnet Sessions - Use the pull down 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 to 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

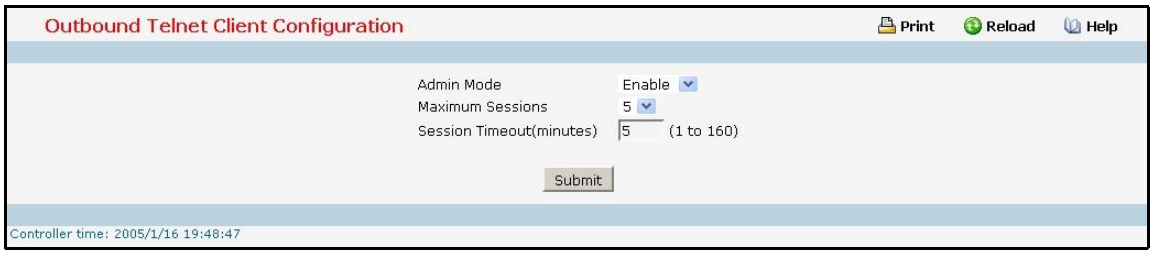
Telnet Session Timeout (minutes) - Specify how many minutes of inactivity should occur on a telnet session before the session is logged off. You may enter any number from 1 to 160. The factory default is 5.

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.

11.2.2.10 Configuring Outbound Telnet Client Configuration Page



Selection Criteria

Admin Mode - Specifies if the Outbound Telnet service is Enable or Disable. Default value is Enable.

Maximum Sessions - Specifies the maximum number of Outbound Telnet Sessions allowed. Default value is 5. Valid Range is (0 to 5).

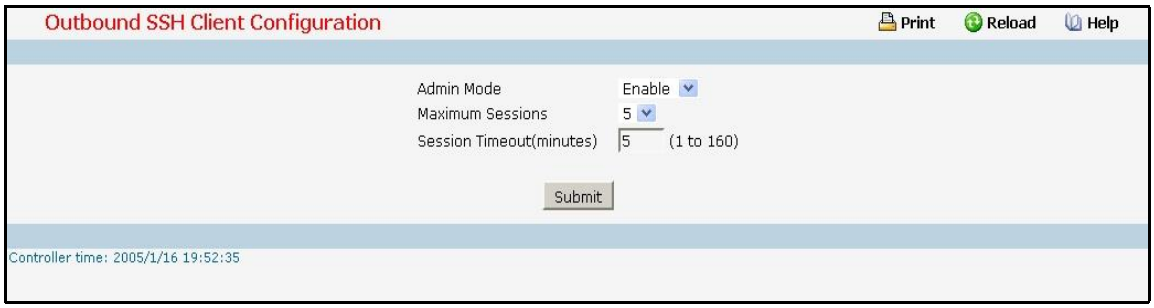
Configurable Data

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.

11.2.2.11 Configuring Outbound SSH Client Configuration Page



Selection Criteria

Admin Mode - Specifies if the Outbound Telnet service is Enable or Disable. Default value is Enable.

Maximum Sessions - Specifies the maximum number of Outbound Telnet Sessions allowed. Default value is 5. Valid Range is (0 to 5).

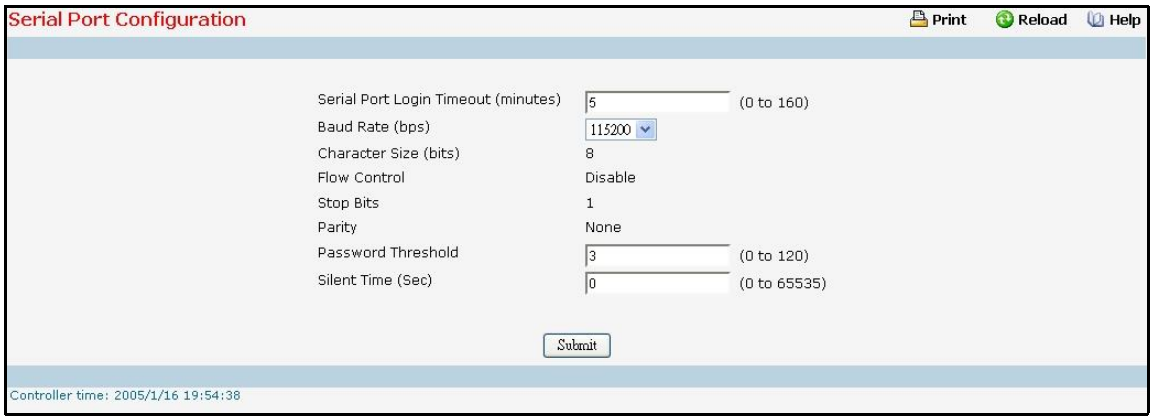
Configurable Data

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.

11.2.2.12 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 115200 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 Managing System Utilities

11.2.3.1 Saving All Configuration Changed Page

Command Buttons

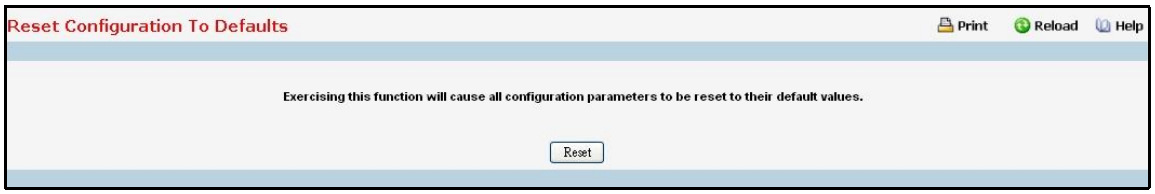
Save - Click this button to have configuration changes you have made saved across a system reboot. All changes submitted since the previous save or system reboot will be retained by the switch.

11.2.3.2 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.

11.2.3.3 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.

11.2.3.4 Erase Startup Configuration File

Command Buttons

Erase - Erase the text-based configuration file stored in non-volatile memory. You will be shown a confirmation screen after you select the button.

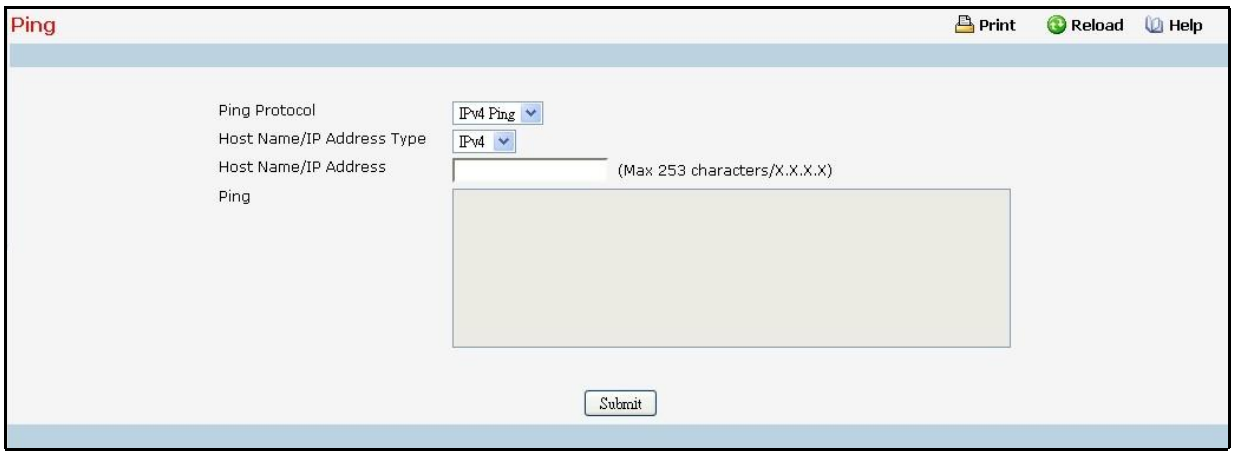
11.2.3.5 Resetting the Passwords to Default Values Page

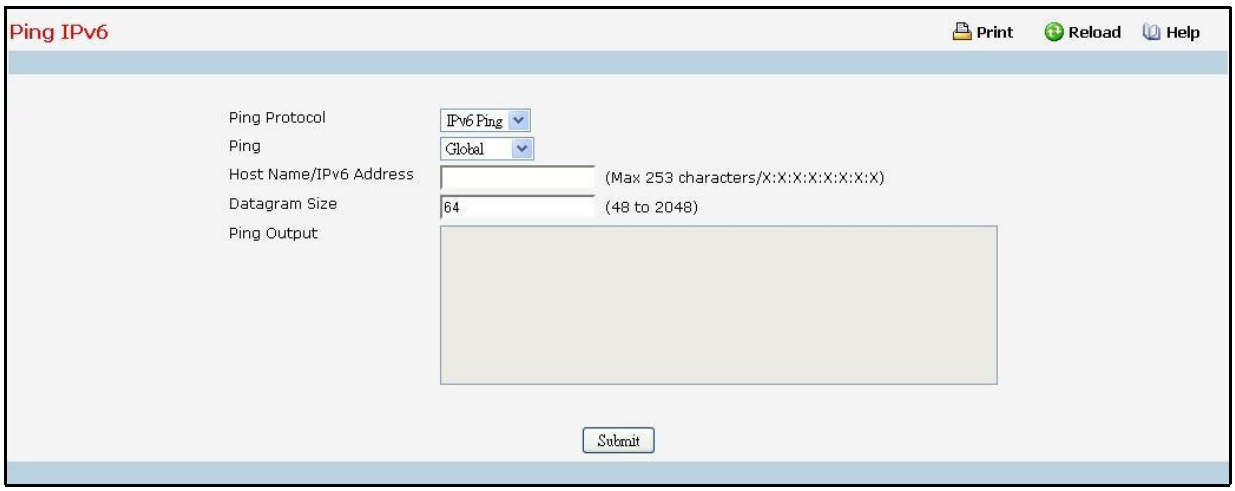
Command Buttons

Reset - Select this button to have all passwords reset to their factory default values.

11.2.3.6 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

Ping Protocol - Select using which type of address type (IPv4/IPv6) to ping

Interface - Select an IPv6 interface

Ping - Select ‘Global’ or ‘Link Local’ for IPv6 Ping

Configurable Data

Host Name/IP Address Address Type - Select the address type for IPv4/IPv6 Address or Host Name.

Host Name/IP Address - Enter the IP Address or Host Name of the station you want the switch to ping. The initial value is blank. The IP Address or Host Name you enter is not retained across a power cycle. Hostnames are composed of series of labels concatenated with dots. Each label must be between 1 and 63 characters long, and the entire hostname has a maximum of 255 characters.

Host Name/IPv6 Address - Enter the IPv6 address or Hostname of the station you want the switch to ping. The initial value is blank. The IPv6 Address or Hostname you enter is not retained across a power cycle.

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 - The reply result received from switch.

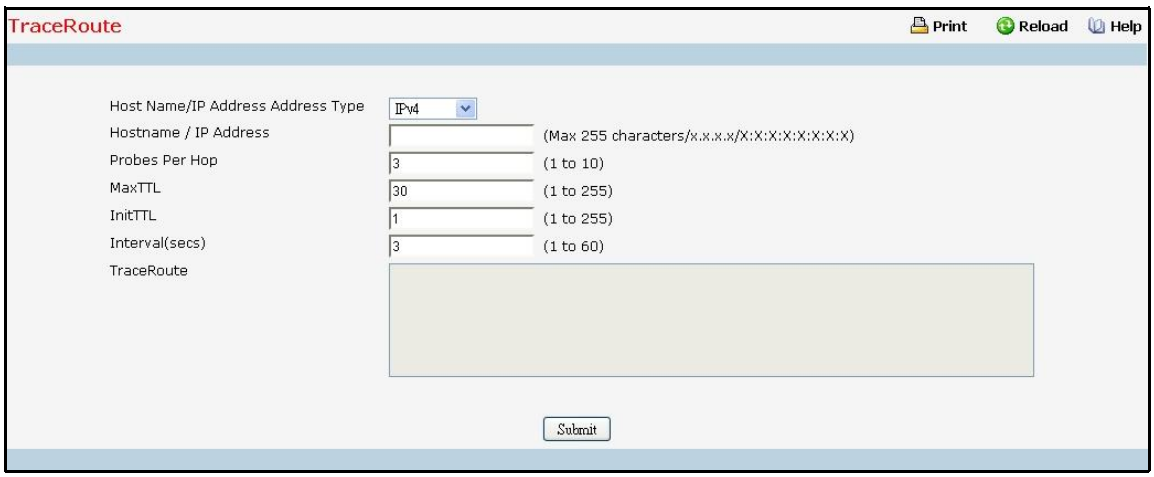
Command Buttons

Submit - This will initiate the Ping.

11.2.3.7 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.



Configurable Data

Host Name/IP Address Address Type- Select the address type for IPv4 Address or Host Name.

IPv4 - Select the way "IPv4 Address" to trace.

IPv4 DNS- Select the way "host name" to trace.

IPv6 DNS- Select the way "Host Name V6" to trace.

IPv6 - Select the way "IPv6 Address" to trace.

IP Address/Hostname - Enter the IP address or Hostname of the station you want the switch to discover path. The initial value is blank. Hostnames are composed of series of labels concatenated with dots. Each label must be between 1 and 63 characters long, and the entire hostname has a maximum of 255 characters. The IP Address or Hostname 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.

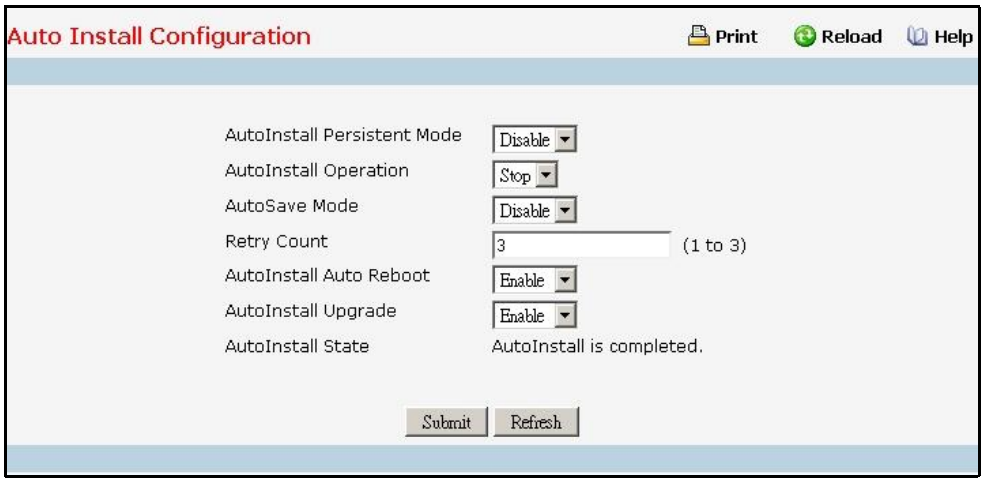
Command Buttons

Submit - This will initiate the traceroute.

11.2.3.8 Auto Install Function

The AutoInstall feature enables automatic firmware image installation and configuration of a switch when the device is turned on and, during the boot process. Automatic installation of the image and configuration file can also occur if the switch is booted from a saved configuration with the AutoInstall Persistent mode enabled.

Use this menu to configure the parameters for Auto Install which is used to upgrade the configuration and image of the switch automatically.



Configurable Data

AutoInstall Persistent Mode - An indication of whether the AutoInstall persistent mode is currently enabled or disabled.

AutoInstall Operation - An indication of whether the AutoInstall operational mode is currently started or stopped.

AutoSave Mode - An indication of whether the AutoSave is currently enabled or disabled.

Retry Count - Number of times the unicast TFTP tries should be made for the DHCP specified file before falling back for broadcast TFTP tries. The range of the Retry Count is (1 to 3). The default is 3.

AutoInstall Auto Reboot - An indication of whether the AutoReboot is currently enabled or disabled.

AutoInstall Upgrade - Enable/Disable to allow only the newer image version.

Non-Configurable Data

AutoInstall State - The current status of the AutoInstall process.

Command Buttons

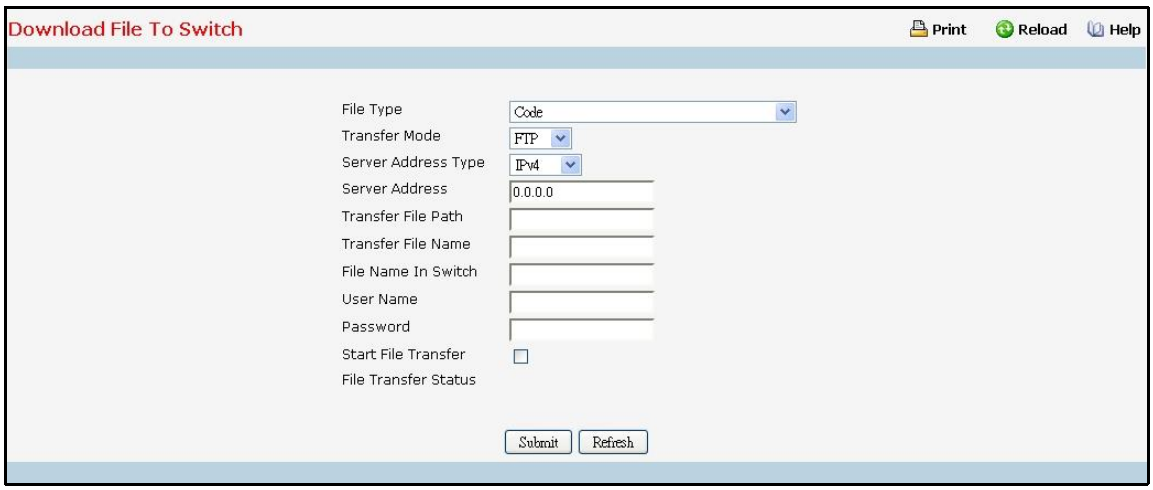
Submit - Update the switch with the values on the screen. If you want the switch to retain the new values across a power cycle you must perform a save.

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

11.2.4 File Management

11.2.4.1 Downloading File to Switch Page

Use this menu to download a file to the switch.



Configurable Data

File Type - Specify what type of file you want to download:

Config 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.

Transfer Mode - Specify the protocol of mode to upload. The available options are FTP and TFTP.

Server Address Type - Specify either IPv4 or IPv6 or DNS to indicate the format of the TFTP/FTP Server Address field. The factory default is IPv4.

User Name - Specify the user account of the FTP site.

User Password - Specify the user password of the FTP site.

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

Link-Local Address - Indicate whether to use IPv6 link local address to transfer.

Transfer File Path - Enter the path on the TFTP server where the selected file is located. You may enter up to 160 characters. The factory default is blank.

Transfer File Name - Enter the name on the TFTP server of the file you want to download. You may enter up to 32 characters. The factory default is blank.

File Name In Switch - 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

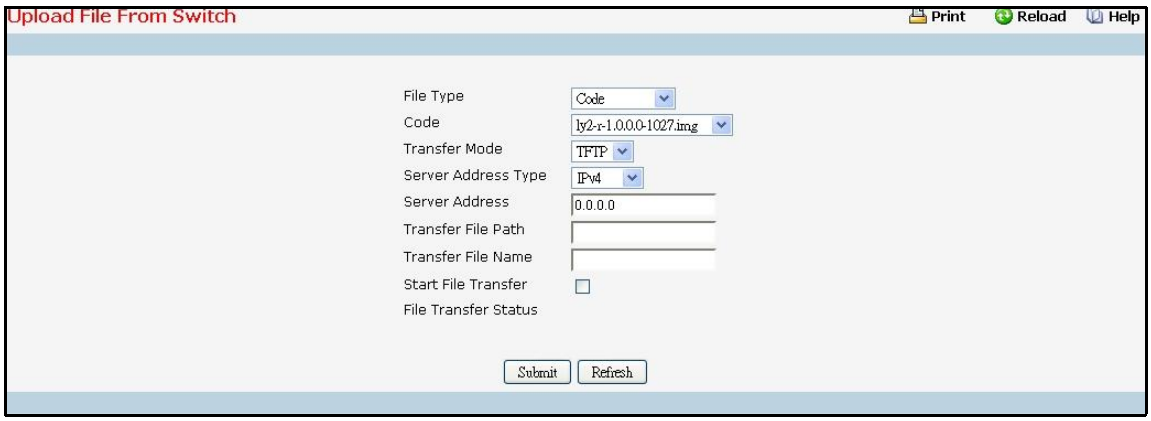
The last row of the table is used to display information about the progress of the file transfer. The screen will refresh automatically until the file transfer completes.

Command Buttons

Submit - Send the updated screen to the switch and perform the file download.

11.2.4.2 Uploading File from Switch Page

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



Configurable Data

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.

Transfer Mode - Specify the protocol of mode to upload. The available options are FTP and TFTP.

User Name - Specify the user account of the FTP site.

Password - Specify the user password of the FTP site.

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

Link-Local Address - Indicate whether to use IPv6 link local address to transfer.

Transfer File Path - Enter the path on the TFTP server where you want to put the file being uploaded. You may enter up to 160 characters. The factory default is blank.

Transfer File Name - Enter the name you want to give the file being uploaded. You may enter up to 30 characters. The factory default is blank.

Code/Cofiguration/Config Script - 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

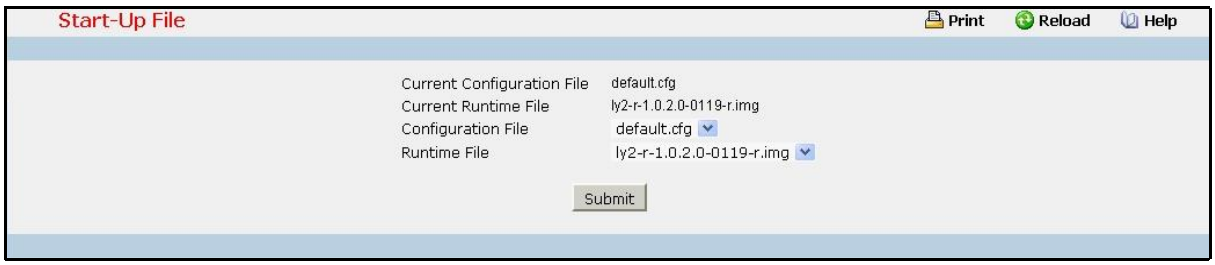
The last row of the table is used to display information about the progress of the file transfer. The screen will refresh automatically until the file transfer completes.

Command Buttons

Submit - Send the updated screen to the switch and perform the file upload.

11.2.4.3 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.

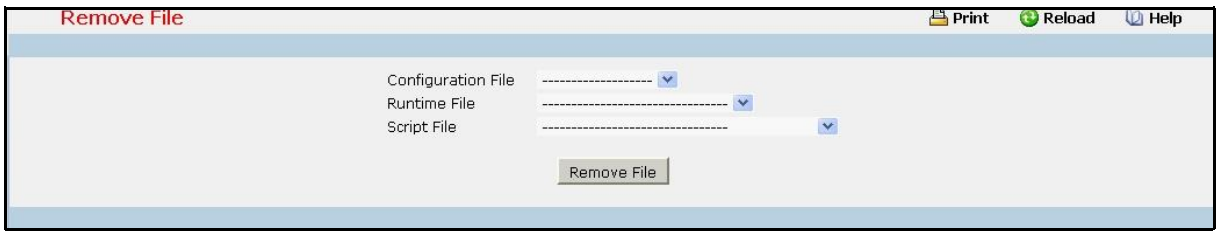
Current Runtime File - Current Run-time operation codes.

Command Buttons

Submit - Send the updated screen to the switch and specify the file start-up.

11.2.4.4 Removing 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.

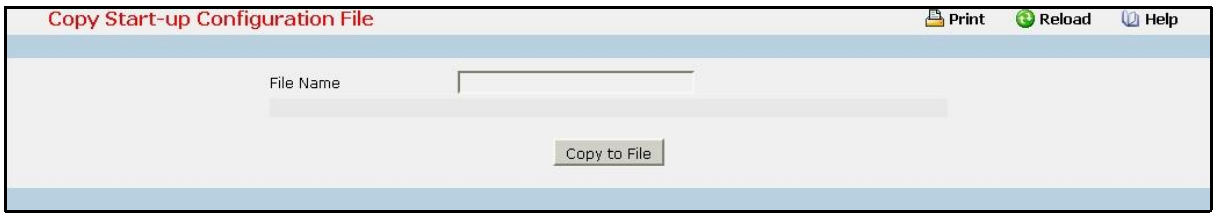
Script File - Configuration script files.

Command Buttons

Remove File - Send the updated screen to the switch and perform the file remove.

11.2.4.5 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.

11.2.5 User Management

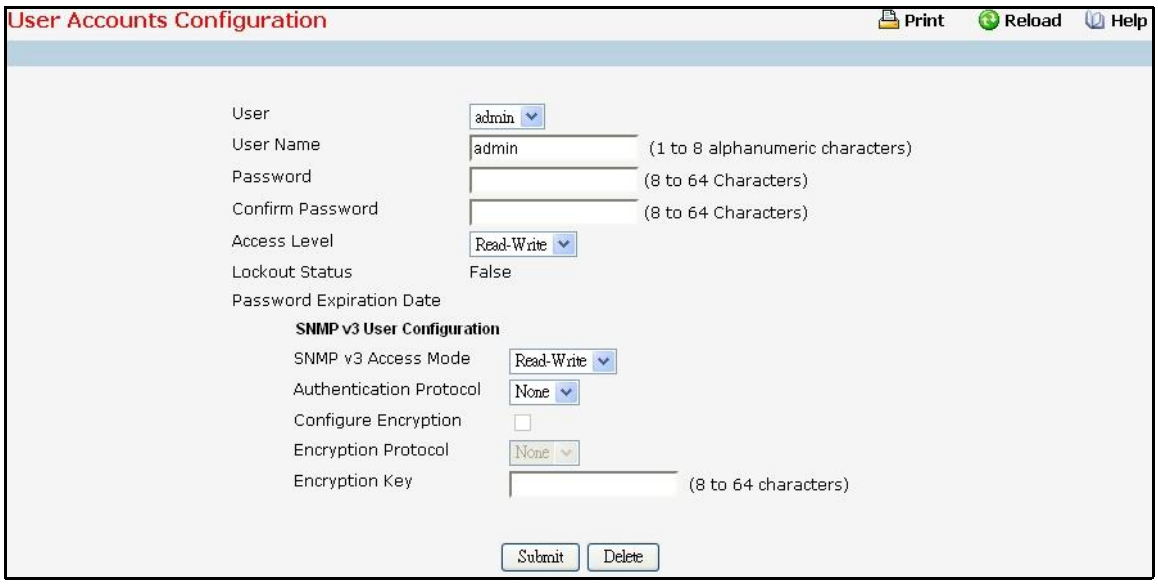
11.2.5.1 Defining User Accounts Page

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

Access Level - User access level. The lowest user access level is 1 (Read-Only), and 15 (Read-Write) is the highest. To suspend a user's access, set level to 0 (only a level 15 user has this ability).

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 (*).

Configure Encryption - The check box must be checked in order to change the Encryption Protocol and Encryption Key.

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

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.

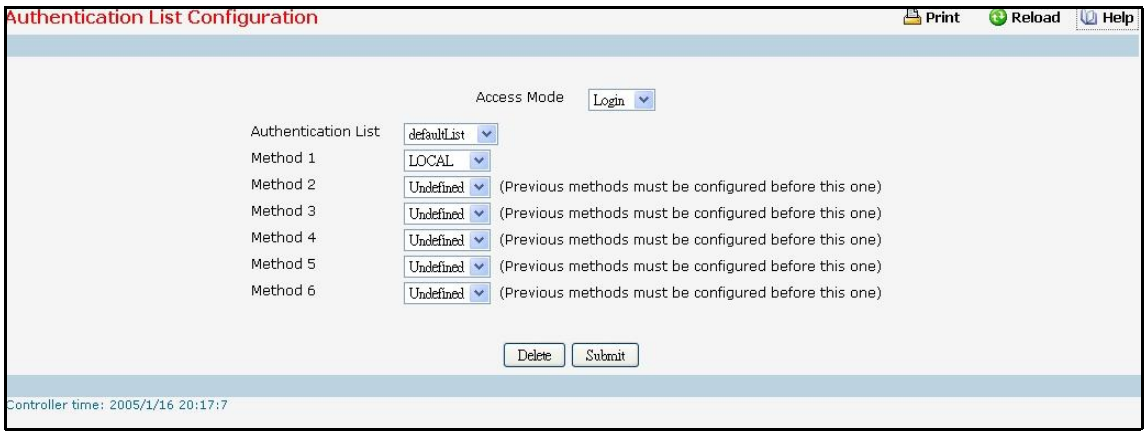
Command Buttons

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.

11.2.5.2 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.



Access Mode- A login list or enable 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

Authentication List - Select the authentication list you want to configure. Use dropdown menu to select defaultList, networkList, enableList, Create. Select 'create' to define a new list. When you create a new list, 'undefined' is set initially.

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:

Enable- uses the enable password for authentication.

Line- uses the Line password for authentication.

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

None- no authentication is used.

Undefined- the authentication method is unspecified (this may not be assigned as the first method)

LDAP- the user's ID and password will be authenticated using the LDAP server.

Method 2 -Use the dropdown menu to select the method, if any, that should appear second in the selected authentication 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.

Method 3 -Use the dropdown menu to select the method, if any, that should appear second in the selected authentication 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.

Method 4 - Use the dropdown menu to select the method, if any, that should appear fourth in the selected authentication list. This is the method that will be used if the third method times out. If you select a method that does not time out as the fourth method, the fifth method will not be tried.

Method 5 - Use the dropdown menu to select the method, if any, that should appear fifth in the selected authentication list. This is the method that will be used if the fourth method times out. If you select a method that does not time out as the fifth method, the sixth method will not be tried.

Method 6 - Use the dropdown menu to select the method, if any, that should appear sixth in the selected authentication 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.

11.2.5.3 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.

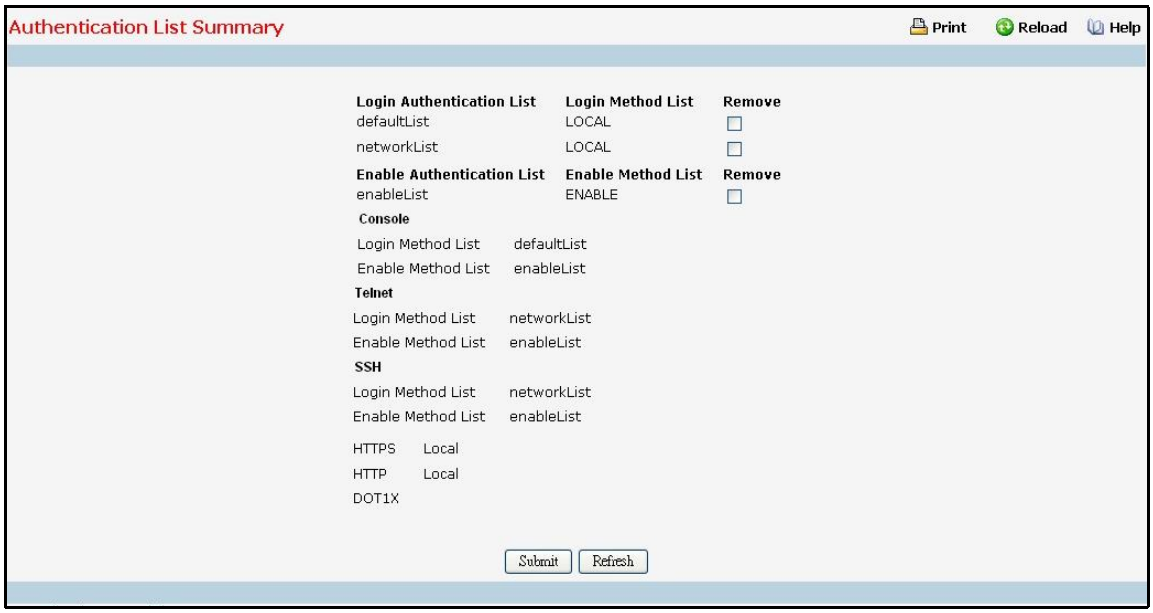
Session Time - Shows the total session time.

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

Command Buttons

Refresh - Refresh the information on the page.

11.2.5.4 Viewing Authentication List Summary Page



Non-Configurable Data

Login Authentication List - Shows the Login authentication profiles.

Enable Authentication List - Shows the Enable authentication profiles.

Login/Enable Method List - User authentication methods. Possible options are:

(1) Enable - uses the enable password for authentication.

(2) Line - uses the Line password for authentication.

(3) Local - the user's locally stored ID and password will be used for authentication

(4) None - the user is not authenticated

(5) Radius - the user's ID and password will be authenticated using the RADIUS server instead of locally

(6) TACACS+ - the user's ID and password will be authenticated using the TACACS+ server

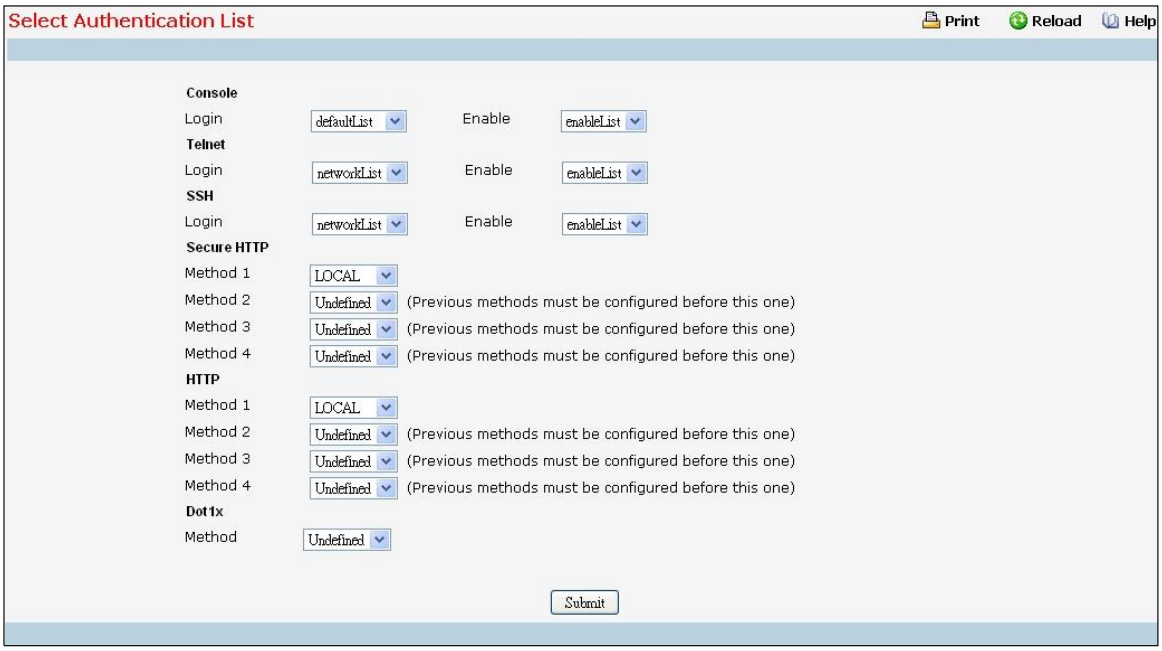
(7) LDAP - the user's ID and password will be authenticated using the LDAP server

The Authentication Lists and Authentication Methods configured for each List of Console, Telnet, SSH, HTTPS, HTTP and DOT1X are displayed respectively.

Command Buttons

Refresh - Update the information on the page. Summit- 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.

11.2.5.5 Configuring Authentication List



Configurable Data

Console - Authentication profiles used to authenticate console users.

Login or Enable - Specify the login list and enable list which will be used to validate switch or port access for the users associated with the list

Telnet - Authentication profiles used to authenticate Telnet users.

Login or Enable - Specify the login list and enable list which will be used to validate switch or port access for the users associated with the list.

Secure Telnet (SSH) - Authentication profiles used to authenticate Secure Shell (SSH) users. SSH provides clients secure and encrypted remote connections to a device

Login or Enable - Specify the login list and enable list which will be used to validate switch or port access for the users associated with the list.

HTTP and Secure HTTP - Authentication method used for HTTP access and Secure HTTP access, respectively. Possible field values are:

Method 1 - Use the dropdown menu to select the method that should appear first in the selected authentication 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. The options are:

Undefined - the authentication method is disabled (this may not be assigned as the first method)

Enable - uses the enable password for authentication.

Line - uses the Line password for authentication.

Local - the user's locally stored ID and password will be used for authentication

None - the user is not authenticated

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

LDAP - the user's ID and password will be authenticated using the LDAP server

Method 2 - Use the dropdown menu to select the method, if any, that should appear second in the selected authentication 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.

Method 3 - Use the dropdown menu to select the method, if any, that should appear third in the selected authentication list. This is the method that will be used if the second method times out. If you select a method that does not time out as the third method, the fourth method will not be tried.

Method 4 - Use the dropdown menu to select the method, if any, that should appear fourth in the selected authentication list.

DOT1X - Authentication method used for Dot1x access. Possible field values are:

Method - Use the dropdown menu to select the method that should appear in the selected authentication list. The options are:

Undefined - the authentication method is disabled.

IAS - the user's ID and password in Internal Authentication Server Database will be used for authentication

Local - the user's locally stored ID and password will be used for authentication.

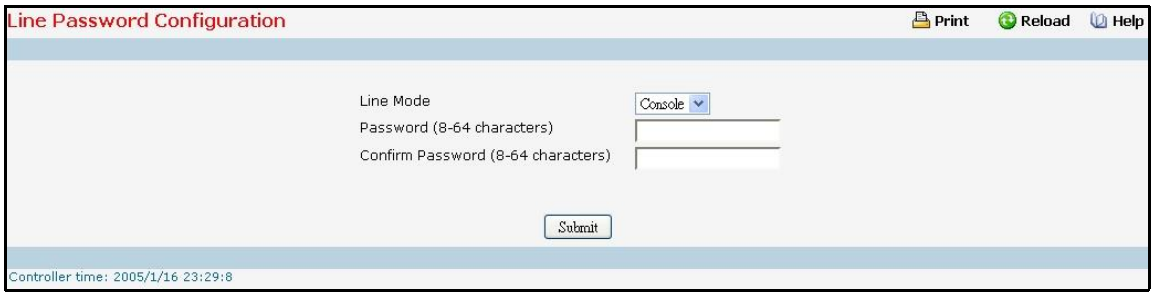
None - the user is not authenticated.

Radius - the user's ID and password will be authenticated using the RADIUS serve

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

11.2.5.6 Configuring Line Password



Configuration Data

Line Mode - Select the line mode from the drop-down list.

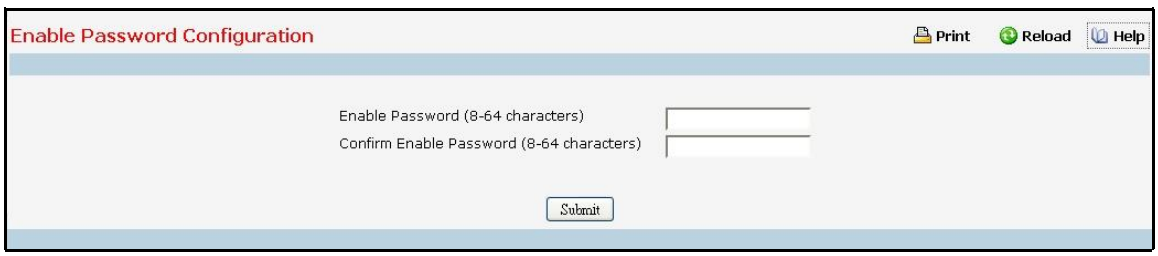
Line Password (8-64 characters) - The line password for accessing the device via a console, Telnet, or Secure Telnet session.

Confirm Password (8-64 characters) - Confirms the new line password. The password appears in the ..... format or ***** based on the browser used.

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.

11.2.5.7 Configuring Enable Password



Configuration Data

Enable Password (8-64 characters) - The enable password is for accessing the device via a console, Telnet, or Secure Telnet session.

Confirm Enable Password (8-64 characters) - Confirms the new enable password. The password appears in the ..... format or ***** based on the browser used.

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.

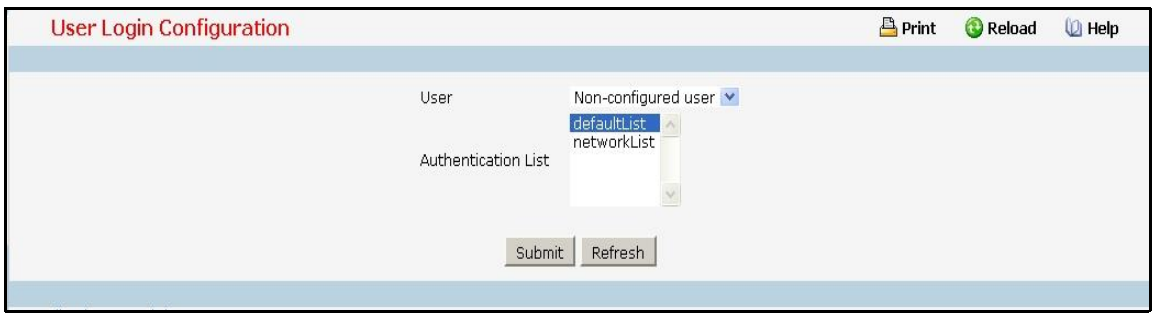
11.2.5.8 Defining User Login Page

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

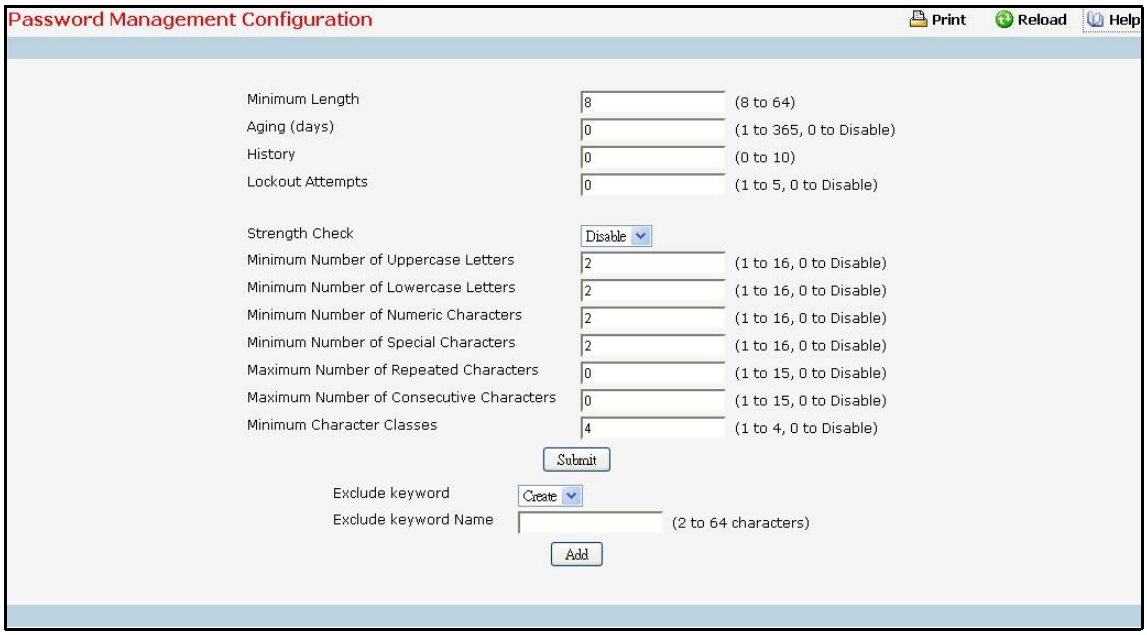
Authentication List - Select the authentication login list you want to assign to the user for system login.

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.

11.2.5.9 Defining Password Management



Configurable Data

Minimum Length - Valid range for user passwords is (8 to 64) characters in length. Default value is 8.

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.

Lockout Attempts - The number of allowable failed local authentication attempts before the user's account is locked. The value ranges from (1 to 5). A value of 0 indicates that user accounts will never be locked. Default value is 0.

Strength Check - Enable or disable the password strength check feature. Enabling this feature forces the user to configure passwords that comply with the strong password configuration. Default value is Disable.

History - The number of previous passwords to store for prevention of password reuse. This ensures that each user does not reuse passwords often. The value ranges from (0 to 10). A value of 0 indicates that no previous passwords will be stored. Default value is 0.

Lockout Attempts - The number of allowable failed local authentication attempts before the user's account is locked. The value ranges from (1 to 5). A value of 0 indicates that user accounts will never be locked. Default value is 0.

Minimum Number of Uppercase Letters - Valid range for user passwords is (0 to 16) number of characters. Default value is 2.

Minimum Number of Lowercase Letters - Valid range for user passwords is (0 to 16) number of characters. Default value is 2.

Minimum Number of Numeric Characters - Valid range for user passwords is (0 to 16) number of characters. Default value is 2.

Minimum Number of Special Characters - Valid range for user passwords is (0 to 16) number of characters. Default value is 2

Maximum Number of Repeated Characters - Valid range for user passwords is (0 to 15) number of characters. Default value is 0.

Maximum Number of Consecutive Characters - Valid range for user passwords is (0 to 15) number of characters. Default value is 0.

Minimum Character Classes - Valid range for user passwords is (0 to 4) number of characters. Default value is 4.

Exclude Keyword - The password to be configured should not contain the keyword mentioned in this field. The valid range for the keyword is (2 to 64) characters in length.

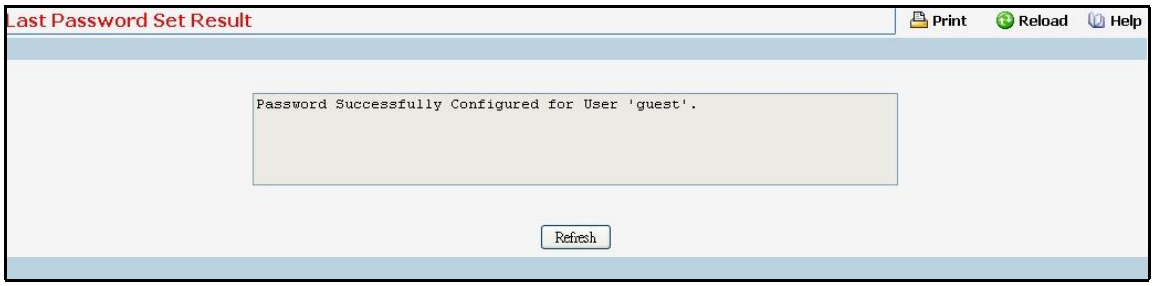
Exclude Keyword Name - This field appears only on selection of create option from 'Exclude Keyword' combo box. The valid range for the keyword is (2 to 64) characters in length.

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.

Add/Delete - Add or Delete the exclude keyword.

11.2.5.10 Last Password Set Result



Non-Configurable Data

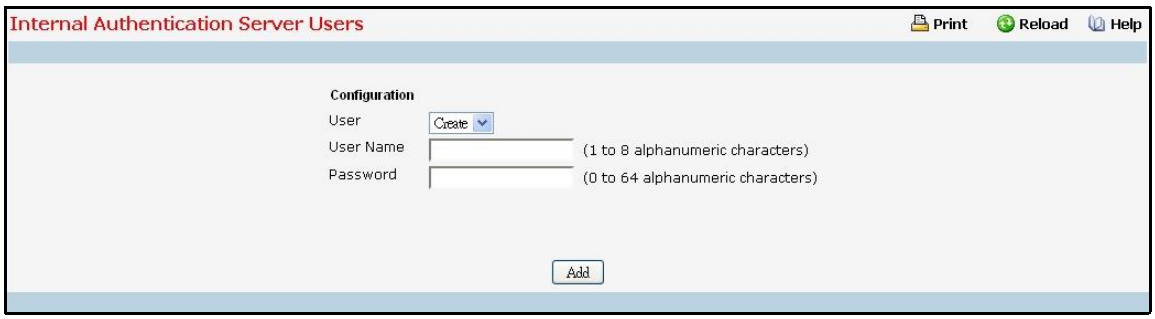
Last Password Set Result - Displays the last (User/Line/Enable) Password configuration result.

Command Buttons

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

11.2.5.11 Defining Internal Authentication Server Users

Use this page to configure Internal Authentication Server Users.



Selection Criteria

User - You can use this screen to reconfigure an existing account, or to create a new one. Use this pull-down menu to select one of the existing accounts, or select 'Create' to add a new one, provided the maximum of 100 accounts has not been reached.

Configurable Data

User Name - Enter the name for the new user. User names can be up to 32 Alpha numeric 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. Passwords can be up to 64 characters in length, they are case sensitive and special characters are permitted.

Command Buttons

Add - This is used to create a new User Name. This button is visible only when the 'Create' option is selected in the 'User' field.

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 - Deletes the currently selected user account.

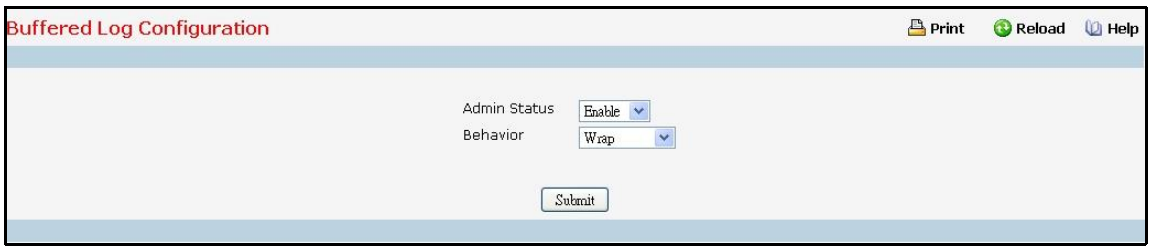
Clear All Users - Deletes all the created IAS users.

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

11.2.6 Viewing Logs

11.2.6.1 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.

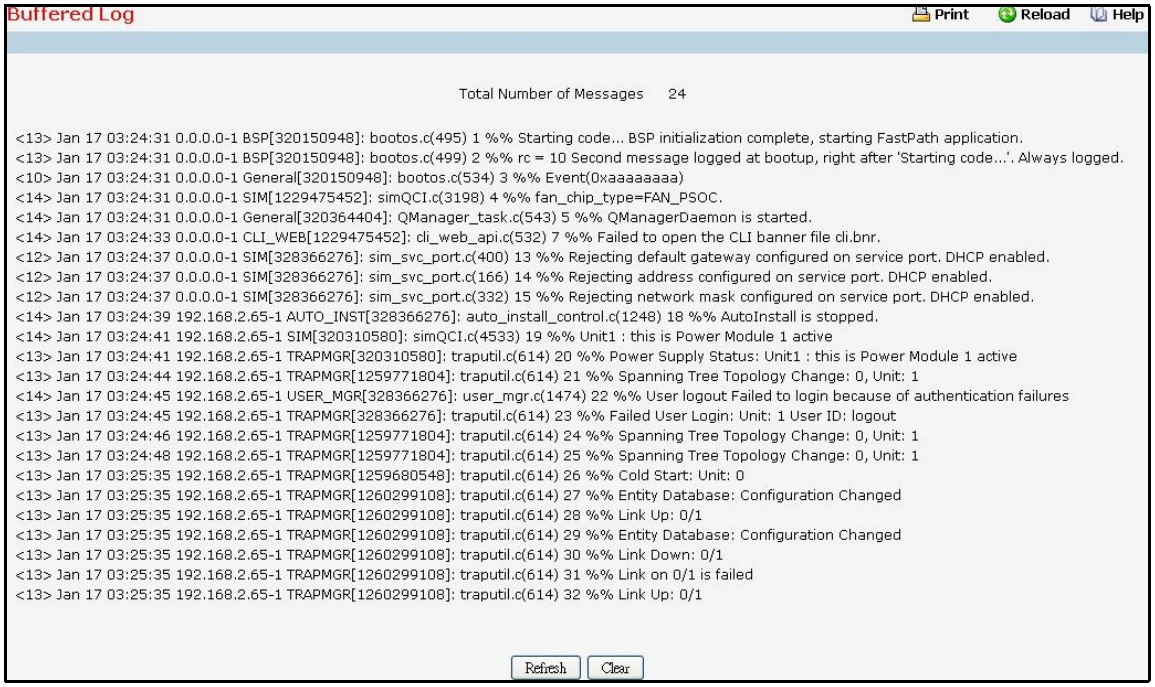
Behavior - Indicates the behavior of the log when it is full. It can either wrap around or stop when the log space is filled.

Command Buttons

Submit - Update the switch with the values you entered.

11.2.6.2 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

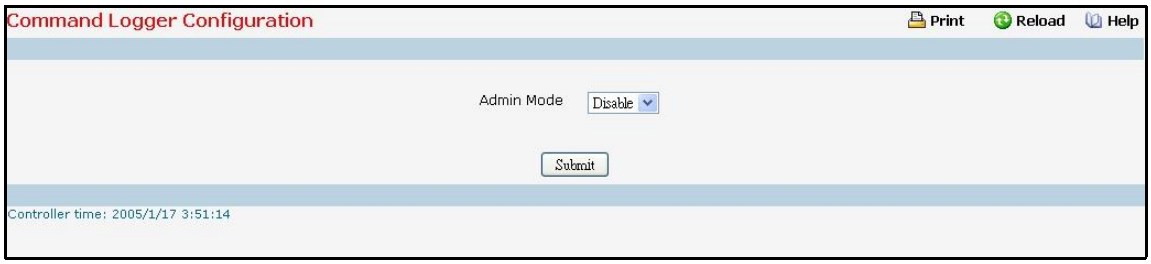
Number of log messages displayed: For the buffered log, only the latest 128 entries are displayed on the webpage

Command Buttons

Refresh - Refresh the page with the latest log entries.

Clear Log - Clear all entries in the log.

11.2.6.3 Configuring Command Logger Page



Configurable Criteria

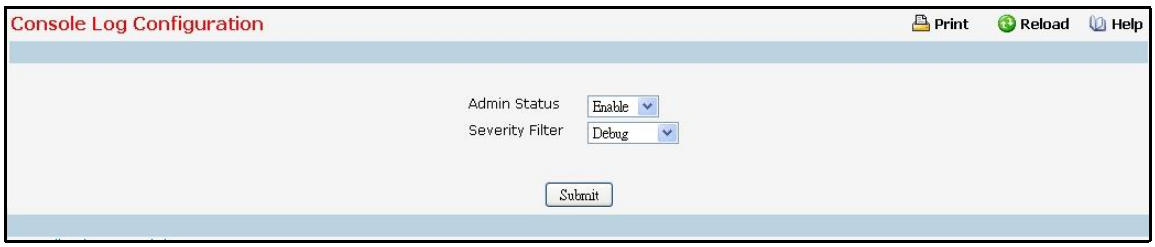
Admin Mode - Enable/Disable the operation of the CLI Command logging by selecting the corresponding pull-down field and clicking Submit.

Command Buttons

Submit - Update the switch with the values you entered.

11.2.6.4 Configuring Console Log Page

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



Configurable 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 pull-down 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 pull-down entry field. These severity levels have been enumerated below:

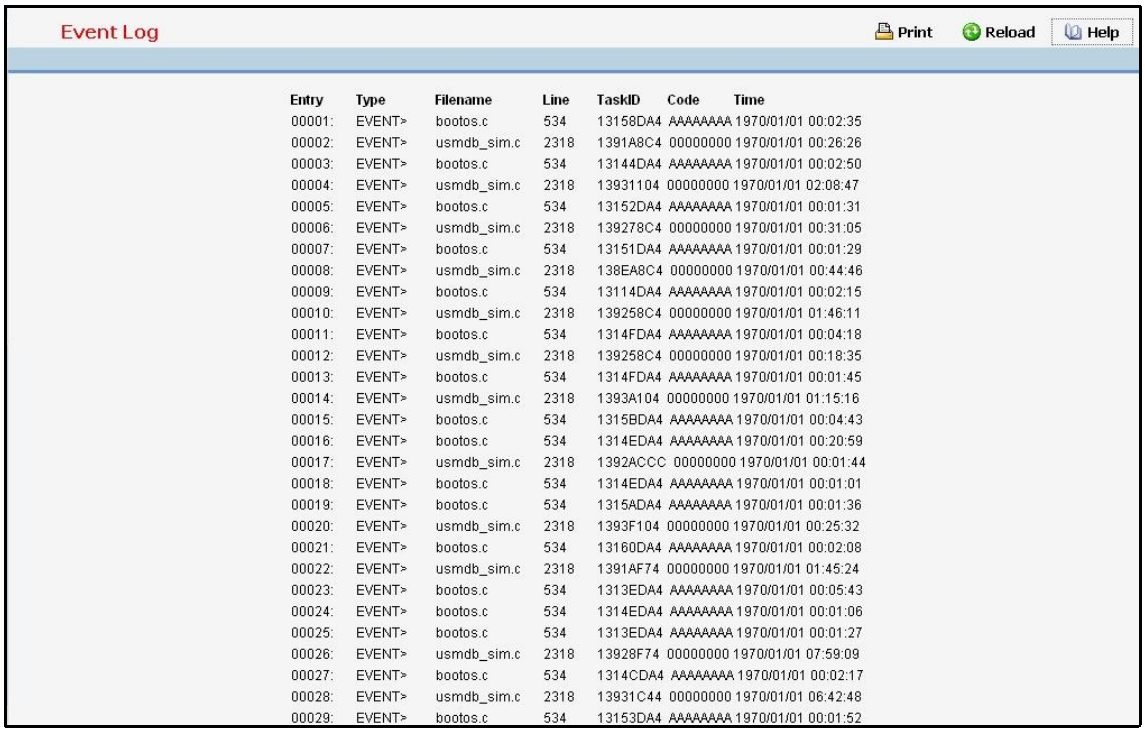
- Emergency (0): system is unusable
- Alert (1): action must be taken immediately
- Critical (2): critical conditions
- Error (3): error conditions
- Warning (4): warning conditions
- Notice(5): normal but significant conditions
- Info (6): informational messages
- Debug(7): debug-level messages

Command Buttons

Submit - Update the switch with the values you entered.

11.2.6.5 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	Type	Filename	Line	TaskID	Code	Time
00001:	EVENT>	bootos.c	534	13158DA4	AAAAAAAA	1970/01/01 00:02:35
00002:	EVENT>	usmdb_sim.c	2318	1391A8C4	00000000	1970/01/01 00:26:26
00003:	EVENT>	bootos.c	534	13144DA4	AAAAAAAA	1970/01/01 00:02:50
00004:	EVENT>	usmdb_sim.c	2318	13931104	00000000	1970/01/01 02:08:47
00005:	EVENT>	bootos.c	534	13152DA4	AAAAAAAA	1970/01/01 00:01:31
00006:	EVENT>	usmdb_sim.c	2318	139278C4	00000000	1970/01/01 00:31:05
00007:	EVENT>	bootos.c	534	13151DA4	AAAAAAAA	1970/01/01 00:01:29
00008:	EVENT>	usmdb_sim.c	2318	138EA8C4	00000000	1970/01/01 00:44:46
00009:	EVENT>	bootos.c	534	13114DA4	AAAAAAAA	1970/01/01 00:02:15
00010:	EVENT>	usmdb_sim.c	2318	139258C4	00000000	1970/01/01 01:46:11
00011:	EVENT>	bootos.c	534	1314FDA4	AAAAAAAA	1970/01/01 00:04:18
00012:	EVENT>	usmdb_sim.c	2318	139258C4	00000000	1970/01/01 00:18:35
00013:	EVENT>	bootos.c	534	1314FDA4	AAAAAAAA	1970/01/01 00:01:45
00014:	EVENT>	usmdb_sim.c	2318	1393A104	00000000	1970/01/01 01:15:16
00015:	EVENT>	bootos.c	534	1315BDA4	AAAAAAAA	1970/01/01 00:04:43
00016:	EVENT>	bootos.c	534	1314EDA4	AAAAAAAA	1970/01/01 00:20:59
00017:	EVENT>	usmdb_sim.c	2318	1392ACCC	00000000	1970/01/01 00:01:44
00018:	EVENT>	bootos.c	534	1314EDA4	AAAAAAAA	1970/01/01 00:01:01
00019:	EVENT>	bootos.c	534	1315ADA4	AAAAAAAA	1970/01/01 00:01:36
00020:	EVENT>	usmdb_sim.c	2318	1393F104	00000000	1970/01/01 00:25:32
00021:	EVENT>	bootos.c	534	13160DA4	AAAAAAAA	1970/01/01 00:02:08
00022:	EVENT>	usmdb_sim.c	2318	1391AF74	00000000	1970/01/01 01:45:24
00023:	EVENT>	bootos.c	534	1313EDA4	AAAAAAAA	1970/01/01 00:05:43
00024:	EVENT>	bootos.c	534	1314EDA4	AAAAAAAA	1970/01/01 00:01:06
00025:	EVENT>	bootos.c	534	1313EDA4	AAAAAAAA	1970/01/01 00:01:27
00026:	EVENT>	usmdb_sim.c	2318	13928F74	00000000	1970/01/01 07:59:09
00027:	EVENT>	bootos.c	534	1314CDA4	AAAAAAAA	1970/01/01 00:02:17
00028:	EVENT>	usmdb_sim.c	2318	13931C44	00000000	1970/01/01 06:42:48
00029:	EVENT>	bootos.c	534	13153DA4	AAAAAAAA	1970/01/01 00:01:52

Non-Configurable Data

Entry - The number of the entry within the event log. The most recent entry is first.

Filename - The 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.

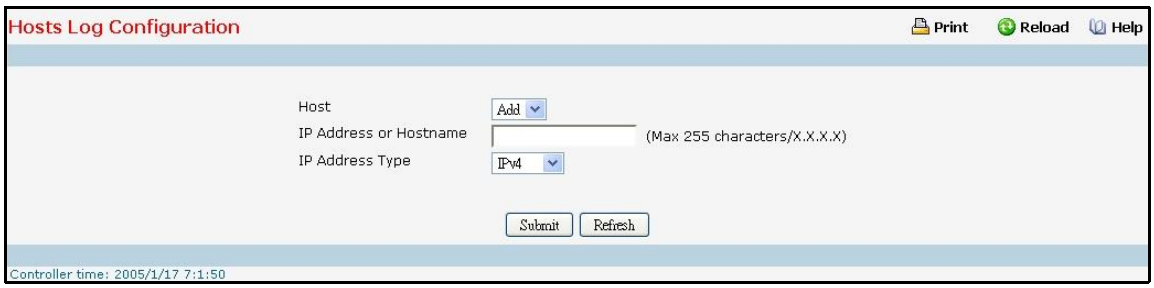
Time - The time the event occurred, measured from the previous reset.

Command Buttons

Refresh - Update the information on the page.

Clear Log - Remove all log information.

11.2.6.6 Configuring Hosts configuration Page



Configurable 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.

IP Address or Hostname - IP address or Hostname of the remote host for syslog. Available only during addition of a new Host. Host Names are composed of series of labels concatenated with dots. The labels must start with a letter, end with a letter or digit, and have as interior characters only letters, digits, and hyphen. Each Label must be 63 characters or less, and the entire Host name has a maximum of 255 characters. Refer RFC 1034 (3.5. Preferred name syntax) for specifying the Host names.

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 pull-down 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

IP Address Type - 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 whether the host has been configured to be actively logging or not.

Command Buttons

Submit - Update the switch with the values you entered.

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

Delete - Delete a configured host.

11.2.6.7 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.

Configurable 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 pull-down 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 pull-down entry field. These severity levels have been enumerated below:

- Emergency (0): system is unusable
- Alert (1): action must be taken immediately

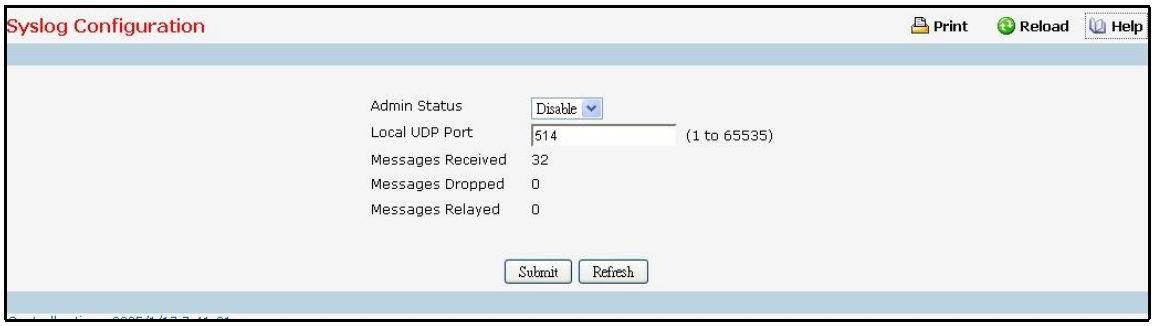
Critical (2): critical conditions

- 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.

11.2.6.8 Configuring syslog configuration Page



Configurable 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 pull-down entry field.

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.

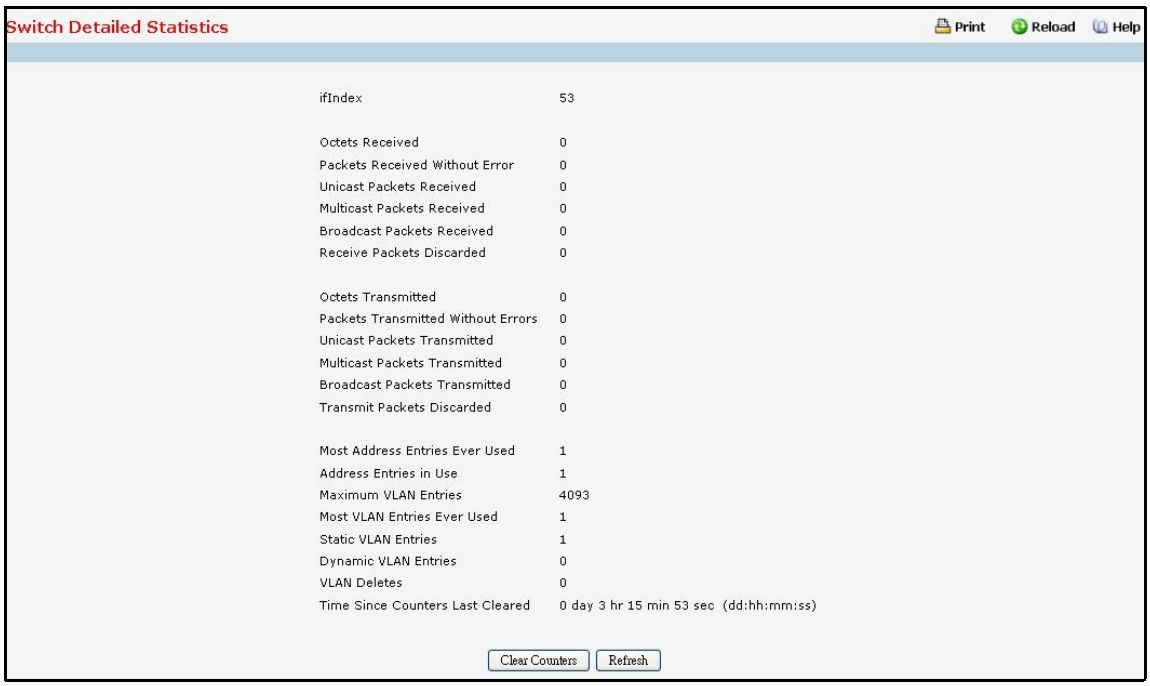
Command Buttons

Submit - Update the switch with the values you entered.

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

11.2.7 Viewing Statistics

11.2.7.1 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).

Packets Received Without Errors - The total number of packets (including broadcast packets and multicast packets) received by the processor.

Unicast Packets Received - The number of subnetwork-unicast packets delivered to a higher-layer protocol.

Multicast Packets Received - The total number of packets received that were directed to a multicast address. Note that this number does not include packets directed to the broadcast address.

Broadcast Packets Received - The total number of packets received that were directed to the broadcast address. Note that this does not include multicast packets.

Receive Packets Discarded - The number of inbound packets which were chosen to be discarded even though no errors had been detected to prevent their being deliverable to a higher-layer protocol. A possible reason for discarding a packet could be to free up buffer space.

Octets Transmitted - The total number of octets transmitted out of the interface, including framing characters.

Packets Transmitted Without Errors - The total number of packets transmitted out of the interface.

Unicast Packets Transmitted - The total number of packets that higher-level protocols requested be transmitted to a subnetwork-unicast address, including those that were discarded or not sent.

Multicast Packets Transmitted - The total number of packets that higher-level protocols requested be transmitted to a Multicast address, including those that were discarded or not sent.

Broadcast Packets Transmitted - The total number of packets that higher-level protocols requested be transmitted to the Broadcast address, including those that were discarded or not sent.

Transmit Packets Discarded - The number of outbound packets which were chosen to be discarded even though no errors had been detected to prevent their being deliverable to a higher-layer protocol. A possible reason for discarding a packet could be to free up buffer space.

Most Address Entries Ever Used - The highest number of Forwarding Database Address Table entries that have been learned by this switch since the most recent reboot.

Address Entries in Use - The number of Learned and static entries in the Forwarding Database Address Table for this switch.

Maximum VLAN Entries - The maximum number of Virtual LANs (VLANs) allowed on this switch.

Most VLAN Entries Ever Used - The largest number of VLANs that have been active on this switch since the last reboot.

Static VLAN Entries - The number of presently active VLAN entries on this switch that have been created statically.

Dynamic VLAN Entries - The number of presently active VLAN entries on this switch that have been created by GVRP registration.

VLAN Deletes - The number of VLANs on this switch that have been created and then deleted since the last reboot.

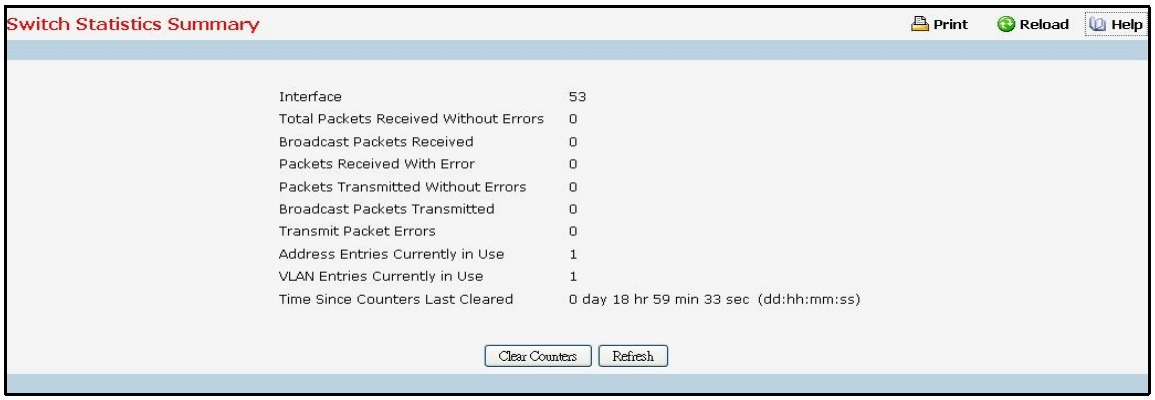
Time Since Counters Last Cleared - The elapsed time, in days, hours, minutes, and seconds, since the statistics for this switch were last cleared.

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.

11.2.7.2 Viewing the whole Switch Summary Statistics Page



Non-Configurable Data

Interface - This object indicates the interface index of the interface table entry associated with the Processor of this switch

Packets Received Without Errors - The total number of packets (including broadcast packets and multicast packets) received by the processor.

Broadcast Packets Received - The total number of packets received that were directed to the broadcast address. Note that this does not include multicast packets.

Packets Received with 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.

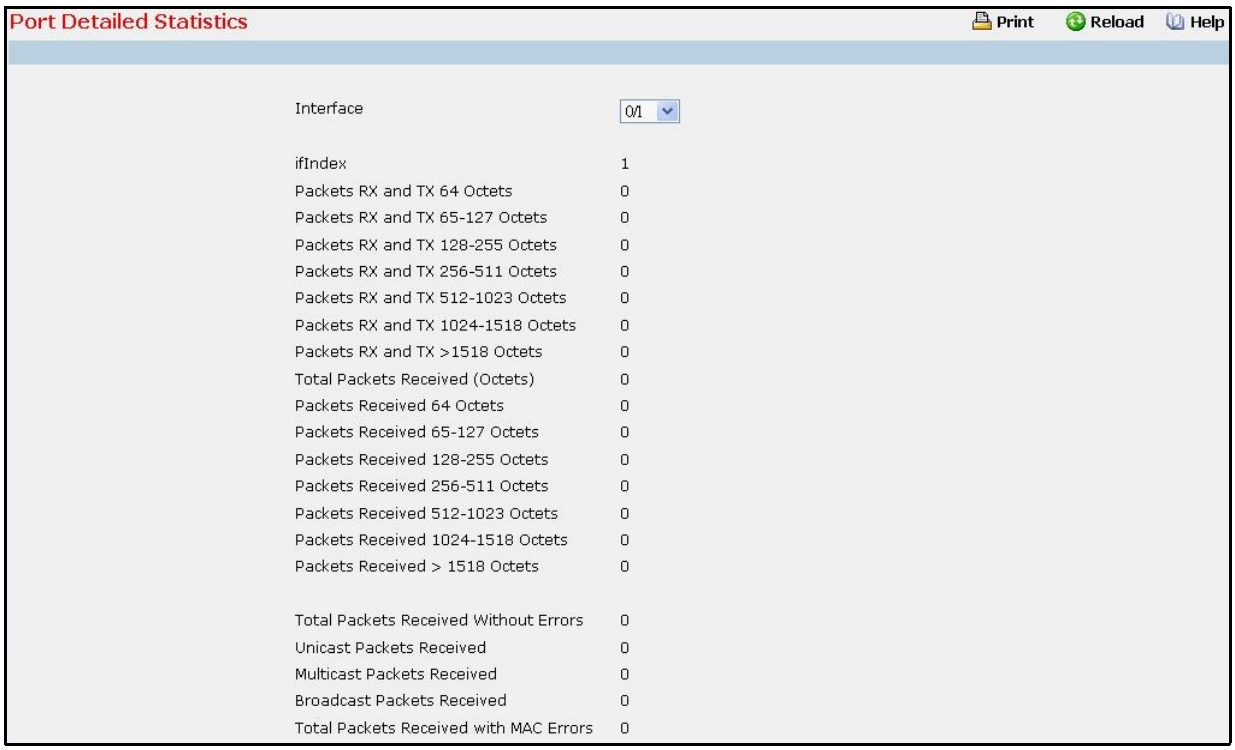
Time Since Counters Last Cleared - The elapsed time, in days, hours, minutes, and seconds since the statistics for this switch were last cleared.

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.

11.2.7.3 Viewing Each Port Detailed Statistics Page



Selection Criteria

Interface - 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 > 1518 Octets - The total number of packets (including bad packets) received or transmitted that were longer than 1518 octets in length (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 > 1518 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 20ms. The allowed range to detect jabber is between 20ms and 150ms.

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).

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).

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.

Receive Packets Discarded - A count of valid frames received which were discarded (i.e. filtered) by the forwarding process.

802.3x Pause Frames Received - A count of MAC Control frames received on this interface with an opcode indicating the PAUSE operation. This counter does not increment when the interface is operating in half-duplex mode.

Unacceptable Frame Type - The number of frames discarded from this port due to being an unacceptable frame type.

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) and were otherwise well formed. This counter has a max increment rate of 815 counts per sec at 10 Mb/s.

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 number of frames that exceeded the max permitted frame size. This counter has a max increment rate of 815 counts per sec at 10 Mb/s.

Underrun Errors - The total number of frames discarded because the transmit FIFO buffer became empty during frame transmission.

Total Transmit Packets Discarded - The sum of single collision frames discarded, multiple collision frames discarded, and excessive frames discarded.

Single Collision Frames - A count of the number of successfully transmitted frames on a particular interface for which transmission is inhibited by exactly one collision.

Multiple Collision Frames - A count of the number of successfully transmitted frames on a particular interface for which transmission is inhibited by more than one collision.

Excessive Collision Frames - A count of frames for which transmission on a particular interface fails due to excessive collisions.

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

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

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

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

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

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

802.3x Pause Frames Transmitted - A count of MAC Control frames transmitted on this interface with an opcode indicating the PAUSE operation. This counter does not increment when the interface is operating in half-duplex mode.

GVRP PDUs Received - The count of GVRP PDUs received in the GARP layer.

GVRP PDUs Transmitted - The count of GVRP PDUs transmitted from the GARP layer.

GVRP Failed Registrations - The number of times attempted GVRP registrations could not be completed.

GMRP PDUs Received - The count of GMRP PDUs received from the GARP layer.

GMRP PDUs Transmitted - The count of GMRP PDUs transmitted from the GARP layer.

GMRP Failed Registrations - The number of times attempted GMRP registrations could not be completed.

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 frames of any type that have been received by this Authenticator

Received PFC Frames - Displays the total number of received PFC frames on the selected interface.

Transmitted PFC Frames - Displays the total number of transmitted PFC frames by the selected interface.

Time Since Counters Last Cleared - The elapsed time, in days, hours, minutes, and seconds since the statistics for this port were last cleared.

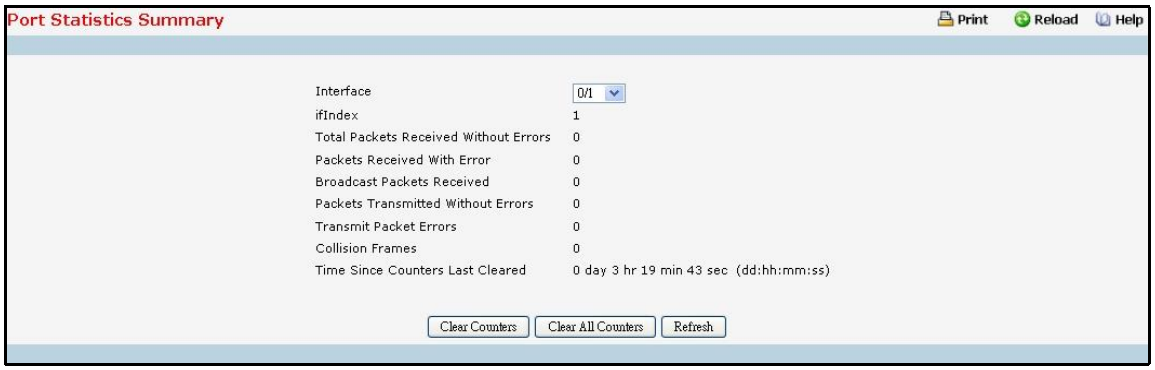
Command Buttons

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.

11.2.7.4 Viewing Each Port Summary Statistics Page



Selection Criteria

Interface - 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.

11.2.8 Managing SNMP and Trap

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.

Configurable Criteria

Community - You can use this screen to reconfigure an existing community, or to create a new one. Use this pull-down menu to select one of the existing community names, or select 'Create' to add a new one.

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

Community - 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.

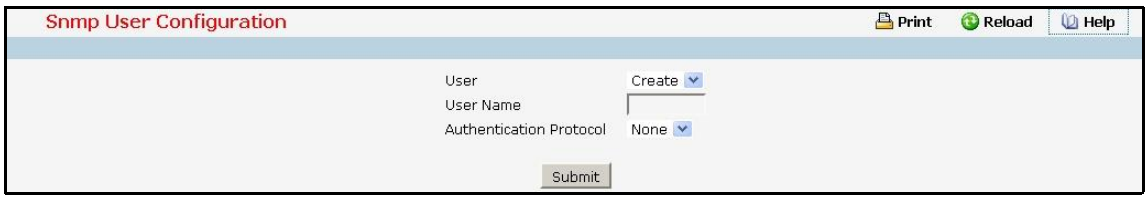
Command Buttons

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 User

This menu will display an entry for every SNMP user.



Selection Criteria

User - You can use this screen to reconfigure an existing SNMP user, or to create a new one. Use this pull-down menu to select one of the existing SNMP user, or select 'Create' to add a new one.

Configurable Data

Authentication Protocol - Specify the SNMPv3 Authentication Protocol setting for the selected user account. The valid Authentication Protocols are None, MD5 or SHA.

Encryption Protocol - Specify the SNMPv3 Encryption Protocol setting for the selected user account. The valid Encryption Protocol are None or DES.

User Name - Enter SNMP user name you want to create. (You can only enter data in this field when you are creating a new account.) User names are up to 8 characters in length and are case insensitive. Valid characters include all alphanumeric characters as well as the dash ('-') and underscore ('_') characters.

Authentication Password - Enter new or changed password for the authentication protocol for this SNMP user. Passwords are up to 64 alphanumeric characters in length and are case sensitive.

Encryption Password - Enter new or changed password for the encryption protocol for this SNMP user. Passwords are up to 64 alphanumeric characters in length and are case sensitive

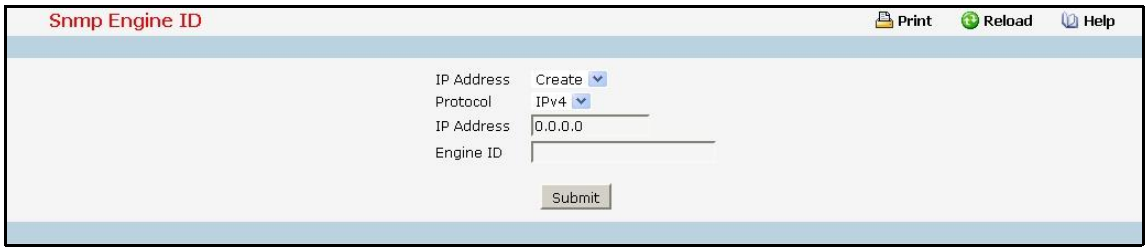
Command Buttons

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 SNMP User. If you want the switch to retain the new values across a power cycle, you must perform a save.

11.2.8.3 Configuring SNMP EngineID

This menu will display an entry for configuring remote EngineID.



Selection Criteria

IP Address - You can use this screen to reconfigure an existing host, or to create a new one. Use this pull-down menu to select one of the existing host, or select 'Create' to add a new one.

Configurable Data

Protocol - Select IPv4 or IPv6 to configure the corresponding attributes.

IP Address - Enter the IP address of SNMP host which will receive SNMP trap/inform from this switch. Enter 4 numbers between 0 and 255 separated by periods.

Engine ID - Enter new or changed Engine ID for the selected host. The Engine ID is up to 24 hexadecimal characters in length.

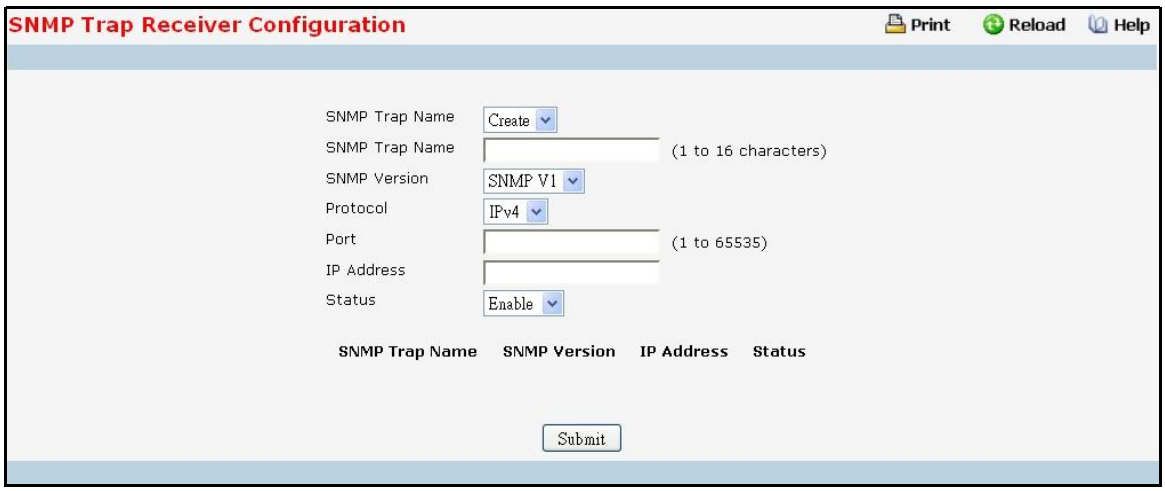
Command Buttons

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 SNMP Engine ID. If you want the switch to retain the new values across a power cycle, you must perform a save.

11.2.8.4 Configuring SNMP Trap Receiver Configuration Page

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



Configurable Data

SNMP Trap 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.

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.

SNMP v3 - Uses SNMP v3 to send traps to the receiver.

Protocol -This field allows the user to select the type of protocol used for the SNMP Trap Receiver Configuration.

IPv4 - Choose IPv4 to enter the address in IPv4 format.

IPv6 - Choose IPv6 to enter the address in IPv6 format.

DNS - Choose DNS to enter the address in DNS format.

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

Port - This field is used to set the SNMP Trap Port Number. The value must be in the range of 1 to 65535. The default port value is 162. The currently configured value is shown when the web page is displayed.

Status - Select the receiver's status from the pull-down menu:

Enable - send traps to the receiver.

Disable - do not send traps to the receiver.

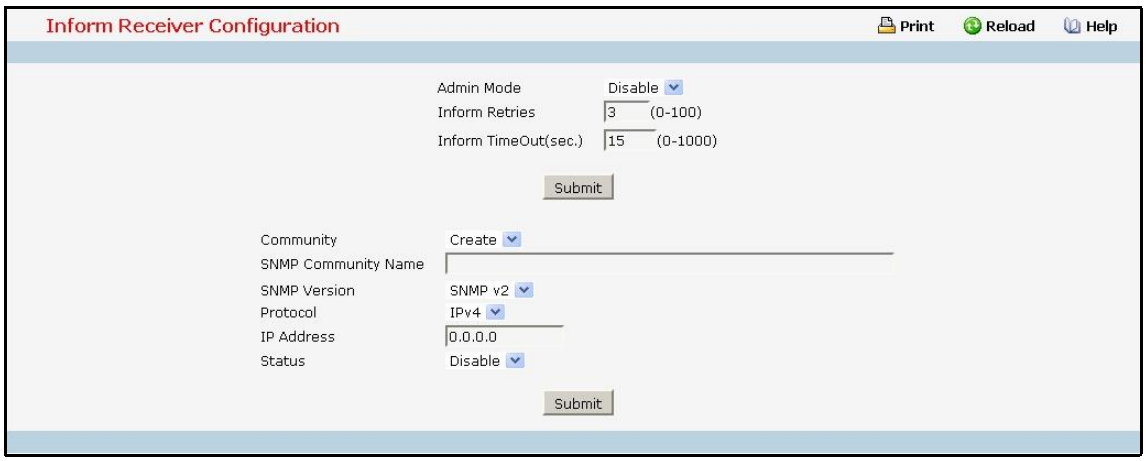
Command Buttons

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.

11.2.8.5 Inform Receiver Configuration

This menu will display an entry for every active SNMP Inform Receiver.



Selection Criteria

Community/User - You can use this screen to reconfigure an existing community or SNMP user, or to create a new one. Use this pull-down menu to select one of the existing community names or SNMP user, or select 'Create' to add a new one.

Configurable Data

Admin Mode - You can use this screen to enable or disable the inform function.

Inform Retries - Specify how many times to resend the inform. The valid retry value is 0 to 100. Default retry value is 3 times.

Inform Timeout - Specify how many seconds does the switch to wait for the inform ACK. If the inform ACK is not received within the configured timeout value, switch will resend the inform according to the retry setting. The valid timeout value is 0 to 1000 seconds. Default timeout value is 15 seconds.

SNMP Version - Select the inform version to be used by the receiver from the pull down menu:

SNMP v2 - Uses SNMP v2 to send informs to the receiver.

SNMP v3 - Uses SNMP v3 to send informs to the receiver.

Protocol - Select IPv4, IPv6 or DNS to configure the corresponding attributes.

Security Level - Select the SNMP User's security status from the pull-down menu:

noAuthNoPriv - Authentication Protocol is "None".

authNoPriv - Authentication Protocol is setting and Encryption Protocol is "None".

authPriv - Both Authentication Protocol and Encryption Protocol is setting.

Status - Select the receiver's status from the pull-down menu:

Enable - Send informs to the receiver

Disable - Do not send informs to the receiver.

11.2.8.6 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.

Configurable Data

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 pull-down entry field. The factory default is disabled.

DVMRP Traps - Enabled or disable activation of DVMRP traps by selecting the corresponding line on the pull-down entry field. The factory default is disabled.

PIM Traps - Enabled or disable activation of PIM traps by selecting the corresponding line on the pull-down entry field. The factory default is disabled.

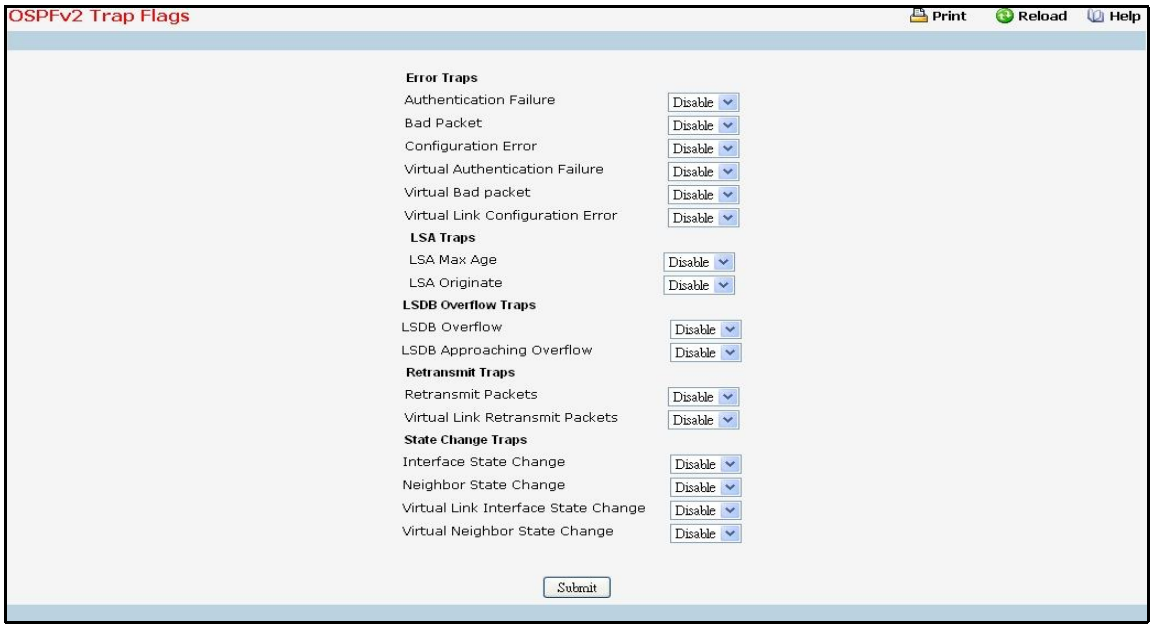
Captive Portal Trap Mode- Enable or disable activation of Captive Portal traps by selecting the corresponding line on the pull-down entry field. The factory default is disabled.

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.

11.2.8.7 OSPFv2 Trap Flags

Use the OSPFv2 Trap Flags page to specify which OSPFv2 traps you want to enable. When the condition identified by an active trap is encountered by the switch a trap message will be sent to any enabled SNMP Trap Receivers, and a message will be written to the trap log.



Configurable Data

Error Traps

Authentication Failure- his trap signifies that a packet has been received on a non-virtual interface from a router whose authentication key or authentication type conflicts with this router's authentication key or authentication type. The factory default is disabled.

Bad Packet- This trap signifies that an OSPF packet has been received on a non-virtual interface that cannot be parsed. The factory default is disabled.

Configuration Error- This trap signifies that a packet has been received on a non-virtual interface from a router whose configuration parameters conflict with this router's configuration parameters. The factory default is disabled.

Virtual Authentication Failure- This trap signifies that a packet has been received on a virtual interface from a router whose authentication key or authentication type conflicts with this router's authentication key or authentication type. The factory default is disabled.

Virtual Bad packet- This trap signifies that an OSPF packet has been received on a virtual interface that cannot be parsed. The factory default is disabled.

Virtual Link Configuration Error- This trap signifies that a packet has been received on a virtual interface from a router whose configuration parameters conflict with this router's configuration parameters. The factory default is disabled.

LSA Traps

LSA Max Age - This trap signifies that one of the LSA in the router's link-state database has aged to MaxAge. The factory default is disabled.

LSA Originate - This trap signifies that a new LSA has been originated by this router. This trap should not be invoked for simple refreshes of LSAs(which happens every 30 minutes), but instead will only be invoked when an LSA is (re)originated due to a topology change. Additionally, this trap does not include LSAs that are being flushed because they have reached MaxAge. The factory default is disabled.

LSDB Overflow Traps

LSDB Overflow - This trap signifies that the number of LSAs in the router's link-state database has exceeded OSPF External LSDB Limit. The factory default is disabled.

LSDB Approaching Overflow - This trap signifies that the number of LSAs in the router's link-state database has exceeded ninety percent of OSPF External LSDB Limit. The factory default is disabled.

Retransmit Traps

Retransmit Packets - This trap signifies that an OSPF packet has been retransmitted on a non-virtual interface. All packets that may be retransmitted are associated with an LSDB entry. The LS type, LS ID, and Router ID are used to identify the LSDB entry. The factory default is disabled.

Virtual Link Retransmit Packets - This trap signifies that an OSPF packet has been retransmitted on a virtual interface. All packets that may be retransmitted are associated with an LSDB entry. The LS type, LS ID, and Router ID are used to identify the LSDB entry. The factory default is disabled.

State Change Traps

Interface State Change- This trap signifies that there has been a change in the state of a non-virtual OSPF interface. This trap should be generated when the interface state regresses (e.g., goes from DR to Down) or progresses to a terminal state (i.e., Point-to-Point, DR Other, DR, or Backup). The factory default is disabled.

Neighbor State Change - This trap signifies that there has been a change in the state of a non-virtual OSPF neighbor. This trap should be generated when the neighbor state regresses (e.g., goes from Attempt or Full to 1-Way or Down) or progresses to a terminal state (e.g., 2-Way or Full). When a neighbor transitions from or to Full on non-broadcast multi-access and broadcast networks, the trap should be generated by the designated router. A designated router transitioning to Down will be noted by OSPF Interface State Change. The factory default is disabled.

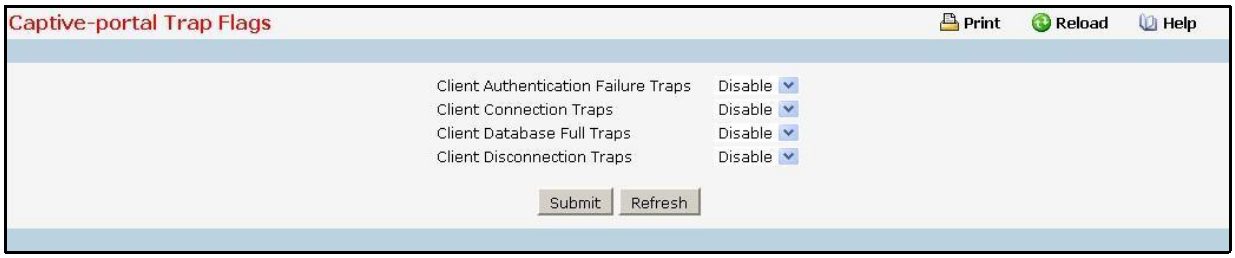
Virtual Link Interface State Change - This trap signifies that there has been a change in the state of an OSPF virtual interface. This trap should be generated when the interface state regresses (e.g., goes from Point-to-Point to Down) or progresses to a terminal state (i.e., Point-to-Point). The factory default is disabled.

Virtual Neighbor State Change - This trap signifies that there has been a change in the state of an OSPF virtual neighbor. This trap should be generated when the neighbor state regresses (e.g., goes from Attempt or Full to 1-Way or Down) or progresses to a terminal state (e.g., Full). The factory default is disabled.

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.

11.2.8.8 Captive Portal Trap Flags Page



Non-Configurable Data

Client Authentication Failure Traps - If you enable this field, the SNMP agent sends a trap when a client attempts to authenticate with a captive portal but is unsuccessful.

Client Connection Traps - If you enable this field, the SNMP agent sends a trap when a client authenticates with and connects to a captive portal.

Client Database Full Traps - If you enable this field, the SNMP agent sends a trap each time an entry cannot be added to the client database because it is full.

Client Disconnection Traps - If you enable this field, the SNMP agent sends a trap when a client disconnects from a captive portal.

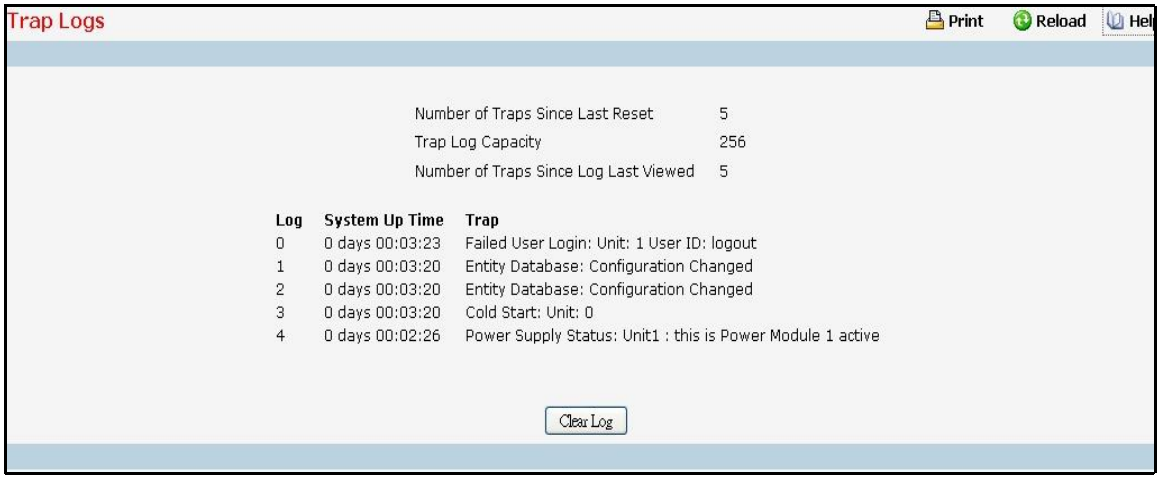
Command Buttons

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.

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

11.2.8.9 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.

Number of Traps Since Log Last Viewed - The number of traps that have occurred since the traps were last displayed. Displaying the traps by any method (terminal interface display, Web display, upload file from switch etc.) will cause this counter to be cleared to 0.

Log - The sequence number of this trap.

System Up Time - The time at which this trap occurred, expressed in days, hours, minutes and seconds since the last reboot of the switch.

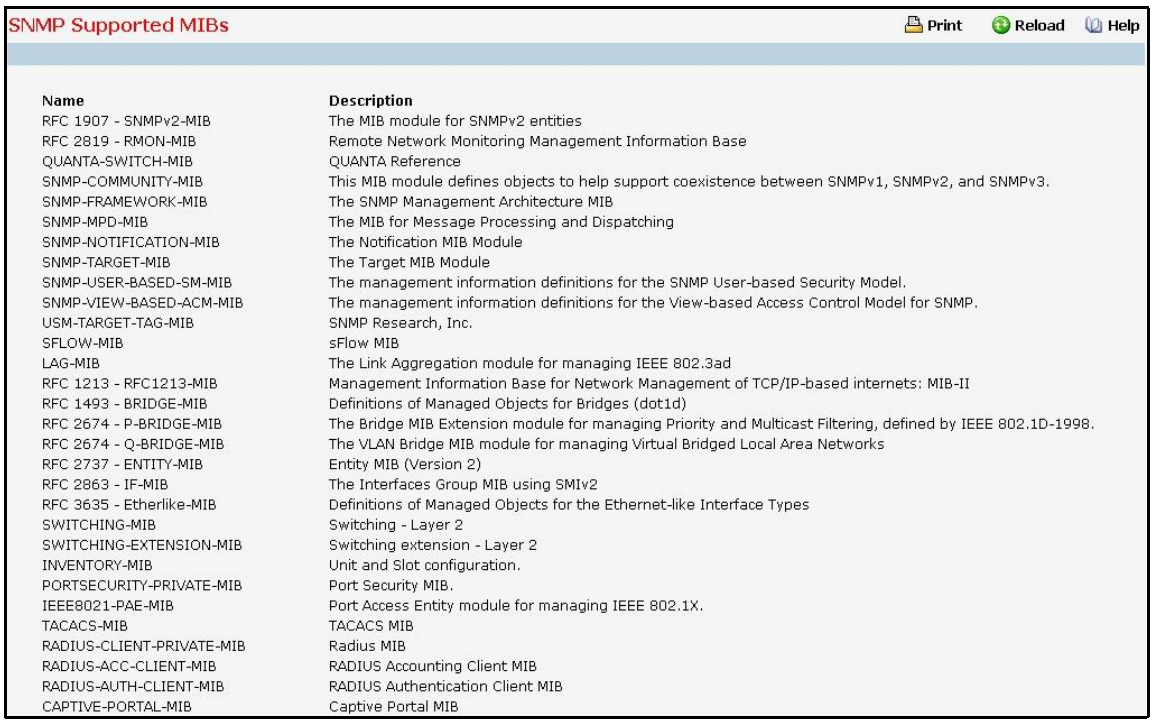
Trap - Information identifying the trap.

Command Buttons

Clear Log - Clear all entries in the log. Subsequent displays of the log will only show new log entries.

11.2.8.10 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.
PORTSECURITY-PRIVATE-MIB	Port Security MIB.
IEEE8021-PAE-MIB	Port Access Entity module for managing IEEE 802.1X.
TACACS-MIB	TACACS MIB
RADIUS-CLIENT-PRIVATE-MIB	Radius MIB
RADIUS-ACC-CLIENT-MIB	RADIUS Accounting Client MIB
RADIUS-AUTH-CLIENT-MIB	RADIUS Authentication Client MIB
CAPTIVE-PORTAL-MIB	Captive Portal MIB

Non-configurable Data

Name - The RFC number if applicable and the name of the MIB.

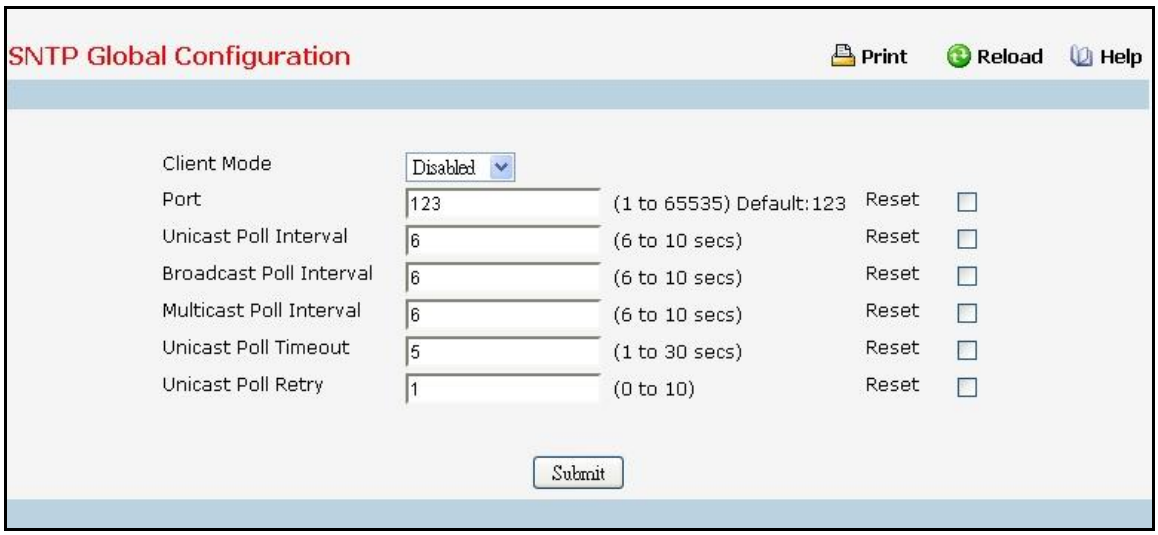
Description - The RFC title or MIB description.

Command Buttons

Refresh - Update the data.

11.2.9 Managing SNTP

11.2.9.1 Configuring SNTP Global Configuration Page



Configurable Data

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

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

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.

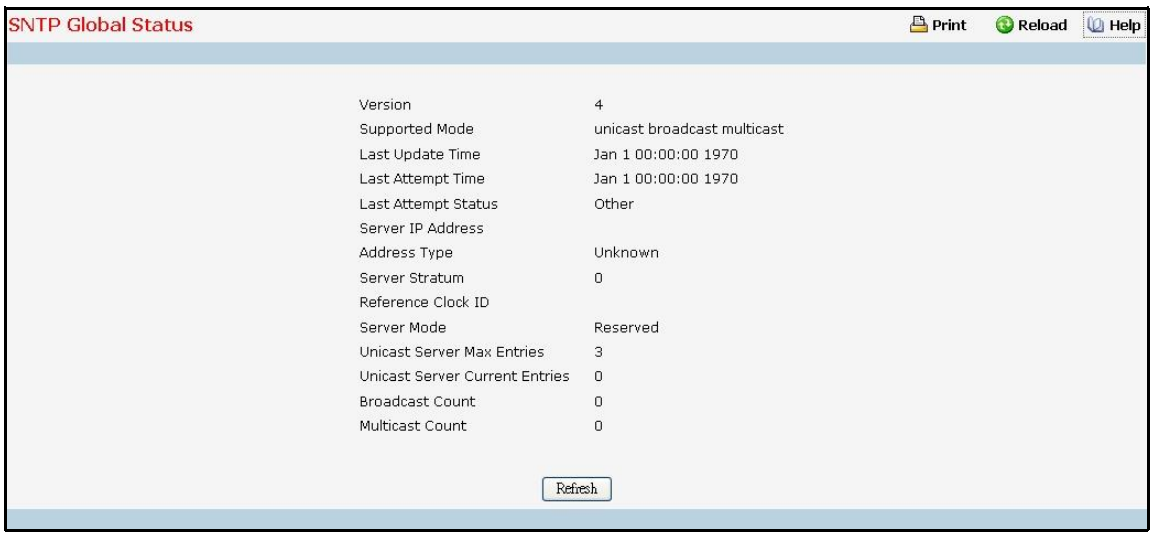
Unicast Poll Timeout - Specifies the number of seconds to wait for an SNTP response when configured in unicast mode. Allowed range is (1 to 30). Default value is 5.

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.

11.2.9.2 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 - The SNTP version supported by the server is not compatible with the version supported by the client.
- Server Unsynchronized - 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.

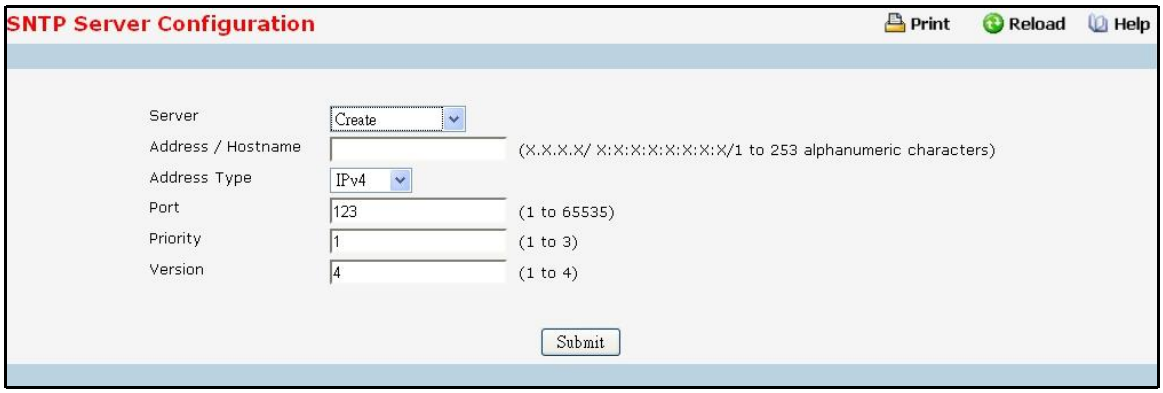
Unicast Sever Max Entries - Specifies the maximum number of unicast server entries that can be configured on this client.

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.

11.2.9.3 Configuring SNTP Server Page



Configurable Data

Server - Specifies all the existing Server Addresses along with an additional option "Create". When the user selects "Create" another text box "Address" appears where the user may enter Address for Server to be configured.

Address Type - Specifies the address type of the configured SNTP Server address. Allowed types are :

- IPv4
- IPv6
- DNS
- DNSv6

Address/Hostname - Specifies the address of the SNTP server. This is a text string of up to 253 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.

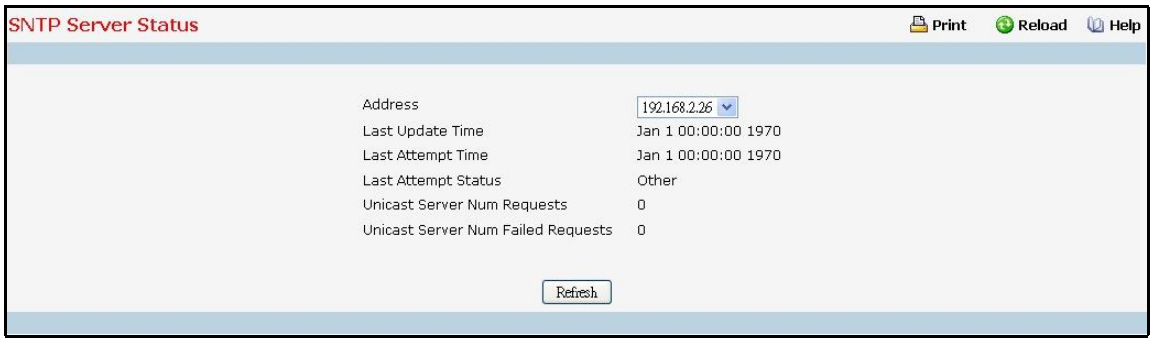
Version - Specifies the NTP Version running on the server. Allowed range is (1 to 4). Default value is 4.

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.

11.2.9.4 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 Unsynchronized - 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.

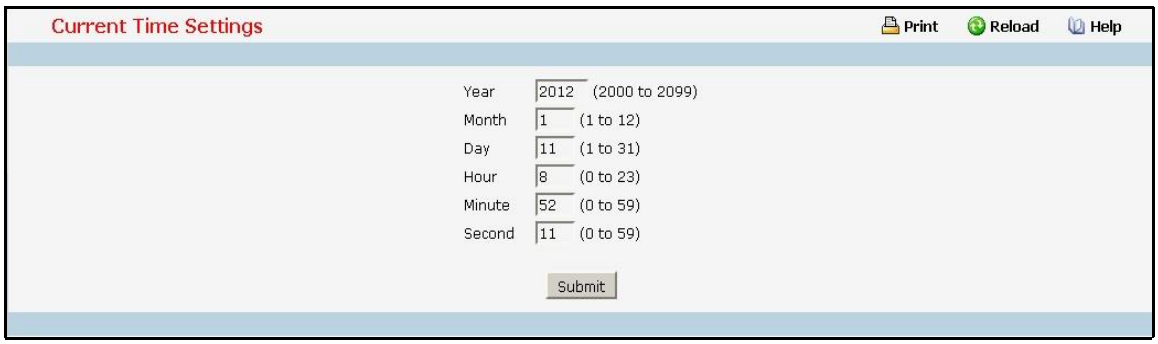
Unicast Server Num Requests - Specifies the number of SNTP requests made to this server since last time agent reboots.

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

Command Buttons

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

11.2.9.5 Configuring Current Time Settings Page



Configurable Data

Year - Year (4-digit). (Range: 2000 - 2037).

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).

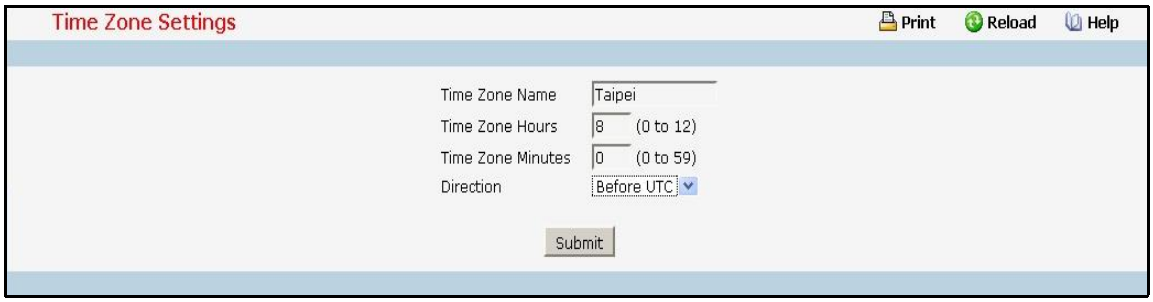
Second - Second (Range: 0 - 59).

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.

11.2.9.6 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

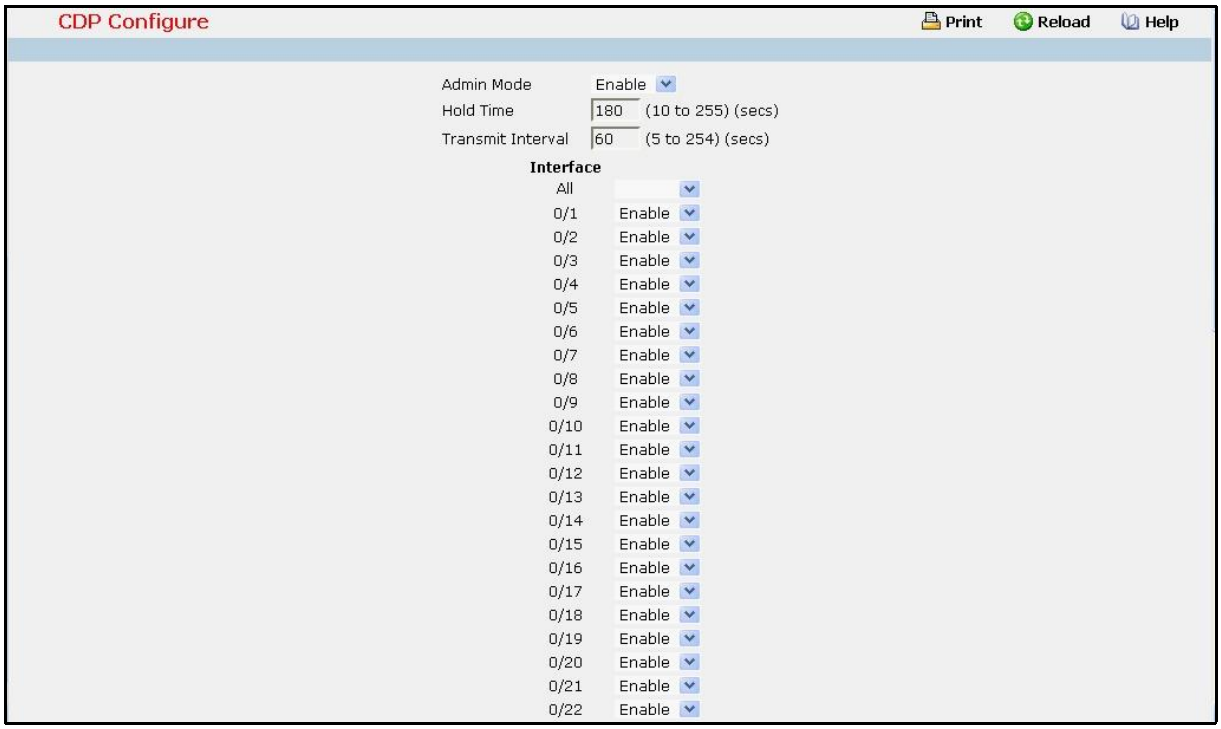
Command Buttons

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.

11.2.10 Managing CDP Function

11.2.10.1 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.

Interface - Specifies the list of ports.

Configurable Data

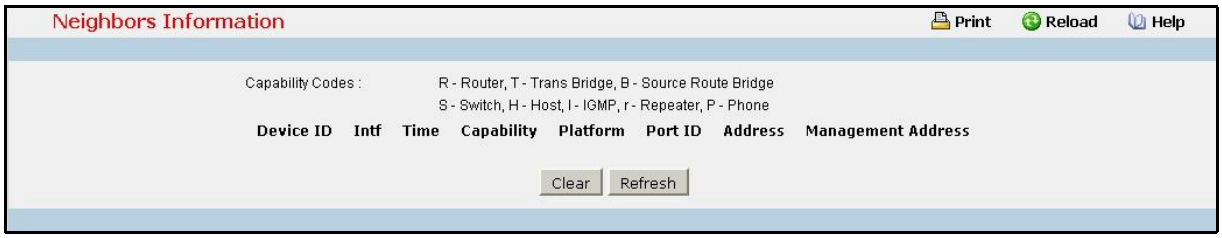
Hold Time - the legal time period of a received CDP packet.

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.

11.2.10.2 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.

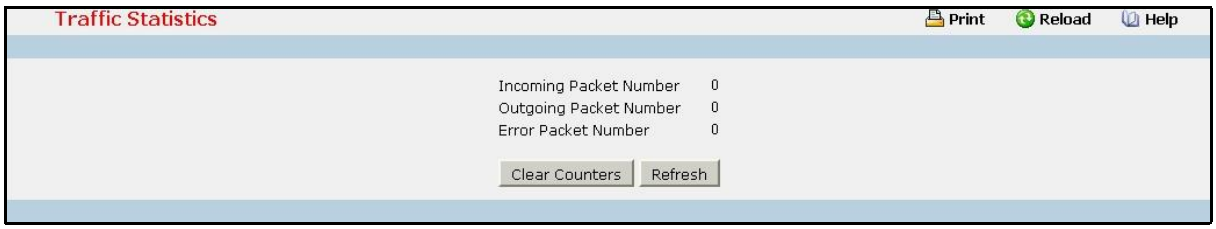
Command Buttons

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.

11.2.10.3 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.

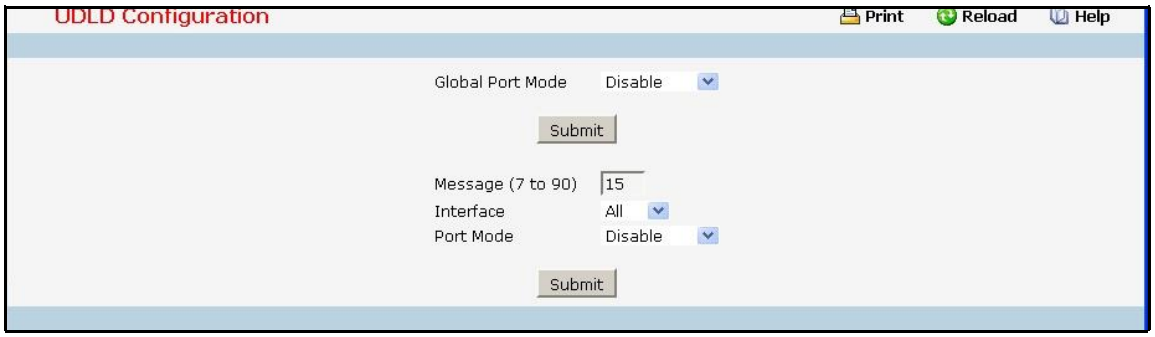
Command Buttons

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.

11.2.11 Managing UDLD

11.2.11.1 Configuring UDLD



Selection Criteria

Global Port Mode - Specifies the UDLD Global Port mode. It has three options: Disable, Normal and Aggressive.

Interface - Specifies the list of all the physical ports on which UDLD can be configured.

Port Mode - Specifies the UDLD Port mode for the selected interface. It has three options: Disable, Normal and Aggressive.

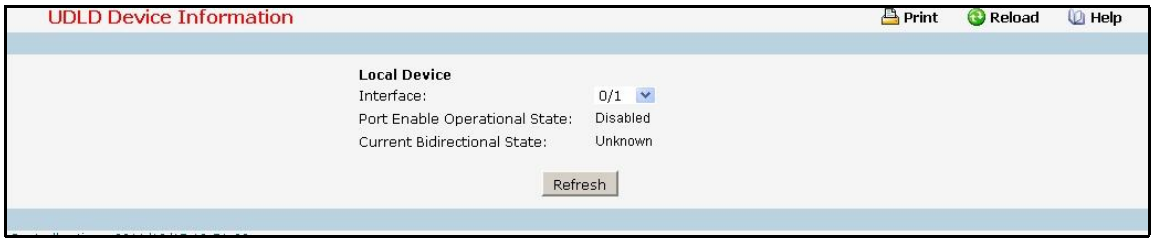
Configurable Data

Message - Specifies the Message Interval in seconds to send of messages in steady state. The range is from (7 to 90). Default value is 15 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.

11.2.11.2 Viewing UDLD Device Information



Selection Criteria

Interface - Specifies the list of all the physical ports on which UDLD can be configured.

Non-Configurable Data

Port Enable Operational State - Specifies the Port Enable Operational State of the selected port.

Current Bidirectional State - Specifies the Bidirectional State of the selected port.

Current Operational State - Specifies the runtime Operational State of the selected port. This section will be hidden if the port doesn't enable UDLD.

Current Message Interval - Specifies the runtime Message Interval of the selected port. This section will be hidden if the port doesn't enable UDLD.

Current Timeout Interval - Specifies the runtime Timeout Interval of the selected port. This section will be hidden if the port doesn't enable UDLD.

Remote Device - Specifies all the remote devices information as following.

Expiration time - Specifies the runtime Expiration Time of the remote entry.

Device ID - Specifies the Device Id associated with the remote system.

Device Name - Specifies the Device Name associated with the remote system.

Port ID - Specifies the Port Id associated with the remote system.

Neighbor echo device - Specifies the Device Id included in Echo TLV associated with the remote system.

Neighbor echo port - Specifies the port Id included in Echo TLV associated with the remote system.

Message interval - Specifies the Message interval associated with the remote system.

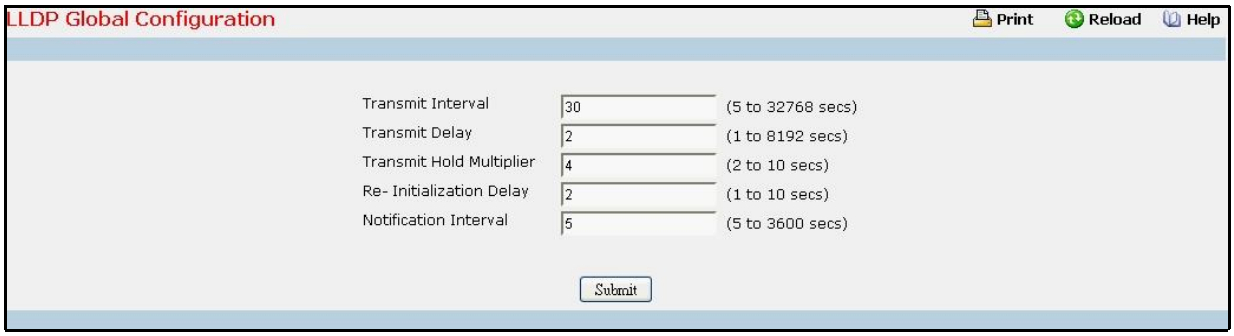
Timeout interval - Specifies the Timeout interval associated with the remote system.

Command Buttons

Refresh - Updates the information on the page.

11.2.12 Managing LLDP

11.2.12.1 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.

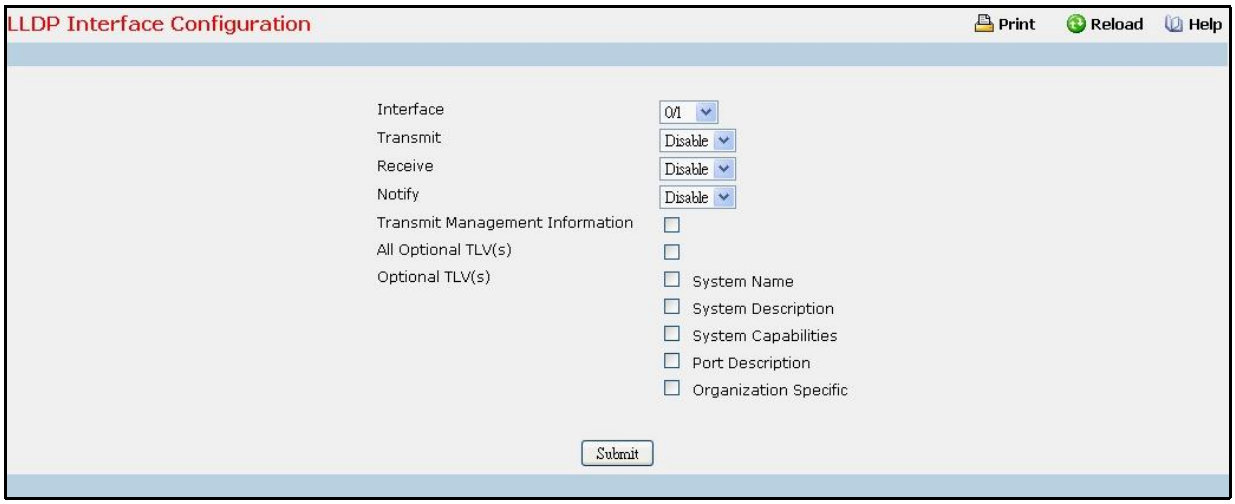
Re-Initialization Delay - Specifies the delay before re-initialization. The range is from (1 to 10). Default value is 2 seconds.

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.

11.2.12.2 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.

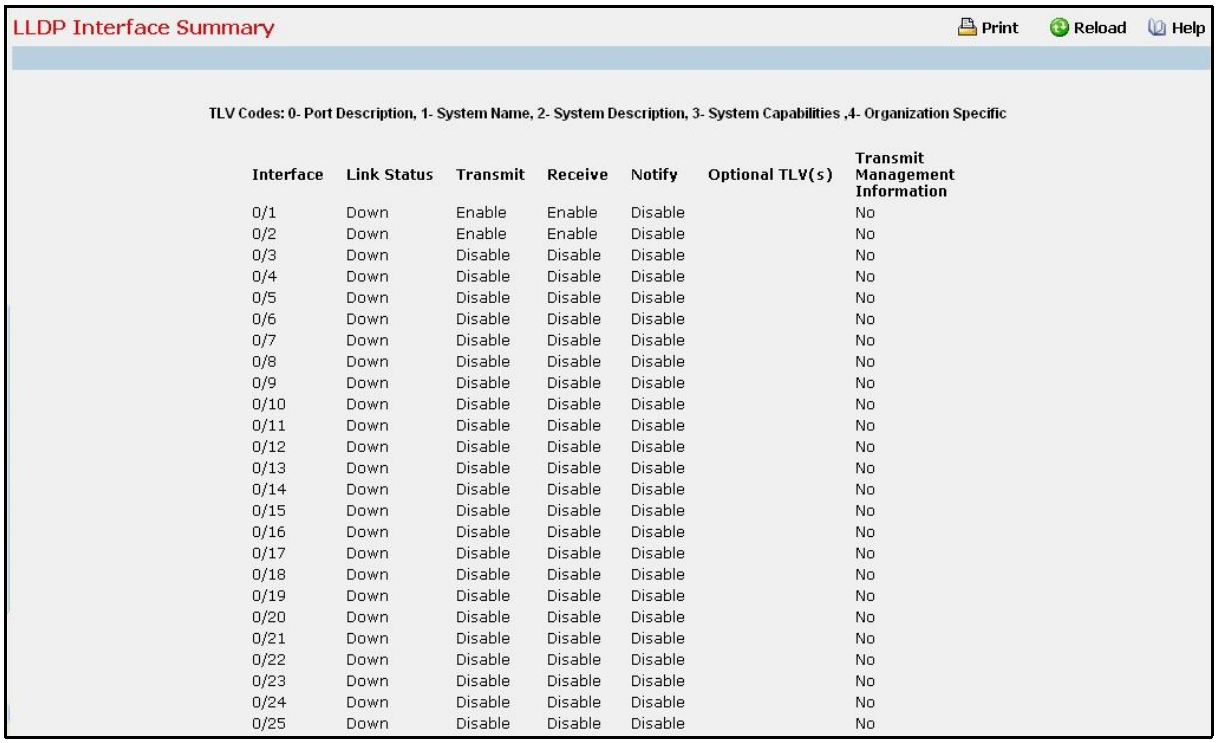
Optional TLV(s)

- 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.

11.2.12.3 Viewing LLDP Interface Summary Page



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.

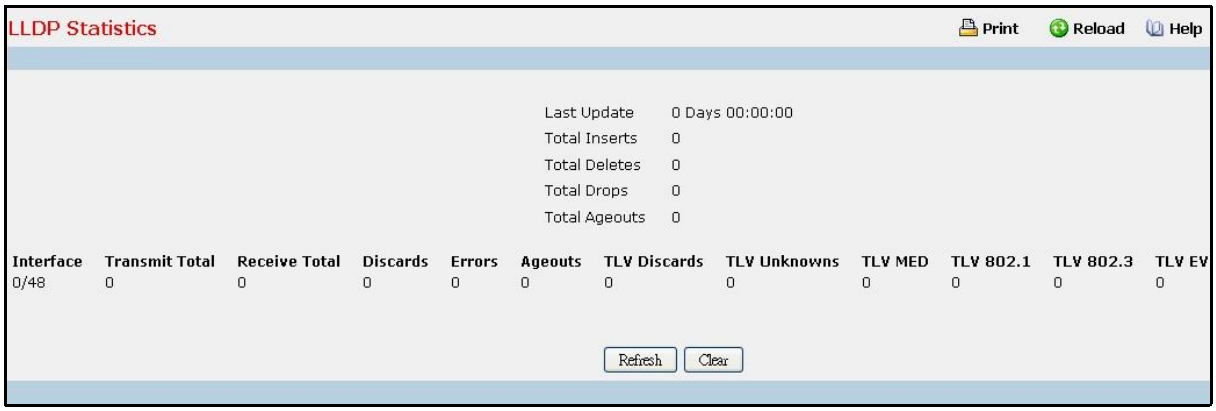
Optional TLV(s) - Specifies the LLDP - 802.1AB optional TLV(s) that are included.

Transmit Management Information - Specifies whether management address is transmitted in LLDP frames.

Command Buttons

Refresh - Updates the information on the page.

11.2.12.4 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 Ageouts - 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.

Ageouts - 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.

TLV EVB - Specifies the total number of LLDP TLVs received on the local ports which are of type EVB.

TLV DCBX - Specifies the total number of LLDP TLVs received on the local ports which are of type DCBX.

Command Buttons

Refresh - Updates the information on the page.

Clear - Clears LLDP Statistics of all the interfaces.

11.2.12.5 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-Negotiation 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.

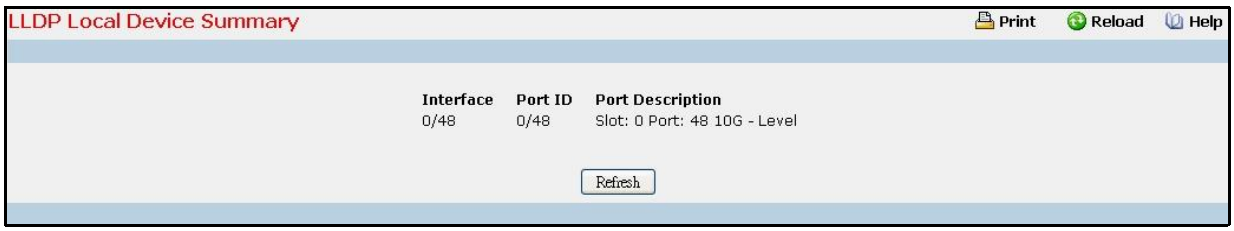
VLAN Name - Specifies the VLAN name.

Protocol Identity - Specifies the particular protocols that are accessible through the port.

Command Buttons

Refresh - Updates the information on the page.

11.2.12.6 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.

11.2.12.7 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-Negotiation 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.

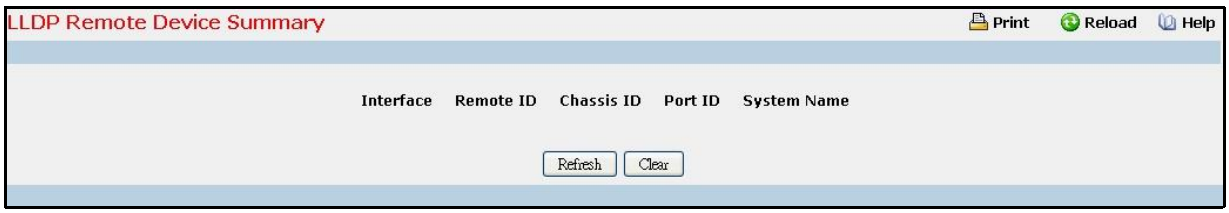
VLAN Name - Specifies the VLAN name.

Protocol Identity - Specifies the particular protocols that are accessible through the port.

Command Buttons

Refresh - Updates the information on the page.

11.2.12.8 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.

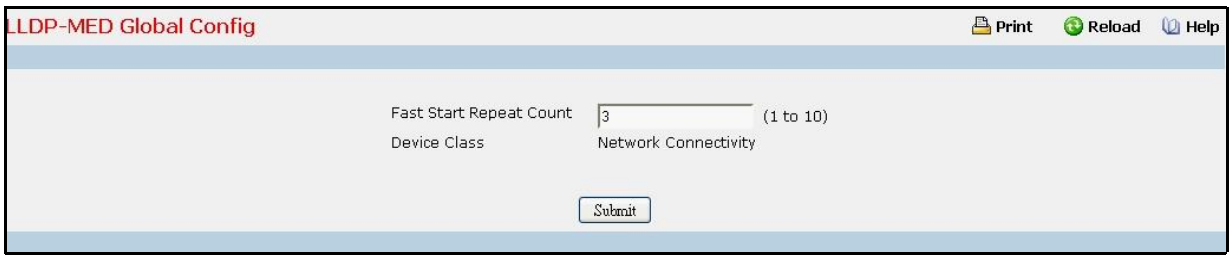
Command Buttons

Refresh - Updates the information on the page.

Clear - Clears LLDP Remote Device information received on all the interfaces.

11.2.13 Managing LLDP-MED

11.2.13.1 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.

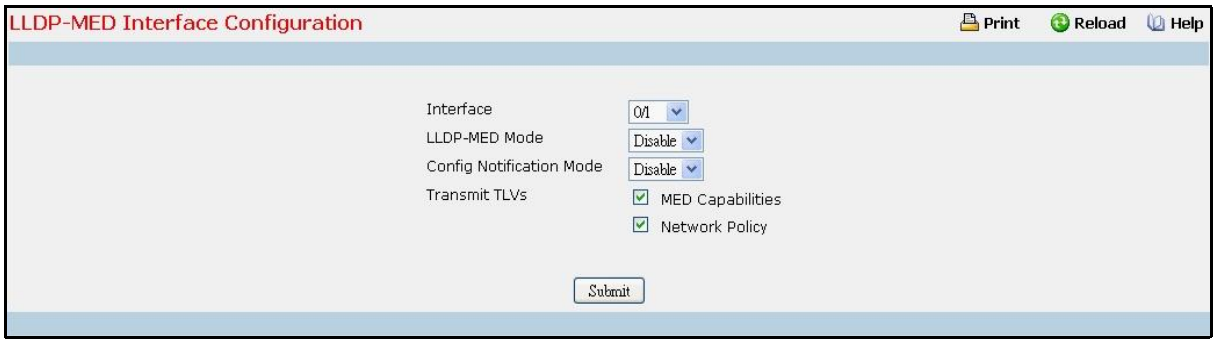
Non-Configurable Data

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.

11.2.13.2 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 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.

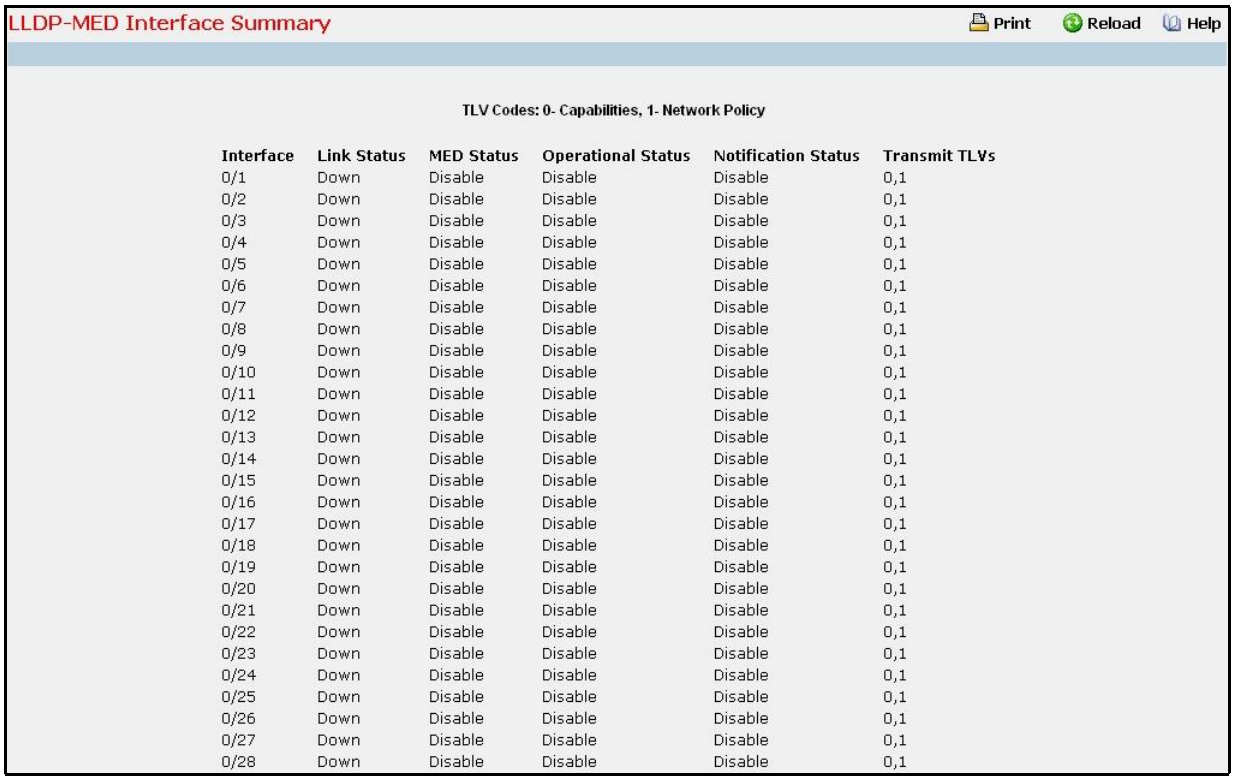
Extended Power via MDI - PD - To transmit the extended PD TLV in LLDP frames.

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.

11.2.13.3 Configuring LLDP-MED Interface Summary Page



LLDP-MED Interface Summary

Print Reload Help

TLV Codes: 0- Capabilities, 1- Network Policy

Interface	Link Status	MED Status	Operational Status	Notification Status	Transmit TLVs
0/1	Down	Disable	Disable	Disable	0,1
0/2	Down	Disable	Disable	Disable	0,1
0/3	Down	Disable	Disable	Disable	0,1
0/4	Down	Disable	Disable	Disable	0,1
0/5	Down	Disable	Disable	Disable	0,1
0/6	Down	Disable	Disable	Disable	0,1
0/7	Down	Disable	Disable	Disable	0,1
0/8	Down	Disable	Disable	Disable	0,1
0/9	Down	Disable	Disable	Disable	0,1
0/10	Down	Disable	Disable	Disable	0,1
0/11	Down	Disable	Disable	Disable	0,1
0/12	Down	Disable	Disable	Disable	0,1
0/13	Down	Disable	Disable	Disable	0,1
0/14	Down	Disable	Disable	Disable	0,1
0/15	Down	Disable	Disable	Disable	0,1
0/16	Down	Disable	Disable	Disable	0,1
0/17	Down	Disable	Disable	Disable	0,1
0/18	Down	Disable	Disable	Disable	0,1
0/19	Down	Disable	Disable	Disable	0,1
0/20	Down	Disable	Disable	Disable	0,1
0/21	Down	Disable	Disable	Disable	0,1
0/22	Down	Disable	Disable	Disable	0,1
0/23	Down	Disable	Disable	Disable	0,1
0/24	Down	Disable	Disable	Disable	0,1
0/25	Down	Disable	Disable	Disable	0,1
0/26	Down	Disable	Disable	Disable	0,1
0/27	Down	Disable	Disable	Disable	0,1
0/28	Down	Disable	Disable	Disable	0,1

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.

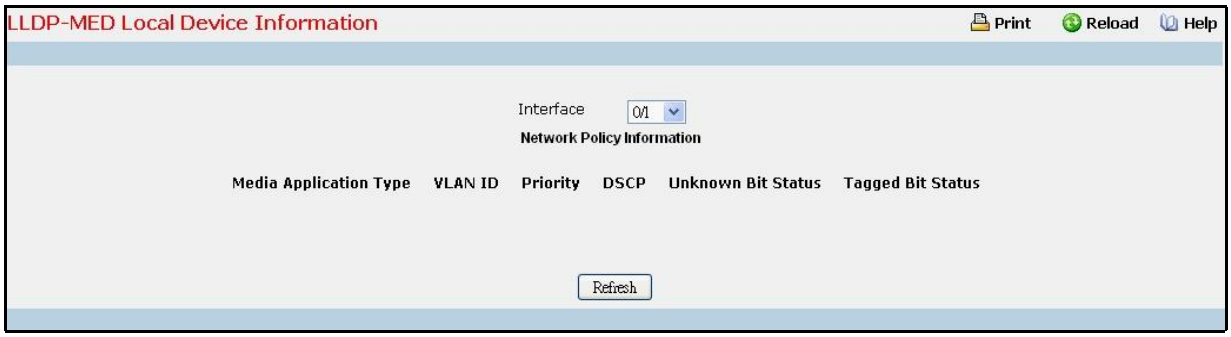
Notification Status - Specifies the LLDP-MED topology notification mode of the interface.

Transmit TLV(s) - Specifies the LLDP-MED transmit TLV(s) that are included.

Command Buttons

Refresh - Updates the information on the page.

11.2.13.4 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.

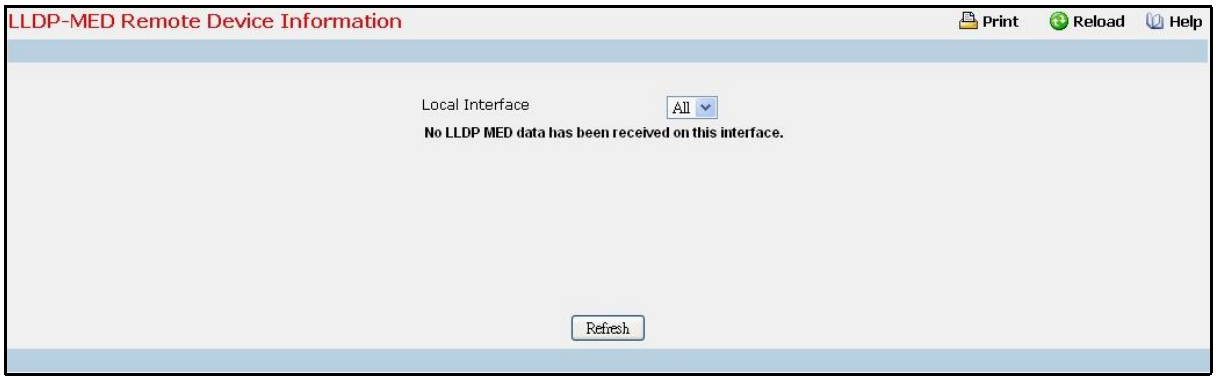
Source - Specifies power source of this port.

Priority - Specifies PD port power priority.

Command Buttons

Refresh - Updates the information on the page.

11.2.13.5 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 were received in MED TLV on this port.

Supported Capabilities - Specifies supported capabilities that were received in MED TLV on this port.

Enabled Capabilities - Specifies enabled capabilities that were 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 manufacturer’s 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.

11.2.14 Managing sFlow

11.2.14.1 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.

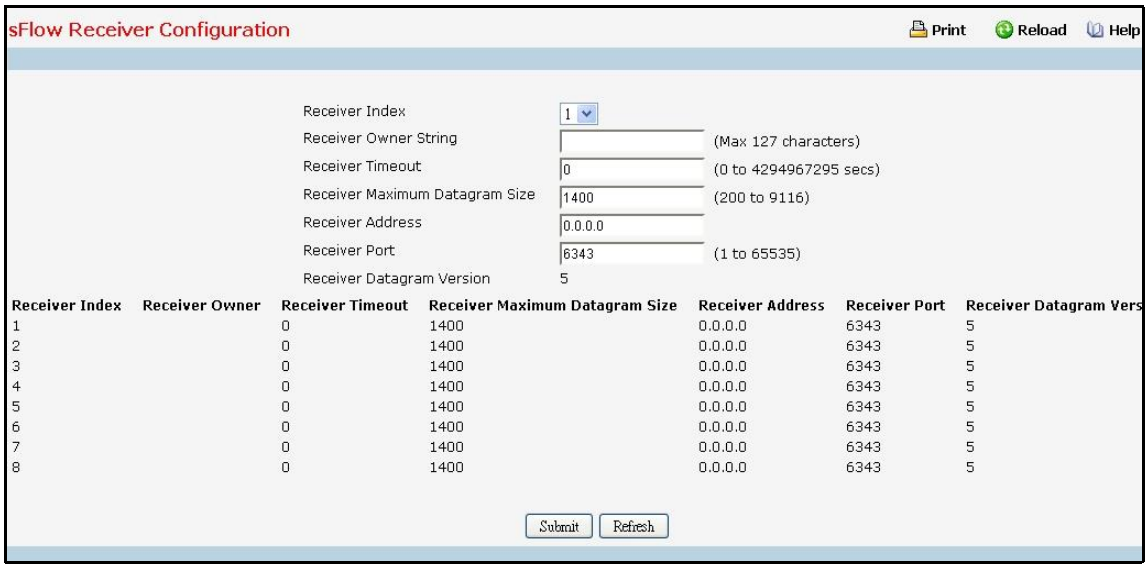
Agent Address - The IP address associated with this agent.

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.

11.2.14.2 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 String- The entity making use of this sFlow Receiver Table 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 sFlow Receiver Table 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. Maximum of 127 characters are allowed.

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.

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)

Receiver Address - The IP address of the sFlow collector. If set to 0.0.0.0, no sFlow datagrams will be sent.

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.

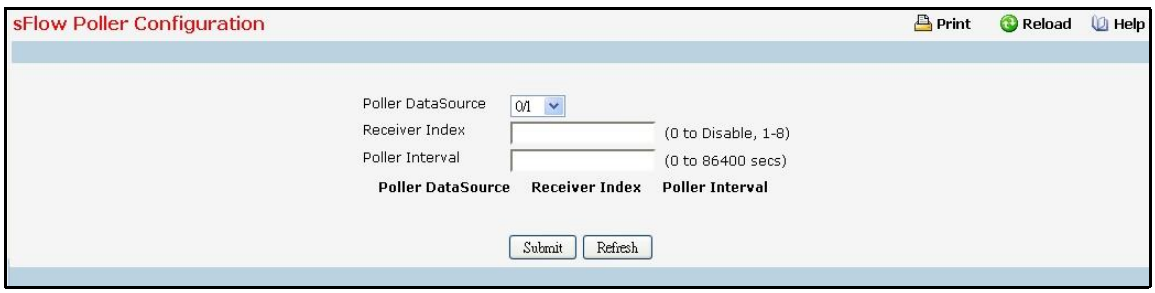
sFlow Receiver Datagram Version - The version of sFlow datagrams that should be sent.

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.

11.2.14.3 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

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

Poller DataSource - 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)

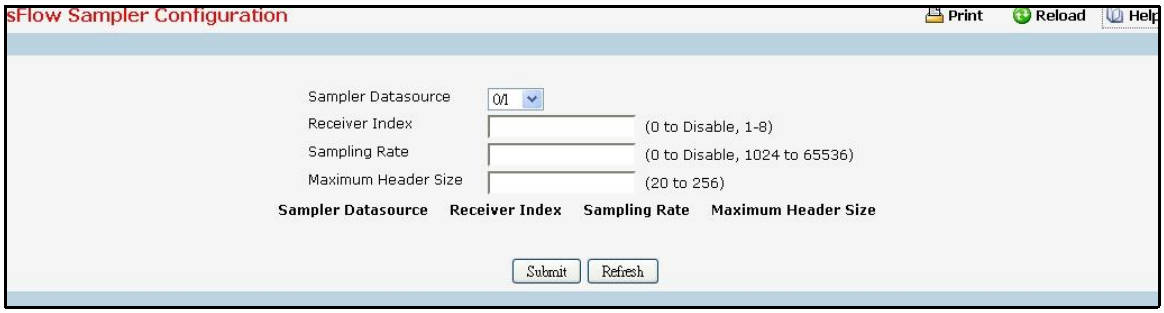
Poller Interval - The maximum number of seconds between successive samples of the counters associated with this data source.

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.

11.2.14.4 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

Sampler Datasource - 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

Sampler Datasource - sFlowDataSource for this flow sampler.

Receiver Index - The sFlowReceiver for this sFlow sampler.

Sampling Rate - The statistical sampling rate for packet sampling from this source.

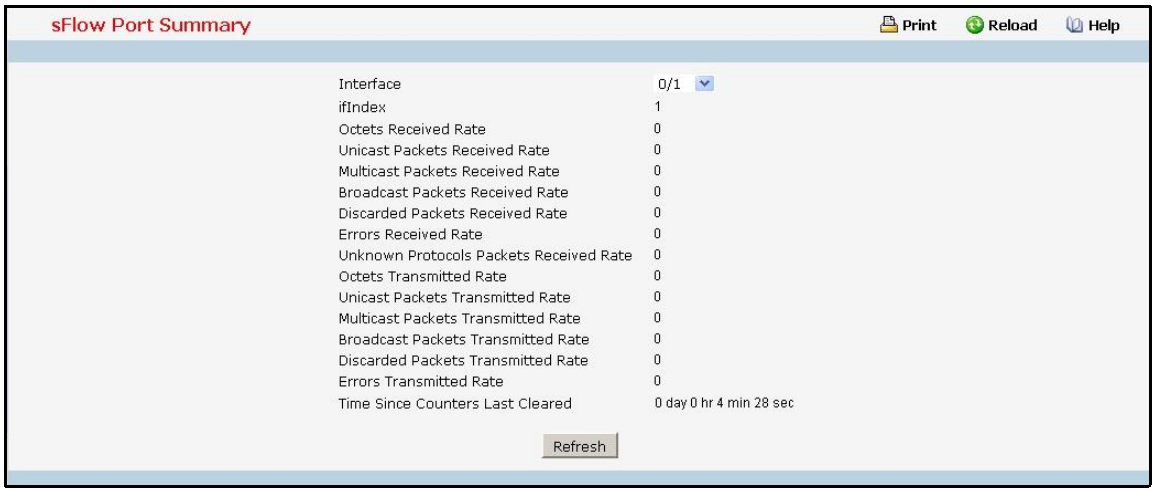
Maximum Header Size - The maximum number of bytes that should be copied from a sampled packet.

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.

11.2.14.5 Viewing sFlow Port Summary Page



Selection Criteria

Interface - Selects the interface for which data is to be displayed or configured.

Non-Configurable Data

Interface - 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.

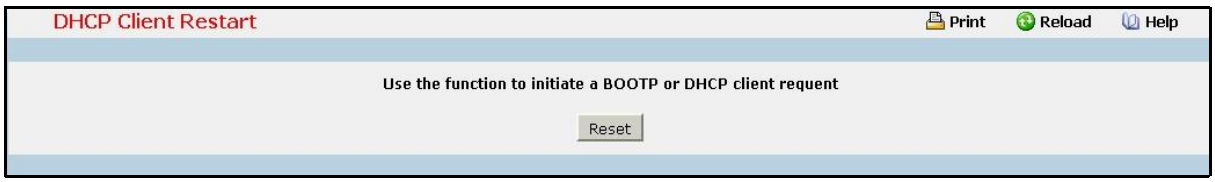
Command Buttons

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

11.2.15 Managing DHCP Client

11.2.15.1 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.

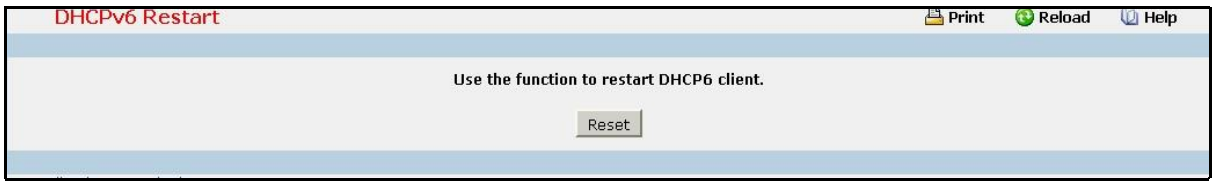


Command Buttons

Reset - Send the updated screen to the switch to restart the DHCP client.

11.2.15.2 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.

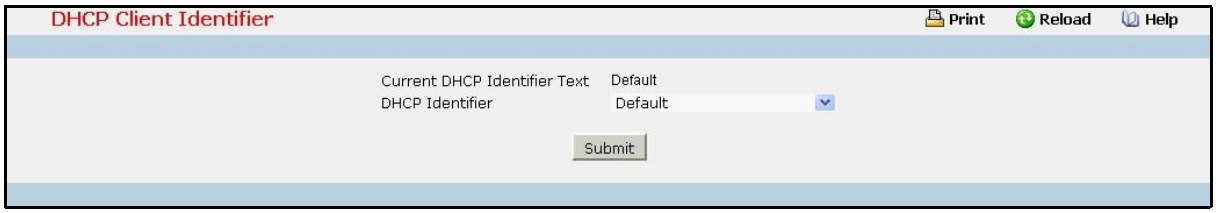


Command Buttons

Reset - Send the updated screen to the switch perform the restart DHCP6 client.

11.2.15.3 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.

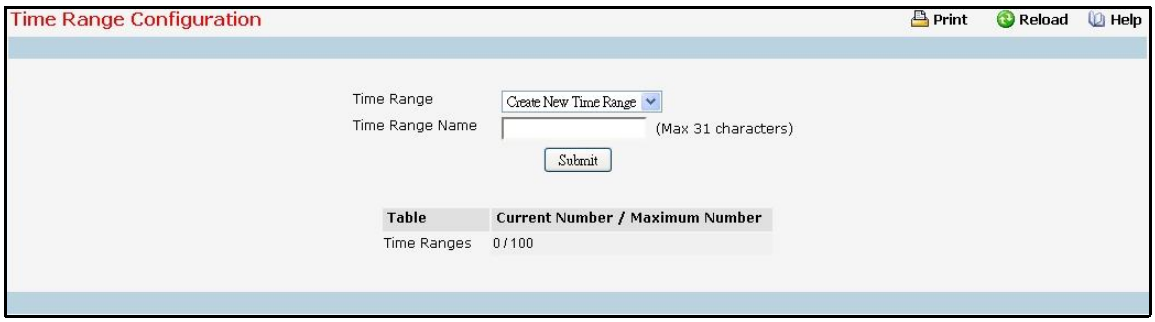
Command Buttons

Submit - Send the updated screen to the switch perform the setting DHCP client identifier.

11.2.16 Managing Time Ranges

11.2.16.1 Time Zone Settings

A Time Range consists of one absolute time entry and/or one or more periodic time entries. Depending on the type, a time range entry consists of start time or end time or both. Absolute and periodic time entries for the Time Range are specified/created using the Time Range Entry Configuration menu.



Selection Criteria

Time Range - A new Time Range may be created or an existing Time Range can be deleted based on selection.

Configurable Data

Time Range Name - Specifies Time Range Name string which may include alphabetic, numeric, dash, underscore or space characters only. The name must start with an alphabetic character and can have <1-31> alphanumeric characters only. This field displays the name of the currently selected Time Range if the Time Range has already been created.

Non-Configurable Data

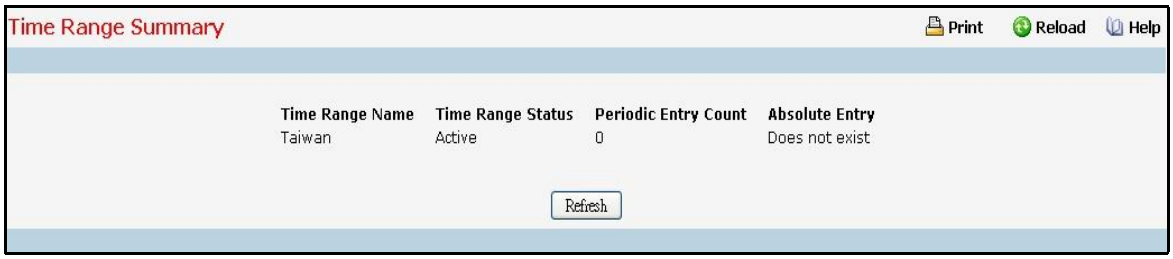
Table - Displays the current number/maximum number of Time Ranges.

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 - Removes the currently selected Time Range from the switch configuration.

11.2.16.2 Time Range Summary



Non-Configurable Data

Time Range Name - Time Range identifier.

Time Range Status - Status of the Time Range - Active/Inactive.

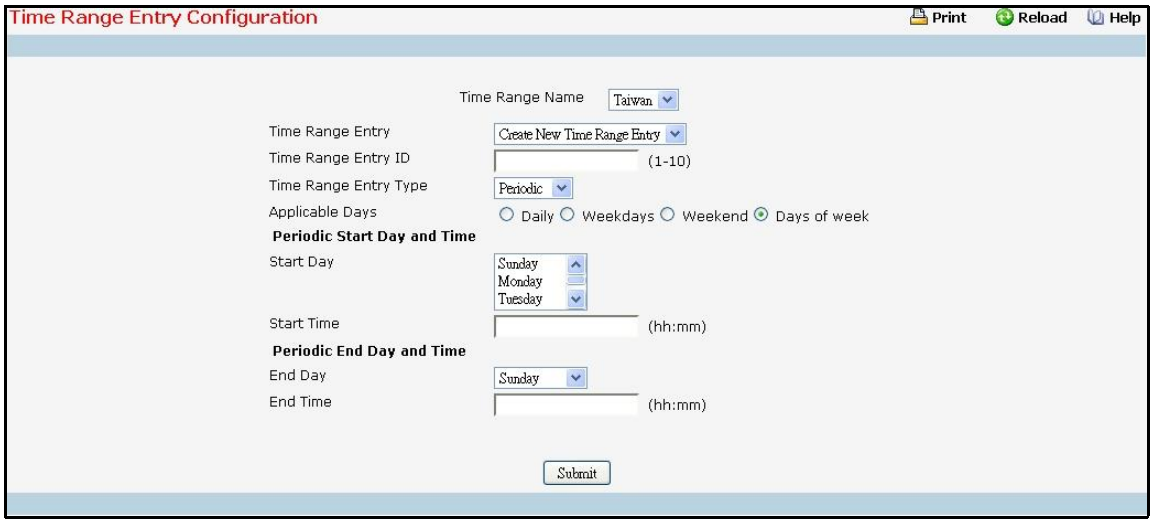
Periodic Entry Count - The number of periodic time entries currently configured for the Time Range.

Absolute Entry - Specifies whether an absolute time entry is currently configured for the Time Range.

Command Buttons

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

11.2.16.3 Time Range Entry Configuration



Selection Criteria

Time Range Name - Select the time range for which to create or delete a time entry.

Time Range Entry - Select an existing time range entry or select 'Create New Time Range Entry' to add a new time range entry. New time range entries cannot be created if the maximum number of entries has been reached. A time range entry can either be an absolute entry or periodic entry. Only one absolute entry can be configured per time range.

Configurable Data

Time Range Entry ID - Enter a whole number in the range of (1 to 10) that will be used to identify the time range entry.

Time Range Entry Type - Specify what type of entry should be created. The choices are Absolute or Periodic.

Start Date - Select the day of the month of the absolute entry's start date.

Start Month - Select the month of the absolute entry's start date.

Start Year - Select the year of the absolute entry's start date.

Start Time - Specify the absolute start time in hh:mm format.

End Date - Select the day of the month of the absolute entry's end date.

End Month - Select the month of the absolute entry's end date.

End Year - Select the year of the absolute entry's end date.

End Time - Specify the absolute end time in hh:mm format.

Absolute Start Date and Time - Specifies the absolute entries start date and time.

Absolute End Date and Time - Specifies the absolute entries end date and time.

Applicable Days - Specify the applicable day(s) of week for periodic entry.

- Option 'Daily' indicates that periodic entry is applicable on every day of week.
- Option 'Weekdays' indicates that periodic entry is applicable only on weekdays.

- Option 'Weekend' indicates that periodic entry is applicable only on weekend.
- Option 'Days of week' enables selection of applicable periodic entry start day and end day from 'Start Day' and 'End Day' fields of the page.

Start Day - Select the day(s) of the week of the periodic entry's start day. Multiple days can be selected. On selecting multiple days for the 'Start Day' field, the 'End Day' field takes the same input. Hence selecting multiple days for the start day does not require any input for the end day.

Start Time - Specify the periodic start time in hh:mm format.

End Day - Select the day of the week of the periodic entry's end day.

End Time - Specify the periodic end time in hh:mm format.

Command Buttons

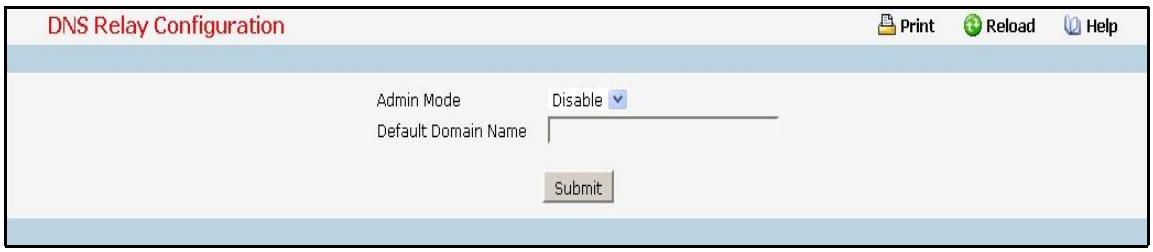
Submit - Update the switch with the values on the screen. If you want the switch to retain the new values across a power cycle you must perform a save.

Delete - Removes the currently selected entry from the selected time range.

11.2.17 Managing DNS Relay Function

11.2.17.1 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.



Configurable Data

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.

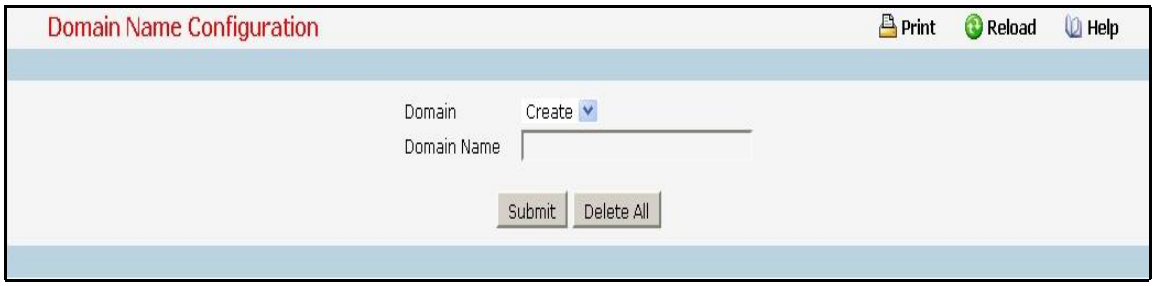
Default Domain Name - Default domain name used to complete unqualified host names. Do not include the initial period that separates an unqualified name from the domain name. This is a text string of up to 253 characters.

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.

11.2.17.2 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 253 characters.

Command Buttons

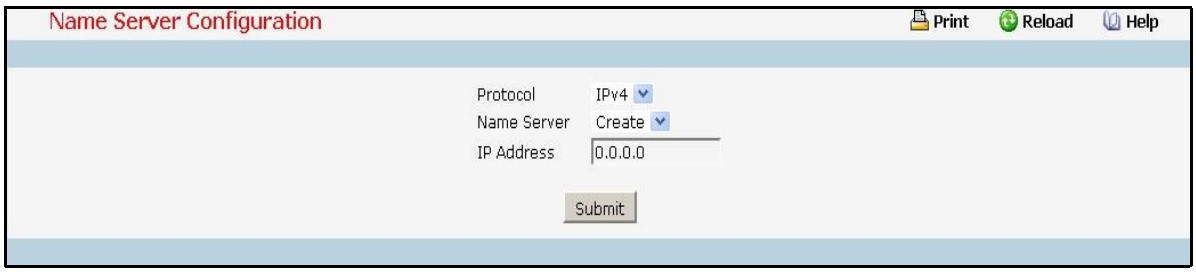
Submit - Sends the updated configuration to the switch. Configuration changes take effect immediately.

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.

11.2.17.3 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

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

Protocol - Select IPv4 or IPv6 to configure the corresponding attributes.

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.

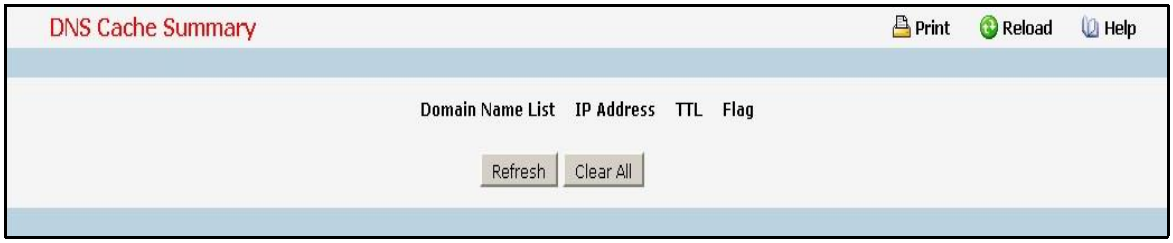
Delete - Deletes the domain name server entry. Sends the updated configuration to the switch. Configuration changes take effect immediately.

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.

11.2.17.4 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.

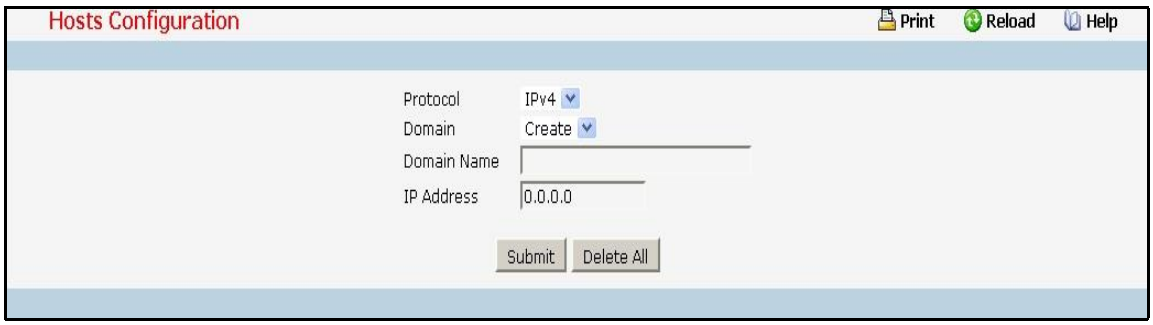
Command Buttons

Refresh - Refresh the page with the latest DNS cache entries.

Clear All - Clear all entries in the DNS cache.

11.2.17.5 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 253 characters. IP

Address - Specifies the address of the host.

Command Buttons

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

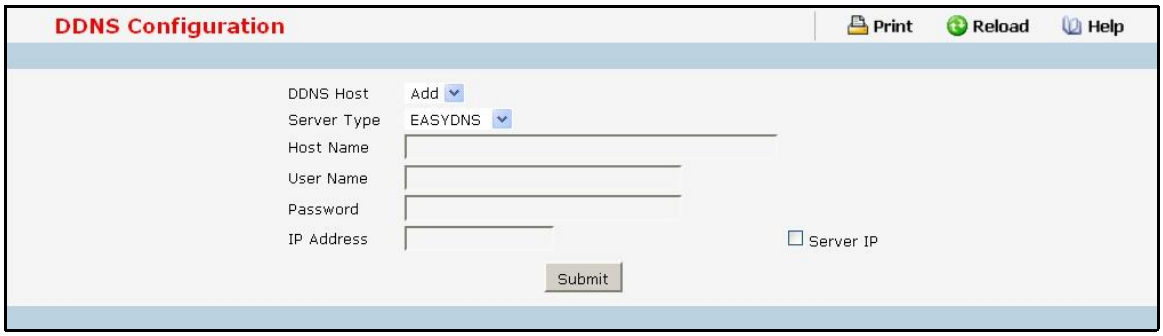
Delete - Deletes the host entry. Sends the updated configuration to the switch. Configuration changes take effect immediately.

Delete All - Deletes all the host entries. Sends the updated configuration to the switch. Configuration changes take effect immediately.

11.2.18 Managing DDNS Function

11.2.18.1 Configuring DDNS Configuration Page

The DDNS protocol provides user to update IP address of the specified host name to the DDNS provider.



Selection Criteria

DDNS Host - Selects the DDNS Host for which data is to be displayed or configured. If the add item is selected, a new DDNS Host can be configured.

Server Type - Selects the server type of DDNS server. You can choose any of the following type

- EASYDNS
- DYNDNS
- DHS
- ODS
- DYNS
- ZONEEDIT
- TZO

Configurable Data

Host Name - The hostname you want to be updated. Length is must equal or less than 253.

User Name - The account registered on DDNS server. Length is must equal or less than 32.

Password - The password of the account. Length is must equal or less than 32.

IP Address - The IP address you want to be updated.

Server IP - If this option is selected, the IP Address will be set to In-Band Mgmt IP address.

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.

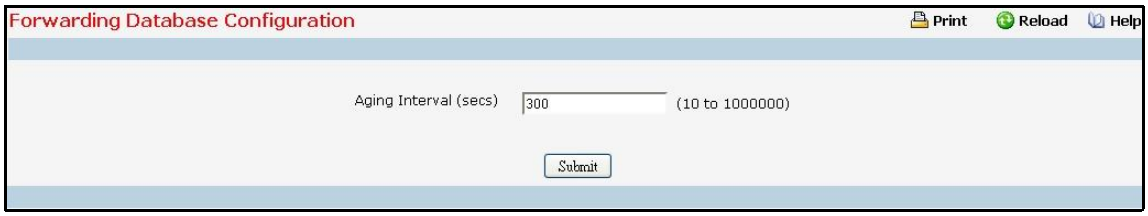
Remove - Remove the selected DDNS configuration.

11.3 Switching Menu

11.3.1 Defining Forwarding Database

11.3.1.1 Configuring MAC Table aging interval time Page

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



Configurable Data

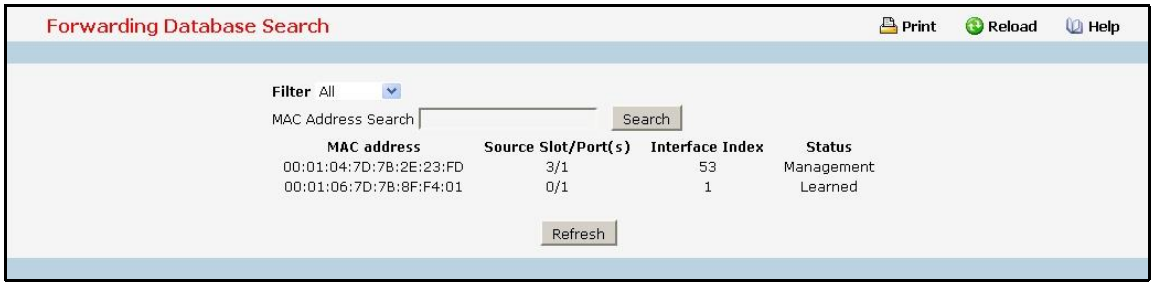
Aging Interval (secs) - The forwarding database contains static entries, which are never aged out, and dynamically learned entries, which are removed if they are not updated within a given time. You specify that time by entering a value for the Address Ageing Timeout. You may enter any number of seconds 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.

11.3.1.2 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.

Interface Index - The Interface Index 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.

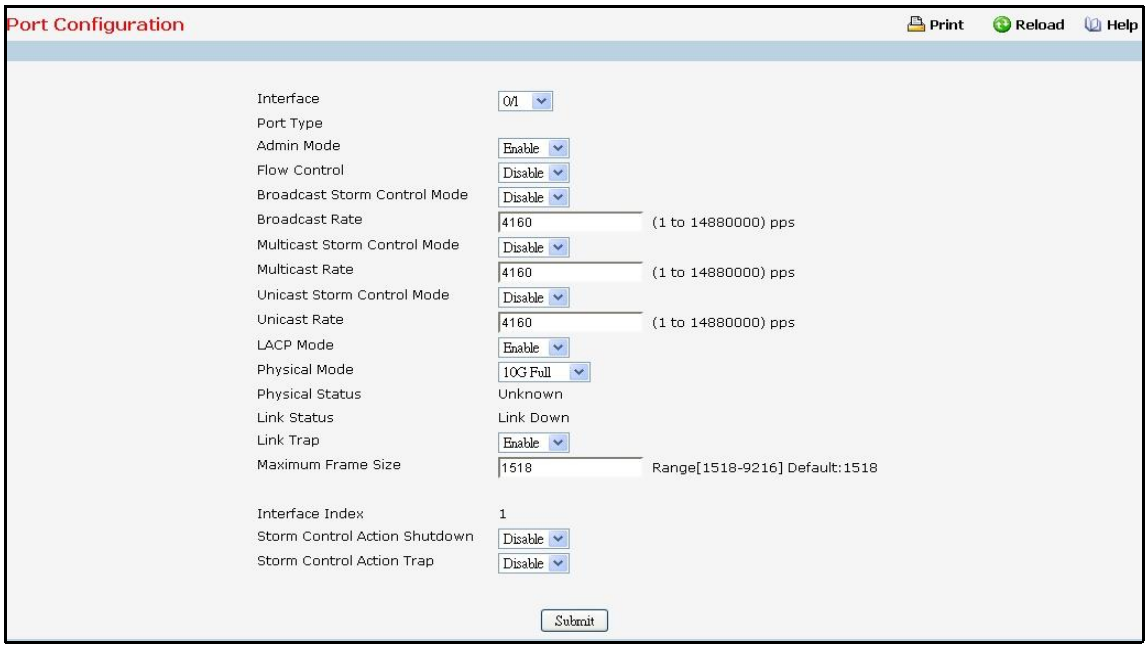
Command Buttons

Search - Search for the specified MAC address.

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

11.3.2 Managing Switch Interface

11.3.2.1 Configuring Switch Interface Page



Selection Criteria

Interface - Selects the interface for which data is to be displayed or configured.

Configurable Data

Admin Mode - Use the pull-down menu to select the Port control administration state. You must select enable if you want the port to participate in the network. The factory default is enabled.

Broadcast Storm Control - Enable or disable this option by selecting the corresponding line on the pull-down entry field. When you specify Enable for Broadcast Storm Recovery and the broadcast traffic on the specified Ethernet port exceeds the configured threshold, the switch blocks (discards) the broadcast traffic. The factory default is disabled.

Broadcast Rate - Set the packet rate value on selected interface. The valid values are from (1 to 14880000) pps.

Multicast Storm Control - Enable or disable this option by selecting the corresponding line on the pull-down entry field. When you specify Enable for Multicast Storm Recovery and the multicast traffic on the specified Ethernet port exceeds the configured threshold, the switch blocks (discards) the multicast traffic. The factory default is disabled.

Multicast Rate - Set the packet rate value on selected interface. The valid values are from (1 to 14880000) pps.

Unicast Storm Control - Enable or disable this option by selecting the corresponding line on the pull-down entry field. When you specify Enable for Unicast Storm Recovery and the unicast traffic on the specified Ethernet port exceeds the configured threshold, the switch blocks (discards) the unicast traffic. The factory default is disabled.

Unicast Rate - Set the packet rate value on selected interface. The valid values are from (1 to 14880000) pps..

Flow Control - Used to enable or disable flow control feature on the selected interface.

LACP Mode - Selects the Link Aggregation Control Protocol administration state. The mode must be enabled in order for the port to participate in Link Aggregation. May be enabled or disabled by selecting the corresponding line on the pull-down entry field. The factory default is enabled.

Physical Mode - Use the pull-down menu to select the port's speed and duplex mode. If you select auto the duplex mode and speed will be set by the auto-negotiation process. Note that the port's maximum capability (full duplex and 100 Mbps) will be advertised. Otherwise, your selection will determine the port's duplex mode and transmission rate. The factory default is auto. The selection when applied against the "All" option in Slot/Port is applied to all applicable interfaces only.

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

Maximum Frame Size - The maximum Ethernet frame size the interface supports or is configured, including Ethernet header, CRC, and payload. (1518 to 9216). The default maximum frame size is 1518.

Storm Control Action Shutdown - Used to enable or disable to shut down the selected interface while the storm is detected.

Storm Control Action Trap - Used to enable or disable to send trap for the selected interface while the storm is detected.

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.

Mirrored - the port is a mirrored port.

Probe - the port is a monitoring port. Look at the Port Monitoring screens for more information.

Physical Status - Indicates the port speed and duplex mode for Physical interfaces. Does not report Physical Status for LAG interfaces. Physical status is unknown when a port is down.

Link Status - Indicates whether the Link is up or down.

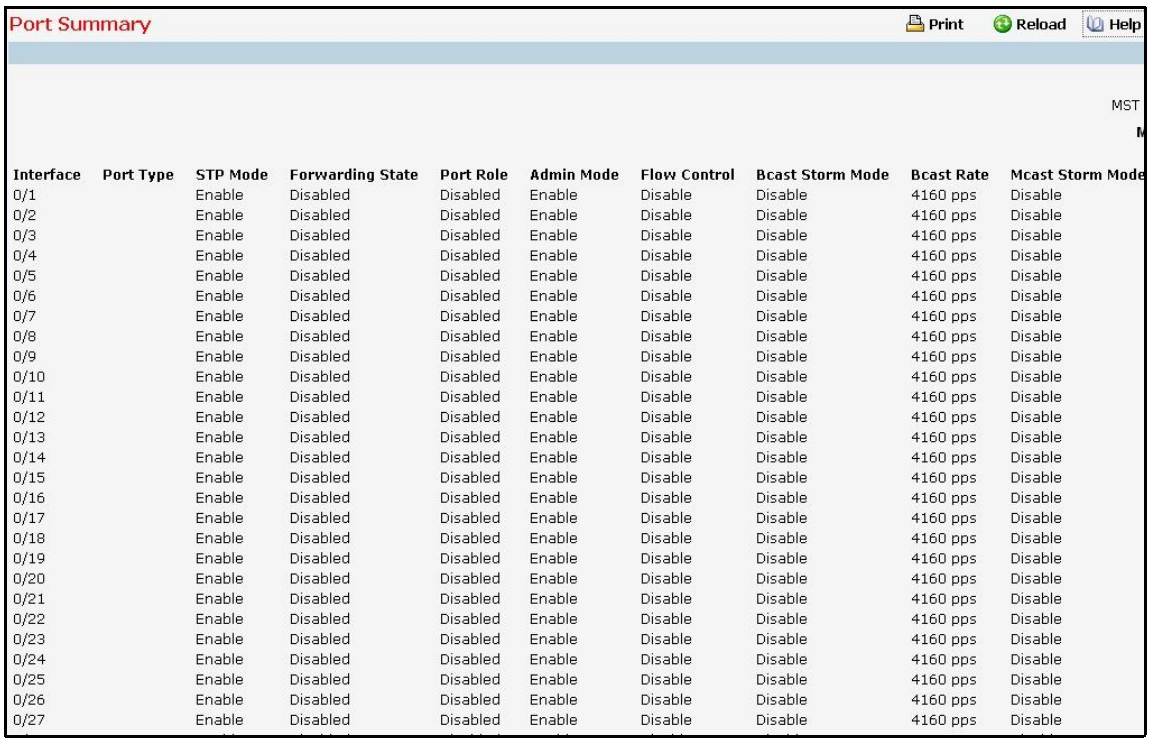
Interface Index - The interface index of the interface table entry associated with this port.

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.

11.3.2.2 Viewing Switch Interface Configuration Page

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



Port Summary

Print Reload Help

MST

Interface	Port Type	STP Mode	Forwarding State	Port Role	Admin Mode	Flow Control	Bcast Storm Mode	Bcast Rate	Mcast Storm Mode
0/1		Enable	Disabled	Disabled	Enable	Disable	Disable	4160 pps	Disable
0/2		Enable	Disabled	Disabled	Enable	Disable	Disable	4160 pps	Disable
0/3		Enable	Disabled	Disabled	Enable	Disable	Disable	4160 pps	Disable
0/4		Enable	Disabled	Disabled	Enable	Disable	Disable	4160 pps	Disable
0/5		Enable	Disabled	Disabled	Enable	Disable	Disable	4160 pps	Disable
0/6		Enable	Disabled	Disabled	Enable	Disable	Disable	4160 pps	Disable
0/7		Enable	Disabled	Disabled	Enable	Disable	Disable	4160 pps	Disable
0/8		Enable	Disabled	Disabled	Enable	Disable	Disable	4160 pps	Disable
0/9		Enable	Disabled	Disabled	Enable	Disable	Disable	4160 pps	Disable
0/10		Enable	Disabled	Disabled	Enable	Disable	Disable	4160 pps	Disable
0/11		Enable	Disabled	Disabled	Enable	Disable	Disable	4160 pps	Disable
0/12		Enable	Disabled	Disabled	Enable	Disable	Disable	4160 pps	Disable
0/13		Enable	Disabled	Disabled	Enable	Disable	Disable	4160 pps	Disable
0/14		Enable	Disabled	Disabled	Enable	Disable	Disable	4160 pps	Disable
0/15		Enable	Disabled	Disabled	Enable	Disable	Disable	4160 pps	Disable
0/16		Enable	Disabled	Disabled	Enable	Disable	Disable	4160 pps	Disable
0/17		Enable	Disabled	Disabled	Enable	Disable	Disable	4160 pps	Disable
0/18		Enable	Disabled	Disabled	Enable	Disable	Disable	4160 pps	Disable
0/19		Enable	Disabled	Disabled	Enable	Disable	Disable	4160 pps	Disable
0/20		Enable	Disabled	Disabled	Enable	Disable	Disable	4160 pps	Disable
0/21		Enable	Disabled	Disabled	Enable	Disable	Disable	4160 pps	Disable
0/22		Enable	Disabled	Disabled	Enable	Disable	Disable	4160 pps	Disable
0/23		Enable	Disabled	Disabled	Enable	Disable	Disable	4160 pps	Disable
0/24		Enable	Disabled	Disabled	Enable	Disable	Disable	4160 pps	Disable
0/25		Enable	Disabled	Disabled	Enable	Disable	Disable	4160 pps	Disable
0/26		Enable	Disabled	Disabled	Enable	Disable	Disable	4160 pps	Disable
0/27		Enable	Disabled	Disabled	Enable	Disable	Disable	4160 pps	Disable

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

Interface - Identifies the port

Port Type - For normal ports this field will be blank. Otherwise the possible values are:

Port Channel - the port is a member of a Link Aggregation trunk. Look at the LAG screens for more information.

Mirrored - the port is a mirrored port.

Probe - the port is a monitoring port. Look at the Port Monitoring 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 Status -Indicates the port speed and duplex mode for Physical interfaces. Does not report Physical Status for LAG interfaces. Physical status is unknown when a port is down.

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.

Broadcast Storm Control - Indicates whether broadcast storm control is enabled or disabled for the port. The factory default is disabled.

Bcast Rate - Set the packet rate value on selected interface. The valid values are from (1 to 14880000) pps.

Multicast Storm Control -Indicates whether multicast storm control is enabled or disabled for the port. The factory default is disabled.

Mcast Rate - Set the packet rate value on selected interface. The valid values are from (1 to 14880000) pps.

Unicast Storm Control -Indicates whether unicast storm control is enabled or disabled for the port. The factory default is disabled.

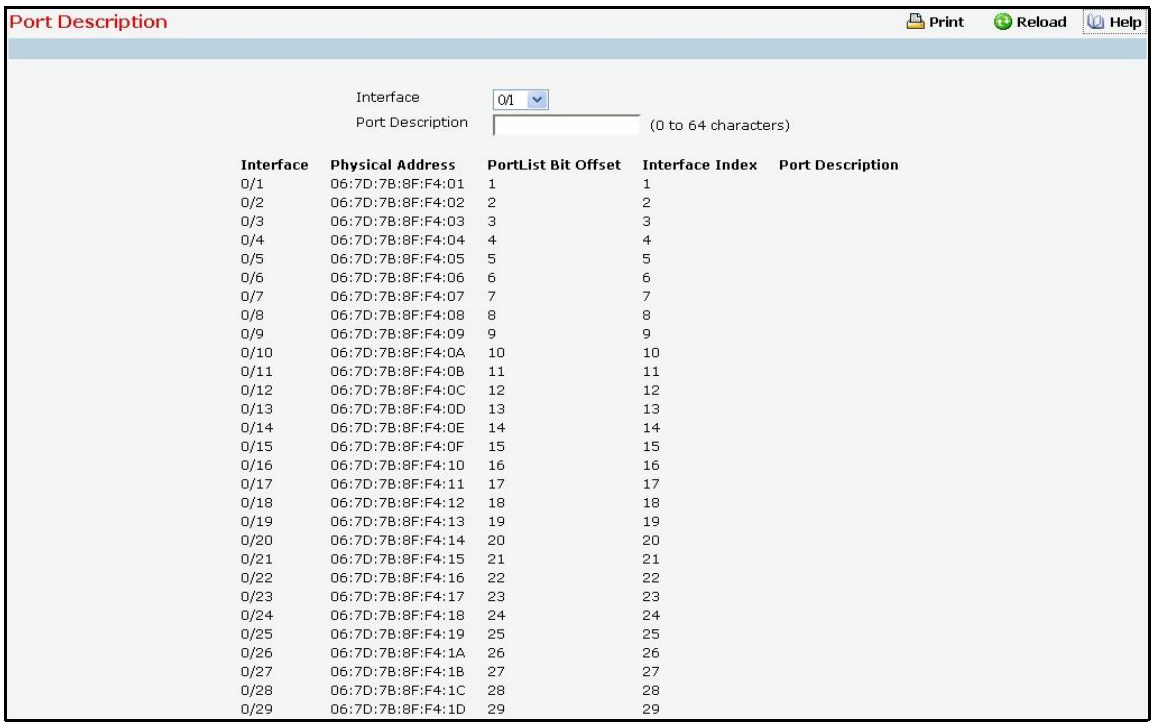
Ucast Rate - Set the packet rate value on selected interface. The valid values are from (1 to 14880000) pps.

Command Buttons

Refresh - Refresh the configuration value again.

11.3.2.3 Configuring Port Description Function Page

This screen configures and displays the description for all ports in the box.



Interface	Physical Address	PortList Bit Offset	Interface Index	Port Description
0/1	06:7D:7B:8F:F4:01	1	1	
0/2	06:7D:7B:8F:F4:02	2	2	
0/3	06:7D:7B:8F:F4:03	3	3	
0/4	06:7D:7B:8F:F4:04	4	4	
0/5	06:7D:7B:8F:F4:05	5	5	
0/6	06:7D:7B:8F:F4:06	6	6	
0/7	06:7D:7B:8F:F4:07	7	7	
0/8	06:7D:7B:8F:F4:08	8	8	
0/9	06:7D:7B:8F:F4:09	9	9	
0/10	06:7D:7B:8F:F4:0A	10	10	
0/11	06:7D:7B:8F:F4:0B	11	11	
0/12	06:7D:7B:8F:F4:0C	12	12	
0/13	06:7D:7B:8F:F4:0D	13	13	
0/14	06:7D:7B:8F:F4:0E	14	14	
0/15	06:7D:7B:8F:F4:0F	15	15	
0/16	06:7D:7B:8F:F4:10	16	16	
0/17	06:7D:7B:8F:F4:11	17	17	
0/18	06:7D:7B:8F:F4:12	18	18	
0/19	06:7D:7B:8F:F4:13	19	19	
0/20	06:7D:7B:8F:F4:14	20	20	
0/21	06:7D:7B:8F:F4:15	21	21	
0/22	06:7D:7B:8F:F4:16	22	22	
0/23	06:7D:7B:8F:F4:17	23	23	
0/24	06:7D:7B:8F:F4:18	24	24	
0/25	06:7D:7B:8F:F4:19	25	25	
0/26	06:7D:7B:8F:F4:1A	26	26	
0/27	06:7D:7B:8F:F4:1B	27	27	
0/28	06:7D:7B:8F:F4:1C	28	28	
0/29	06:7D:7B:8F:F4:1D	29	29	

Selection Criteria

Interface - 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

Interface - 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.

Interface Index - 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

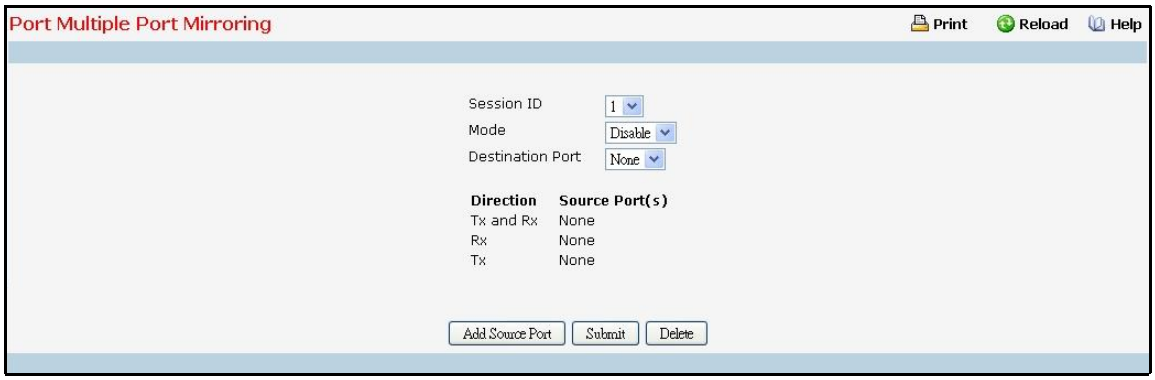
Submit - Send the updated screen to the switch and cause the changes to take effect on the switch.

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

11.3.2.4 Configuring Cable Test Function Page

Below 10-Giga Interface doesn't have this feature

11.3.2.5 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.

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 52 source ports can be selected per session.

Non-Configurable Data

Direction - Specifies the direction of traffic on source port(s) which will be sent to the probe port. Possible values are Tx and Rx.

Command Buttons

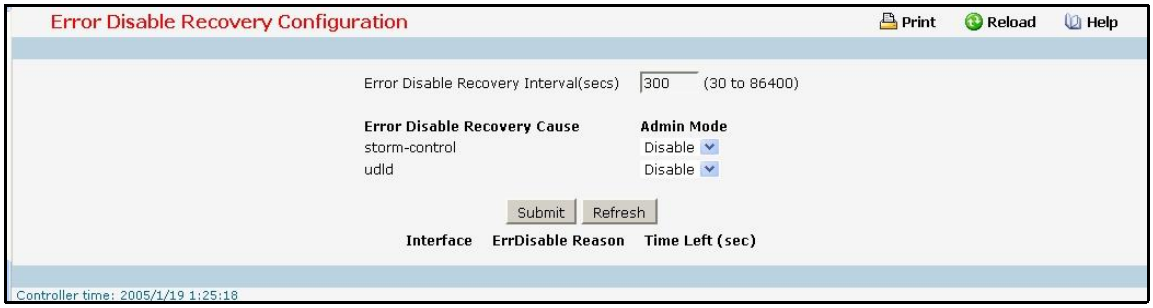
Add Source Ports - To add Source Port(s) to the selected session.

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.

11.3.2.6 Configuring Error Disable Recovery



Selection Criteria

storm-control - Enables or disables the specify Error Disable Recovery Cause by storm-control. The factory default is disabled.

udld - Enables or disables the specify Error Disable Recovery Cause by UDLD. The factory default is disabled.

Configurable Data

Error Disable Recovery Interval - This specifies the interval value for Error Disable Recovery. The factory default is 300 seconds. The range of Interval is (30 to 86400).

Non-Configurable Data

Interface - This specifies the interface which is shut down by Error Disable.

ErrDisable Reason - This specifies the reason why this interface is shutdown.

Time Left (sec) - This specifies the left time of this interface will be enabled.

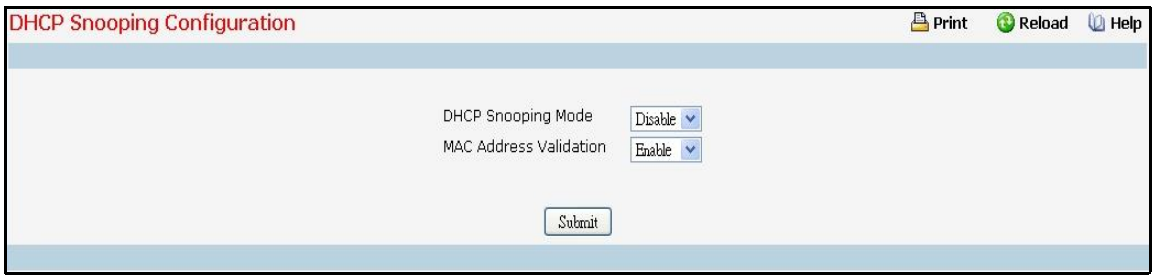
Command Buttons

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.

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

11.3.3 Managing DHCP Snooping

11.3.3.1 Configuring DHCP Snooping Configuration Page



Configurable Data

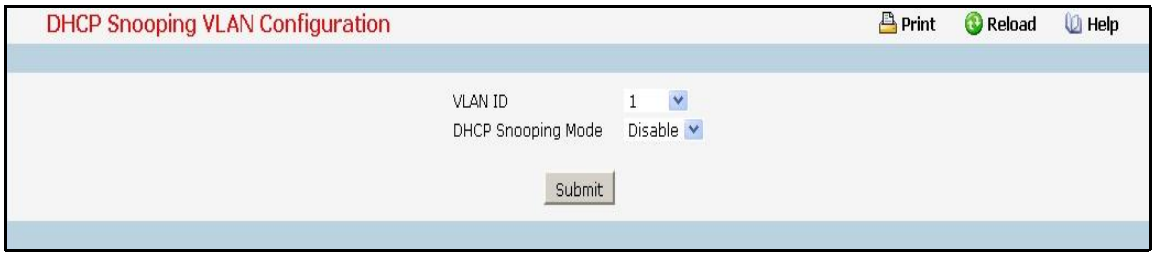
DHCP Snooping Mode - Enables or disables the DHCP Snooping feature. The factory default is disabled.

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.

11.3.3.2 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.

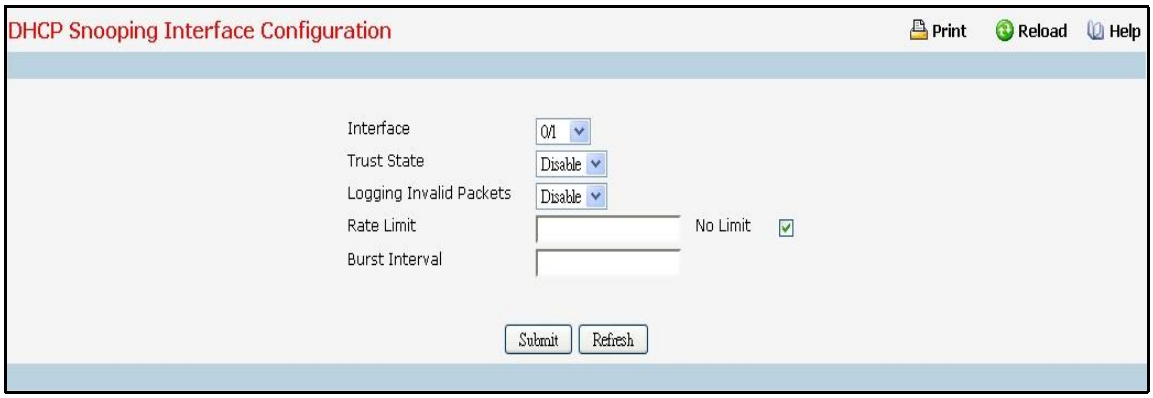
Configurable Data

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.

11.3.3.3 Configuring DHCP Snooping Interface Configuration Page



Selection Criteria

Interface - 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).

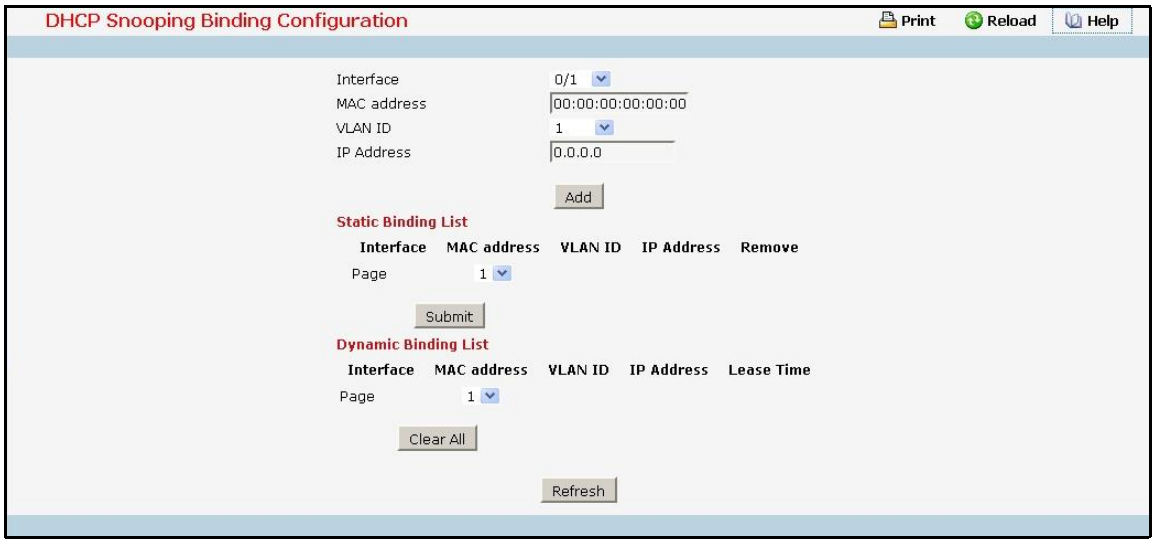
No Limit - Selecting this option specifies that the value of Rate Limit will be configured to -1. If the rate limit is -1 burst interval has no meaning, hence it is disabled.

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.

11.3.3.4 Configuring DHCP Snooping Static Binding Configuration Page



Configurable Data

Interface - 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 4093).

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.

- Interface - 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.

- Interface - 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

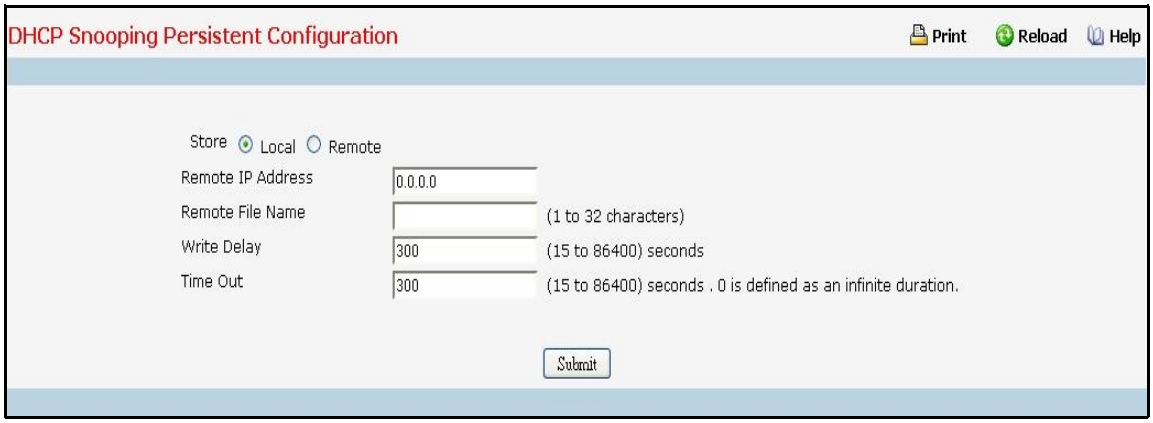
Add - Adds DHCP snooping binding entry into the database.

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.

11.3.3.5 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.

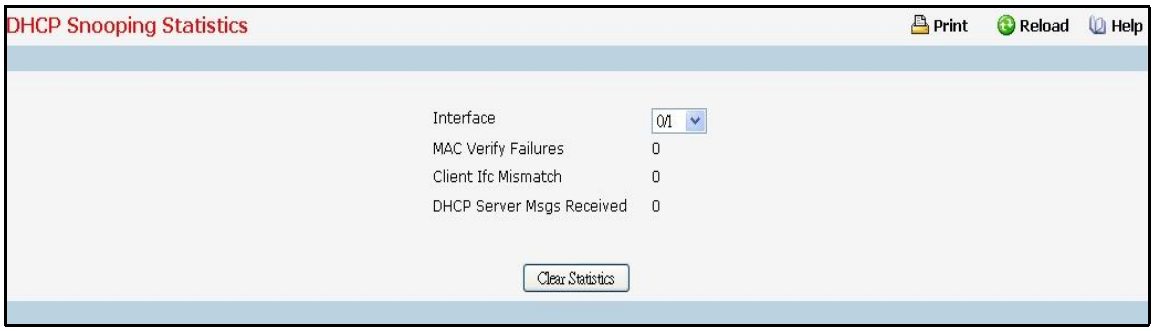
Time Out - Configure DHCP snooping bindings store timeout. The range of Time Out is (15 to 86400). 0 is defined as an infinite duration.

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.

11.3.3.6 DHCP Snooping Interface Statistics Page



Selection Criteria

Interface - Select the untrusted 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.

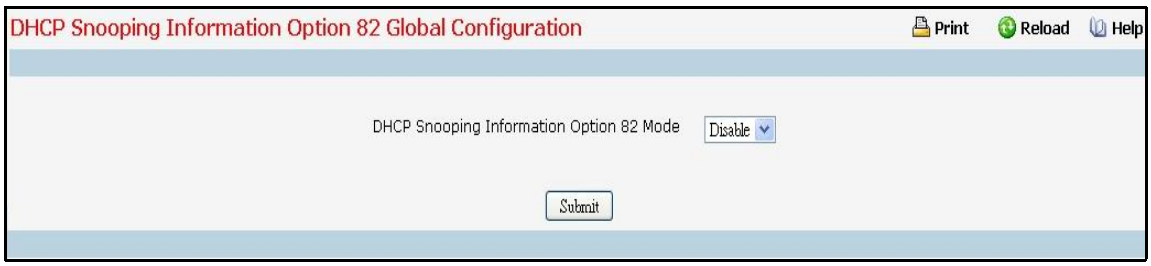
DHCP Server Msgs Received - The number of Server messages that are dropped on an untrusted port.

Command Buttons

Clear Statistics - Clears all interfaces statistics.

11.3.4 DHCP Snooping Information Option 82

11.3.4.1 Configuring DHCP Snooping Information Option 82 Global



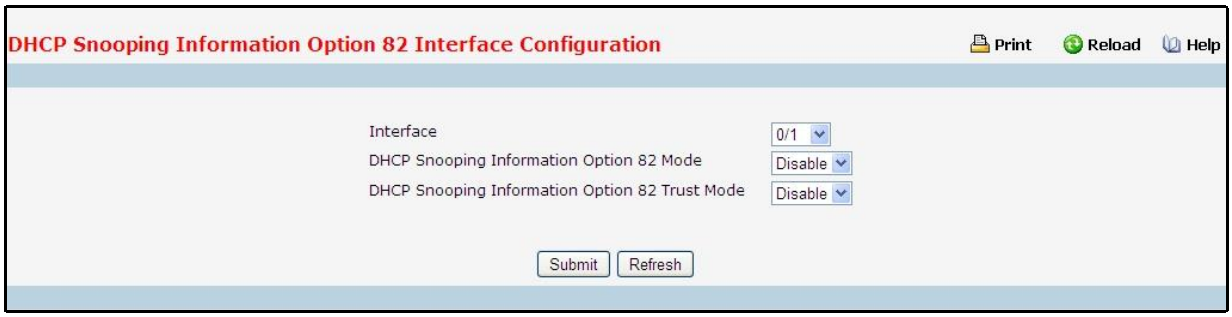
Configurable Data

DHCP Snooping Information Option 82 Mode - Enables or Disables the DHCP Snooping Information Option 82 feature. The factory default is Disable.

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.

11.3.4.2 Configuring DHCP Snooping Information Option 82 Interface



Selection Criteria

Interface - Selects the interface for which data is to be displayed or configured.

Configurable Data

DHCP Snooping Information Option 82 Mode - Enables or Disables DHCP Snooping Information Option 82 Mode on selected interface. The factory default is Disable.

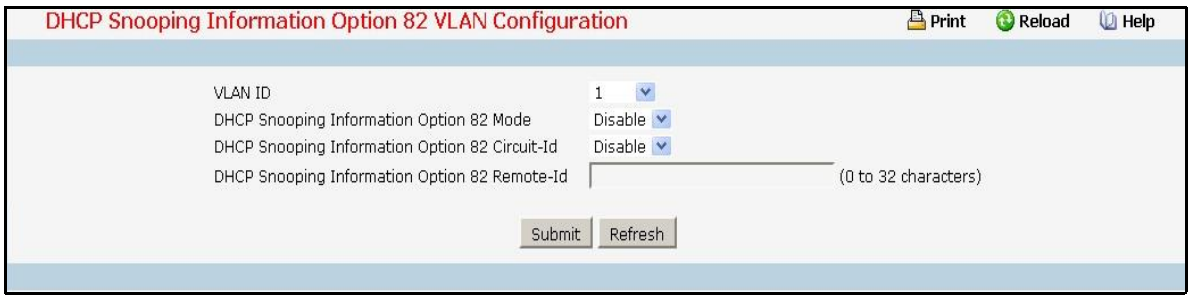
DHCP Snooping Information Option 82 Trust Mode - If this is Enabled, DHCP Snooping Information Option 82 application considers selected port as trusted. The factory default is Disable.

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.

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

11.3.4.3 Configuring DHCP Snooping Information Option 82 VLAN



Selection Criteria

VLAN ID - Selects the VLAN for which data is to be displayed or configured.

Configurable Data

DHCP Snooping Information Option 82 Mode - Enables or Disables the DHCP Snooping Information Option 82 feature on selected VLAN. The factory default is Disable.

DHCP Snooping Information Option 82 Circuit-Id - Enables or Disables the DHCP Snooping Information Option 82 Circuit-Identifier feature on selected VLAN. The factory default is Disable.

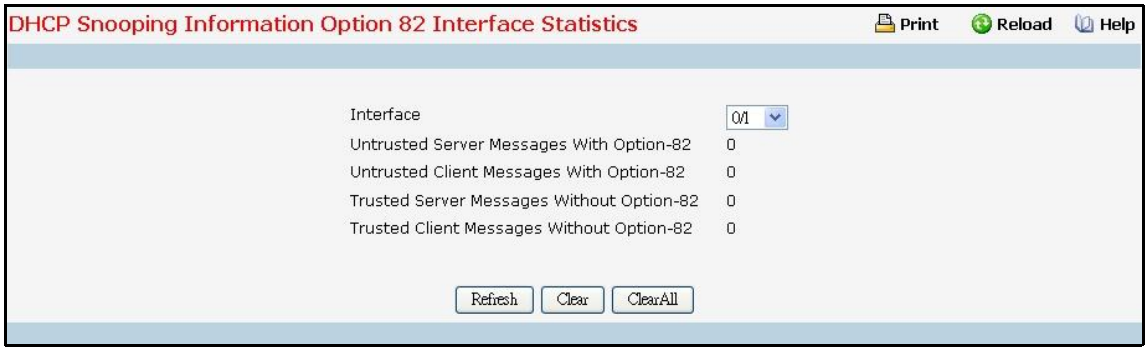
DHCP Snooping Information Option 82 Remote-Id - Sets or Resets the DHCP Snooping Information Option 82 Remote-Identifier string on selected VLAN. The factory default is NULL string. Range is (0 to 32 characters).

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.

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

11.3.4.4 DHCP Snooping Information Option 82 Interface Statistics



Selection Criteria

Interface - Select the DHCP L2 Relay enabled interface for which statistics to be displayed.

Non-Configurable Data

Untrusted Server Messages with Option-82 - Number of DHCP Reply packets received with Option-82 on untrusted DHCP Snooping Information Option 82 interface

Untrusted Client Messages with Option-82 - Number of DHCP Request packets received with Option-82 on untrusted DHCP Snooping Information Option 82 interface.

Trusted Server Messages without Option-82 - Number of DHCP Reply packets received without Option-82 on untrusted DHCP Snooping Information Option 82 interface.

Trusted Client Messages without Option-82 - Number of DHCP Request packets received without Option-82 on untrusted DHCP Snooping Information Option 82 interface.

Command Buttons

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

Clear - Clears statistics for the selected interface

ClearAll - Clears statistics for all the interfaces.

11.3.5 Managing IP Source Guard (IPSG)

11.3.5.1 Configuring IPSG Configuration Page

Selection Criteria

Interface - Select the physical interface for which you want to configure data.

Configurable Data

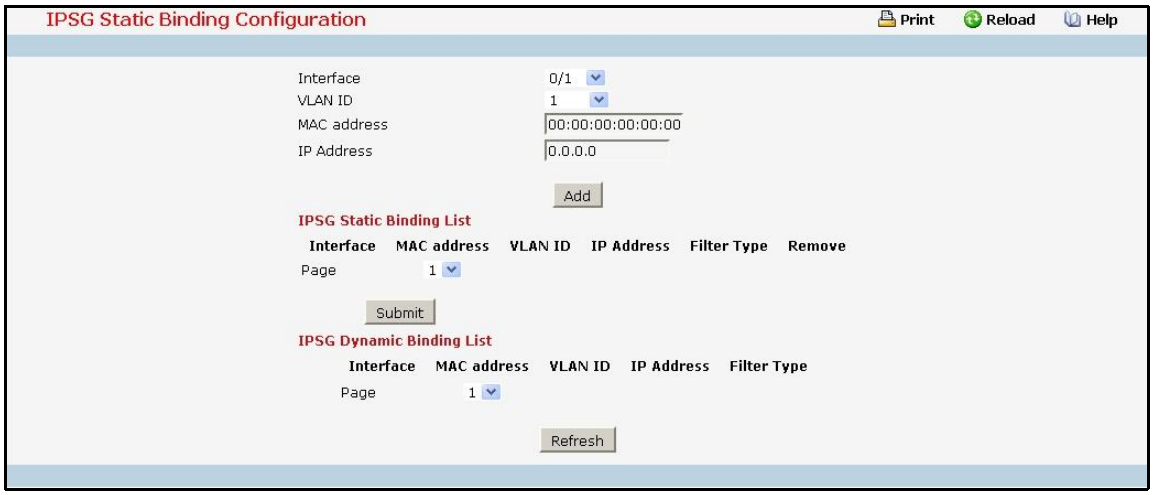
IPSG - Enables or disables validation of Sender IP Address on this interface. If IPSG is Enabled Packets will not be forwarded if Sender IP Address is not in DHCP Snooping Binding database. The factory default is disabled.

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.

11.3.5.2 Configuring IPSG Static Binding Configuration Page



Configurable Data

Interface - 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.

- Interface - 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.

- Interface - 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

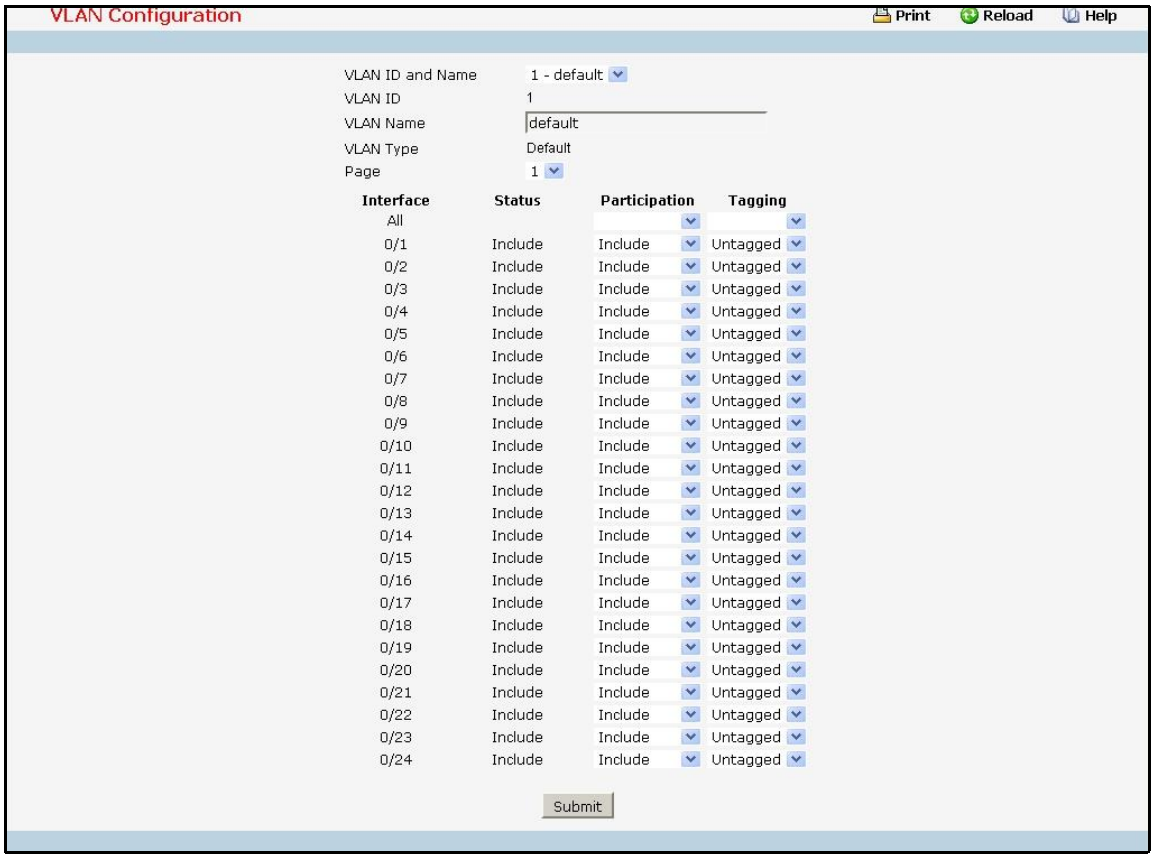
Add - Adds DHCP snooping binding entry into the database.

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.

11.3.6 Managing Port-Based VLAN

11.3.6.1 VLAN Configuration



Selection Criteria

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

Configurable Data

VLAN ID - Specify the VLAN Identifier for the new VLAN. (You can only enter data in this field when you are creating a new VLAN.) The range of the VLAN ID is (1 to 4093).

VLAN Name - Use this optional field to specify a name for the VLAN. It can be up to 32 alphanumeric characters long, including blanks. The default is blank. VLAN ID 1 always has a name of 'Default'.

VLAN Type - This field identifies the type of the VLAN you are configuring. You cannot change the type of the default VLAN (VLAN ID = 1): it is always type 'Default'. When you create a VLAN, using this screen, its type will always be 'Static'. A VLAN that is created by GVRP registration initially has a type of 'Dynamic'. You may use this pull-down menu to change its type to 'Static'.

Participation - Use this field to specify whether a port will participate in this VLAN. The factory default is 'Autodetect'. The possible values are:

- Include - This port is always a member of this VLAN. This is equivalent to registration fixed in the IEEE 802.1Q standard.
- Exclude - This port is never a member of this VLAN. This is equivalent to registration forbidden in the IEEE 802.1Q standard.
- Autodetect - Specifies that port may be dynamically registered in this VLAN via GVRP. The port will not participate in this VLAN unless it receives a GVRP request. This is equivalent to registration normal in the IEEE 802.1Q standard.

Tagging - Select the tagging behavior for this port in this VLAN. The factory default is 'Untagged'. The possible values are:

- Tagged - all frames transmitted for this VLAN will be tagged.
- Untagged - all frames transmitted for this VLAN will be untagged

Non-Configurable Data

Interface - 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.

11.3.6.2 VLAN Status

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 4093).

VLAN Name - The name of the VLAN. VLAN ID 1 is always named `Default`.

VLAN Type - The VLAN type:

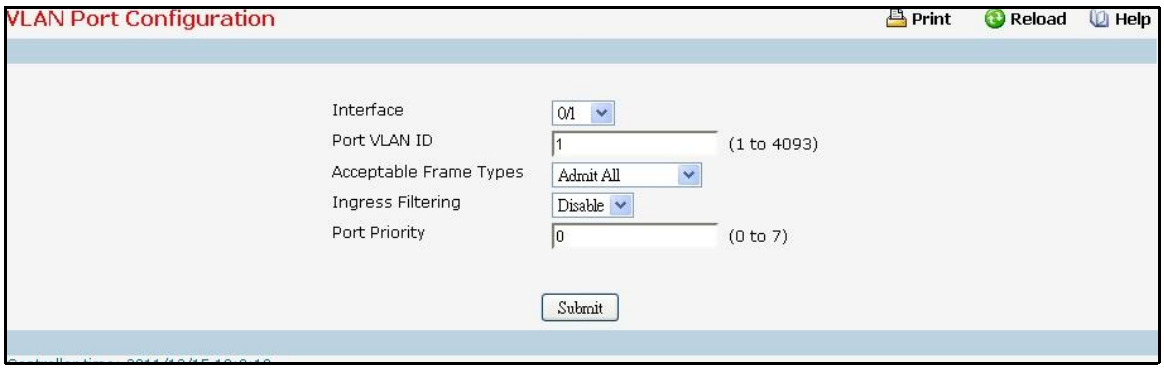
- Default (VLAN ID = 1) -- always present
- Static -- a VLAN you have configured
- Dynamic -- a VLAN created by GVRP registration that you have not converted to static, and that GVRP may therefore remove

Interface - Indicates which port is associated with the fields on this line.

Command Buttons

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

11.3.6.3 VLAN Port Configuration



Selection Criteria

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

Configurable Data

Port VLAN ID - Specify the VLAN ID you want assigned to untagged or priority tagged frames received on this port. The value ranges (1 to 4093). The factory default is 1 .

Acceptable Frame Types - Specify how you want the port to handle untagged and priority tagged frames. If you select 'AdmitTaggedOnly', the port will discard any untagged or priority tagged frames it receives. If you select 'AdmitUntaggedOnly', the port discard 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'.

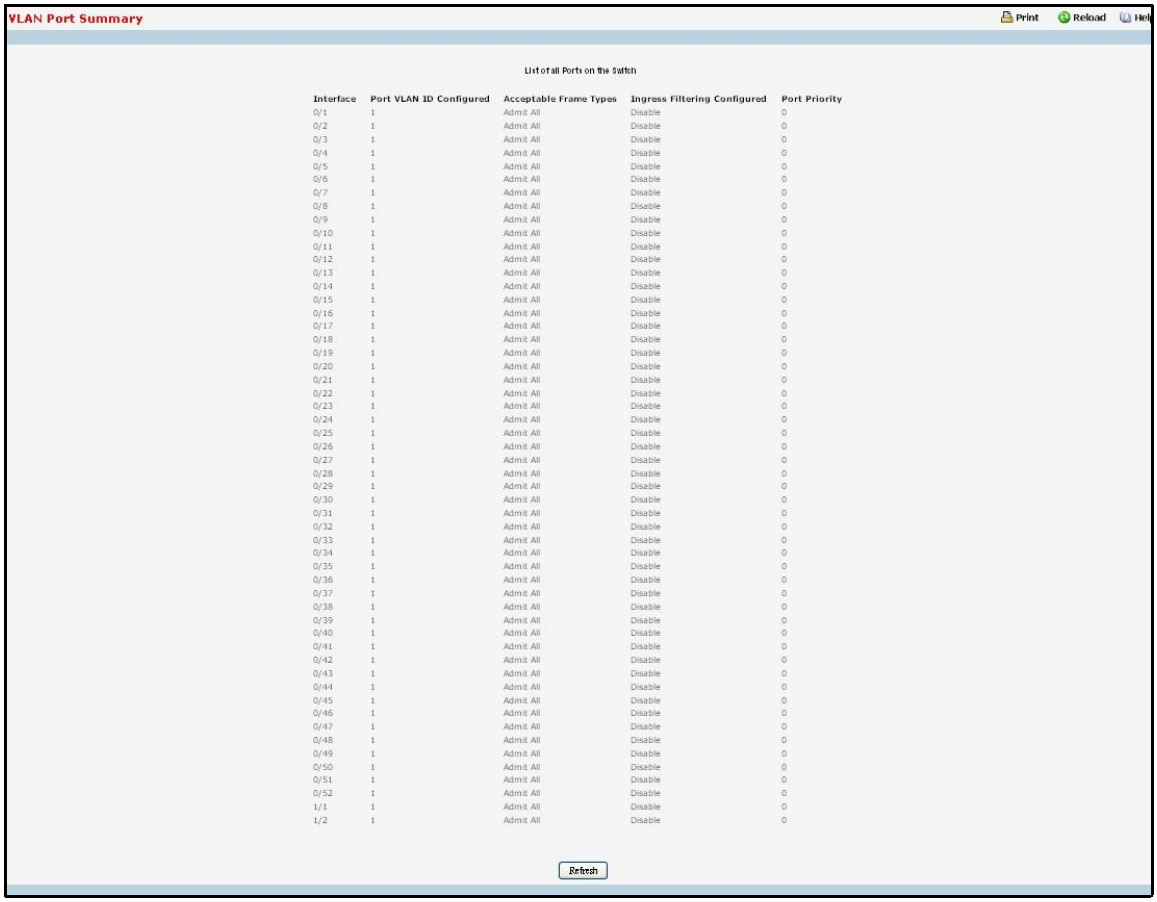
Ingress Filtering - Specify how you want the port to handle tagged frames. If you enable Ingress Filtering on the pull-down menu, a tagged frame will be discarded if this port is not a member of the VLAN identified by the VLAN ID in the tag. If you select disable from the pull-down menu, all tagged frames will be accepted. The factory default is disable.

Port Priority - Specify the default 802.1p priority assigned to untagged packets arriving at the port. The value ranges from (0 to 7) .Default value is 0.

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.

11.3.6.4 VLAN Port Summary



Non-Configurable Data

Interface - The interface.

Port VLAN ID Configured - 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 Configured - 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.

Command Buttons

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

11.3.6.5 Reset VLAN Configuration

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.

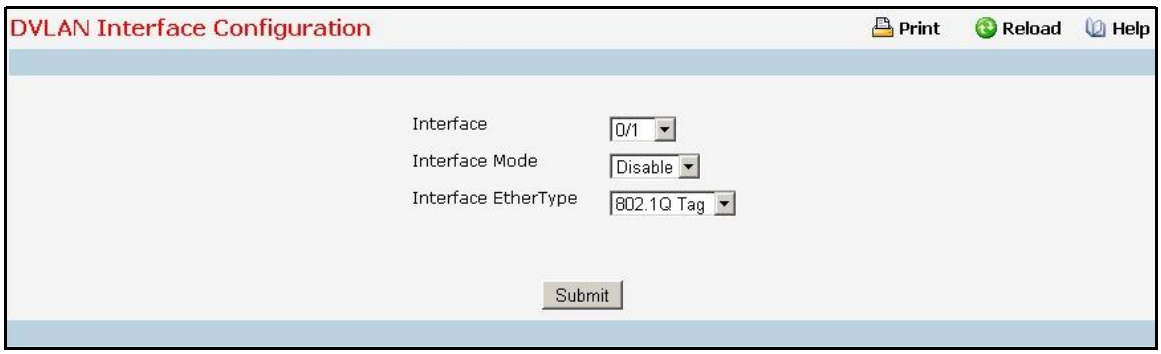
- All ports are configured to an Acceptable Frame Types value of Admit All Frames. ●

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.

11.3.7 Managing DVLAN

11.3.7.1 DVLAN Interface Configuration



Selection Criteria

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

Configurable Data

Interface Mode - This specifies the administrative mode via which Double VLAN Tagging can be enabled or disabled. The default value for this is Disable

Interface EtherType - The two-byte hex EtherType to be used as the first 16 bits of the DVLAN tag.

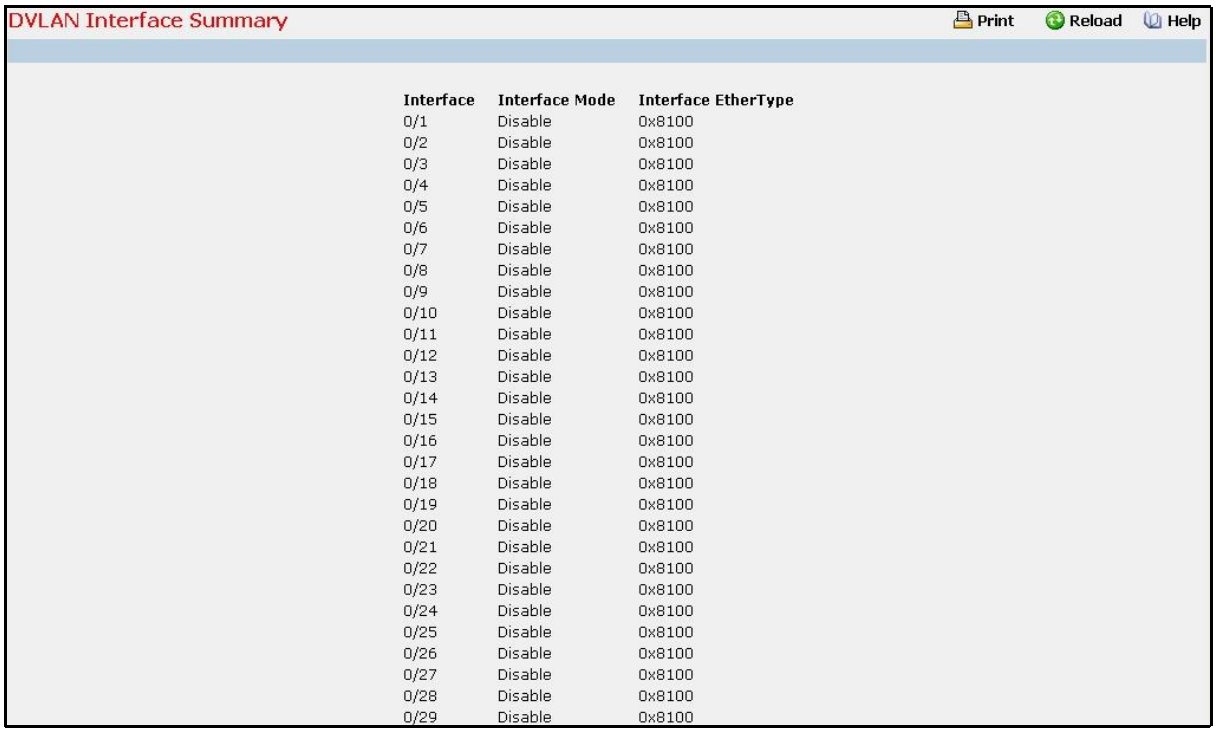
- 802.1Q Tag - Commonly used tag representing 0x8100
- vMAN Tag - Commonly used tag representing 0x88A8
- Custom Tag - Configure the EtherType by providing a Custom value

Custom Value - Configure the value of the Custom Tag in the range from (1 to 65535). This feild is visible only when Custom Tag is selected.

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.

11.3.7.2 DVLAN Interface Summary



Interface	Interface Mode	Interface EtherType
0/1	Disable	0x8100
0/2	Disable	0x8100
0/3	Disable	0x8100
0/4	Disable	0x8100
0/5	Disable	0x8100
0/6	Disable	0x8100
0/7	Disable	0x8100
0/8	Disable	0x8100
0/9	Disable	0x8100
0/10	Disable	0x8100
0/11	Disable	0x8100
0/12	Disable	0x8100
0/13	Disable	0x8100
0/14	Disable	0x8100
0/15	Disable	0x8100
0/16	Disable	0x8100
0/17	Disable	0x8100
0/18	Disable	0x8100
0/19	Disable	0x8100
0/20	Disable	0x8100
0/21	Disable	0x8100
0/22	Disable	0x8100
0/23	Disable	0x8100
0/24	Disable	0x8100
0/25	Disable	0x8100
0/26	Disable	0x8100
0/27	Disable	0x8100
0/28	Disable	0x8100
0/29	Disable	0x8100

Non-Configurable Data

Interface - 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.

Interface EtherType - This specifies the Interface EtherType configured.

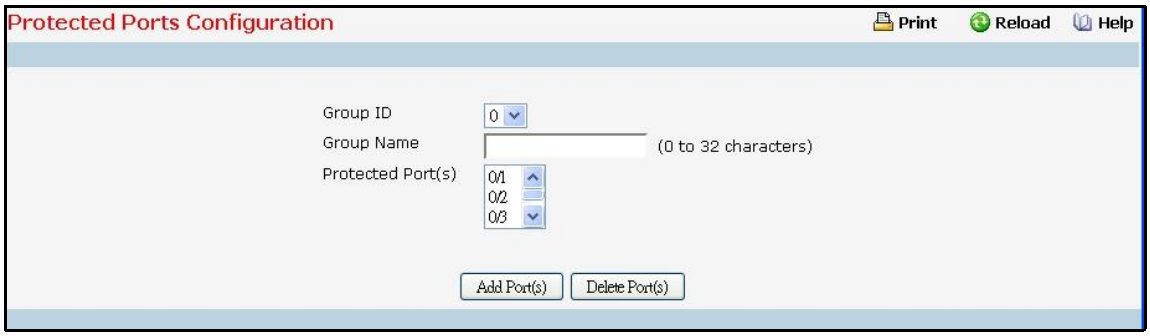
Command Buttons

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

11.3.8 Managing Protected Ports

11.3.8.1 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

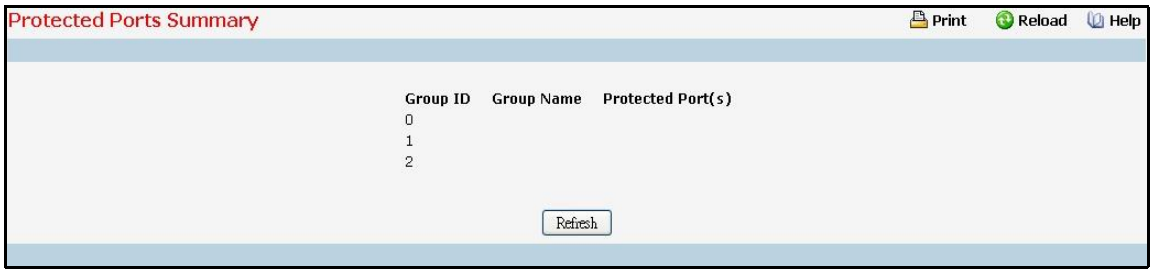
Group Name - It is a name associated with the protected ports group used for identification purposes. It can be up to 32 alphanumeric characters long, including blanks. The default is blank. This field is optional.

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.

11.3.8.2 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.

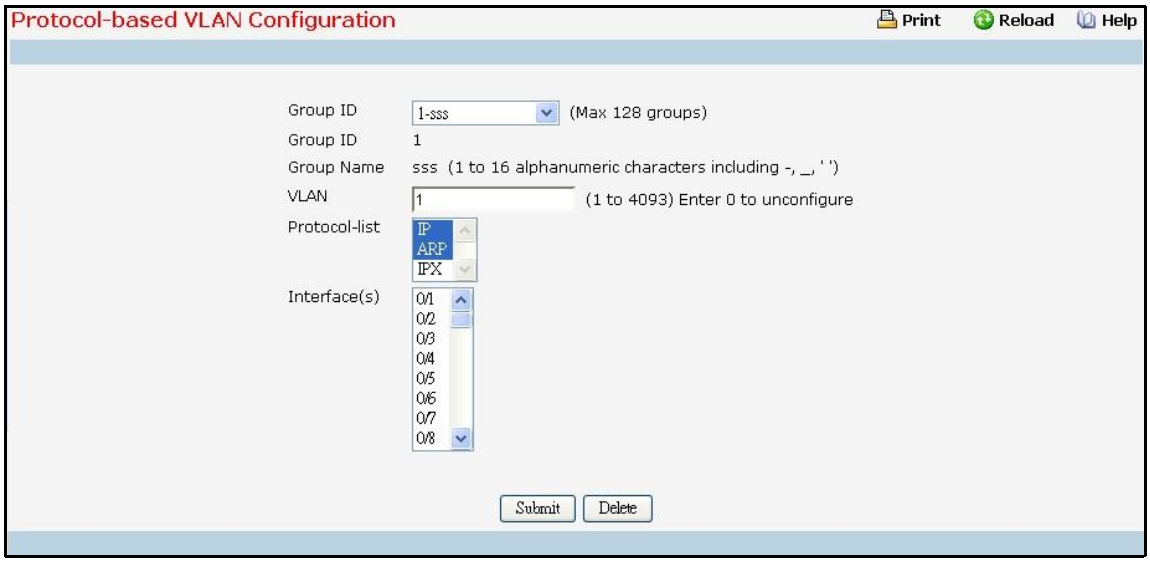
11.3.9 Managing Protocol-based VLAN

11.3.9.1 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 4093) . All the ports in the group will assign this VLAN ID to untagged packets received for the protocols you included in this group.

Interface(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

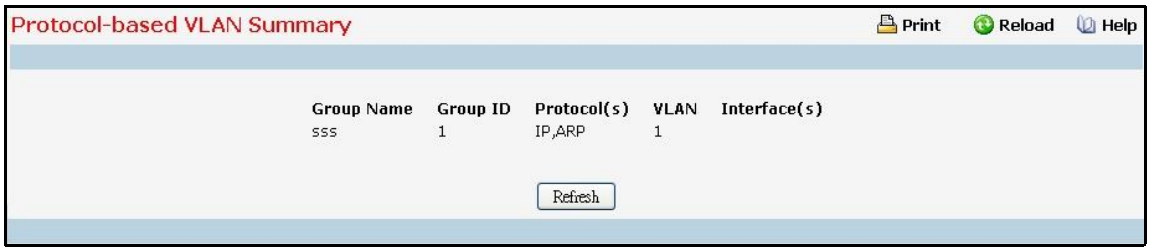
Group ID - A number used to identify the group created by the user. Group IDs are automatically assigned when a group is created by the user.

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.

11.3.9.2 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.

Interface(s) - The interfaces associated with the group.

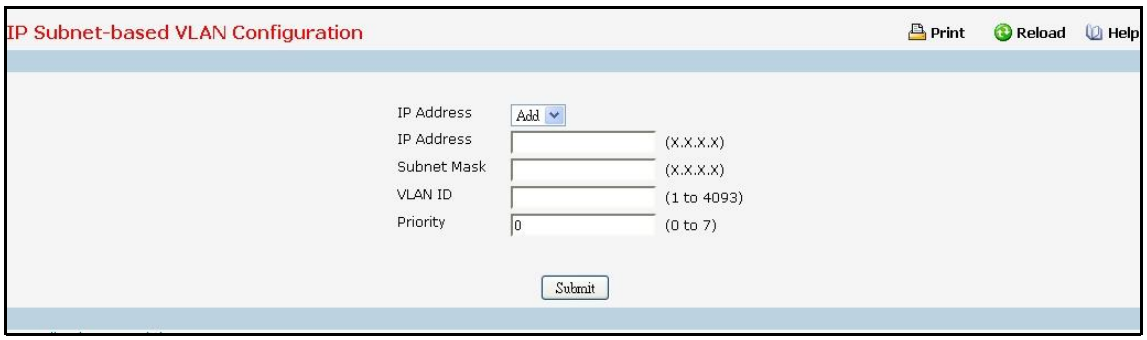
Command Buttons

Refresh - Update the screen with the latest information.

11.3.10 Managing IP Subnet-based VLAN

11.3.10.1 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 4093).

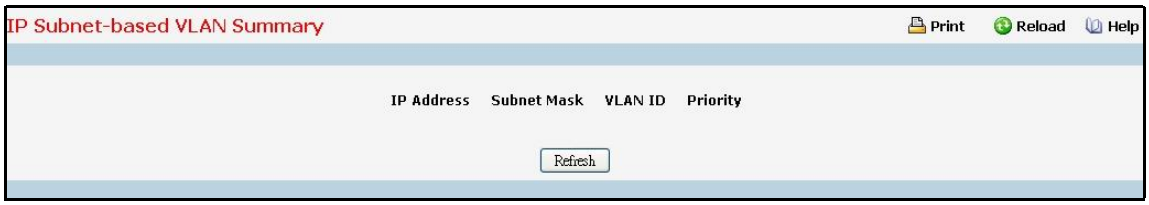
Priority - Priority can be any number in the range of (0 to 7).

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.

11.3.10.2 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 4093).

Priority - The Priority to which above mentioned IP Subnet is being bound.

Command Buttons

Refresh - Update the screen with the latest information.

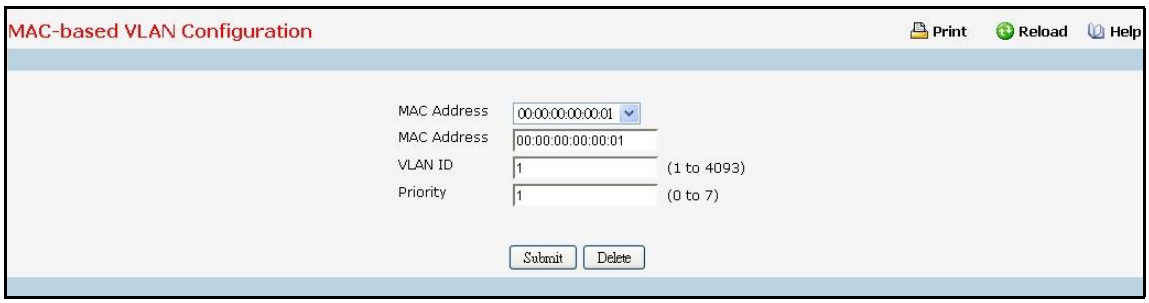
11.3.11 Managing MAC-based VLAN

11.3.11.1 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.



Selection Criteria

MAC Address - Selects the MAC Address bound to a VLAN. To add another MAC VLAN entry, select "Add" option.

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.

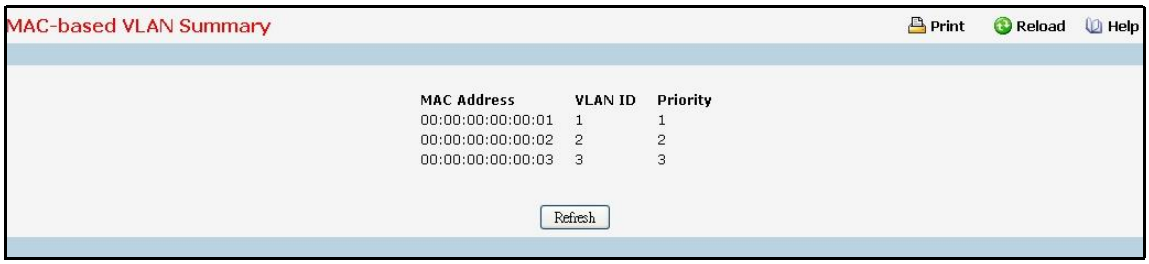
VLAN ID - VLAN ID can be any number in the range of (1 to 4093).

Priority - Priority can be any number in the range of (0 to 7).

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.

11.3.11.2 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.

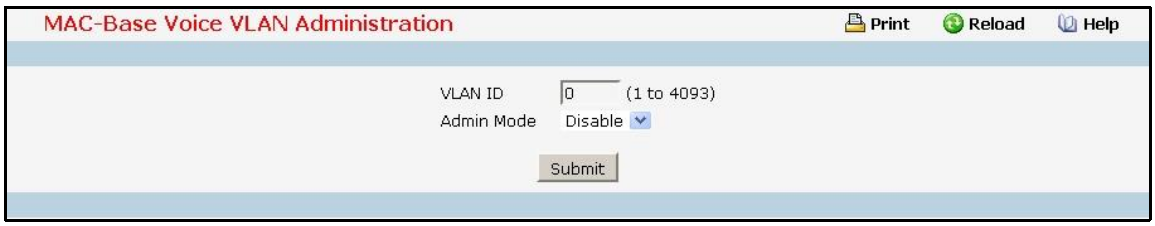
Priority - The Priority to which a MAC Address is bound.

Command Buttons

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

11.3.12 Managing MAC-based Voice VLAN

11.3.12.1 MAC-based Voice VLAN Administration Page



Configurable Data

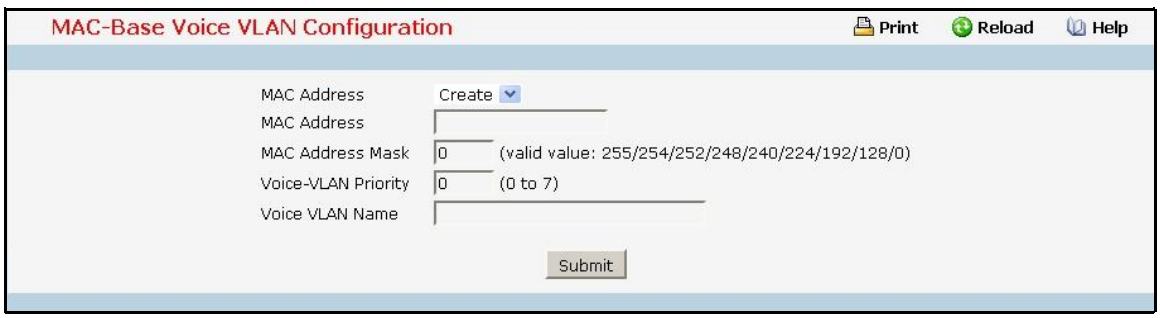
VLAN ID - Sets the VLAN as a Voice VLAN.

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.

11.3.12.2 MAC-based Voice VLAN Configuration Page



Selection Criteria

MAC Address - You can use this screen to create a new one. Use this pull-down 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:C2:00:00:2F

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.

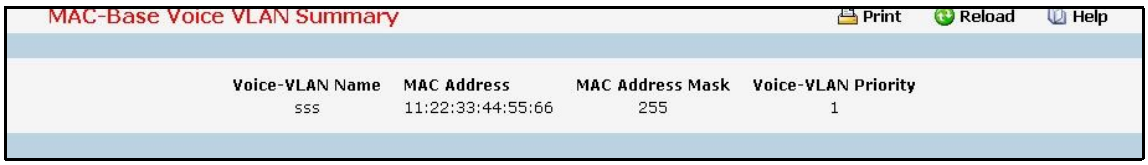
Command Buttons

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.

11.3.12.3 Viewing MAC-based 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.

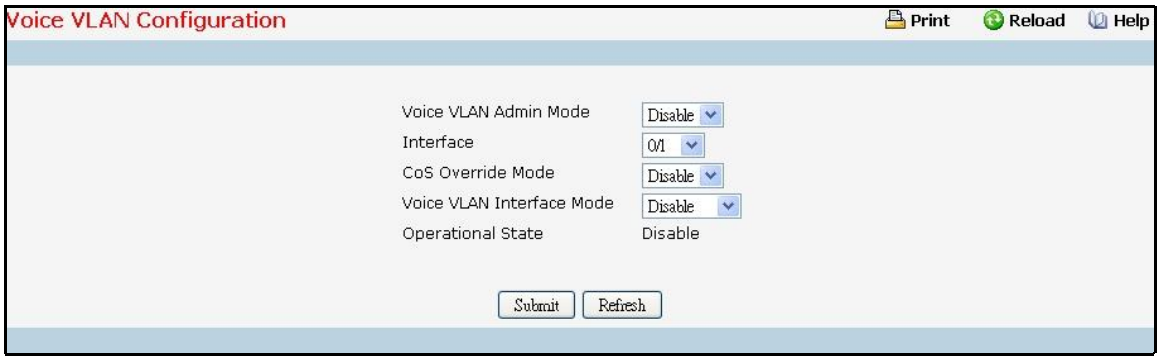
MAC Address Mask - The MAC Address Mask for the Voice VLAN. The value is the last eight digit of the mask code of the MAC address.

Voice-VLAN Priority - The priority-id is the priority of the voice traffic.

11.3.13 Managing Voice VLAN

11.3.13.1 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 pull-down menu. The default is Disable.

Interface - 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.

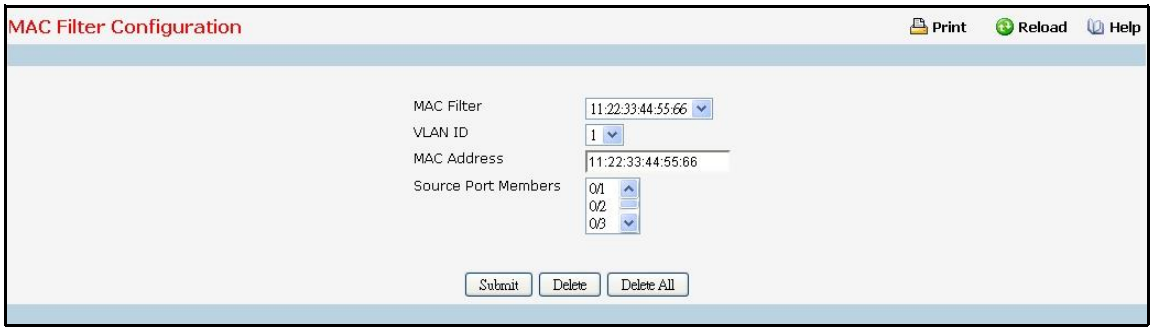
Command Buttons

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

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

11.3.14 Managing MAC Filters

11.3.14.1 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" 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
- 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

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.

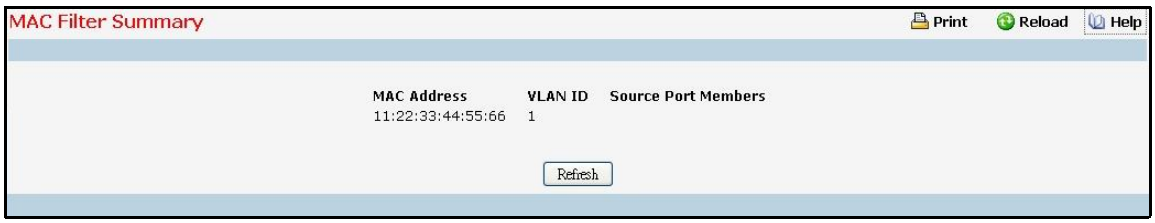
Command Buttons

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.

11.3.14.2 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.

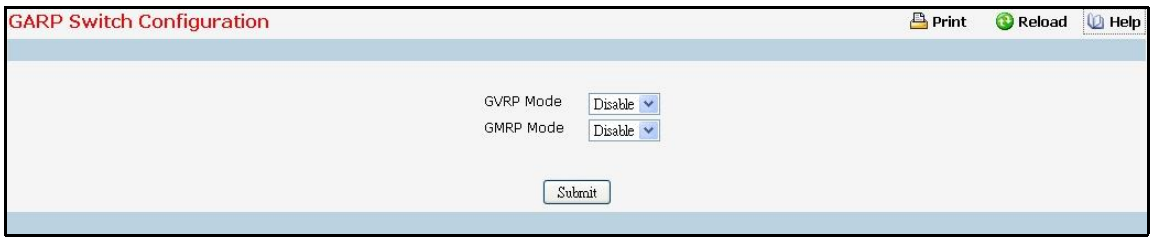
Source Port Members - A list of ports to be used for filtering inbound packets.

Command Buttons

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

11.3.15 Managing GARP

11.3.15.1 Configuring the whole Switch GARP Configuration Page



It can take up to 10 seconds for GARP configuration changes to take effect.

Configurable Data

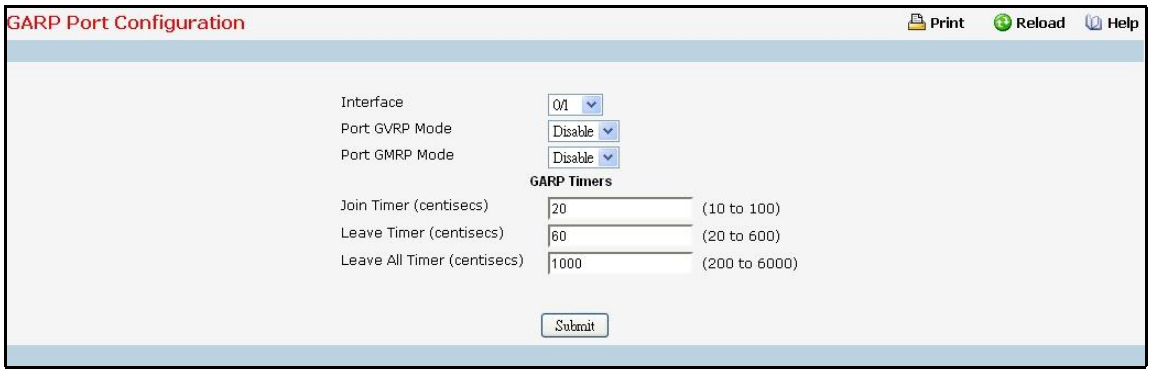
GVRP Mode - Choose the GARP VLAN Registration Protocol administrative mode for the switch by selecting enable or disable from the pull down menu. The factory default is disabled.

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.

11.3.15.2 Configuring each Port GARP Configuration Page



It can take up to 10 seconds for GARP configuration changes to take effect.

Selection Criteria

Interface - 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'.

Configurable Data

Port GVRP Mode - Choose the GARP VLAN Registration Protocol administrative mode for the port by selecting enable or disable from the pull down menu. If you select disable, the protocol will not be active and the Join Time, Leave Time, and Leave All Time will have no effect. The factory default is disabled.

Port GMRP Mode - Choose the GARP Multicast Registration Protocol administrative mode for the port by selecting enable or disable from the pull down menu. If you select disable, the protocol will not be active, and Join Time, Leave Time, and Leave All Time have no effect. The factory default is disabled.

Join Time (centiseconds) - Specify the time between the transmission of GARP PDUs registering (or re-registering) membership for a VLAN or multicast group in centiseconds. Enter a number between 10 and 100 (0.1 to 1.0 seconds). The factory default is 20 centiseconds (0.2 seconds). An instance of this timer exists for each GARP participant for each port.

Leave Time (centiseconds) - Specify the time to wait after receiving an unregister request for a VLAN or multicast group before deleting the associated entry, in centiseconds. This allows time for another station to assert registration for the same attribute in order to maintain uninterrupted service. Enter a number between 30 and 600 (0.3 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.

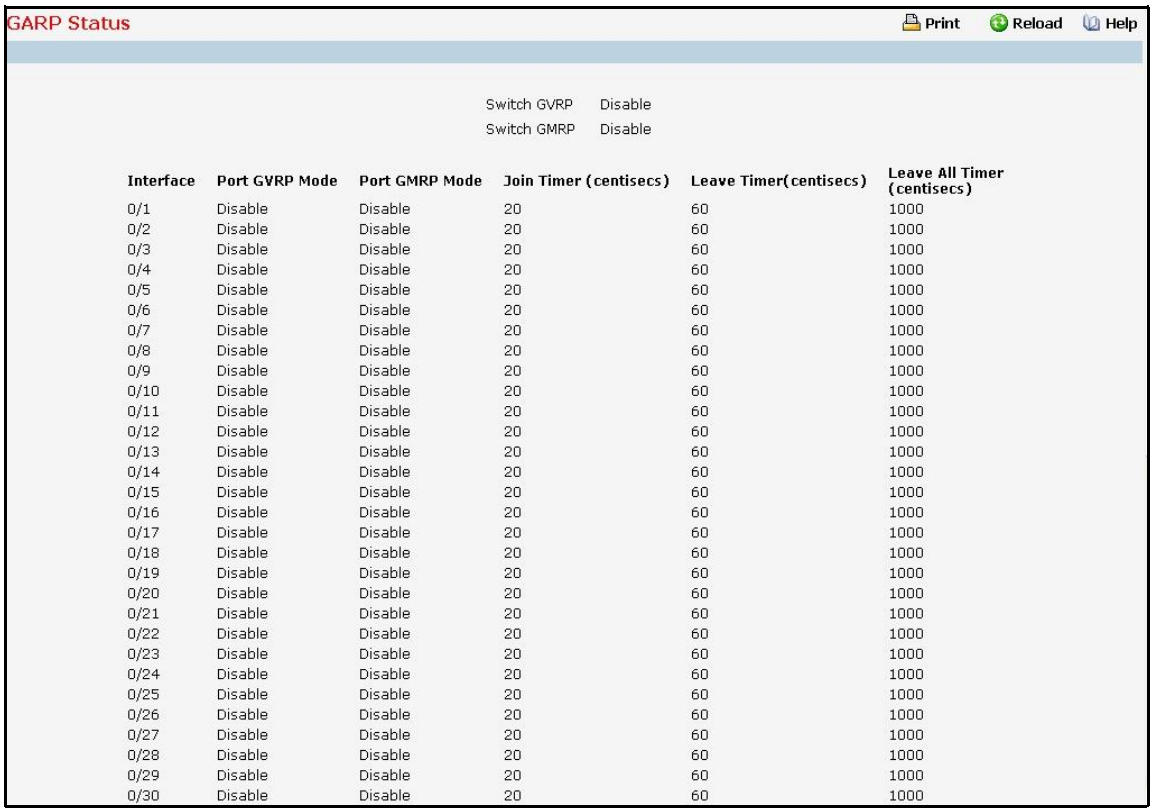
Leave All Time (centiseconds) - The Leave All Time controls how frequently LeaveAll PDUs are generated. A LeaveAll PDU indicates that all registrations will shortly be deregistered. Participants will need to rejoin in order to maintain registration. The Leave All Period Timer is set to a random value 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.

11.3.15.3 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.



Interface	Port GVRP Mode	Port GMRP Mode	Join Timer (centisecs)	Leave Timer(centisecs)	Leave All Timer (centisecs)
0/1	Disable	Disable	20	60	1000
0/2	Disable	Disable	20	60	1000
0/3	Disable	Disable	20	60	1000
0/4	Disable	Disable	20	60	1000
0/5	Disable	Disable	20	60	1000
0/6	Disable	Disable	20	60	1000
0/7	Disable	Disable	20	60	1000
0/8	Disable	Disable	20	60	1000
0/9	Disable	Disable	20	60	1000
0/10	Disable	Disable	20	60	1000
0/11	Disable	Disable	20	60	1000
0/12	Disable	Disable	20	60	1000
0/13	Disable	Disable	20	60	1000
0/14	Disable	Disable	20	60	1000
0/15	Disable	Disable	20	60	1000
0/16	Disable	Disable	20	60	1000
0/17	Disable	Disable	20	60	1000
0/18	Disable	Disable	20	60	1000
0/19	Disable	Disable	20	60	1000
0/20	Disable	Disable	20	60	1000
0/21	Disable	Disable	20	60	1000
0/22	Disable	Disable	20	60	1000
0/23	Disable	Disable	20	60	1000
0/24	Disable	Disable	20	60	1000
0/25	Disable	Disable	20	60	1000
0/26	Disable	Disable	20	60	1000
0/27	Disable	Disable	20	60	1000
0/28	Disable	Disable	20	60	1000
0/29	Disable	Disable	20	60	1000
0/30	Disable	Disable	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.

Interface - 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 30 to 600 centiseconds (0.3 to 6.0 seconds). The factory default is 60 centiseconds (0.6 seconds).

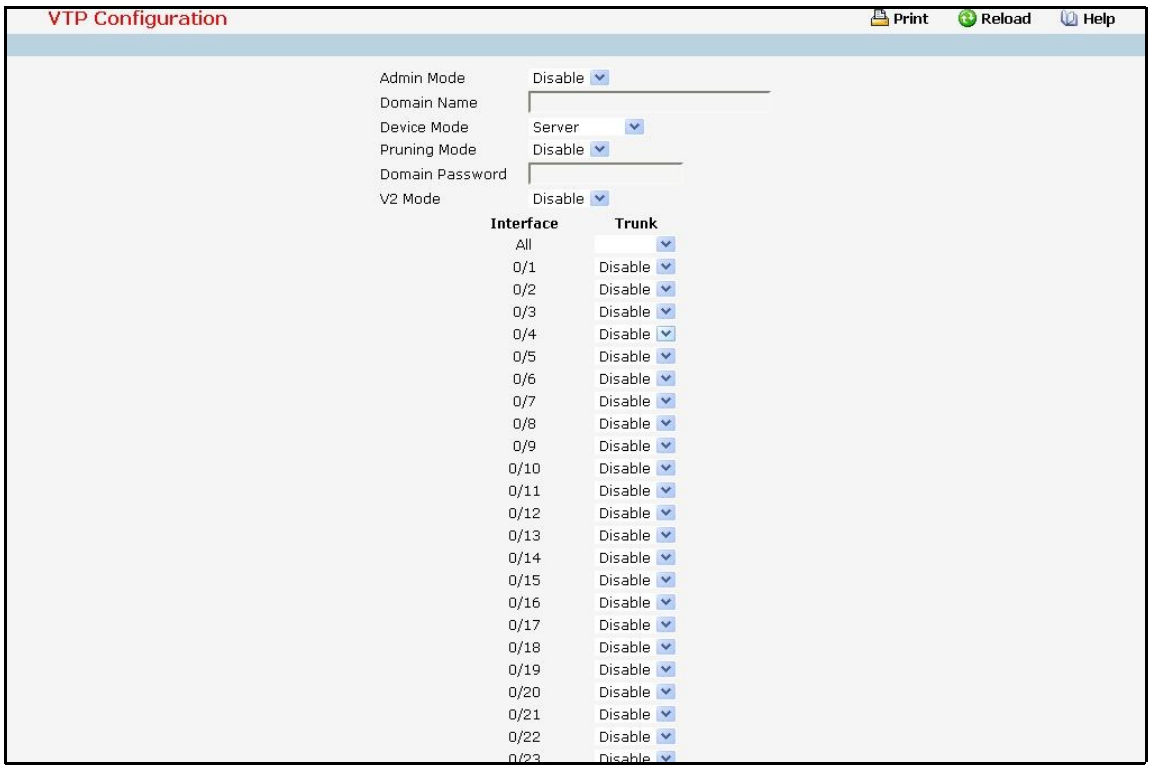
Leave All Time (centiseconds) -This Leave All Time controls how frequently LeaveAll PDUs are generated. A LeaveAll PDU indicates that all registrations will shortly be deregistered. Participants will need to rejoin in order to maintain registration. An instance of this timer exists for each GARP participant 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).

Command Buttons

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

11.3.16 Managing VTP

11.3.16.1 Configuring VTP Configuration Page



Configurable Data

Admin Mode - Enable or disable the VTP feature.

Device Mode - Use the pull-down 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.

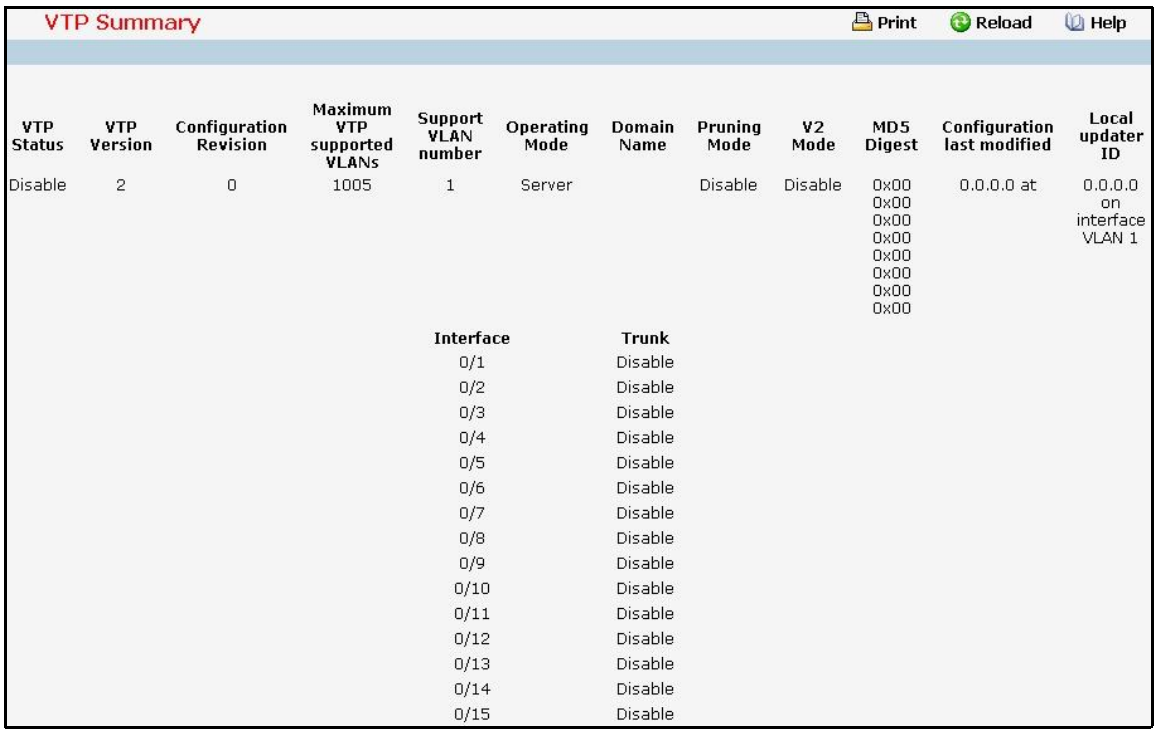
Domain Name - Set the name of the VTP administrative domain.

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.

11.3.16.2 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.

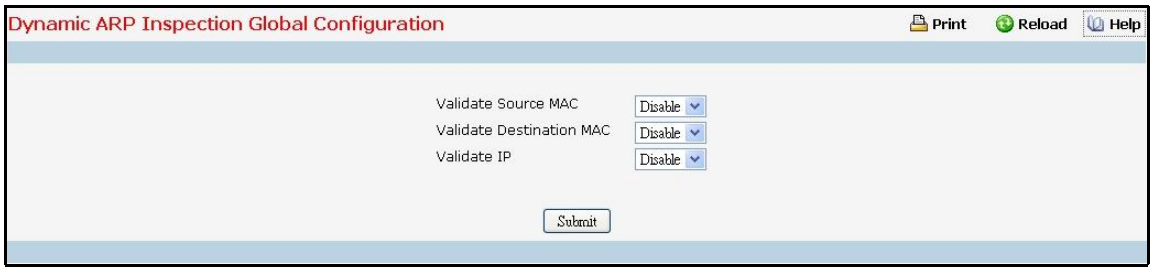
Configuration last modified - Displays the time stamp of the last configuration modification and the IP address of the switch that caused the configuration change to the database.

Local updater ID - Displays the Local updater ID for the VTP domain status.

Trunkport - Displays the VTP trunkport.

11.3.17 Managing Dynamic ARP Inspection (DAI)

11.3.17.1 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.

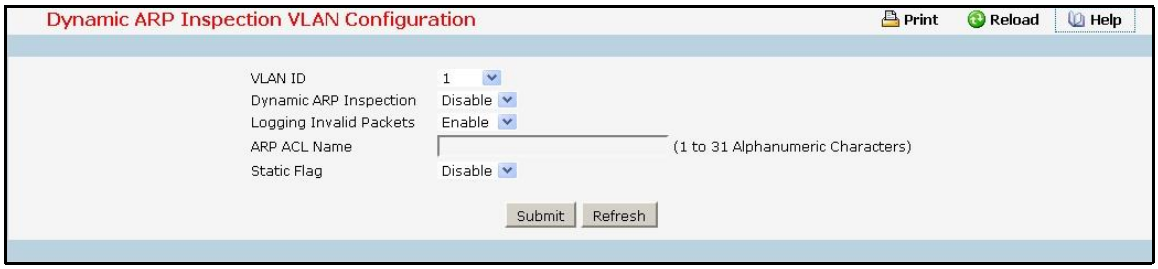
Validate Destination MAC - Choose the DAI Destination MAC Validation Mode for the switch by selecting Enable or Disable from the pull down menu. If you select Enable, Destination MAC validation for the ARP Response packets will be enabled. The factory default is disable.

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.

11.3.17.2 Configuring DAI VLAN Configuration Page



Selection Criteria

VLAN ID - 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.

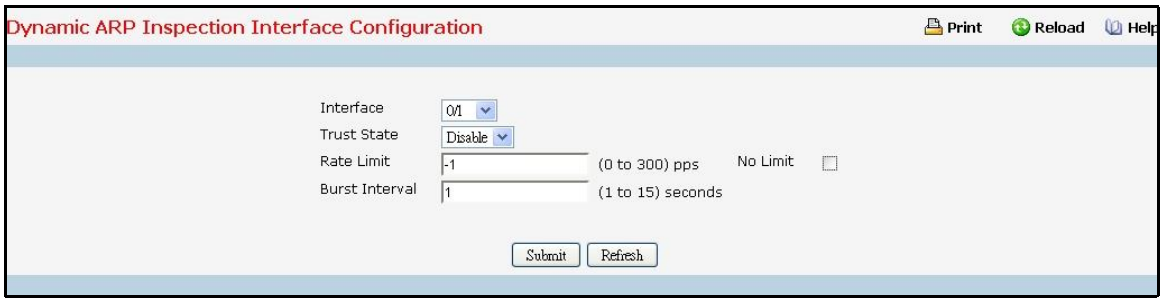
Static Flag - This flag is used to determine whether the ARP packet needs validation using the DHCP snooping database in case ARP ACL rules don't match. If the flag is enabled then the ARP Packet will be validated by the ARP ACL Rules only. If the flag is disabled then the ARP Packet needs further validation 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.

11.3.17.3 Configuring DAI Interface Configuration Page



Selection Criteria

Interface - 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 -1 there is no limit. The Range is (0 to 300 pps). The factory default is 15pps (packets per second).

No Limit - Selecting this option specifies that the value of Rate Limit will be configured to -1. If the rate limit is -1 burst interval has no meaning, hence it is disabled.

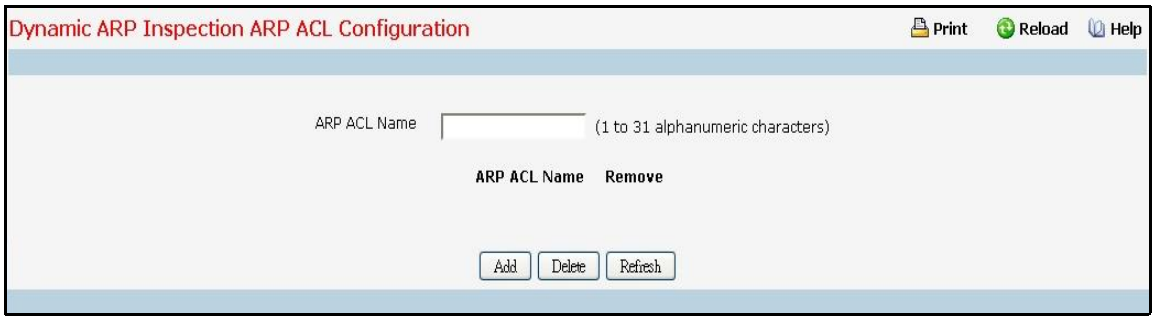
Burst Interval - This Specifies the burst interval value for rate limiting purpose on this interface. The Range is (1 to 15 seconds). If the rate limit is -1 burst interval has no meaning. The factory default is 1 second.

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.

11.3.17.4 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.

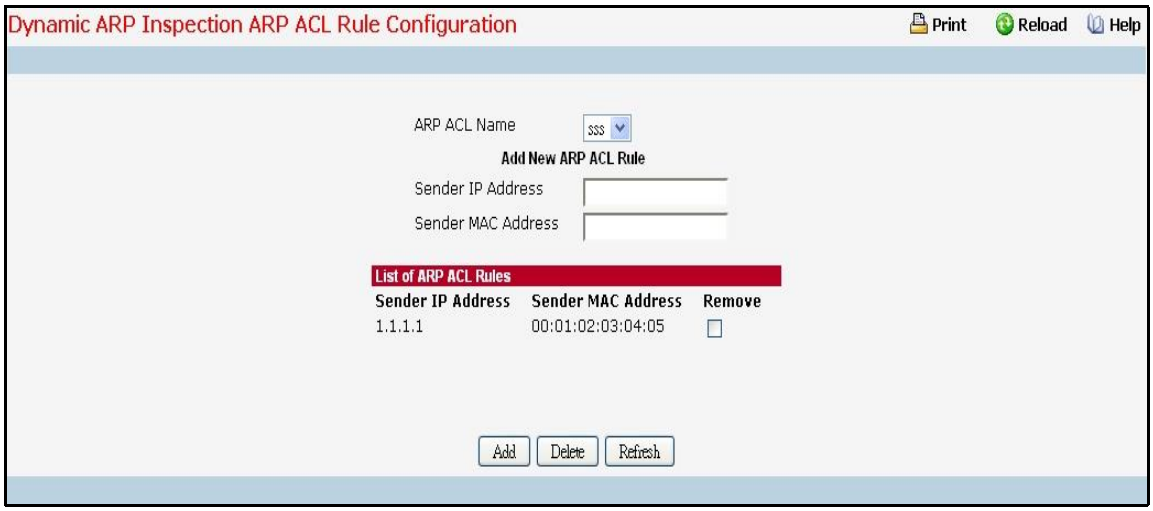
Command Buttons

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.

11.3.17.5 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.

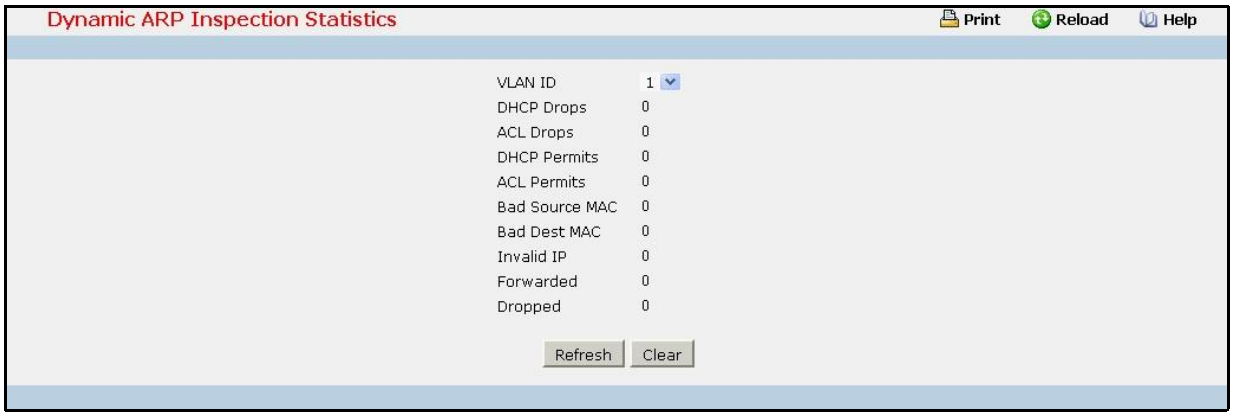
Command Buttons

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.

11.3.17.6 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.

11.3.18 Managing IGMP Snooping

11.3.18.1 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.

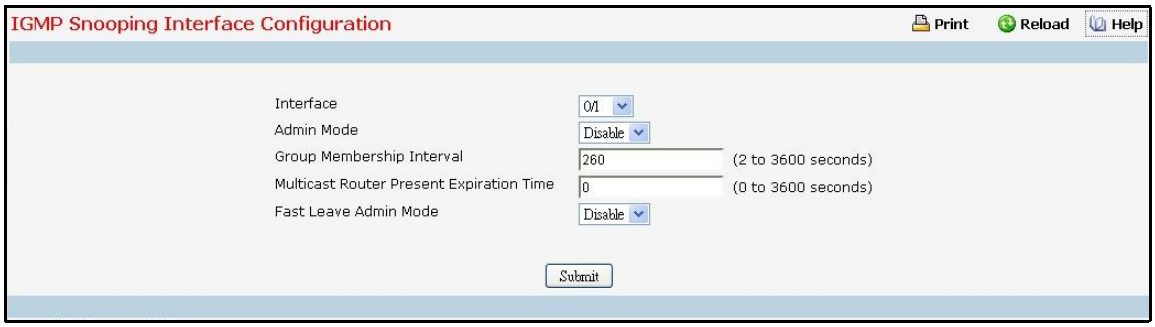
Data Frames Forwarded by the CPU - The number of data frames forwarded by the CPU.

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.

11.3.18.2 Defining IGMP Snooping Interface Configuration Page



Selection Criteria

Interface - 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 pull-down menu. The default is disable.

Fast Leave Admin mode - Select the Fast Leave mode for a particular interface from the pull-down menu. The default is disable.

Configurable Data

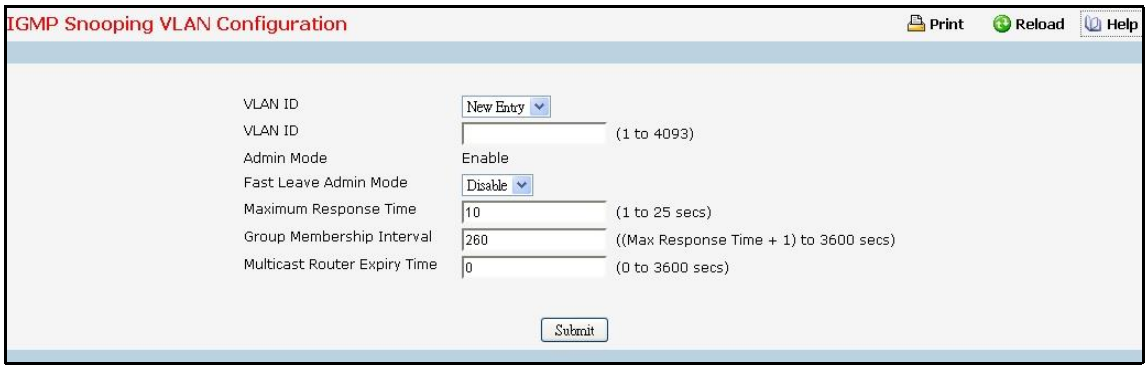
Group Membership Interval - Specify the amount of time you want the switch to wait for a report for a particular group on a particular interface before it deletes that interface from the group. Enter a value between 1 and 3600 seconds. The default is 260 seconds.

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.

11.3.18.3 Configuring IGMP Snooping VLAN Page



Selection Criteria

VLAN ID - Specifies list of VLAN IDs for which IGMP Snooping is enabled.

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.

Fast Leave Admin Mode - Enable or disable the IGMP Snooping Fast Leave Mode for the specified VLAN ID.

Group Membership Interval - Sets the value for group membership interval of IGMP Snooping for the specified VLAN ID. Valid range is (Maximum Response Time + 1) to 3600.

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

Non-Configurable Data

Admin Mode - Enable or disable the IGMP Snooping for the specified VLAN ID.

Command Buttons

Submit - Update the switch with the values you entered.

Disable - Update the switch with the default values.

11.3.18.4 Viewing IGMP Snooping VLAN Status Page

Non-Configurable Data

VLAN ID - All VLAN Ids for which the IGMP Snooping mode is Enable.

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.

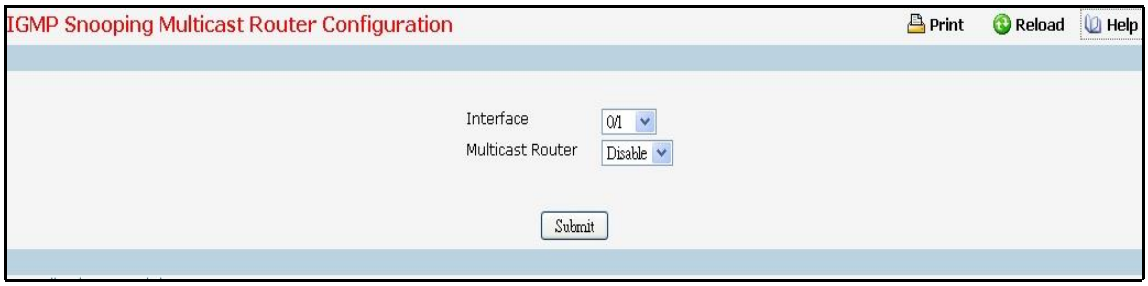
Maximum Response Time - Maximum Response Time of IGMP Snooping for the specified VLAN ID. Valid range is 1 to 25.Its value should be greater than group membership interval value.

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

11.3.18.5 Configuring Multicast Router Page



Selection Criteria

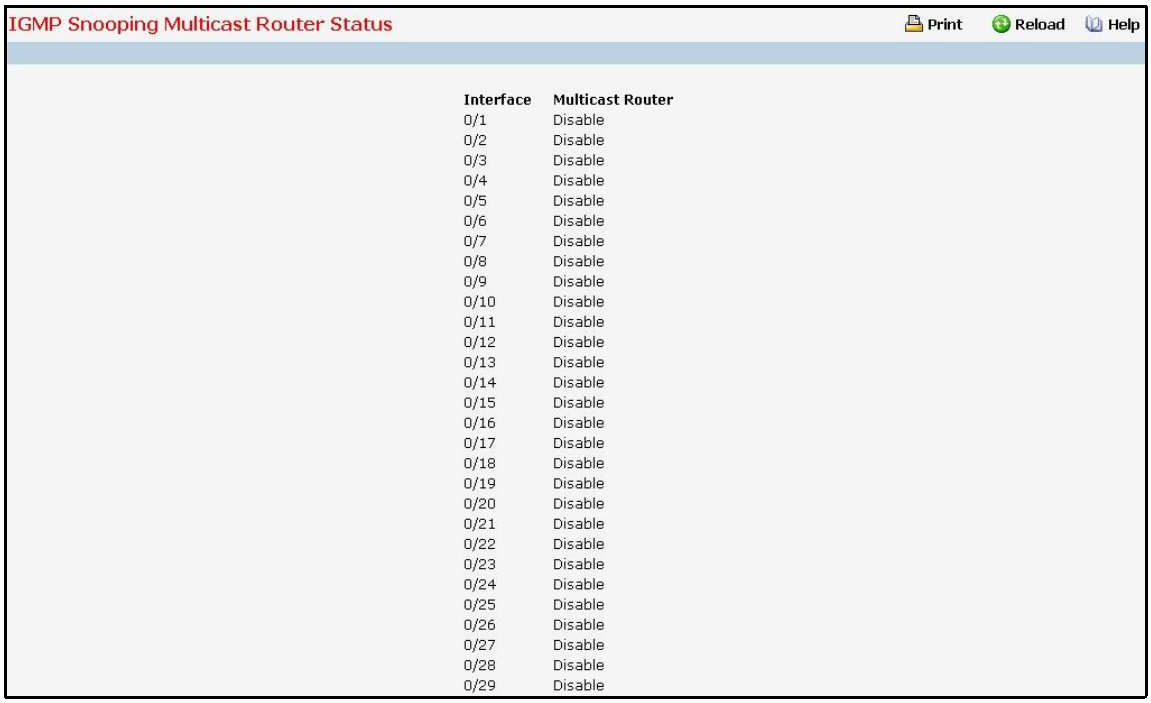
Interface - The select box lists all interfaces. Select the interface for which you want Multicast Router to be enabled.

Multicast Router - Enable or disable Multicast Router on the selected Slot/Port.

Command Buttons

Submit - Update the switch with the values you entered.

11.3.18.6 Viewing Multicast Router Statistics Page



Selection Criteria

Interface - The single select box lists all physical and LAG interfaces. Select the interface for which you want to display the statistics.

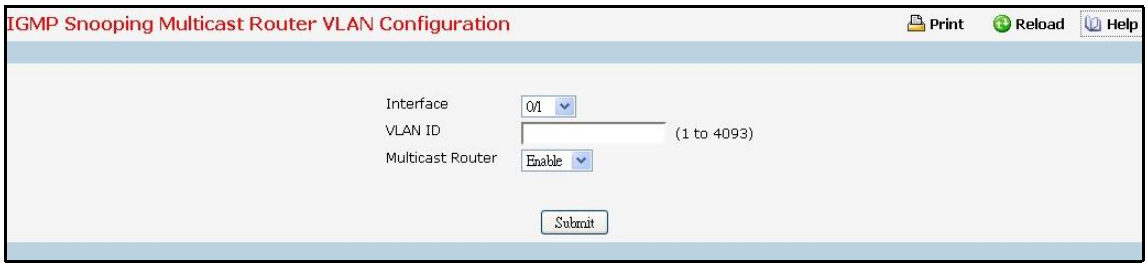
Non-Configurable Data

Multicast Router - Specifies for the selected interface whether multicast router is enable or disabled.

Command Buttons

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

11.3.18.7 Configuring Multicast Router VLAN Page



Selection Criteria

Interface - The select box lists all interfaces. 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.

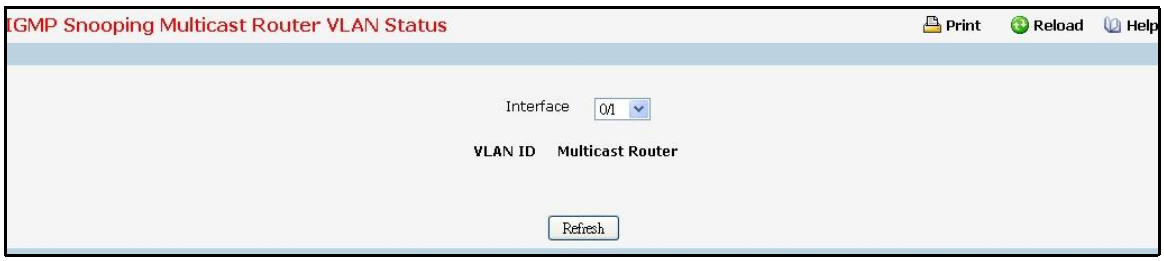
Configurable Data

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.

11.3.18.8 Viewing Multicast Router VLAN Status Page



Selection Criteria

Interface - The select box lists all interfaces. Select the interface for which you want to display the statistics.

Non-Configurable Data

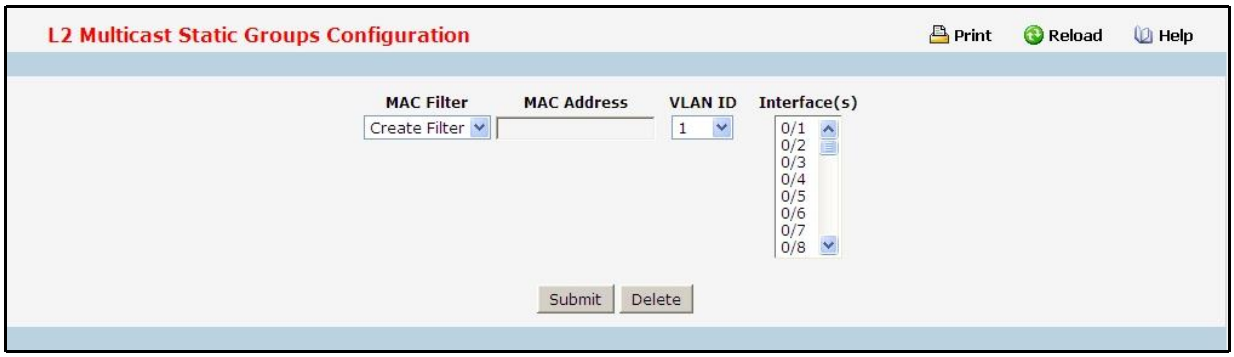
VLAN ID - All VLAN Ids for which the Multicast Router Mode is Enabled

Multicast Router - Multicast Router Mode for VLAN ID.

Command Buttons

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

11.3.18.9 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

Interface(s) - List the interfaces you want included into L2Mcast Group.

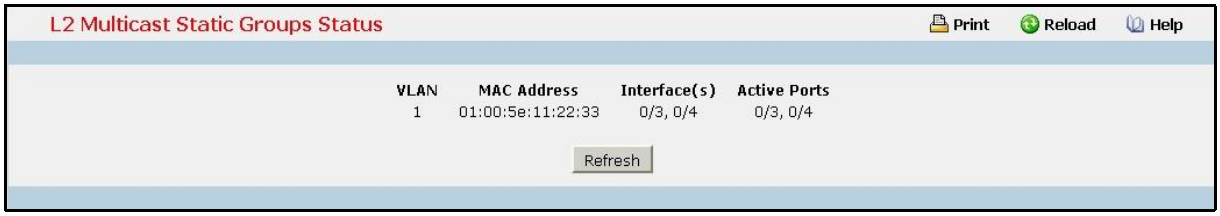
Command Buttons

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.

11.3.18.10 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.

Interface(s) - the interface number belongs to this Multicast Group.

Active Ports - The active interface number belongs to this Multicast Group.

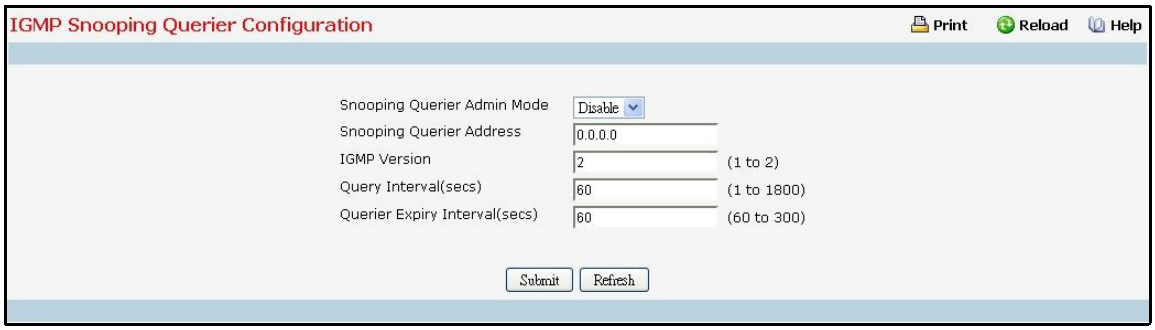
Command Buttons

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

11.3.19 Managing IGMP Snooping Querier

11.3.19.1 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 pull-down 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.

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.

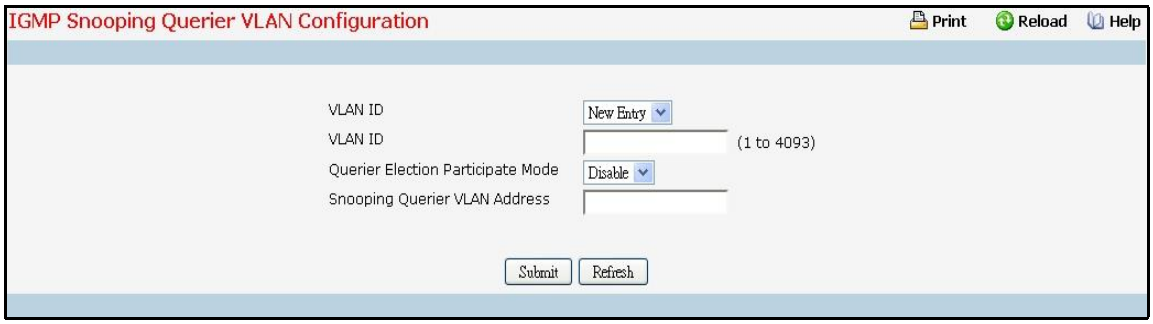
Querier Expiry Interval - Specify the time interval in seconds after which the last querier information is removed. The Querier Expiry Interval must be a value in the range of 60 and 300. The default value is 60.

Command Buttons

Submit - Update the switch with the configured values.

Refresh - Reload the information on the page.

11.3.19.2 Configuring IGMP Snooping Querier VLAN Configuration Page



Selection Criteria

VLAN ID - Selects the VLAN ID on which IGMP Snooping Querier is enabled.

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.

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.

Snooping Querier VLAN Address - Specify the Snooping Querier Address to be used as source address in periodic IGMP queries sent on the specified VLAN.

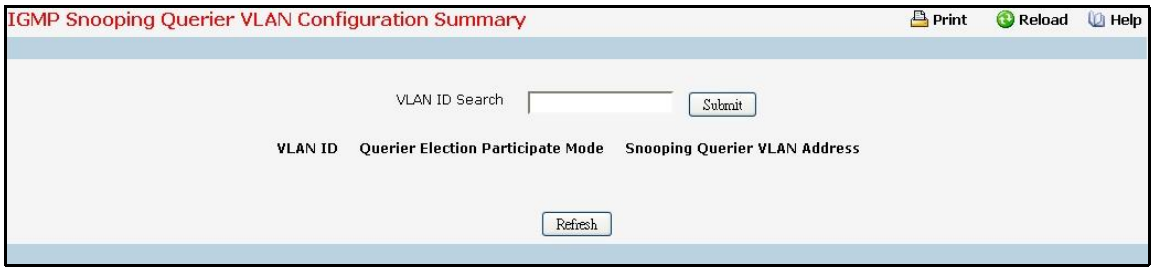
Configurable Button

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.

11.3.19.3 IGMP Snooping Querier VLAN Configuration Summary Page



Non-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.

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.

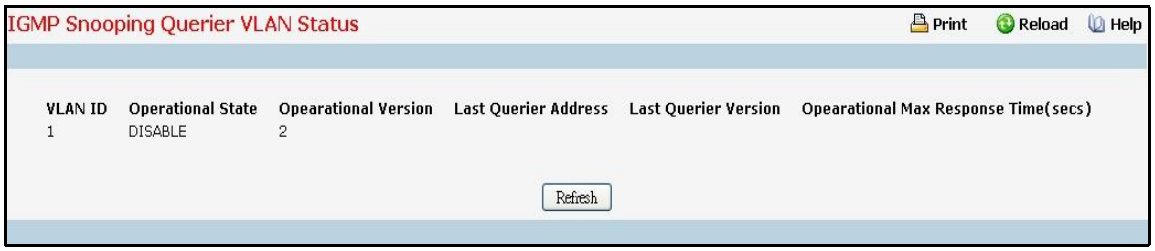
Snooping Querier VLAN Address - Displays the Snooping Querier Address to be used as source address in periodic IGMP queries sent on the specified VLAN.

Command Buttons

Search - Search for the specified VLAN ID.

Refresh - Reload the information on the page.

11.3.19.4 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.

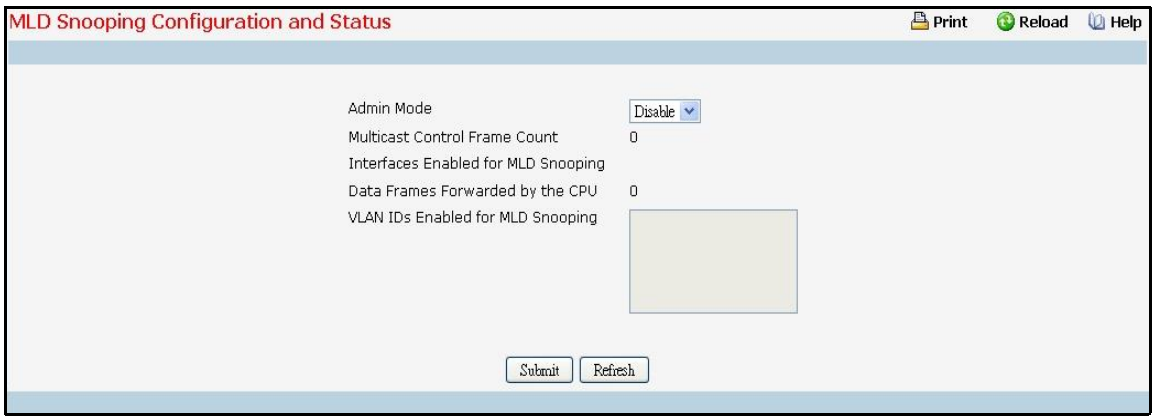
Command Buttons

Refresh - Reload the information on the page.

11.3.20 Managing MLD Snooping

11.3.20.1 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.

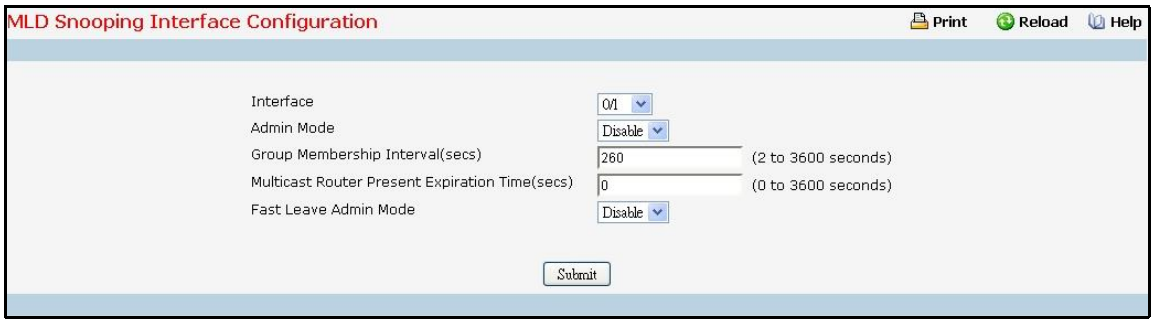
Data Frames Forwarded by the CPU - The number of data frames forwarded by the CPU.

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.

11.3.20.2 Configuring MLD Snooping Interface Configuration Page



Selection Criteria

Interface - 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 pull-down menu. The default is disable.

Fast Leave Admin mode - Select the Fast Leave mode for the a particular interface from the pull-down 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.

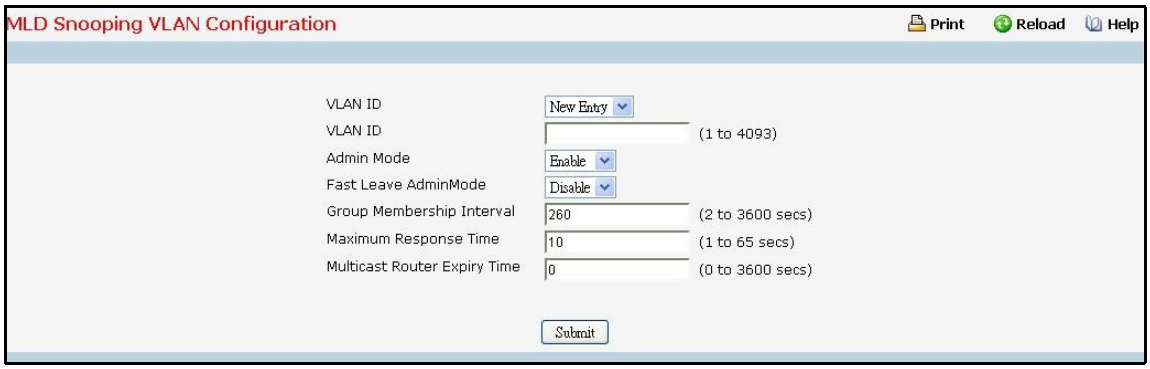
Max Response Time - Specify the amount of time you want the switch to wait after sending a query on an interface because it did not receive a report for a particular group on that interface. Enter a value greater or equal to 1 and less than the Group Membership Interval in seconds. The default is 10 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.

11.3.20.3 Configuring MLD Snooping VLAN Configuration Page



Selection Criteria

VLAN ID - Specifies list of VLAN IDs for which MLD Snooping is enabled.

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 MLD Snooping for the specified VLAN ID.

Fast Leave Admin Mode - Enable or disable the MLD Snooping Fast Leave Mode for the specified VLAN ID.

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.

Command Buttons

Submit - Update the switch with the values you entered.

Delete - Update the switch with the default values.

11.3.20.4 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.

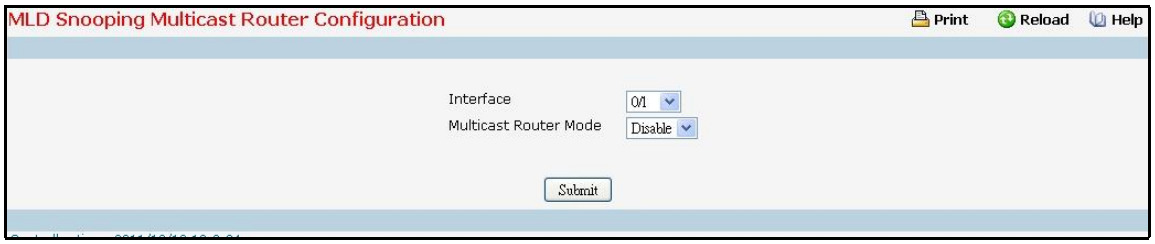
Maximum Response Time - Maximum Response Time of MLD Snooping for the specified VLAN ID. Valid range is 1 to 65. Its value should be greater than group membership interval value.

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

11.3.20.5 Configuring MLD Snooping Multicast Router Configuration Page



Selection Criteria

Interface - The select box lists all Slot/Ports. Select the interface for which you want Multicast Router to be enabled.

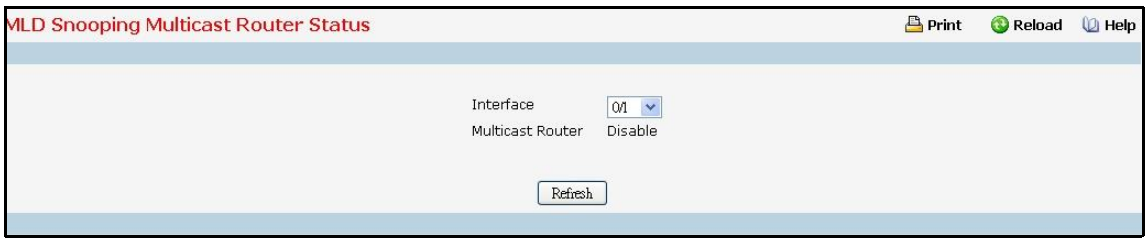
Configurable Data

Multicast Router - Enable or disable Multicast Router on the selected Slot/Port.

Command Buttons

Submit - Update the switch with the values you entered.

11.3.20.6 Configuring MLD Snooping Multicast Router Status Page



Selection Criteria

Interface - The single select box lists all physical and LAG interfaces. Select the interface for which you want to display the status.

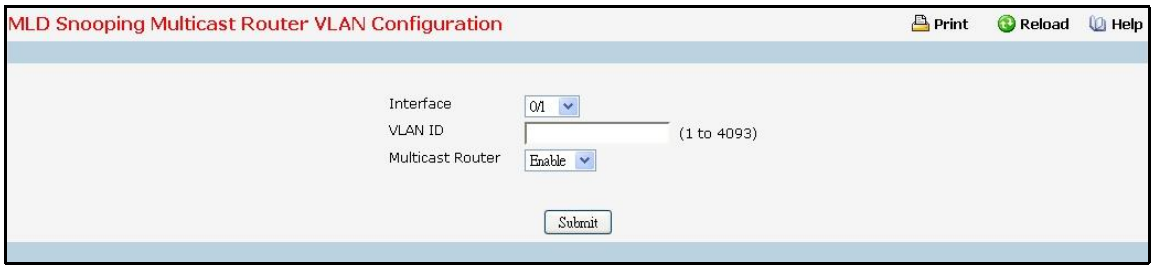
Non-Configurable Data

Multicast Router - Specifies for the selected interface whether multicast router is enable or disabled.

Command Buttons

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

11.3.20.7 Configuring MLD Snooping Multicast VLAN Configuration Page



Selection Criteria

Interface - The select box lists all interfaces. Select the interface for which you want Multicast Router to be enabled

Configurable Data

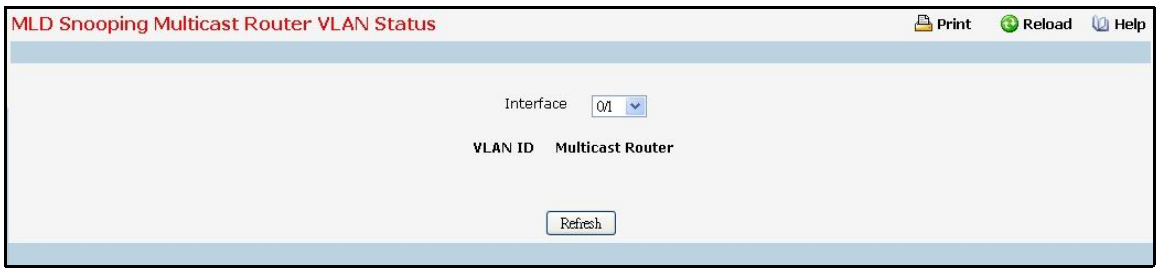
VLAN ID - VLAN ID for which the Multicast Router Mode is to be Enabled or Disabled.

Multicast Router - For the VLAN ID, multicast router may be enabled or disabled using this.

Command Buttons

Submit - Update the switch with the values you entered.

11.3.20.8 Configuring MLD Snooping Multicast Router VLAN Status Page



Selection Criteria

Interface - The select box lists all interfaces. Select the interface for which you want to display the status.

Non-Configurable Data

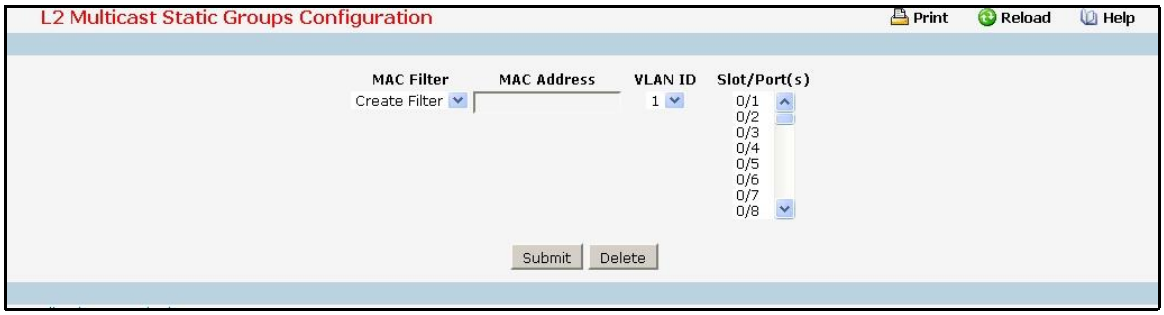
VLAN ID - All VLAN Ids for which the Multicast Router Mode is Enabled.

Multicast Router - Multicast Router Mode for VLAN ID.

Command Buttons

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

11.3.20.9 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.

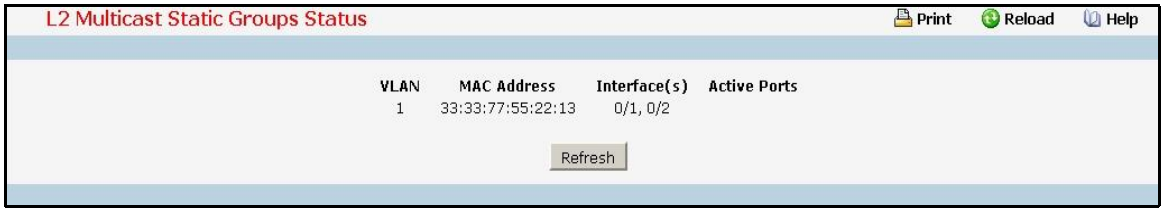
Command Buttons

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.

11.3.20.10 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.

Interface(s) - the interface number belongs to this Multicast Group.

Active Ports - The active interface number belongs to this Multicast Group.

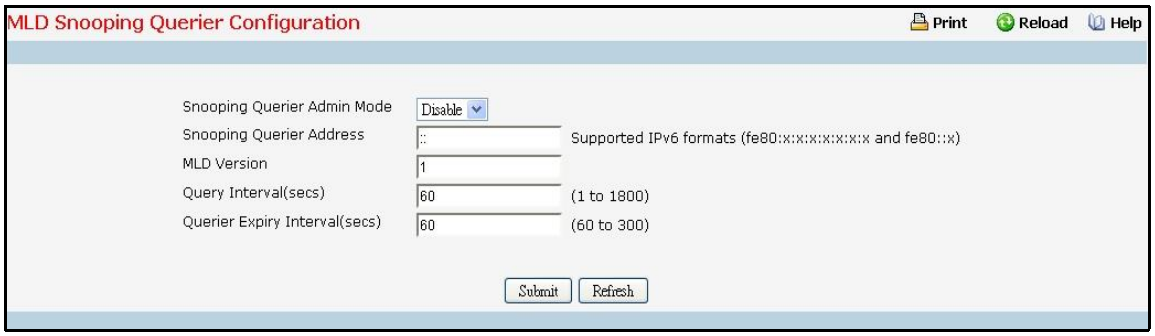
Command Buttons

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

11.3.21 Managing MLD Snooping Querier

11.3.21.1 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.



Configurable Data

Snooping Querier Admin Mode - Select the administrative mode for MLD Snooping for the switch from the pull-down menu. The default is disable.

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.

Query Interval (secs) - 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.

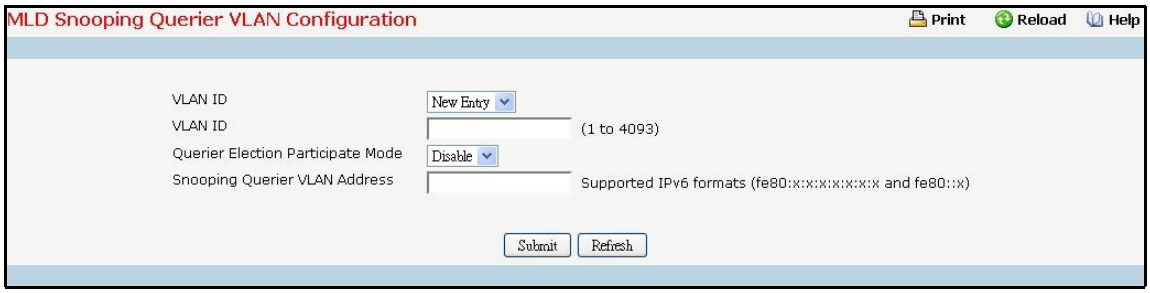
Querier Expiry Interval (secs) - Specify the time interval in seconds after which the last querier information is removed. The Querier Expiry Interval must be a value in the range of 60 and 300. The default value is 60.

Configurable Data

Submit - Update the switch with the configured values.

Refresh - Reload the information on the page.

11.3.21.2 Configuring MLD Snooping Querier VLAN Configuration Page



Selection Criteria

VLAN ID - Selects the VLAN ID on which MLD Snooping Querier is enabled.

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.

Querier Election Participate Mode - Enable or disable the MLD 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.

Snooping Querier VLAN Address - Specify the Snooping Querier Address to be used as source address in periodic MLD queries sent on the specified VLAN.

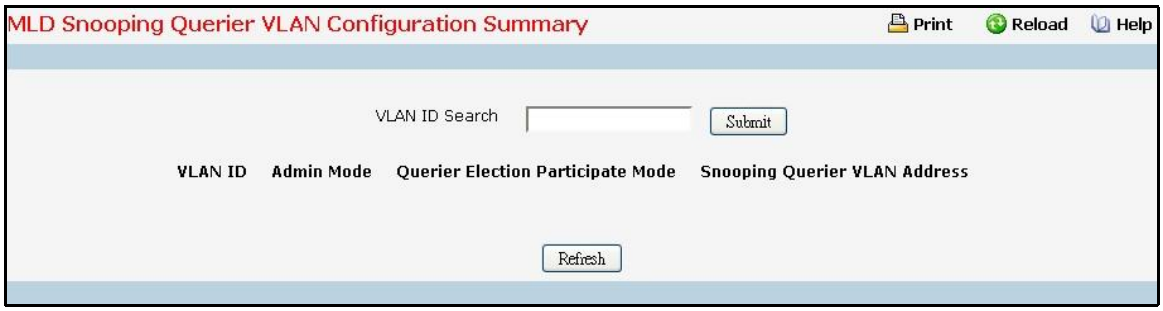
Command Buttons

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.

11.3.21.3 Configuring MLD Snooping VLAN Configuration Summary Page



Configurable Data

VLAN ID Search - Enter VLAN ID, and 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.

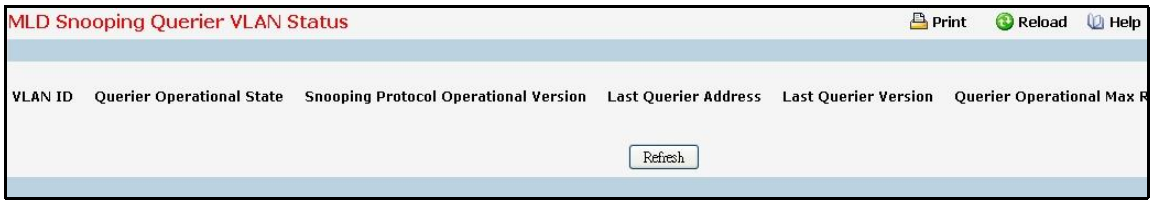
Snooping Querier VLAN Address - Displays the Snooping Querier Address to be used as source address in periodic MLD queries sent on the specified VLAN.

Command Buttons

Search - Search for the specified VLAN ID.

Refresh - Reload the information on the page.

11.3.21.4 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.

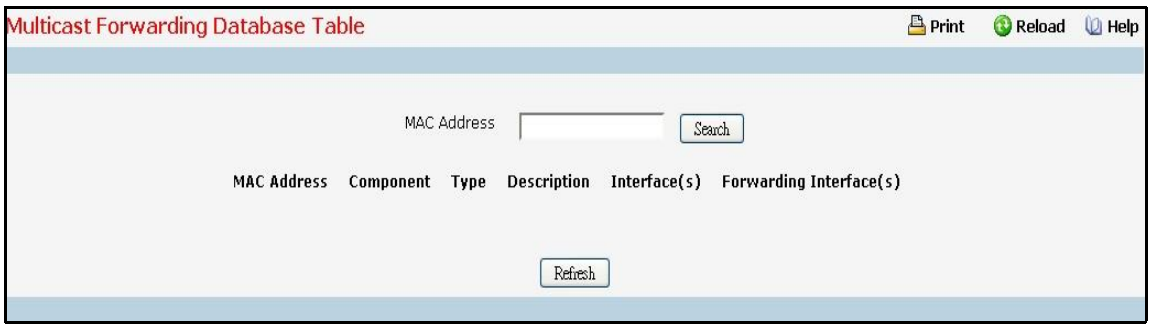
Last Querier Version - Displays the IGMP protocol version of the last querier from which a query was snooped on the VLAN.

Operational Max Response Time - Displays maximum response time to be used in the queries that are sent by the Snooping Querier.

11.3.22 Viewing Multicast Forwarding Database

11.3.22.1 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.

Interface(s) - The list of interfaces that are designated for forwarding (Fwd:) and filtering (Flt:) for the selected address.

Forwarding Interface(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.

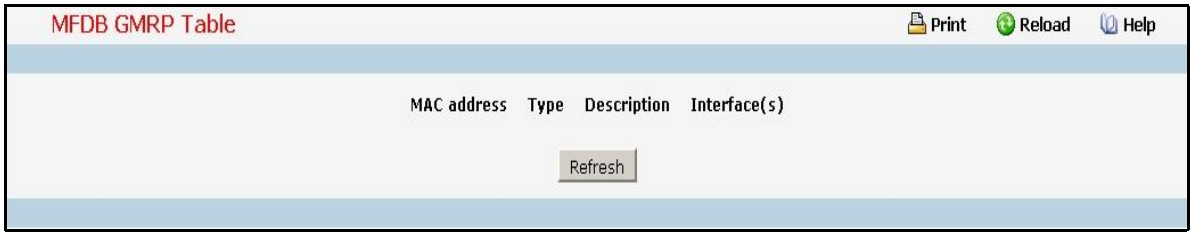
Command Buttons

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.

11.3.22.2 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.

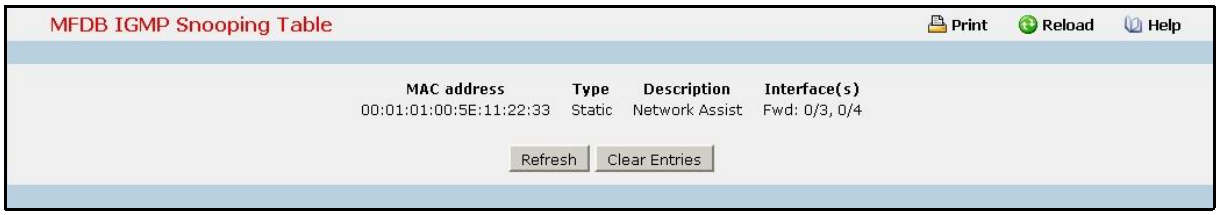
Description - The text description of this multicast table entry. Possible values are Management Configured, Network Configured, and Network Assisted.

Interface(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.

11.3.22.3 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.

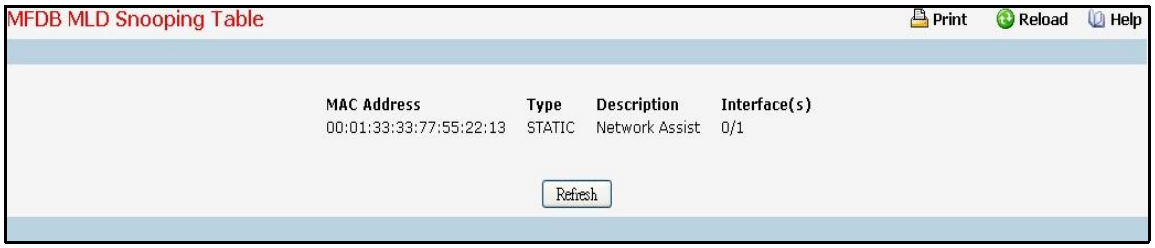
Interface(s) - The list of interfaces that are designated for forwarding (Fwd:) and filtering (Flt:).

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.

11.3.22.4 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.

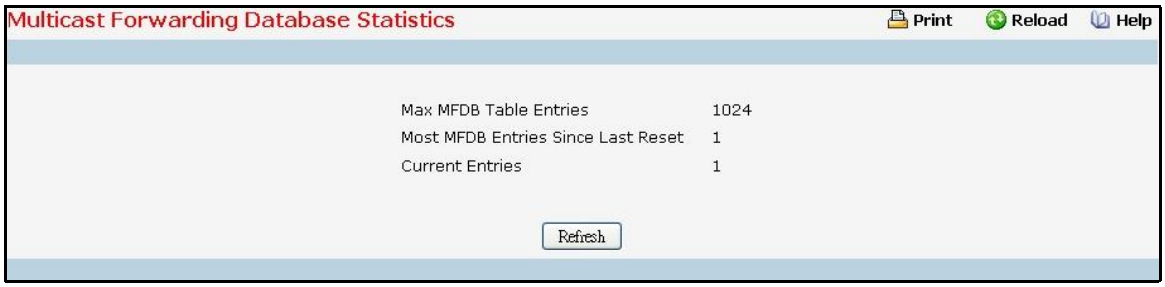
Interface(s) - The list of interfaces that are designated for forwarding (Fwd:) and filtering (Flt:).

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.

11.3.22.5 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.

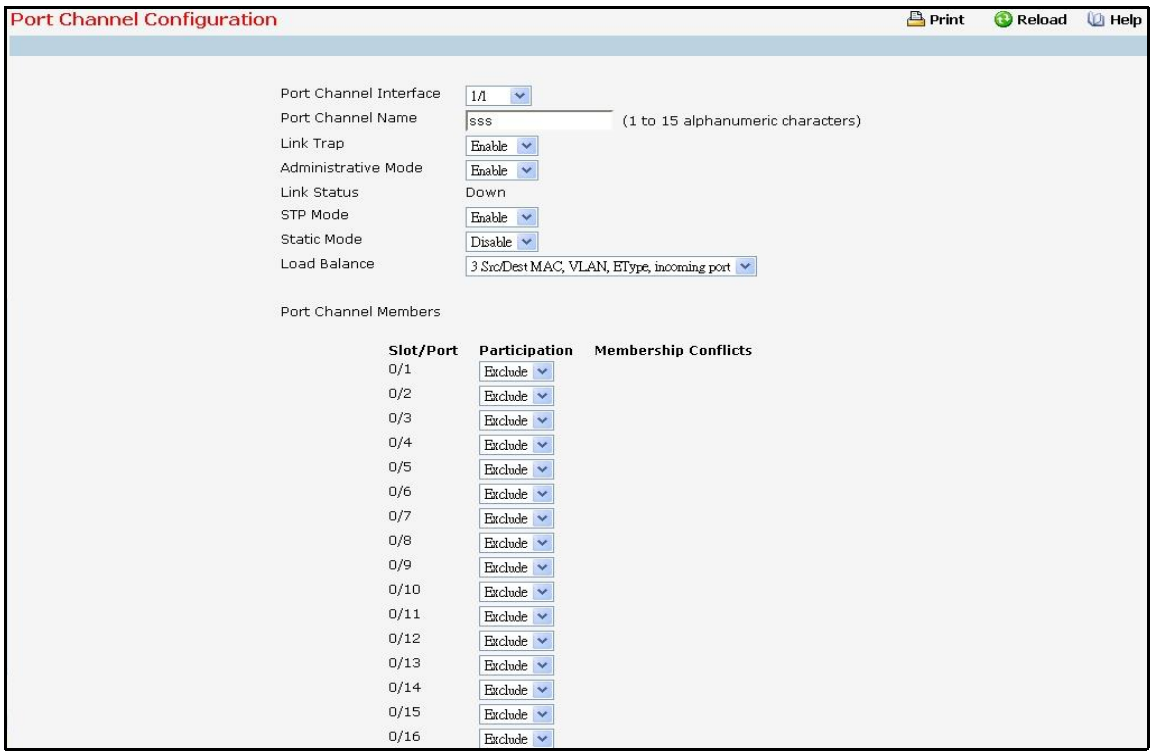
Current Entries - The current number of entries in the Multicast Forwarding Database table.

Command Buttons

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

11.3.23 Managing Port-Channel

11.3.23.1 Configuring Port-Channel Configuration Page



Selection Criteria

Port Channel Interface - 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 64 Port Channels.

Configurable Data

Port Channel Name -Enter the name you want assigned to the Port Channel. You may enter any string of up to 15 alphanumeric characters. A valid name has to be specified in order to create the Port Channel.

Link Trap - Specify whether you want to have a trap sent when link status changes. The factory default is enable, which will cause the trap to be sent.

Administrative Mode - Select enable or disable from the pull down menu. When the Port Channel is disabled no traffic will flow and LACPDUs will be dropped, but the links that form the Port Channel will not be released. The factory default is 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 enable or disable from the pull down menu. When the Port Channel is enabled it does not transmit or process received LAGPDUs i.e. the member ports do not transmit LAGPDUs and all the LAGPDUs it may receive are dropped. The factory default is disable.

Load Balance Mode - Select load balance mode from the pull down menu. The factory default is Source XOR Destination MAC address.

- Source MAC, VLAN, Ethertype, and incoming port
- Destination MAC, VLAN, EtherType and incoming port
- Source/Destination MAC, VLAN, Ethertype, and incoming port. This is the factory default. Source IP and Source TCP/UDP Port Destination IP and Destination TCP/UDP Port
- Source/Destination IP and source/destination TCP/UDP Port

Enhanced hashing mode.

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.

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.

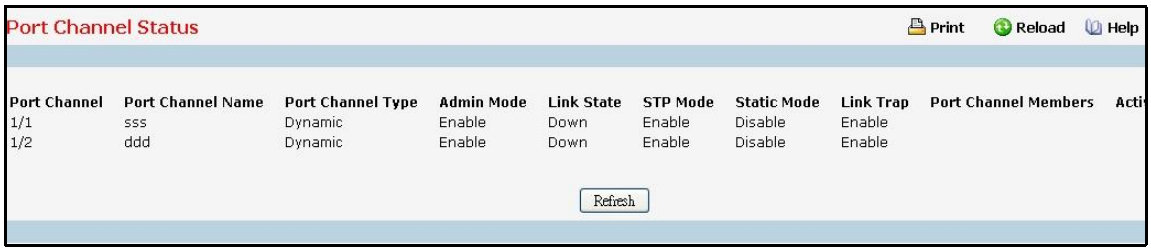
Command Buttons

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.

11.3.23.2 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-balance mode of port channel. The possible values are:

- Source MAC, VLAN, Ethertype, and source port
- Destination MAC, VLAN, EtherType and source port.
- Source/Destination MAC, VLAN, Ethertype, and source port

Source IP and Source TCP/UDP Port.

- Destination IP and Destination TCP/UDP Port
- Source/Destination IP and source/destination TCP/UDP Port

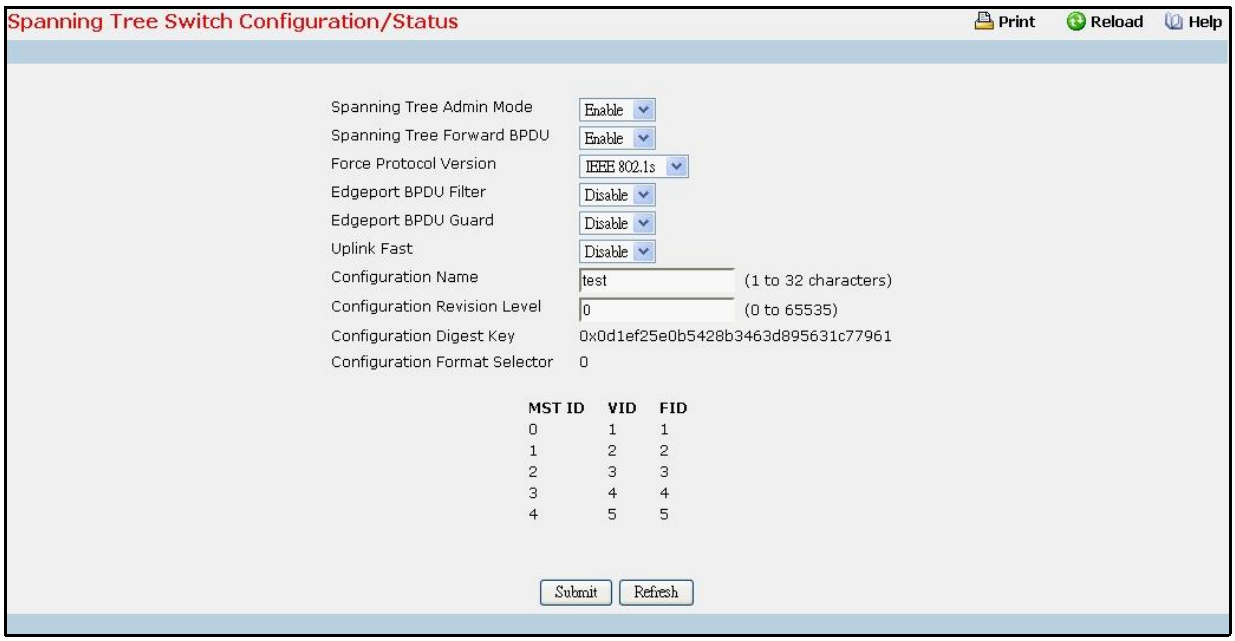
Enhanced hashing mode

Command Buttons

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

11.3.24 Managing Spanning Tree

11.3.24.1 Configuring Switch Spanning Tree Configuration Page



Selection Criteria

Spanning Tree Admin 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.

Edgeport BPDU Filter - Specifies whether Edgeport BPDU Filter is enabled on the switch. Value is enabled or disabled.

Edgeport BPDU Guard - Specifies whether Edgeport BPDU Guard is enabled on the switch. Value is enabled or disabled.

Uplink Fast - Specifies whether Uplink Fast is enabled on the switch. Value is enabled or disabled.

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.

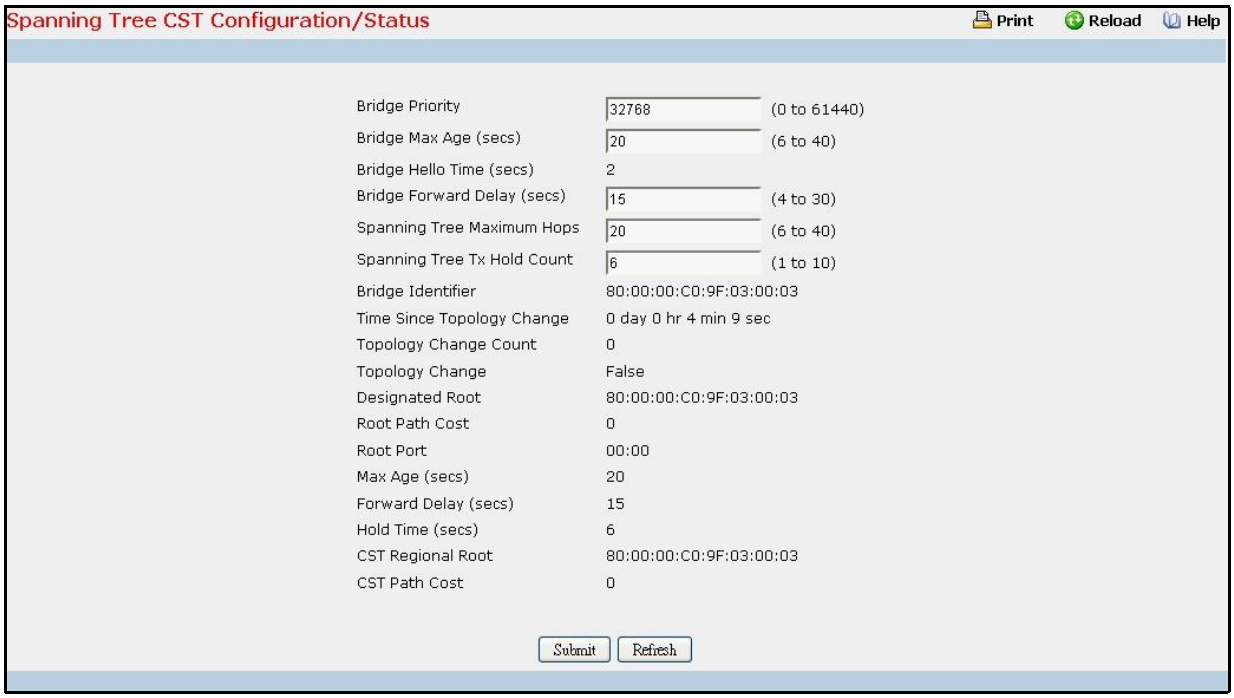
FID Table - Table consisting of the FIDs and the corresponding VLAN IDs associated with each of them.

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.

11.3.24.2 Configuring Spanning Tree CST Configuration Page



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 transmissions of Configuration BPDUs.

CST Regional Root - Priority and base MAC address of the CST Regional Root. CST

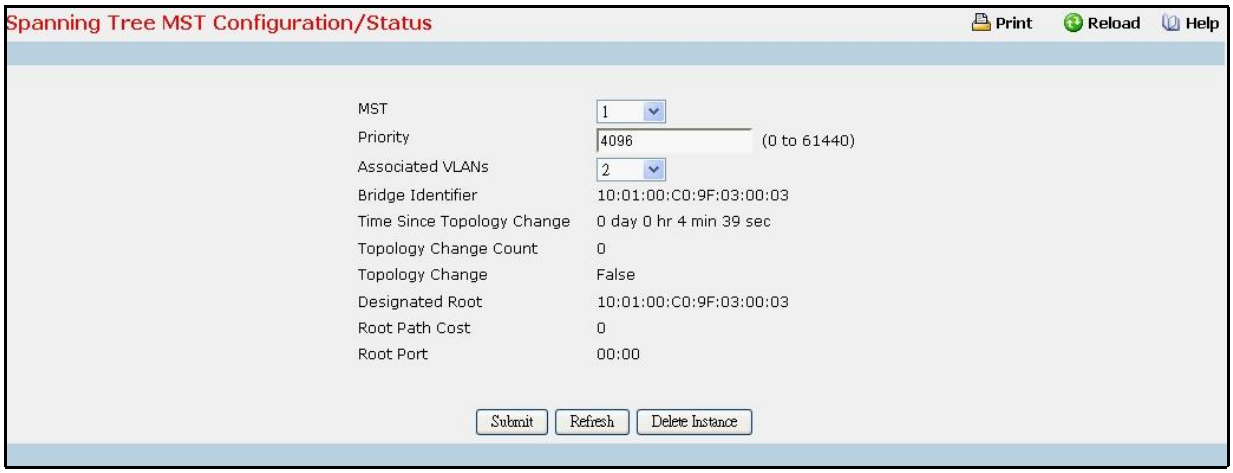
Path Cost - Path Cost to the CST tree Regional Root.

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 - Refresh the screen with most recent data.

11.3.24.3 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.

Associated VLANs - This gives a list of VLANs associated to the MST instance. Non-configured VLANs can be added to or deleted from the MST instance by selecting Add/Delete option and entering the VLAN ID in the VLAN ID-Individual/Range text-box.

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.

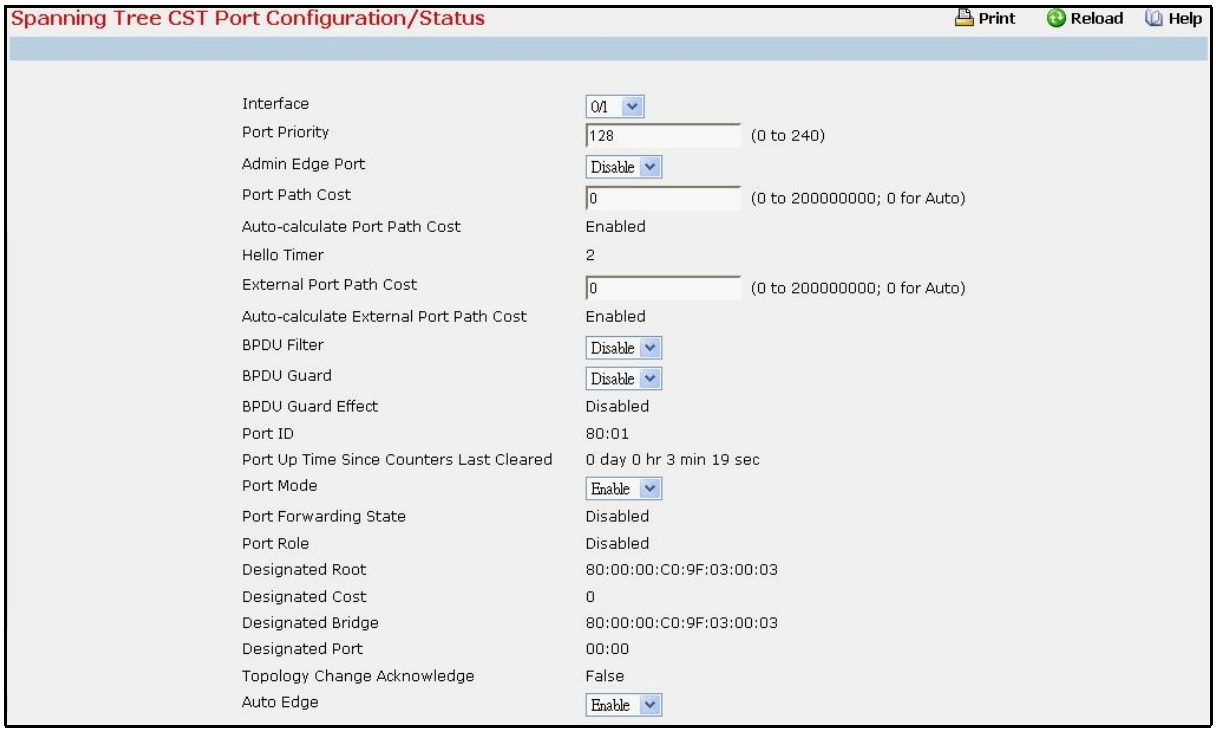
Command Buttons

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 - Refresh the screen with most recent data.

11.3.24.4 Configuring each Port CST Configuration Page



Selection Criteria

Interface - 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.

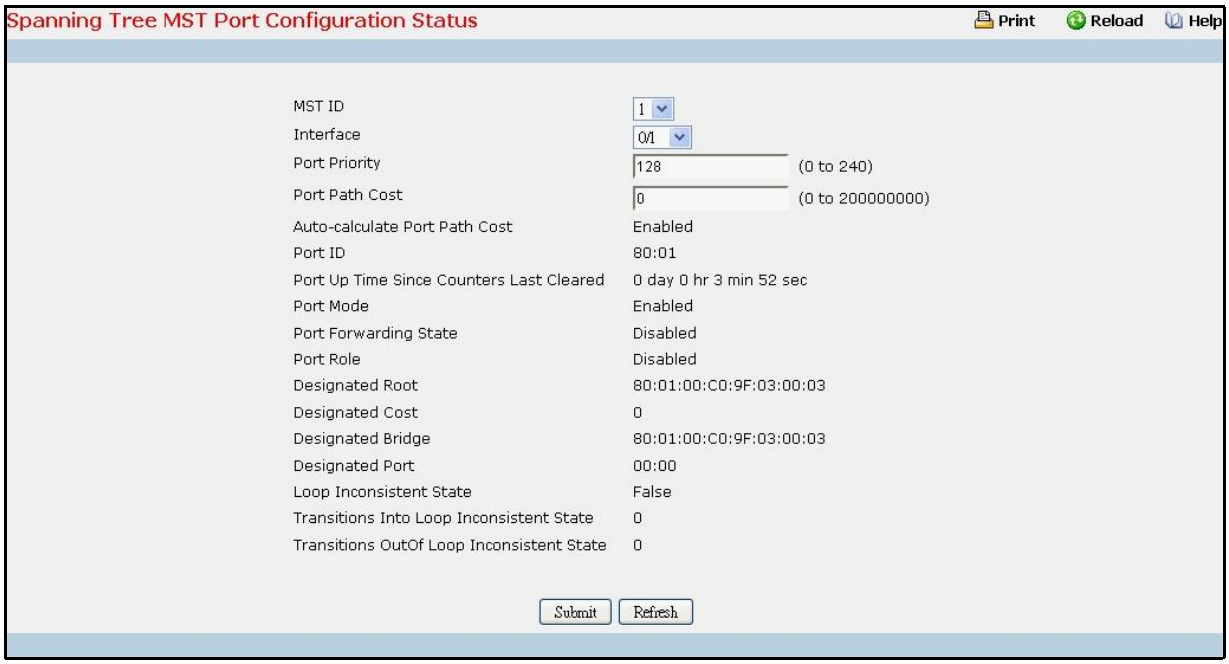
Command Buttons

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 - Refresh the screen with most recent data.

Force - Clicking this button will force the port to send out 802.1w or 802.1s BPDUs.

11.3.24.5 Configuring each Port MST Configuration Page



Selection Criteria

MST ID - Selects one MST instance from existing MST instances.

Interface - 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.

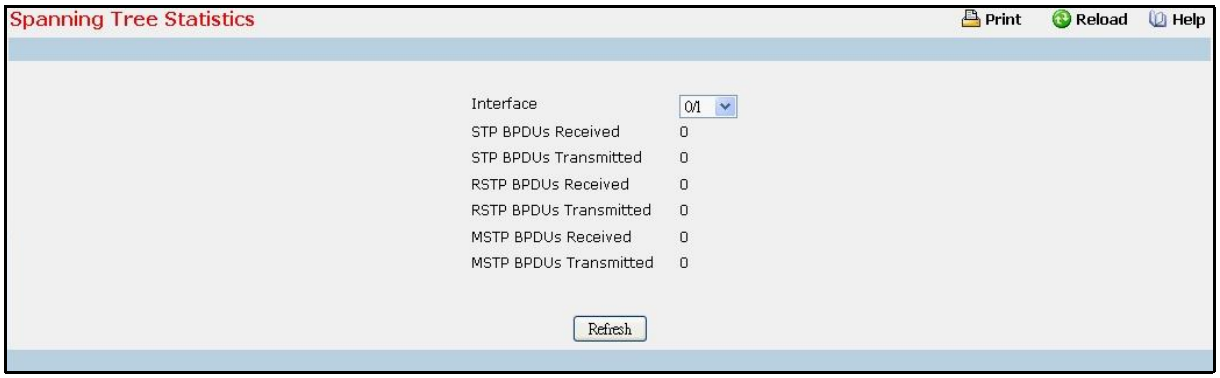
Transitions Out Of Loop Inconsistent State - The number of times this interface has transitioned out of loop inconsistent state.

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 - Refresh the screen with most recent data.

11.3.24.6 Viewing Spanning Tree Statistics Page



Selection Criteria

Interface - 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.

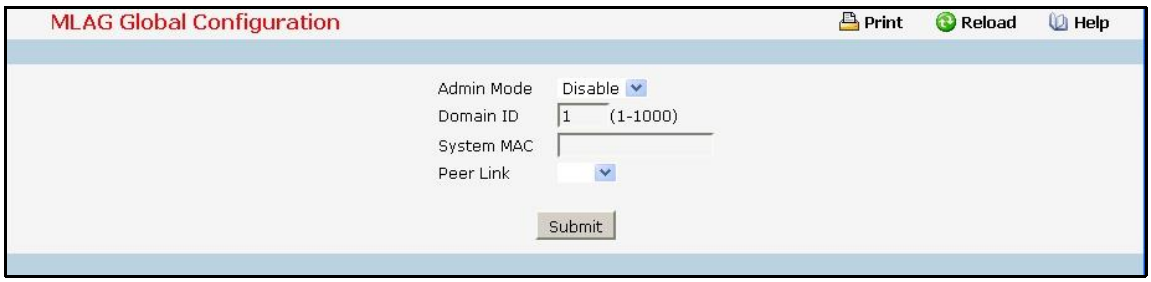
MSTP BPDUs Transmitted - Number of MSTP BPDUs transmitted from the selected port.

Command Buttons

Refresh - Refresh the screen with most recent data.

11.3.25 Managing MLAG

11.3.25.1 Configuring MLAG Global



Selection Criteria

Admin Mode - To enable a Multi-chassis Link Aggregation (MLAG), which allows links that are physically connected to two different devices to appear as a single port channel to a third device..

Peer Link - To create a Multi-chassis Link Aggregation (MLAG) peer link by designating the port channel that you want on each device as the peer link for the specified MLAG domain.

Configurable Data

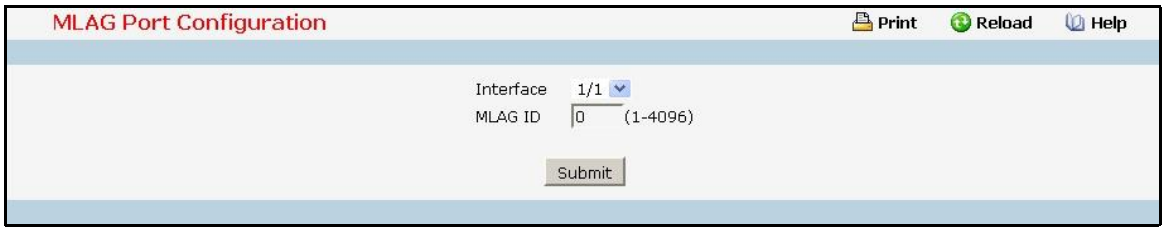
Domain ID - To enable a Multi-chassis Link Aggregation (MLAG), which allows links that are physically connected to two different devices to appear as a single port channel to a third device.

System MAC -To enable a Multi-chassis Link Aggregation (MLAG), which allows links that are physically connected to two different devices to appear as a single port channel to a third device..

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.

11.3.25.2 Configuring MLAG Port



Selection Criteria

Interface - You can use this to set up parameter for a interface.

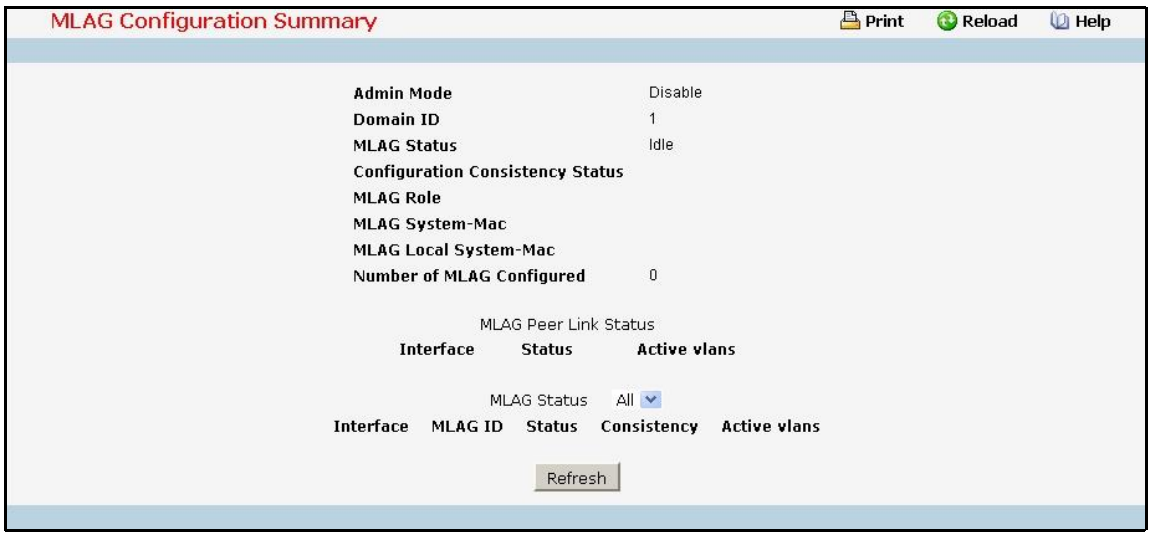
Configurable Data

MLAG ID - To move other port channels into a Multi-chassis Link Aggregation (MLAG) to connect to the downstream device, use the mlag command. The range is from 1 and 4096.

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.

11.3.25.3 Viewing MLAG Configuration Summary



Selection Criteria

MLAG Status - You can use this to see MLAG parameters for an interface(s).

Non-Configurable Data

Admin Mode - Displays the administrative mode for MLAG functionality on the switch.

Domain ID - Represents the domain identify number of MLAG peer devices.

MLAG Status - Represents the operation status of MLAG.

Configuration Consistency Status - Represents the configuration consistency status of MLAG peer devices.

MLAG Role - Represents the role of MLAG peer device

MLAG System-Mac - Represents the operation system MAC address of MLAG peer devices.

MLAG Local System-Mac - Represents the statically defined system MAC address of MLAG peer devices.

Number of MLAG Configured - Represents the number of MLAG port-channel member

---Field of MLAG Peer Link Status---

Interface - MLAG Peer Link interface (Port Channel).

Status - Get Operation Status of peer link port channel

Active vlans - The VLAN which port channel belong to

---Field of MLAG Status---

Interface - MLAG interface (Port Channel).

MLAG ID - Get MLAG ID

Status - Get Operation Status of specific port channel

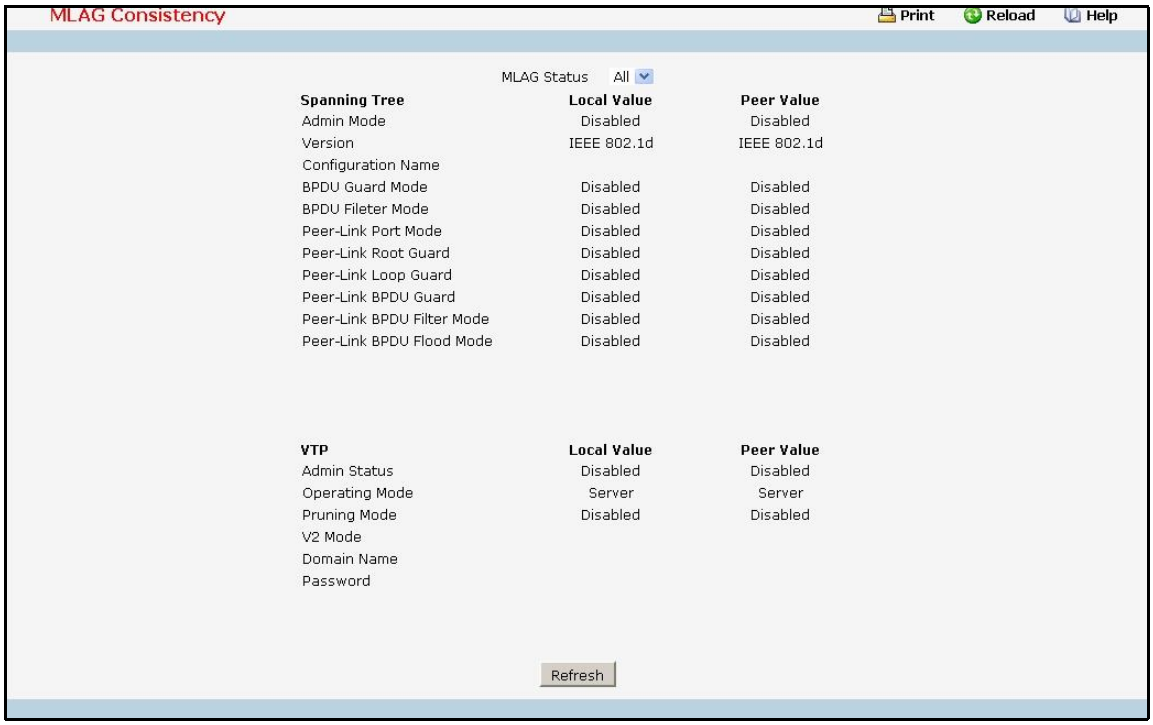
Consistency - Represents the configuration consistency status of MLAG port-channel member.

Active vlans - Represents the VLAN which MLAG peer link port or port-channel member belong to.

Command Buttons

Refresh - Update the data.

11.3.25.4 Viewing MLAG Consistency



Selection Criteria

MLAG Status - You can use this to select a MLAG ID to see its parameter.

Non-Configurable Data

Spanning Tree - Check the switch configuration about Spanning Tree for consistency parameter.. The parameter of global include—

Admin Mode: Indicates whether administrative mode is enabled or disabled of MLAG peer devices.

Version: Represents the version of 802.1 currently supported (IEEE 802.1s, IEEE 802.1w, or IEEE 802.1d) based upon the Force Protocol Version parameter of MLAG peer devices.

Configuration Name: Represents the configured name of MLAG peer devices.

BPDU Guard Mode: Indicates whether BPDU guard mode is enabled or disabled of MLAG peer devices.

BPDU Filter Mode: Indicates whether BPDU filter mode is enabled or disabled of MLAG peer devices.

Peer-Link Port Mode: Indicates whether port mode on peer link port is enabled or disabled of MLAG peer devices.

Peer-Link Root Guard: Indicates whether root guard mode on peer link port is enabled or disabled of MLAG peer devices.

Peer-Link Loop Guard: Indicates whether loop guard mode on peer link port is enabled or disabled of MLAG peer devices.

Peer-Link BPDU Guard: Indicates whether loop guard mode on peer link port is enabled or disabled of MLAG peer devices.

Peer-Link BPDU Filter Mode: Indicates whether BPDU filter mode on peer link port is enabled or disabled of MLAG peer devices.

Peer-Link BPDU Flood Mode: Indicates whether BPDU flood mode on peer link port is enabled or disabled of MLAG peer devices.

The parameter of single MLAG ID include—

Port Mode: Indicates whether port mode on MLAG member is enabled or disabled of MLAG peer devices.

Root Guard: Indicates whether root guard mode on MLAG member is enabled or disabled of MLAG peer devices.

Loop Guard: Indicates whether loop guard mode on MLAG member is enabled or disabled of MLAG peer devices.

BPDU Guard: Indicates whether BPDU guard mode on MLAG member is enabled or disabled of MLAG peer devices.

BPDU Filter Mode: Indicates whether BPDU filter mode on MLAG member is enabled or disabled of MLAG peer devices.

BPDU Flood Mode: Indicates whether BPDU flood mode on MLAG member is enabled or disabled of MLAG peer devices.

VTP - Check the switch configuration about VTP for consistency parameter.

The parameter of global include—

Admin Status: Indicates whether administrative mode is enabled or disabled of MLAG peer devices.

Operating Mode: Displays the VTP operating mode of MLAG peer devices, which can be server, client, or transparent.

Pruning Mode: Displays whether pruning is enabled or disabled of MLAG peer devices. V2

Mode: Displays if VTP version 2 mode is enabled of MLAG peer devices.

Domain Name: Displays the name that identifies the administrative domain of MLAG peer devices.

Password: Displays the VTP domain password of MLAG peer devices.

The parameter of single MLAG ID include—

Port Trunk Mode: Indicates whether trunk mode is enabled or disabled on MLAG member of MLAG peer devices.

Local Value - -Get the parameter value in local side.

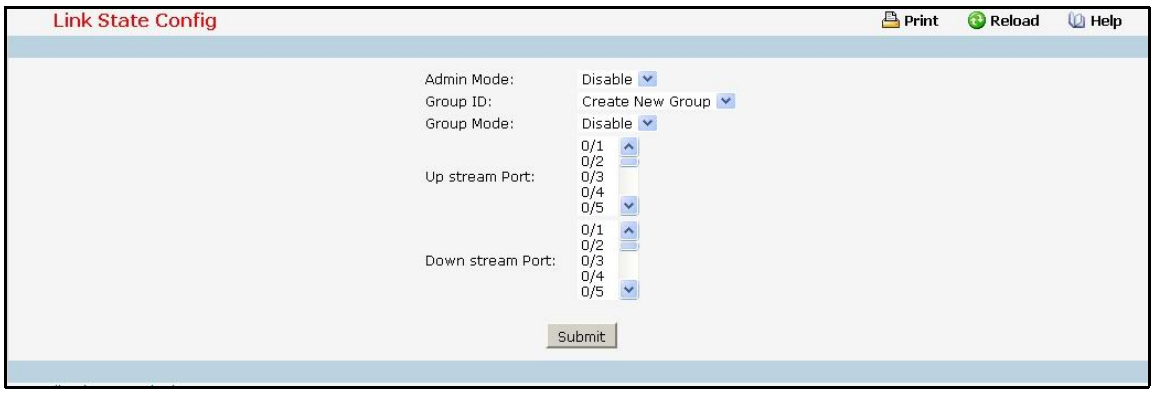
Peer Value - Get the parameter value in peer side.

Command Buttons

Refresh - Update the data.

11.3.26 Managing Link State

11.3.26.1 Configuring Link State Configuration Page



Selection Criteria

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.

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.

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.

Configurable Data

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 Mode - Choose the group administrative mode for the switch by selecting enable or disable from the pull-down menu. The factory default is disabled.

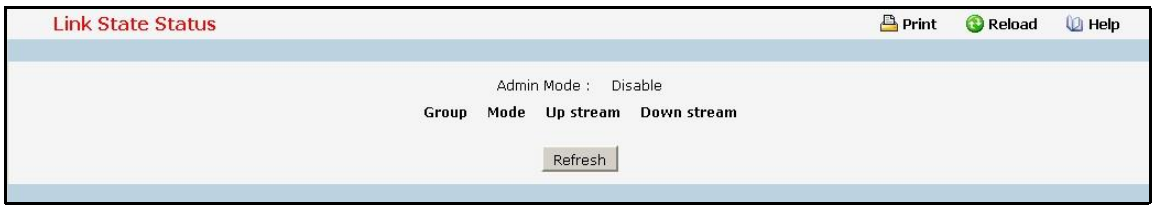
Command Buttons

Submit - Update the switch with the values 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 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.

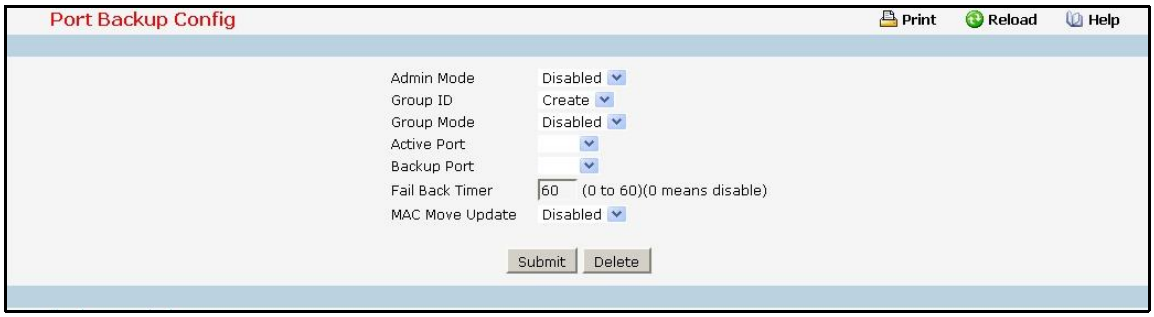
Command Buttons

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

11.3.27 Managing Port-Backup

11.3.27.1 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

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.

Configurable Data

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 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 pairs for six 1Gbps are configurable for active port.

Backup port - Choose the backup port for a group. 6 port pairs for six 1Gbps are configurable for backup port.

Fail Back Timer - Configure the time delay for activating the active port.

MAC Move Update - Choose the MAC Move Update mode for the switch by selecting enable or disable from the pull-down menu.

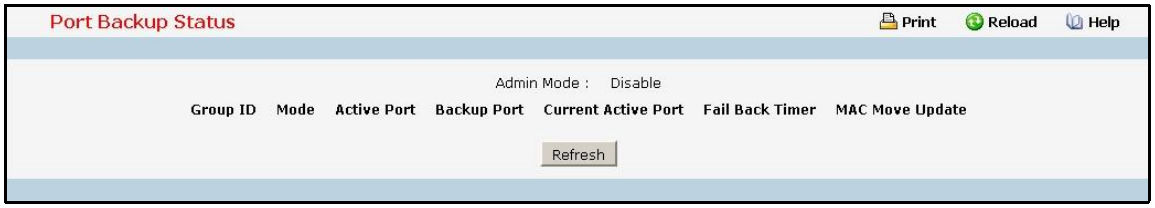
Command Buttons

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.

11.3.27.2 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.

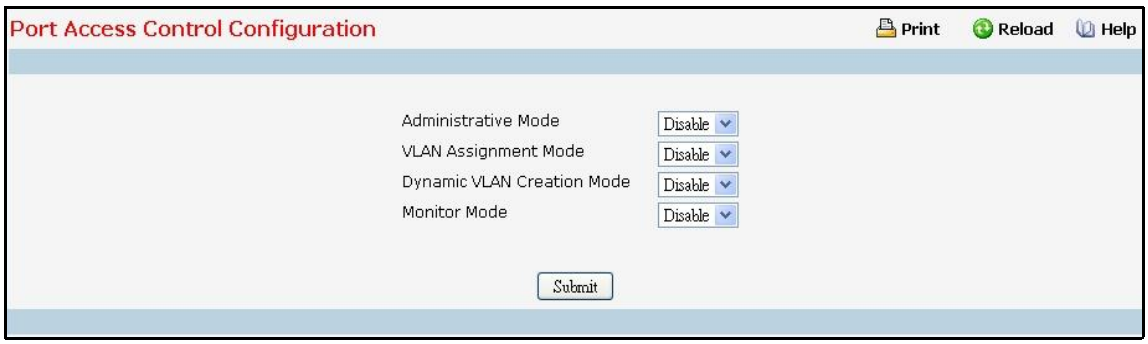
Command Buttons

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

11.4 Security Menu

11.4.1 Managing Access Control (802.1x)

11.4.1.1 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.

VLAN Assignment Mode - This selector lists the two options for VLAN Assignment mode: Enable and Disable. The default value is Disable.

Dynamic VLAN Creation Mode - This selector lists the two options for Dynamic VLAN Creation Mode: Enable and Disable. The default value is Disable.

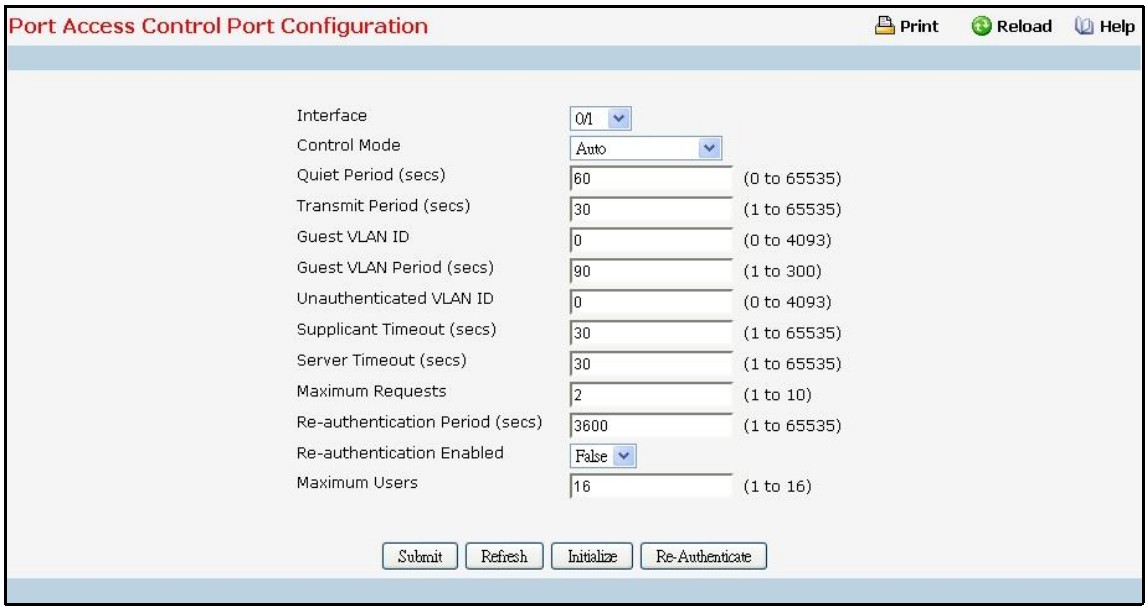
Monitor Mode - This selector lists the two options for Monitor Mode: Enable and Disable. The default value is Disable. The feature monitors the dot1x authentication process and helps in diagnosis the authentication failure cases.

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.

11.4.1.2 Configuring each Port Access Control Configuration Page



Selection Criteria

Interface - 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.

Unauthenticated VLAN ID - This input field allows the user to enter the Unauthenticated VLAN ID for the selected port. The valid range is (0 to 4093).The default value is 0. Changing the value will not change the configuration until the Submit button is pressed. Enter 0 to clear the Unauthenticated VLAN ID on the interface.

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

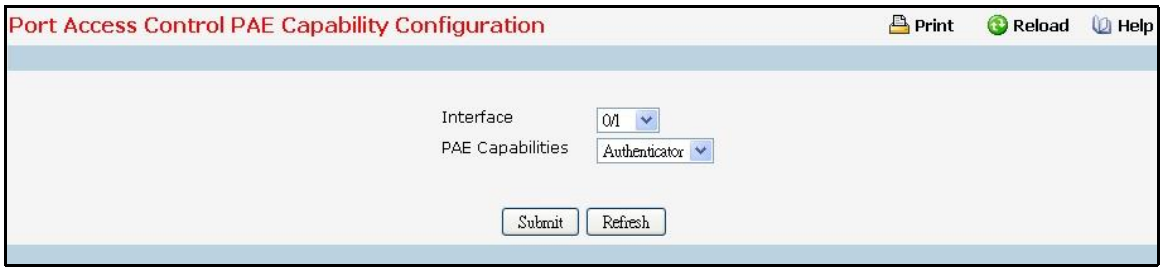
Initialize - This button begins the initialization sequence on the selected port. This button is only selectable if the control mode is 'auto'. If the button is not selectable, it will be grayed out. Once this button is pressed, the action is immediate. It is not required to press the Submit button for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

11.4.1.3 Configuring Port Access Control PAE Capability



Selection Criteria

Interface - 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.

Configurable Data

PAE Capabilities - This selector lists the options for Port Access Entity (PAE) configuration. The options are:

authenticator: Port Access Entity (PAE) is set to Authenticator.

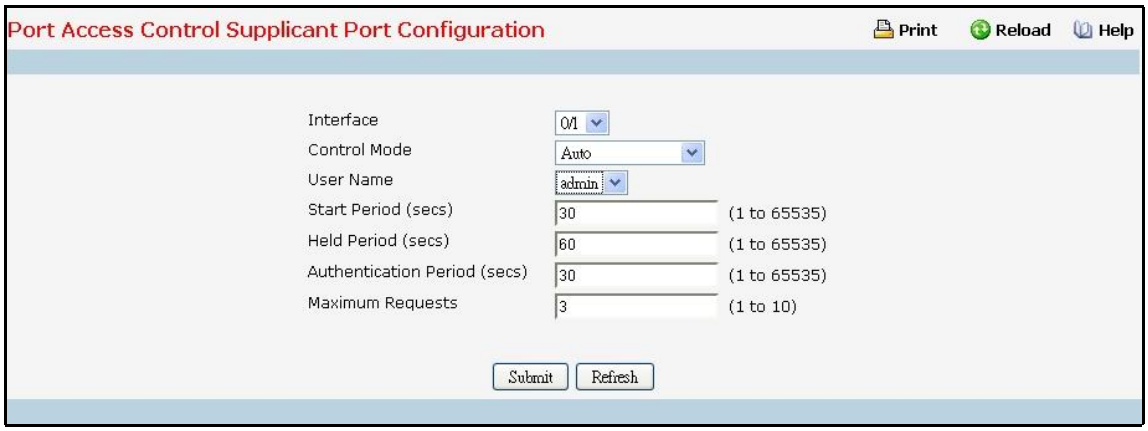
supplicant: Port Access Entity (PAE) is set to Supplicant.

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.

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

11.4.1.4 Configuring Port Access Control Supplicant Port



Selection Criteria

Interface - 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.

User Name - Select the users that will have access to the specified port. The possible values are admin and guest.

Configurable Data

Start Period (secs) - This input field allows the user to configure the start period for the selected port. This command sets the value, in seconds, of the timer used by the Supplicant state machine on this port to define periods of time after which it will send start message again on Authenticator absence. The start period must be a number in the range of 1 and 65535. The default value is 30 seconds. Changing the value will not change the configuration until the Submit button is pressed.

Held Period (secs) - This input field allows the user to configure the Held period for the selected port. The held period is the value, in seconds, of the timer used by the supplicant state machine on the specified port to determine when to send the next EAPOL start frame to the Authenticator on previous authentication failure. The Held period must be a number in the range of 1 and 65535. The default value is 60 seconds. Changing the value will not change the configuration until the Submit button is pressed.

Authentication Period (secs) - This input field allows the user to configure the Authentication period for the selected port. The Authentication period is the value, in seconds, of the timer used by the supplicant backend state machine on the specified port to determine the timeout value for the EAPOL messages that are sent out to the Authenticator. The Authentication period must be a number in the range of 1 and 65535. The default value is 30 seconds. Changing the value will not change the configuration until the Submit button is pressed.

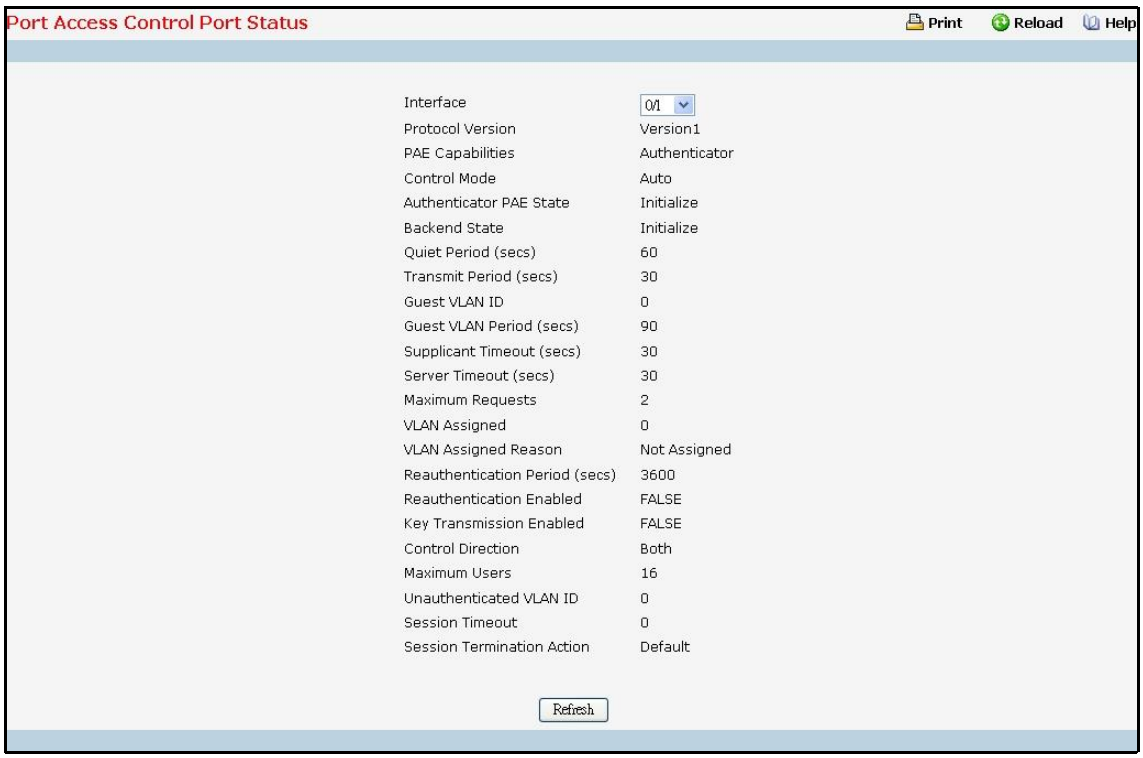
Maximum Requests - This input field allows the user to configure the Maximum start messages that can be sent on the selected port. The maximum start request value is the maximum number of start messages to be sent continuously to detect the presence/absence of the Authenticator. The maximum start requests value must be in the range of 1 and 10. 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.

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

11.4.1.5 Viewing each Port Access Control Configuration Information Page



Selection Criteria

Interface - 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

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.

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.

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".

Supplicant PAE State - This field displays the current state of the Supplicant PAE state machine. This field is present only for Supplicant.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"

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 4093.

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.

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

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.

Key Transmission Enabled- This field displays if key transmission is enabled on the selected port. This is not a configurable field. The possible values are 'true' and 'false'. If the value is 'false' key transmission will not occur. Otherwise Key transmission is supported on the selected port.

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.

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 4093.

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.

Logical Port - This field displays the logical port number associated with the supplicant that is connected to the port. This field is not configurable. This field is displayed when the port control mode of the selected port is mac-based.

Supplicant MAC Address - This field displays the supplicant's MAC address that is connected to the port. This field is not configurable. This field is displayed when the port control mode of the selected port is mac-based.

Authenticator PAE State- This field displays the current state of the authenticator PAE state machine. This field is present only when the port control mode for the selected interface is mac-based.Possible values are:

- "Initialize"
- "Disconnected"
- "Connecting"
- "Authenticating"
- "Authenticated"
- "Aborting"
- "Held"
- "ForceAuthorized"

Backend Authentication State - This field displays the current state of the backend authentication state machine.This field is present only when the port control mode for the selected interface is mac-based. Possible values are:

- "Request"
- "Response"
- "Success"
- "Fail"
- "Timeout"
- "Initialize"
- "Idle"

VLAN Assigned - This field displays the VLAN ID assigned to the supplicant by the Authenticator. This field is not configurable. This field is displayed when the port control mode of the selected port is mac-based.

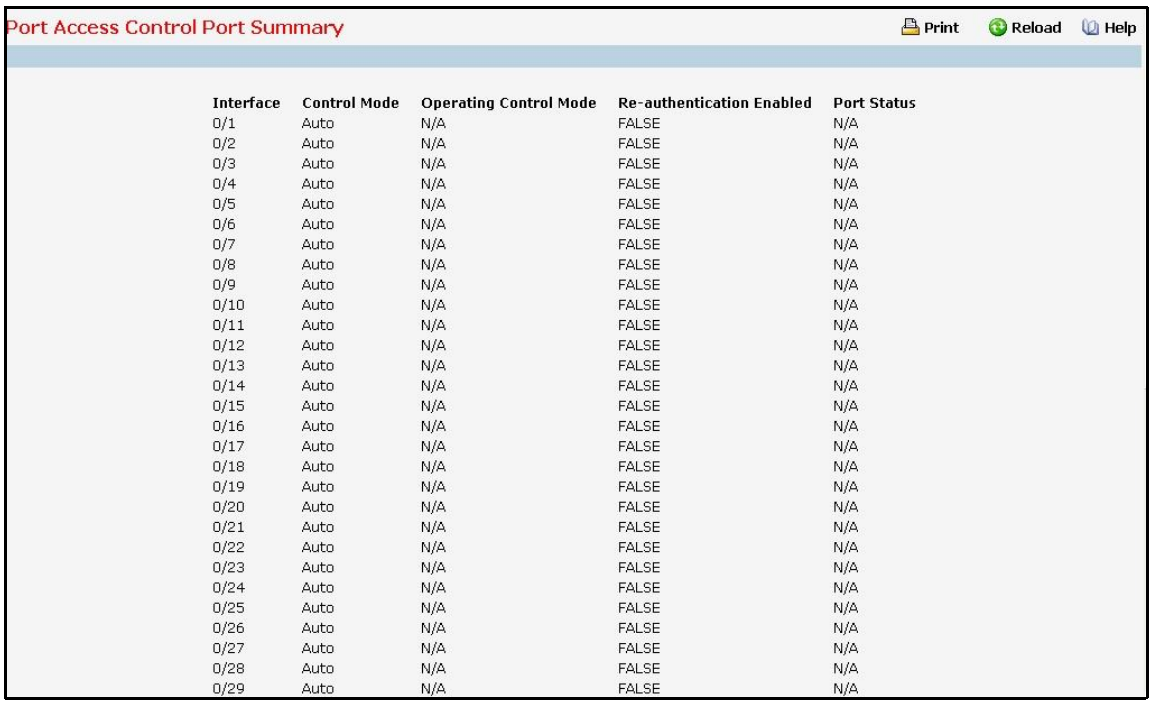
VLAN Assigned Reason - This field displays reason for the VLAN ID assigned by the authenticator.This field is not configurable. This field is displayed when the port control mode of the selected port is mac-based.

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.

11.4.1.6 Viewing Access Control Summary Page



Interface	Control Mode	Operating Control Mode	Re-authentication Enabled	Port Status
0/1	Auto	N/A	FALSE	N/A
0/2	Auto	N/A	FALSE	N/A
0/3	Auto	N/A	FALSE	N/A
0/4	Auto	N/A	FALSE	N/A
0/5	Auto	N/A	FALSE	N/A
0/6	Auto	N/A	FALSE	N/A
0/7	Auto	N/A	FALSE	N/A
0/8	Auto	N/A	FALSE	N/A
0/9	Auto	N/A	FALSE	N/A
0/10	Auto	N/A	FALSE	N/A
0/11	Auto	N/A	FALSE	N/A
0/12	Auto	N/A	FALSE	N/A
0/13	Auto	N/A	FALSE	N/A
0/14	Auto	N/A	FALSE	N/A
0/15	Auto	N/A	FALSE	N/A
0/16	Auto	N/A	FALSE	N/A
0/17	Auto	N/A	FALSE	N/A
0/18	Auto	N/A	FALSE	N/A
0/19	Auto	N/A	FALSE	N/A
0/20	Auto	N/A	FALSE	N/A
0/21	Auto	N/A	FALSE	N/A
0/22	Auto	N/A	FALSE	N/A
0/23	Auto	N/A	FALSE	N/A
0/24	Auto	N/A	FALSE	N/A
0/25	Auto	N/A	FALSE	N/A
0/26	Auto	N/A	FALSE	N/A
0/27	Auto	N/A	FALSE	N/A
0/28	Auto	N/A	FALSE	N/A
0/29	Auto	N/A	FALSE	N/A

Non-Configurable Data

Interface - 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
- N/A: If the port is in detached state it cannot participate in port access control.

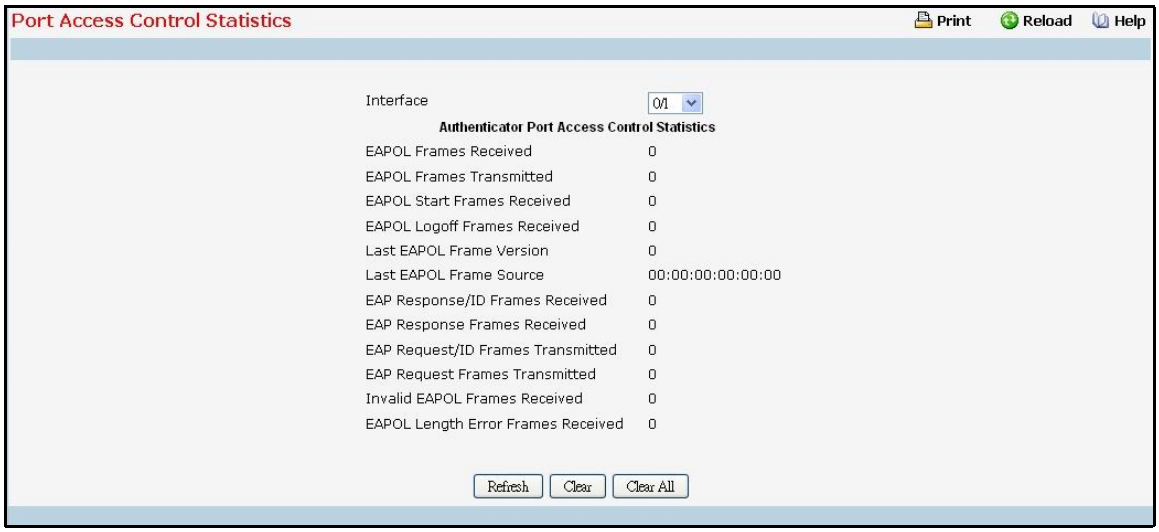
Reauthentication Enabled - This field shows whether reauthentication of the supplicant for the specified port is allowed. The possible values are 'true' and 'false'. If the value is 'true' reauthentication will occur. Otherwise, reauthentication will not be allowed.

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.

11.4.1.7 Viewing each Port Access Control Statistics Page



Selection Criteria

Interface - 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

Authentication Port Access Control Statistcs: If the Port is an Authenticator.

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.

Supplicant Port Access Control Statistcs: If the Port is a Supplicant.

EAPOL Frames Received - This displays the number of valid EAPOL frames of any type that have been received by this supplicant.

EAPOL Frames Transmitted - This displays the number of EAPOL frames of any type that have been transmitted by this supplicant.

EAPOL Start Frames Received - This displays the number of EAPOL start frames that have been received by this supplicant.

EAPOL Logoff Frames Received - This displays the number of EAPOL logoff frames that have been received by this supplicant.

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 supplicant.

EAP Response Frames Received - This displays the number of valid EAP response frames (other than response/identity frames) that have been received by this supplicant.

EAP Request/Id Frames Transmitted - This displays the number of EAP request/identity frames that have been transmitted by this supplicant.

EAP Request Frames Transmitted - This displays the number of EAP request frames (other than request/identity frames) that have been transmitted by this supplicant.

Invalid EAPOL Frames Received - This displays the number of EAPOL frames that have been received by this supplicant in which the frame type is not recognized.

EAPOL Length Error Frames Received - This displays the number of EAPOL frames that have been received by this supplicant 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.

11.4.1.8 Defining Port Access Client Summary Page

Non-Configurable Data

Interface Displays - the interface address of the supplicant device.

Logical Interface - The dot1x Logical Port.

User Name - Displays the user name representing the supplicant device.

Supp Mac Address - Displays the supplicant device's MAC address.

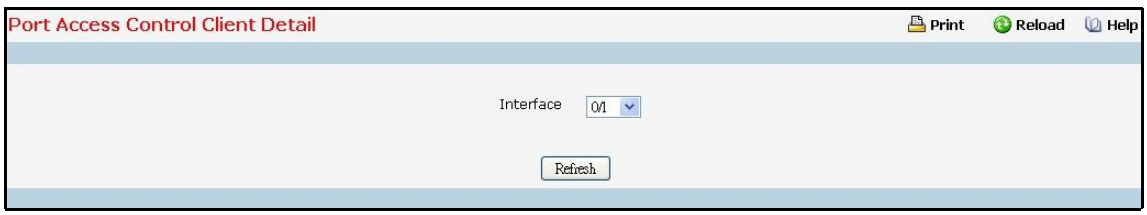
Session Time - Displays the time since the supplicant logged in. The value is in seconds.

Filter ID - The policy filter ID assigned by the authenticator to the supplicant device.

Command Buttons

Refresh - Update the information on the page.

11.4.1.9 Defining Port Access Client Summary Page



Selection Criteria

Interface - 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

Logical Interface - The dot1x Logical Port.

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.

Dot1x Logical Port VLAN Assigned Displays the reason for the VLAN ID assigned by the authenticator to the supplicant device.

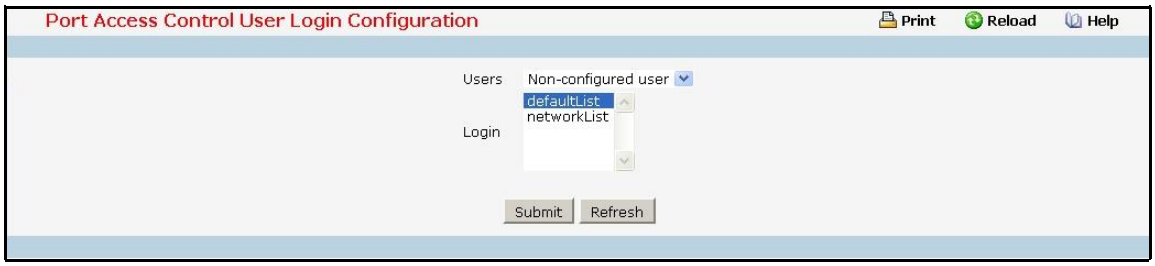
Session Timeout Displays the session timeout set by the radius server to the supplicant device.

Termination Action Displays the termination action set by the radius server to the supplicant device.

Command Buttons

Refresh - Update the information on the page.

11.4.1.10 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

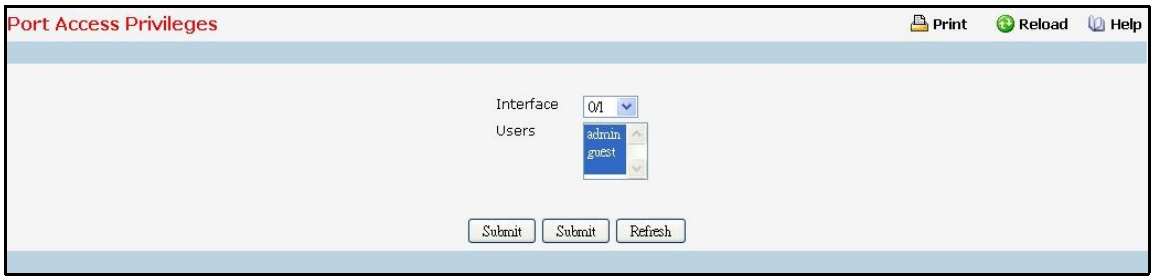
Login - Selects the login to apply to the specified user. All configured logins are displayed.

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.

11.4.1.11 Defining each Port Access Privileges Page



Selection Criteria

Interface - Selects the port to configure.

Configurable Data

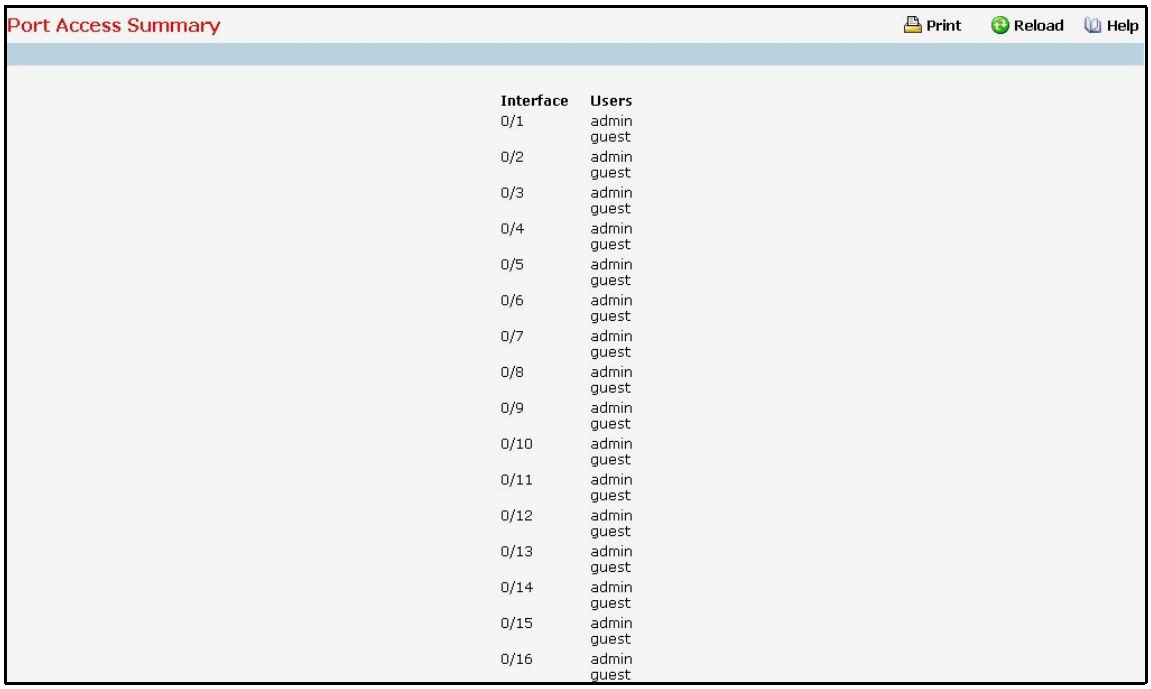
Users - Selects the users that have access to the specified port or ports.

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.

11.4.1.12 Viewing each Port Access Privileges Summary Page



Non-Configurable Data

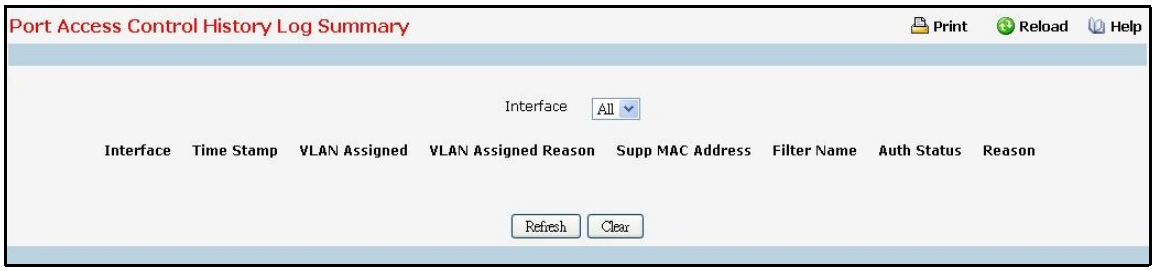
Interface - Displays the port in Slot/Port format.

Users - Displays the users that have access to the port.

Command Buttons

Refresh - Update the information on the page.

11.4.1.13 Viewing Port Access Control History Log Summary



Selection Criteria

Interface - Selects the port to configure.

Configurable Data

Users - Selects the users that have access to the specified port or ports.

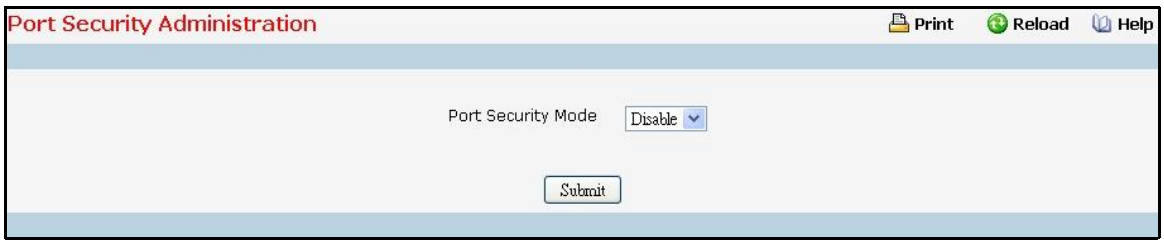
Command Buttons

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.

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

11.4.2 Managing Port Security

11.4.2.1 Configuring Port Security Administration Mode Page



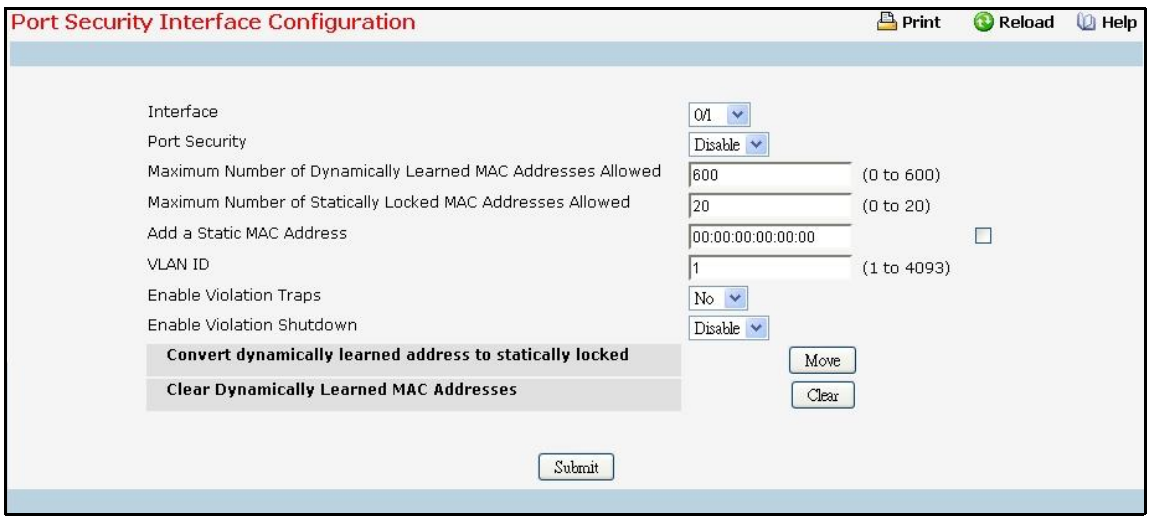
Configurable Data

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

Command Buttons

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

11.4.2.2 Configuring Port Security Interface Page



Selection Criteria

Interface - Selects the interface to be configured.

Configurable Data

Port Security - Enables or disables the Port Security feature for the selected interface.

Maximum Number of Dynamically Learned MAC Addresses Allowed - Sets the maximum number of dynamically learned MAC addresses on the selected interface. Valid range is (0 to 600).Default value is 600.

Add a static MAC address - By default the field is disabled, set the checkbox to add a MAC address to the list of statically locked MAC addresses for the selected interface.

VLAN ID - By default the field is disabled, set the checkbox to add corresponding VLAN ID for the MAC Address being added to the list of statically locked MAC addresses 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.

Maximum Number of Statically Locked MAC Addresses Allowed - Sets the maximum number of statically locked MAC addresses on the selected interface. Valid range is (0 to 20).Default value is 20.

Convert dynamically learned address to statically locked - Apply Button "Move" to convert dynamic MAC address entries to Static MAC address entries. Shows "Static Limit Reached. No Dynamic Addresses will be moved." when added Static MAC entries reaches to configured value of Maximum Number of Statically Locked MAC Addresses Allowed.

Clear Dynamically Learned MAC Addresses-Clears the Dynamic MAC addresses of the selected interface.

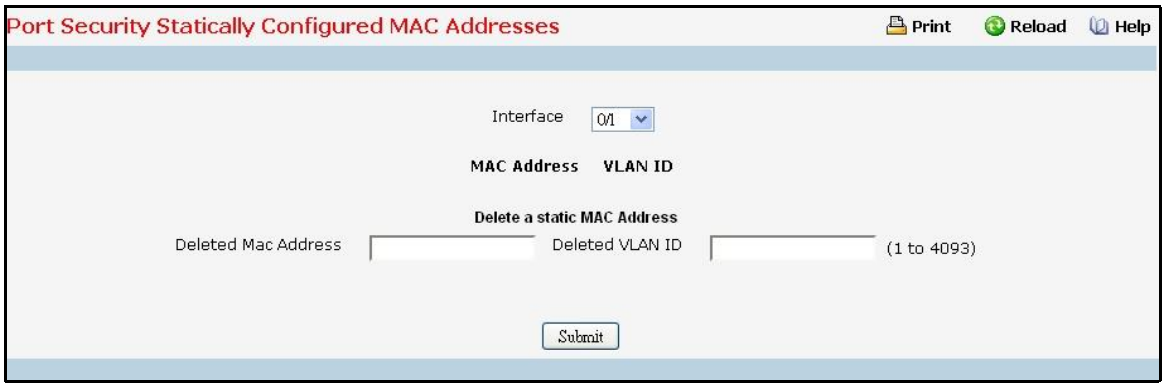
Command Buttons

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.

11.4.2.3 Deleting Port Security Statically Configured MAC Address Page



Selection Criteria

Interface - Select the physical interface for which you want to display data.

Configurable data

VLAN ID - Accepts user input for the VLAN ID corresponding to the MAC address being deleted.

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

Non-configurable data

Delete a Static MAC Address - Deletes the MAC address from the Port-Security Static MAC address table.

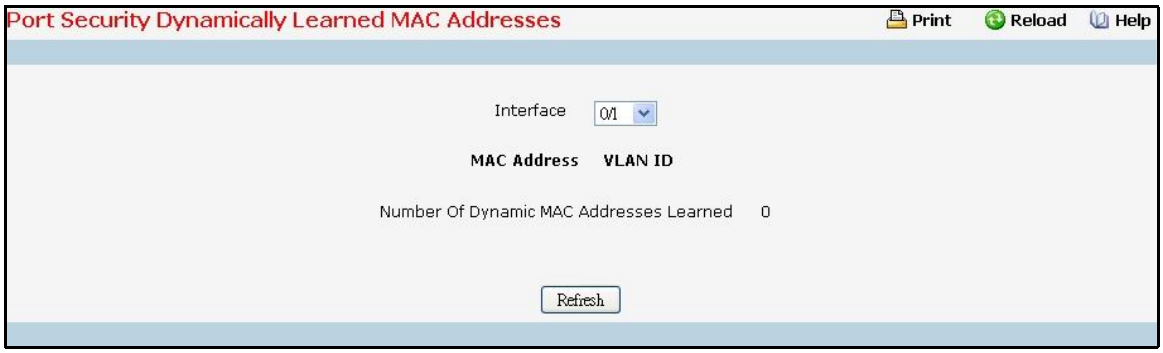
MAC Address - Displays the user specified statically locked MAC address.

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.

11.4.2.4 Viewing Port Security Dynamically Learnt MAC Address Page



Selection Criteria

Interface - 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.

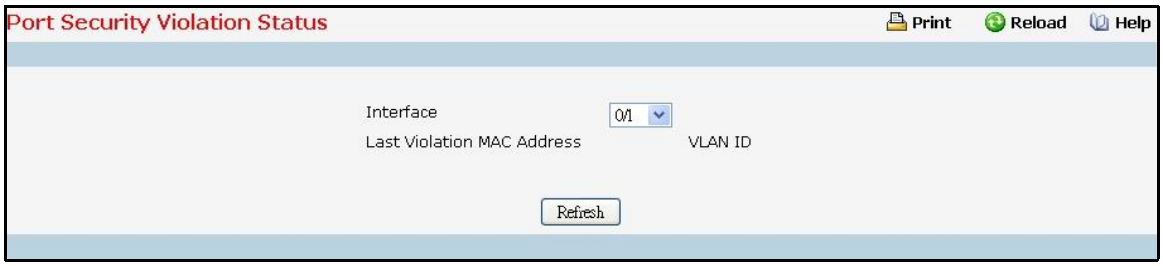
VLAN ID - Displays the VLAN ID corresponding to the MAC address.

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

Command Buttons

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

11.4.2.5 Viewing Port Security Violation Status Page



Selection Criteria

Interface - 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.

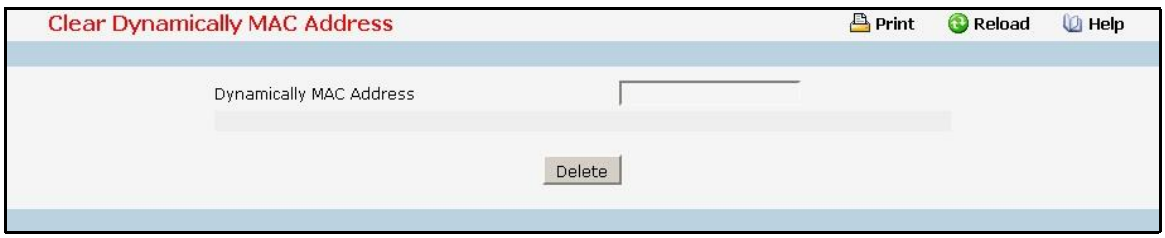
VLAN ID - Displays the VLAN ID corresponding to the Last Violation MAC address.

Command Buttons

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

11.4.2.6 Clearing Port Security Dynamically Learned MAC Addresses Page

Use this menu to delete a Dynamic MAC address of port security on switch.



Configurable Data

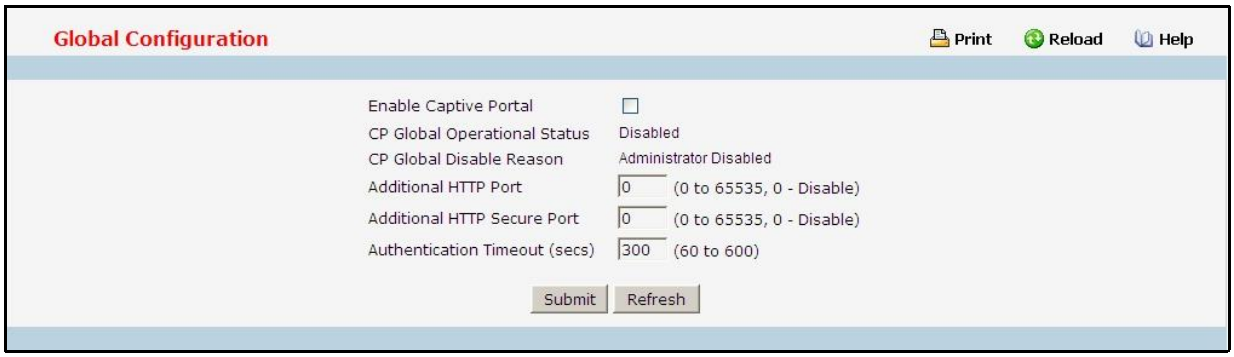
Dynamically MAC Address - Accepts user input for the MAC address to be deleted. The factory default is blank

Command Buttons

Delete - Send the updated screen to the switch perform the MAC clear

11.4.3 Managing Captive Portal

11.4.3.1 Configuring Captive Portal Global Configuration Page



Configurable Data

Enable Captive Portal - Select the check box to enable the CP feature on the switch. Clear the check box to disable the captive portal feature.

Additional HTTP Port - HTTP traffic uses port 80, but you can configure an additional port for HTTP traffic. Enter a port number between 0-65535 (excluding ports 80, 443, and the configured switch management port).

Additional HTTP Secure Port - HTTP traffic over SSL (HTTPS) uses port 443, but you can configure an additional port for HTTPS traffic. Enter a port number between 0-65535 (excluding ports 80, 443, and the configured switch management port).

Authentication Timeout - To access the network through a portal, the client must first enter authentication information on an authentication Web page. Enter the number of seconds to keep the authentication session open with the client. When the timeout expires, the switch disconnects any active TCP or SSL connection with the client.

Non-Configurable Data

CP Global Operational Status - Shows whether the CP feature is enabled.

CP Global Disable Reason - If CP is disabled, this field displays the reason, which can be one of the following:

· None

· Administratively Disabled ·

No IPv4 Address

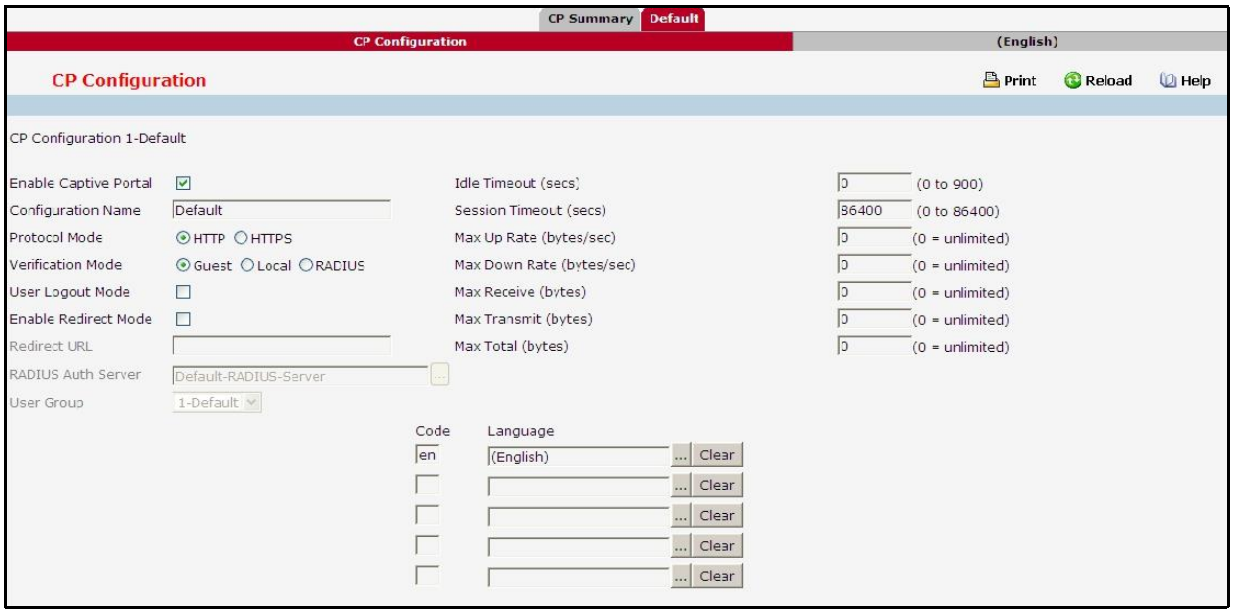
· Routing Enabled, but no IPv4 routing interface

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.

11.4.3.2 Captive Portal Configuration Page



Configurable Data

Enable Captive Portal - Select the check box to enable the CP. Clear the check box to disable it.

Configuration Name - This field allows you to change the name of the portal added from the CP Summary page.

Protocol Mode - Choose whether to use HTTP or HTTPs as the protocol for the portal to use during the verification process.

- HTTP: Does not use encryption during verification
- HTTPS: Uses the Secure Sockets Layer (SSL), which requires a certificate to provide encryption. The certificate is presented to the user at connection time.

Verification Mode - Select the mode for the CP to use to verify clients:

- Guest: The user does not need to be authenticated by a database.
- Local: The switch uses a local database to authenticated users.
- RADIUS: The switch uses a database on a remote RADIUS server to authenticate users.

User Logout Mode- Select this option to allow an authenticated client to deauthenticate from the network. If this option is clear or the user does not specifically request logout, the client connection status remains authenticated until the CP deauthenticates the user, for example by reaching the idle timeout or session timeout values.

Enable Redirect Mode- Select this option to specify that the CP should redirect the newly authenticated client to the configured URL. If this option is clear, the user sees the locale-specific welcome page after a successful verification.

Redirect URL- Specify the URL to which the newly authenticated client is redirected if the URL Redirect Mode is enabled.

RADIUS Auth Server- If the verification mode is RADIUS, click the ... button and select the name of the RADIUS server used for client authentications.

Idle Timeout- Enter the number of seconds a user can remain idle before automatically being logged out. If the value is set to 0, the timeout is not enforced.The default value is 0.

Session Timeout- Enter the number of seconds to wait before terminating a session. A user is logged out once the session timeout is reached. If the value is set to 0, the timeout is not enforced. The default value is 86400 (24 hours).

Max Up Rate- Enter the maximum speed, in bytes per second, that a client can transmit traffic when using the captive portal. This setting limits the bandwidth at which the client can send data into the network.

Max Down Rate- Enter the maximum speed, in bytes per second, that a client can receive traffic when using the captive portal. This setting limits the bandwidth at which the client can receive data from the network.

Max Receive- Enter the maximum number of bytes that a client is allowed to receive when using the captive portal. After this limit has been reached the user will be disconnected.

Max Transmit- Enter the maximum number of bytes that a client is allowed to transmit when using the captive portal. After this limit has been reached the user will be disconnected.

Max Total- Enter the maximum number of bytes the user is allowed to transfer (sum of bytes transmitted and received). After this limit has been reached the user will be disconnected.

User Group- If the Verification Mode is Local or RADIUS, assign an existing User Group to the captive portal or create a new group. All users who belong to the group are permitted to access the network through this portal. The User Group list is the same for all CP configurations on the switch.

Code- Enter the IANA Language Subtag code for the language. All codes are listed in the IANA Language Subtag Registry. If the language is currently supported by the switch, the code is filled in automatically when you select the language.

Language- To add a captive portal configuration in a language that is supported by the switch, click the ... button to display and select the language to use for the captive portal.

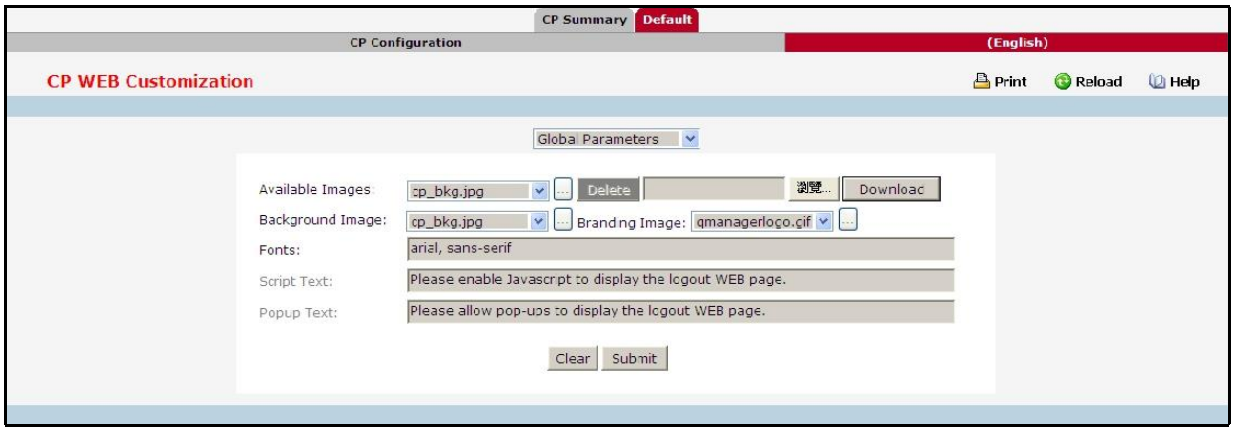
Command Buttons

Clear - All configurations will be set to the default values for this CP.

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.

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

11.4.3.3 Captive Portal Web Customization Page



Configurable Data

Available Images - The menu shows the images that are available to use for the page branding and the account image. To add images, click Browse and select an image on your local system (or accessible from your local system). Click Download to download the image to the switch. The image should be 5KB max, 200x200 pixels, GIF or JPG format. To delete an image from the list, select the file name from the menu and click Delete. You can only delete images that you download.

Branding Image - Select the name of the image file to display on the top left corner of the page. This image is used for branding purposes, such as the company logo.

Background Image - Select the name of the image to display as the page background. Use the drop-down menu to display the file names of the available images. Click the ... button to display the available images. Click the image to select it. To specify that no background image is to be used, select <No Selection>.

Fonts - Enter the name of the font to use for all text on the CP page.

Script Text- Specify the text to indicate that users must enable JavaScript to display the logout WEB page. This field is only applicable when the User Logout Mode is enabled, but you can modify the text whether the feature is enabled or disabled.

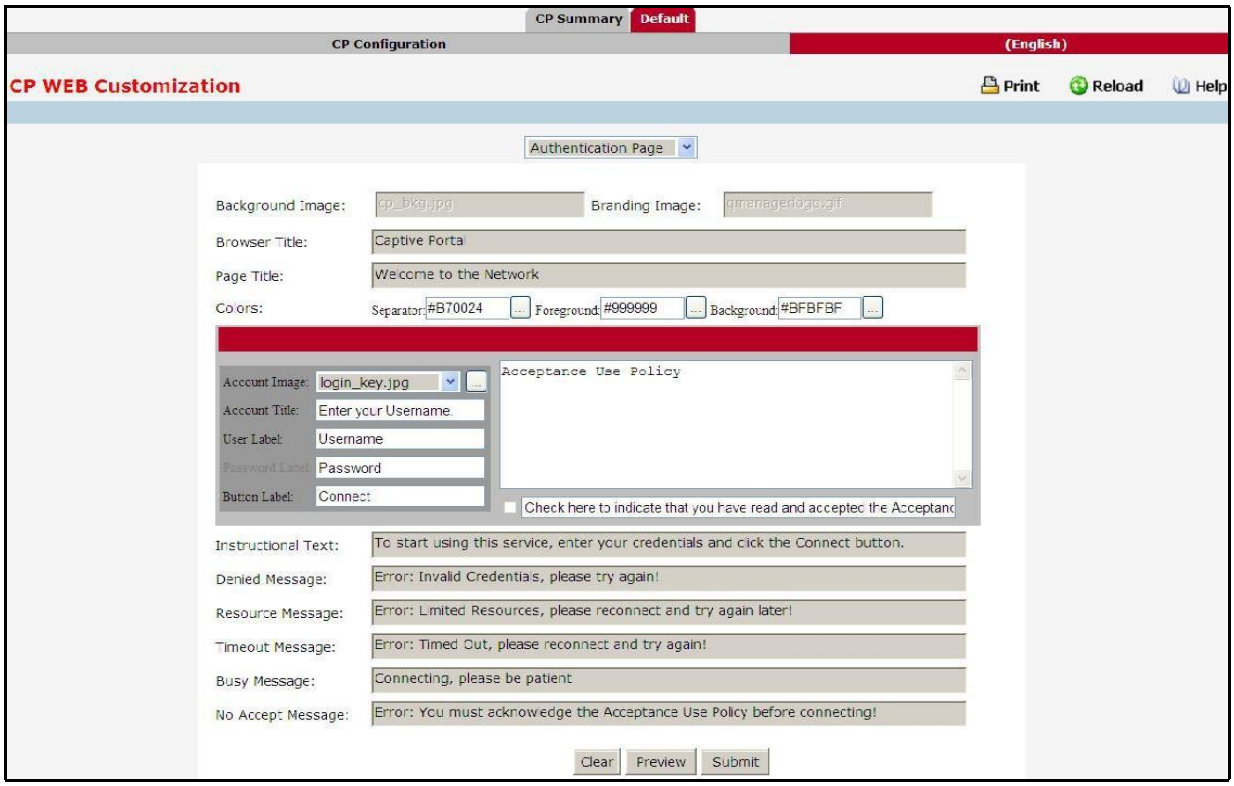
Popup Text - Specify the text to indicate that users must allow pop-up windows to display the logout WEB page. This field is only applicable when the User Logout Mode is enabled, but you can modify the text whether the feature is enabled or disabled.

Command Buttons

Clear - All configurations will be set to the default values for this CP.

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.

11.4.3.4 Captive Portal Web Customization Authentication Page



Configurable Data

Background Image - Shows the name of the current background image on the Authentication Page. This field can be modified from the CP WEB Customization Global Parameters page.

Branding Image - Shows the name of the current branding image on the Authentication Page. This field can be modified from the CP WEB Customization Global Parameters page.

Browser Title - Enter the text to display on the client's Web browser title bar or tab.

Page Title - Enter the text to use as the page title. This is the text that identifies the page.

Colors - Select the colors to use for the CP page. Click the ... button, and then select the color to use. The sample account information is updated with the colors you choose.

Account Image - Select the image that will display on the Captive Portal page above the login field. The image display area is 55H X 310W pixels.

Account Title - Enter the summary text to display that instructs users to authenticate.

User Label- Enter the text to display next to the field where the user enters the username.

Password Label - Enter the text to display next to the field where the user enters the password.

Button Label - Enter the text to display on the button the user clicks to connect to the network.

Acceptance Use Policy Text Box - Enter the text to display in the Acceptance Use Policy field. The acceptance use policy instructs users about the conditions under which they are allowed to access the network. The policy can contain up to 8192 text characters.

Acceptance Check Box Prompt - Enter the text to display next to the box that the user must select to indicate that he or she accepts the terms of use.

Instructional Text - Enter the detailed text to display that instructs users to authenticate. This text appears under the button.

Denied Message - Enter the text to display when the user does not provide valid authentication information. This message displays after the user clicks the button to connect to the network.

Resource Message - Enter the text to display when the system has rejected authentication due to system resource limitations. This message displays after the user clicks the button to connect to the network.

Timeout Message - Enter the text to display when the system has rejected authentication because the authentication transaction took too long. This could be due to user input time, or a timeout due to the overall transaction.

Busy Message - Enter the text to display when the user does not provide valid authentication information. This message displays after the user clicks the button to connect to the network.

No Accept Message - Enter the text to display when the user did not accept the acceptance use policy. This message displays after the user clicks the button to connect to the network.

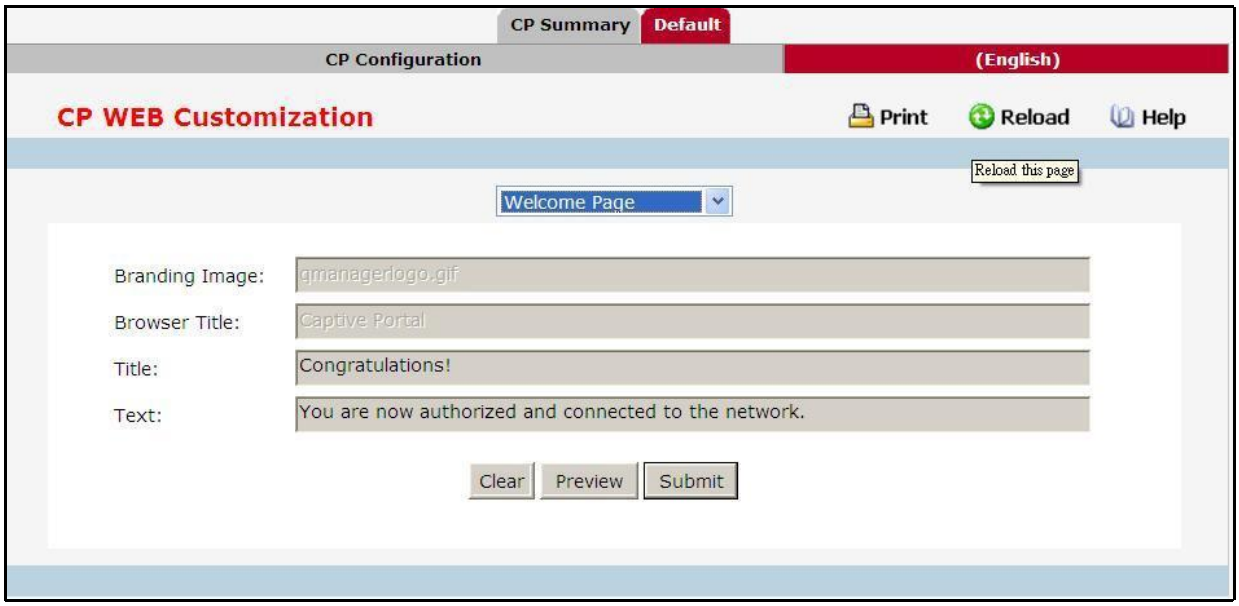
Command Buttons

Clear - Clear all the configuration to the default value for this CP.

Preview - Preview the web page of the confguration.

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.

11.4.3.5 Captive Portal Web Customization Welcome Page



Configurable Data

Background Image - Shows the name of the current background image on the Welcome Page. This field can be modified from the CP WEB Customization Global Parameters page.

Branding Image - Shows the name of the current branding image on the Welcome Page. This field can be modified from the CP WEB Customization Global Parameters page.

Welcome Title - Enter the title to display to greet the user after he or she successfully connects to the network.

Welcome Text - Enter the optional text to display to further identify the network to be access by the CP user. This message displays under the Welcome Title.

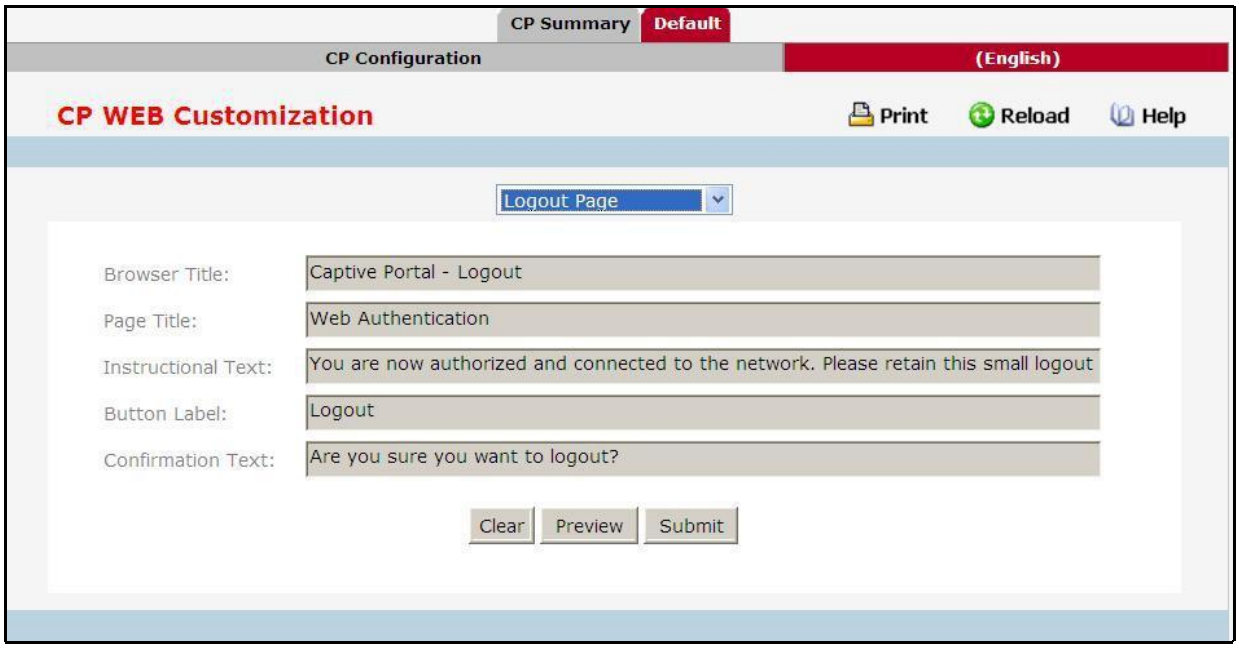
Command Buttons

Clear - Clear all the configuration to the default value for this CP.

Preview - Preview the web page of the confguration.

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.

11.4.3.6 Captive Portal Web Customization Logout Page



Configurable Data

Browser Title - Enter the text to display on the title bar of the Logout page.

Page Title - Enter the text to use as the page title. This is the text that identifies the page.

Instructional Text - Enter the detailed text to display that confirms that the user has been authenticated and instructs the user how to deauthenticate.

Button Label - Enter the text to display on the button the user clicks to deauthenticate. Confirmation Text Enter the detailed text to display that prompts users to confirm the deauthentication process.

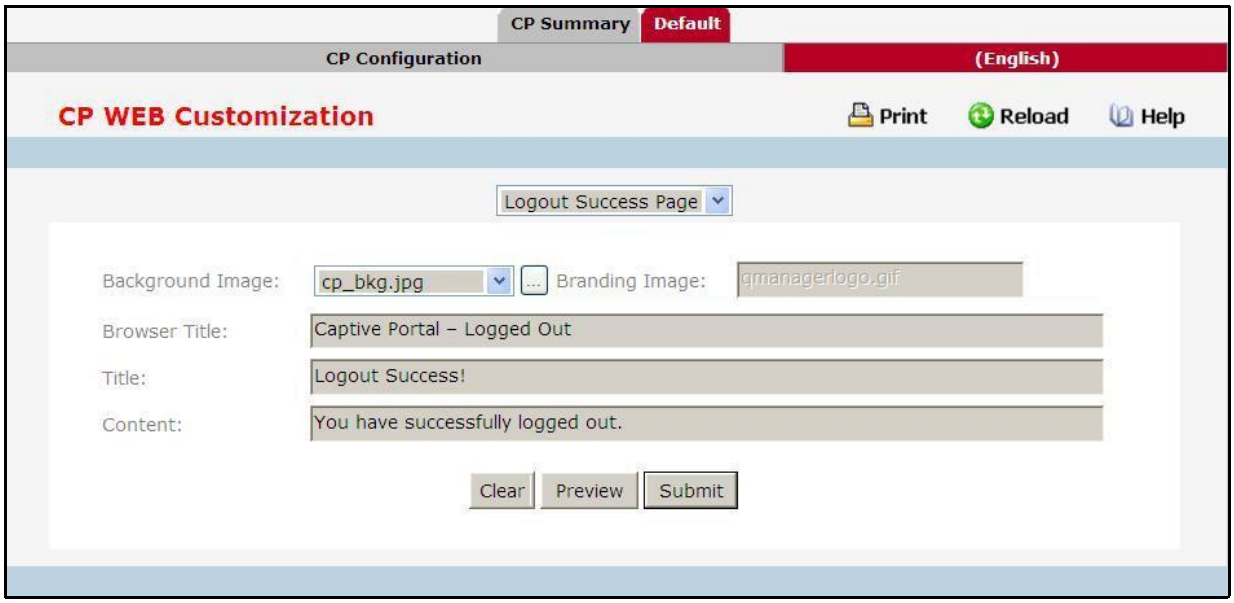
Command Buttons

Clear - Clear all the configuration to the default value for this CP.

Preview - Preview the web page of the confguration.

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.

11.4.3.7 Captive Portal Web Customization Logout Page



Configurable Data

Background Image - Shows the name of the current background image on the Logout Success page. This field can be modified from the CP WEB Customization Global Parameters page.

Branding Image - Shows the name of the current branding image on the Logout Success page. This field can be modified from the CP WEB Customization Global Parameters page.

Browser Title - Enter the text to display on the title bar of the Logout Success page.

Title - Enter the text to use as the page title. This is the text that identifies the page.

Content - Enter the text to display that confirms that the user has been deauthenticated.

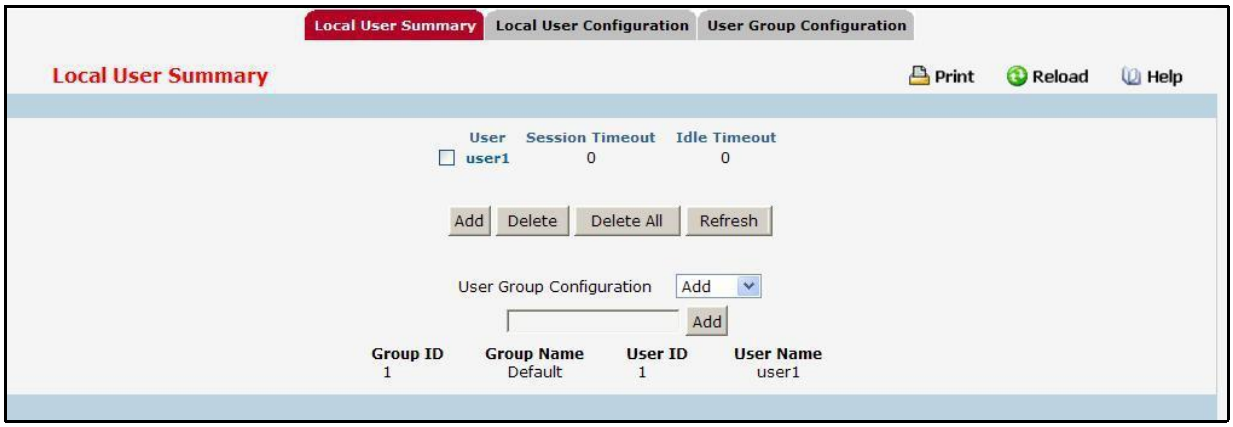
Command Buttons

Clear - Clear all the configuration to the default value for this CP.

Preview - Preview the web page of the confguration.

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.

11.4.3.8 Captive Portal Local User Summary Page



Non-Configurable Data

User - Identifies the name of the user.

Session Timeout - Shows the number of seconds a user is permitted to remain connected to the network. Once the Session Timeout value is reached, the user is logged out automatically.

Idle Timeout - Shows the number of seconds the user can remain idle before the switch automatically logs the user out. A value of 0 means that the user will not be logged out automatically.

Command Buttons

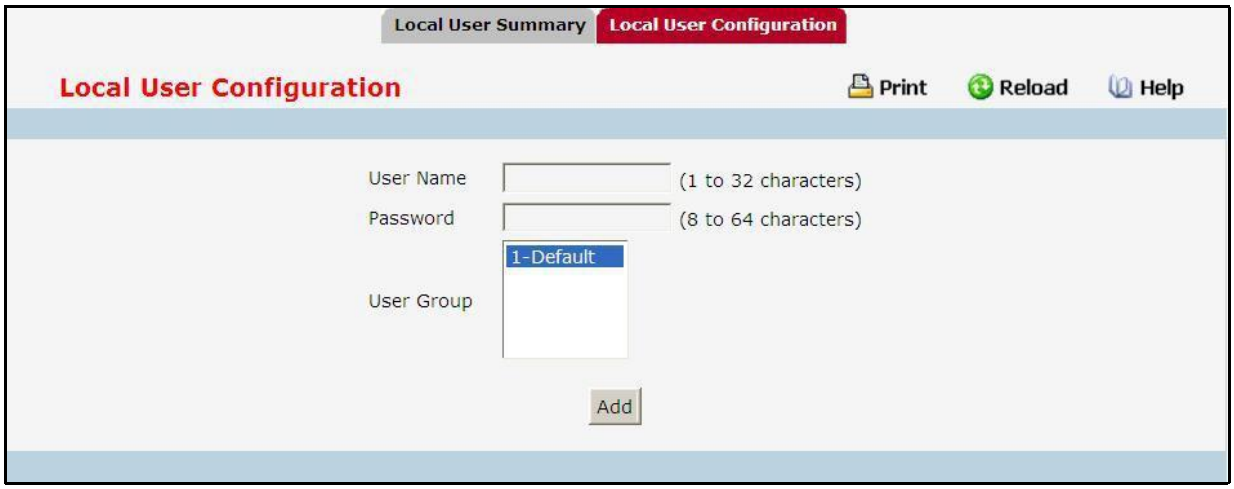
Add -Click Add to add a new user to the Local User database.

Delete -Select the check box next to the user to remove and click Delete. Select multiple check boxes to delete more than one user at a time.

Delete All -Click Delete All to remove all configured users from the local database.

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

11.4.3.9 Captive Portal Add a Local User Page



Configurable Data

User Name - Enter the name of the user.

Password - Enter a password for the user. The password length can be from 8 to 64 characters.

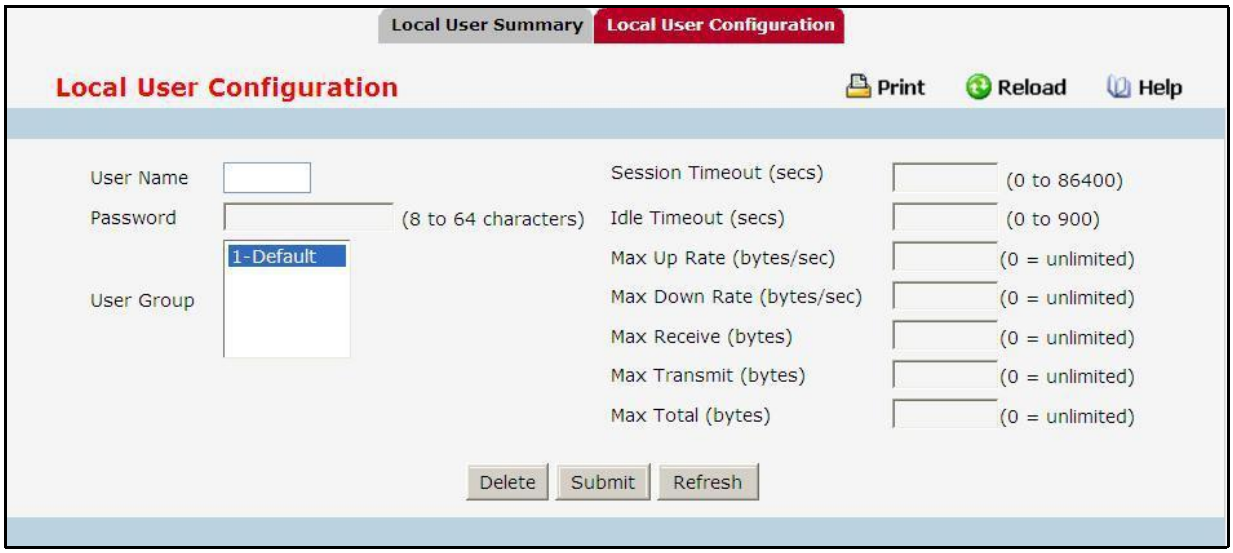
User Group - Assign the user to at least one User Group. To assign a user to more than one group, press the Ctrl key and click each group.

New users are assigned to the 1-Default user group by default.

Command Buttons

Add - Add a user account.

11.4.3.10 Captive Portal Local User Configuration Page



Configurable Data

User Name - Enter the name of the user.

Password - Enter a password for the user. The password length can be from 8 to 64 characters.

User Group - Assign the user to at least one User Group. To assign a user to more than one group, press the Ctrl key and click each group.

New users are assigned to the 1-Default user group by default.

Session Timeout - Shows the number of seconds a user is permitted to remain connected to the network. Once the Session Timeout value is reached, the user is logged out automatically.

Idle Timeout - Enter the number of seconds the user can remain idle before the switch automatically logs the user out. A value of 0 means that the user does not have an idle timeout limit.

Max Up Rate - Enter the maximum speed, in bytes per second, that the user can transmit traffic when using the captive portal. This setting limits the bandwidth at which the user can send data into the network.

Max Down Rate - Enter the maximum speed, in bytes per second, that the user can receive traffic when using the captive portal. This setting limits the bandwidth at which the user can receive data from the network.

Max Receive - Enter the maximum number of bytes that the user is allowed to receive when using the captive portal. After this limit has been reached the user will be disconnected.

Max Transmit - Enter the maximum number of bytes that the user is allowed to transmit when using the captive portal. After this limit has been reached the user will be disconnected.

Max Total - Enter the maximum number of bytes the user is allowed to transfer (sum of bytes transmitted and received). After this limit has been reached the user will be disconnected.

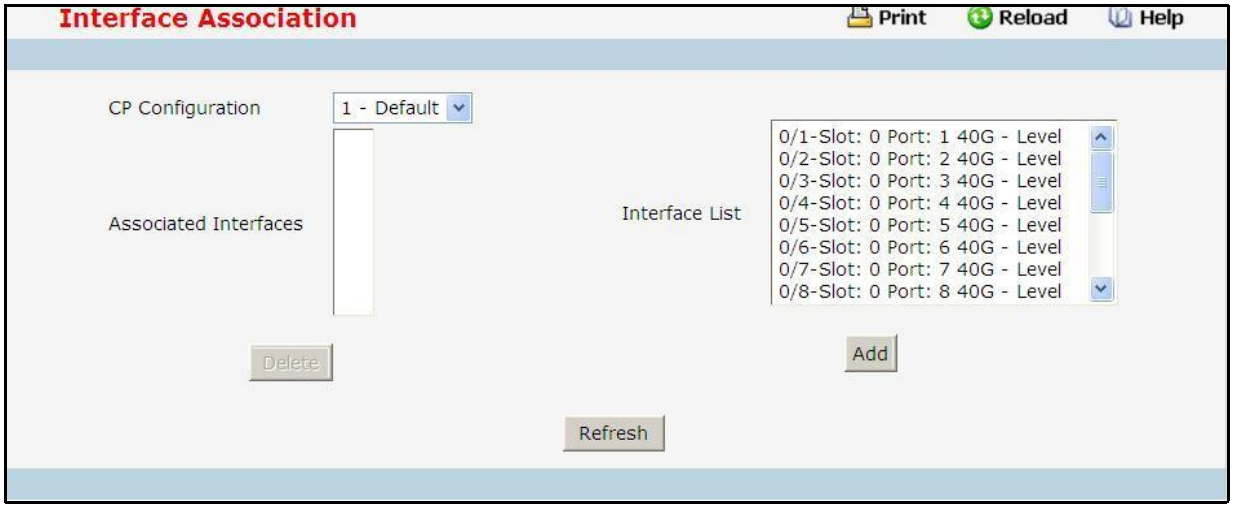
Command Buttons

Delete - Click Delete to remove the user from the local database.

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.

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

11.4.3.11 Captive Portal Interface Association Page



Configurable Data

CP Configuration - Lists the captive portals configured on the switch by number and name.

Associated Interfaces - Lists the wireless interfaces that are currently associated with the selected captive portal. The interface is identified by its wireless network number and SSID.

Interface List - Lists the wireless interfaces available on the switch that are not currently associated with a CP. Each interface is identified by its wireless network number and SSID.

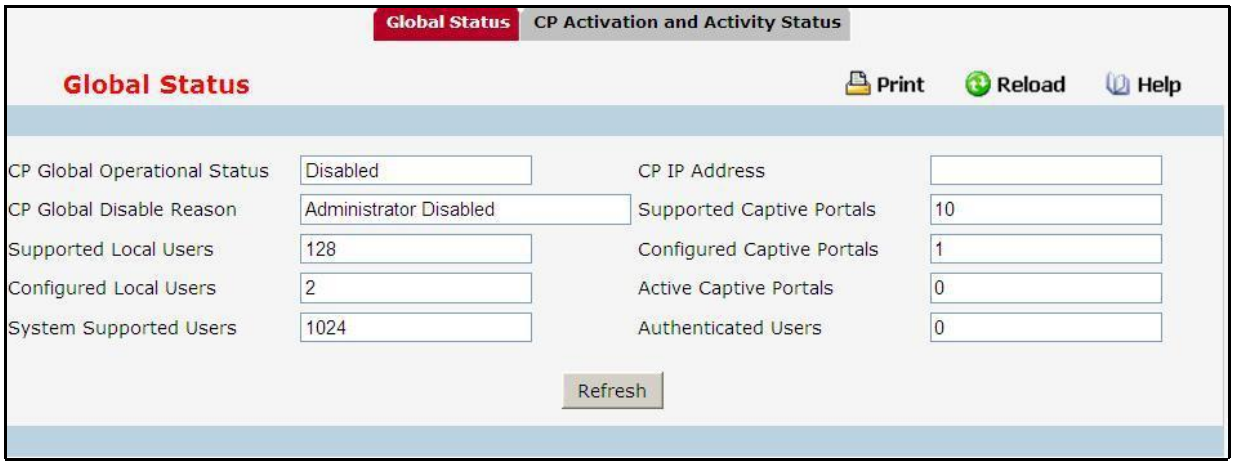
Command Buttons

Delete - when you click delet, the interface is removed from the Associated Interface list and appears in the Interface List.

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

Add - Associates the selected Captive Portal and interfaces from Interface List.

11.4.3.12 Captive Portal CP Status Page



Non-Configurable Data

CP Global Operational Status - Shows whether the CP feature is enabled.

CP Global Disable Reason - Indicates the reason for the CP to be disabled, which can be one of the following:

· None

· Administratively Disabled ·

No IPv4 Address

· Routing Enabled, but no IPv4 routing interface

Supported Local Users - Shows the number of entries that the Local User database supports.

Configured Local Users - Shows the number of local users configured on the switch.

System Supported Users - Shows the number of authenticated users that the system can support. CP

IP Address - Shows the captive portal IP address

Supported Captive Portals - Shows the number of supported captive portals in the system.

Configured Captive Portals - Shows the number of captive portals configured on the switch.

Active Captive Portals - Shows the number of captive portal instances that are operationally enabled.

Authenticated Users - Shows the number of users currently authenticated to all captive portal instances on this switch.

Command Buttons

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

11.4.3.13 Captive Portal CP Activation and Activity Status Page

Non-Configurable Data

Operational Status - Indicates whether the captive portal is enabled or disabled.

Disable Reason - If the captive portal is disabled, then this field indicates the reason. The portal instance may be disabled for the following reasons:

· None - CP is enabled.

· Administratively Disabled

· RADIUS Authentication mode enabled, but RADIUS server is not defined. ·

Not associated with any interfaces.

· The associated interfaces do not exist or do not support the CP capability.

Blocked Status - Indicates whether authentication attempts to the captive portal are currently blocked.

· Use the Block and Unblock buttons to control the blocked status. If the CP is blocked, users cannot gain access to the network through the CP. Use this function to temporarily protect the network during unexpected events, such as denial of service attacks.

· Block and Unblock are only available when the CP operational status is Enabled.

Authenticated Users - Shows the number of users that successfully authenticated to this captive portal and are currently using the portal.

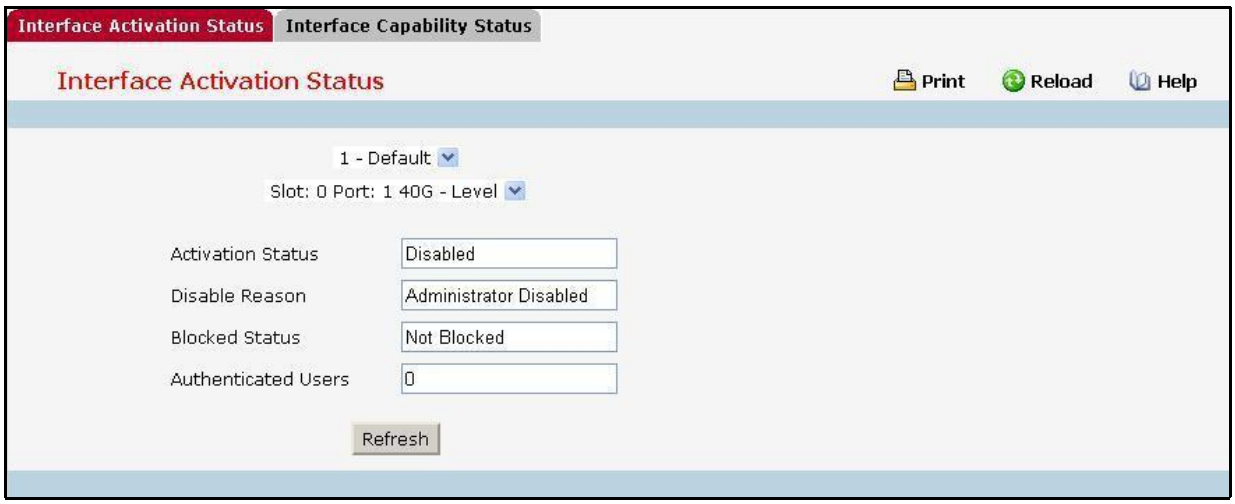
Command Buttons

Block - Click Block to prevent users from gaining access to the network through the selected captive portal.

Unblock - If the Blocked Status of the selected captive portal is Blocked, click Unblock to allow access to the network through the captive portal.

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

11.4.3.14 Captive Portal Interface Activation Status Page



Non-Configurable Data

Operational Status - Shows whether the portal is active on the specified interface.

Disable Reason - If the selected CP is disabled on this interface, this field indicates the reason, which can be one of the following:

- Interface Not Attached
- Disabled by Administrator

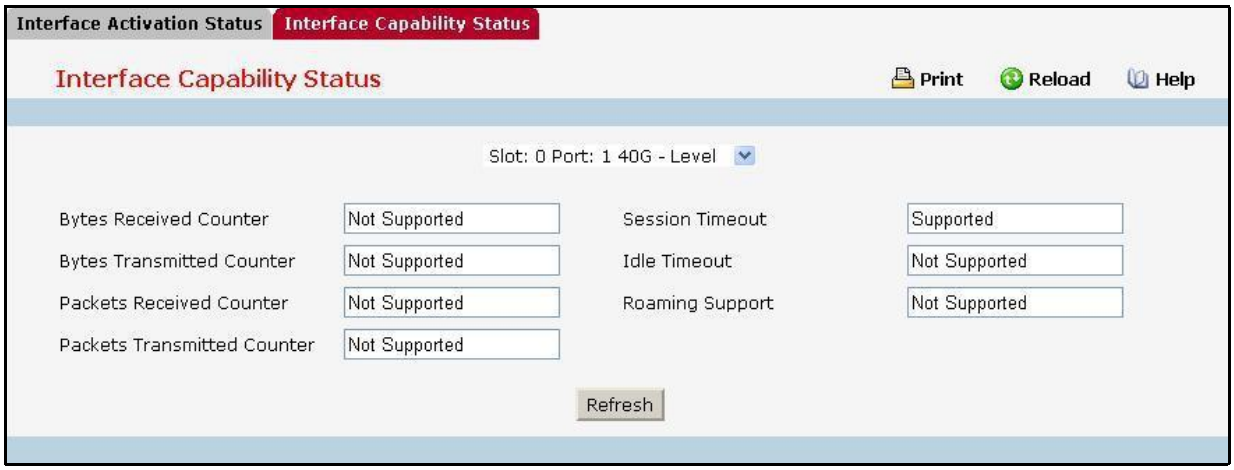
Blocked Status - Indicates whether the captive portal is temporarily blocked for authentications.

Authenticated Users - Displays the number of authenticated users using the captive portal instance on this interface.

Command Buttons

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

11.4.3.15 Captive Portal Interface Capability Status Page



Non-Configurable Data

Session Timeout - Shows whether the interface supports client session timeout. This attribute is supported on all interfaces.

Bytes Received Counter - Shows whether the interface supports displaying the number of bytes received from each client.

Bytes Transmitted Counter - Shows whether the interface supports displaying the number of bytes transmitted to each client.

Roaming Support - Shows whether the interface supports client roaming. Only wireless interfaces support client roaming.

Idle Timeout - Shows whether the interface supports a timeout when the user does not send or receive any traffic.

Packets Received Counter - Shows whether the interface supports displaying the number of packets received from each client.

Packets Transmitted Counter- Shows whether the interface supports displaying the number of packets transmitted to each client.

Command Buttons

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

11.4.3.16 Captive Portal Client Summary Page

Non-Configurable Data

MAC Address - Identifies the MAC address of the wireless client (if applicable). If the MAC address is marked with an asterisk (*), the authenticated client is authenticated by a peer switch. In order words, the cluster controller was not the authenticator.

IP Address - Identifies the IP address of the wireless client (if applicable).

User - Displays the user name (or Guest ID) of the connected client.

Protocol - Shows the current connection protocol, which is either HTTP or HTTPS.

Verification - Shows the current account type, which is Guest, Local, or RADIUS.

Command Buttons

Delete - Click Delete to force the captive portal to disconnect an authenticated client, select the check box next to the client MAC address.

Delete All - Click Delete All to disconnect all clients from all captive portals.

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

11.4.3.17 Captive Portal Client Detail Page

Non-Configurable Data

Client IP Address - Identifies the IP address of the wireless client (if applicable).

CP Configuration - Identifies the CP configuration the wireless client is using.

Protocol - Shows the current connection protocol, which is either HTTP or HTTPS.

Session Time - Shows the amount of time that has passed since the client was authorized.

Captive Portal Client Auth Fail Count - Shows the numberof times that user login failed.

Switch Type - Shows whether the switch handling authentication for this client is the local switch or a peer switch in the cluster.

User Name - Displays the user name (or Guest ID) of the connected client.

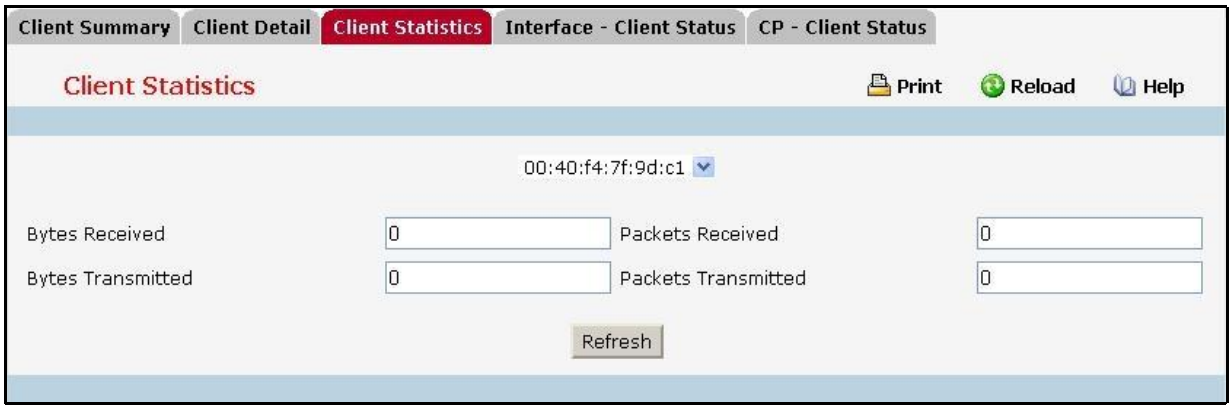
Interface - Identifies the interface the wireless client is using.

Verification - Shows the current account type, which is Guest, Local, or RADIUS.

Command Buttons

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

11.4.3.18 Captive Portal Client Statistics Page



Non-Configurable Data

Bytes Transmitted - Total bytes the client has transmitted.

Bytes Received - Total bytes the client has received.

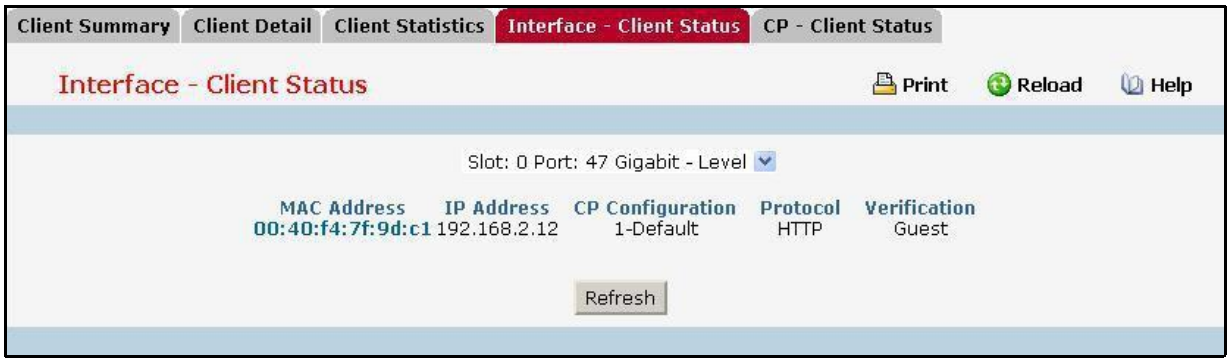
Packets Transmitted - Total packets the client has transmitted.

Packets Received - Total packets the client has received

Command Buttons

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

11.4.3.19 Captive Portal Interface - Client Status Page



Non-Configurable Data

MAC Address - Identifies the MAC address of the wireless client. If the MAC address is marked with an asterisk (*), the authenticated client is authenticated by a peer switch. In order words, the cluster controller was not the authenticator.

IP Address - Identifies the IP address of the wireless client.

CP Configuration - Identifies the captive portal the client used to access the network.

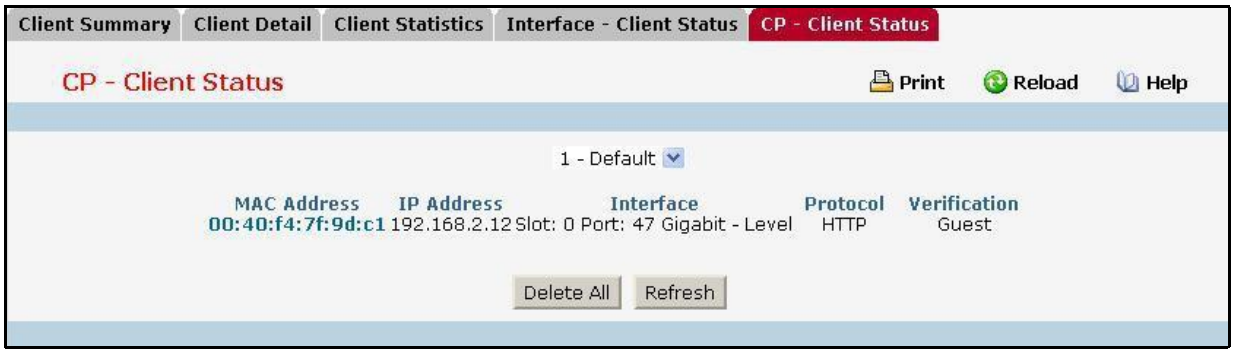
Protocol - Shows the current connection protocol, which is either HTTP or HTTPS.

Verification - Shows the current account type, which is Guest, Local, or RADIUS.

Command Buttons

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

11.4.3.20 Captive Portal CP - Client Status Page



Non-Configurable Data

MAC Address - Identifies the MAC address of the wireless client (if applicable). If the MAC address is marked with an asterisk (*), the authenticated client is authenticated by a peer switch. In order words, the cluster controller was not the authenticator.

IP Address - Identifies the IP address of the wireless client (if applicable).

User - Displays the user name (or Guest ID) of the connected client.

Protocol - Shows the current connection protocol, which is either HTTP or HTTPS.

Verification - Shows the current account type, which is Guest, Local, or RADIUS.

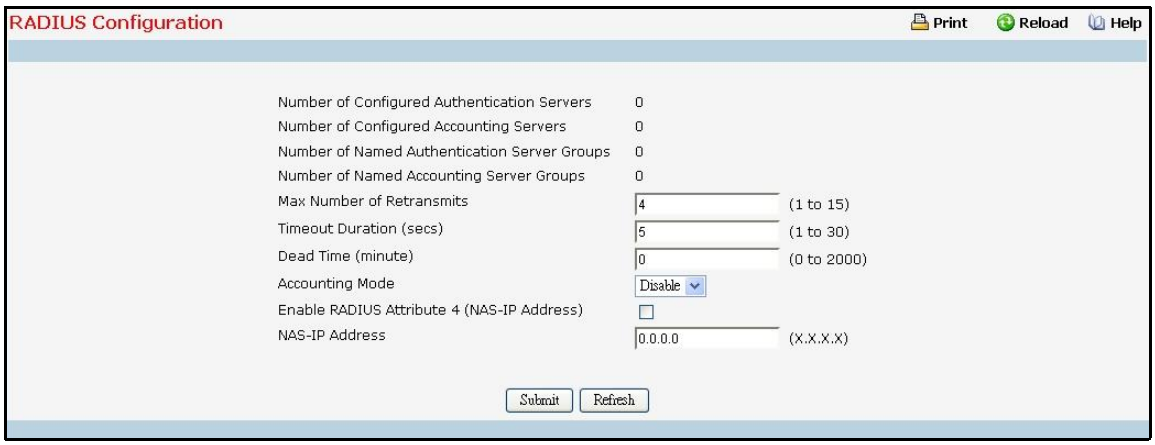
Command Buttons

Delete All - Click Delete All to disconnect all clients from all captive portals.

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

11.4.4 Managing RADIUS

11.4.4.1 Configuring RADIUS Configuration Page



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.

Accounting Mode - Selects if the RADIUS accounting mode is enabled or disabled.

Enable Radius Attribute 4 (NAS-IP Address) -To set the network access server (NAS) IP address for the RADIUS server, select the option and enter the IP address of the NAS in the available field. The address should be unique to the NAS within the scope of the RADIUS server. The NAS IP address is only used in Access-Request packets. By default this mode is disabled.

NAS-IP Address - The NAS-IP-Address of the RADIUS authentication client referred to in this table entry. By default it is not configured.

Non-Configurable Data

Number of Configured Authentication Servers - Displays the number of configured Authentication RADIUS servers. The value can range from 0 to 32.

Number of Configured Accounting Servers - Displays the number of RADIUS Accounting Servers configured. The value can range from 0 to 32.

Number of Named Authentication Server Groups - Displays the number of Named RADIUS server Authentication groups configured.

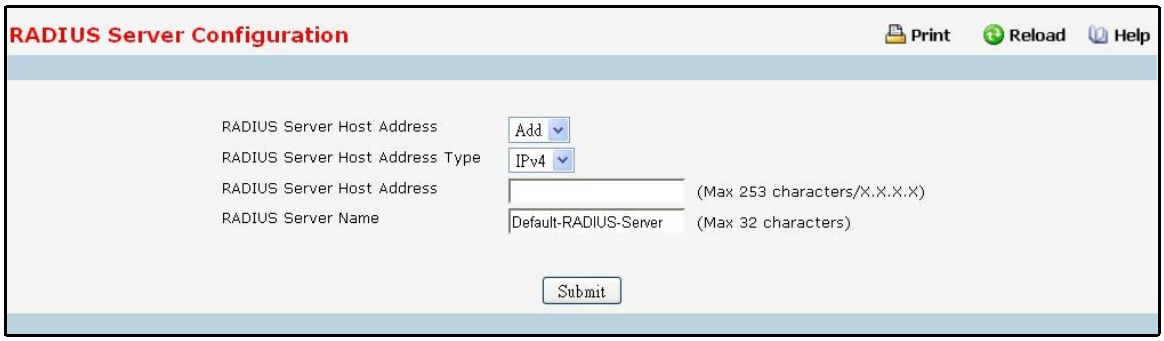
Number of Named Accounting Server Groups - Displays the number of Named RADIUS server Accounting groups configured.

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.

Refresh - Update the information on the page.

11.4.4.2 Configuring RADIUS Server Configuration Page



Selection Criteria

RADIUS Server Host Address -Use the drop-down menu to select the IP address of the RADIUS server to view or configure. Select Add to configure additional RADIUS servers.

Primary Server - Sets the selected server to the Primary (Yes) or Secondary (No) server. If you configure multiple RADIUS servers with the same RADIUS Server Name, designate one server as the primary and the other(s) as the backup server(s). The switch attempts to use the primary server first, and if the primary server does not respond, the switch attempts to use one of the backup servers with the same RADIUS Server Name. If the server is not set as Primary, by default it is set as Secondary.

Message Authenticator - Enable or disable the message authenticator attribute for the selected server.

Configurable Data

RADIUS Server Host Address - IP Address or Hostname of the configured RADIUS server. Hostnames are composed of series of labels concatenated with dots. Each label must be between 1 and 63 characters long, and the entire hostname has a maximum of 253 characters. This object cannot be changed after creation.

Port - The UDP port used by this server. The valid range is 0 - 65535. The default port for RADIUS authentication is 1812.

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.

RADIUS Server Name - Shows the RADIUS server name. To change the name, enter up to 31 alphanumeric characters. Spaces, hyphens, and underscores are also permitted. If you do not assign a name, the server is assigned the default name Default-RADIUS-Server. You can use the same name for multiple RADIUS Authentication servers. RADIUS clients can use RADIUS servers with the same name as backups for each other.

Non-Configurable Data

Current - Indicates whether the selected RADIUS server is the current server (Yes) or a backup server (No). If more than one RADIUS server is configured with the same name, the switch selects one of the servers to be the current server from the group of servers with the same name. When the switch sends a RADIUS request to the named server, the request is directed to the server selected as the current server. Initially the primary server is selected as the current server. If the primary

server fails, one of the other servers becomes the current server. If the primary server is not configured, the current server is the most recently configured RADIUS server.

Secret Configured - Indicates if the shared secret for this server has been configured.

Command Buttons

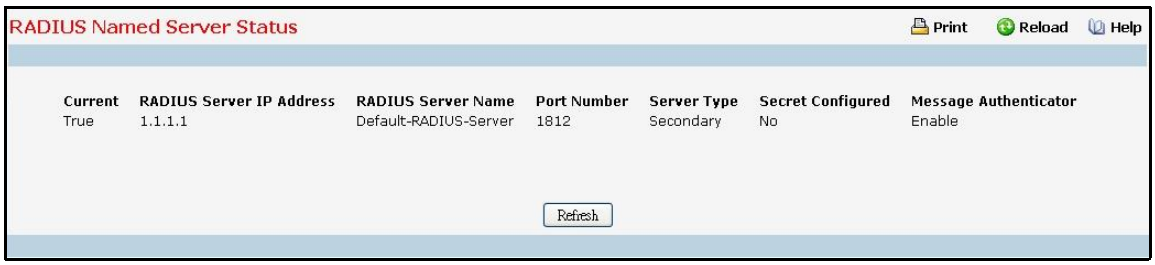
Submit - Sends the updated screen to the switch and causes the changes to take effect on the switch but these changes will not be retained across a power cycle unless a save is performed.

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.

11.4.4.3 RADIUS Named Server Status

Use this panel to view the information about the RADIUS servers configured on the system.



Non-Configurable Data

Current - Indicates whether the selected RADIUS server is the current server (True) or a backup server (False). If more than one RADIUS server is configured with the same name, the switch selects one of the servers to be the current server from the group of servers with the same name.When the switch sends a RADIUS request to the named server, the request is directed to the server selected as the current server. Initially the primary server is selected as the current server. If the primary server fails, one of the other servers becomes the current server. If the primary server is not configured, the current server is the most recently configured RADIUS server.

RADIUS Server IP Address - Shows the IP address of the RADIUS server.

RADIUS Server Name - Shows the RADIUS server name.Multiple RADIUS servers can have the same name. In this case, RADIUS clients can use RADIUS servers with the same name as backups for each other.

Port Number - Identifies the authentication port the server uses to verify the RADIUS server authentication. The port is a UDP port.

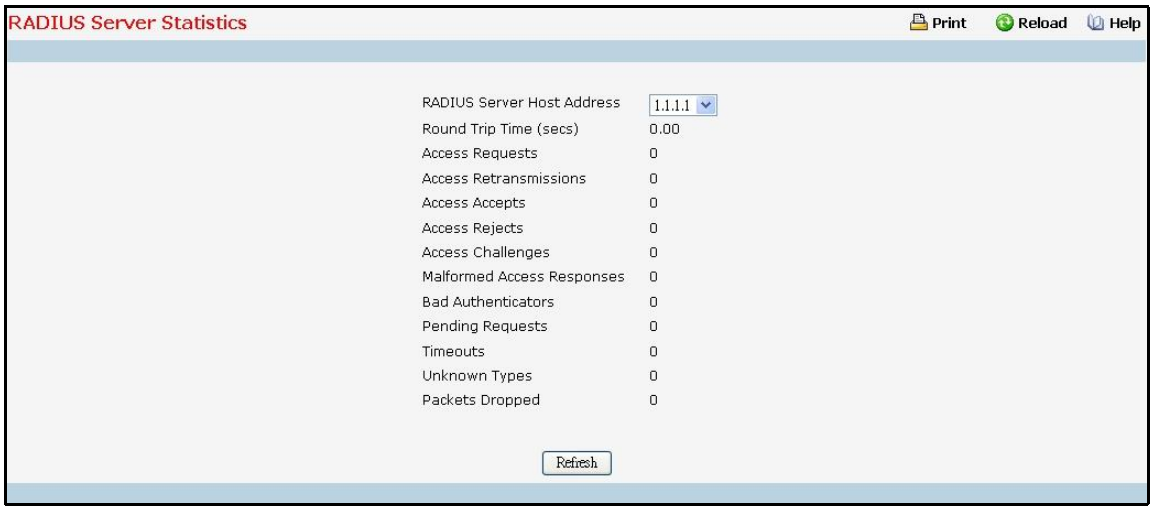
Server Type - Shows whether the server is a Primary or Secondary server.

Secret Configured - Indicates whether the shared secret for this server has been configured.

Command Buttons

Refresh - Update the information on the page.

11.4.4.4 Viewing RADIUS Server Statistics Page



Selection Criteria

RADIUS Server Host 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.

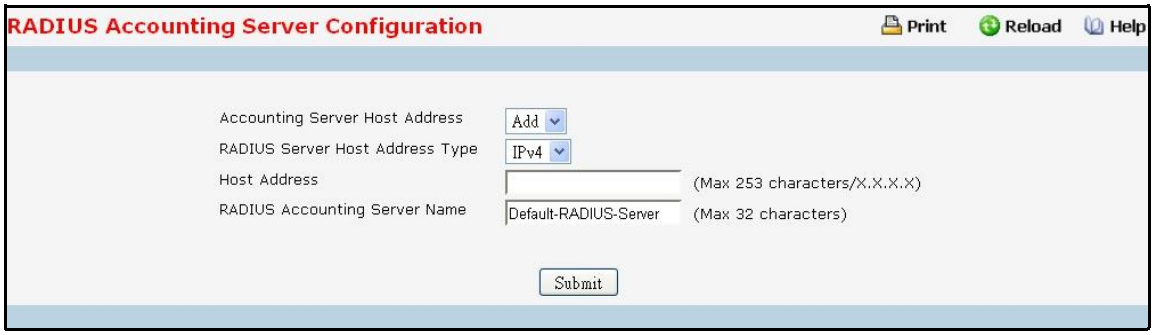
Unknown Types - The number of RADIUS packets of unknown type which were received from this server on the authentication port.

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.

11.4.4.5 Defining RADIUS Accounting Server Configuration Page



Selection Criteria

Accounting Server Host 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

Host Address- IP Address or Hostname of the configured Accounting RADIUS server. Hostnames are composed of series of labels concatenated with dots. Each label must be between 1 and 63 characters long, and the entire hostname has a maximum of 253 characters. This object cannot be changed after creation.

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. The default port for RADIUS accounting is 1813.

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.

RADIUS Accounting Server Name - Enter the name of the RADIUS accounting server. The name can contain up to 32 alphanumeric characters. Spaces, hyphens, and underscores are also permitted. If you do not assign a name, the server is assigned the default name Default-RADIUS-Server.You cannot use the same name for multiple RADIUS accounting servers.

Non-Configurable Data

Secret Configured - Indicates if the secret has been configured for this accounting server.

Command Buttons

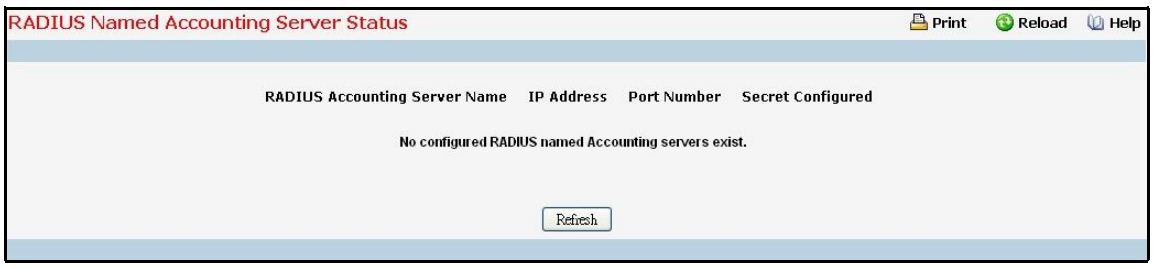
Submit - Sends the updated screen to the switch and causes the changes to take effect on the switch but these changes will not be retained across a power cycle unless a save is performed.

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.

11.4.4.6 RADIUS Named Accounting Server Status

The RADIUS Named Accounting Server Status page shows summary information about the accounting servers configured on the system.



Non-Configurable Data

RADIUS Accounting Server Name - Shows the RADIUS accounting server name.Multiple RADIUS accounting servers can have the same name. In this case, RADIUS clients can use RADIUS servers with the same name as backups for each other.

IP Address - Shows the IP address of the RADIUS server.

Port Number - Identifies the authentication port the server uses to verify the RADIUS server authentication. The port is a UDP port.

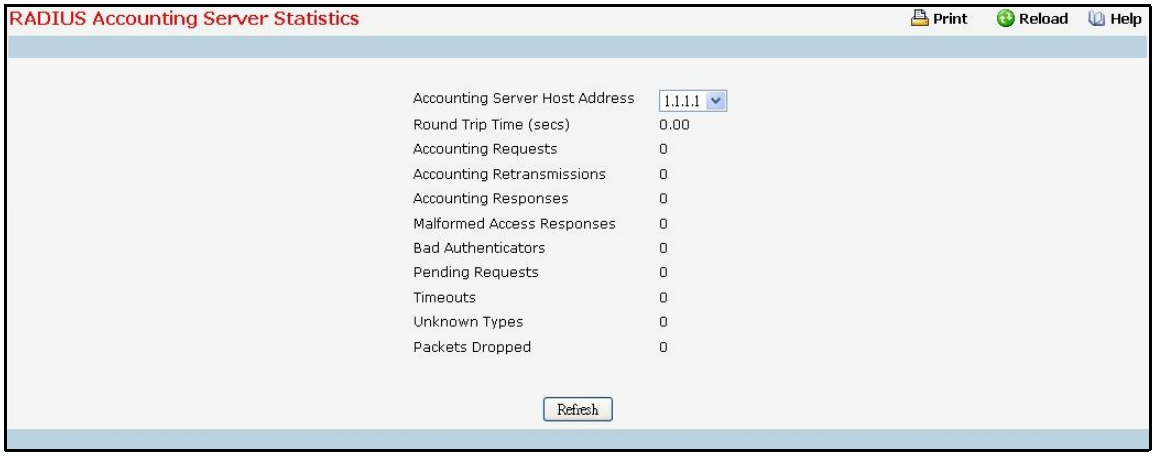
Secret Configured - Indicates whether the shared secret for this server has been configured.

Command Buttons

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

11.4.4.7 Viewing RADIUS Accounting Server Statistics Page

Use the RADIUS Accounting Server Statistics page to view statistical information for each RADIUS server configured on the system.



Selection Criteria

Accounting Server Host Address- Use the drop-down menu to select the IP address of the RADIUS accounting server for which to display statistics.

Non-Configurable 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.

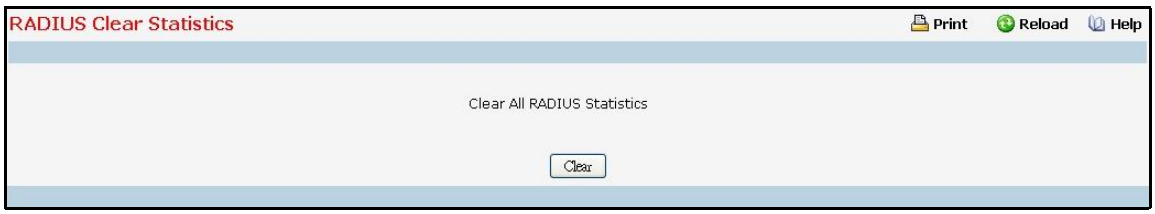
Unknown Types - Displays the number of RADIUS packets of unknown type that were received from this server on the accounting port.

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.

11.4.4.8 Resetting All RADIUS Statistics Page

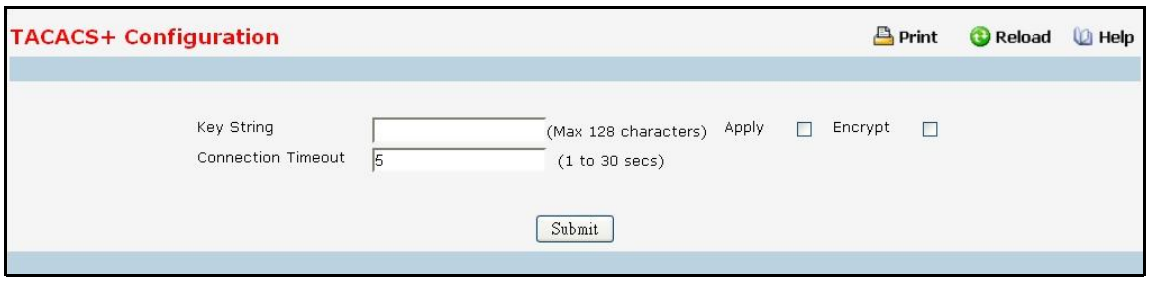


Command Buttons

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

11.4.5 Managing TACACS+ Configuration

11.4.5.1 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.

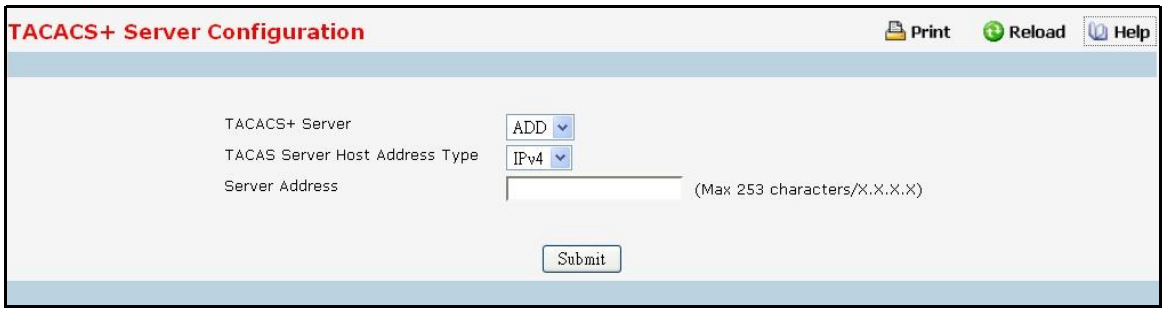
Connection Timeout - The maximum number of seconds allowed to establish a TCP connection between the device and the TACACS+ server.

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.

11.4.5.2 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

Server Address - Specifies the TACACS+ Server IP address or Hostname. Hostnames are composed of series of labels concatenated with dots. Each label must be between 1 and 63 characters long, and the entire hostname has a maximum of 253 characters.

Priority - Specifies the order in which the TACACS+ servers are used. Default value is 0. It should be within the range 0-65535.

Port - Specifies the authentication port. Default value is 49. 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. Default is blank. The key must match the encryption used on the TACACS+ server.

Apply - Allows you to enter the key in the Key String field. If the checkbox is not checked, you will not be able to enter the key. By default its unchecked.

Connection Timeout - The amount of time that passes before the connection between the device and the TACACS+ server time out. The range is (1 to 30). Default valiue is 5. Enter 0 to set it to default value.

Command Buttons

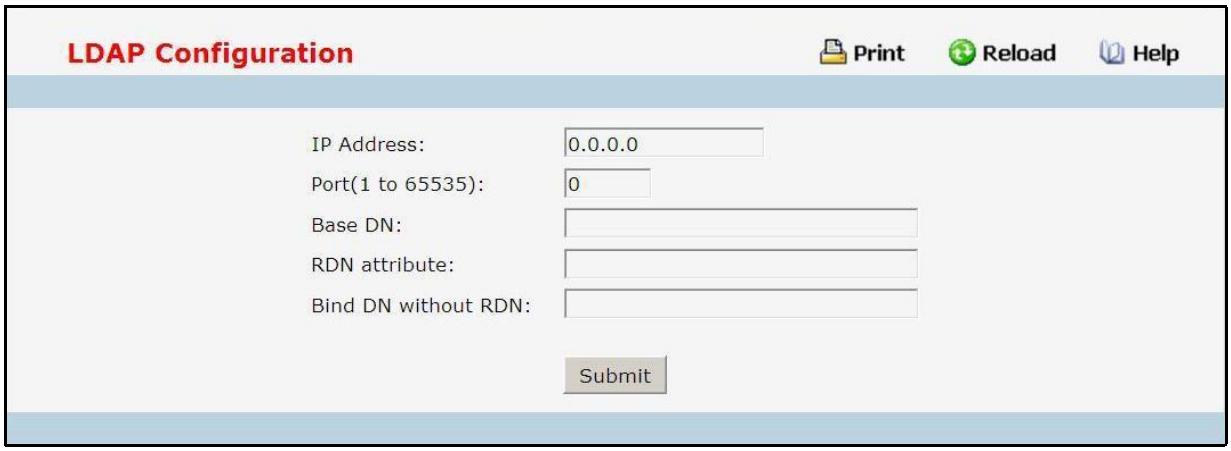
Submit - Send the updated screen to the switch and cause the changes to take effect on the switch but these changes will not be retained across a power cycle unless a save is performed.

Remove - Remove the selected server from the configuration.

11.4.6 Managing LDAP Configuration

11.4.6.1 Configuring LDAP Configuration Page

If RDN(Relative Distinguished Name) attribute is "cn"(common name), and bind DN(Distinguished Name) without RDN is "dc=test,dc=com". User name is "root", and password is "1234".Then the bind DN is "cn=root,dc=test,dc=com", and password is "1234". (OU stands for "Organization Unit". DC stands for "Domain Component".)



Configurable Data

IP Address - Specifies the LDAP server's IP address.

Port - The port number that server are listening. Default is 389.

Base DN - Base distinguished name, default is empty string.

RDN attribute - RDN attribute of bind DN, default is empty string.

Bind DN without RDN - Partial bind DN exclude RDN with it, default is empty string.

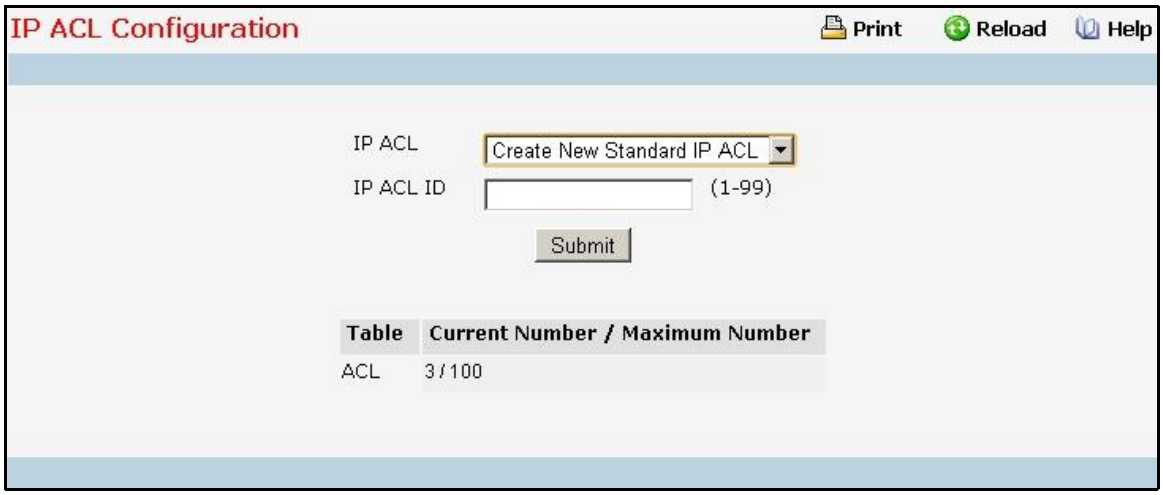
Command Buttons

Submit - Update the LDAP configuration with the values you entered. If you want the switch to retain the new values across a power cycle you must perform a save.

11.4.7 Managing Access Control Lists

11.4.7.1 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.

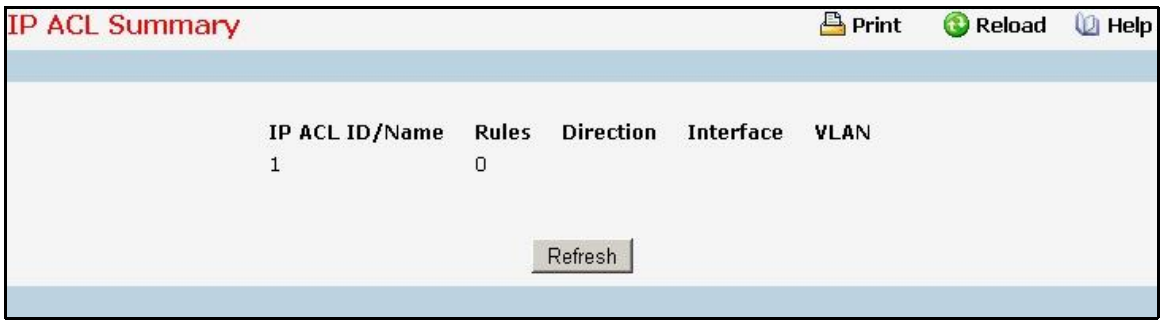
Max Size - The maximum number of IP ACLs.

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.

11.4.7.2 Viewing IP Access Control List Summary Page



Non-Configurable Data

IP ACL ID/Name - 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
- Outbound

Interface - The interfaces to which the IP ACL applies.

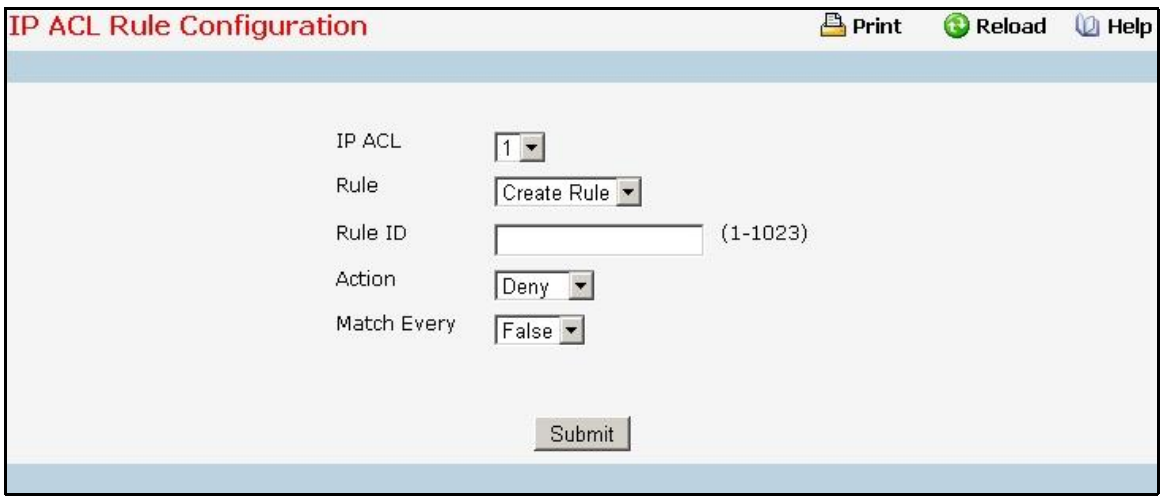
VLAN(s) - VLAN(s) to which the IP ACL applies.

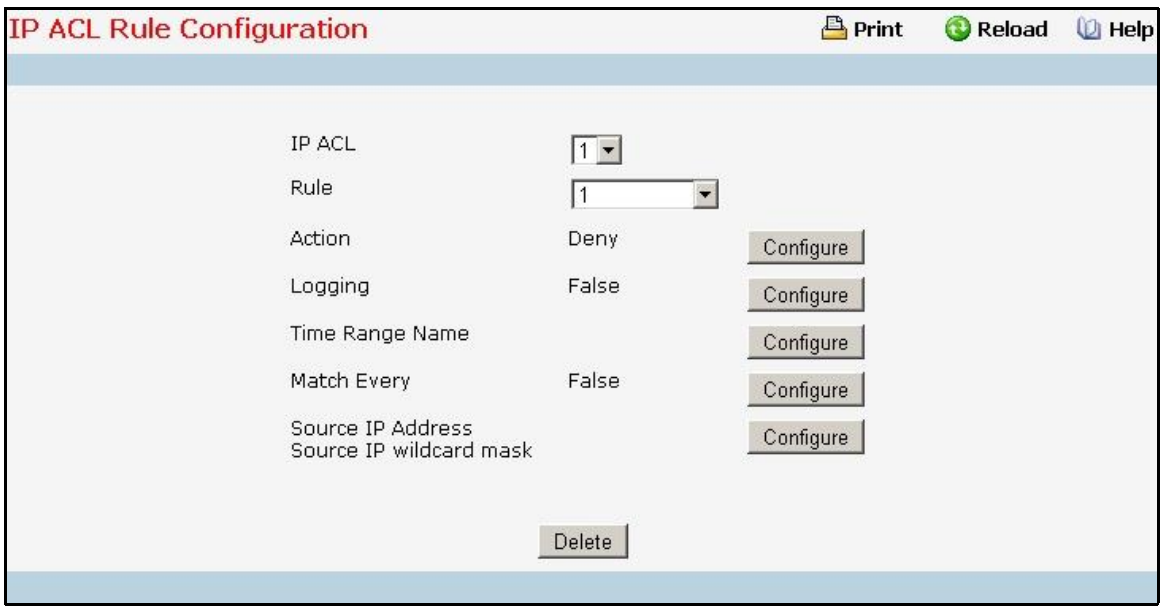
Command Buttons

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

11.4.7.3 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 - 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 255 that will be used to identify the rule. An IP ACL may have up to 255 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.

Time Range Name - Select the time range name to be associated with the IP ACL rule. On selecting the option 'other' from the list, a non-existing time range name can be specified in the "Time Range Name (other)" field.

Assign Queue ID - Specifies the hardware egress queue identifier used to handle all packets matching this IP ACL rule. Valid range of Queue Ids is (0 to 7). This field is visible when 'Permit' is chosen as 'Action'.

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.

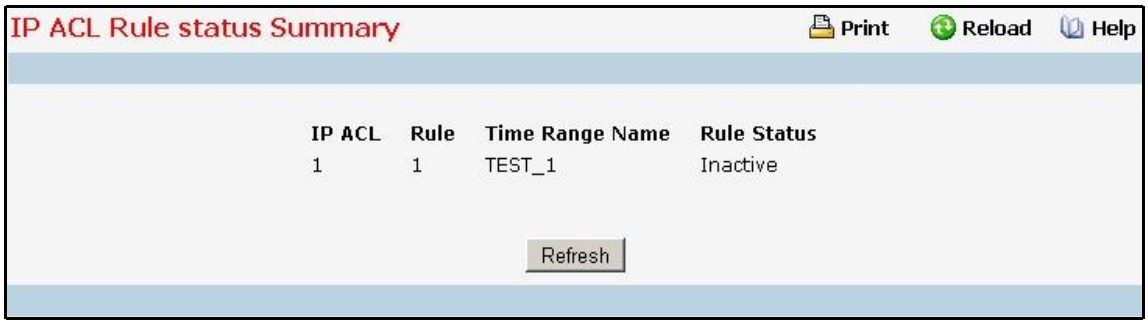
- IP DSCP Configuration Specify the IP DiffServ Code Point (DSCP) field. The DSCP is defined as the high-order six bits of the Service Type octet in the IP header. This is an optional configuration. Enter an integer from 0 to 63. The IP DSCP is selected by possibly selection one of the DSCP keyword from 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.

11.4.7.4 IP ACL Rule status Summary Page



Non-Configurable Data

IP ACL Name - IP ACL identifier.

Rule - Rule number.

Time Range Name - Indicates the name of the time range associated to the rule.

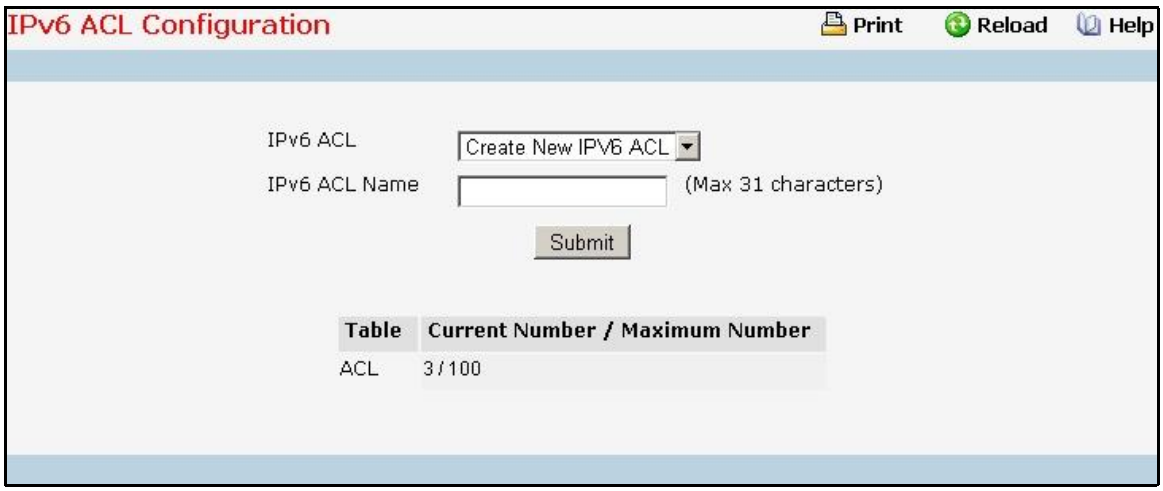
Rule Status - Indicates the status of the rule. Rule status is shown only for the rules which are time based. For non time based rules, rule status is considered to be active.

Command Buttons

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

11.4.7.5 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.

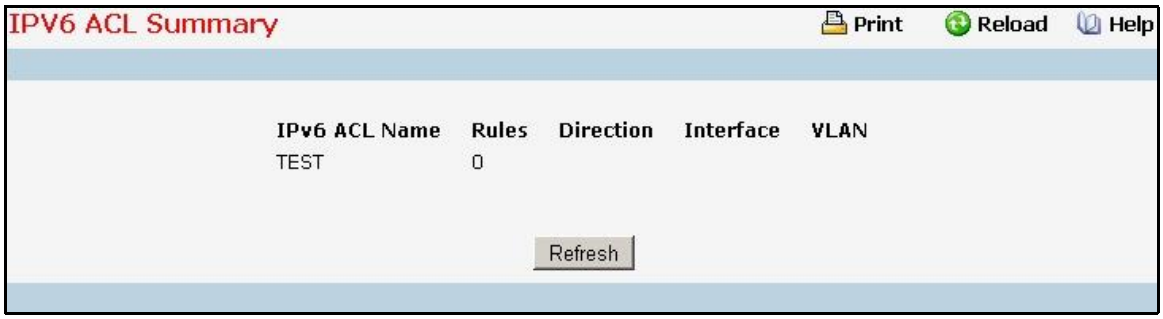
Command Buttons

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.

11.4.7.6 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
- Outbound

Interface - The interfaces to which the IPv6 ACL applies.

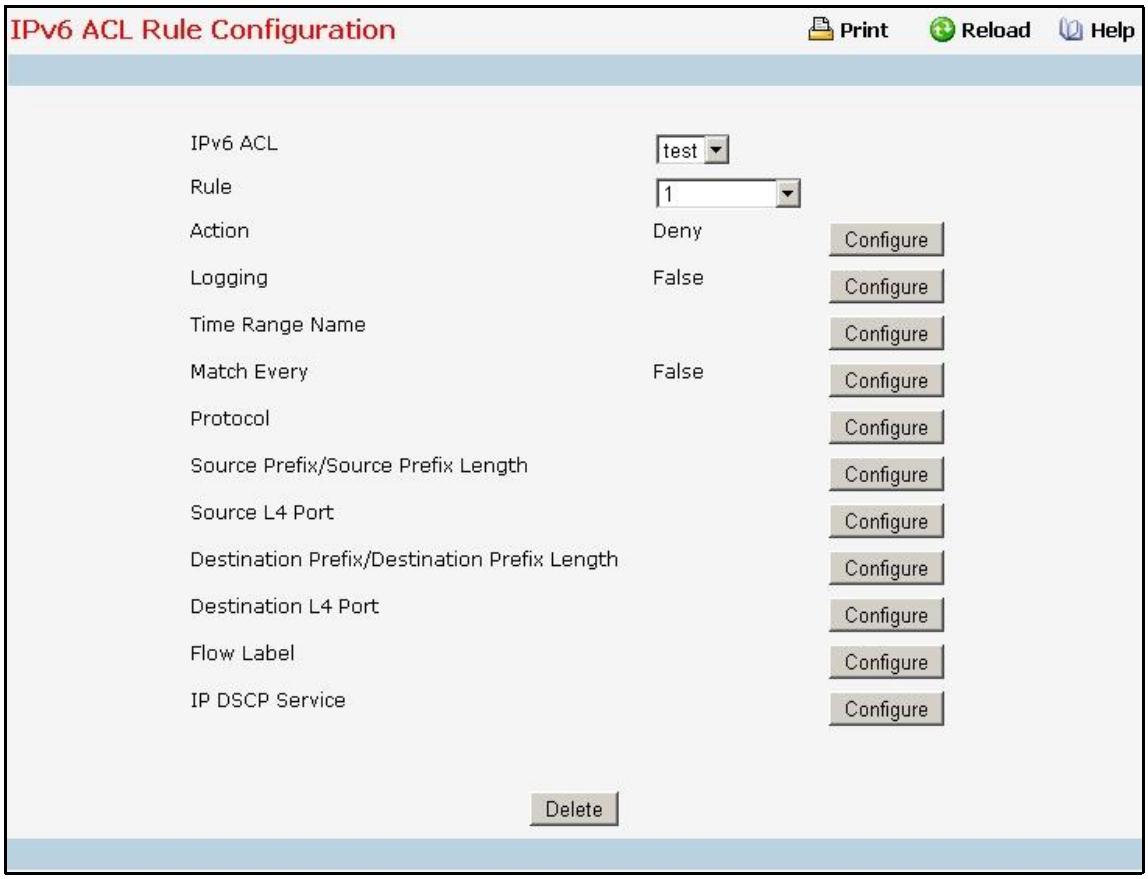
VLAN(s) - VLAN(s) to which the IPv6 ACL applies.

Command Buttons

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

11.4.7.7 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 255) 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.

Time Range Name - Select the time range name to be associated with the IPv6 ACL rule. On selecting the option 'other' from the list, a non-existing time range name can be specified in the "Time Range Name (other)" field.

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.

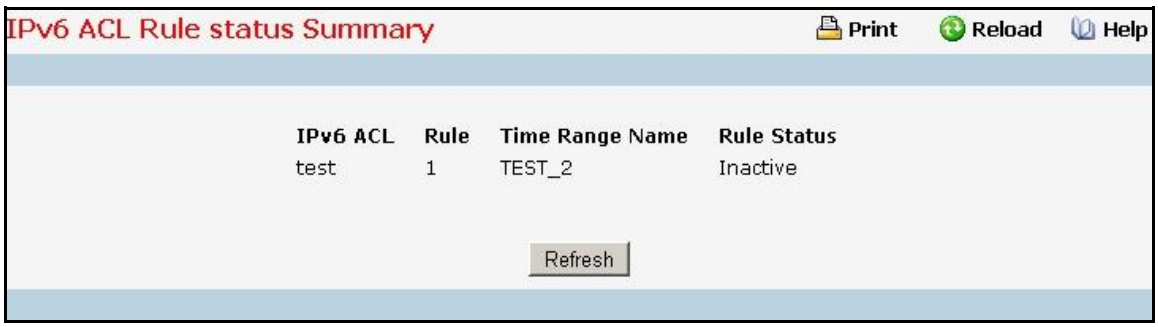
Enter an integer from 0 to 63. The IPv6 DSCP is selected by possibly selection one of the DSCP keyword from a dropdown box. If a value is to be selected by specifying its numeric value, then select the 'Other' option in the dropdown box and a text box will appear where the numeric value of the DSCP can 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.

11.4.7.8 IPv6 ACL Rule status Summary Page



Non-Configurable Data

IPv6 ACL Name - IPv6 ACL identifier.

Rule - Rule number.

Time Range Name - Indicates the name of the time range associated to the rule.

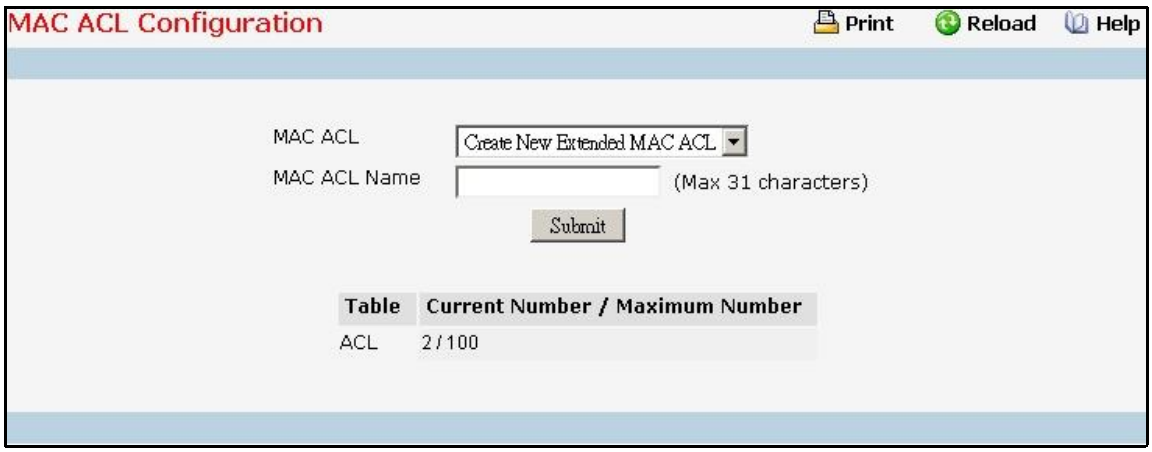
Rule Status - Indicates the status of the rule. Rule status is shown only for the rules which are time based. For non time based rules, rule status is considered to be active.

Command Buttons

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

11.4.7.9 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.

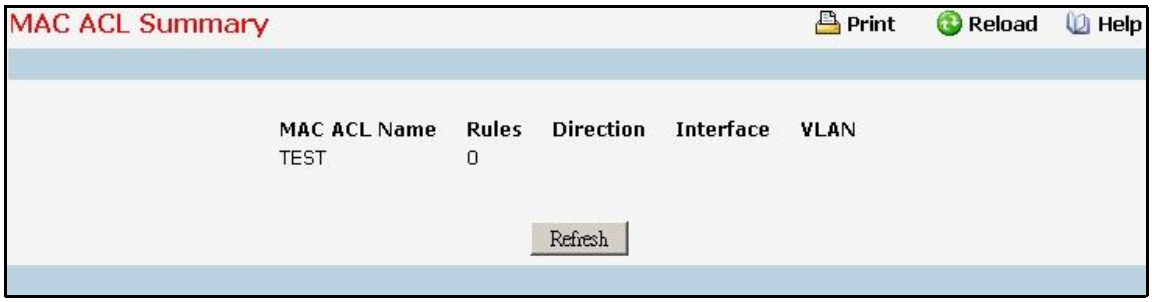
Command Buttons

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.

11.4.7.10 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
- Outbound

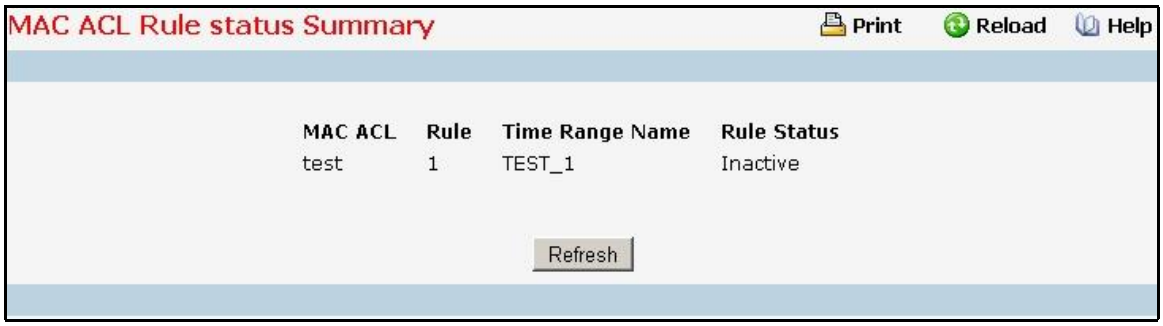
Interface - The interfaces to which the MAC ACL applies.

VLAN(s) - VLAN(s) to which the MAC ACL applies.

Command Buttons

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

11.4.7.11 MAC ACL Rule status Summary Page



Non-Configurable Data

MAC ACL Name - MAC ACL identifier.

Rule - Rule number.

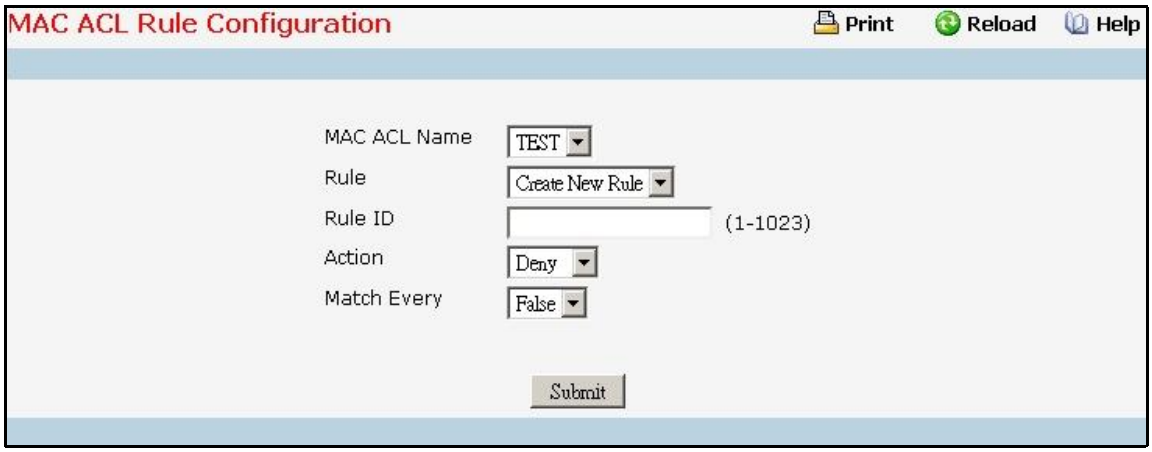
Time Range Name - Indicates the name of the time range associated to the rule.

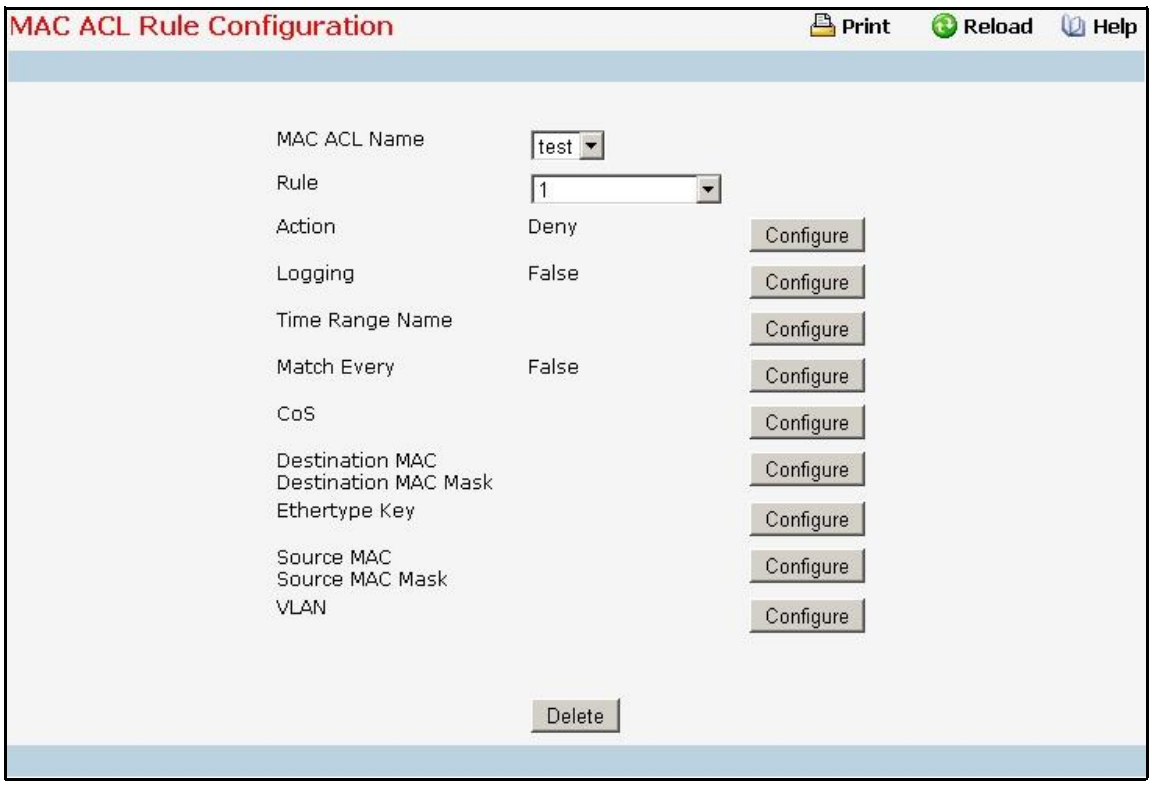
Rule Status - Indicates the status of the rule. Rule status is shown only for the rules which are time based. For non time based rules, rule status is considered to be active.

Command Buttons

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

11.4.7.12 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 255) 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.

Time Range Name - Select the time range name to be associated with the MAC ACL rule. On selecting the option 'other' from the list, a non-existing time range name can be specified in the "Time Range Name (other)" field.

Assign Queue ID - Specifies the hardware egress queue identifier used to handle all packets matching this ACL rule. Valid range of Queue Ids is (0 to 7).

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 4093). 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.

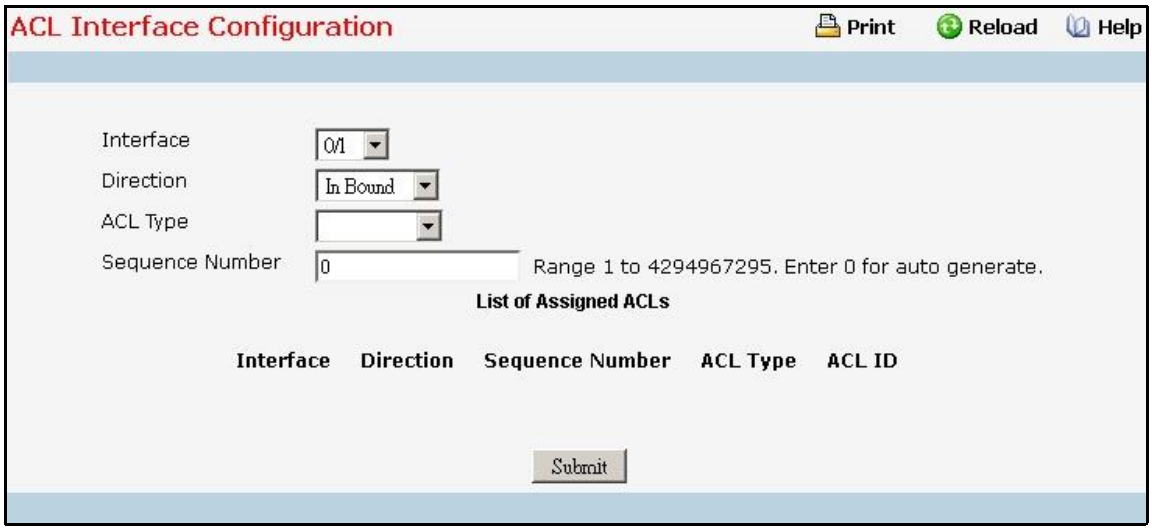
Command Buttons

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.

11.4.7.13 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
- Outbound

⚠ Outbound direction is depended on the used chipset.

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

Interface - 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.

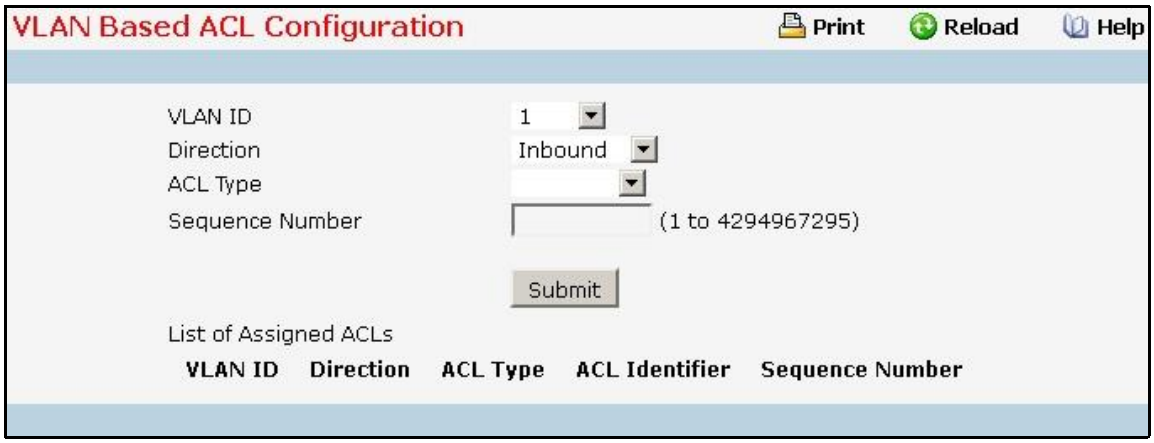
Sequence Number - Displays the Sequence Number signifying the order of specified ACL relative to other ACLs assigned to selected interface and direction.

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.

11.4.7.14 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
- Outbound

⚠ Outbound direction is depended on the used chipset.

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.

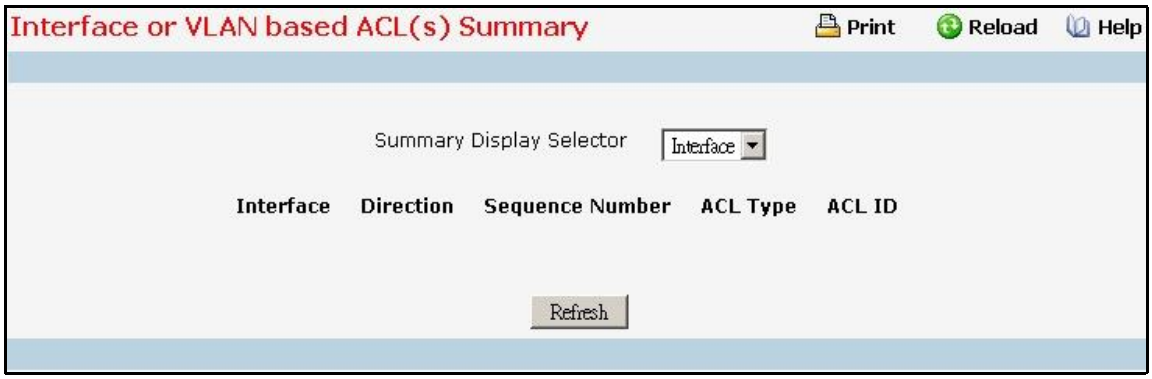
Sequence Number - Displays the Sequence Number signifying the order of specified ACL relative to other ACLs assigned to selected VLAN and direction.

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.

11.4.7.15 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.

Interface - 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
- Outbound

ACL Type - Displays the type of ACL assigned to selected VLAN and direction.

ACL ID - 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.

11.4.8 Managing IP Filter Configuration

11.4.8.1 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.

Configurable Data

Admin Mode - Selects the IP Filter admin mode for enable or disable.

IP Filter - You can use this screen to reconfigure an existing IP Filter, or to create a new one. Use this pulldown menu to select one of the existing IP Filter Names, or select 'Create' to add a new one.

Protocol - Select IPv4 or IPv6 to configure the corresponding attributes.IP Filter Name - The IP Filter Name, it identifies each IP Filter. IP Filter name in the IP Filter must be unique. A valid entry is a case-sensitive string of up to 64 characters.

Client IP Address - Taken together, the Client IP Address and Client IP Mask denote a range of IP addresses from which clients may access this device. 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 clients may use access this device. 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.

Prefix/Prefix Length - The combination of IPv6 Prefix and IPv6 Prefix length denote a range of IP Addresses from which clients may access this device.

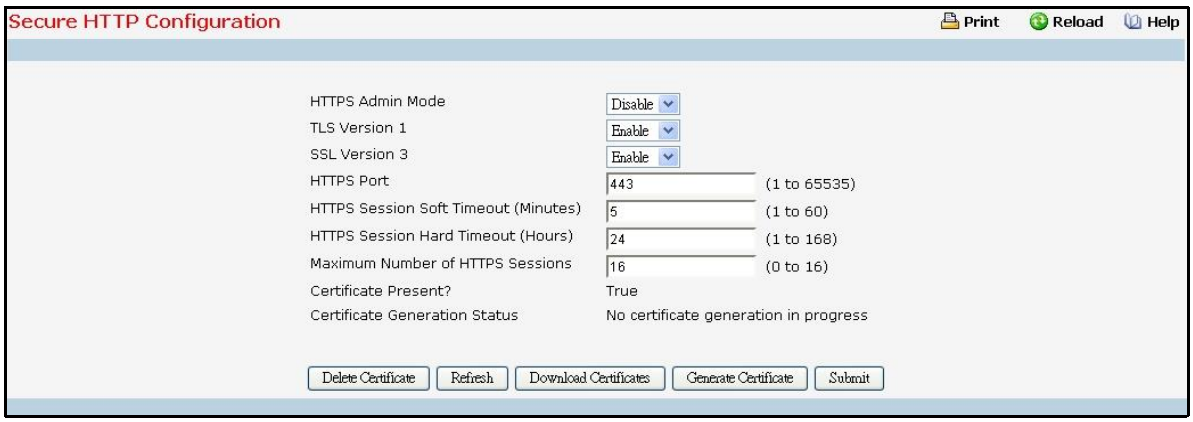
Command Buttons

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.

Delete - Delete the currently selected IP Filter Name. If you want the switch to retain the new values across a power cycle, you must perform a save.

11.4.9 Managing Secure HTTP Configuration

11.4.9.1 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.

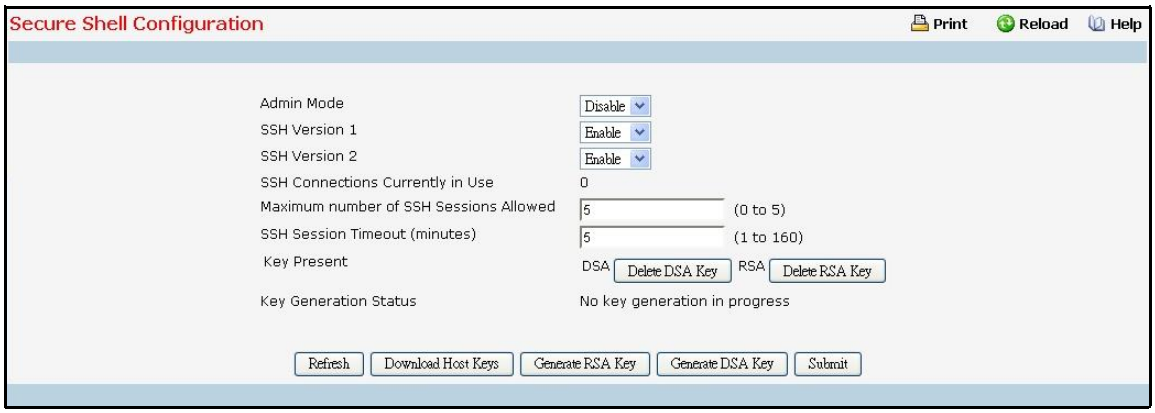
Generate Certificate - Begin generating the Certificate. Note that to generate SSL Certificate files SSL must be administratively disabled.

Delete Certificate - Used to delete the corresponding certificate, if it is present.

Refresh - Use to refresh page.

11.4.10 Managing Secure Shell Configuration

11.4.10.1 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.

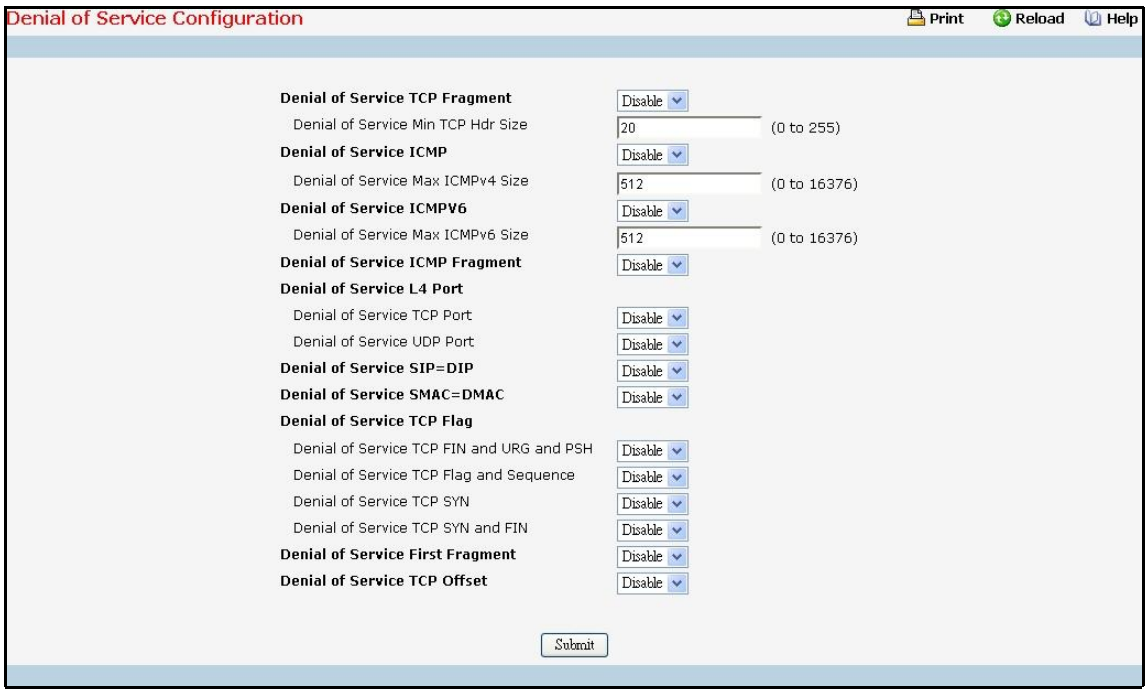
Generate RSA Host Keys - Begin generating the RSA host keys. Note that to generate SSH key files SSH must be administratively disabled and there can be no active SSH sessions.

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.

Refresh - Use to refresh page.

11.4.11 Managing Denial of Service Page



Selection Criteria

Denial of Service TCP Fragment - Enable or disable this option by selecting the corresponding line on the pull-down entry field. Enabling TCP Fragment DoS prevention causes the switch to drop packets that have a TCP header smaller than the configured Min TCP Hdr Size. The factory default is disabled.

Denial of Service ICMP - Enable or disable this option by selecting the corresponding line on the pull-down entry field. Enabling ICMP DoS prevention causes the switch to drop ICMP packets that have a type set to ECHO_REQ (ping) and a payload size greater than the configured ICMP payload Size. The factory default is disabled.

Denial of Service ICMPv6 - Enable or disable this option by selecting the corresponding line on the pull-down entry field. Enabling ICMPv6 DoS prevention causes the switch to drop ICMP v6 packets that have a type set to ECHO_REQ (ping) and a size payload greater than the configured ICMPv6 payload Size. The factory default is disabled.

Denial of Service ICMP Fragment - Enable or disable this option by selecting the corresponding line on the pull-down entry field. Enabling ICMP Fragment DoS prevention causes the switch to drop ICMP Fragmented packets. The factory default is disabled.

Denial of Service TCP Port - Enable or disable this option by selecting the corresponding line on the pull-down 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.

Denial of Service UDP Port - Enable or disable this option by selecting the corresponding line on the pull-down 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.

Denial of Service SIP=DIP - Enable or disable this option by selecting the corresponding line on the pull-down 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.

Denial of Service SMAC=DMAC - Enable or disable this option by selecting the corresponding line on the pull-down 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.

Denial of Service TCP FIN&URG&PSH - Enable or disable this option by selecting the corresponding line on the pull-down 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.

Denial of Service TCP Flag & Sequence - Enable or disable this option by selecting the corresponding line on the pull-down 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.

Denial of Service TCP SYN - Enable or disable this option by selecting the corresponding line on the pull-down entry field. Enabling TCP SYN DoS prevention causes the switch to drop packets that have TCP Flags SYN set. The factory default is disabled.

Denial of Service TCP SYN&FIN - Enable or disable this option by selecting the corresponding line on the pull-down 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.

Denial of Service First Fragment - Enable or disable this option by selecting the corresponding line on the pull-down entry field. Enabling First Fragment DoS prevention causes the switch to drop packets that have a more fragment equal to 1 and cooperate with other DoS options. The factory default is disabled.

Denial of Service TCP Offset - Enable or disable this option by selecting the corresponding line on the pull-down 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

Denial of Service 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.

Denial of Service Max ICMPv4 Payload Size - Specify the Max ICMPv4 Payload Size allowed. If ICMP DoS prevention is enabled, the switch will drop IPv4 ICMP ping packets that have a payload size greater than this configured Max ICMP Payload Size. The factory default value is 512.

Denial of Service Max ICMPv6 Pkt Size - Specify the Max IPv6 ICMP Payload Size allowed. If ICMP DoS prevention is enabled, the switch will drop IPv6 ICMP ping packets that have a payload size greater than this configured Max ICMP Payload 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.

11.5 QOS Menu

11.5.1 Managing Differentiated Services

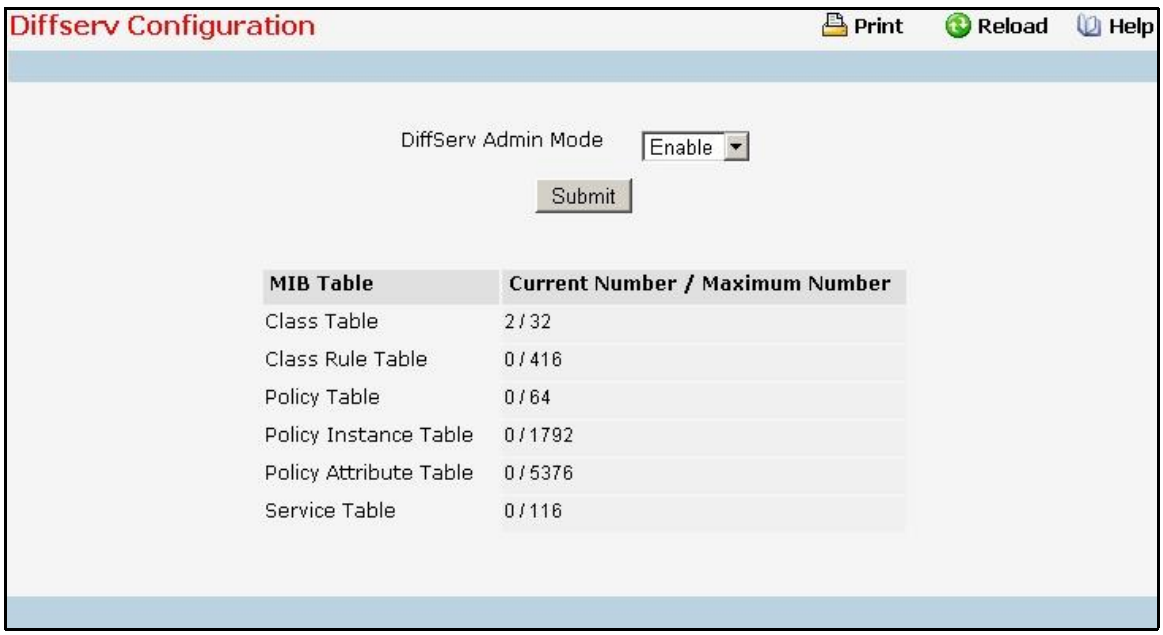
11.5.1.1 Defining DiffServ Configuration Page

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.

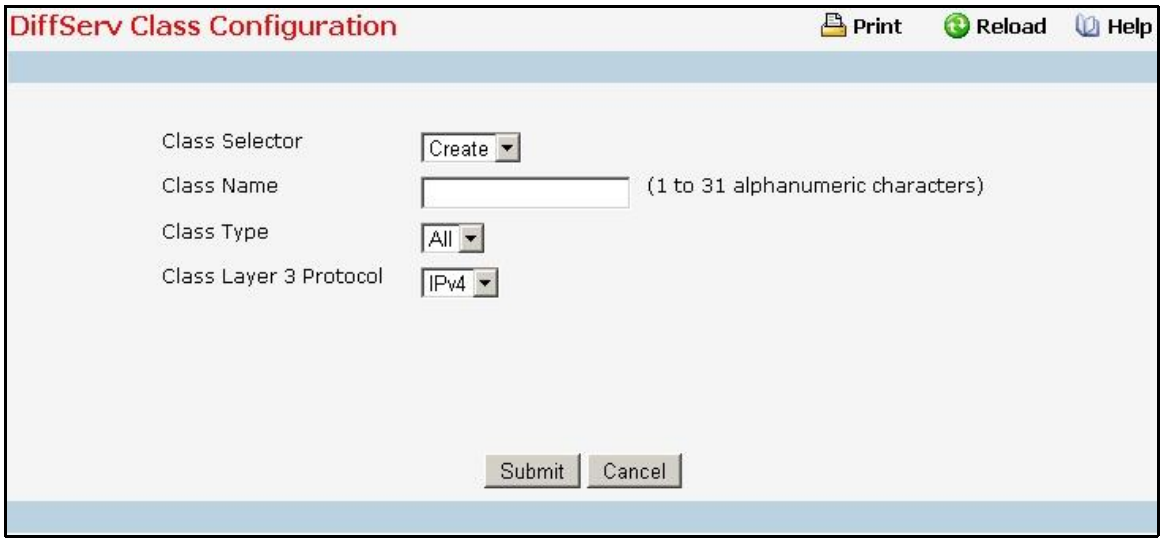
Policy Attributes table - Displays the number of configured policy attributes (attached to the policy class instances) out of the total allowed on the switch.

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.

11.5.1.2 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.

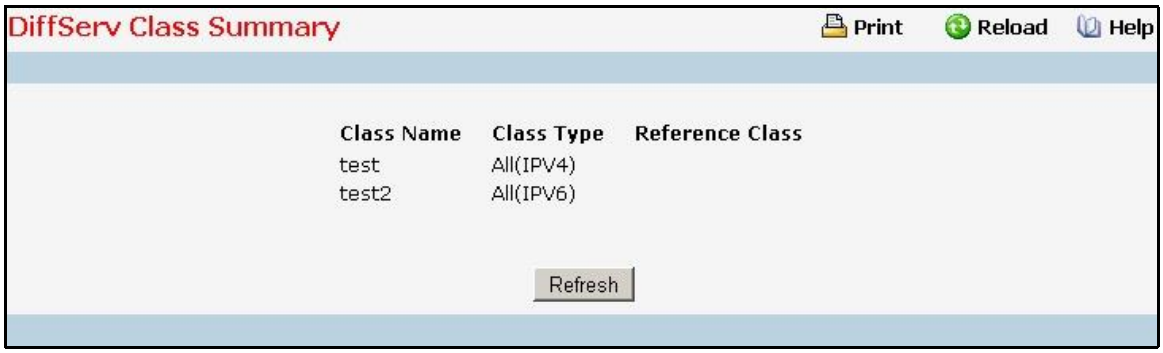
Rename - Allows to rename a specified class.

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.

11.5.1.3 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 with the layer 3 protocol of the class. Class types are platform dependent.

Reference Class - Displays name of the configured class of type

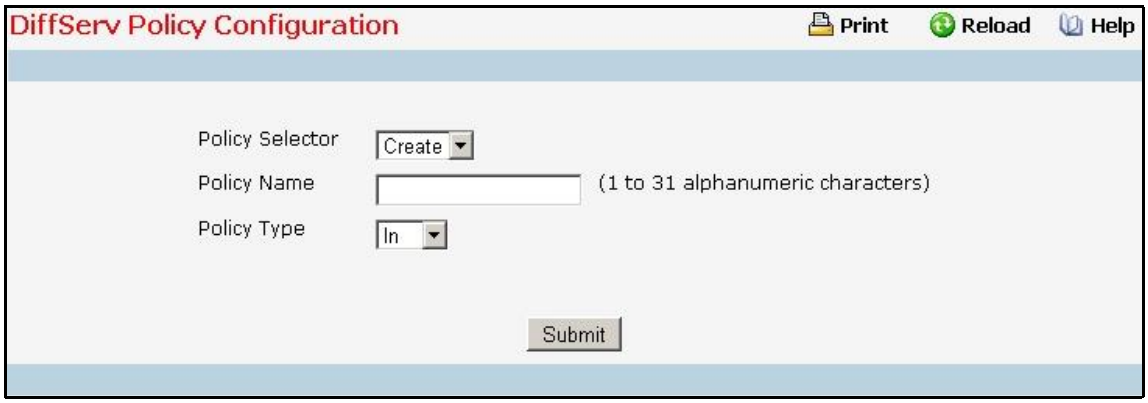
- All

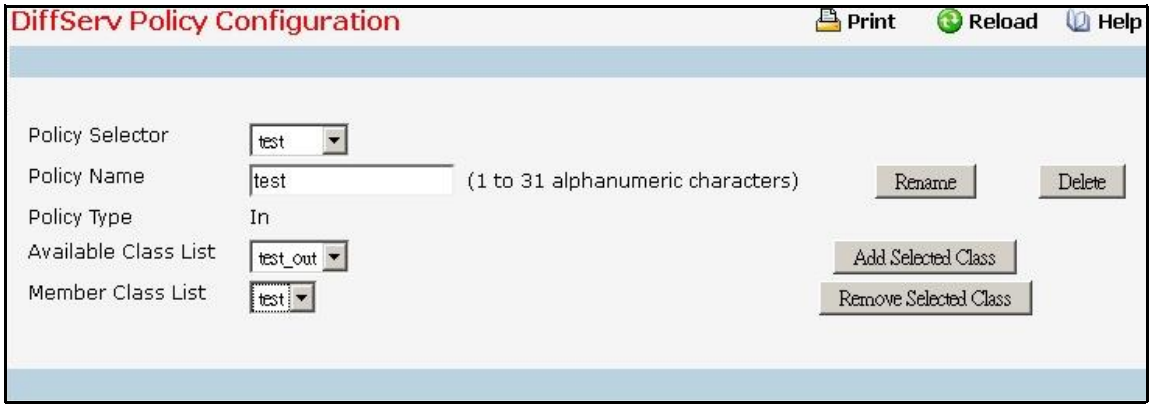
referenced by the specified class of the same type.

Command Buttons

Refresh - Refresh the currently selected filter.

11.5.1.4 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. Out indicates the type is specific to outbound traffic direction. Only when a new policy is created, this field is a selector field. After policy creation this becomes a non-configurable field displaying the configured policy type.

Available Class List - This lists all existing DiffServ class names, from which one can be selected. This field is a selector field only when a new policy class instance is to be created. After creation of the policy class instance this becomes a non-configurable field.

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

Configurable Data

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

Non-Configurable Data

Policy Type - In indicates the type is specific to inbound traffic direction. Out indicates the type is specific to outbound traffic direction. Only when a new policy is created, this field is a selector field. After policy creation this becomes a non-configurable field displaying the configured policy type.

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.

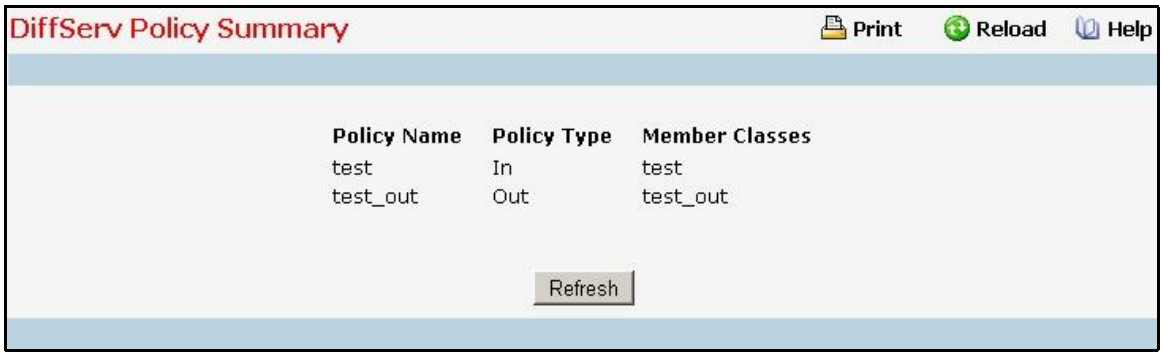
Delete - Delete the currently selected filter.

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.

11.5.1.5 Viewing DiffServ Policy Summary Page



Non-Configurable Data

Policy Name - Displays name of the DiffServ policy.

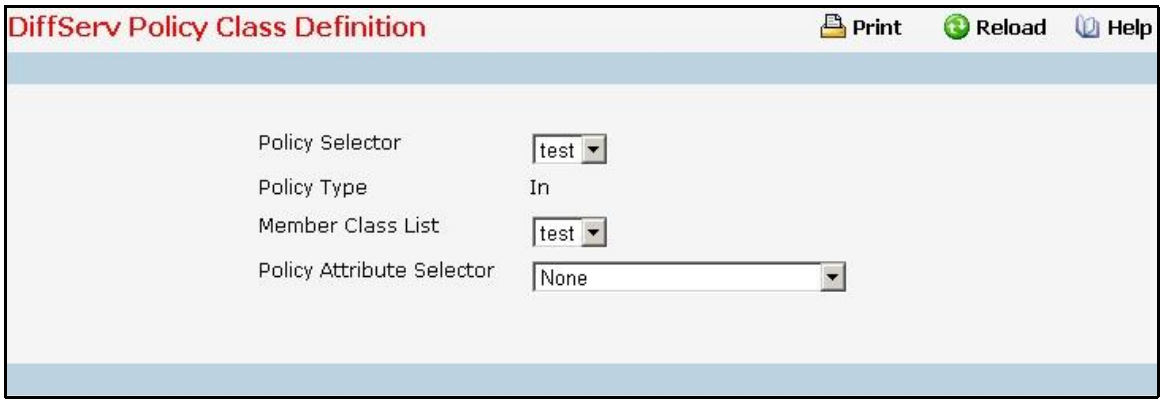
Policy Type - Displays type of the policy as 'In' or 'Out'.

Member Classes - Displays name of each class instance within the policy.

Command Buttons

Refresh - Refresh the currently selected filter.

11.5.1.6 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.

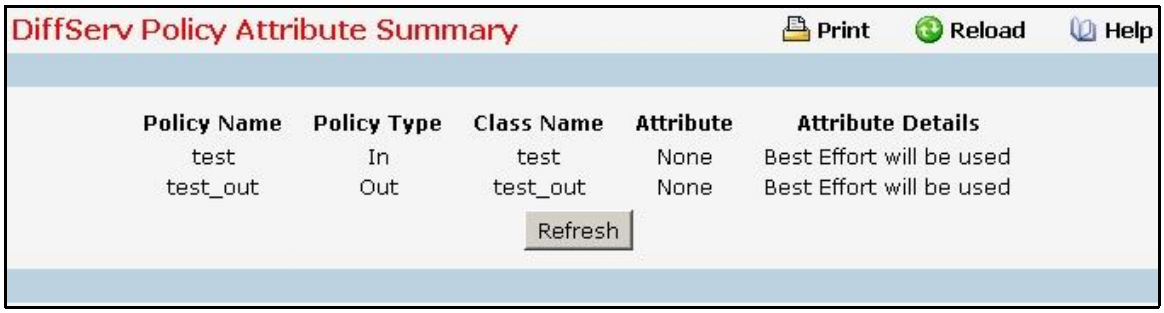
Non-Configurable Data

Policy Type - Displays type of the configured policy.

Command Buttons

Configure Selected Attribute - Only one configuration criterion can be specified per invocation of this button. Based on the selected configuration criterion, an individual configuration screen is provided.

11.5.1.7 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' or 'Out'.

Class Name - Displays name of the DiffServ class to which this policy is attached.

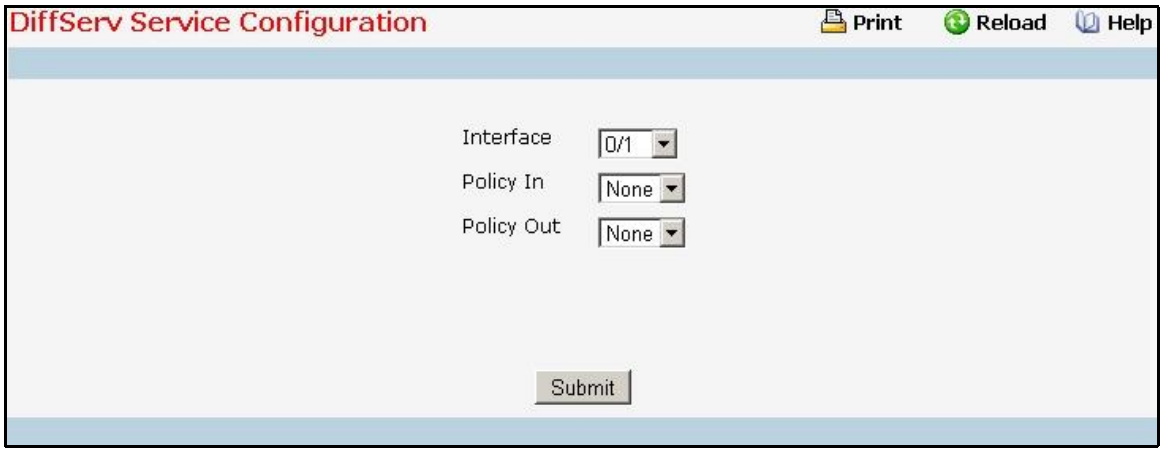
Attribute - Displays the attributes attached to the policy class instances.

Attribute Details - Displays the configured values of the attached attributes.

Command Buttons

Refresh - Refresh the displayed data.

11.5.1.8 Configuring DiffServ Service Configuration Page



Selection Criteria

Interface - 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.

Policy Out - This lists all the policy names of type 'Out' from which one can be selected. If 'none' is selected, this will detach the policy from the interface in this direction. This field is not shown for Read/Write users where outbound service policy attachment is not supported by the platform.

Non-Configurable Data

This information is only displayed when Slot/Port is specified as 'All'.

Interface - Shows the Slot/Port that uniquely specifies an interface.

Direction - Shows that the traffic direction of this service interface is In.

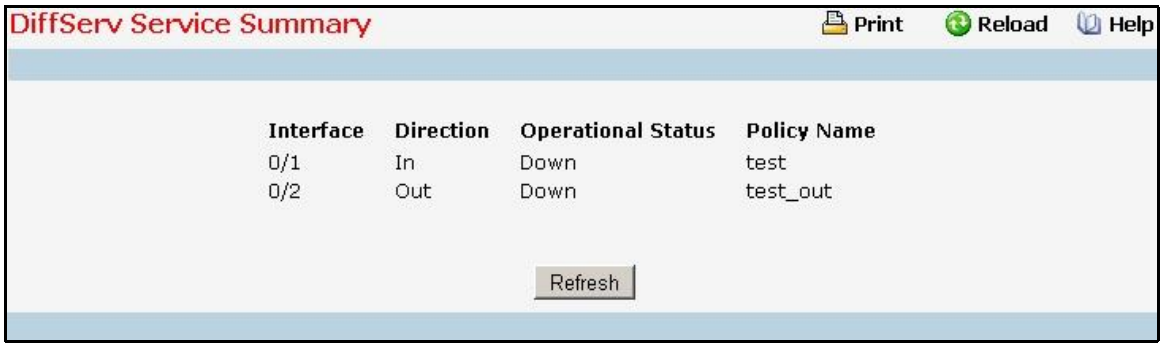
Operational Status - Shows the operational status of this service interface, either Up or Down.

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.

11.5.1.9 Viewing DiffServ Service Summary Page



Non-Configurable Data

Slot/Port - Shows the Slot/Port that uniquely specifies an interface.

Direction - Shows traffic direction for this service interface.

Operational Status - Shows the operational status of this service interface, either Up or Down.

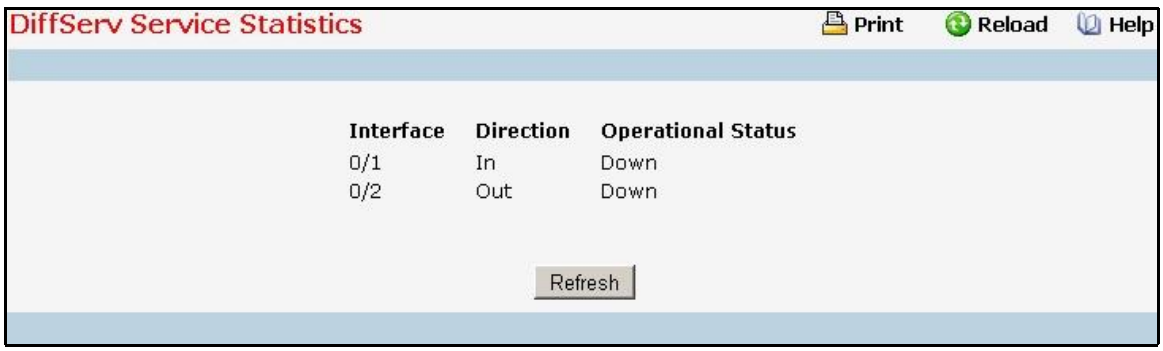
Policy Name - Shows the name of the attached policy.

Command Buttons

Refresh - Refresh the displayed data.

11.5.1.10 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

Interface - Shows the Slot/Port that uniquely specifies an interface.

Direction - Shows traffic direction for this service interface.

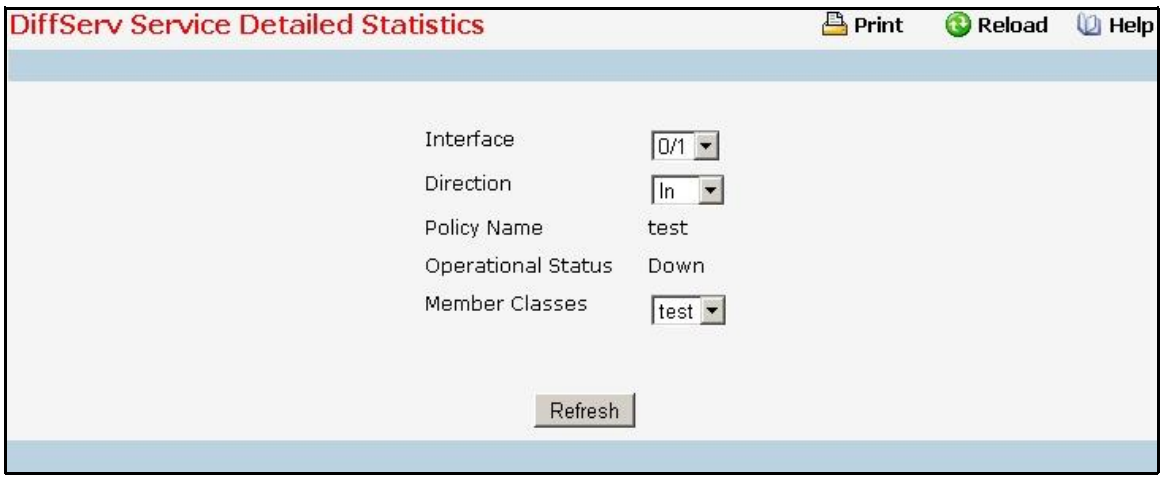
Operational Status - Shows the operational status of this service interface, either Up or Down.

Command Buttons

Refresh - Refresh the displayed data.

11.5.1.11 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.

11.5.2 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.

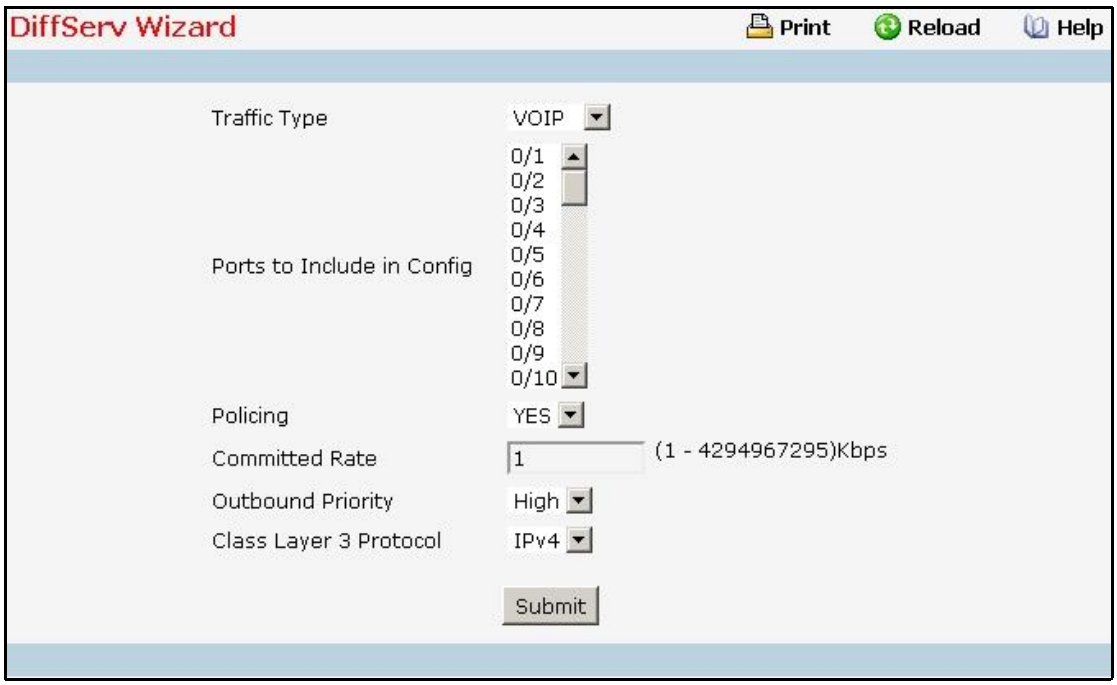
If Policing is set to NO, then all traffic will be marked as specified below:

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.

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

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.

11.5.3 Managing Auto VoIP

Voice over Internet Protocol (VoIP) allows you to make telephone calls using a computer network over a data network like the Internet. With the increased prominence of delay-sensitive applications (voice, video, and other multimedia applications) deployed in networks today, proper QoS configuration will ensure high-quality application performance. The Auto VoIP feature is intended to provide an easy classification mechanism for voice packets so that they can be prioritized above data packets in order to provide better QoS.

The Auto-VoIP feature explicitly matches VoIP streams in Ethernet switches and provides them with a better class of service than ordinary traffic. If you enable the Auto-VoIP feature on an interface, the interface scans incoming traffic for the following call-control protocols:

- Session Initiation Protocol (SIP)
- H.323
- Skinny Client Control Protocol (SCCP)

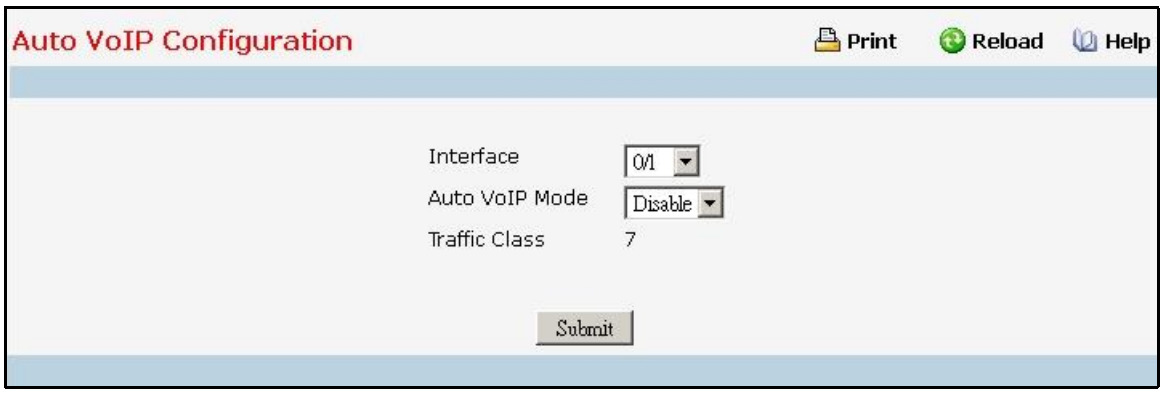
When a call-control protocol is detected the switch assigns the traffic in that session to the highest CoS queue, which is generally used for time-sensitive traffic.

The Auto VoIP folder contains links to the following features:

- “Auto VoIP Configuration”
- “Auto VoIP Summary”

11.5.3.1 Configuring Auto VoIP Configuration Page

Use the Auto VoIP Configuration page to configure the Auto VoIP settings.



Selection Criteria

Interface - Specifies all Auto VoIP configurable interfaces. The option "All" represents the most recent configuration settings done for All Ports. These may be overridden on a per-interface basis.

Configurable Data

Auto VoIP Mode - It is used to enable or disable the Auto VoIP mode.

Auto VoIP Mode can only be one of the following:

- Enable
- Disable

Default value is Disabled.

Non-Configurable Data

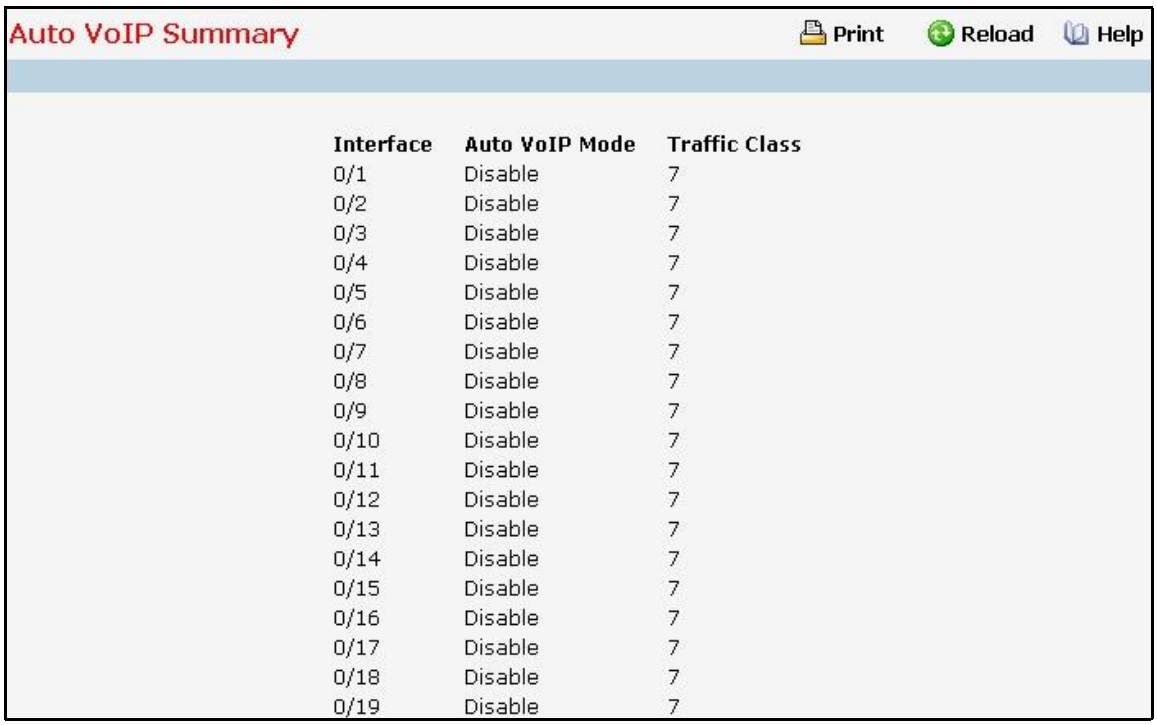
Traffic Class - It displays the Traffic Class used for VoIP traffic.

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.

11.5.3.2 Viewing Auto VoIP Summary Page

Use the Auto VoIP Summary page to display the Auto VoIP settings.



Interface	Auto VoIP Mode	Traffic Class
0/1	Disable	7
0/2	Disable	7
0/3	Disable	7
0/4	Disable	7
0/5	Disable	7
0/6	Disable	7
0/7	Disable	7
0/8	Disable	7
0/9	Disable	7
0/10	Disable	7
0/11	Disable	7
0/12	Disable	7
0/13	Disable	7
0/14	Disable	7
0/15	Disable	7
0/16	Disable	7
0/17	Disable	7
0/18	Disable	7
0/19	Disable	7

Non-Configurable Data

Interface - Specifies the port whose settings are displayed in the current table row.

Auto VoIP Mode - Displays whether the mode is enabled or disabled.

Traffic Class - It displays the Traffic Class used for VoIP traffic.

Command Buttons

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

11.5.4 Managing iSCSI

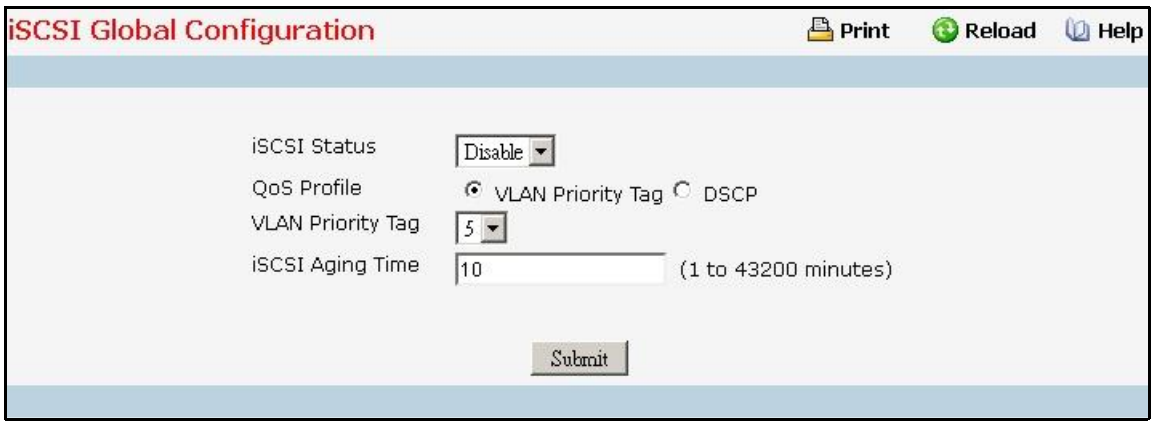
iSCSI Optimization provides a means of giving traffic between iSCSI initiator and target systems special Quality of Service (QoS) treatment. This is accomplished by monitoring traffic to detect packets used by iSCSI stations to establish iSCSI sessions and connections. Data from these exchanges is used to create classification rules that assign the traffic between the stations to a configured traffic class. Packets in the flow are queued and scheduled for egress on the destination port based on these rules.

The iSCSI Optimization folder contains links to the following web pages:

- ”iSCSI Global Configuration”
- ”iSCSI Targets Table”
- ”iSCSI Sessions”
- ”iSCSI Sessions Detailed”

11.5.4.1 Configuring iSCSI Global Configuration Page

Use the iSCSI Optimization-Global Parameters page to configure iSCSI Optimization on the switch.



Selection Criteria

iSCSI Status - Use to either Enable or Disable iSCSI Optimization. The default is Disable.

QoS Profile - Select the quality of service profile that will be applied to iSCSI flows.

- VLAN Priority Tag
- DSCP

By default, iSCSI flows are assigned to the highest VPT/DSCP mapped to the highest queue not used for stack management or voice VLAN. Be sure to configure the relevant Class of Service parameters for the queue in order to complete the setting.

DSCP - If using DSCP, assign a DSCP value to iSCSI session packets

VLAN Priority Tag - If using VLAN Priority Tag, assign a VLAN Priority Tag value to iSCSI session packets

Remark - Use to either Enable or Disable the Remark mode. The default is Disable. Enabling Remark allows the packets to be updated with IP-DSCP values. Remarking packets with priority data provides special QoS treatment as the packets continue through the network

Configurable Data

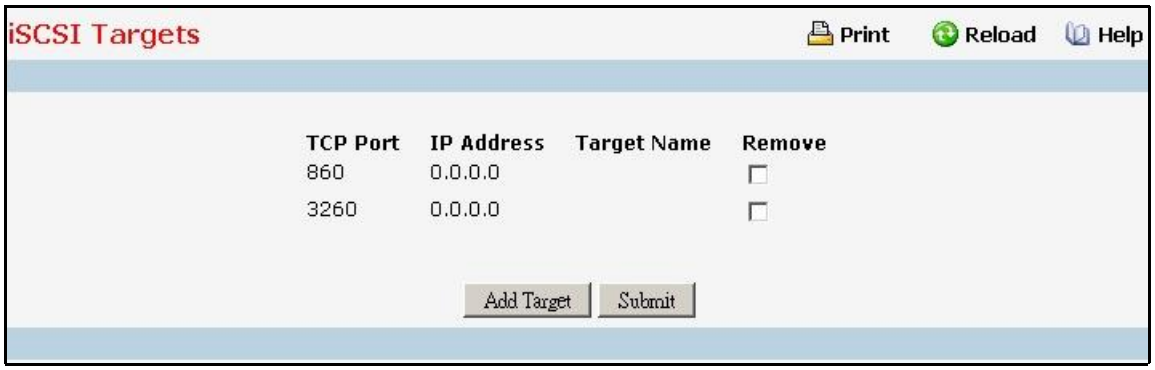
iSCSI Aging Time - Set the number of minutes a session can be inactive prior to removal.

Command Buttons

Submit - Send the updated configuration to the switch.

11.5.4.2 Configuring iSCSI Targets Page

Use the iSCSI Targets Table page to assign target ports/port IP address combinations for iSCSI Optimization on the switch.



Non-Configurable Data

TCP Port - Shows the TCP port numbers for the targets monitoring iSCSI traffic. The well-known iSCSI ports 3260 and 860 are configured as the default ports. The default ports can be removed. Up to 16 TCP ports can be defined in the system

IP Address - Shows the IP address of the iSCSI target.

Target Name - Shows the name assigned to the Target.

Remove - Select the checkbox associated with a target and click the Submit button to remove a target.

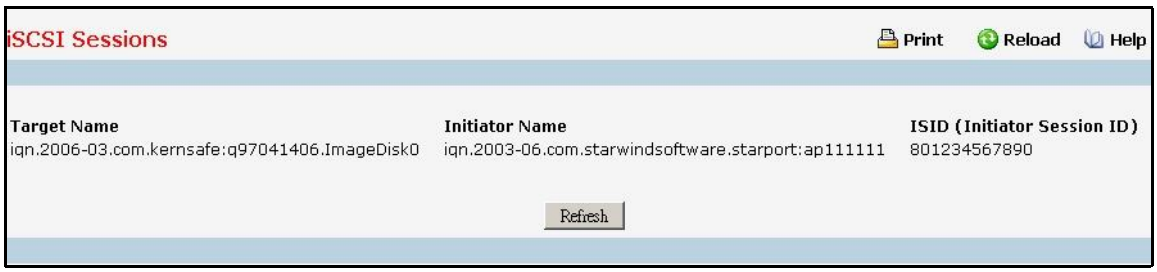
Command Buttons

Add Target - Click the Add Target button to add an new iSCSI target

Submit - Send the updated configuration to the switch.

11.5.4.3 Viewing iSCSI Sessions Page

Use the iSCSI Sessions page to view iSCSI sessions.



Non-Configurable Data

Target Name - Shows the name assigned to the target.

Initiator Name - Shows the name of the initiator.

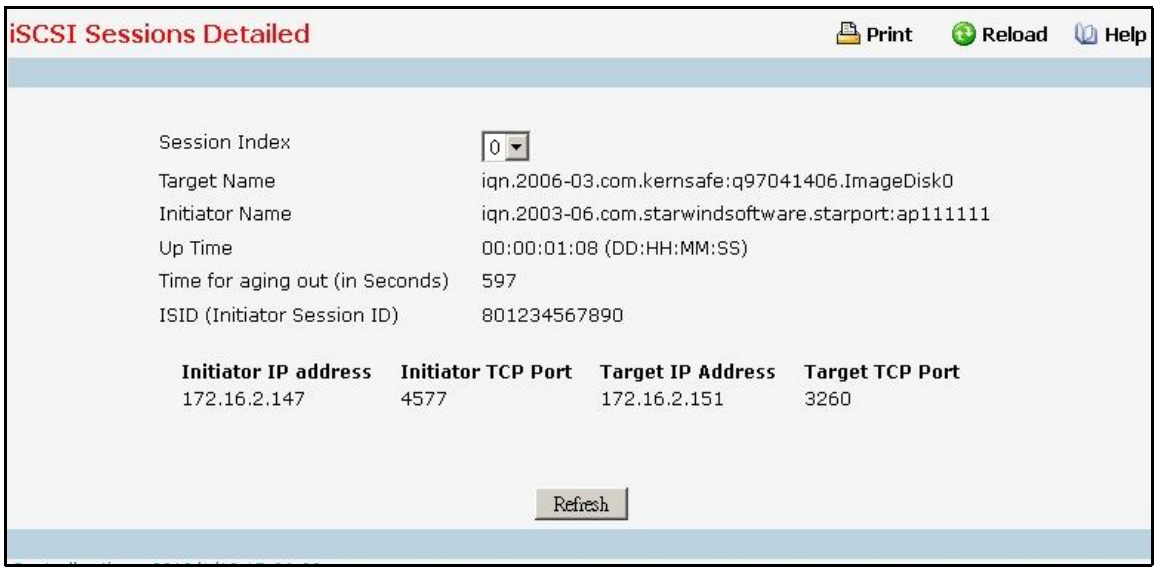
ISID (Initiator Session ID) - Shows the unique indentifier an initiator assigns to the session endpoint. When it is combined with the iSCSI initiator name, it provides a unique name in the world for the SCSI initiator port.

Command Buttons

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

11.5.4.4 Viewing iSCSI Sessions Detailed Page

Use the iSCSI Sessions Detailed page to view detailed information on iSCSI sessions.



Non-Configurable Data

Target Name - Shows the name assigned to the target.

Initiator Name - Shows the name of the initiator.

Up Time - Show the time that has elapsed since the session was created.

Time for aging out (in Seconds) - Show the time (in seconds) left before the session is set to expire.

ISID (Initiator Session ID) - Shows the unique indentifier an initiator assigns to the session endpoint. When it is combined with the iSCSI initiator name, it provides a unique name in the world for the SCSI initiator port.

Initiator IP Address - Shows the Initiator IP Address.

Initiator TCP Port - Shows the Initiator TCP Port number of one of the connections between the Target and initiator.

Target IP Address - Shows the IP Address of the Target.

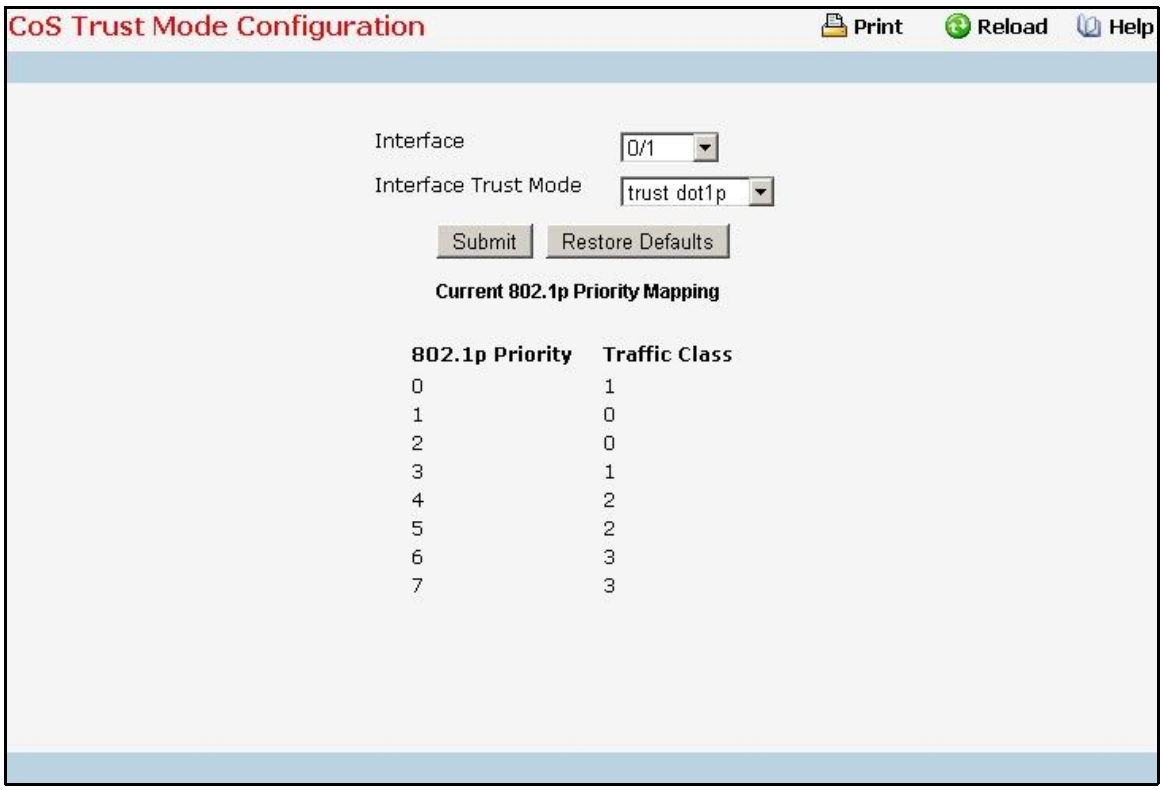
Target TCP Port - Shows the Target TCP Port number of one of the connections between the Target and Initiator.

Command Buttons

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

11.5.5 Managing Class of Service

11.5.5.1 Configuring Trust Mode Configuration Page



Selection Criteria

Interface - 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).

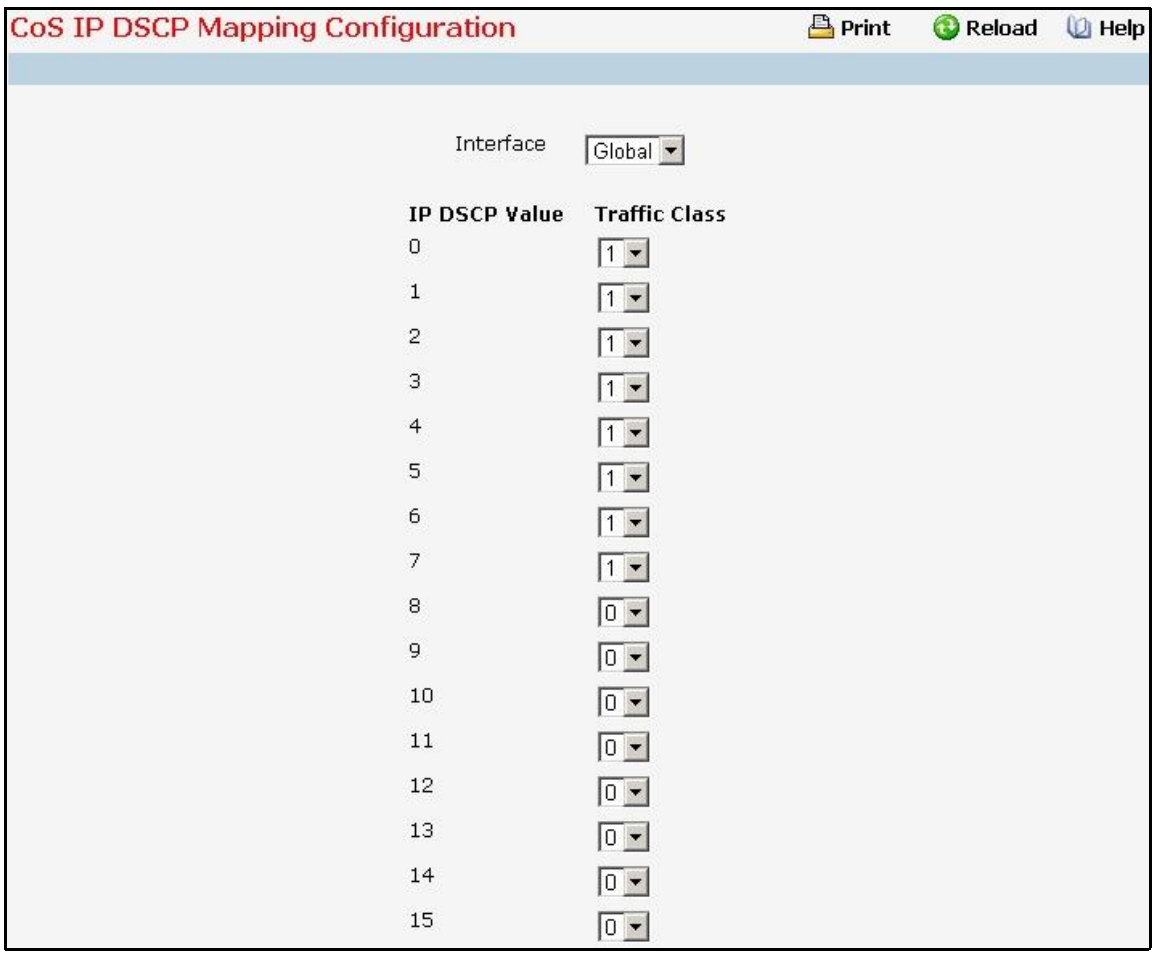
Current 802.1p Priority Mapping - Displays the current 802.1p priority mapping configuration.

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.

11.5.5.2 Managing DSCP Mapping Configuration Page



Selection Criteria

Interface - 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

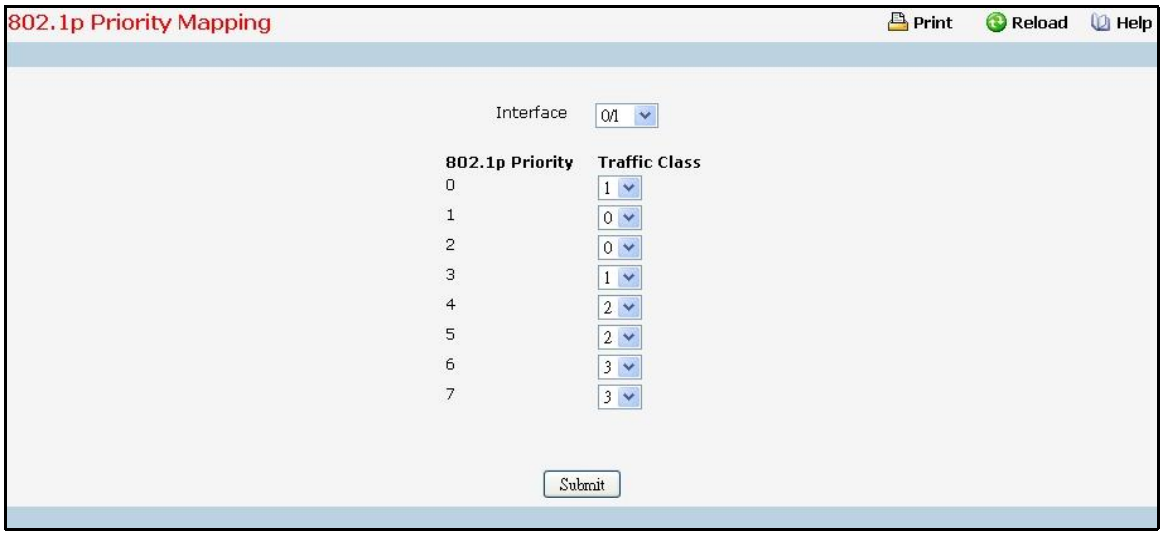
IP DSCP Value - Specify the IP DiffServ Code Point (DSCP) Value.

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.

11.5.5.3 Defining 802.1p Priority Mapping Page



Selection Criteria

Interface - 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.

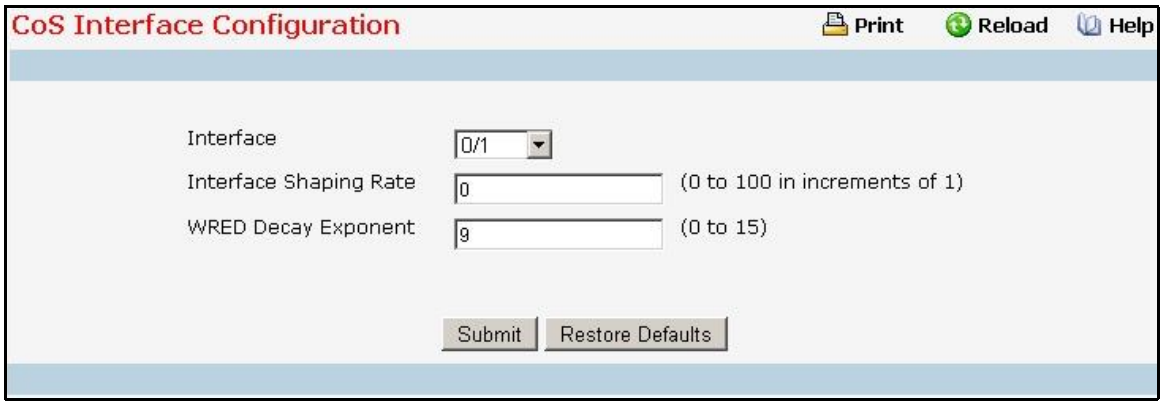
Non-Configurable Data

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.

11.5.5.4 cConfiguring CoS interface



Selection Criteria

Interface - 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 1. The value 0 means maximum is unlimited.

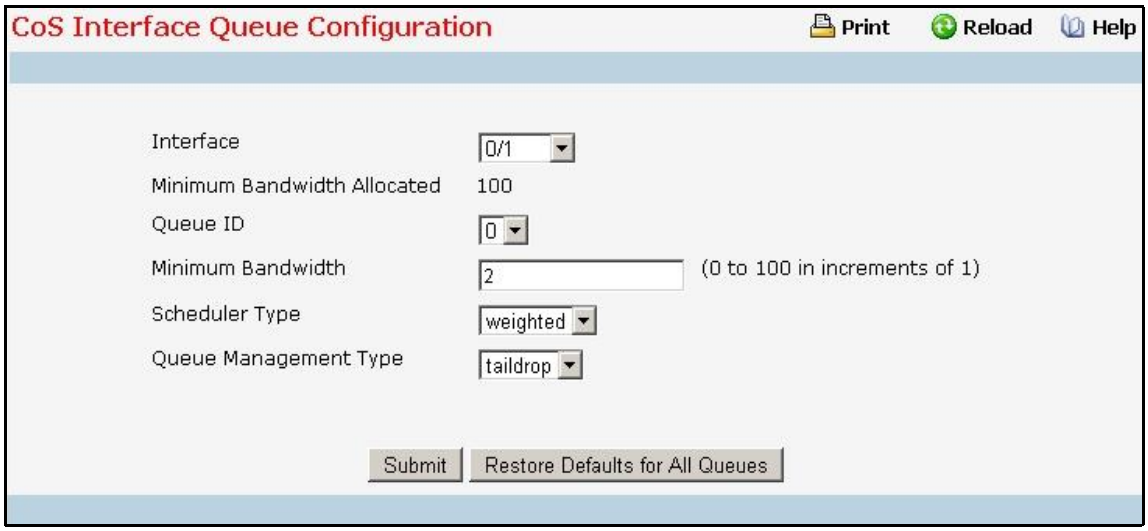
WRED Decay Exponent - Specifies the decay exponent value used with the WRED average queue length calculation algorithm. Default value is 9. Valid Range is (0 to 15).

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.

11.5.5.5 Configuring CoS interface queue



Selection Criteria

Interface - 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.

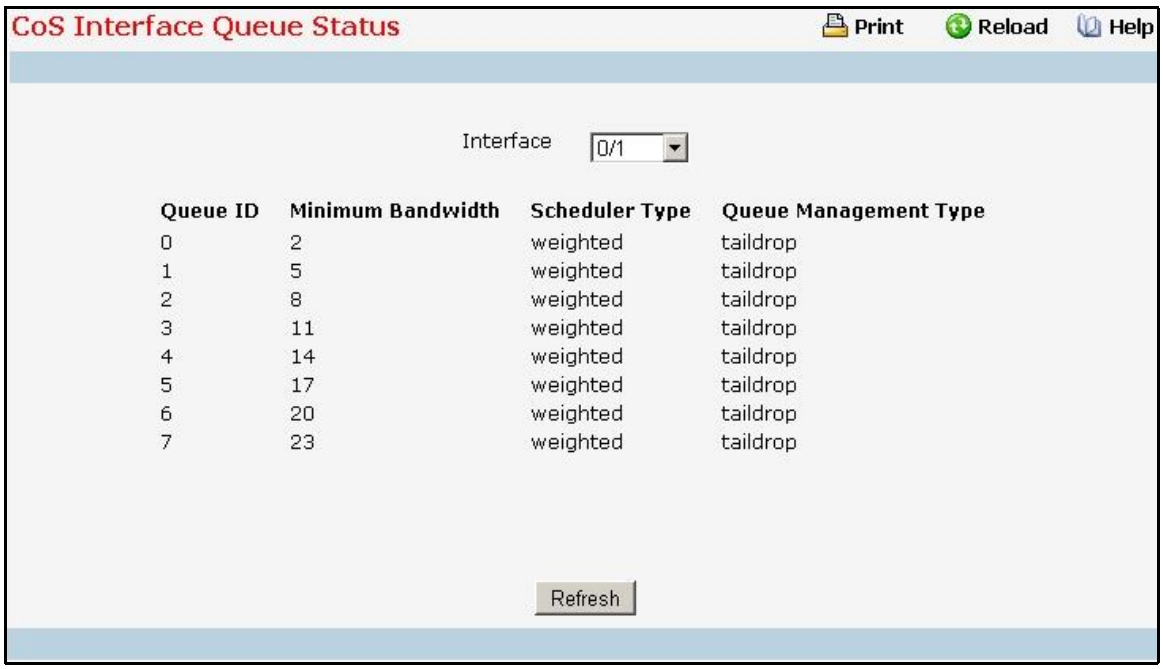
Minimum Bandwidth - Specifies the minimum guaranteed bandwidth allotted to this queue. Setting this value higher than its corresponding Maximum Bandwidth automatically increases the maximum to the same value. Default value is 0. Valid Range is (0 to 100) in increments of 1 . The value 0 means no guaranteed 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.

11.5.5.6 Viewing CoS interface queue status



Selection Criteria

Interface - 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:

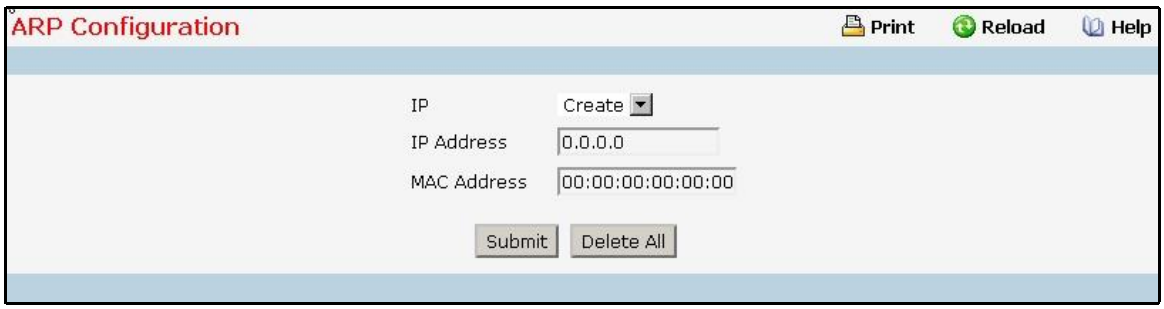
- taildrop

11.6 Routing Menu

11.6.1 Managing ARP Table

11.6.1.1 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

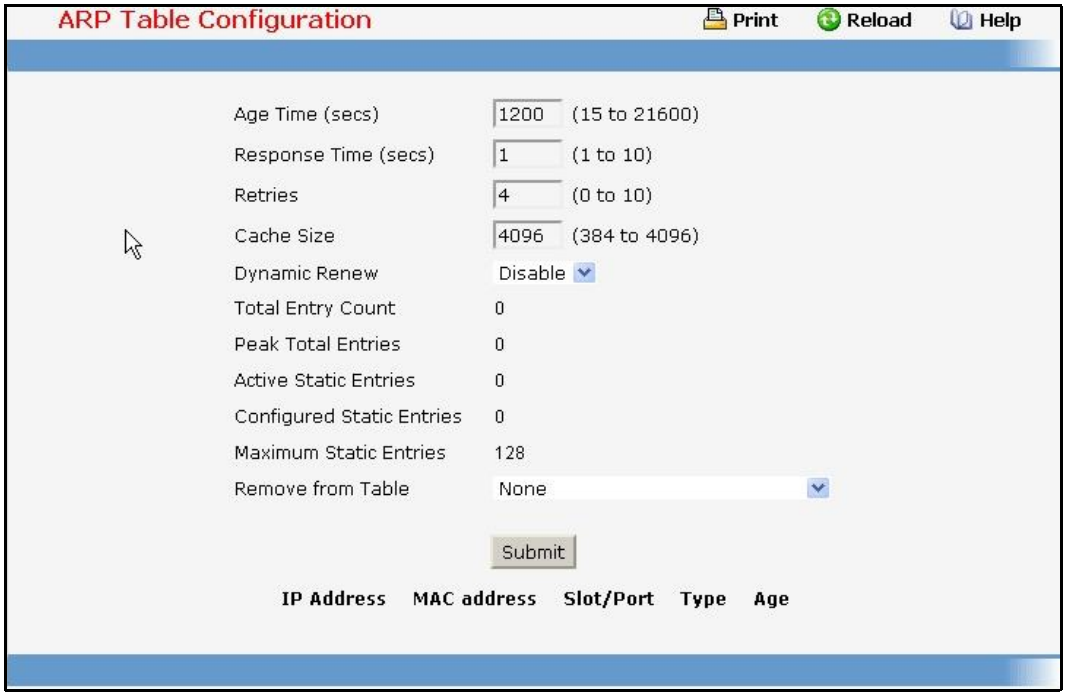
Submit - Update the switch with the values on this screen. If you want the switch to retain the new values across a power cycle, you must perform a save.

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.

11.6.1.2 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.

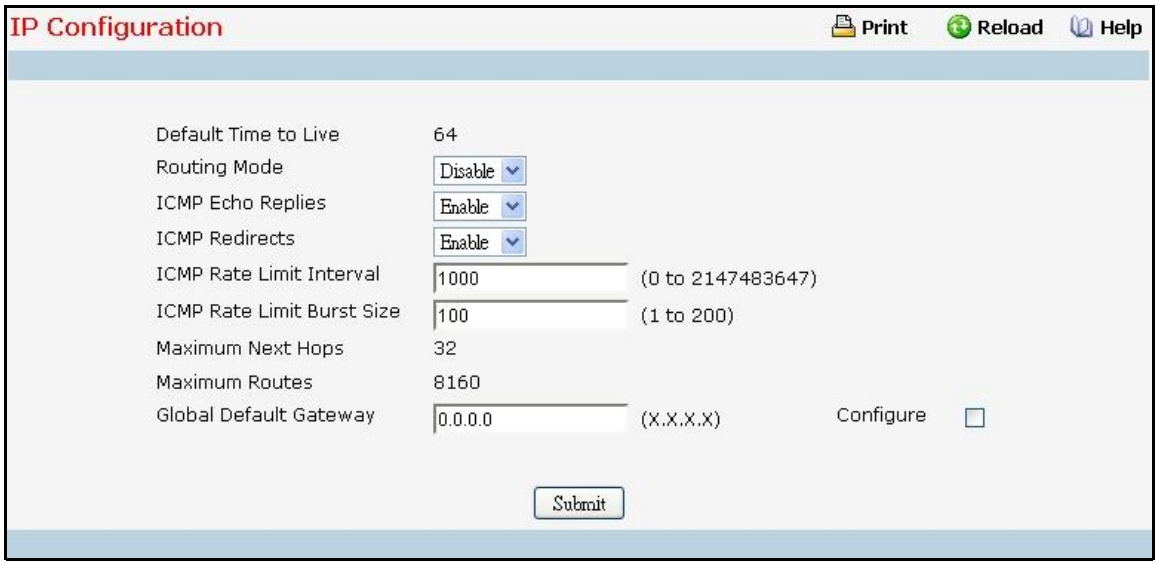
Command Buttons

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.

11.6.2 Managing IP Interfaces

11.6.2.1 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 pull-down menu. You must enable routing for the switch before you can route through any of the interfaces. The default value is disable.

ICMP Echo Replies - Select enable or disable from the pull-down menu. If it is enable then only the router can send ECHO replies. By default ICMP Echo Replies is Enable.

ICMP Redirects - If it is enabled globally and on interface level then only the router can send ICMP Redirects. By default ICMP Redirects is Enable.

ICMP Rate Limit Interval - To control the ICMP error packets user can specify the number of ICMP error packets are allowed per burst interval. By default Rate Limit is 100 packets/sec i.e. burst interval is 1000 msec. To disable ICMP Rate limiting set this field to '0'. Valid Rate Interval must be in the range (0 to 2147483647).

ICMP Rate Limit Burst Size -To control the ICMP error packets user can specify the number of ICMP error packets are allowed per burst interval. By Default burst size 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).

Global Default Gateway - This is an optional and select the Configure check box to edit this field, Sets the global default gateway to the manually configured value. A default gateway configured with this command is more preferred than a default gateway learned from a DHCP server. Only one default gateway can be configured. If you invoke this command multiple times, each command replaces the previous value.

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.

Maximum Routes - The maximum number of routes (routing table size) 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.

Delete Global Default Gateway - Deletes the configured global default gateway address.

11.6.2.2 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.

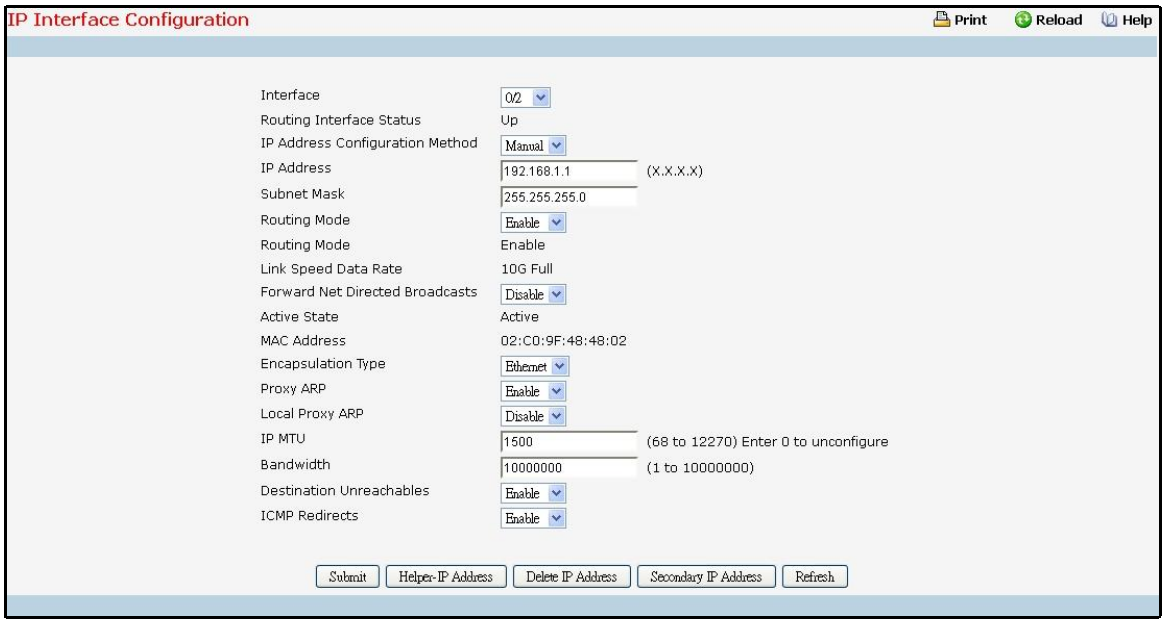
IcmpOutAddrMasks - The number of ICMP Address Mask Request messages sent.

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.

11.6.2.3 Configuring IP Interfaces



Selection Criteria

Interface - Select the interface for which data is to be displayed or configured.

IP Address Configuration Method - The Source of the IP Address, select whether it is configured manually or learned through DHCP. Method 'None' should be used to reset the DHCP method. NOTE: When the configuration method is changed from DHCP to None there will be a minor delay before the page refreshes.

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 pull-down 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 pull-down 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 pull-down menu.

Local Proxy Arp - Select to disable or enable Local Proxy ARP for the specified interface from the pull-down menu.

Destination Unreachables - Specifies the Mode of Sending ICMP Destination Unreachables on this interface. If this is Disabled then this interface will not send ICMP Destination Unreachables. By default Destination Unreachables mode is enable.

ICMP Redirects- The router sends an ICMP Redirect on an interface only if Redirects are enabled both globally and on the interface. By Default ICMP Redirects Mode is Enable.

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 size of IP packets sent on an interface. Valid range is 68 bytes to link MTU. When the IP MTU is unconfigured, the router uses the link MTU as the IP MTU. The IP MTU is the maximum frame size minus the length of the layer 2 header. By default IP MTU is 1500.

Non-Configurable Data

Routing Interface Status - This field indicates that the specified IP interface is up or down for IPv4 routing.

Link Speed Data Rate - The physical link data rate of the specified interface.

Active State - The state of the specified interface is either Active or Inactive. An interface is considered active if it the link is up and it is in forwarding state.

MAC Address - The burned-in physical address of the specified interface. The format is six two-digit hexadecimal numbers separated by colons, for example 00:06:29:32:81:40.

Command Buttons

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

Delete IP Address - Delete the IP Address from the interface. Note that the address can not be deleted if there are secondary addresses configured.

Restart DHCP IP Address - Restart the IP Address learned through DHCP.

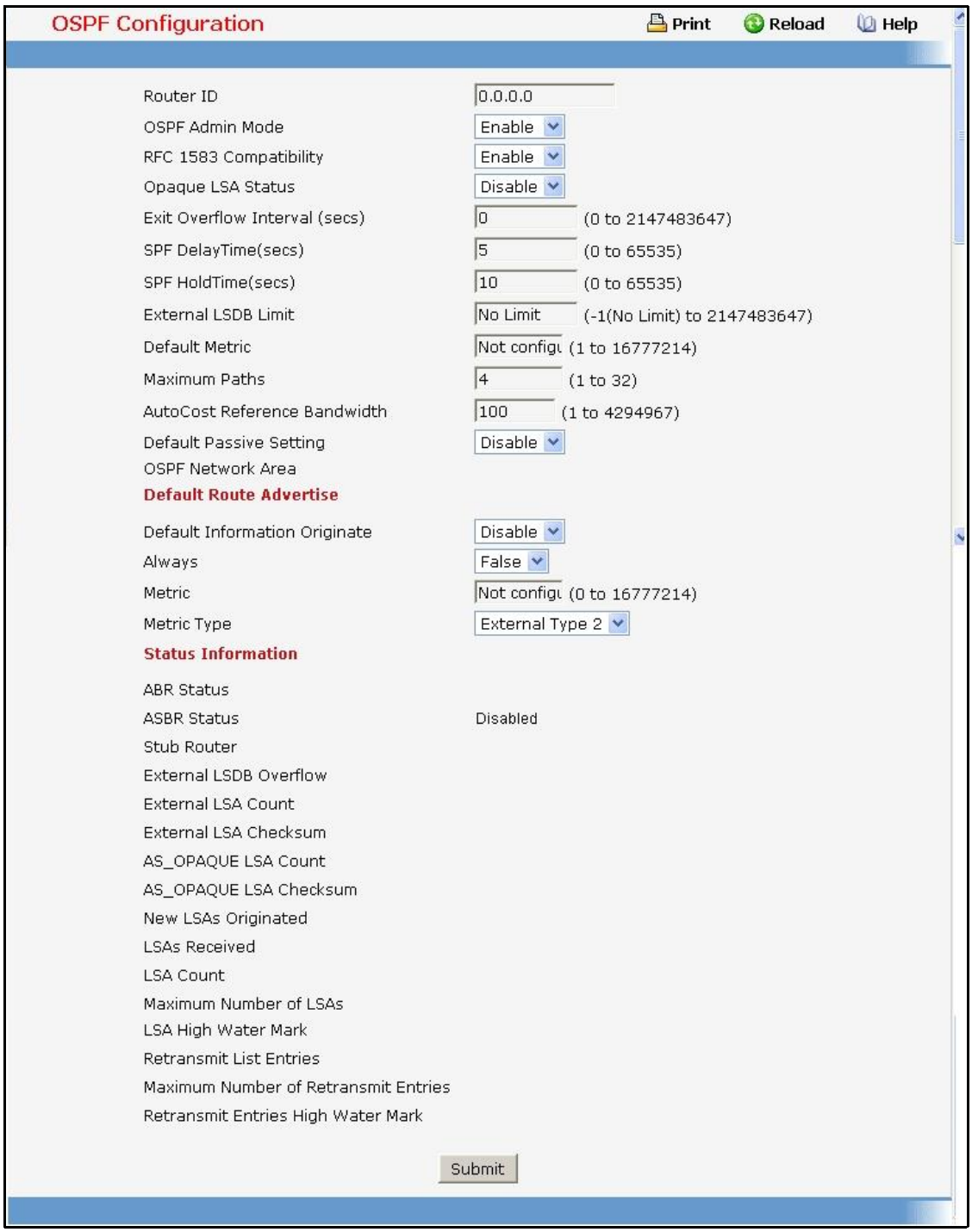
Secondary IP Address - Proceed to the Secondary IP Address configuration screen.

Display DHCP Parameters - Displays the DHCP Lease parameters. This button will be activated if the selected IP interface has an active DHCP lease.

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

11.6.3 Managing OSPF

11.6.3.1 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 pull-down 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 pull-down 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.

Opaque LSA Status- Set this parameter to Enable to if OSPF should store and flood opaque LSAs. The default value is Enable. An opaque LSA is used for flooding user-defined information within an OSPF router domain.

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.

External LSDB Limit- The maximum number of External LSAs that can be stored in the database. Default value for limit is -1. 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 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).

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. Default value is 100. 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 is Disable.

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.

Helper Support Mode- Configures how unit will act when a neighbor performs a warm restart. The possible values are:

Planned - Indicates that OSPF should only help a restarting neighbor during planned events.

Always - Indicates that OSPF help a restarting neighbor during all planned and unplanned warm restart events.

Disabled - Disables OSPF from acting as a helpful neighbor.

Helper Strict LSA Checking - When enabled, the unit will exit helper mode whenever the topology changes.

Non-Configurable Data

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.

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.

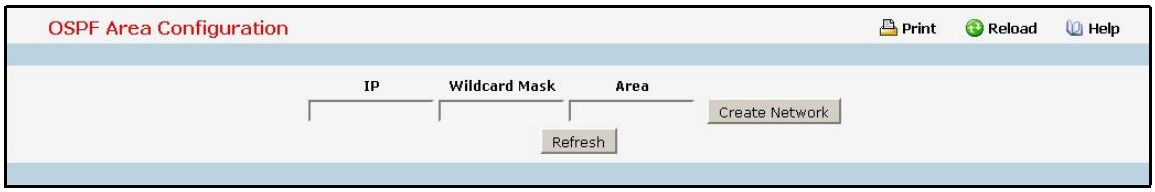
New LSAs Originated - In any given OSPF area, a router will originate several LSAs. Each router originates a router-LSA. If the router is also the Designated Router for any of the area's networks, it will originate network-LSAs for those networks. This value represents the number of LSAs originated by 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.

11.6.3.2 Network Area Configuring



Configurable Data

IP - Apply this IP for the Network Area setting.

Wildcard Mask - Use Wildcard Mask to filter IP range.

Area - Configure the OSPF Router Area for the Network Area setting.

Non-Configurable Data

IP - Show IP for the Network Area setting.

Wildcard Mask - Show Wildcard Mask of the Network Area setting.

Area - Show area for the Network Area setting.

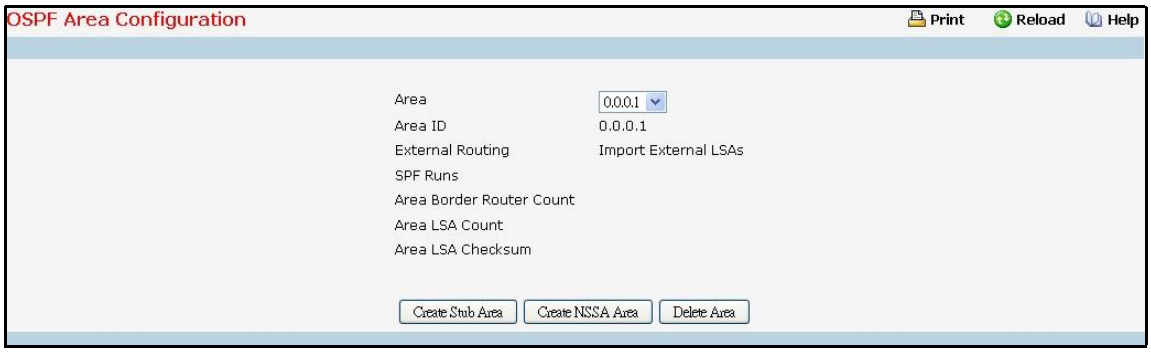
Command Buttons

Create Network - Create an OSPF Area for the IP network.

Delete - Removes the specified IP network from the router configuration.

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

11.6.3.3 Configuring Area



Selection Criteria

Area ID - Select the area to be configured.

Configurable Data

Import Summary LSAs - Select enable or disable from the pull down menu. If you select enable summary LSAs will be imported into stub/NSSA areas. Defaults to Enable.

Originate Default Route - Select enable or disable from the pull down menu. It sets the default information origination configuration for the specified NSSA. It has to be enabled to be able to configure NSSA's Metric Value and Metric Type attributes. Defaults to Disable.

Stub Area Specific Parameter

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. By default it is 1.

NSSA Specific Parameters

Metric Value - Set the Metric value for NSSA. The valid range of values is (1 to 16777214). By default it is 10.

Metric Type - Select the type of metric specified in the Metric Value field. By default it is Non-comparable Cost.

Comparable Cost - External Type 1 metrics that are comparable to the OSPF metric.

Non-comparable Cost - External Type 2 metrics that are assumed be larger than the cost of the OSPF 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. Defaults to 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). By default it is 40.

Redistribute Mode - Enable or Disable the Redistribute Mode into the NSSA. Defaults to Enable.

Non-Configurable Data

External Routing - Indicates whether the area is configured as a stub area, not-so-stubby-area (NSSA), or regular area. External LSAs are not flooded into stub areas.

Import External LSAs - Import and propagate external LSAs

Import No LSAs - Do not import and propagate external LSAs

SPF Runs - The number of times that the intra-area route table has been calculated using this area's link-state database. This is typically done using Dijkstra's algorithm.

Area Border Router Count - The total number of area border routers reachable within this area. This is initially zero, and is calculated in each SPF Pass.

Area LSA Count - The total number of link-state advertisements in this area's link-state database, excluding AS External LSAs.

Area LSA Checksum - The 32-bit unsigned sum of the link-state advertisements' LS checksums contained in this area's link-state database. This sum excludes external (LS type 5) link-state advertisements. The sum can be used to determine if there has been a change in a router's link state database, and to compare the link-state database of two routers. This value is in hexadecimal.

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 - 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 Area - Deletes the area if none of the OSPF router interfaces are in that area.

11.6.3.4 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.

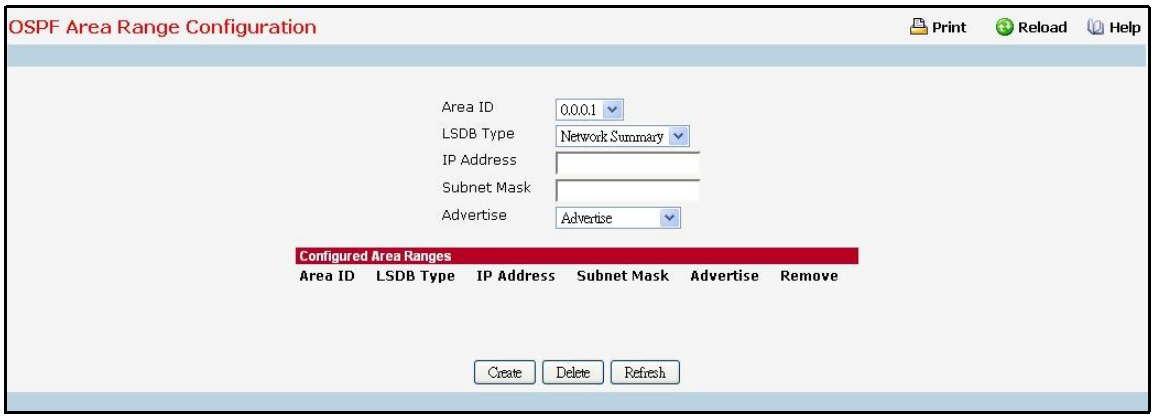
Metric Value - Set the metric value you want applied for the default route advertised into the area. Valid values range from 1 to 16,777,215.

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.

11.6.3.5 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 pull-down menu. If you selected enable the address range will be advertised outside the area via a Network Summary LSA. The default is enable.

Remove - Check box to remove the particular entry from the table.

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

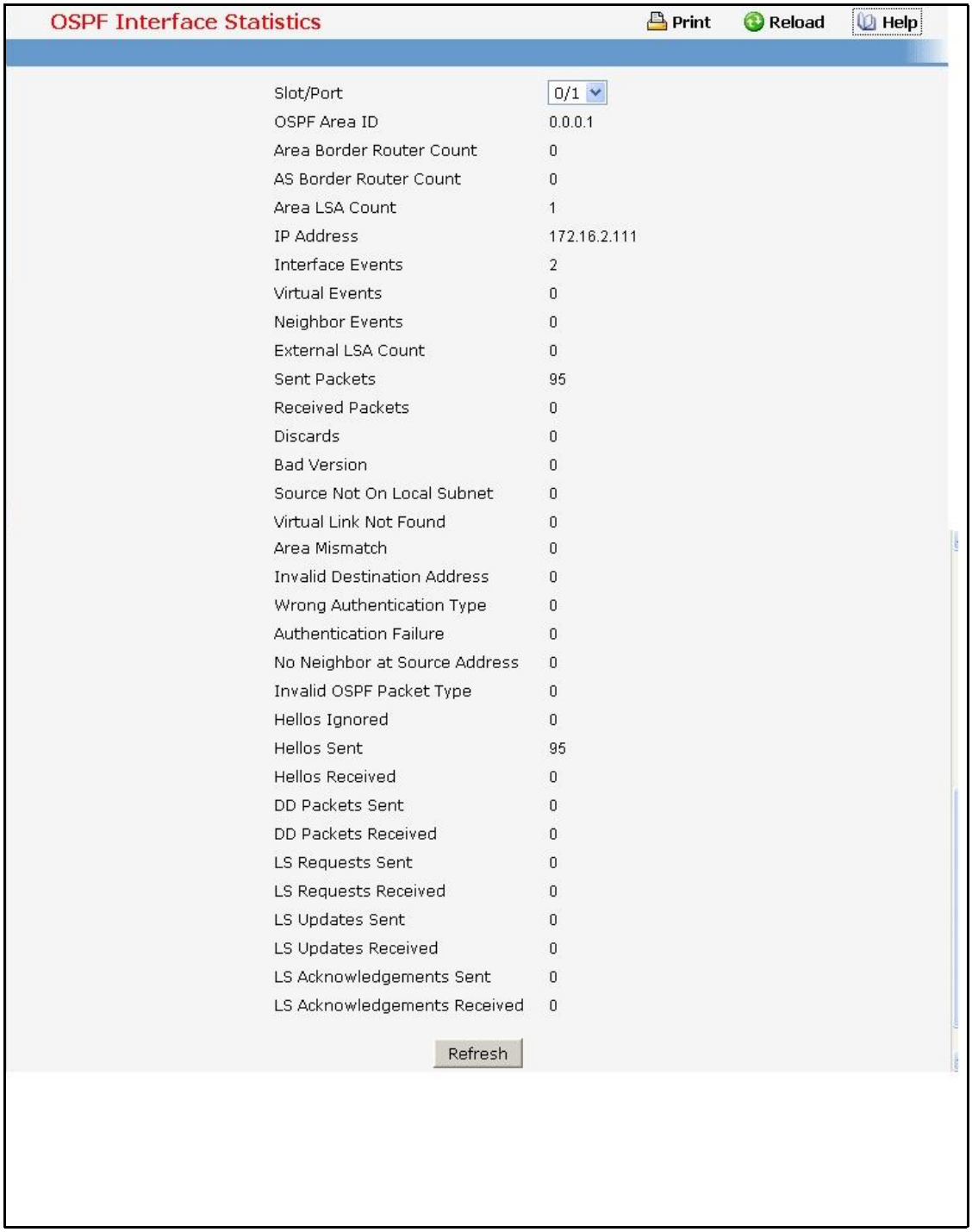
Create - Send the updated configuration to the switch. Configuration changes take effect immediately. These changes will not be retained across a power cycle unless a save is performed. The new address range will be added to the display in the non-configurable data area.

Delete - Removes the specified address range from the area configuration.

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

11.6.3.6 View Interface Statistics

This panel displays statistics for the selected interface. The information will be displayed only if OSPF is enabled.



Selection Criteria

Interface - 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.

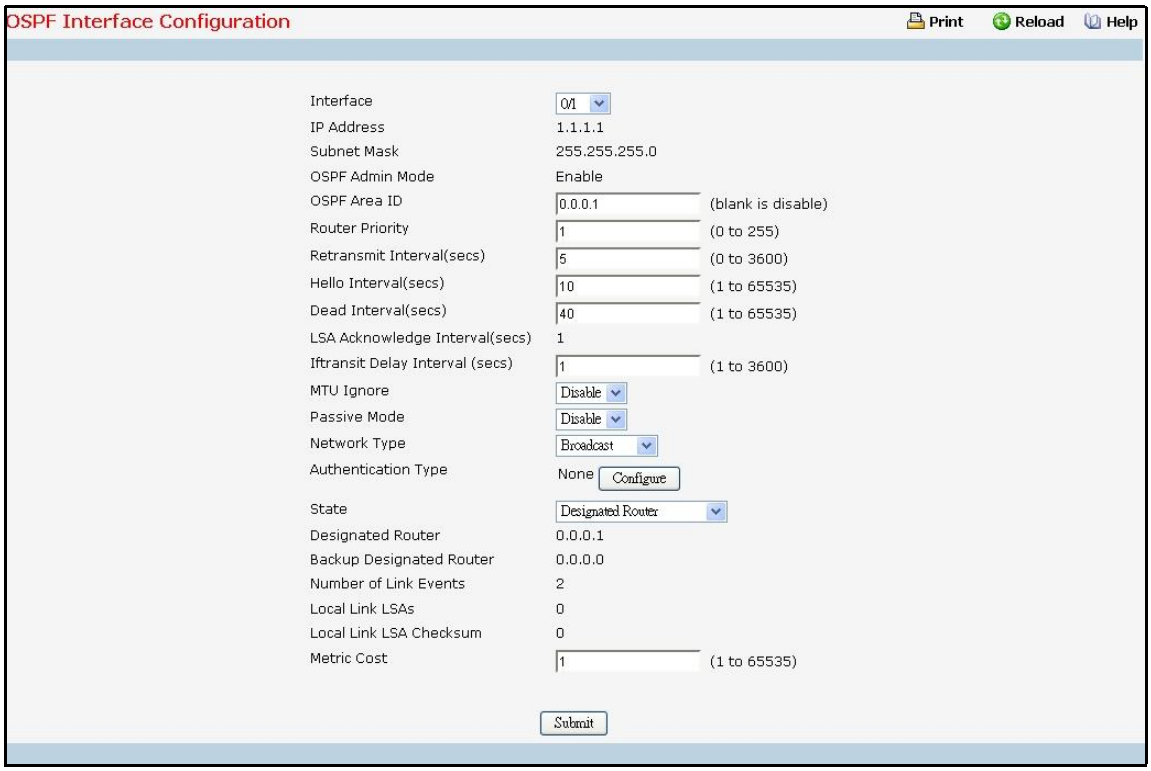
LS Acknowledgements Sent - The number of LS acknowledgements sent on this interface by this router.

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.

11.6.3.7 Configuring OSPF Interface



Selection Criteria

Interface - 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.

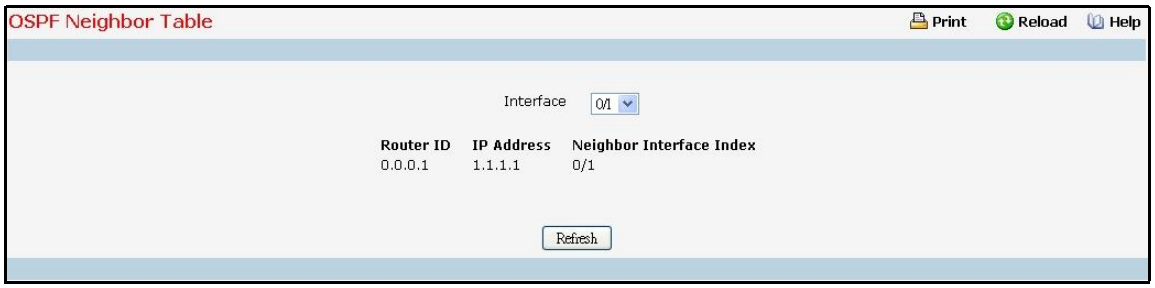
Command Buttons

Configure - 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.

11.6.3.8 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

Interface - 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 neighbor on the selected Interface.

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.

11.6.3.9 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

Neighbor IP Address - Selects the IP Address of the neighbor for which data is to be displayed. Non-Configurable Data

Interface - The local interface which connect to neighbor.

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.

Up Time - The Up Time of the OSPF neighbor, which says how long the neighbor is active

Restart Helper Status - The status of a helpful neighbor can be the following:

Not Restarting - The neighbor is not restarting.

Planned Restart - The neighbor is restarting due to a user initiated failover.

Unplanned Restart - The neighbor is restarting due to an unplanned failover.

Restart Reason - The reason for the last restart.

Remaining Grace Time - The number of seconds remaining in the current graceful restart interval. This row is only included if the router is currently acting as a restart helper for the neighbor.

Restart Helper Exit Reason - The reason behind the last restart of the a helpful neighbor can be the following:

None - Graceful restart has not been attempted. In

Progress - Restart is in progress.

Completed - The previous graceful restart completed successfully.

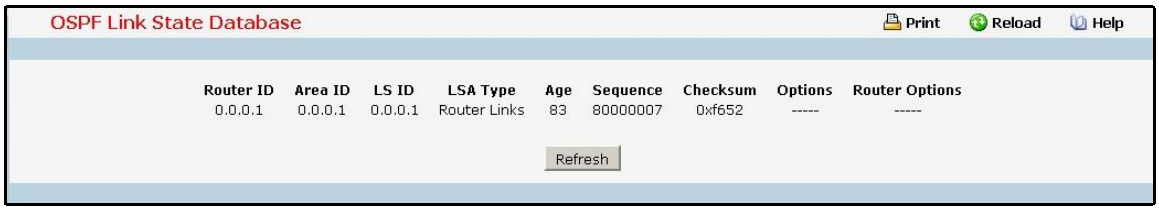
Timed Out - The previous graceful restart timed out.

Topology Changed - The previous graceful restart terminated prematurely because of a topology change.

Command Buttons

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

11.6.3.10 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.

External LSDB Table

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.

Router ID - The Router ID value of the advertising router for this LSA.

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.

AS Opaque LSDB Table

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.

Router ID - The Router ID value of the advertising router for this LSA.

Age - The time since the link state advertisement was first originated, in seconds.

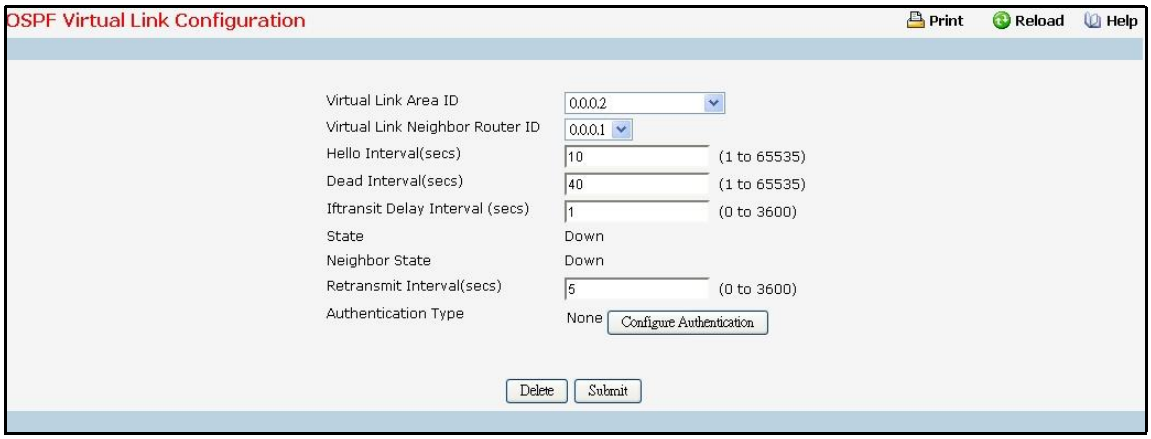
Sequence - The sequence number field is a signed 32-bit integer. It is used to detect old and duplicate link state advertisements. The larger the sequence number, the more recent the advertisement.

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.

Command Buttons

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

11.6.3.11 Configuring OSPF Virtual Link



Selection Criteria

Virtual Link Area ID - Select option 'Create New Virtual Link' 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.

Virtual Link Neighbor Router ID - Select the Virtual Link Neighbor Router ID for which you want to display or configure data.

Virtual Interface Area ID - Select the Virtual Link Interface Area ID for which you want to display or configure data.

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

State - The current state of the selected Virtual Link. 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.

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.

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.

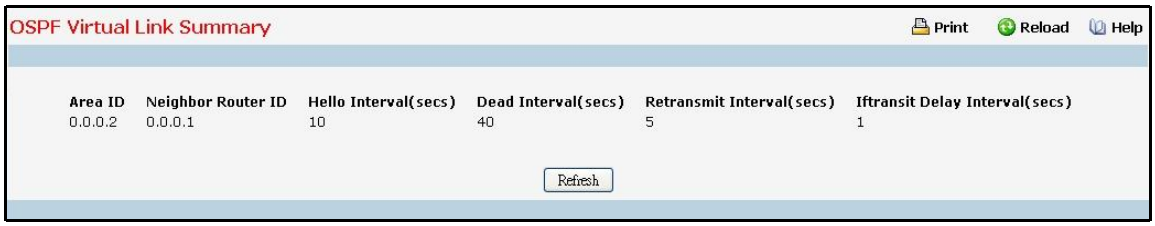
Submit - Send the updated configuration to the switch. Configuration changes take effect immediately. These changes will not be retained across a power cycle unless a save is performed.

Delete - Removes the specified virtual link from the router configuration.

Create - Creates the specified virtual link for the router configuration.

Cancel - Discards the changes made on the page.

11.6.3.12 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 (secs) - 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 (secs) - 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 (secs) - 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.

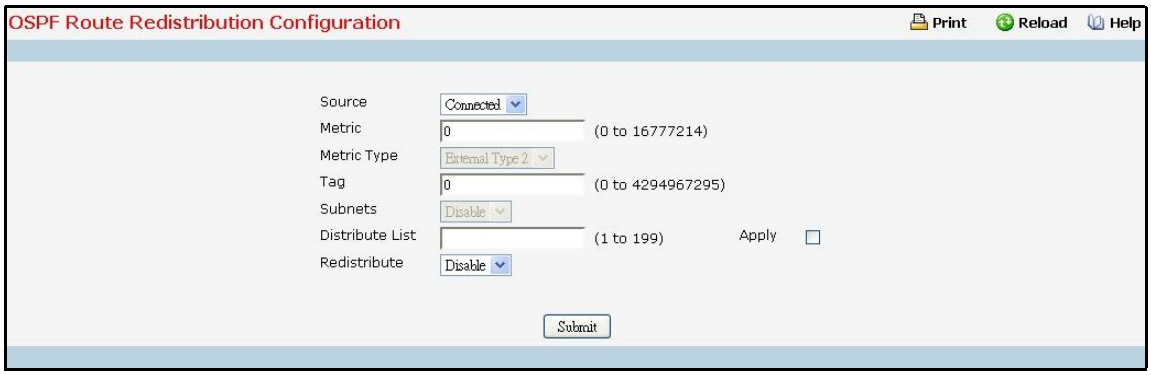
Iftransit Delay Interval - The OSPF Transit Delay for the virtual link in units of seconds. It specifies the estimated number of seconds it takes to transmit a link state update packet over this interface.

Command Buttons

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

11.6.3.13 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

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'.

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. Default value is 0.

Subnets - Sets whether the subnetted routes should be redistributed or not. Default value is Disable.

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.

Redistribute - Enables or disables the redistribution for the selected source protocol. It has to be enabled to be able to configure any of the route redistribution attributes except the 'Distribute List' field. Default value is Disable.

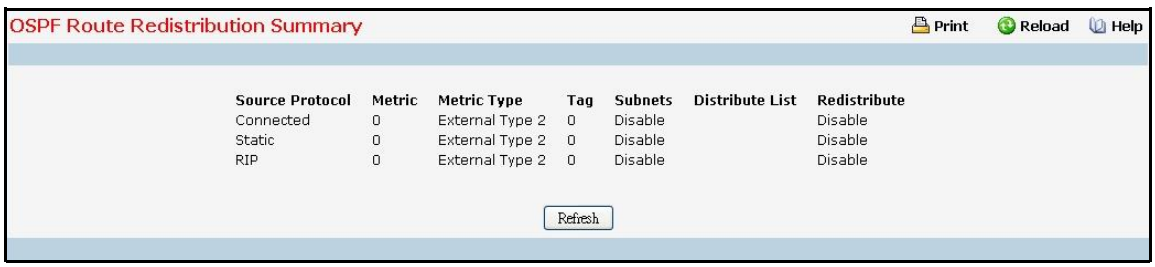
Command Buttons

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.

11.6.3.14 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.

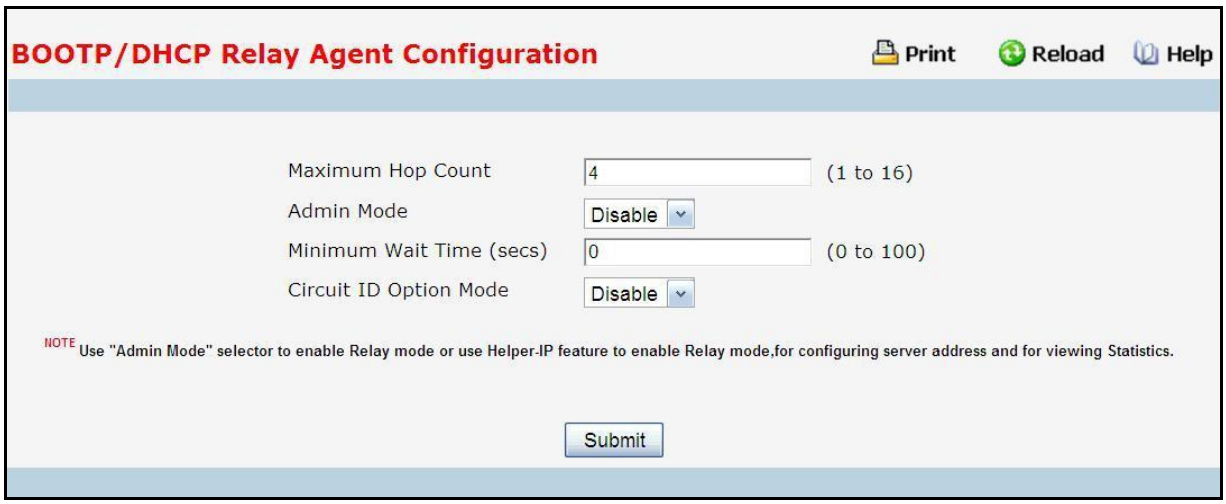
Distribute List - The Access List that filters the routes to be redistributed by the Destination Protocol. Display 0 when not configured.

Command Buttons

Refresh - Displays the latest OSPF Route Redistribution Configuration data.

11.6.4 Managing BOOTP/DHCP Relay Agent

11.6.4.1 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 in IP Helper module.

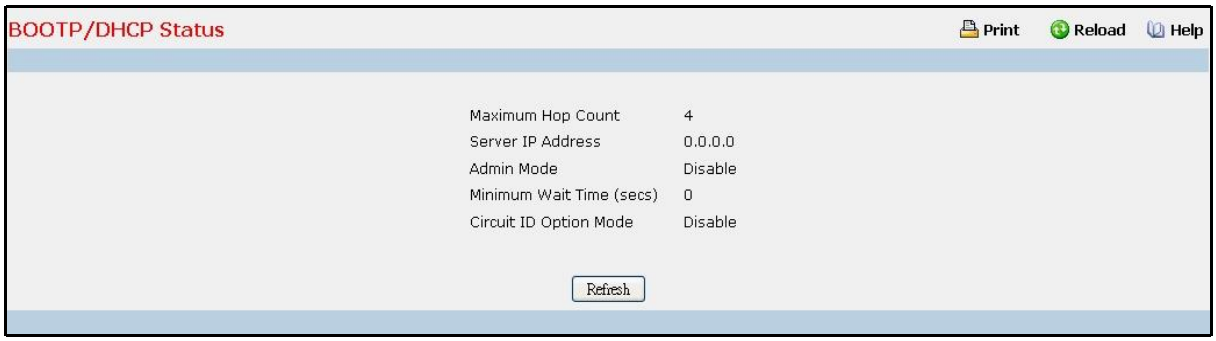
Minimum Wait Time (secs)- Enter a time in seconds. This value will be compared to the time stamp in the client's request packets, which should represent the time since the client was powered up. Packets will only be forwarded when the time stamp exceeds the minimum wait time.

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.

11.6.4.2 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.

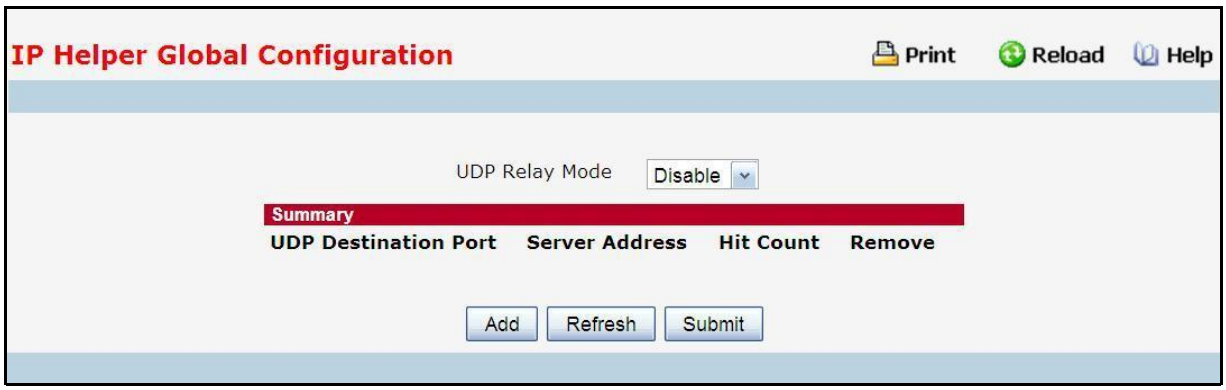
Packets Discarded - The total number of BOOTP/DHCP packets discarded by this Relay Agent since the last time the switch was reset.

Command Buttons

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

11.6.5 Managing IP Helper

11.6.5.1 Configuring Global IP Helper



Configurable Data

UDP Relay Mode - Select enable or disable from the pull down menu. User must enable Relay Mode to relay any other protocols for which an IP helper address has been configured. By Default UDP Relay Mode is disabled.

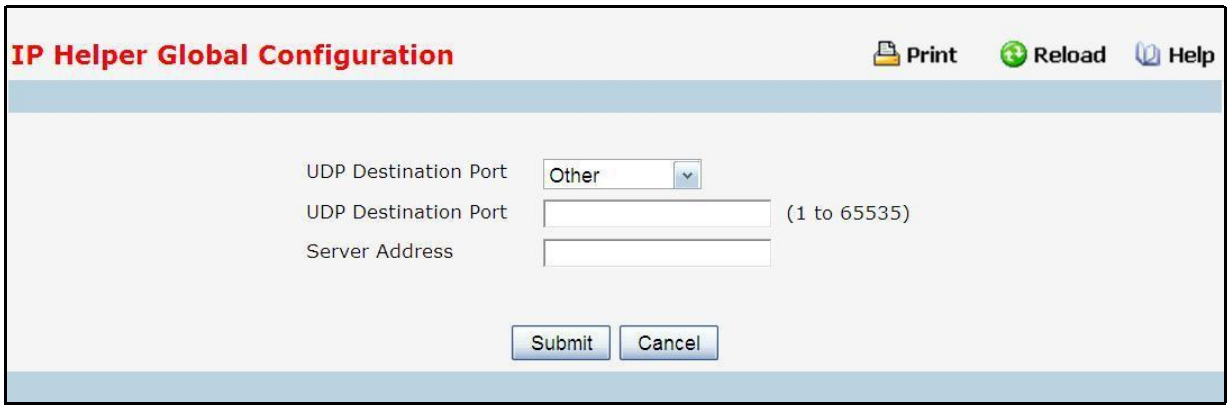
Remove - Removes the specified UDP Relay when selected and "Submit" is pressed.

Command Buttons

Add - Used to add UDP Relay/Helper IP configuration.

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.

11.6.5.2 Adding Global IP Helper Address



Configurable Data

UDP Destination Port (1 to 65535) - The destination UDP port ID/Port Name of UDP packets to be relayed. Select the protocol from the menu. If the user wants to configure other than the listed protocols, select Other from the menu. Then user will be prompted with the UDP Destination Port field. Select the DefaultSet to configure for the relay entry for the default set of protocols.

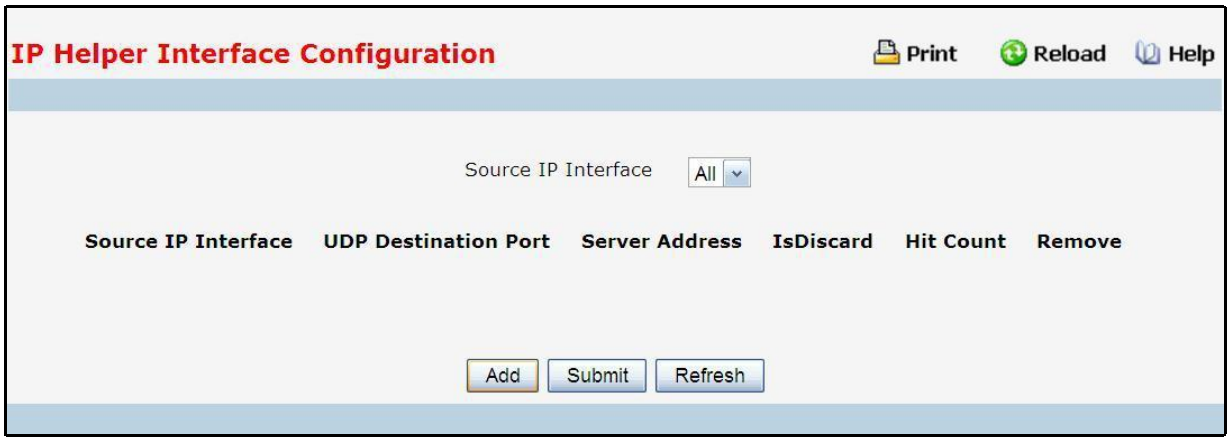
Server Address - The Server Address to which the packets with the given UDP Destination Port will be relayed.

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.

Cancel - Discards the changes made on the page.

11.6.5.3 Configuring Interface IP Helper



Configurable Data

Source IP Interface - Select the interface from the pull down menu to get the relay entries configured on a particular interface. If "All" is selected all the configured relay entries on all interfaces will be displayed.

Remove - Removes the specified UDP Relay Entry when selected and "Submit" is pressed.

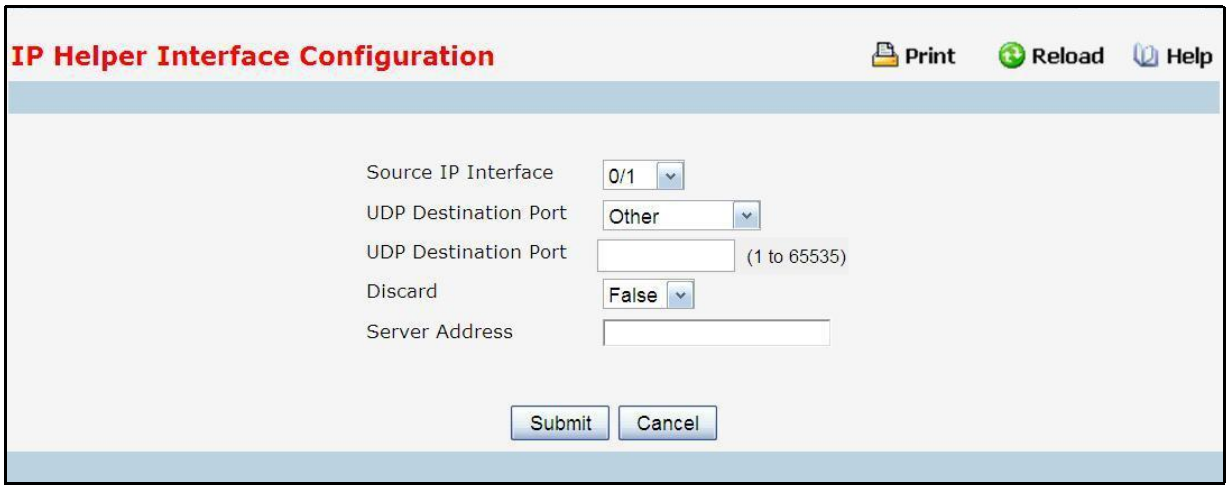
Command Buttons

Add - Used to add UDP Relay/Helper IP configuration.

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.

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

11.6.5.4 Adding Interface IP Helper Address



Configurable Data

Source IP Interface - Select the interface from the pull-down menu for which user wants to configure the relay entry

UDP Destination Port - Select the Destination UDP port Name from the pull down menu or configure the port number to configure the Relay Entry on selected interface.

Discard - If True, packets arriving on the given interface with the given destination UDP port are discarded rather than relayed. Discard entries are used to override global IP helper address entries which otherwise might apply to a packet.

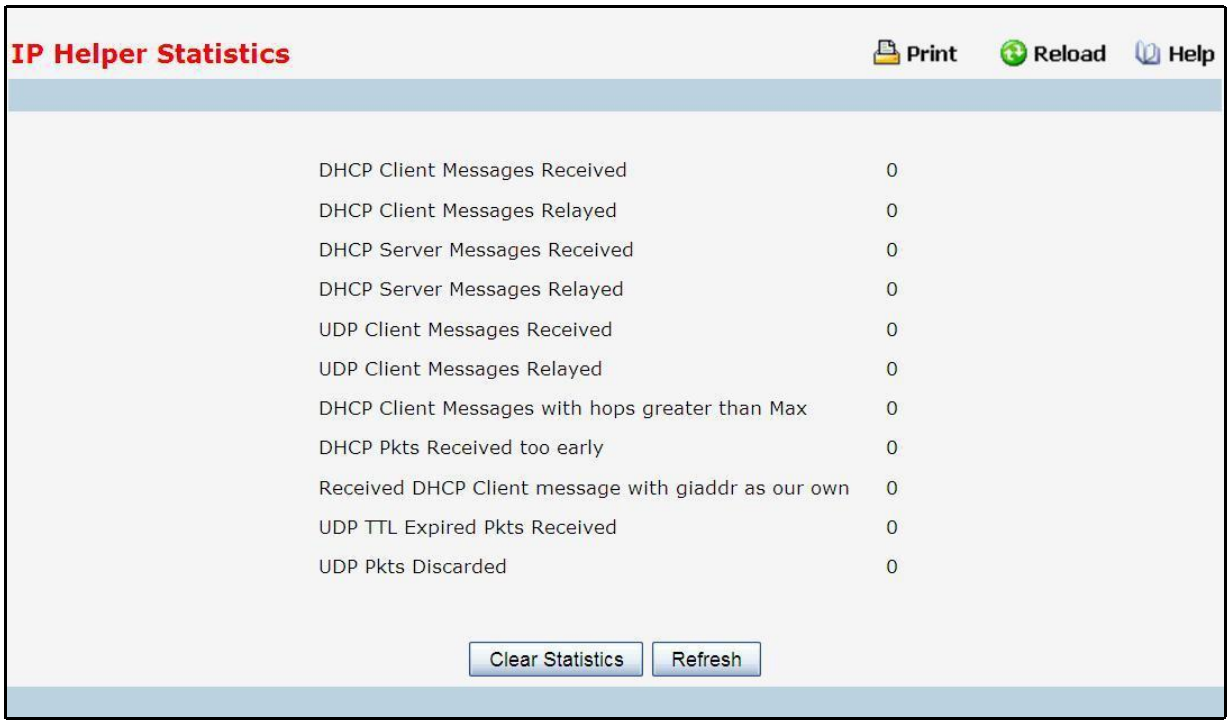
Server Address - The IPv4 address of the server to which packets are relayed for the specific UDP Destination Port.

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.

Cancel - Discards the changes made on the page.

11.6.5.5 Viewing IP Helper Statistics



Non-Configurable Data

DHCP Client Messages Received - The number of valid messages received from a DHCP client. The count is only incremented if IP helper is enabled globally, the ingress routing interface is up, and the packet passes a number of validity checks, such as having a TTL >1 and having valid source and destination IP addresses.

DHCP Client Messages Relayed - The number of DHCP client messages relayed to a server. If a message is relayed to multiple servers, the count is incremented once for each server.

DHCP Server Messages Received - The number of DHCP responses received from the DHCP server. This count only includes messages that the DHCP server unicasts to the relay agent for relay to the client.

DHCP Server Messages Relayed - Specifies the number of DHCP server messages relayed to a client.

UDP Client Messages Received - The number of valid UDP packets received. This count includes DHCP messages and all other protocols relayed. Conditions are similar to those for the first statistic in this table.

UDP Client Messages Relayed - The number of UDP packets relayed. This count includes DHCP messages relayed as well as all other protocols. The count is incremented for each server to which a packet is sent.

DHCP Client Messages with hops greater than Max - Specifies the number of DHCP Client Messages with hops greater than Max.

DHCP Pkts Received too early - Specifies the number of DHCP Pkts Received too early.

Received DHCP Client message with giaddr as our own - Specifies the number of DHCP Client messages received with giaddr as our own.

UDP TTL Expired Pkts Received - Specifies the number of UDP packets received with expired TTL.

UDP Pkts Discarded - Specifies the number of UDP packets discarded.

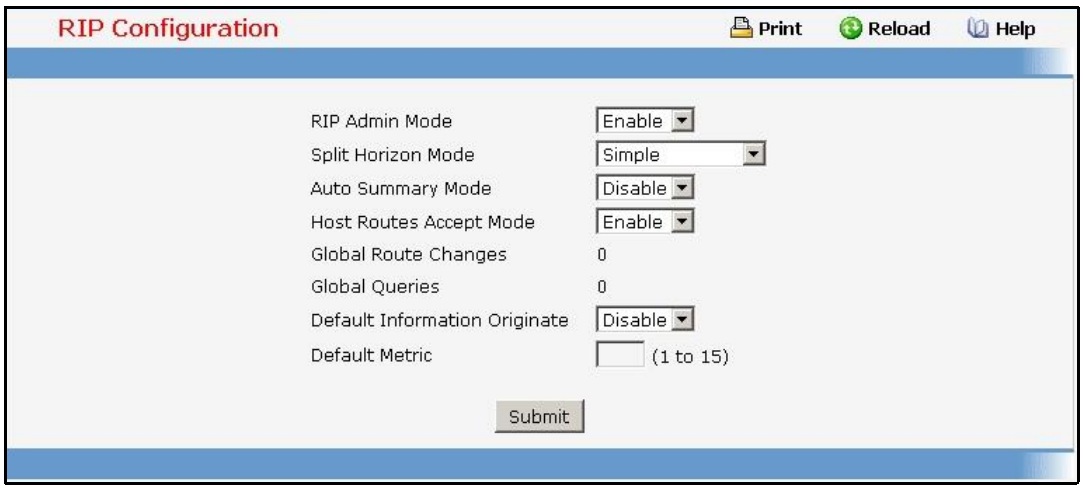
Command Buttons

Clear Statistics - Resets all helper Statistics.

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

11.6.6 Managing Routing Information Protocol (RIP)

11.6.6.1 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

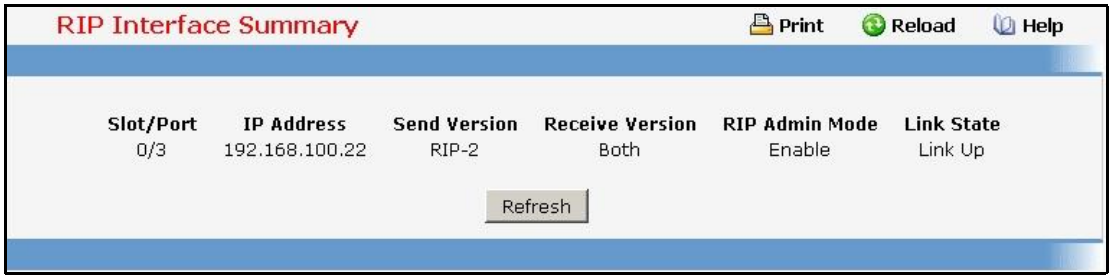
Global Route Changes - The number of route changes made to the IP Route Database by RIP. This does not include the refresh of a route's age.

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.

11.6.6.2 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.

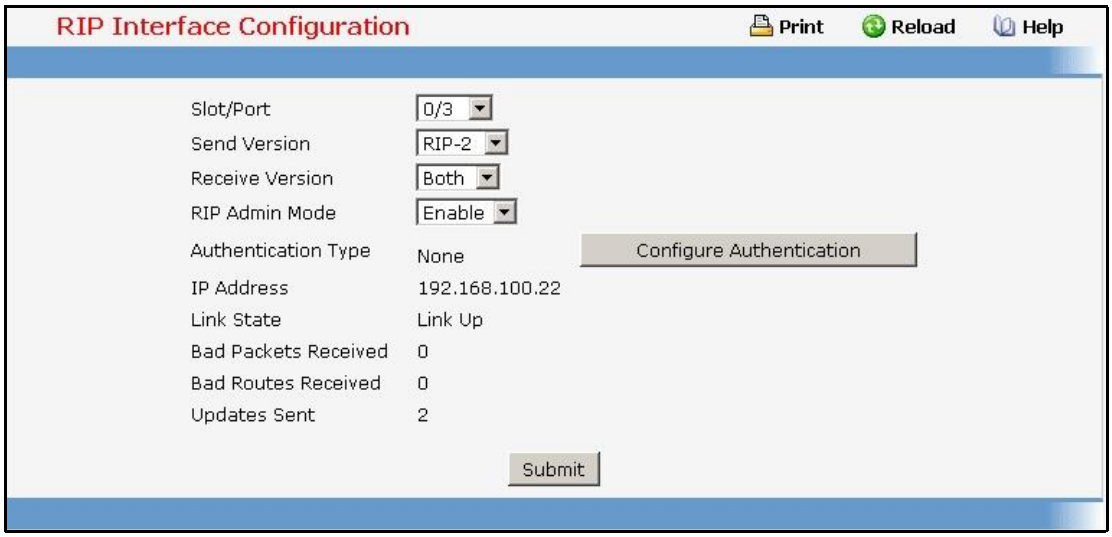
RIP Admin Mode - Whether RIP is enabled or disabled on the interface.

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.

11.6.6.3 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.

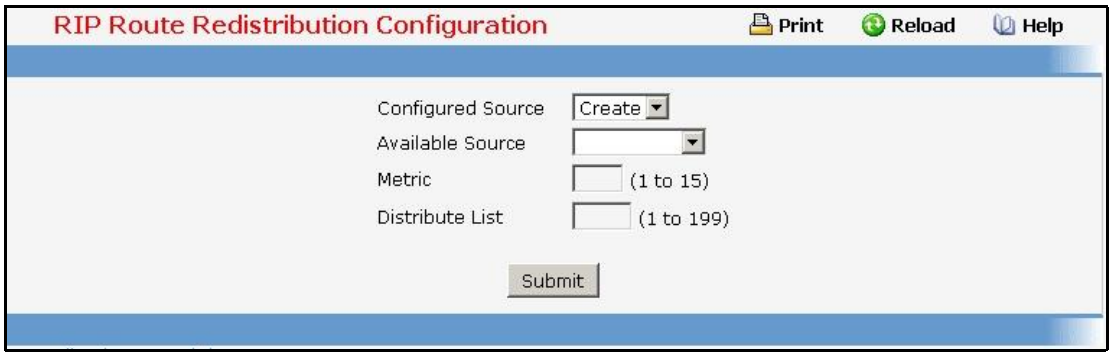
Command Buttons

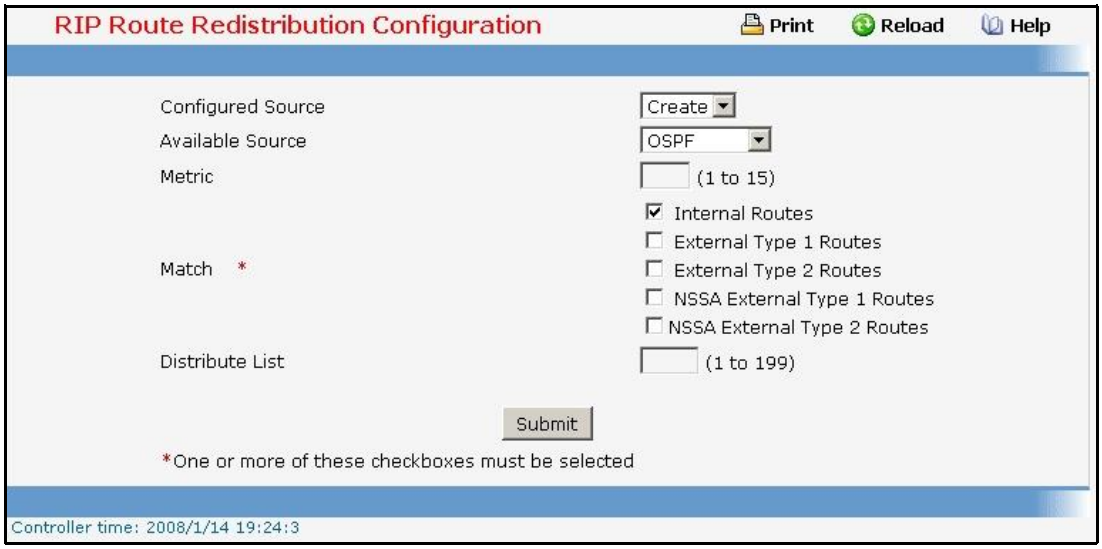
Configure Authentication - Display a new screen where you can select the authentication method for the virtual link.

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.

11.6.6.4 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.

11.6.6.5 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

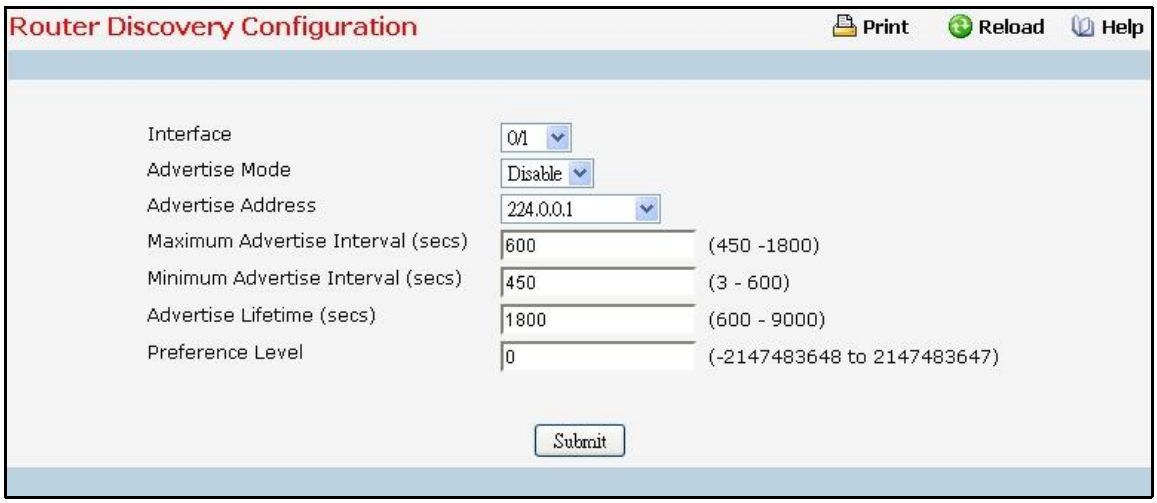
Distribute List - The Access List that filters the routes to be redistributed by the Destination Protocol. Displays 0 when not configured.

Command Buttons

Refresh - Displays the latest RIP Route Redistribution Configuration data.

11.6.7 Managing Router Discovery

11.6.7.1 Configuring Router Discovery



Selection Criteria

Interface - 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.

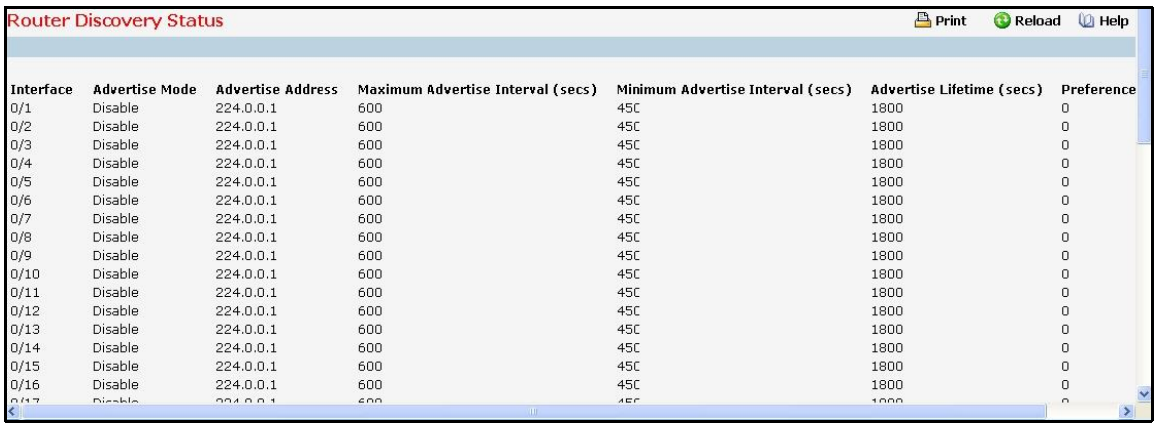
Advertise Lifetime (secs) - Enter the value (in seconds) to be used as the lifetime field in router advertisements sent from the interface. This is the maximum length of time that the advertised addresses are to be considered as valid router addresses by hosts.

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.

11.6.7.2 Viewing Router Discovery Status



Interface	Advertise Mode	Advertise Address	Maximum Advertise Interval (secs)	Minimum Advertise Interval (secs)	Advertise Lifetime (secs)	Preference
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

Non-Configurable Data

Interface - 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.

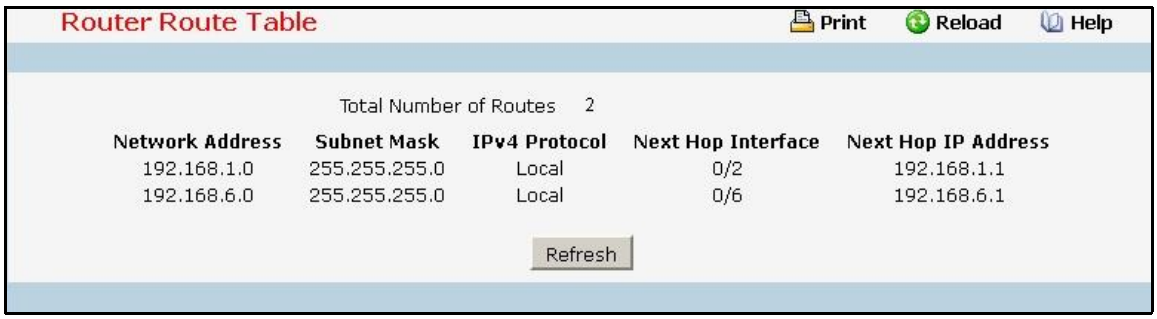
Preference Level - The preference level of the router as a default router relative to other routers on the same subnet. Higher numbered addresses are preferred.

Command Buttons

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

11.6.8 Managing Route Table

11.6.8.1 Viewing Router Route Table



Non-Configurable Data

Total Number of Routes - The total number of routes in the route table.

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.

IPv4 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 External
- RIP

Next Hop Interface - The outgoing router interface to use when forwarding traffic to the destination. For a Reject Route the next hop would be "Null0" interface.

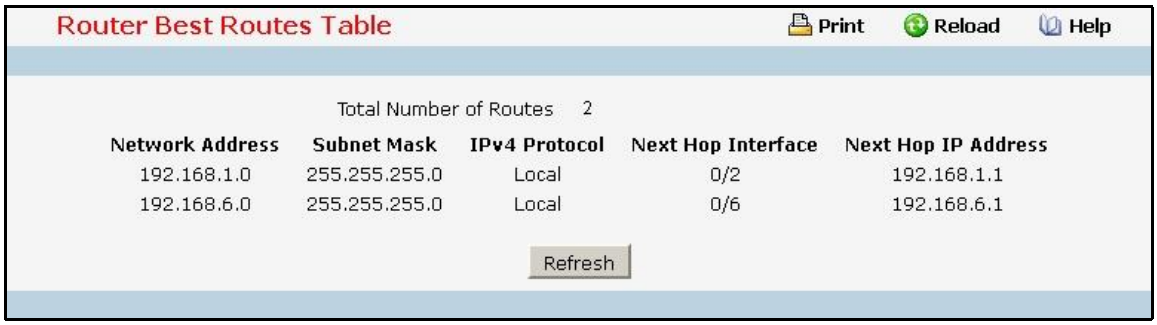
Next Hop IP Address - The outgoing router IP address to use when forwarding traffic to the next router (if any) in the path towards the destination. The next router will always be one of the adjacent neighbors or the IP address of the local interface for a directly attached network.

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.

11.6.8.2 Viewing Router Best Route Table



Non-Configurable Data

Total Number of Routes - The total number of routes in the route table.

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.

IPv4 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 External
- RIP

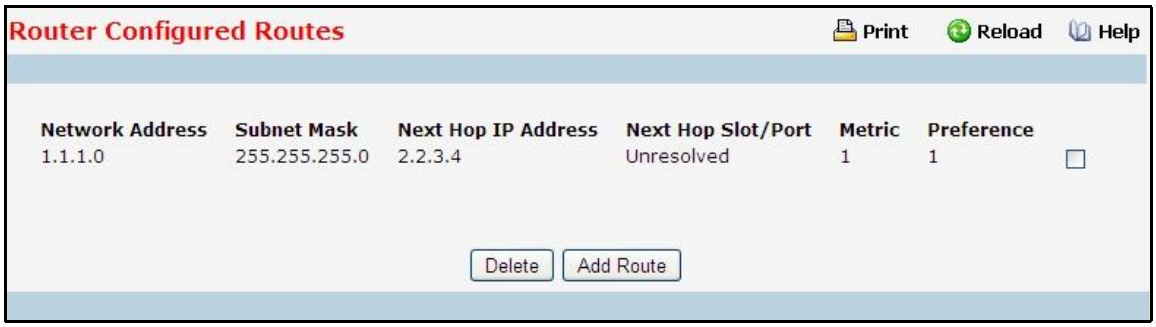
Next Hop Interface - The outgoing router interface to use when forwarding traffic to the destination.

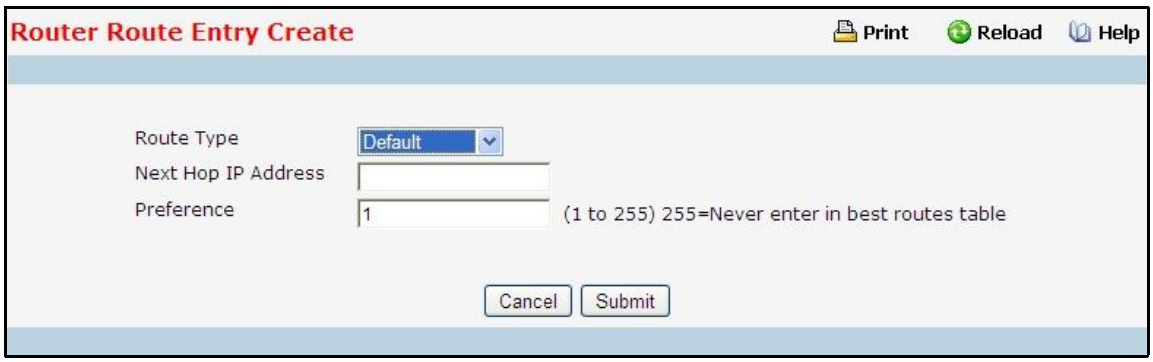
Next Hop IP Address - The outgoing router IP address to use when forwarding traffic to the next router (if any) in the path towards the destination. The next router will always be one of the adjacent neighbors or the IP address of the local interface for a directly attached network.

Command Buttons

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

11.6.8.3 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.

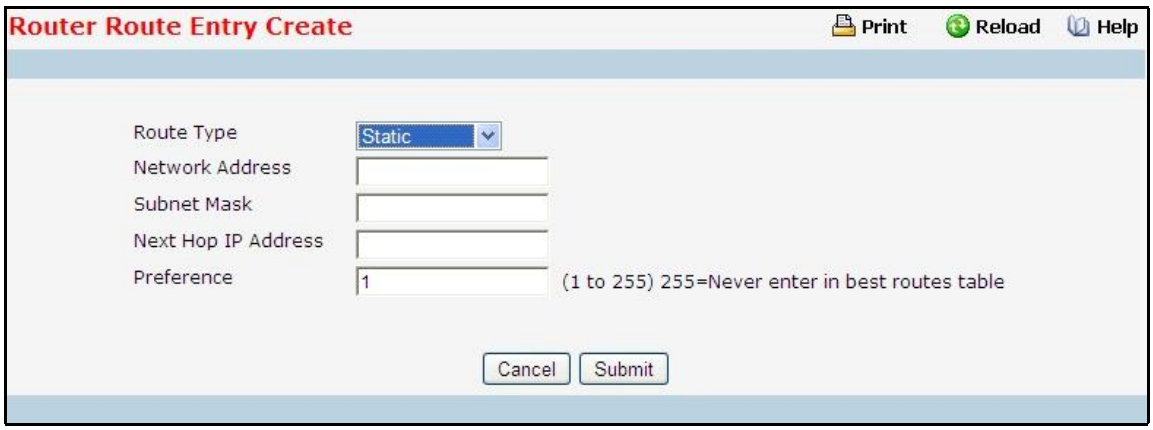
Next Hop IP Address - The outgoing router IP address to use when forwarding traffic to the next router (if any) in the path towards the destination. The next router will always be one of the adjacent neighbors or the IP address of the local interface for a directly attached network.

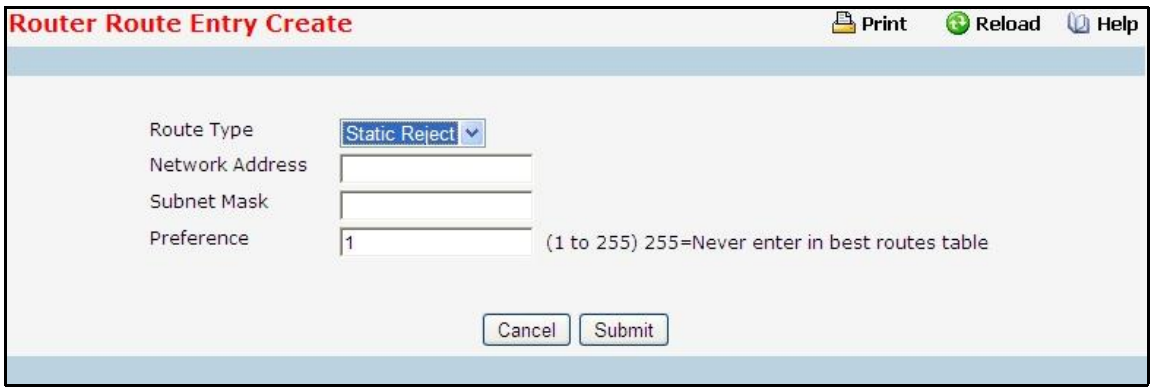
Metric - Administrative cost of the path to the destination. If no value is entered, default is 1. The range is from 0 to 255.

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.

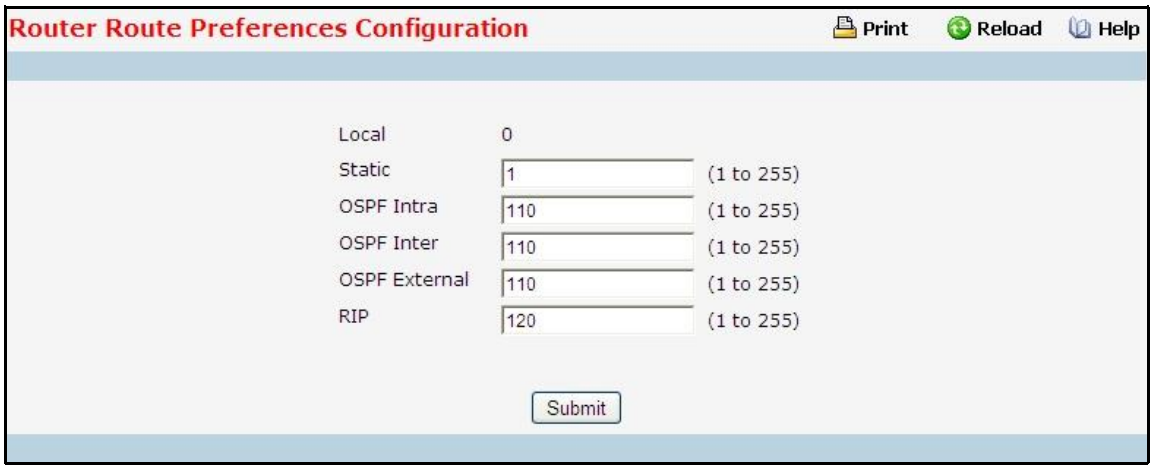

Router Route Entry Create
Print
Reload
Help
Route Type
Static
Network Address
Subnet Mask
Next Hop IP Address
Preference
1
(1 to 255) 255=Never enter in best routes table
Cancel
Submit


Router Route Entry Create
Print
Reload
Help
Route Type
Static Reject
Network Address
Subnet Mask
Preference
1
(1 to 255) 255=Never enter in best routes table
Cancel
Submit

11.6.8.4 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.

OSPF Inter - The OSPF inter route preference value in the router. The default value is 110. The range is 1 to 255.

OSPF External - The OSPF External route preference value in the router. The default value is 110. The range is 1 to 255.

RIP - The RIP route preference value in the router. The default value is 120. The range is 1 to 255.

Non-Configurable Data

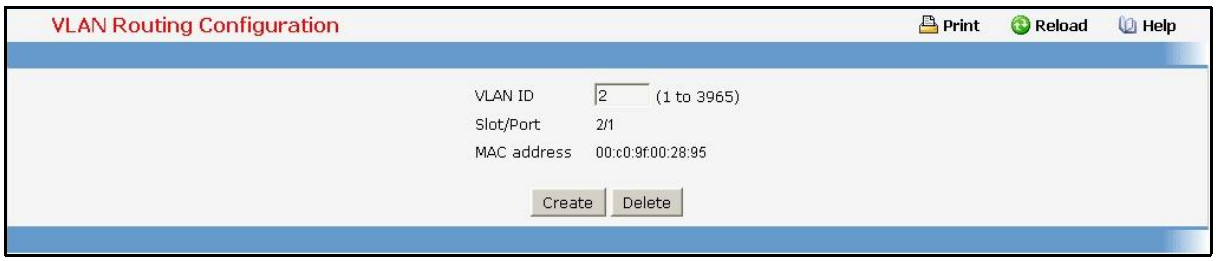
Local - This field displays the local route preference value.

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.

11.6.9 Managing VLAN Routing

11.6.9.1 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.

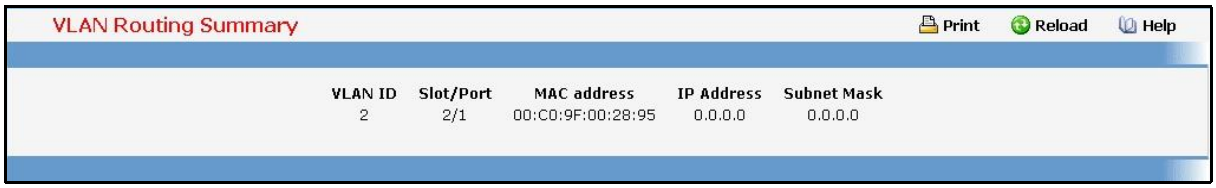
Instructions for creating a VLAN

- 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.

11.6.9.2 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.

11.6.10 Managing VRRP

11.6.10.1 Configuring VRRP

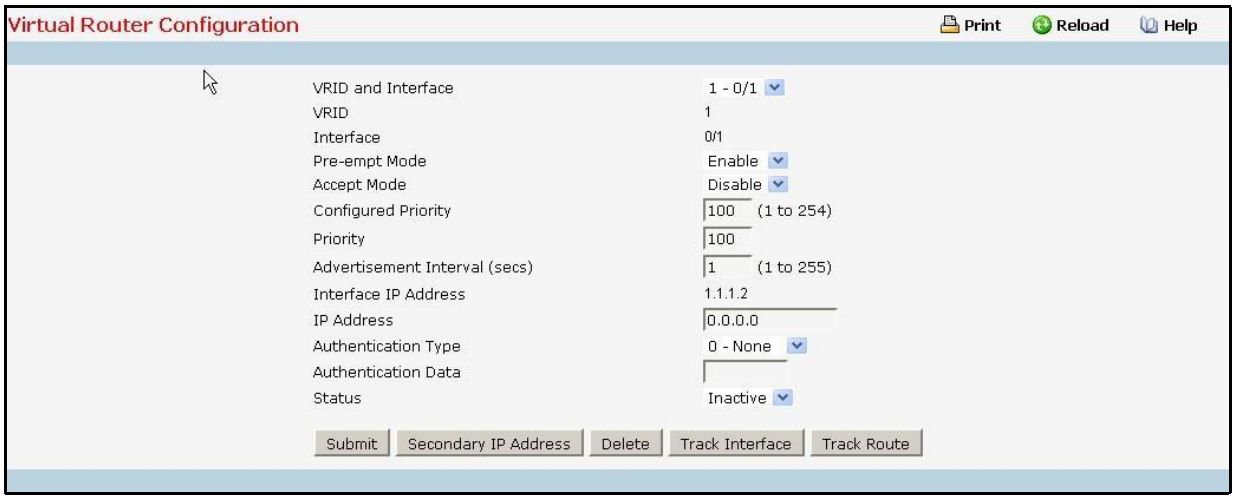
Configurable Data

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.

11.6.10.2 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 .

Interface - 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.

Accept Mode - Select enable or disable from the pull down menu. If you select enable the VRRP master will accept all types of data packets addressed to IP address(es) associated with the virtual router and on selecting disable the VRRP master will discard all types of data packets addressed to IP address(es) associated with the virtual router if it is not the IP address owner. The default is disable.

Configured 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.

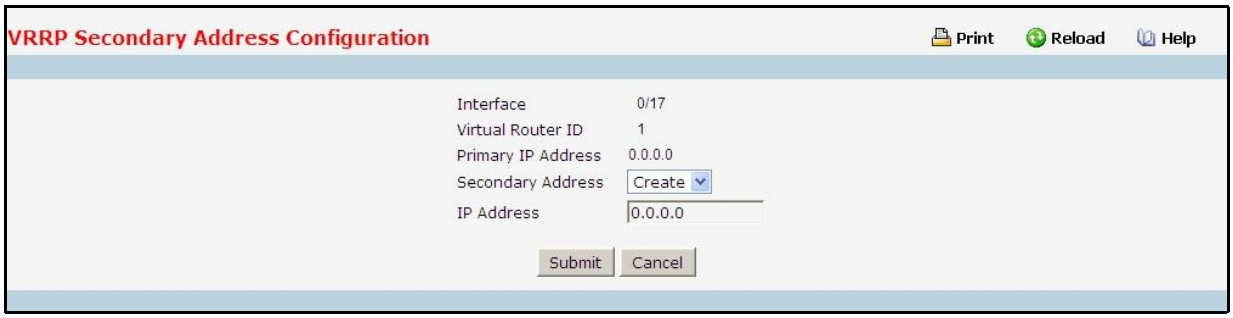
Delete - Delete the selected Virtual Router. Note that the router can not be deleted if there are secondary addresses configured.

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.

11.6.10.3 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

Interface - 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.

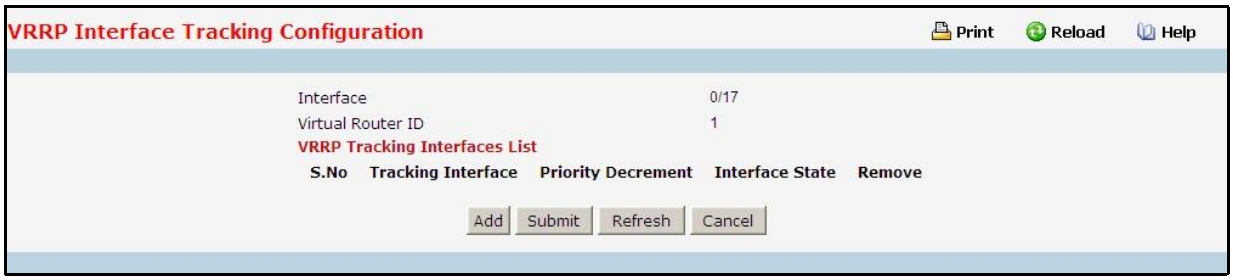
Command Buttons

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.

11.6.10.4 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

Interface - 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

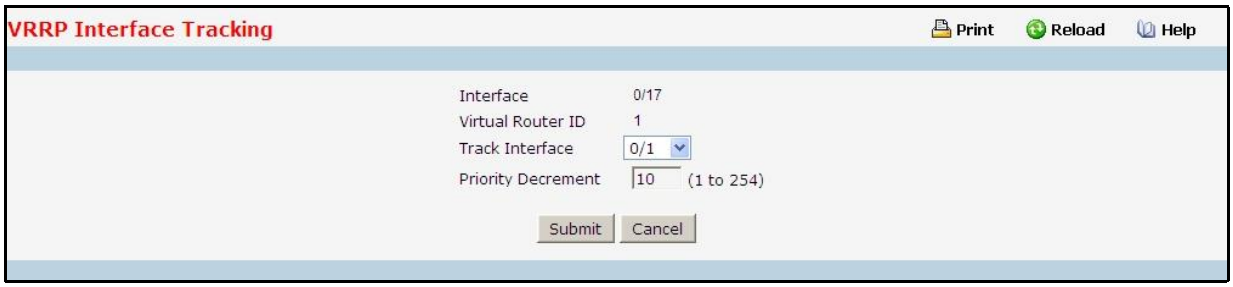
Add - Proceed to the VRRP Track interface screen.

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.

11.6.10.5 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

Interface - The interface for which data is to be displayed.

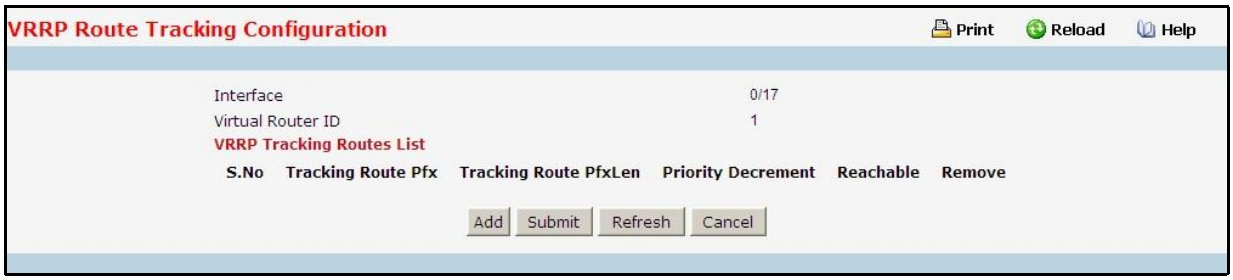
Virtual Router ID - The Virtual Router ID for which data is to be displayed.

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.

11.6.10.6 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

Interface - 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

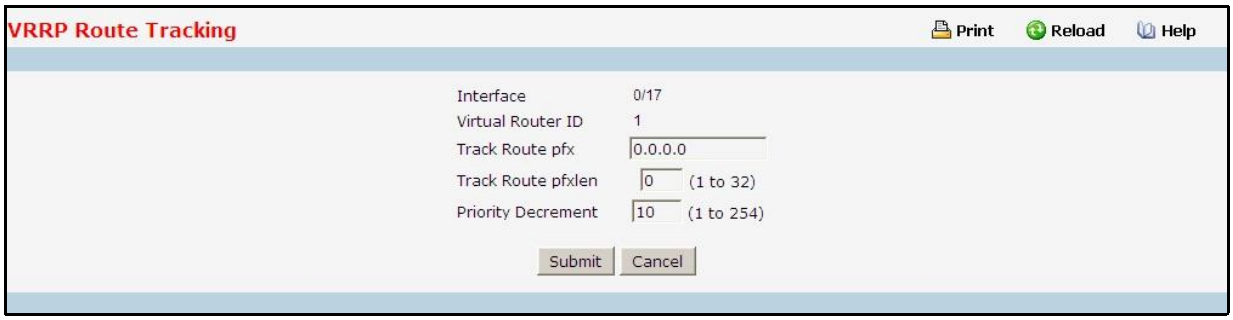
Add - Proceed to the VRRP Track Route screen.

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.

11.6.10.7 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

Interface - The interface for which data is to be displayed.

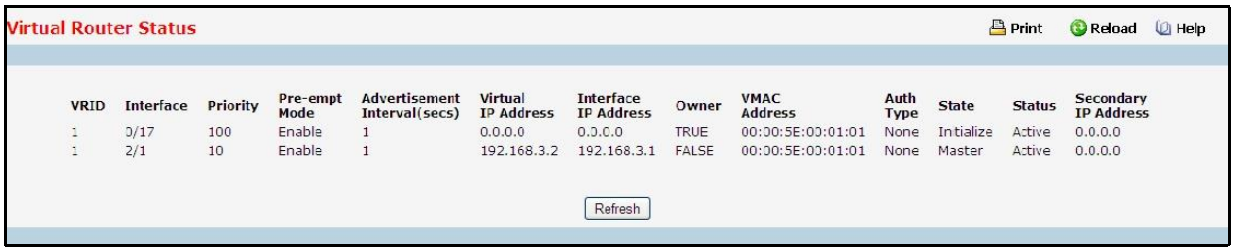
Virtual Router ID - The Virtual Router ID for which data is to be displayed.

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.

11.6.10.8 Viewing Virtual Router Status



Non-Configurable Data

VRID - Virtual Router Identifier.

Interface - 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:

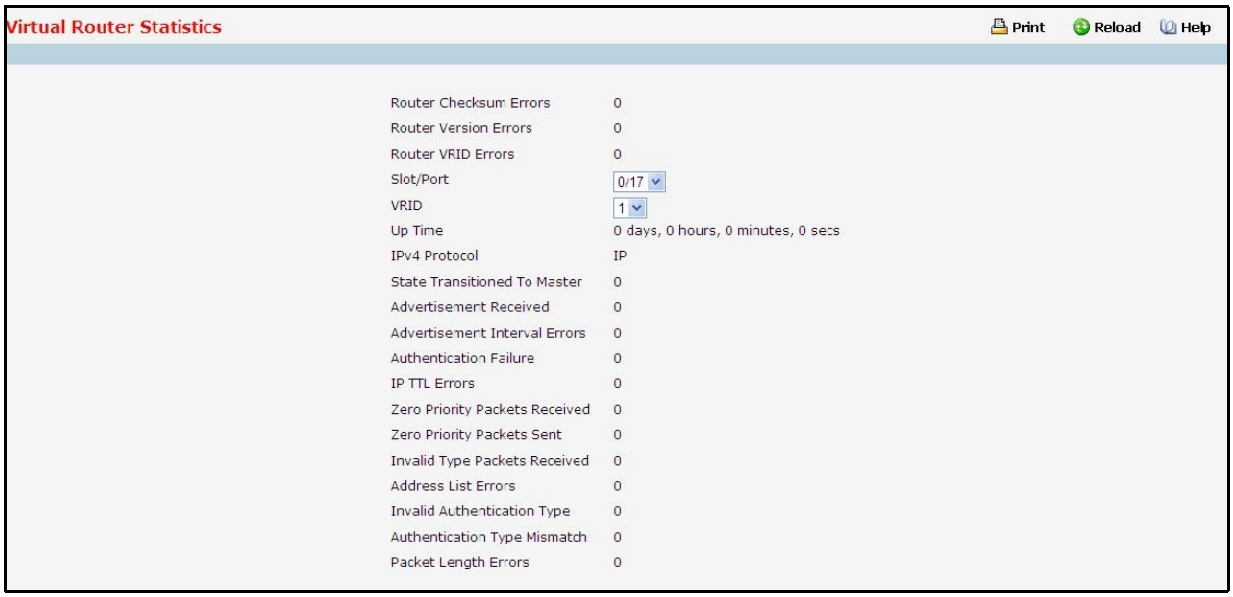
- Inactive
- Active

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.

11.6.10.9 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.

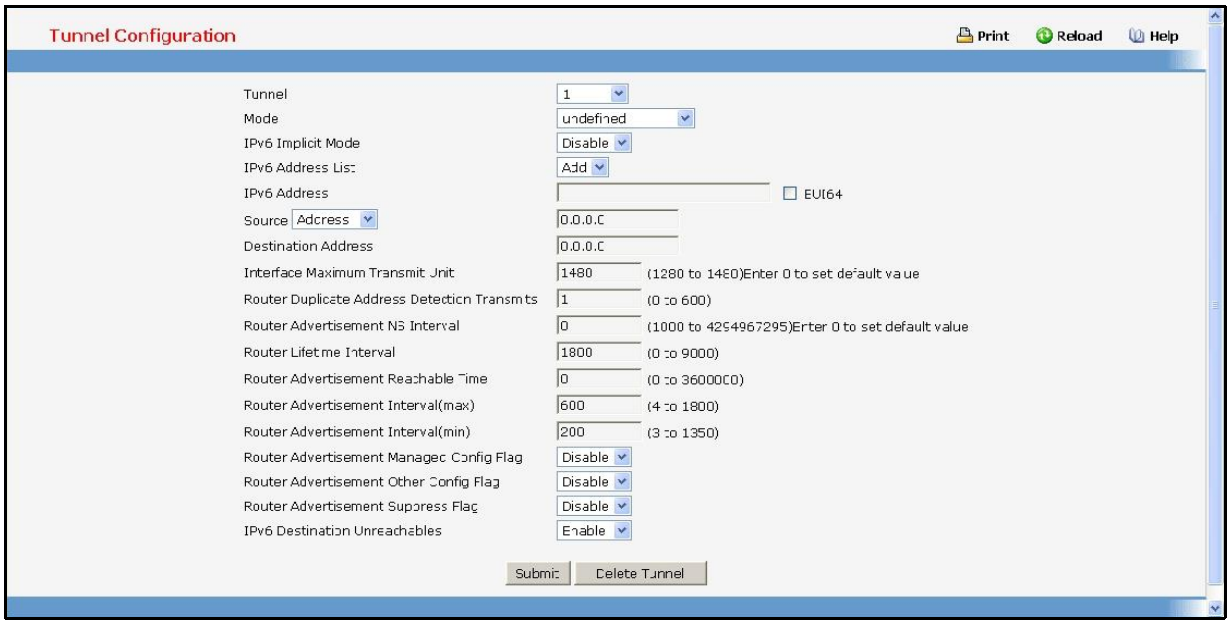
Command Buttons

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

11.6.11 Managing Tunnels

11.6.11.1 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)

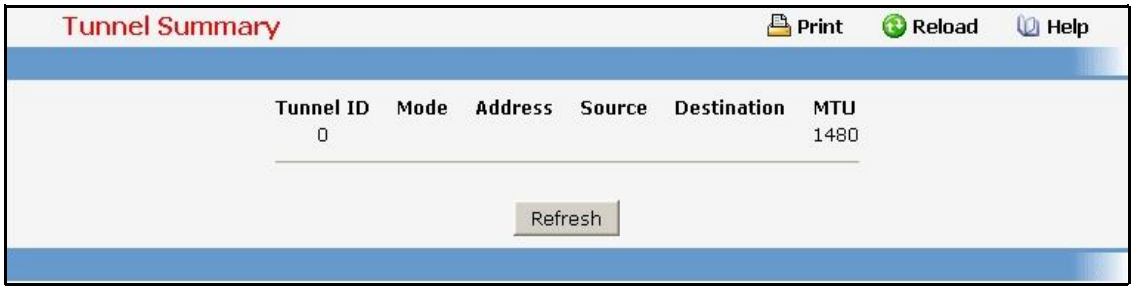
Command Buttons

Submit - Update the system with the values on this screen.

Delete Tunnel - Remove the selected interface.

11.6.11.2 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.

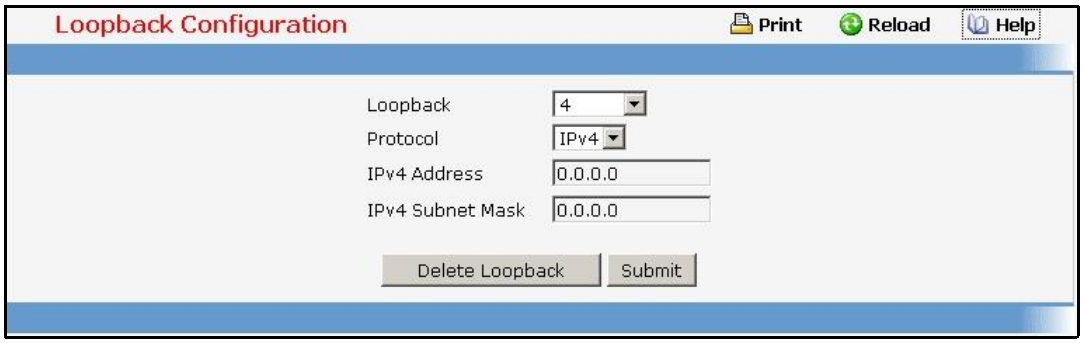
Command Buttons

Refresh - Refresh the page with the latest Tunnel entries.

11.6.12 Managing Loopbacks

11.6.12.1 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.

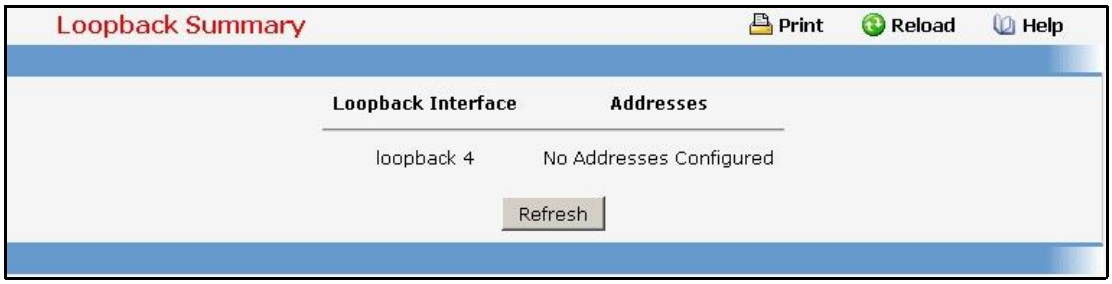
Add Secondary - Add the user specified Secondary IPv4 Address.

Delete Selected Secondary - Remove the selected Secondary IPv4 Address.

Delete Selected Address - Remove the selected IPv6 Address.

11.6.12.2 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.

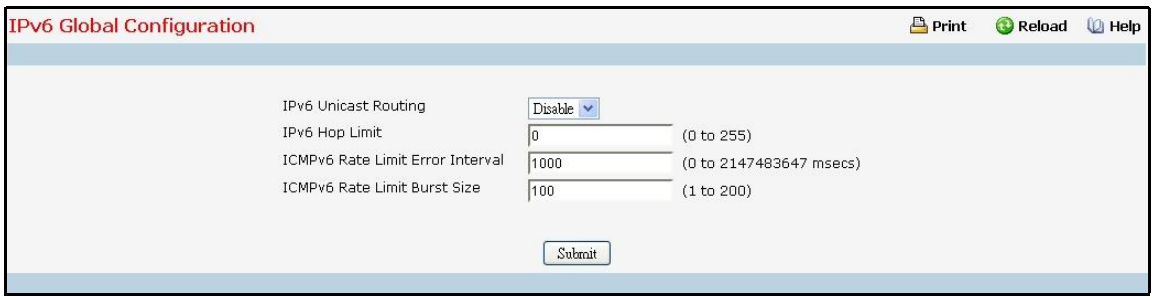
Addresses - A list of the addresses configured on the loopback interface.

Command Buttons

Refresh - Refresh the page.

11.7 IPv6 Menu

11.7.1 Managing IPv6 Global Configuration Page



Configurable Data

IPv6 Unicast Routing - Globally enable or disable IPv6 unicast routing on the entity.

IPv6 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.

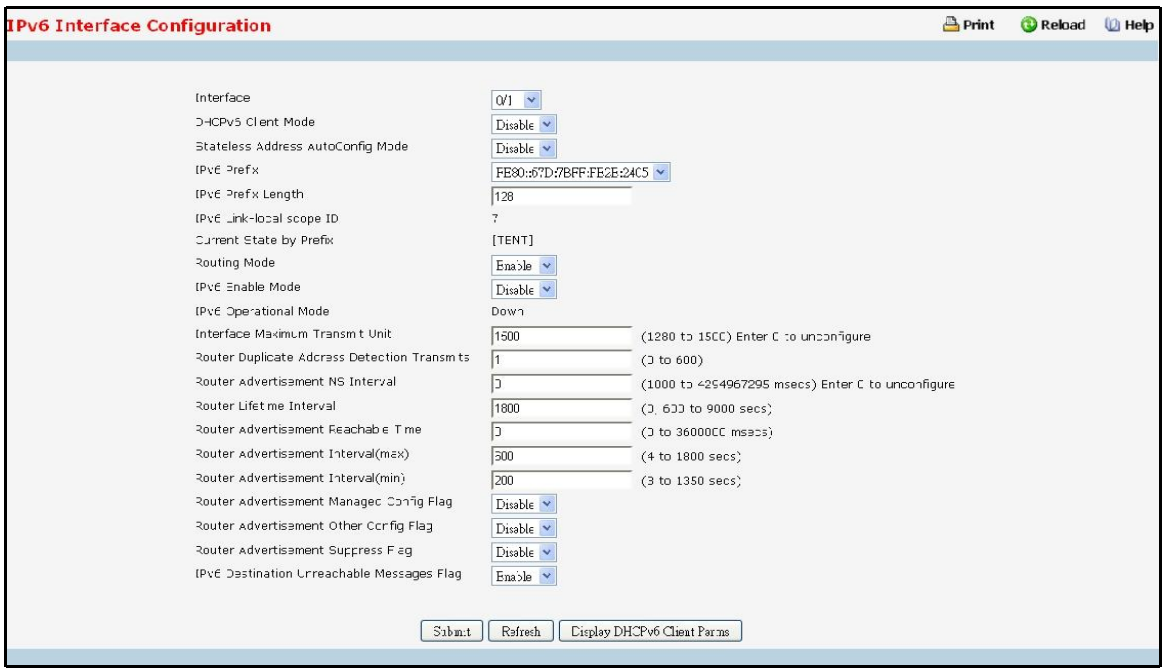
ICMPv6 Rate Limit Error Interval - To control the ICMPv6 error packets user can specify the number of ICMP error packets are allowed per burst interval. By Default Ratelimit is 100 packets/sec i.e burst interval is 1000 msec. To disable ICMP Ratelimiting set this field to '0'.Valid Rate Interval must 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.

11.7.2 Managing 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.

Configurable Data

DHCPv6 Client Mode - Enables or Disables DHCPv6 Client mode on an interface. At any point of time only one interface can act as a Client. Default value is disable.

Stateless Address AutoConfig Mode - Enables or Disables Stateless Address AutoConfig mode on an interface. Default value is disable.

IPv6 Prefix - Select "Add" to Add new IPv6 prefix. Select "None" to configure parameters other than the IPv6 Prefix. Select one of the listed and configured IPv6 addresses or link local address to view or configure related fields.

IPv6 Prefix - Use it to enter the IPv6 prefix to be added.

IPv6 Prefix Length - Use it to specify the IPv6 prefix length. 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). Preferred lifetime must be in range (0 to 4294967295) seconds.

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 Enable 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(max) - Specifies maximum time allowed between sending router advertisements from the interface. Range of maximum advertisement interval is (4 to 1800).Default value is 600.

Router Advertisement Interval(min) -Specifies minimume time allowed between sending router advertisements from the interface. Range of maximum advertisement interval is (3 to 1350).Default value is 200.

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.

IPv6 Link-local scope ID - Specifies Link-Local address's scope ID on IPv6 interface.

Command Buttons

Submit - Send the updated configuration to the switch. Configuration changes take effect immediately. These changes will not be retained across a power cycle unless a save is performed.

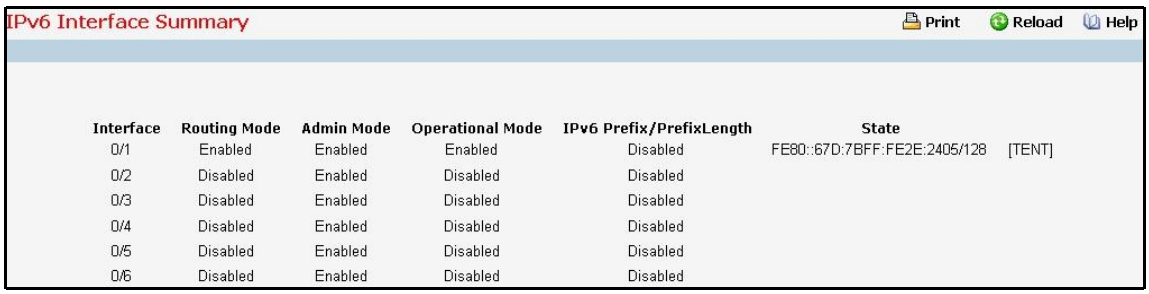
Delete - Delete the IPv6 Address configured on an interface.

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

Delete IPv6 Prefix - Deletes the IPv6 Address configured on selected interface. IPv6 Address acquired through DHCP, Auto-Configured or link-local addresses cannot be deleted by this button.

Display DHCPv6 Client Parms - Displays DHCPv6 Client parameters on an interface.

11.7.3 Viewing IPv6 Interface Summary Page



Interface	Routing Mode	Admin Mode	Operational Mode	IPv6 Prefix/PrefixLength	State	
0/1	Enabled	Enabled	Enabled	Disabled	FE80::67D:7BFF:FE2E:2405/128	[TENT]
0/2	Disabled	Enabled	Disabled	Disabled		
0/3	Disabled	Enabled	Disabled	Disabled		
0/4	Disabled	Enabled	Disabled	Disabled		
0/5	Disabled	Enabled	Disabled	Disabled		
0/6	Disabled	Enabled	Disabled	Disabled		

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.

Operational Mode - Specifies operational mode of an interface.

IPv6 Prefix - Specifies configured IPv6 Prefix on an interface.

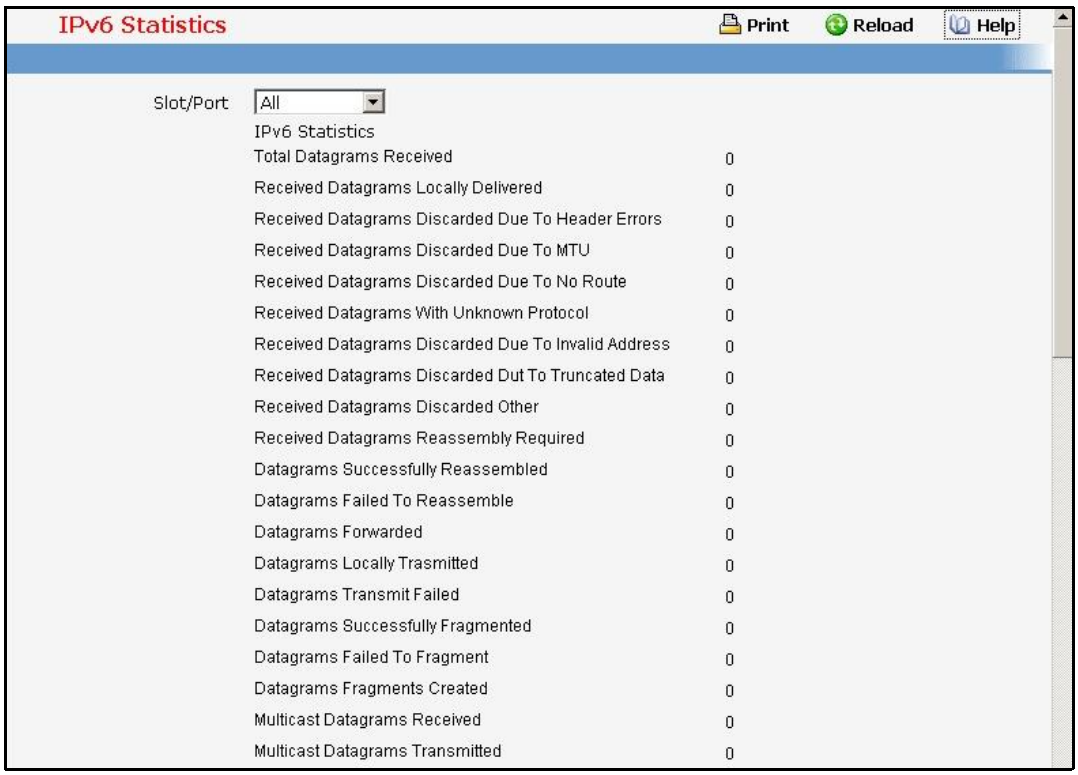
Prefix Length - Specifies configured Prefix Length on an interface.

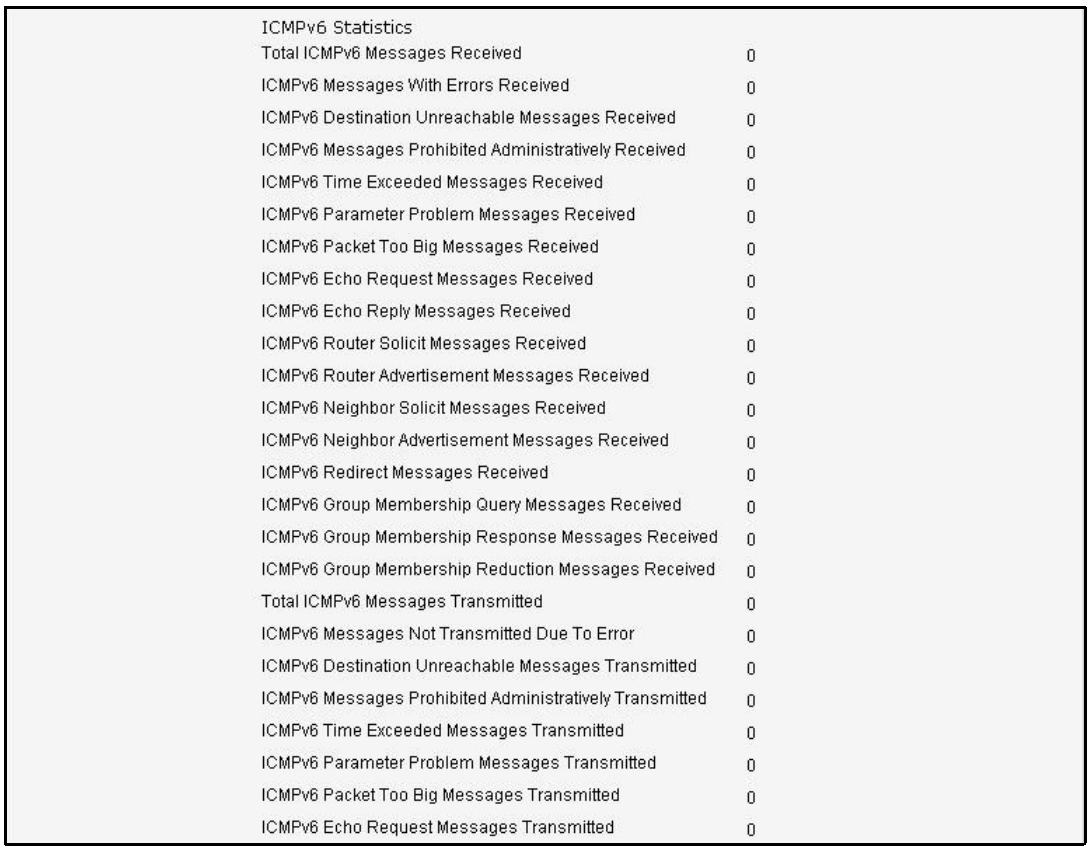
State - Specifies the state of the IPv6 Prefix on the interface. The valid values are: DHCP - If the address is acquired by the DHCPv6 Client running on this interface. AUTO - If the address is Auto-configured on the interface. ACTIVE - If the address is manually configured on the interface or is link-local and is active. TENT - If the address (added manually, link-local, auto-configured or acquired through DHCP) is not operationally active on the interface.

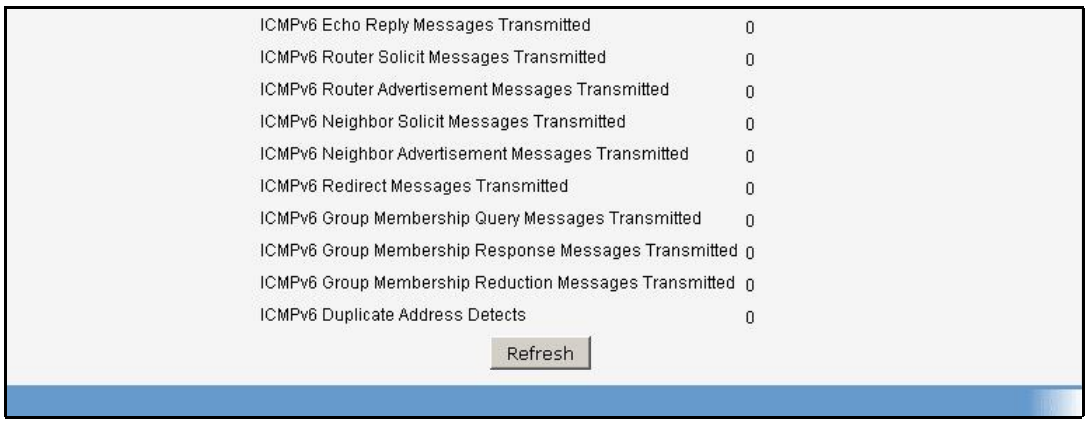
Command Buttons

Refresh - Refreshes the screen with most recent data.

11.7.4 Viewing IPv6 Interface Statistics 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.

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.

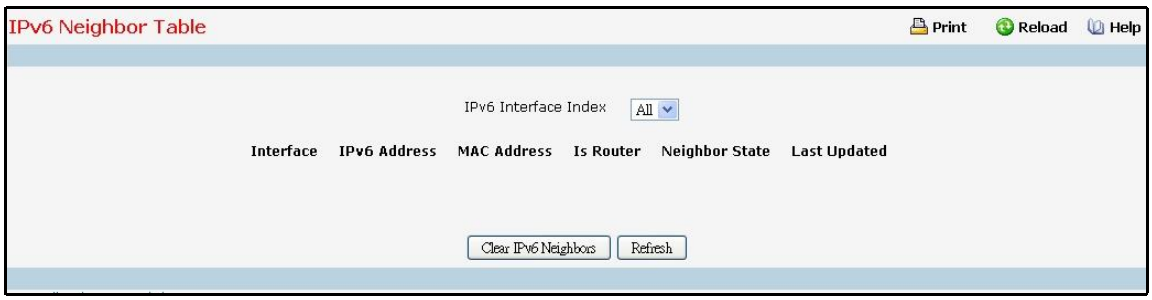
ICMPv6 Group Membership Reduction Messages Transmitted - The number of ICMPv6 Group Membership Reduction messages sent.

ICMPv6 Duplicate Address Detects - The number of duplicate Addresesses detected by the interface.

Command Buttons

Refresh - Refreshes the screen with most recent data.

11.7.5 Viewing IPv6 Neighbor Table Information Page



Selection Criteria

IPv6 Interface Index - 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:

- Unknown - 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.

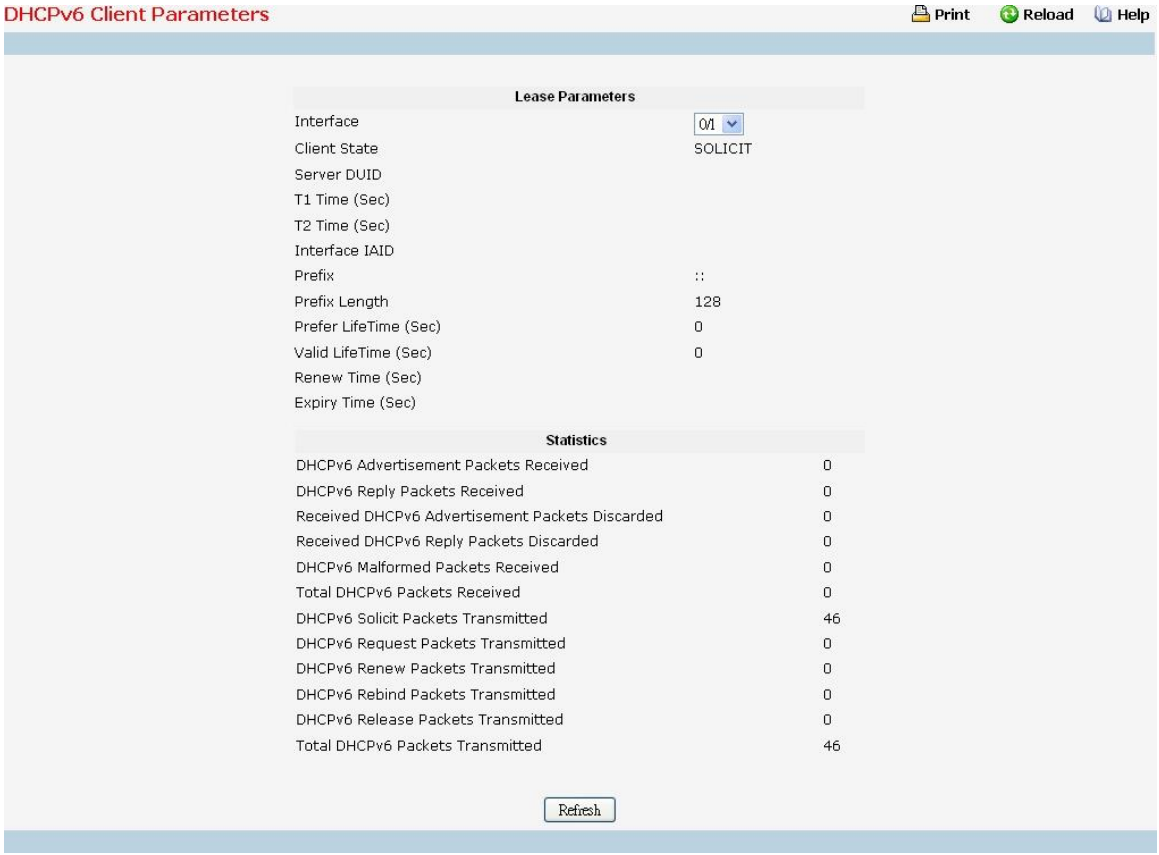
Last Updated - Time since the address was confirmed to be reachable.

Command Buttons

Refresh - Refreshes the screen with most recent data.

Clear IPv6 Neighbors - Clear IPv6 neighbors on selected interface or all interfaces.

11.7.6 Viewing DHCPv6 Client Parameters



Selection Critieria

Interface - Select the interface for which data is to be displayed.

Non-Configurable Data

Lease Parameters

Client State - The State of the DHCPv6 Client on this interface. The valid values are:INACTIVE, SOLICIT, REQUEST, ACTIVE, RENEW, REBIND, RELEASE.

Server DUID - The DHCPv6 Unique Identifier of the DHCPv6 Server on this interface.

T1 Time (Sec) - The T1 (in seconds) time as indicated by the DHCPv6 Server. T1 value indicates the time interval after which the address is requested for renewal.

T2 Time (Sec) - The T2 (in seconds) time as indicated by the DHCPv6 Server. T2 value indicates the time interval after which the Client sends Rebind message to the Server incase there are no replies to the Renew messages.

Interface IAID - An identifier for an identity association chosen by this Client.

Prefix - The IPv6 Prefix leased by the DHCPv6 Server for this interface.

Prefix Length - The Prefix length corresponding to the IPv6 Prefix leased by the DHCPv6 Server.

Prefer LifeTime (Sec) - The preferred life time (in seconds) of the IPv6 Address leased by the DHCPv6 Server.

Valid LifeTime (Sec) - The valid life time (in seconds) of the IPv6 Address leased by the DHCPv6 Server.

Renew Time (Sec) - The time remaining (in seconds) to send a DHCPv6 Renew request to DHCPv6 Server for the leased address.

Expiry Time (Sec) - The time (in seconds) when the DHCPv6 leased address expires.

Statistic

DHCPv6 Advertisement Packets Received - Number of DHCPv6 Advertisement packets received on the selected interface.

DHCPv6 Reply Packets Received - Number of DHCPv6 Reply packets received on the selected interface.

Received DHCPv6 Advertisement Packets Discarded - Number of DHCPv6 Advertisement packets discarded on the selected interface.

Received DHCPv6 Reply Packets Discarded - Number of DHCPv6 Reply packets discarded on the selected interface.

DHCPv6 Malformed Packets Received - Number of DHCPv6 packets that are received malformed on the selected interface.

Total DHCPv6 Packets Received - Total number of DHCPv6 packets received on the selected interface.

DHCPv6 Solicit Packets Transmitted - Number of DHCPv6 Solicit packets transmitted on the selected interface.

DHCPv6 Request Packets Transmitted - Number of DHCPv6 Request packets transmitted on the selected interface.

DHCPv6 Renew Packets Transmitted - Number of DHCPv6 Renew packets transmitted on the selected interface.

DHCPv6 Rebind Packets Transmitted - Number of DHCPv6 Rebind packets transmitted on the selected interface.

DHCPv6 Release Packets Transmitted - Number of DHCPv6 Release packets transmitted on the selected interface.

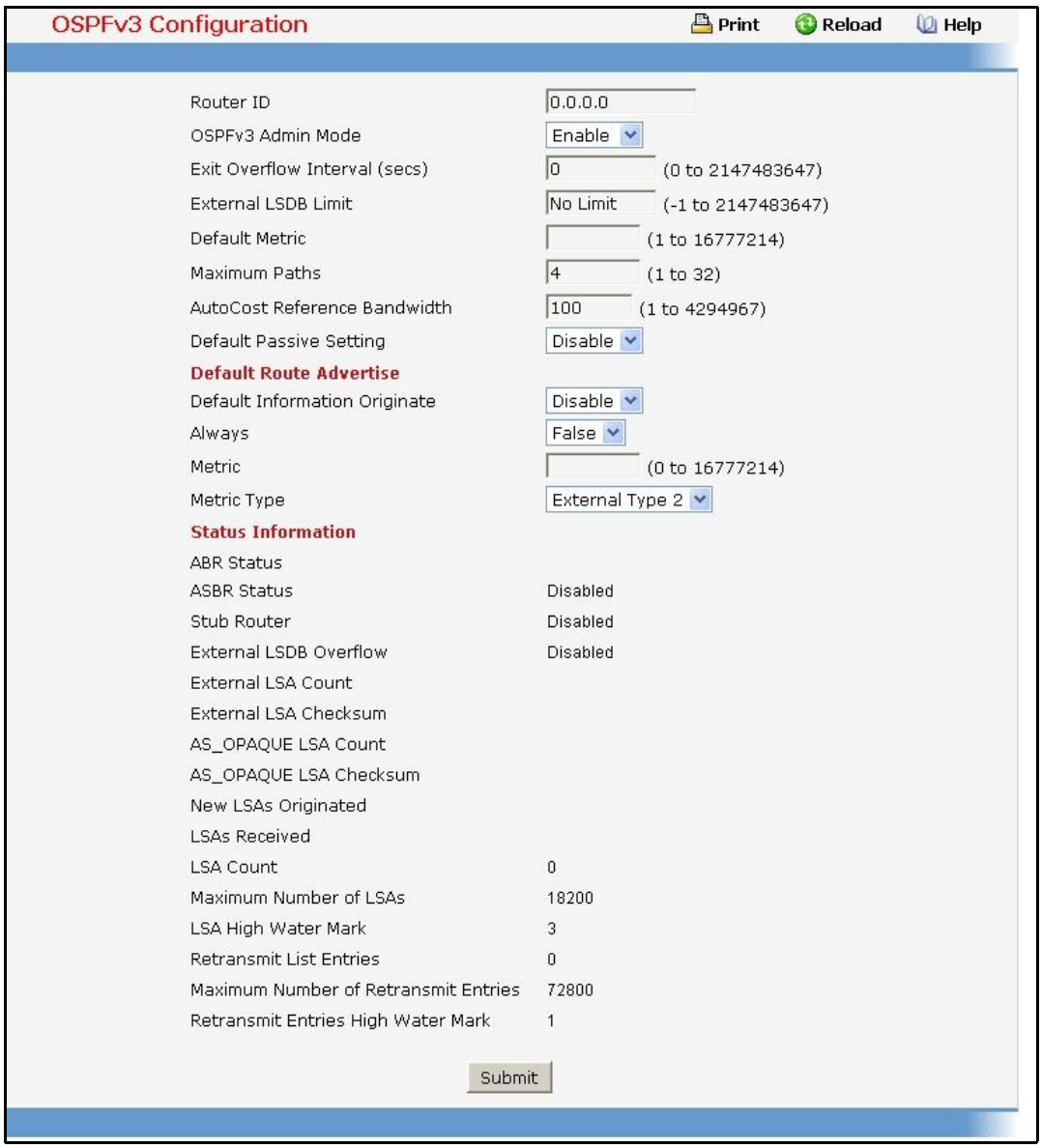
Total DHCPv6 Packets Transmitted - Total number of DHCPv6 packets transmitted on the selected interface.

Command Buttons

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

11.7.7 Managing OSPFv3 Protocol

11.7.7.1 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.

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.

Helper Support Mode - Configures how unit will act when a neighbor performs a warm restart. The possible values are:

Planned - Indicates that OSPF should only help a restarting neighbor during planned events.

Always - Indicates that OSPF help a restarting neighbor during all planned and unplanned warm restart events.

Disabled - Disables OSPF from acting as a helpful neighbor.

Helper Strict LSA Checking - When enabled, the unit will exit helper mode whenever the topology changes.

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.

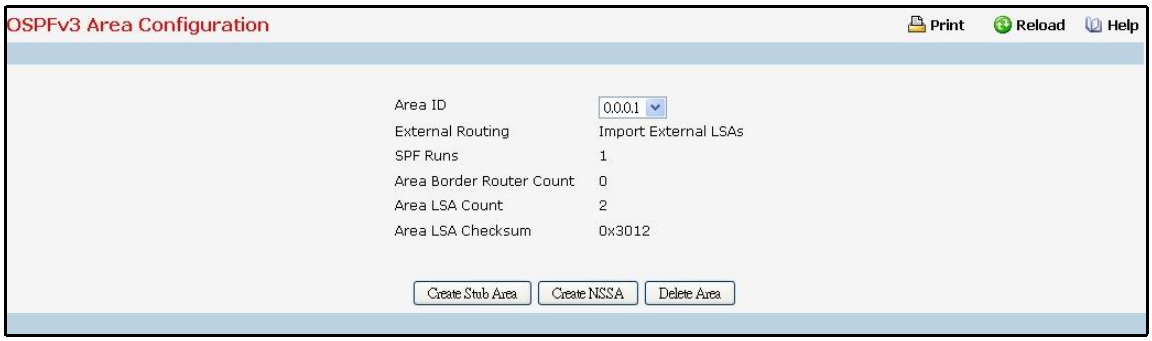
Maximum Number of Retransmit Entries - The maximum number of LSAs that can be waiting for acknowledgment at any given time.

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.

11.7.7.2 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 65535. 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).

Default Metric Type - Select the type of metric specified in the Metric Value field.

- 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). By default it is 40.

No-Redistribute Mode - Enable or Disable the Redistribute Mode into NSSA. By default it is Enable..

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 65535).

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.

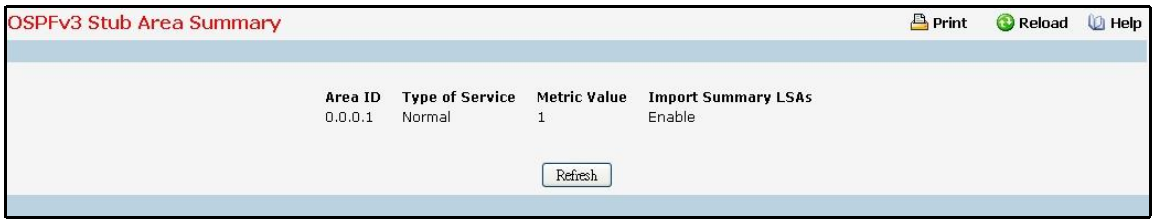
Delete NSSA - Delete the NSSA designation. The area will be returned to normal state.

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.

Delete Area - Deletes the area if none of the OSPF router interfaces are in that area.

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

11.7.7.3 Viewing OSPFv3 Stub Area Summary Page



Non-Configurable Data

Area ID - The Area ID of the Stub area

Type of Service - Displays the type of service of the Stub Area.

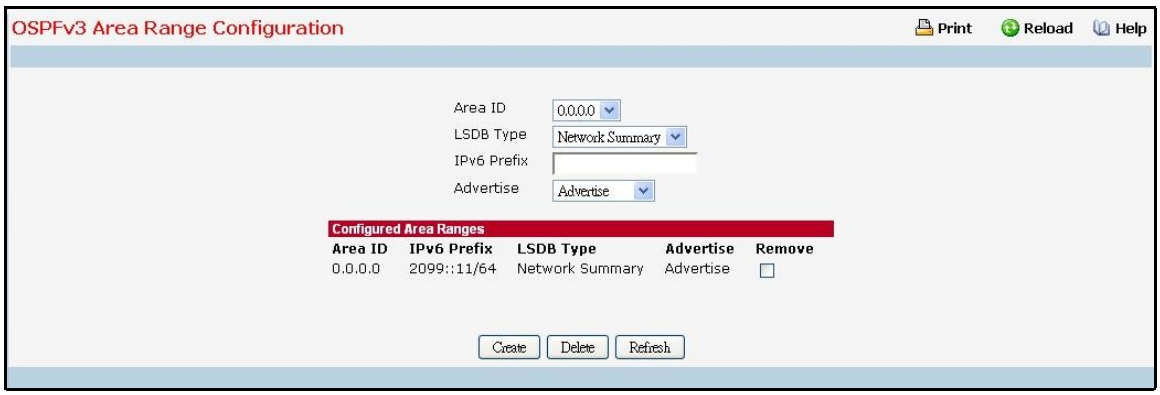
Metric Value - The metric value applied to the default route advertised into the area.

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.

11.7.7.4 Configuring OSPFv3 Area Range Configuration Page



Selection Criteria

Area ID - Selects the area for which data is to be configured.

LSDB Type - Select the type of Link Advertisement associated with the specified area and address range. The default type is 'Network Summary'.

Advertise - Select 'Advertise' or 'Do Not Advertise' from the pull-down menu. If you selected Advertise, the address range will be advertised outside the area via a Network Summary or NSSA External LSA. The default is 'Advertise'.

Configurable Data

IPv6 Prefix - Enter the IPv6 Prefix/Prefix Length for the address range for the selected area.

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.

Advertise - The Advertisement mode for the address range and area.

Remove - Check box to remove the particular entry from the table.

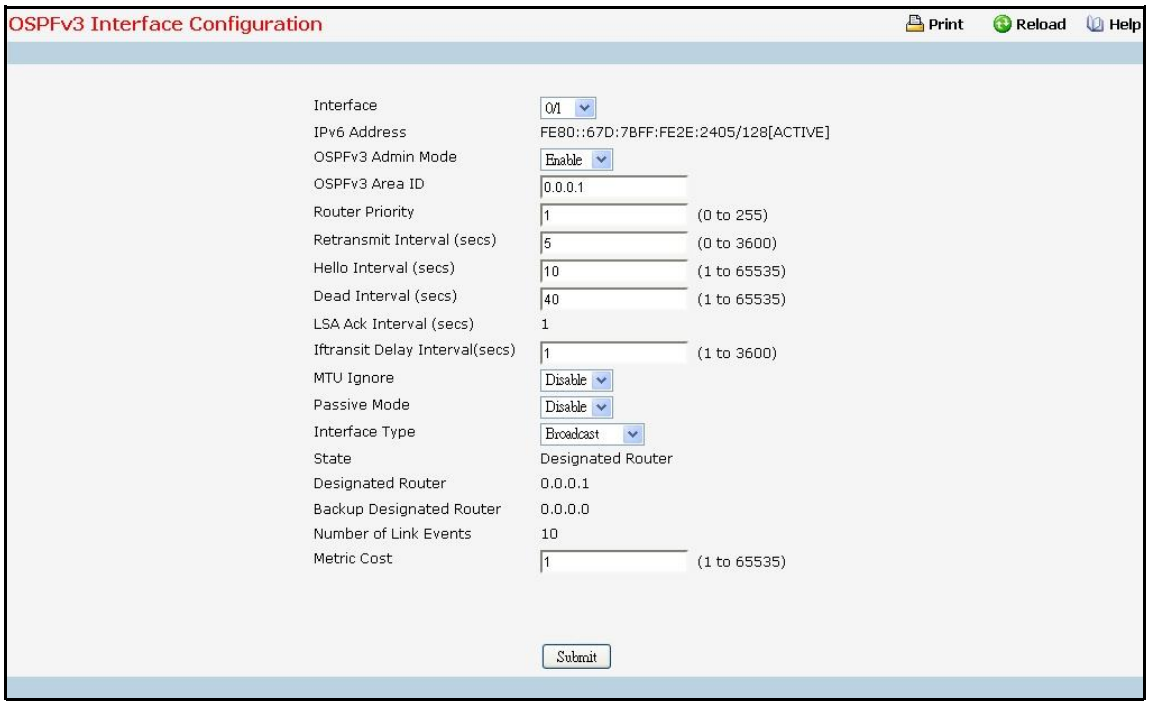
Command Buttons

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.

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

11.7.7.5 Configuring OSPFv3 Interface Configuration Page



Selection Criteria

Interface - 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.

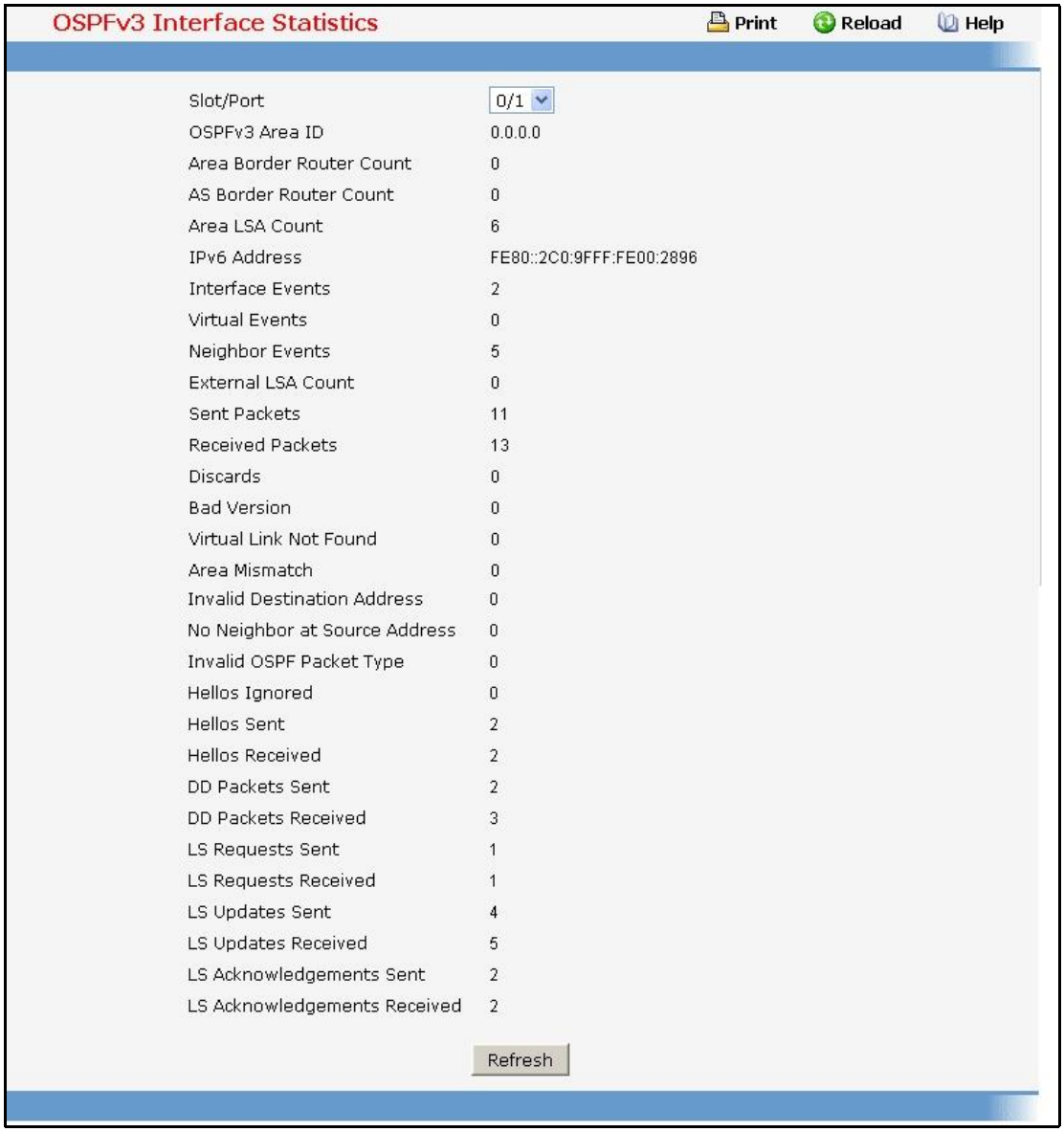
Number of Link Events - This is the number of times the specified OSPFv3 interface has changed its state. This field is only displayed if the OSPFv3 admin mode is enabled.

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.

11.7.7.6 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

Interface - 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.

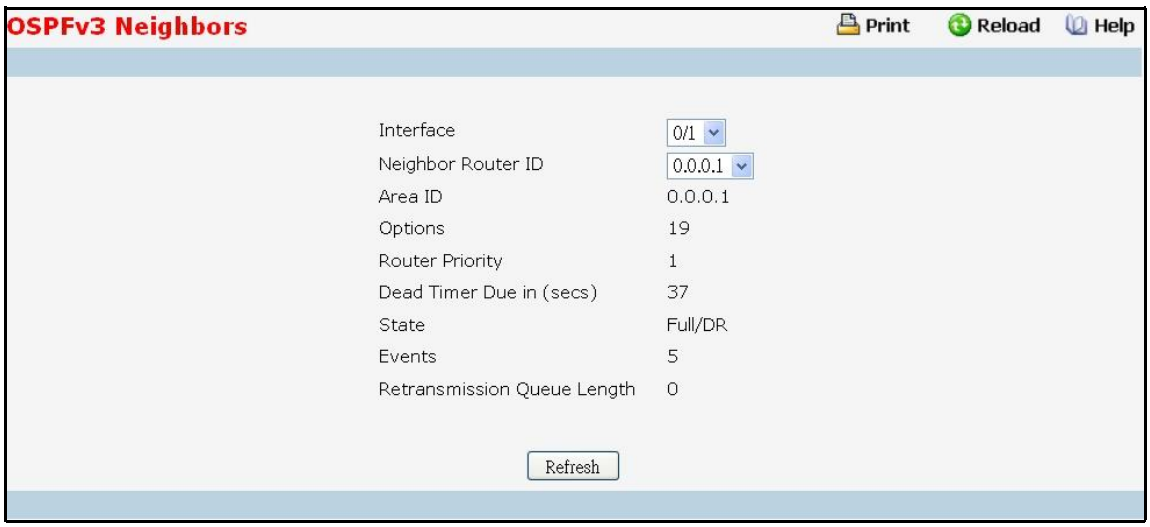
LS Acknowledgements Received - The number of LS acknowledgements received on this interface by this router.

Command Buttons

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

11.7.7.7 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

Interface - 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.

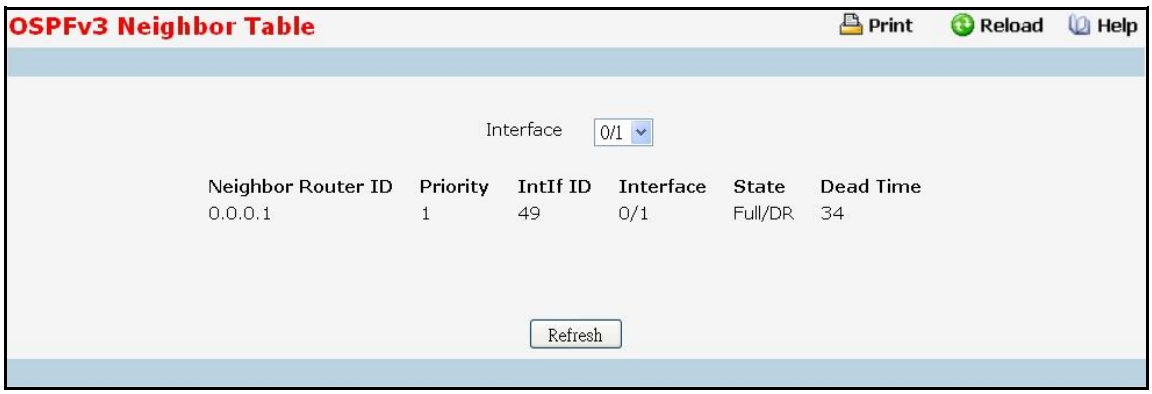
Retransmission Queue Length - Length of the selected neighbor's retransmit queue.

Command Buttons

Refresh - Refresh the page with the latest OSPFv3 neighbor information for the selected interface and Neighbor Router ID.

11.7.7.8 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

Interface - 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.

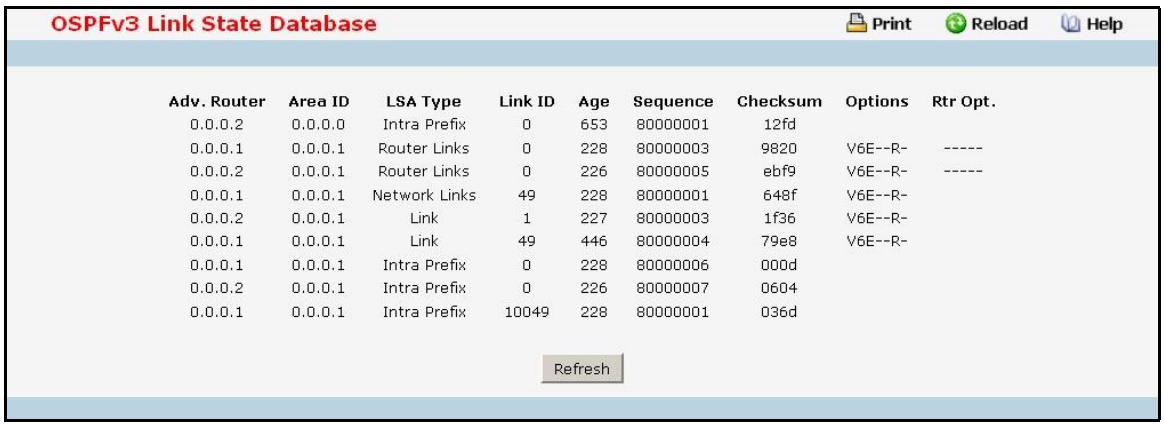
State - State of the relationship with this neighbor.

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 - Refresh the page with the latest OSPFv3 neighbor information for the selected interface.

11.7.7.9 Viewing OSPFv3 Link State Database Information Page



Non-Configurable Data

Adv.Router- The Router ID value of the advertising router for this LSA.

Area ID- The Area to which this LSA belongs to.

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

Link 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.

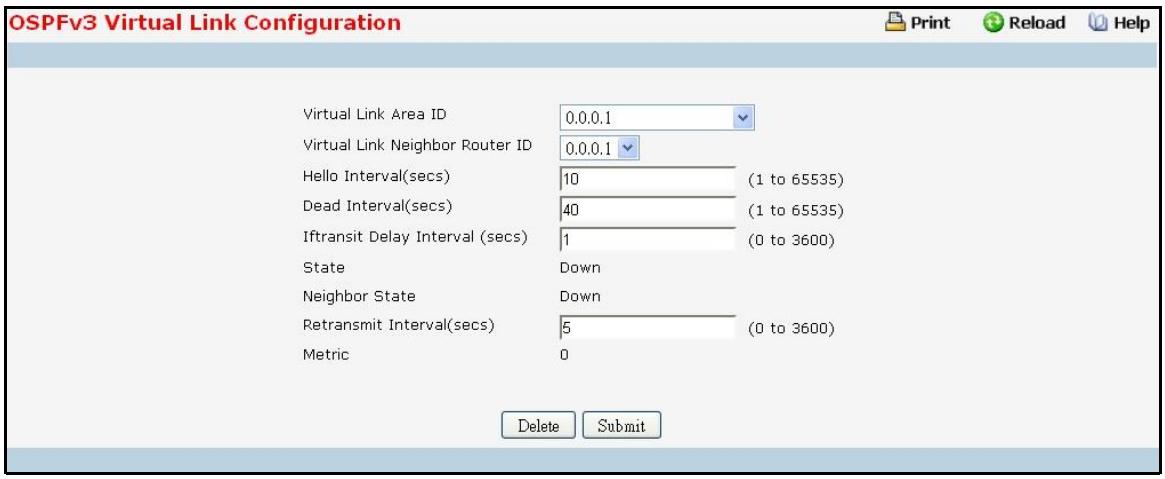
Options - The Options field in the link state advertisement header indicates which optional capabilities are associated with the advertisement.

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.

11.7.7.10 Configuring OSPFv3 Virtual Link Configuration Page



Selection Criteria

Virtual Link Area ID - Select this option from the dropdown menu to create a new virtual link or modify the attributes of an existing virtual link.

Area ID - Select the area id to create the virtual link through.

Virtual Link Neighbor Router ID - Select the router id of an existing virtual link to modify its attributes.

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.

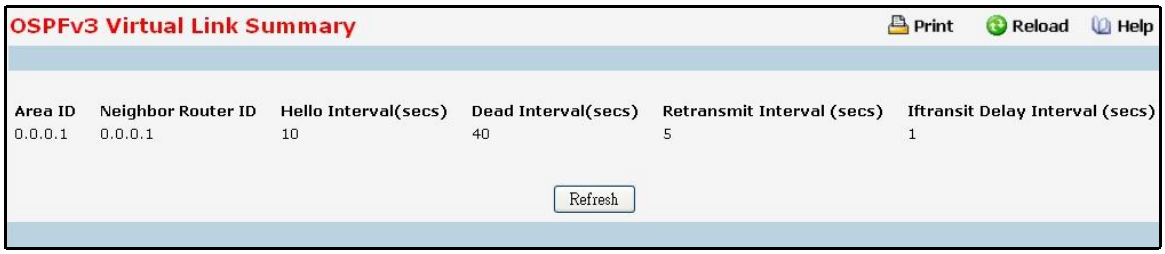
Command Buttons

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.

Create - Creates the specified virtual link.

Delete - Removes the specified virtual link from the router configuration.

11.7.7.11 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.

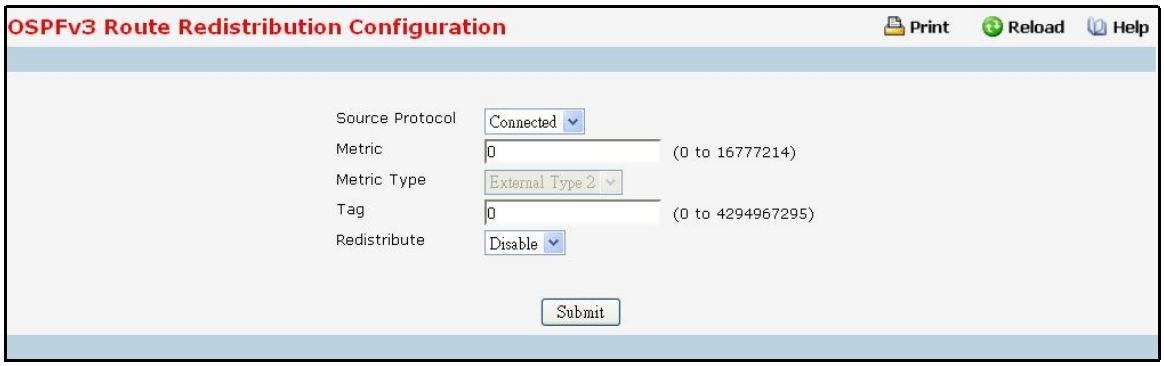
Iftransit Delay Interval - The OSPFv3 Transit Delay for the virtual link in units of seconds. It specifies the estimated number of seconds it takes to transmit a link state update packet over this interface.

Command Buttons

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

11.7.7.12 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.



Selection Criteria

Source Protocol - This selects the Source Protocol to be configured for redistribution by OSPF. The following options are:

- Connected
- Static

By default it is Connected.

Metric Type - Sets the OSPFv3 metric type of redistributed routes. The following options are:

- External Type 1
- External Type 2

By default it is External Type 2.

Redistribute - Enables or disables the redistribution for the selected source protocol. It has to be enabled to be able to configure any of the route redistribution attributes. By default it is Disable.

Configurable Data

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)

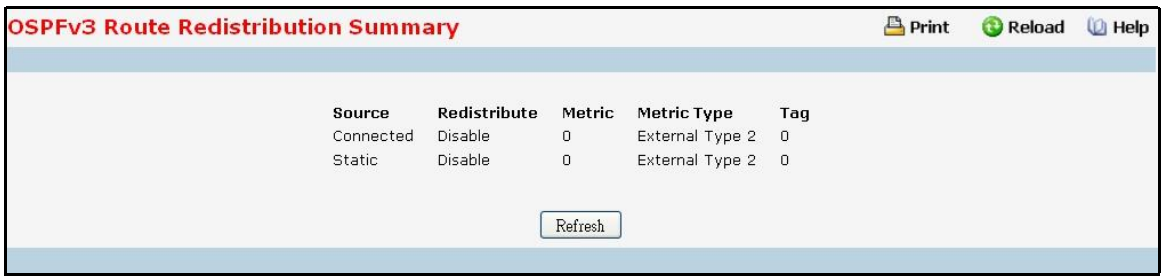
Tag - Sets the tag field in routes redistributed. This field displays the tag if the source was pre-configured, else a default tag value of 0 is displayed. The valid values are (0 to 4294967295)

Command Buttons

Submit - Send the updated configuration to the router. Configuration changes take effect immediately.

11.7.7.13 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.

Redistribute - Enables or disables the redistribution for the selected source protocol.

Metric- The Metric of redistributed routes for the given Source Protocol.

Metric Type - The OSPFv3 metric type of redistributed routes.

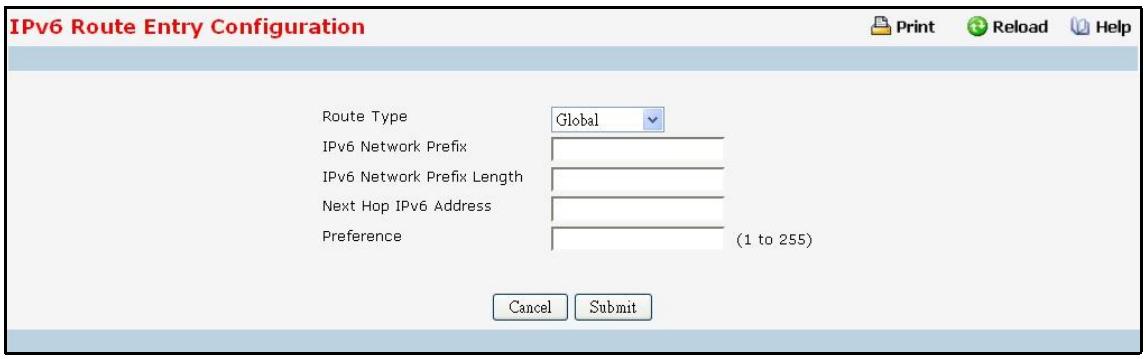
Tag - The tag field in routes redistributed.

Command Buttons

Refresh - Refresh the data on the screen with latest OSPFv3 Route Redistribution Configuration data in the switch.

11.7.8 Managing IPv6 Routes

11.7.8.1 Configuring IPv6 Route Entry Configuration Page



Selection Criteria

Interface - Enter the unit, slot and port number for the Link-local IPv6 Next Hop Address. This field is displayed only if Link-local Next-hop Selector is selected as Link-local.

Route Type - Specify if the Next Hop IPv6 Address is a Global IPv6 Address or a Link-local IPv6 Address or a Static-Reject IPv6 Address.

Configurable Data

IPv6 Network Prefix- Enter an IPv6 Network Address Prefix.

IPv6 Network Prefix Length - Enter the IPv6 Network Address 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.

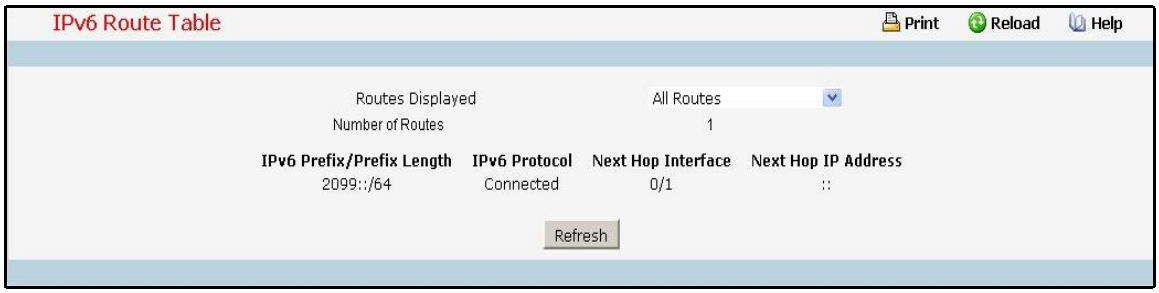
Preference - Enter a Preference Value for the given route. It is optional. If left blank, the preference value configured for the static route type is picked up for the route. The valid range is (1 to 255).

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.

11.7.8.2 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 - Displays the total number of active routes/best routes in the route table. IPv6

Prefix - Displays the Network Prefix for the Active Route.

IPv6 Prefix Length - Displays the Network Prefix Length for the Active Route.

IPv6 Protocol - Displays the Type of Protocol for the Active Route.

Next Hop Interface - Displays the Interface over which the Route is Active.

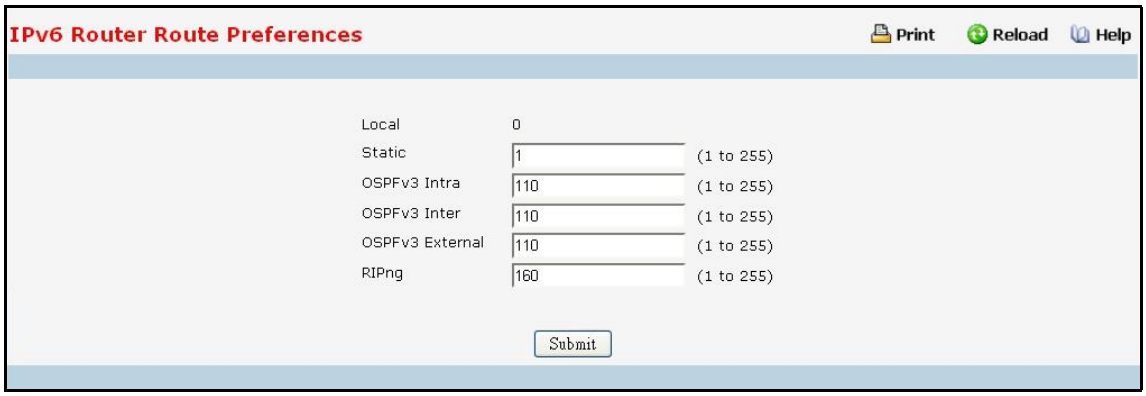
Next Hop Address - Displays the Next Hop IPv6 Address for the Active Route.

Command Buttons

Refresh - Refresh IPv6 route information on the page.

11.7.8.3 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.

RIPng - The RIPng preference value .The default value is 160.

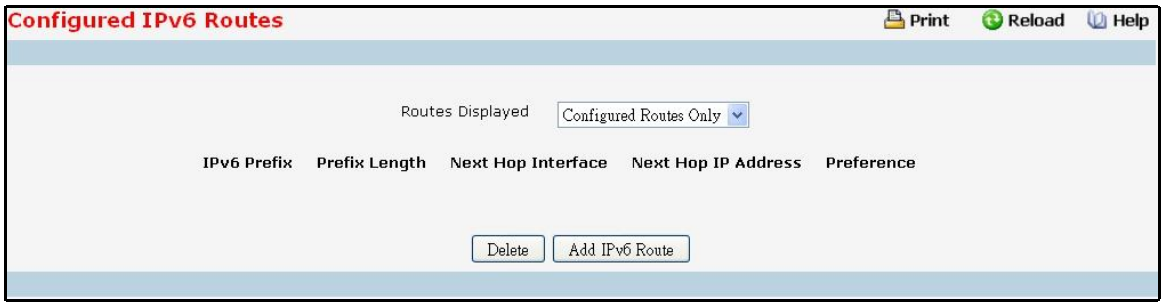
Non-Configurable Data

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.

11.7.8.4 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 - Displays the Network Prefix for the Configured Route.

IPv6 Prefix Length - Displays the Network Prefix Length for the Configured Route..

Next Hop Interface - Displays the Interface over which the Route is Active. For a Reject Route the next hop would be a "Null0" interface.

Next Hop IP Address- Displays the Next Hop IPv6 Address for the Configured Route.

Preference - Displays the Route Preference of the Configured Route.

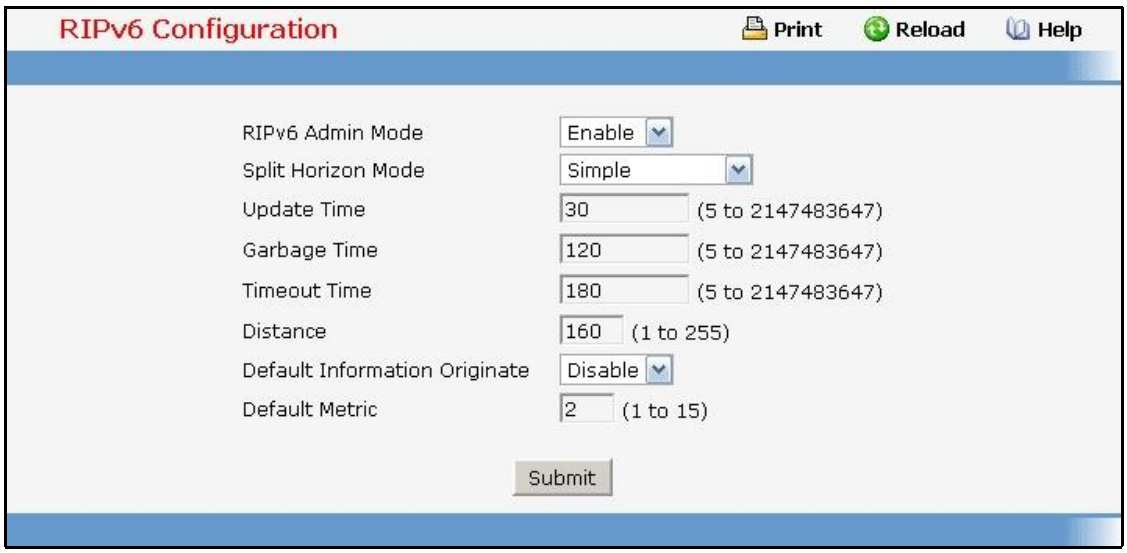
Command Buttons

Add IPv6 Route - Allows the user to configure a new route.

Delete - Deletes the corresponding route.

11.7.9 Managing RIPv6

11.7.9.1 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.

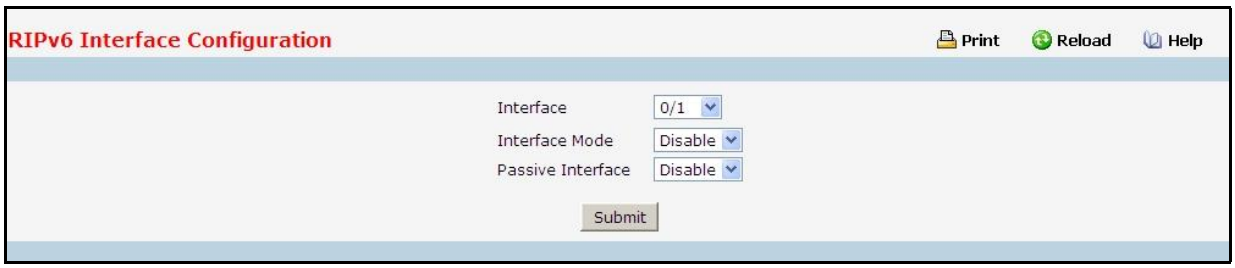
Default Information Originate - Enable or Disable Default Route Advertise.

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.

11.7.9.2 Configuring RIPv6 Interface Configuration Page



Selection Criteria

Interface - 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.

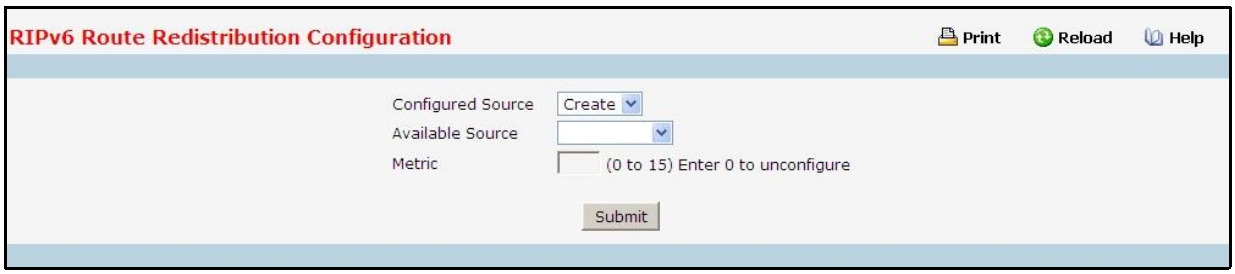
Passive Interface - Select enable or disable from the pulldown menu. The default value is disabled.

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.

11.7.9.3 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.

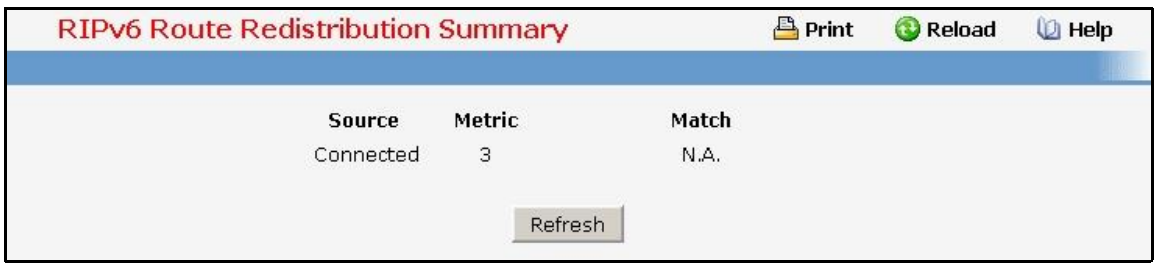
Command Buttons

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.

11.7.9.4 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.

11.8 IPv4 Multicast Menu

11.8.1 Configuring IPv4 Multicast Global

Selection Criteria

Admin Mode - Select enable or disable to set the administrative status of Multicast Forwarding in the router. The default is disable.

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.

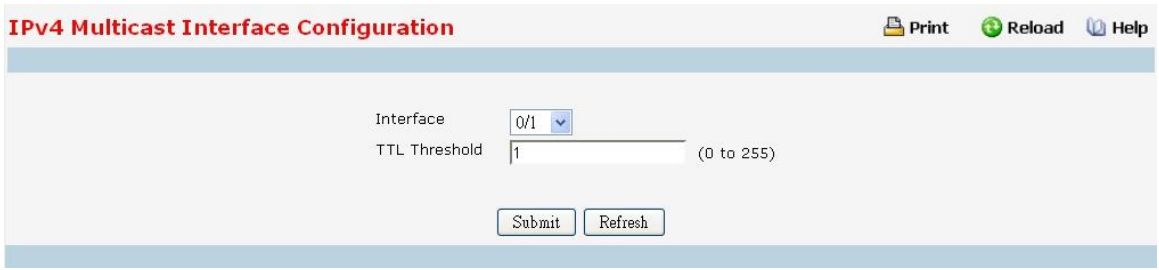
Table Entry Count - The number of multicast route entries currently present in the Multicast route table.

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.

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

11.8.2 Configuring IPv4 Multicast Interface



Selection Criteria

Interface - 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.

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.

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

11.8.3 Configuring Multicast Admin Boundary

Selection Criteria

Admin Mode - Select enable or disable to set the administrative status of Multicast Forwarding in the router. The default is disable.

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.

Table Entry Count - The number of multicast route entries currently present in the Multicast route table.

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.

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

11.8.4 Viewing IPv4 Multicast Admin Boundary Summary

Non-Configurable Data

Interface - 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

Delete - Deletes the selected admin boundary scope entries in the router.

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

11.8.5 Managing DVMRP

11.8.5.1 Configuring DVMRP Global Configuration

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. The default value is 3.

Total Number of Routes - The number of routes in the DVMRP routing table.

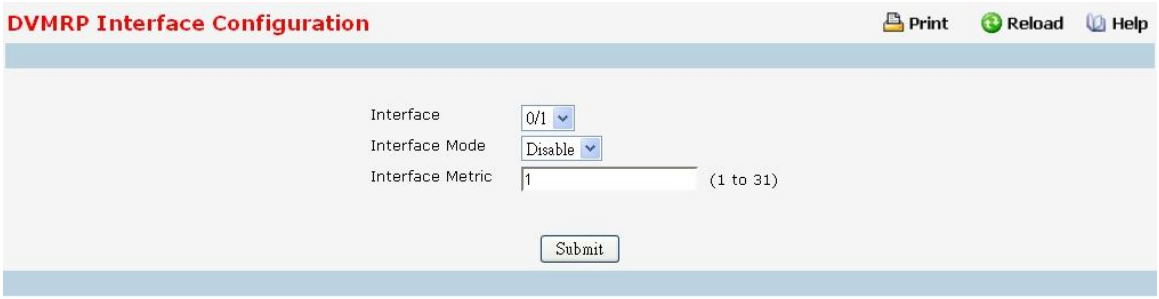
Reachable Routes - The number of routes in the DVMRP routing table that have a non-infinite metric.

Command Buttons

Submit - 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.

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

11.8.5.2 Configuring DVMRP Interface Configuration



Selection Criteria

Interface - 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

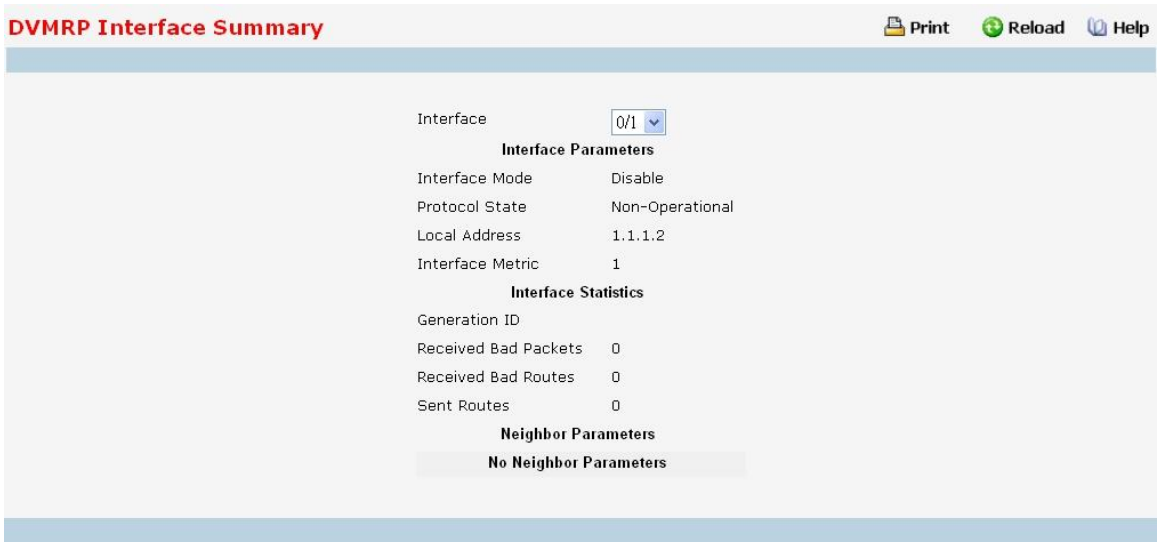
Interface Mode - Select enable or disable from the pull down menu to set the administrative mode of the selected DVMRP routing interface.

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 - 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.

11.8.5.3 Viewing DVMRP Interface Summary



Selection Criteria

Interface - 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 Parameters

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.

Interface Statistic

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 Parameters

Neighbor IP - The IP address of the neighbor whose information is to be displayed. This field appears on the page only when there are finite number of neighbors.

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

11.8.5.4 Viewing DVMRP Next Hop Summary

Non-Configurable Data

Source IP - The IP address used with the source mask to identify the source network for this table entry.

Source Mask - The network mask used with the source IP address.

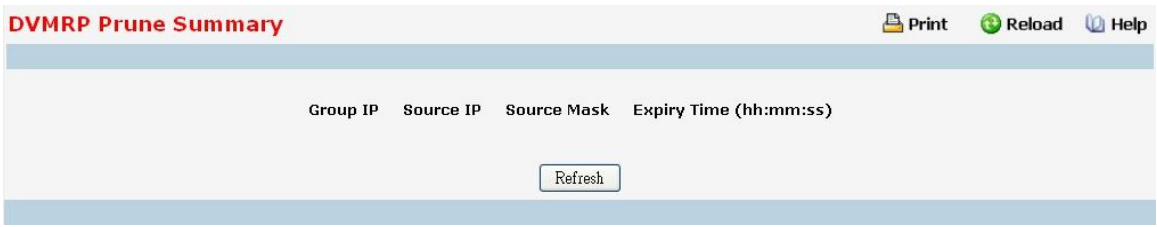
Next Hop Interface - The outgoing interface for this next hop.

Type - The next hop type. 'Leaf' means that no downstream dependent neighbors exist on the outgoing interface. Otherwise, the type is 'branch'.

Command Buttons

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

11.8.5.5 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.

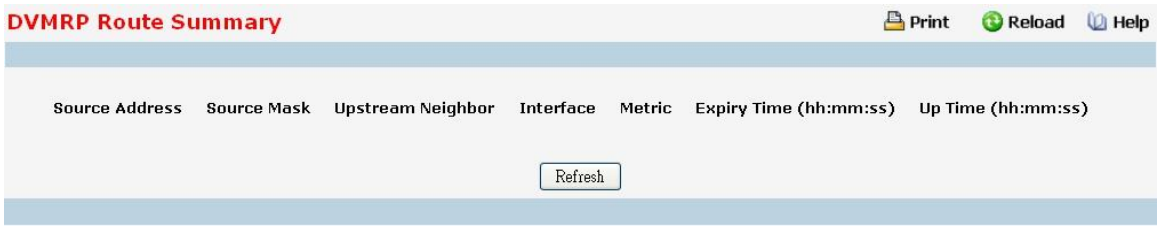
Source Mask - The subnet mask to be combined with the source IP address to identify the source or source network which has been pruned.

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

11.8.5.6 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 Datagram's from these sources are received.

Interface - The interface on which IP Datagram's 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(hh:mm:ss) - The minimum amount of time remaining before this entry will be aged out.

Up Time(hh:mm:ss) - The time since the route represented by this entry was learned by the router.

Command Buttons

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

11.8.6 Managing IGMP

11.8.6.1 Configuring IGMP Global Configuration

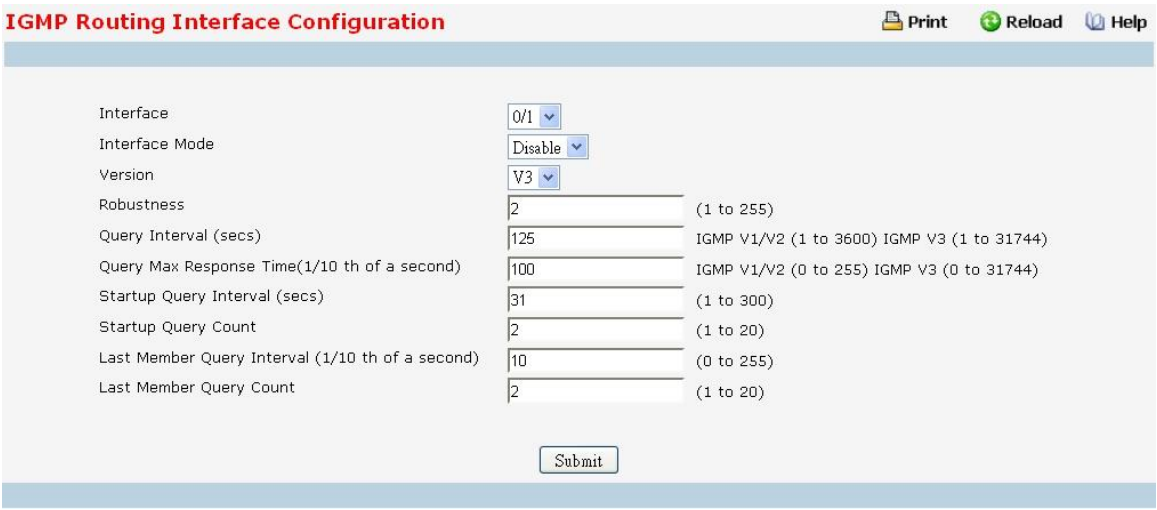
Configurable Data

Admin Mode - Select enable or disable from the pull down menu to set the administrative status of IGMP in the router to active or inactive. The default is disable.

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.

11.8.6.2 Configuring IGMP Rouing interface



Selection Criteria

Interface - Select the slot and port for which data is to be displayed or configured from the pull down 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 pull down 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 10. Valid values are from (0 to 255) .

Startup Query Interval - Enter the number of seconds between the transmission of startup queries on the selected interface. The valid values are from 1 to 300. The default value is 31

Startup Query Count - Enter the number of queries to be sent on startup. The valid values are from 1 to 20. The default value is 2.

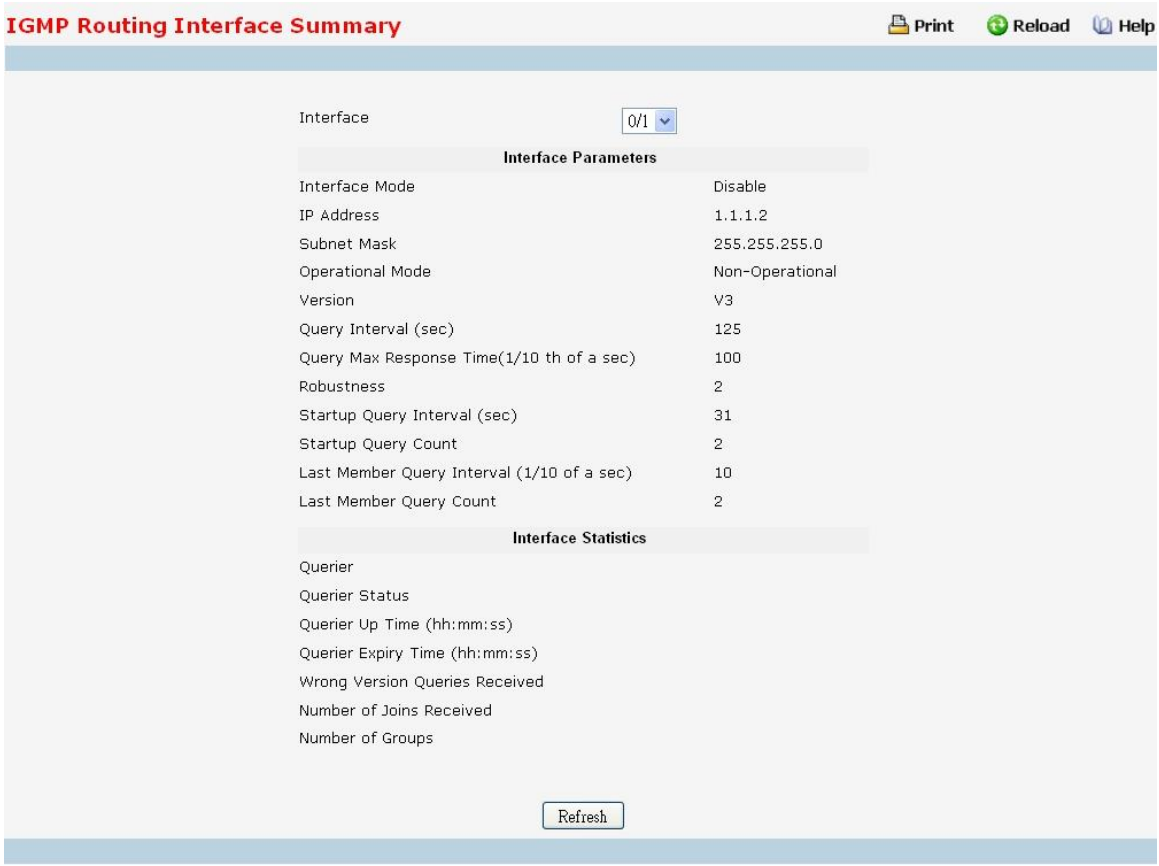
Last Member Query Interval - Enter the last member query interval in tenths of a second. This is the maximum response time to be inserted into group-specific queries sent in response to leave group messages, and is also the amount of time between group-specific query messages. Valid values are from 0 to 255. The default value is 1. This value is not used for IGMP version 1

Last Member Query Count - Enter the number of queries to be sent on receiving a leave group report. Valid values are from 1 to 20. The default value is 2.

Command Buttons

Submit - 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

11.8.6.3 Viewing Routing Interface Summary



Selection Criteria

Interface - Select the slot and port for which data is to be displayed. Slot 0 is the base unit.

Non-Configurable

Interface Parameter

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.

Operational Mode - The operational state of IGMP on the selected interface.

Version - The version of IGMP configured on the selected interface.

Query Interval (sec) - The frequency at which IGMP host-query packets are transmitted on the selected interface.

Query Max Response Time(1/10 th of a sec) - 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 (sec) - 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 (1/10 of a sec) - The last member query interval. The last member query interval is the maximum response time inserted into group-specific queries sent in response to leave group messages, and is also the amount of time between group-specific query messages. This value may be tuned to modify the leave latency of the network. A reduced value results in reduced time to detect the loss of the last member of a group. This value is not used for IGMP version 1.

Last Member Query Count - The number of queries to be sent on receiving a leave group report.

Interface Statistics

Querier - 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 (hh:mm:ss) - The time in seconds since the IGMP interface querier was last changed.

Querier Expiry Time (hh:mm:ss) - 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 - 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.

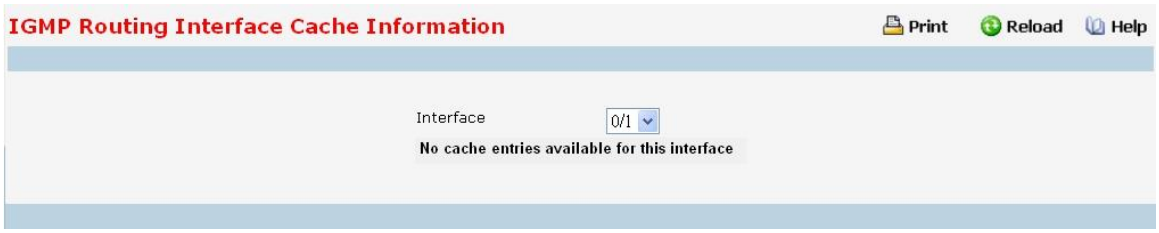
Number of Joins Received - The number of times a group membership has been added on the selected interface; that is, the number of times an entry for this interface has been added to the cache table. This gives an indication of the amount of IGMP activity on the interface.

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 switch.

11.8.6.4 Viewing IGMP Routing Interface Cache Information



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 cannot make this selection, and none of the data on this page displays.

Interface - Select the interface for which data is to 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 (in hh:mm:ss) since this entry was created.

Expiry Time - Cache timer value,which indicates the remaining lifetime (in hh:mm:ss) for each entry.

Version 1 Host Timer - The time (in hh:mm:ss) remaining until the local router assumes 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 (in hh:mm:ss) remaining until the local router assumes 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 switch.

11.8.6.5 Viewing IGMP Routing Interface Source List Information

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 cannot make this selection, and none of the data on this page displays.

Interface - Select the interface for which data is to be displayed.

Non-Configurable Data

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. When NA mode is active the field is blank.

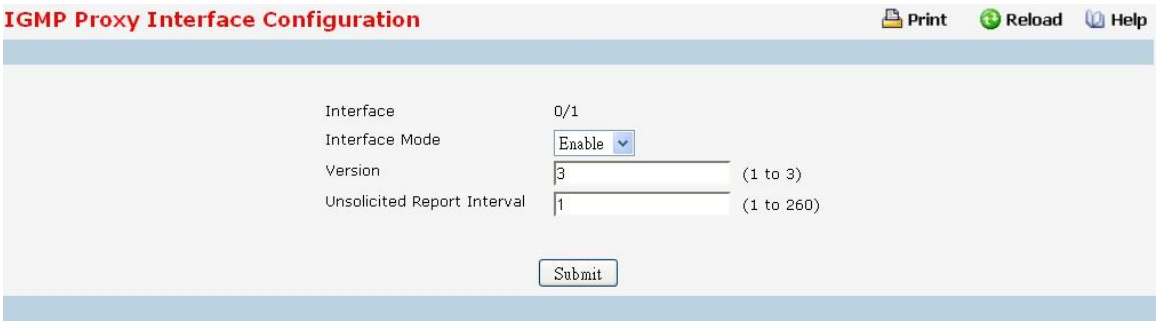
Source Hosts - The source addresses which are members of this multicast address.

Expiry Time - The expiry time interval (in hh:mm:ss) against each source address which are members of this multicast group. This is the Length 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 switch.

11.8.6.6 Configuring IGMP Proxy Interface Configuration



Selection Criteria

Interface - Select the port for which data is to be displayed or configured from the pull down 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 pull down 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.

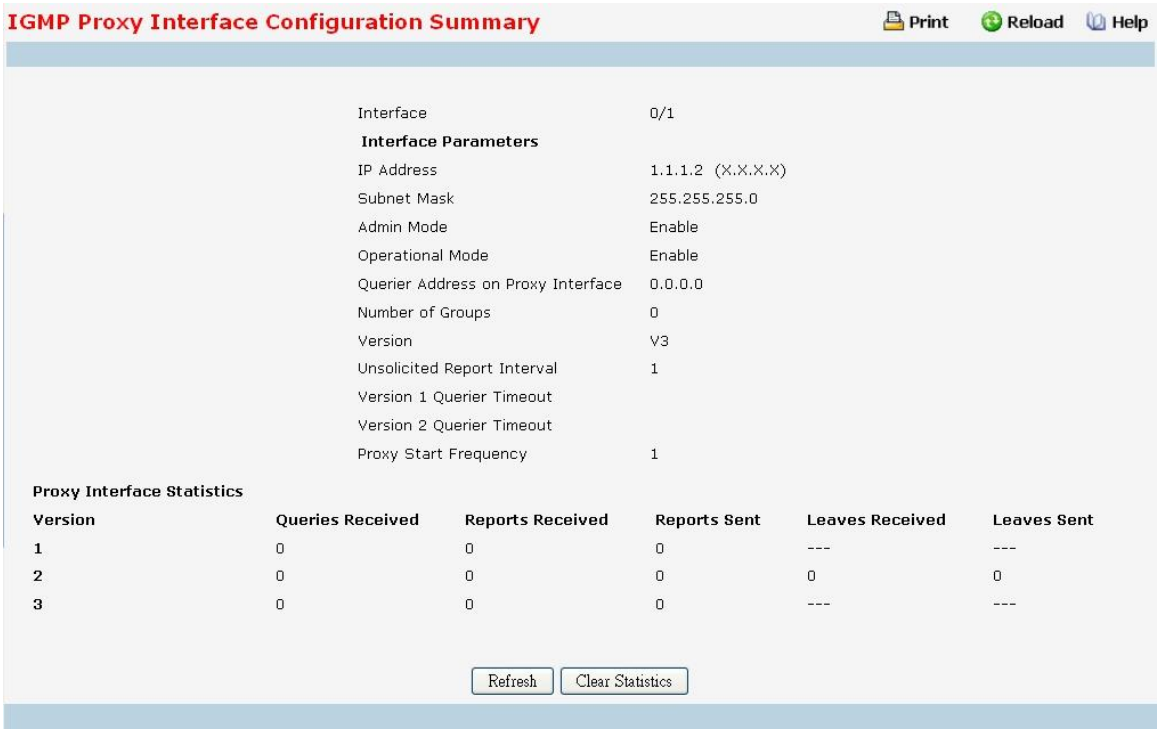
Version - Enter the version of IGMP you want to configure on the selected interface. Valid values are (1 to 3) and the default value is 3. This field is configurable only when IGMP Proxy interface mode is enabled.

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 - 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.

11.8.6.7 Viewing IGMP Proxy Interface Configuration Summary



Non-Configurable Data

Interface - Displays the interface on which IGMP proxy is enabled.

Interface Parameters

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. Cache table.

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.

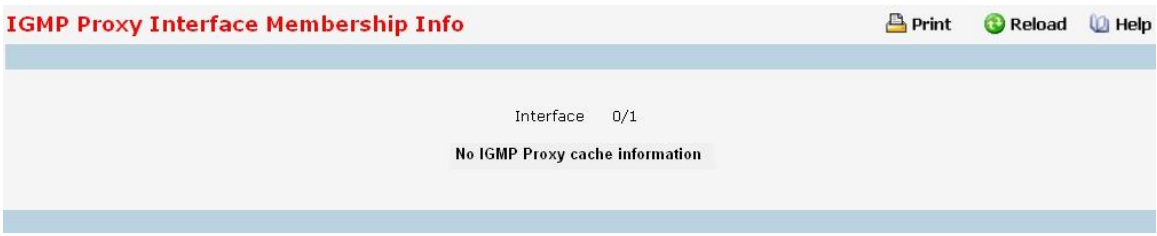
Proxy Interface Statistics - The Queries Received, Reports Received/Sent, Leaves Received/Sent are displayed in the form a table for each IGMP version.

Command Buttons

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

Clear Statistics - Clear the IGMP Proxy interface statistics.

11.8.6.8 Viewing IGMP Proxy Interface MemberShip Information



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

Interface - 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.

Up Time(hh:mm:ss) - The time elapsed since this entry was created in hours, minutes and seconds.

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 switch.

11.8.6.9 Viewing IGMP Proxy Interface Membership Info Detailed

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

Interface - Displays the interface on which IGMP proxy is enabled.

Source Address - 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.

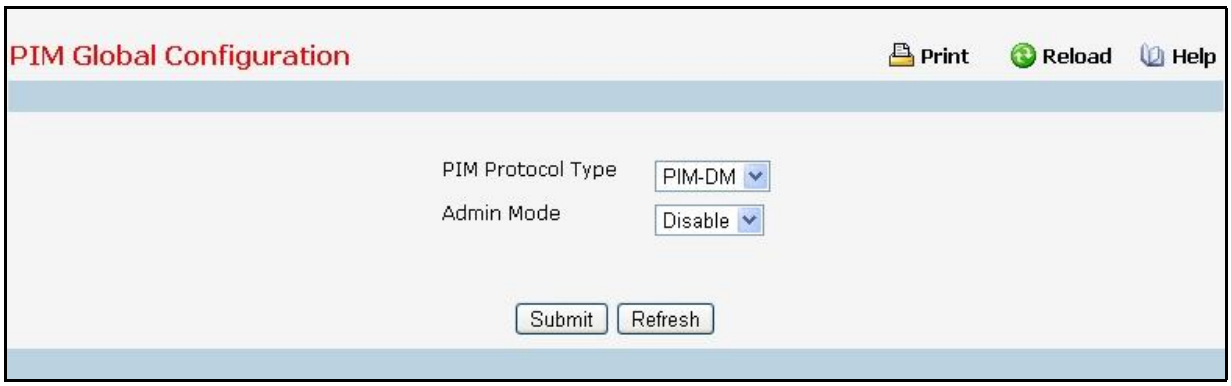
Up Time - Displays the up time since the entry was created in cache table..

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..

11.8.7 Managing PIM Protocol

11.8.7.1 Configuring Global Configuration



Selection Criteria

PIM Protocol Type - The protocol variant of PIM that is to be enabled/disabled i.e, Sparse mode or Dense mode.

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.

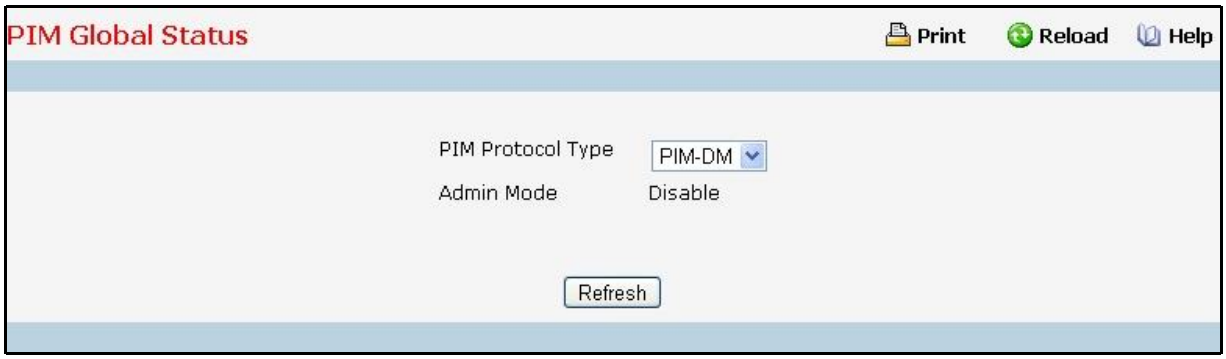
Data Threshold Rate (kbps) - Enter the rate in K bits/second above which the last-hop router will switch to a source-specific shortest path tree. This field is applicable only for PIMSM. The valid values are from (0 to 2000). The default value is 0. NOTE: Non-Zero Data Threshold Rate is currently not supported. Switch on First Packet policy is only supported.

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 switch.

11.8.7.2 Viewing Global Status



Selection Criteria

PIM Protocol Type - The protocol variant of PIM that is to be enabled/disabled i.e, Sparse mode or Dense mode.

Configurable Data

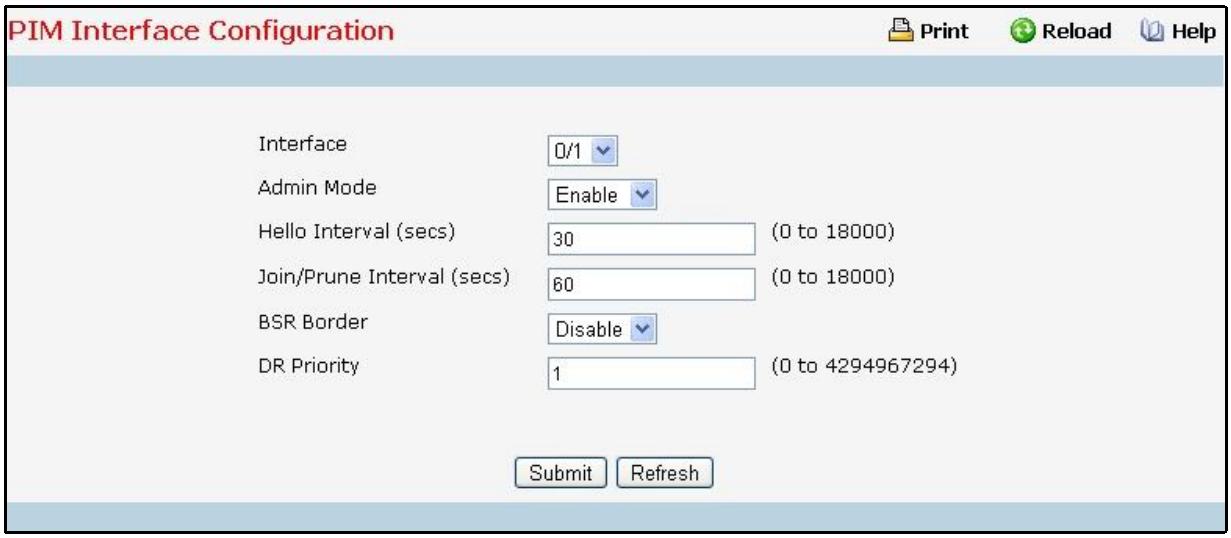
Admin Mode - Select enable or disable from the pulldown menu to set the administrative status of PIM-DM in the router. The default is disabled.

Data Threshold Rate (kbps) - Enter the rate in K bits/second above which the last-hop router will switch to a source-specific shortest path tree. This field is applicable only for PIMSM. The valid values are from (0 to 2000). The default value is 0. NOTE: Non-Zero Data Threshold Rate is currently not supported. Switch on First Packet policy is only supported.

Command Buttons

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

11.8.7.3 ConfiguringInterface Configuraiton



Selection Criteria

Interface - Select the interface for which data is to be displayed or configured.

Admin Mode - Select Enable or Disable to set the administrative status of PIM for the specified interface in the router. The default is Disable.

BSR Border - Select enable or disable to set BSR border status on the selected interface. This field is applicable for PIMSM only.

Configurable Data

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) seconds. The default value is 30 seconds.

Join/Prune Interval (secs) - Enter the frequency (in seconds) at which PIM Join/Prune messages are transmitted on this PIM interface. This field is applicable for PIMSM only. The valid values are from (0 to 18000) seconds. The default value is 60 seconds.

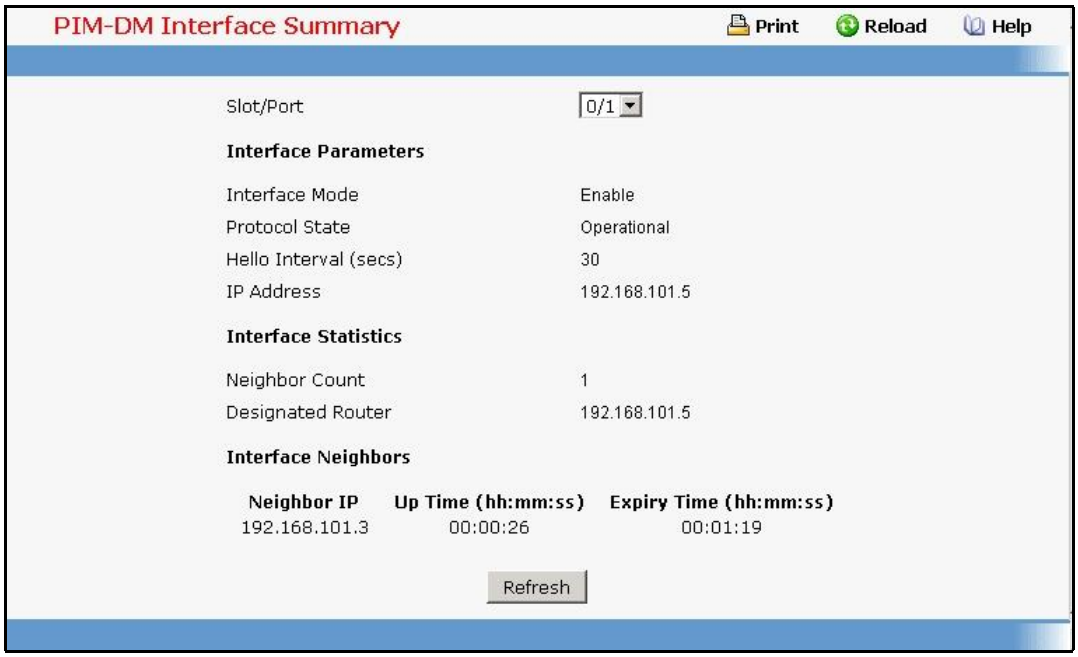
DR Priority - Enter the DR priority for the selected interface. This field is applicable for PIMSM only. The valid values are from (0 to -2) The default value is 1.

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.

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

11.8.7.4 Viewing Interface Summary



Selection Criteria

Interface - Select the interface for which data is to be displayed.

Non-Configurable Data

Admin Mode - The administrative mode of PIM-SM interface in the router: either enable or disable.

Protocol State - The state of PIM in the router: either operational or non-operational.

IP Address - The IP address of the selected PIM interface.

Net Mask- The Net Masks of the selected PIM interface.

Hello Interval (secs)- The frequency (in seconds) at which PIM hello messages are transmitted on the selected interface.

Join/Prune Interval (secs) - The frequency (in seconds) at which PIM Join/Prune messages are transmitted on this PIM interface. This field is always shown with defaults for PIMDM as configurability is not supported in PIMDM.

DR Priority - Indicates the DR priority on the PIM interface. This field is supported in PIMSM only and hence shown for PIMSM only.

BSR Border - Specifies the BSR border mode on the PIM interface. This field is supported in PIMSM only and hence shown for PIMSM only.

Designated Router - The Designated Router on the selected PIM interface. This field is supported in PIMSM only and hence shown for PIMSM only. This field is displayed only when the interface is Operational.

Interface Neighbors

Neighbor Count - The number of PIM neighbors on the selected interface. This field is displayed only when the interface is Operational.

Neighbor IP Address- The IP address of the PIM neighbor for this entry.

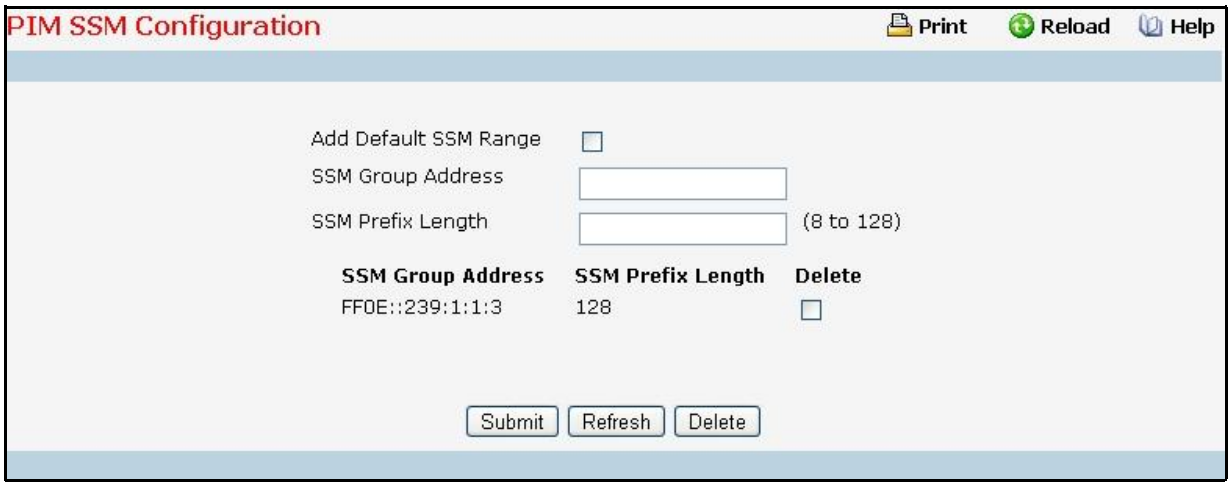
Uptime - The time (in hours:minutes:seconds) since this PIM neighbor (last) became a neighbor of the local router.

Expiry Time - The minimum time (in hours:minutes:seconds) 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.

11.8.7.5 Configuring SSM



Add Default SSM Range - Select this check box to add default SSM range (232.0.0.0/8) .

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.

Non-Configurable Data

SSM Group Address - Displays the source-specific multicast group ip-address.

SSM Group Mask - Displays the source-specific multicast group ip-address mask.

Delete - Check box to delete the particular entry from the table.

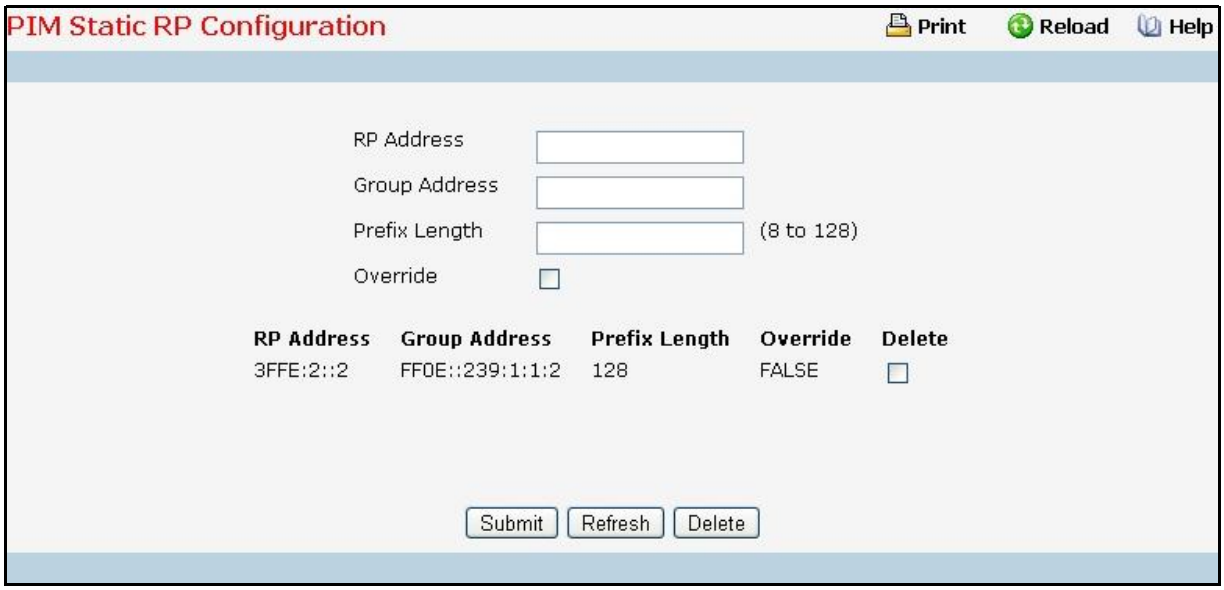
Command Buttons

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.

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

Delete - Deletes the selected SSM ranges in the router.

11.8.7.6 Configuring Static RP



Configurable Data

Group Address - Group Address for which the static RP is to be created or deleted.

Group Mask - Group Mask or which the static RP is to be created or deleted.

RP Address - IP Address of the RP for the group range created or deleted.

Override - The check option to configure the static RP to override the dynamic (candidate) RPs learnt for same group ranges.

Non-Configurable Data

RP Address - IP Address of the RP for the group range created or deleted.

Group Address - Group Address for which the static RP is to be created or deleted.

Group Mask - Group Mask or which the static RP is to be created or deleted.

Delete - Check box to delete the particular entry from the table

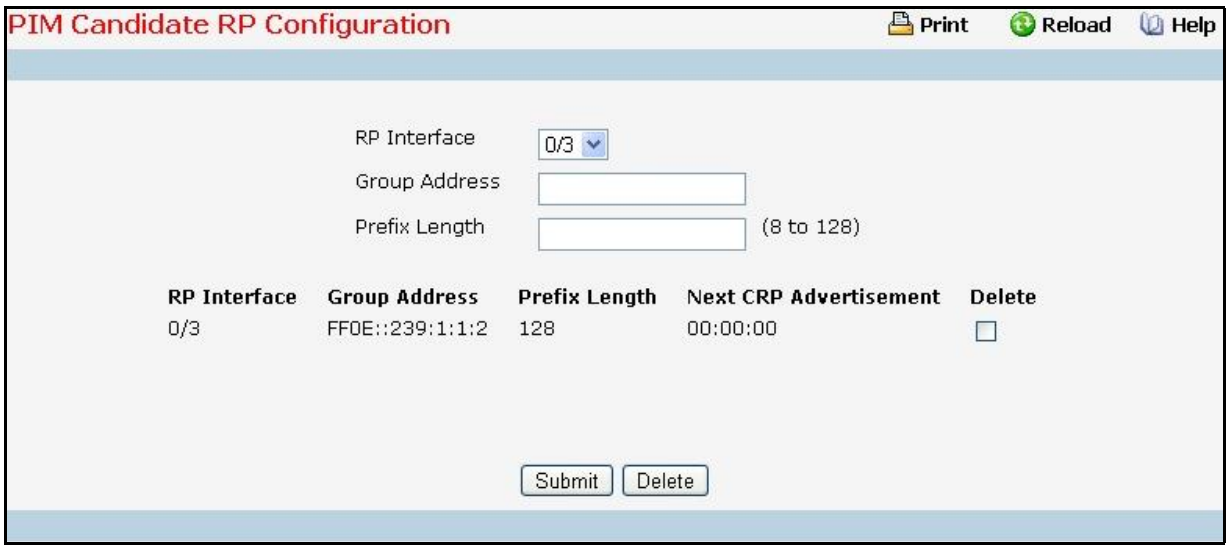
Command Buttons

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.

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

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.

11.8.7.7 Configuring Candidate RP Configuration



Selection Criteria

RP Interface - Select the interface for which the Candidate RP has to be configured.

Configurable Data

Group Address - The group address transmitted in Candidate-RP-Advertisements

Group Mask - The group address mask transmitted in Candidate-RP-Advertisements.

Delete - Check box to delete the particular entry from the table.

Non-Configurable Data

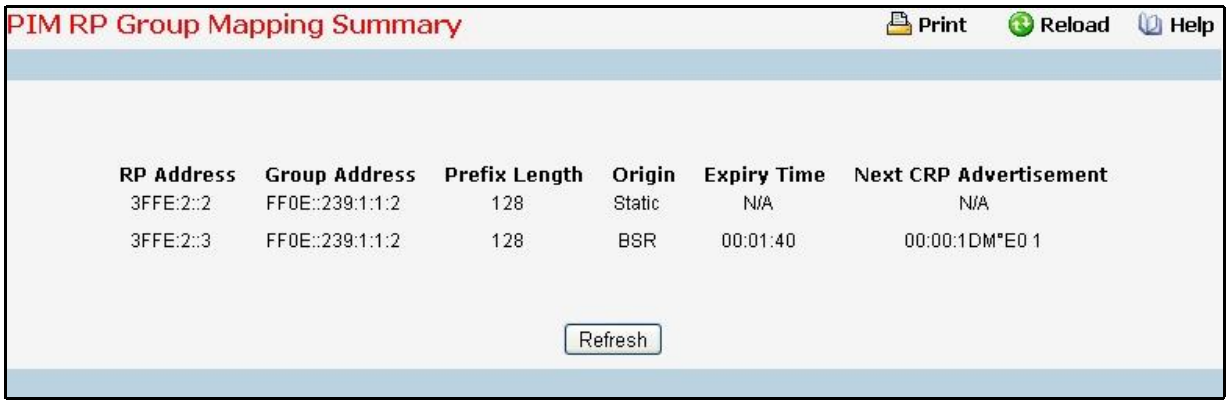
Next CRP Advertisement - The time remaining to send the next Candidate-RP-Advertisement.

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 - 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.

11.8.7.8 Viewing RP Mapping Summary



Non-Configurable Data

RP Address - The IP address of the RP to be used for groups within this group prefix.

Group Address - The IP multicast group address which, when combined with group mask, gives the group prefix for this mapping. This address object is only significant up to prefix length bits. The remainder of the address bits are zero. This is especially important for this field, which is part of the index of this entry. Any non-zero bits would signify an entirely different entry.

Group Mask - The multicast group prefix length that, when combined with group address, gives the group prefix for this mapping.

Origin - Origin from where this group mapping is learnt.

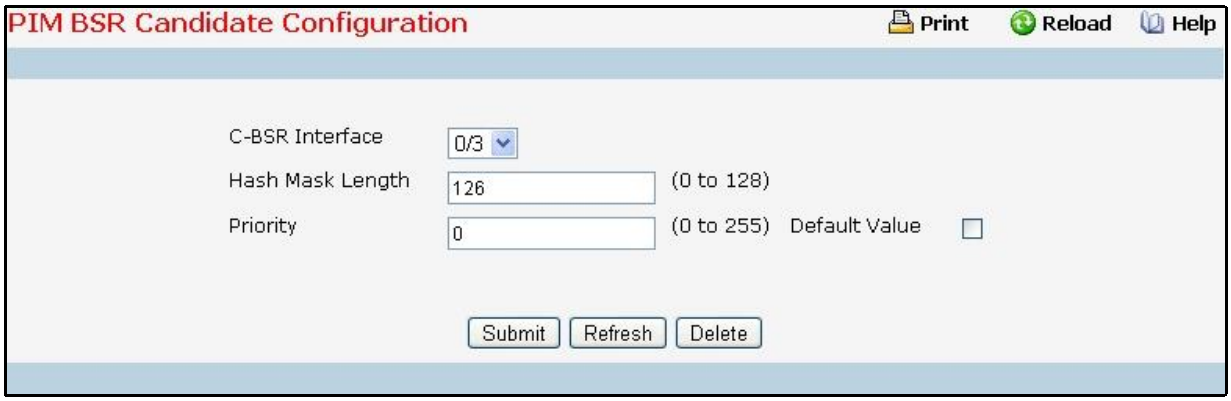
Expiry Time - The minimum time remaining before this entry will be aged out. The value zero indicates that this entry will never be aged out. This field is not-applicable for statically configured entries.

Next CRP Advertisement - The time remaining to send the Next Candidate RP advertisement. This field is not-applicable for statically configured entries.

Command Buttons

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

11.8.7.9 Configuring BSR Candidate Configuration



Selection Criteria

C-BSR Interface - Select the interface for which data is to be displayed.

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. The valid values are from (0 to 255). Default value is 0.

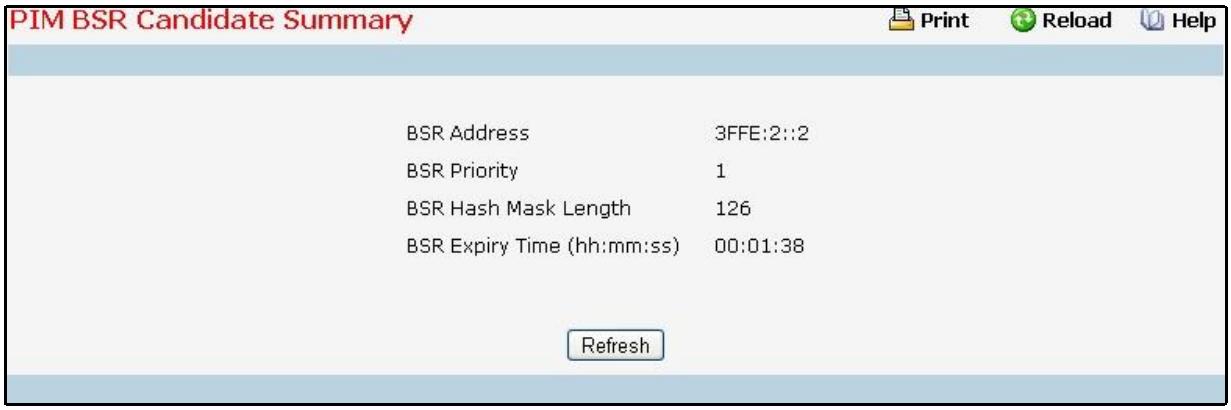
Command Buttons

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.

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

Delete - Deletes the candidate BSR configured on the router.

11.8.7.10 Viewing BSR Candidate Summary



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

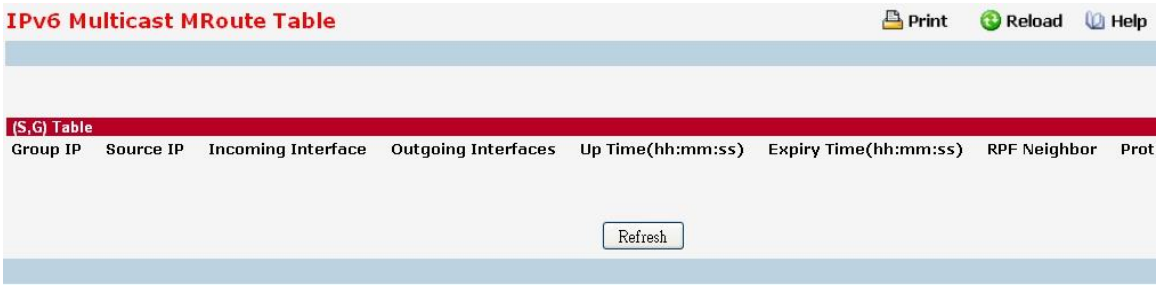
BSR Expiry Time (hh:mm:ss) - Time (in Hours, Minutes and Seconds) in which the learnt elected bootstrap router (BSR) expires.

Command Buttons

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

11.8.8 Viewing IPv4 Multicast Mroute Table

This screen displays contents of the Multicast Route Table in tabular form.



Non-Configurable Data

(*,G)Table

(This table displays the entries for which this router has received MLDv1 Reports. This table is applicable only for PIMSM and will be displayed only when PIMSM is operational and when the above said entries are present.)

Group IP - The IP address of the Multicast Group for which this router has received MLDv1 Reports.

Incoming Interface - The incoming interface on which multicast packets for this source/group arrive.

Outgoing Interface(s) - The list of outgoing interfaces on which multicast packets for this source/group are forwarded.

Up Time - The time (in hours:minutes:seconds) since the entry was created.

Expiry Time - The time (in hours:minutes: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-SM

Flags - The value displayed in this field is valid if the multicast routing protocol running is PIMSM. The default value is RPT.

(S,G)Table

Group IP - The IP address of the Multicast Group for which this router is receiving data.

Source IP - The IP address of the Multicast Source from which this router is receiving data for the Group IP.

Incoming Interface - The incoming interface on which multicast packets for this source/group arrive.

Outgoing Interface(s) - The list of outgoing interfaces on which multicast packets for this source/group are forwarded.

Up Time - The time (in hours:minutes:seconds) since the entry was created.

Expiry Time - The time (in hours:minutes:seconds) before this entry will age out and be removed from the table.

RPF Neighbor - The IP address of the Reverse Path Forwarding neighbor.

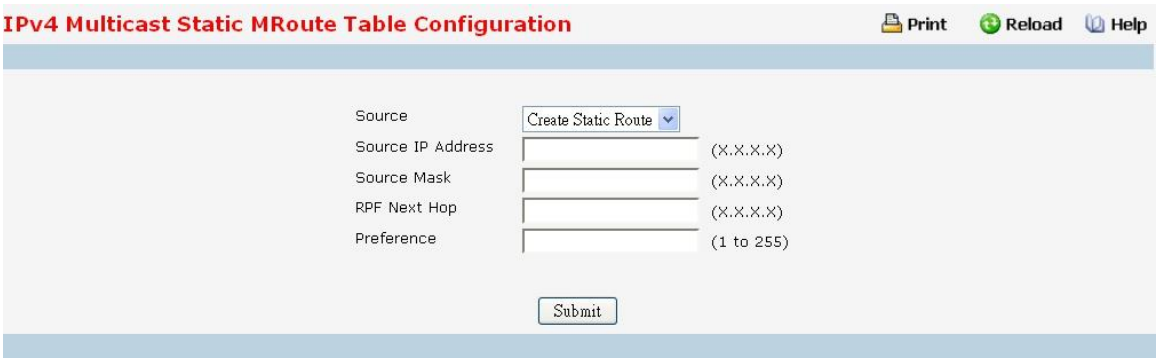
Protocol - The multicast routing protocol which created this entry. The possibilities are: PIM-DM, PIM-SM , MLD-Proxy

Flags - The value displayed in this field is valid if the multicast routing protocol running is PIMSM. The possible values are RPT or SPT. For other protocols an "------" is displayed.

Command Buttons

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

11.8.9 Configuring IPv4 Multicast Static MRoute Table Configuration



This page is used to configure a new or existing static mroute entry.

Configurable Data

Source IP Address - Enter the address of the Multicast data source.

Source Mask - Enter the network mask for the IP address of the Multicast data source to be configured.

RPF Next Hop - Enter the RPF Address for the source range of static mroute entry.

Preference - Enter the preference with which the static mroute to be considered against other matching static mroute entry for a given source. The valid values are from (1 to 255).

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.

11.8.10 Viewing IPv4 Multicast Static MRoute Table Summary

This page is used to summarize the configured static mroute entries.

Configurable Data

Remove - Check Box to Delete the Selected Static MRoute Entry.

Non-Configurable Data

Source IP - The address of the Multicast data source.

Source Mask - The network mask for the IP address of the Multicast data source to be configured.

RPF Next Hop - The RPF Address for the source range of static mroute entry.

Preference - The preference with which the static mroute to be considered against other matching static mroute entry for a given source.

Command Buttons

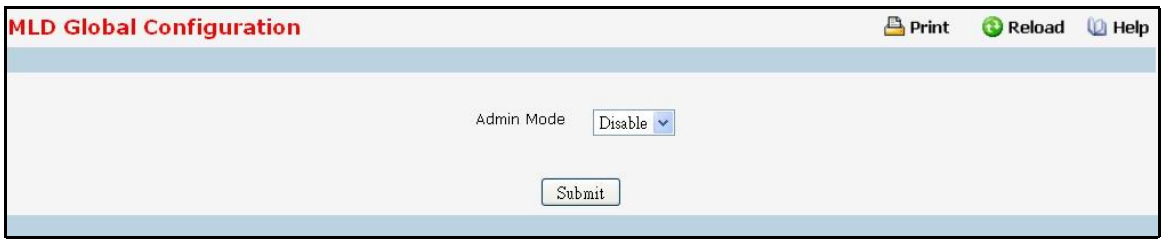
Delete - Deletes the selected static mroute entries in the router. This is used to delete the entries selected using the Checkbox under Remove field

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

11.9 IPv6 Multicast Menu

11.9.1 Managing MLD

11.9.1.1 Configuring MLD Global Configuration Page



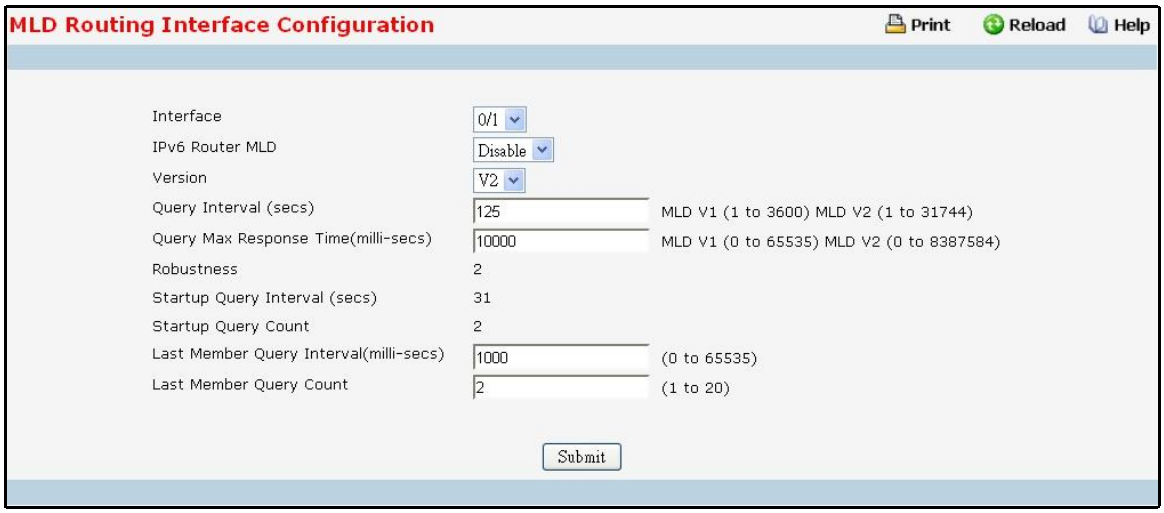
Selection Criteria

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

Interface - Select the interface for which data is to be displayed or configured from the pull down menu. 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 Interface Summary Page

Selection Criteria

Interface - Select the slot and port for which data is to be displayed. Slot 0 is the base unit.

Non-Configurable Data

Interface Parameters

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.

Interface Statistics

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.

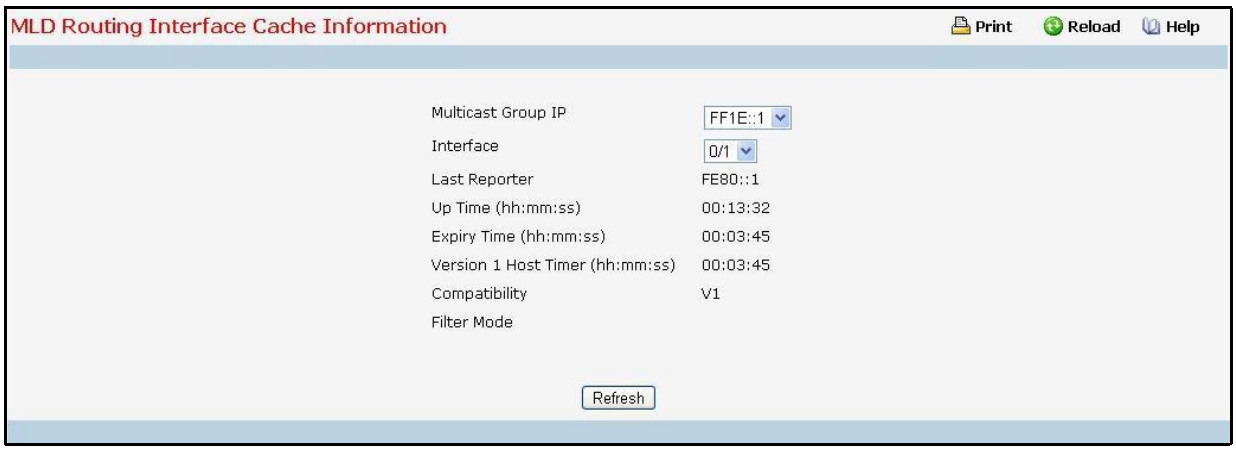
Number of Joins Received - The number of times a group membership has been added on this interface.

Number of Groups - The current number of membership entries for the selected interface in the cache table.

Common Buttons

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

11.9.1.4 Viewing MLD Interface Cache Information



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 cannot make this selection, and none of the data on this page displays.

Interface - Select the interface for which data is to 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 (in hh:mm:ss) since this entry was created.

Expiry Time - Cache timer value,which indicates the remaining lifetime (in hh:mm:ss) for each entry.

Version 1 Host Timer - The time (in hh:mm:ss) remaining until the local router assumes that there are no longer any MLD version 1 members on the IPv6 subnet attached to this interface. When an MLDv1 membership report is received, this timer is reset to the group membership timer.

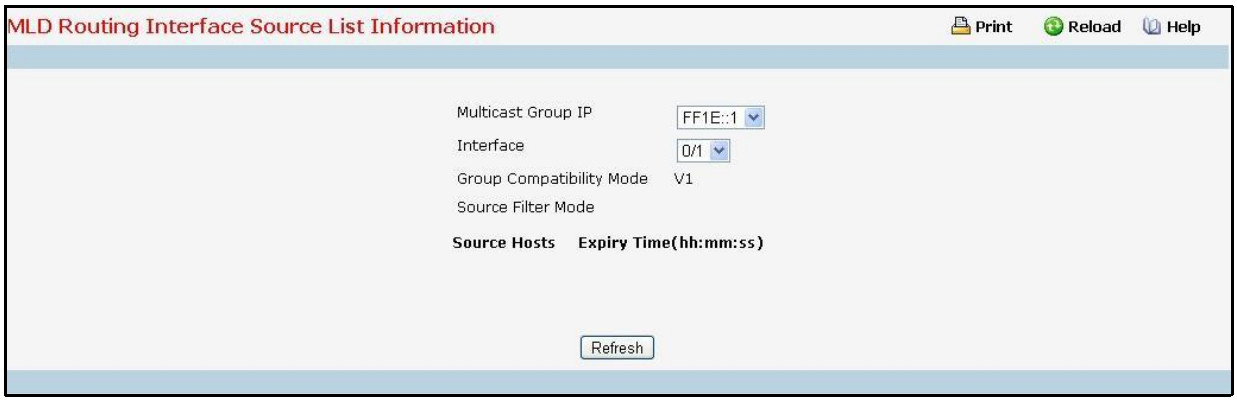
Compatibility - This parameter shows group compatibility mode (V1 or V2) for this group on the specified interface.

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 switch..

11.9.1.5 Viewing MLD Routing Interface Source List Information



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 cannot make this selection, and none of the data on this page displays.

Interface - Select the interface for which data is to be displayed.

Non-Configurable Data

Group Compatibility Mode - This parameter shows group compatibility mode (V1 or V2) for this group on the specified interface.

Source 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.

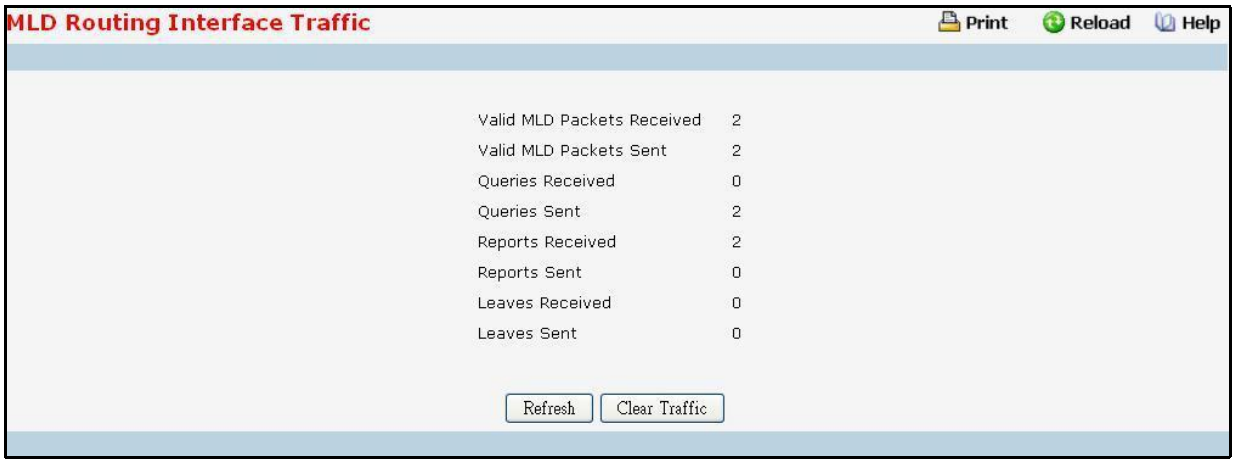
Source Hosts - The source addresses which are members of this multicast address.

Expiry Time - The expiry time interval (in hh:mm:ss) against each source address which are members of this multicast group. This is the Length 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 switch..

11.9.1.6 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.

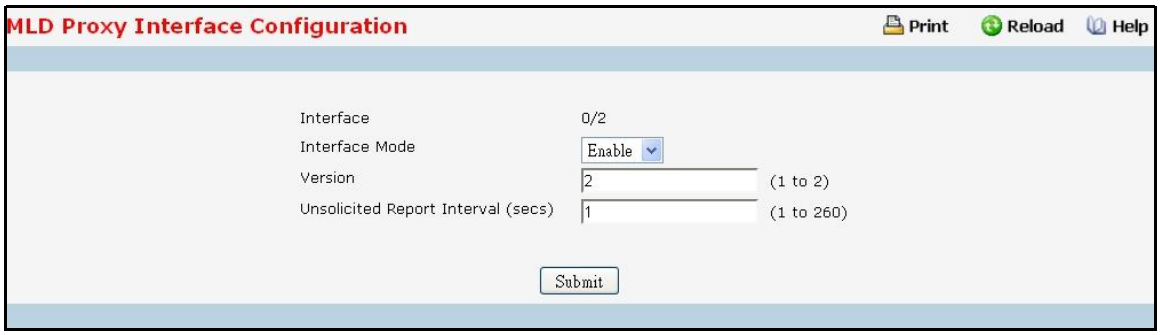
Malformed MLD Packets - The number of Malformed MLD Packets received by the router.

Common Buttons

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.

11.9.1.7 Configuring MLD Proxy Interface Congiuration Page



Selection Criteria

Interface - 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.

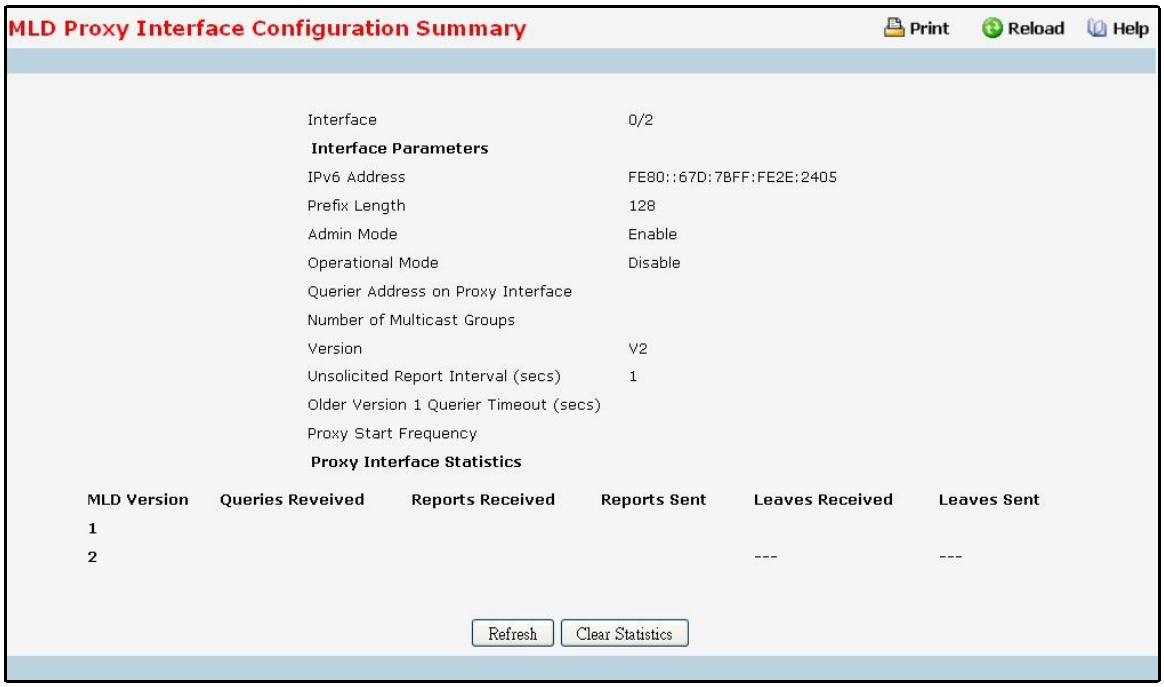
Version - nter the version of MLD you want to configure on the selected interface. Valid values are (1 to 2) and the default value is 2. This field is configurable only when MLD Proxy interface mode is enabled.

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.

11.9.1.8 Viewing MLD Proxy Configration Summary Page



Non-Configurable Data

Interface - Displays the interface on which MLD proxy is enabled.

IPv6 Address - The IPv6 address of the MLD Proxy interface.

Prefix Length - The Prefix Length 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 Multicast 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.

Older 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.

MLDv1 Statistics

Queries Received - The Queries Received for MLD version 1.

Reports Received - The Reports Received for MLD version 1.

Reports Sent - The Reports Sent for MLD version 1.

Leaves Received - The Leaves Received for MLD version 1.

Leaves Sent - The Leaves Sent for MLD version 1.

MLDv2 Statistics

Queries Received - The Queries Received for MLD version 2.

Reports Received - The Reports Received for MLD version 2.

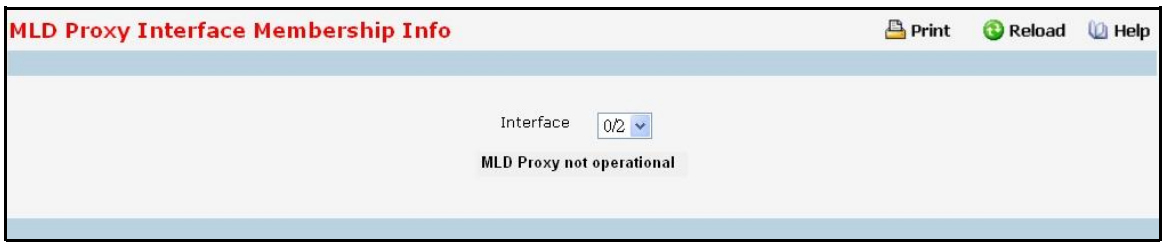
Reports Sent - The Reports Sent for MLD version 2.

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.

11.9.1.9 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

Interface - 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.

11.9.1.10 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

Interface - 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.

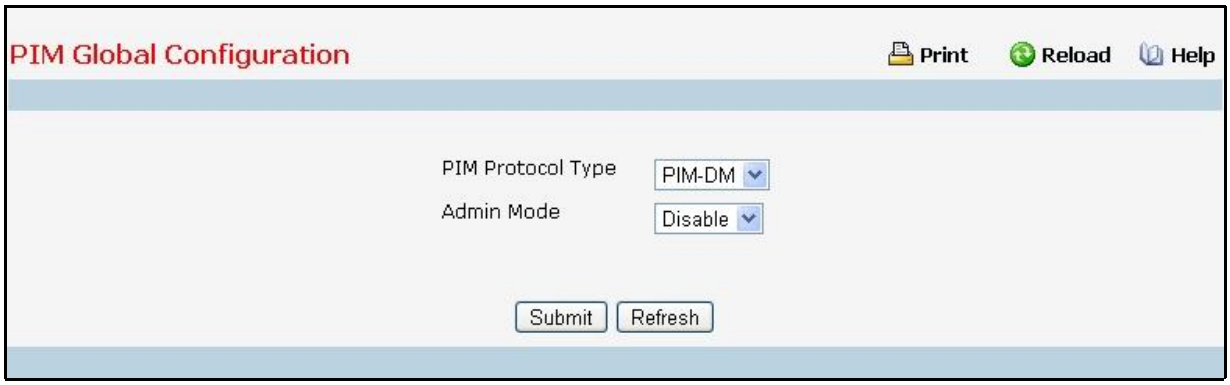
Up Time - Displays the up time since the entry was created in cache table.

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 Protocol

11.9.2.1 Configuring PIM-DM Global Admin Configuration Page



Selection Criteria

PIM Protocol Type - The protocol variant of PIM that is to be enabled/disabled i.e, Sparse mode or Dense mode.

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.

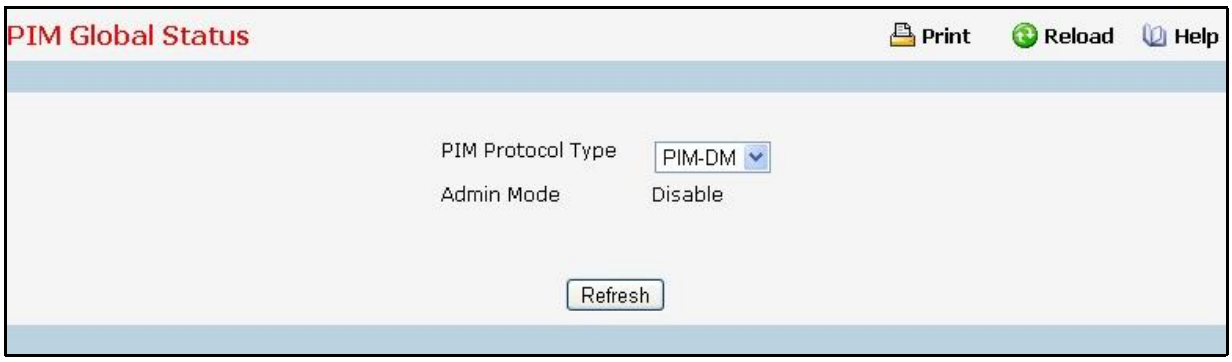
Data Threshold Rate (kbps) - Enter the rate in K bits/second above which the last-hop router will switch to a source-specific shortest path tree. This field is applicable only for PIMSM. The valid values are from (0 to 2000). The default value is 0. NOTE: Non-Zero Data Threshold Rate is currently not supported. Switch on First Packet policy is only supported.

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 switch.

11.9.2.2 PIM Global Status Page



Selection Criteria

PIM Protocol Type - The protocol variant of PIM that is to be enabled/disabled i.e, Sparse mode or Dense mode.

Configurable Data

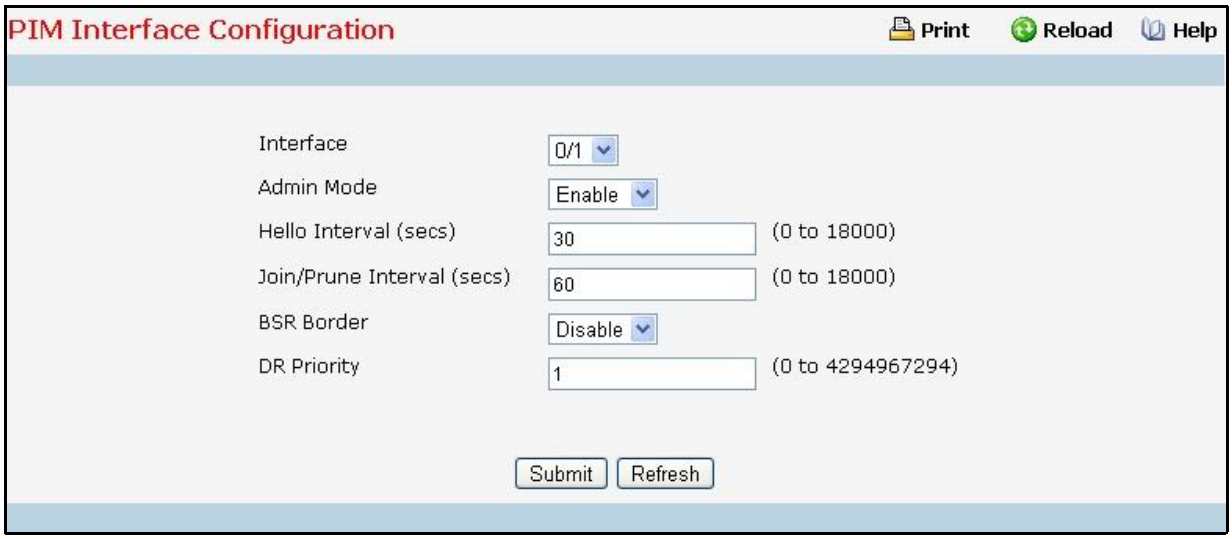
Admin Mode - Select enable or disable from the pulldown menu to set the administrative status of PIM-DM in the router. The default is disabled.

Data Threshold Rate (kbps) - Enter the rate in K bits/second above which the last-hop router will switch to a source-specific shortest path tree. This field is applicable only for PIMSM. The valid values are from (0 to 2000). The default value is 0. NOTE: Non-Zero Data Threshold Rate is currently not supported. Switch on First Packet policy is only supported.

Command Buttons

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

11.9.2.3 Configuring Interface's PIM Configuration Page



Selection Criteria

Interface - Select the interface for which data is to be displayed or configured.

Configurable Data

Admin Mode - Select Enable or Disable to set the administrative status of PIM for the specified interface 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) seconds. The default value is 30 seconds.

Join/Prune Interval (secs) - Enter the frequency (in seconds) at which PIM Join/Prune messages are transmitted on this PIM interface. This field is applicable for PIMSM only. The valid values are from (0 to 18000) seconds. The default value is 60 seconds.

BSR Border - Select enable or disable to set BSR border status on the selected interface. This field is applicable for PIMSM only.

DR Priority - Enter the DR priority for the selected interface. This field is applicable for PIMSM only. The valid values are from (0 to -2) 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.

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

11.9.2.4 Viewing Interface's PIM Configuration Page

Selection Criteria

Interface - Select the interface for which data is to be displayed.

Non-Configurable Data

Admin Mode - The administrative mode of PIM-SM interface in the router: either enable or disable.

Protocol State - The state of PIM in the router: either operational or non-operational.

IP Address - The IP address of the selected PIM interface.

Hello Interval (secs)- The frequency (in seconds) at which PIM hello messages are transmitted on the selected interface.

Join/Prune Interval (secs) - The frequency (in seconds) at which PIM Join/Prune messages are transmitted on this PIM interface. This field is always shown with defaults for PIMDM as configurability is not supported in PIMDM.

DR Priority - Indicates the DR priority on the PIM interface. This field is supported in PIMSM only and hence shown for PIMSM only.

BSR Border - Specifies the BSR border mode on the PIM interface. This field is supported in PIMSM only and hence shown for PIMSM only.

Designated Router - The Designated Router on the selected PIM interface. This field is supported in PIMSM only and hence shown for PIMSM only. This field is displayed only when the interface is Operational.

Interface Neighbors

Neighbor Count - The number of PIM neighbors on the selected interface. This field is displayed only when the interface is Operational.

Neighbor IP Address- The IP address of the PIM neighbor for this entry.

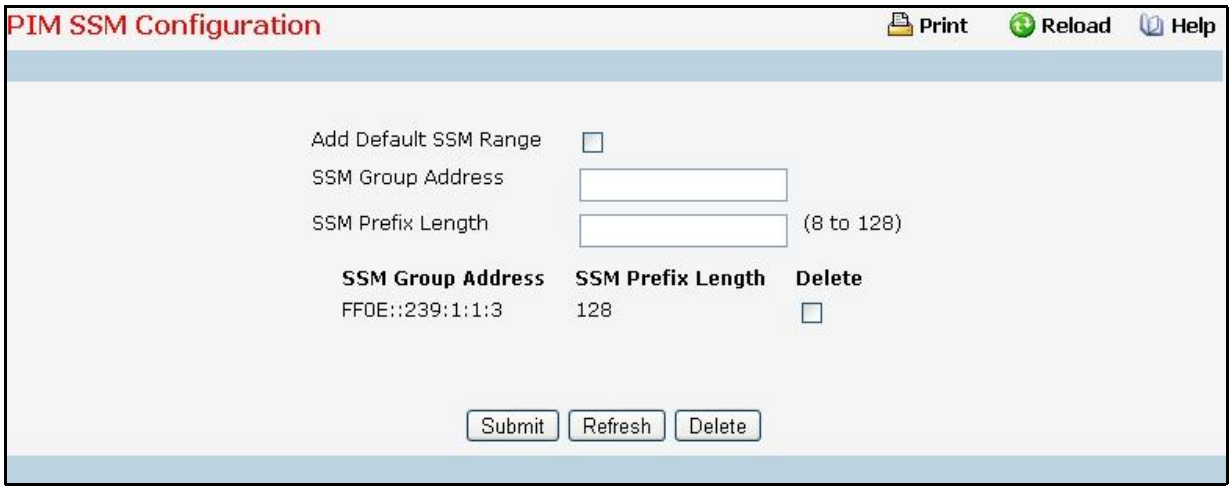
Uptime - The time (in hours:minutes:seconds) since this PIM neighbor (last) became a neighbor of the local router.

Expiry Time - The minimum time (in hours:minutes:seconds) 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 theswitch.

11.9.2.5 Configuring PIM SSM Configuration Page



Configurable Data

Add Default SSM Range - Select this check-box to add default SSM range (FF3x::/32) .

SSM Group Address - Enter the source-specific multicast group ip-address. SSM Group address for 'FF3x::' is represented by 'FF30::' address.

SSM Prefix Length - Enter the source-specific multicast group ip-address prefix length.

Delete - Check Box to delete a particular SSM Group Address and the SSM Prefix Length entry.

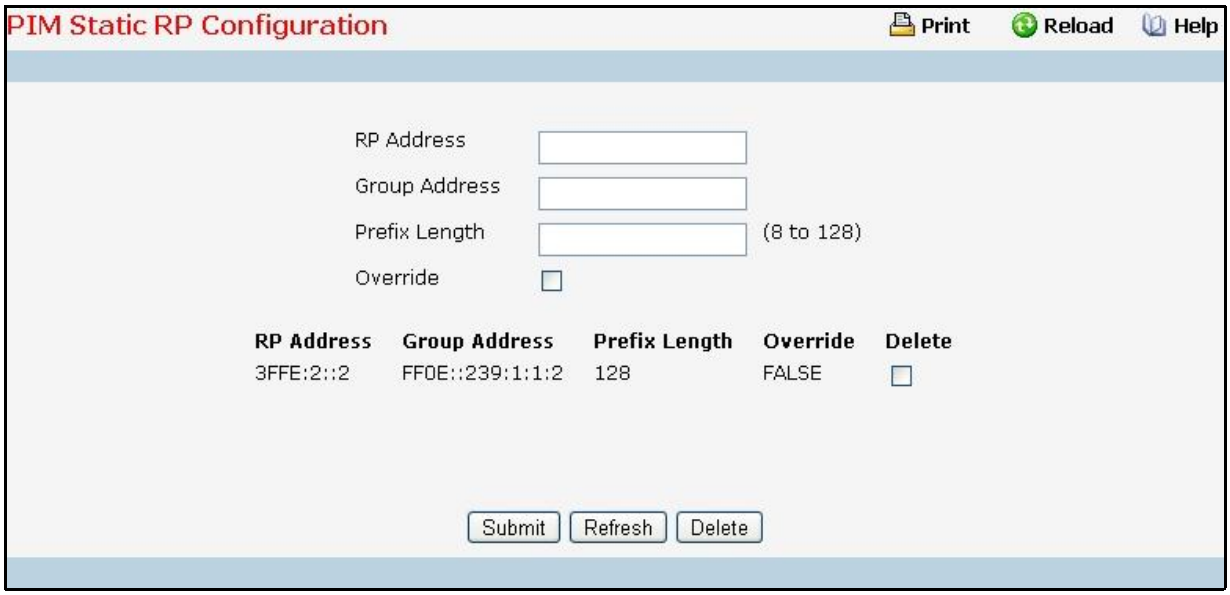
Command Buttons

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.

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

Delete - Deletes the selected SSM ranges in the switch

11.9.2.6 Configuring PIM Static RP Configuration Page



Configurable Data

RP Address - IP Address of the RP for the group range created or deleted.

Group Address - Group Address for which the static RP is to be created or deleted.

Prefix Length - Prefix Length of the Group Address for which the Static RP is to be created or deleted.

Override - The check option to configure the static RP to override the dynamic (candidate) RPs learnt for same group ranges.

Delete - Check box to delete the particular entry from the table.

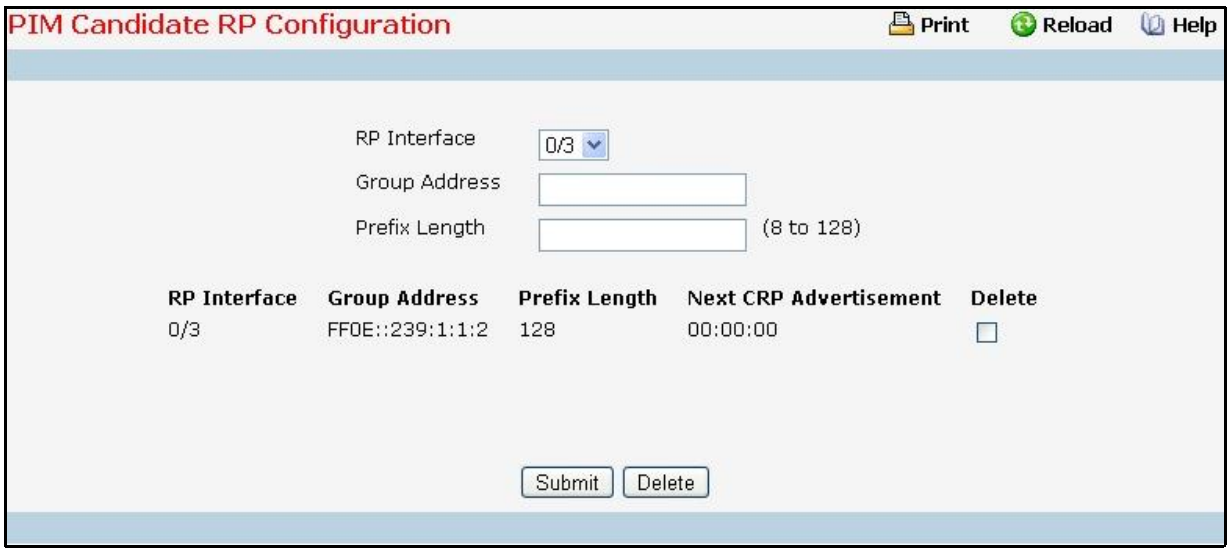
Command Buttons

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.

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

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.

11.9.2.7 Configuring PIM Candidate RP Configuration Page



Selection Criteria

RP Interface - Select the interface for which the Candidate RP has to be configured.

Configurable Data

Group Address - The group address transmitted in Candidate-RP-Advertisements.

Prefix Length - The group address mask transmitted in Candidate-RP-Advertisements.

Delete - Check box to delete the particular entry from the table.

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 - 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.

11.9.2.8 Configuring PIM RP Mapping Summary Page

Non-Configurable Data

RP Address - The IP address of the RP to be used for groups within this group prefix.

Group Address - The IP multicast group address which, when combined with group mask, gives the group prefix for this mapping. This address object is only significant up to prefix length bits. The remainder of the address bits are zero. This is especially important for this field, which is part of the index of this entry. Any non-zero bits would signify an entirely different entry.

Prefix Length - The multicast group prefix length that, when combined with group address, gives the group prefix for this mapping.

Origin - Origin from where this group mapping is learnt.

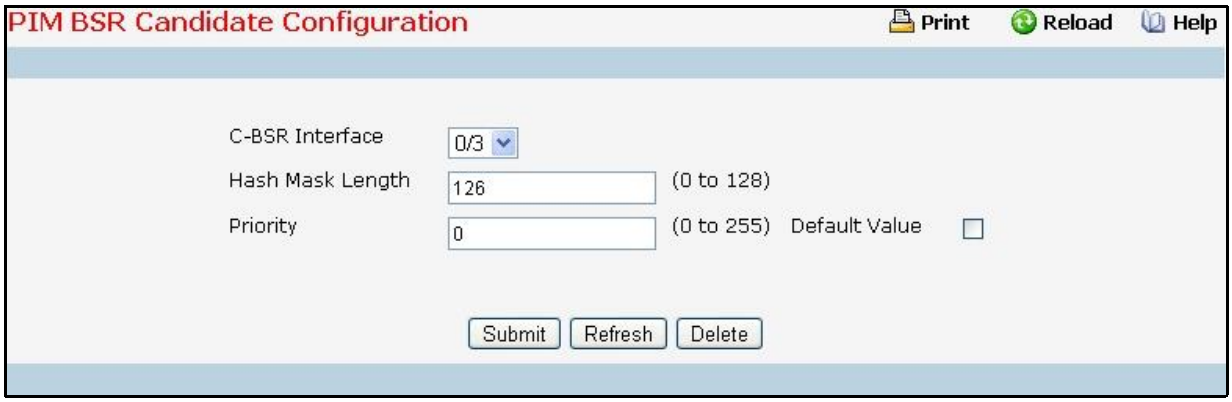
Expiry Time - The minimum time remaining before this entry will be aged out. The value zero indicates that this entry will never be aged out. This field is not-applicable for statically configured entries.

Next CRP Advertisement - The time remaining to send the Next Candidate RP advertisement. This field is not-applicable for statically configured entries.

Command Buttons

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

11.9.2.9 Configuring PIM BSR Candidate Configuration Page



Selection Criteria

C-BSR Interface - Select the interface for which data is to be displayed or configured.

Configurable Data

Hash Mask Length - T 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 126.

Priority - Enter the priority of C-BSR. The valid values are from (0 to 255). Default value is 0.

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.

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

Delete - Deletes the candidate BSR configured on the router.

11.9.2.10 Configuring PIM 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.

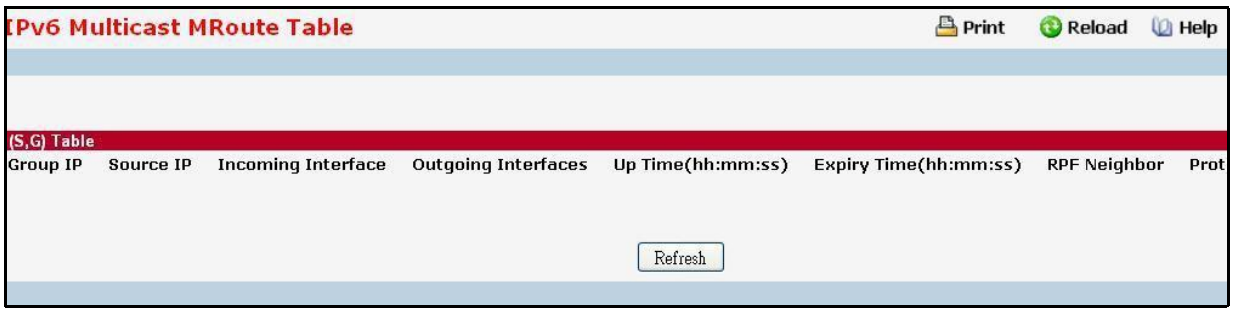
BSR Hash Mask Length - Displays hash mask length of the Elected BSR.

BSR Expiry Time (hh:mm:ss) - Time (in Hours, Minutes, and seconds) in which the learnt elected bootstrap router (BSR) expires.

Command Buttons

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

11.9.3 Viewing IPv6 Multicast MRoute Table



Non-Configurable Data

(*,G)Table

(This table displays the entries for which this router has received MLDv1 Reports. This table is applicable only for PIMSM and will be displayed only when PIMSM is operational and when the above said entries are present.)

Group IP - The IP address of the Multicast Group for which this router has received MLDv1 Reports.

Incoming Interface - The incoming interface on which multicast packets for this source/group arrive.

Outgoing Interface(s) - The list of outgoing interfaces on which multicast packets for this source/group are forwarded.

Up Time - The time (in hours:minutes:seconds) since the entry was created.

Expiry Time - The time (in hours:minutes: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-SM

Flags - The value displayed in this field is valid if the multicast routing protocol running is PIMSM. The default value is RPT.

(S,G)Table

Group IP - The IP address of the Multicast Group for which this router is receiving data.

Source IP - The IP address of the Multicast Source from which this router is receiving data for the Group IP.

Incoming Interface - The incoming interface on which multicast packets for this source/group arrive.

Outgoing Interface(s) - The list of outgoing interfaces on which multicast packets for this source/group are forwarded.

Up Time - The time (in hours:minutes:seconds) since the entry was created.

Expiry Time - The time (in hours:minutes:seconds) before this entry will age out and be removed from the table.

RPF Neighbor - The IP address of the Reverse Path Forwarding neighbor.

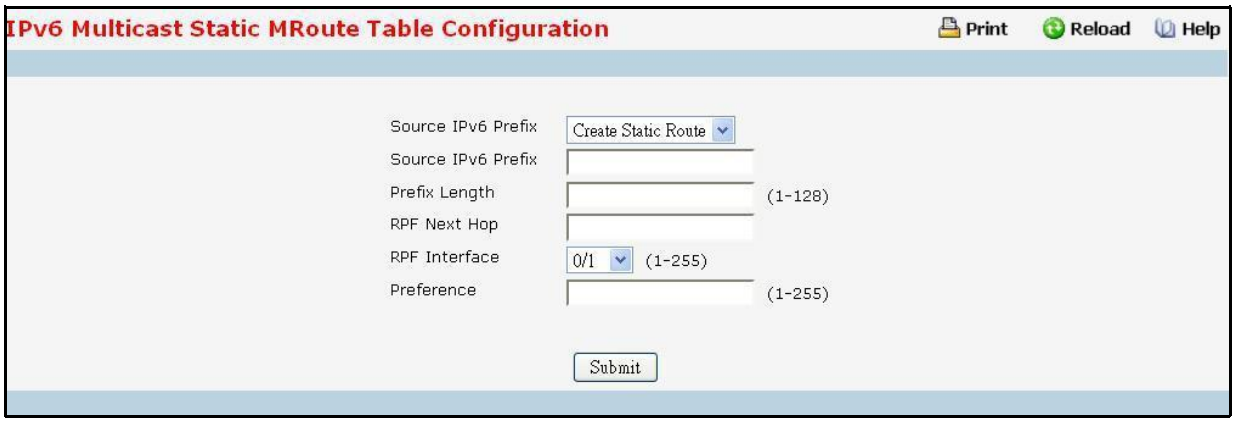
Protocol - The multicast routing protocol which created this entry. The possibilities are:: PIM-DM, PIM-SM, and MLD-Proxy

Flags - The value displayed in this field is valid if the multicast routing protocol running is PIMSM. The possible values are RPT or SPT. For other protocols an "------" is displayed.

Command Buttons

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

11.9.4 Configuring IPv6 Multicast Static MRoute Table Configuration



This page is used to configure a new or existing static mroute entry.

Configurable Data

Source IPv6 Prefix - Enter the IPv6 address of the Multicast data source.

Prefix Length - Enter the Prefix length for the IPv6 address of the Multicast data source to be configured.

RPF Next Hop - Enter the RPF Address for the source range of static mroute entry.

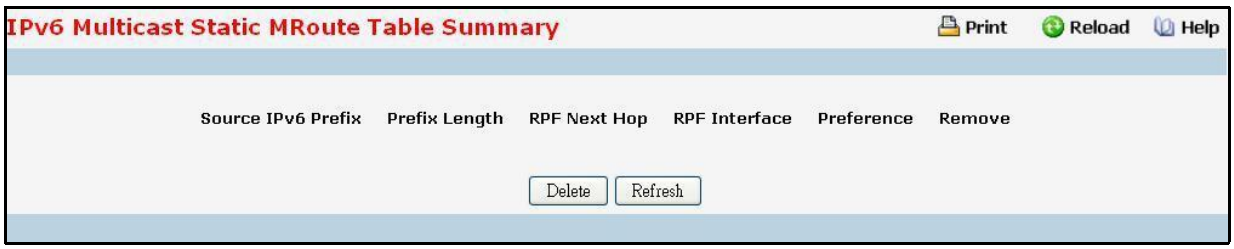
RPF Interface - Enter the RPF interface index if RPF address is link-local.

Preference - Enter the preference with which the static mroute to be considered against other matching static mroute entry for a given source. The valid values are from (1 to 255).

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.

11.9.5 Viewing IPv6 Multicast Static MRoute Table Summary



This page is used to summarize the configured static mroute entries.

Configurable Data

Remove - Check Box to Delete the Selected Static MRoute Entry.

Non-Configurable Data

Source IPv6 Prefix - The IPv6 address of the Multicast data source.

Prefix Length - The Prefix length for the IPv6 address of the Multicast data source.

RPF Next Hop - The RPF Address for the source range of static mroute entry.

RPF Interface - The RPF interface index if RPF address is link-local.

Preference - The preference with which the static mroute to be considered against other matching static mroute entry for a given source.

Command Buttons

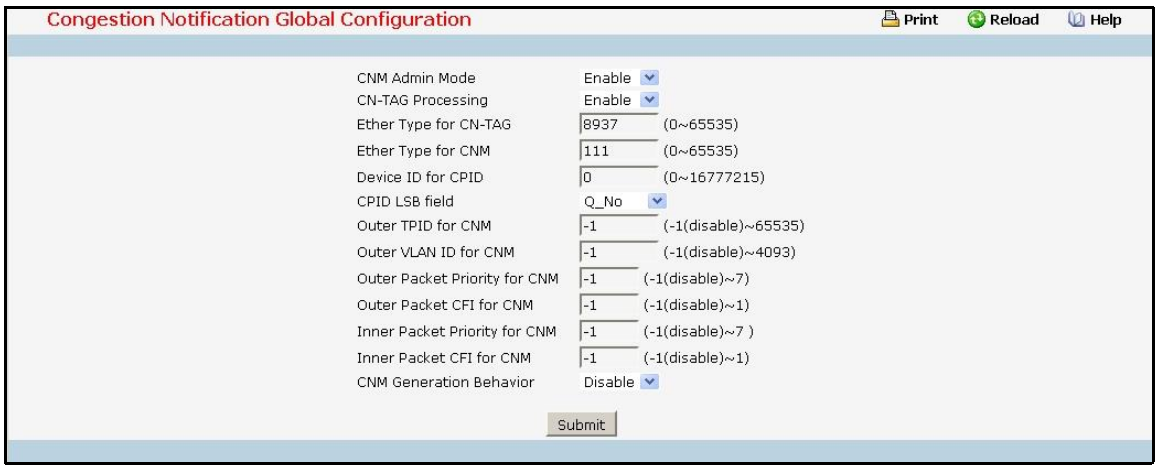
Delete - Deletes the selected static mroute entries in the router. This is used to delete the entries selected using the Checkbox under Remove field.

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

11.10 Data Center

11.10.1 Managing Congestion Notification

11.10.1.1 Configuring Congestion Notification (CN)) Global configuration



Configurable Data

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.

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 4093.

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.

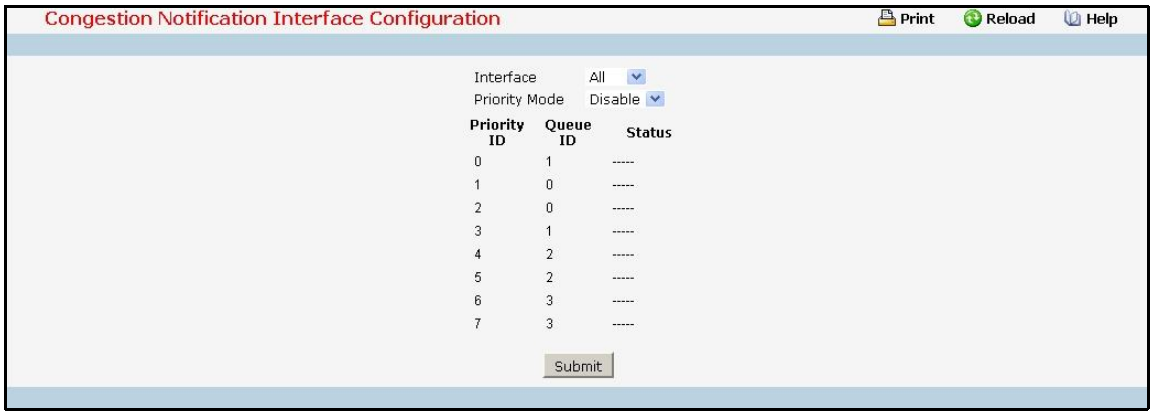
Inner Packet Priority for CNM - Set Inner Packet Priority for Congestion Notification Message (CNM). The system's default Inner Packet Priority for CNM is 0. The valid dot1p range is -1 to 7.

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.

11.10.1.2 Configuring Congestion Notification (CN) Interface configuration



Selection Criteria

Interface - Choose a CN configurable interfaces for setting.

Configurable Data

Priority Mode - Disable all priority ID status for this interface or choose Priority ID from 0 to 7 to Enable the specific priority ID status.

Non-Configurable Data

Priority ID - Specifies the priority ID.

Queue ID - Specifies the queue ID.

Status - Enable or Disable. Show the status of specific priority queue.

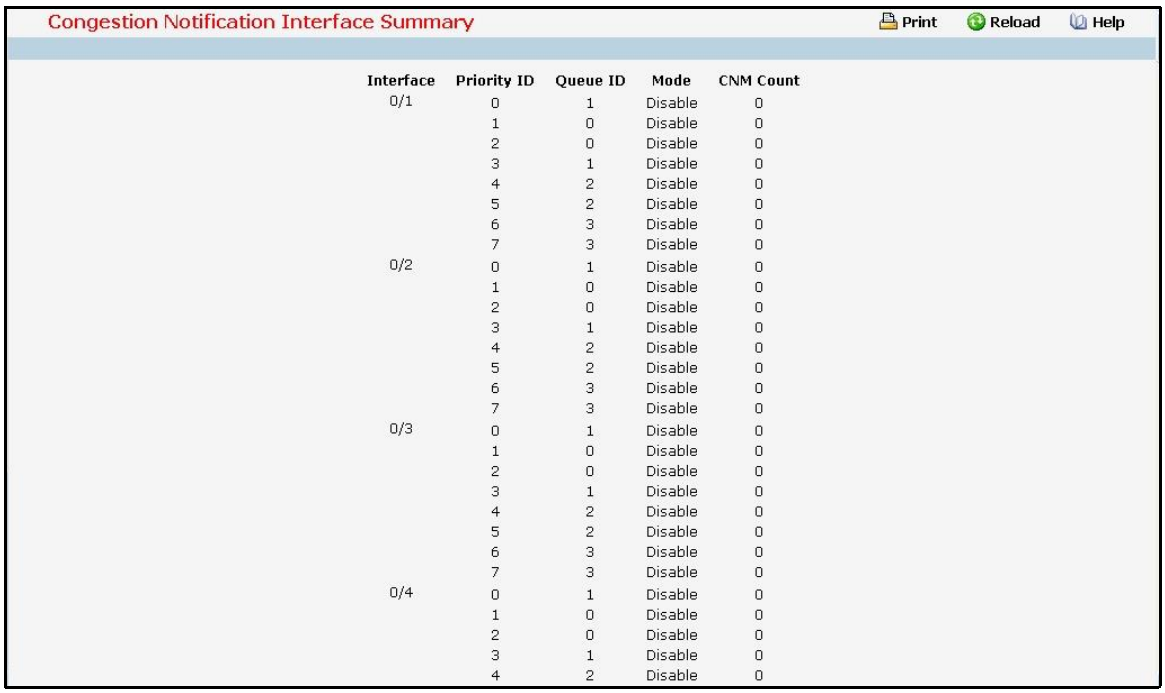
Command Buttons

Enable - Enable the specific priority ID status. Priority ID with the same queue ID has the same staus.

Disable - Disable the specific priority ID status. Priority ID with the same queue ID has the same staus.

Disable All - Disable all priority ID status.

11.10.1.3 Viewing Congestion Notification (CN) interface summary



Interface	Priority ID	Queue ID	Mode	CNM Count
0/1	0	1	Disable	0
	1	0	Disable	0
	2	0	Disable	0
	3	1	Disable	0
	4	2	Disable	0
	5	2	Disable	0
	6	3	Disable	0
	7	3	Disable	0
0/2	0	1	Disable	0
	1	0	Disable	0
	2	0	Disable	0
	3	1	Disable	0
	4	2	Disable	0
	5	2	Disable	0
	6	3	Disable	0
	7	3	Disable	0
0/3	0	1	Disable	0
	1	0	Disable	0
	2	0	Disable	0
	3	1	Disable	0
	4	2	Disable	0
	5	2	Disable	0
	6	3	Disable	0
	7	3	Disable	0
0/4	0	1	Disable	0
	1	0	Disable	0
	2	0	Disable	0
	3	1	Disable	0
	4	2	Disable	0

Non-Configurable Data

Interface - The list of CN configurable interfaces.

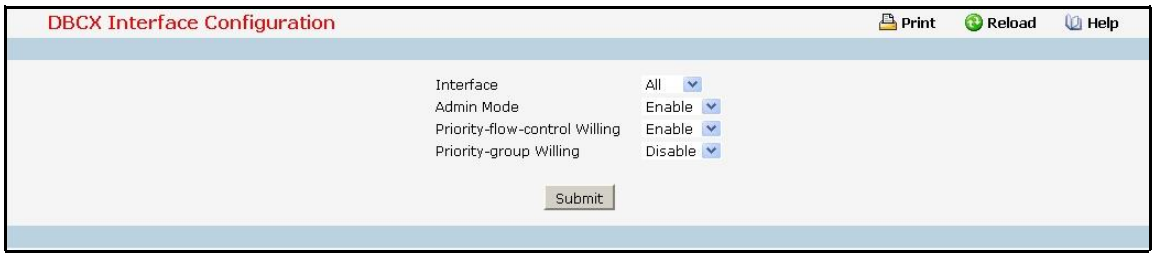
Queue ID - Specifies the ID of priority queues.

Mode - Specifies the mode of priority queues.

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

11.10.2 Managing Data Bridging Exchange

11.10.2.1 Configuring DCBX port configuration



Selection Criteria

Interface - You can use this to set up parameter for an interface.

Configurable Data

Admin Mode - Set administrative mode setting for DCBX

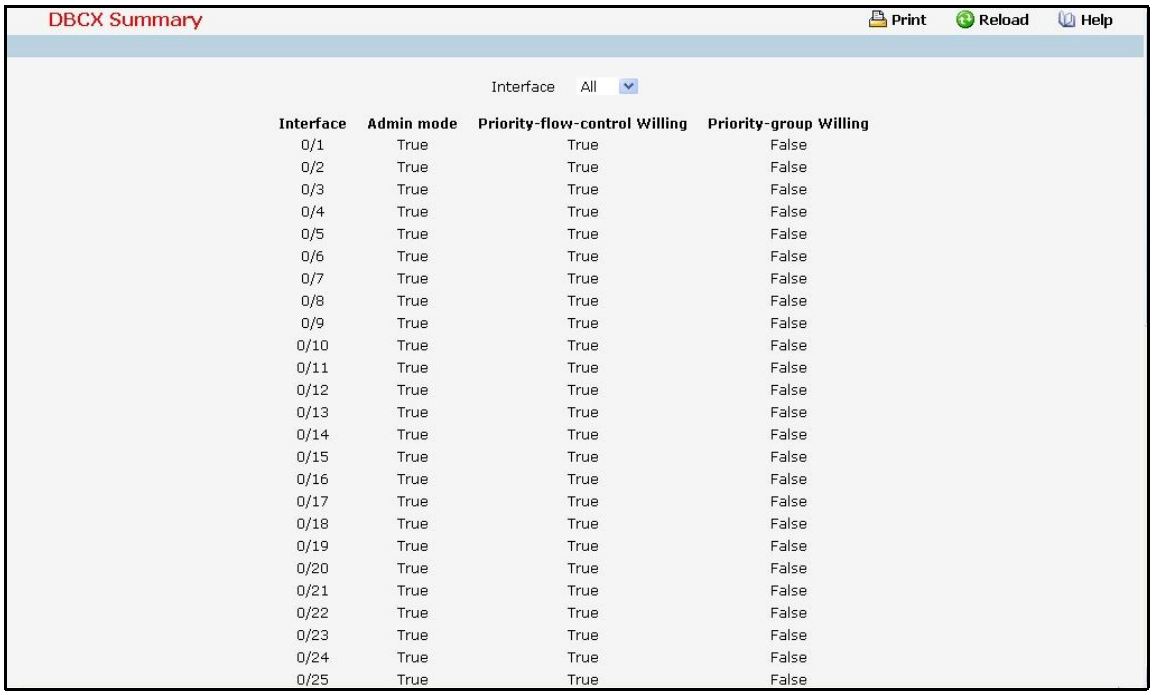
Priority-flow-control Willing - Set willing mode setting for DCBX PFC feature.

Priority-group Willing - Set willing mode setting for DCBX priority group feature.

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.

11.10.2.2 Viewing DCBX Summary



Interface	Admin mode	Priority-flow-control Willing	Priority-group Willing
0/1	True	True	False
0/2	True	True	False
0/3	True	True	False
0/4	True	True	False
0/5	True	True	False
0/6	True	True	False
0/7	True	True	False
0/8	True	True	False
0/9	True	True	False
0/10	True	True	False
0/11	True	True	False
0/12	True	True	False
0/13	True	True	False
0/14	True	True	False
0/15	True	True	False
0/16	True	True	False
0/17	True	True	False
0/18	True	True	False
0/19	True	True	False
0/20	True	True	False
0/21	True	True	False
0/22	True	True	False
0/23	True	True	False
0/24	True	True	False
0/25	True	True	False

Selection Criteria

Interface - You can use this to see parameter for an interface.

Feature - You can use this to get different feature of DCBX such as priority group or PFC

- Priority Flow Control - DCBX's PFC feature
- Priority Group - DCBX's priority group (PG) feature Non-

Configurable Data

Admin Mode - Get administrative mode setting for DCBX

Priority-flow-control Willing - Get willing mode setting for DCBX PFC feature.

Priority-group Willing - Get willing mode setting for DCBX priority group (PG) feature.

---Field of Admin Configuration Type---

Feature - Priority Flow Control or Priority Group

Enable - Get administrative mode setting for DCBX PFC or PG feature

Advertise - Get advertise mode setting for DCBX PFC or PG feature

Willing - Get advertise mode setting for DCBX PFC or PG feature

Priority Mask - Show the action (Drop(0)/No-Drop(1)) to be applied for the corresponding Priority value on the selected interface."Drop" is default.

Group Bandwidth - Get the Scheduling mode of an interface.

Priority Group ID - Get the Scheduling priority map of the PG for an interface Max

Traffic Class - It is always 8

---Field of Operation Type---

Feature - Priority Flow Control or Priority Group

Oper Version - Get opertional version for DCBX PFC or PG feature

Max Version - Get max version for DCBX PFC or PG feature

Errors - Get error reason string- "None", "Cfg Mismatch", "Err Cfg", "Multi-TLVs", "Peer Error", "Multi-Peer", "No TLV",

Operation Mode - Get the operational mode of the PFC or PG for an interface

Syncd With Peer - Get feature sync for DCBX PFC or PG feature

Priority Mask - Get the operational priority map of the PFC for an interface

Group Bandwidth - Get the operational bandwidth of the PG for an interface

Priority Group ID - Get the operational priority map of the PG for an interface Max

Traffic Class - It is always 8

---Field of Peer Configuration Type---

Feature - Priority Flow Control or Priority Group

Local Interface - Which local interface that connect with peer (The same with what port you select to see now in "interface" field)

Status - Get status (Error bit) for Peer DCBX PFC or PG feature

Enable - Get administrative mode setting for Peer DCBX PFC or PG feature

Willing - Get willing mode setting for Peer DCBX PFC or PG feature

Priority Mask - Get priority map for Peer DCBX PFC feature

Group Bandwidth - Get bandwidth of the Peer DCBX PG feature

Priority Group ID - Get priority map for Peer DCBX PG feature

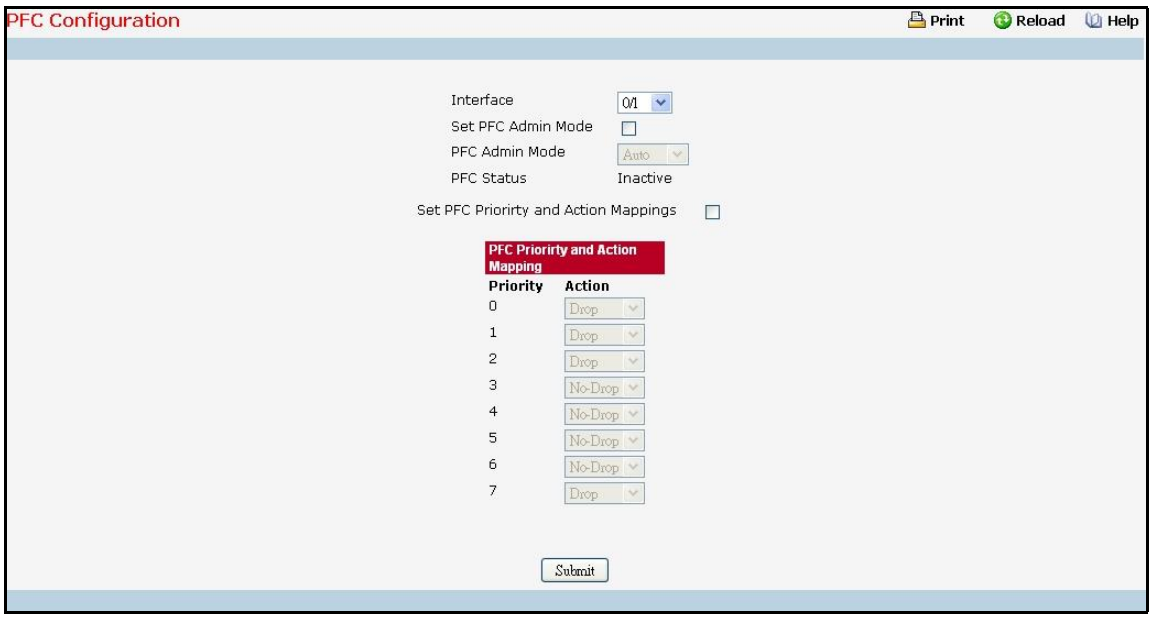
Max Traffic Class - Get the peer number of traffic class.In PFC it is always 8 but in PG it is not always 8

Command Buttons

Refresh - Update the data on the page

11.10.3 Managing PFC

11.10.3.1 Configuring PFC Configuration



Selection Criteria

Interface - Selects the interface to be configured. Select All to specify all interfaces.

Configurable Data

PFC Admin Mode - Enable, disable or auto the PFC for the selected interface. It is disabled by default.

Action - Select the action (Drop/No-Drop) to be applied for the corresponding Priority value on the selected interface. It is No-Drop by default.

Non-Configurable Data

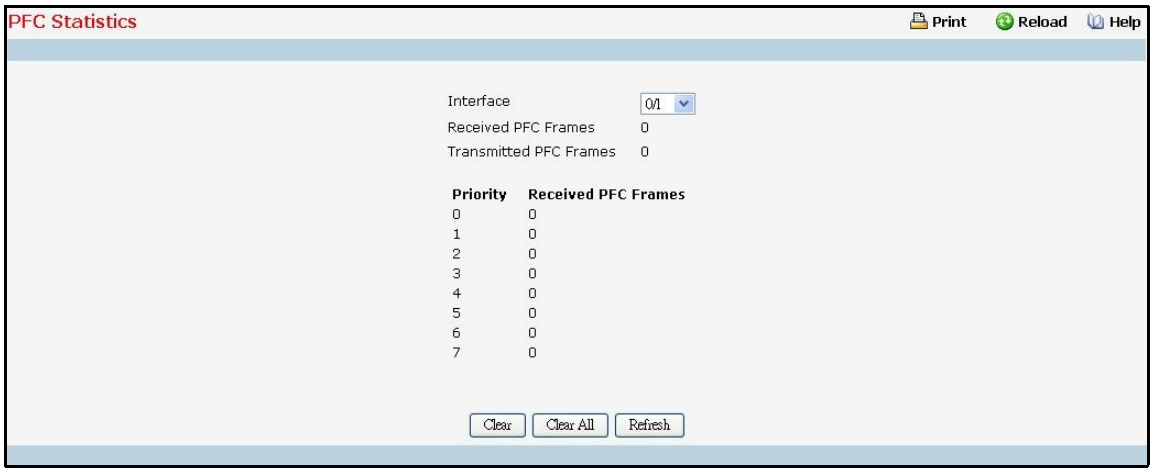
PFC Status - Displays the operational status (Active/Inactive) of PFC on the selected interface.

Priority - This displays the priority value for which an action (Drop/No-Drop) has been configured on the selected interface.

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.

11.10.3.2 Viewing PFC statistics



Selection Criteria

Interface - Select the interface for which data is to be displayed

Non-Configurable Data

Received PFC Frames - This displays the total number of PFC frames that have been received by this interface.

Transmitted PFC Frames - This displays the total number of PFC frames that have been transmitted by this interface.

Priority - This displays the priority value of which the PFC statistics of the selected interface are being shown.

Received PFC Frames - This displays the number of PFC frames that have been received by this interface for this priority.

Command Buttons

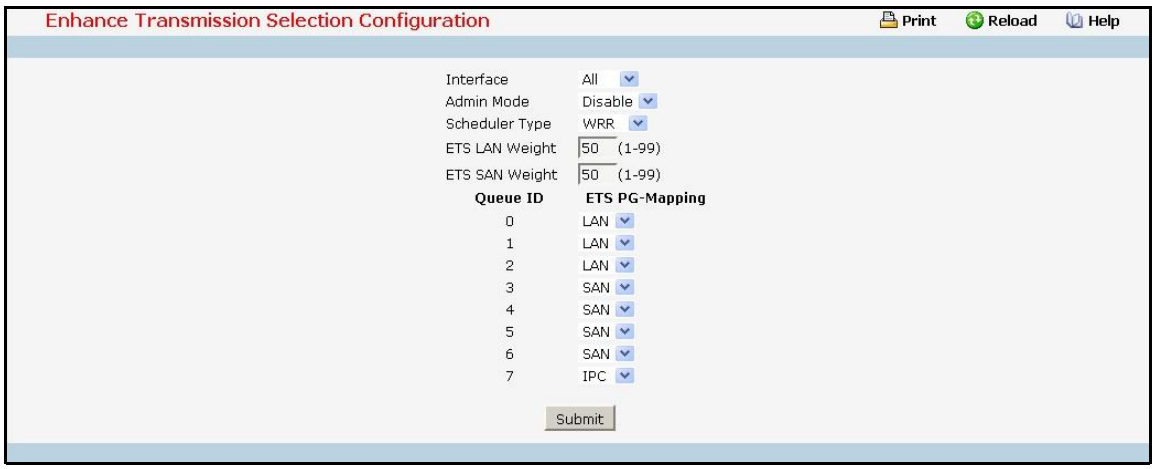
Clear - Clears all the counters, resetting all statistics for this interface to default values.

Clear All - Clears all the counters for all ports, resetting all statistics for all interfaces to default values.

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

11.10.4 Managing ETS

11.10.4.1 Configuring Enhanced Transmission Selection (ETS) interface



Selection Criteria

Interface- Choose a ETS configurable interfaces for setting.

Configurable Data

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.

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.

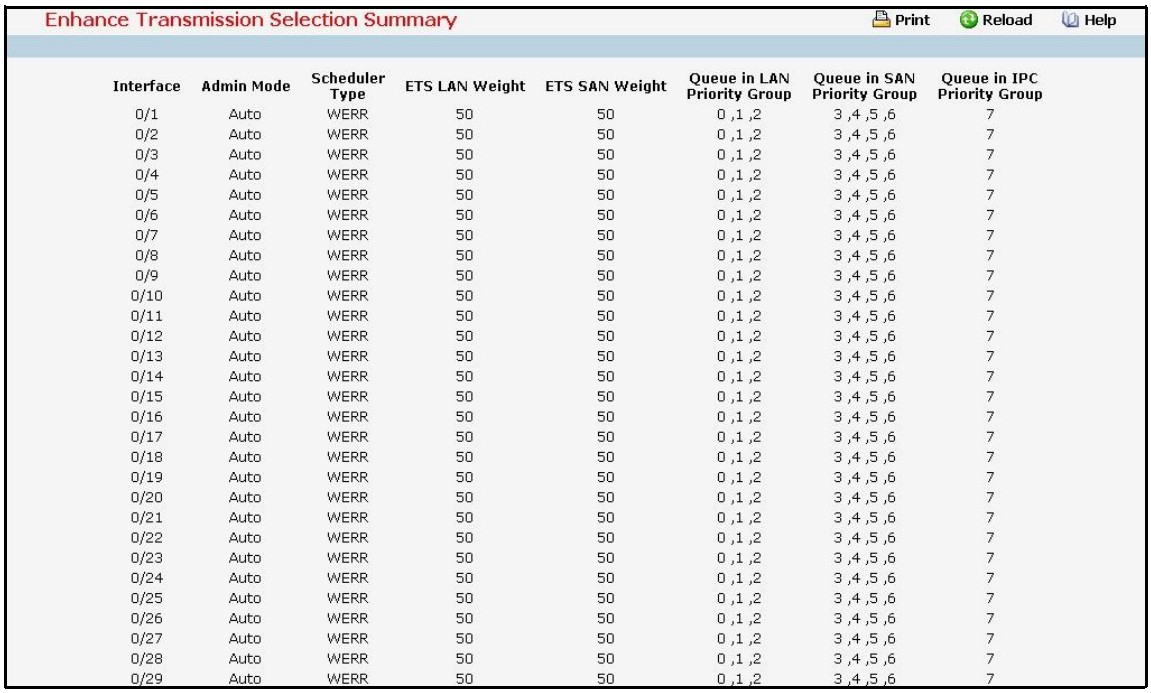
Non-Configurable Data

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.

11.10.4.2 Viewing Enhanced Transmission Selection (ETS) interface status



Enhance Transmission Selection Summary

Print Reload Help

Interface	Admin Mode	Scheduler Type	ETS LAN Weight	ETS SAN Weight	Queue in LAN Priority Group	Queue in SAN Priority Group	Queue in IPC Priority Group
0/1	Auto	WERR	50	50	0 ,1 ,2	3 ,4 ,5 ,6	7
0/2	Auto	WERR	50	50	0 ,1 ,2	3 ,4 ,5 ,6	7
0/3	Auto	WERR	50	50	0 ,1 ,2	3 ,4 ,5 ,6	7
0/4	Auto	WERR	50	50	0 ,1 ,2	3 ,4 ,5 ,6	7
0/5	Auto	WERR	50	50	0 ,1 ,2	3 ,4 ,5 ,6	7
0/6	Auto	WERR	50	50	0 ,1 ,2	3 ,4 ,5 ,6	7
0/7	Auto	WERR	50	50	0 ,1 ,2	3 ,4 ,5 ,6	7
0/8	Auto	WERR	50	50	0 ,1 ,2	3 ,4 ,5 ,6	7
0/9	Auto	WERR	50	50	0 ,1 ,2	3 ,4 ,5 ,6	7
0/10	Auto	WERR	50	50	0 ,1 ,2	3 ,4 ,5 ,6	7
0/11	Auto	WERR	50	50	0 ,1 ,2	3 ,4 ,5 ,6	7
0/12	Auto	WERR	50	50	0 ,1 ,2	3 ,4 ,5 ,6	7
0/13	Auto	WERR	50	50	0 ,1 ,2	3 ,4 ,5 ,6	7
0/14	Auto	WERR	50	50	0 ,1 ,2	3 ,4 ,5 ,6	7
0/15	Auto	WERR	50	50	0 ,1 ,2	3 ,4 ,5 ,6	7
0/16	Auto	WERR	50	50	0 ,1 ,2	3 ,4 ,5 ,6	7
0/17	Auto	WERR	50	50	0 ,1 ,2	3 ,4 ,5 ,6	7
0/18	Auto	WERR	50	50	0 ,1 ,2	3 ,4 ,5 ,6	7
0/19	Auto	WERR	50	50	0 ,1 ,2	3 ,4 ,5 ,6	7
0/20	Auto	WERR	50	50	0 ,1 ,2	3 ,4 ,5 ,6	7
0/21	Auto	WERR	50	50	0 ,1 ,2	3 ,4 ,5 ,6	7
0/22	Auto	WERR	50	50	0 ,1 ,2	3 ,4 ,5 ,6	7
0/23	Auto	WERR	50	50	0 ,1 ,2	3 ,4 ,5 ,6	7
0/24	Auto	WERR	50	50	0 ,1 ,2	3 ,4 ,5 ,6	7
0/25	Auto	WERR	50	50	0 ,1 ,2	3 ,4 ,5 ,6	7
0/26	Auto	WERR	50	50	0 ,1 ,2	3 ,4 ,5 ,6	7
0/27	Auto	WERR	50	50	0 ,1 ,2	3 ,4 ,5 ,6	7
0/28	Auto	WERR	50	50	0 ,1 ,2	3 ,4 ,5 ,6	7
0/29	Auto	WERR	50	50	0 ,1 ,2	3 ,4 ,5 ,6	7

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.

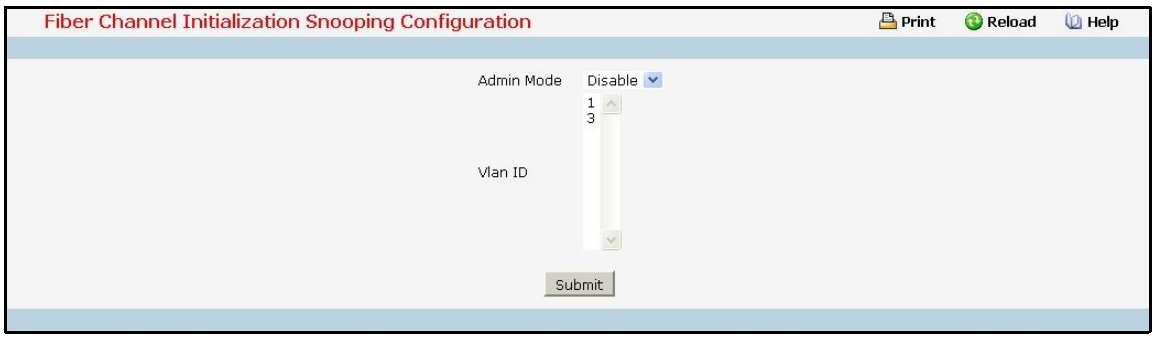
Queue in LAN Priority Group - List of queues in LAN priority group.

Queue in SAN Priority Group - List of queues in SAN priority group.

Queue in IPC Priority Group - List of queues in IPC priority group.

11.10.5 Managing FIP-Snooping

11.10.5.1 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 FIP Snoopingand stop the FIP Snooping process.

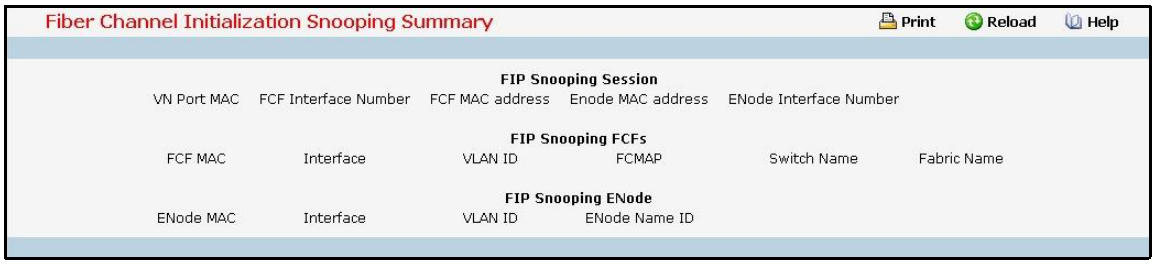
The system's default FIP Snooping admin mode is disabled.

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.

11.10.5.2 Viewing FIP-Snooping Status



Non-Configurable Data

FIP Snooping Session

- VN Port MAC - FCoE MAC address that is used to send the FCoE packets.

FCF Interface Number - The interface to which the FCF is connected

- FCF MAC address - MAC address of the FCF..
- ENode MAC address - MAC address of the ENode.
- ENode Interface Number - The interface to which the ENode is connected FIP

Snooping FCFs

- FCF MAC - MAC address of the FCF.
- FCF Interface Number - 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.

- Switch Name - Name ID.
- Fabric Name - Name of the FCF. FIP

Snooping ENode

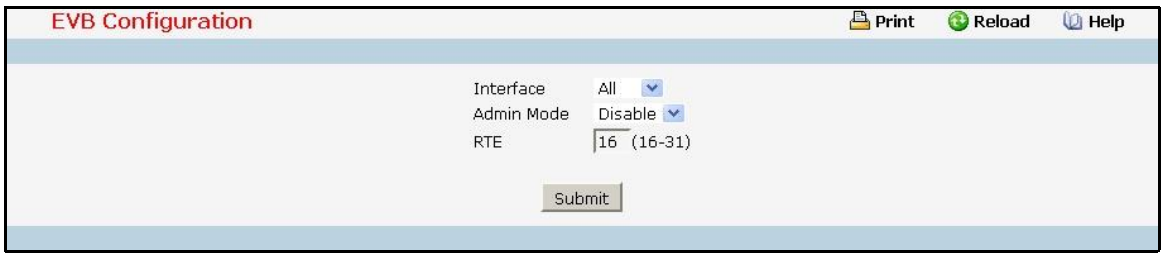
- ENode MAC - MAC address of the ENode.
- ENode Interface Number - Name of the interface to which the ENode is connected.

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

- ENode Name ID - Name ID.

11.10.6 Managing EVB

11.10.6.1 EVB Configuration



Selection Criteria

Interface - You can use this to set up EVB parameter for an interface.

Admin Mode - Set administrative mode for EVB of an interface(s)

Configurable Data

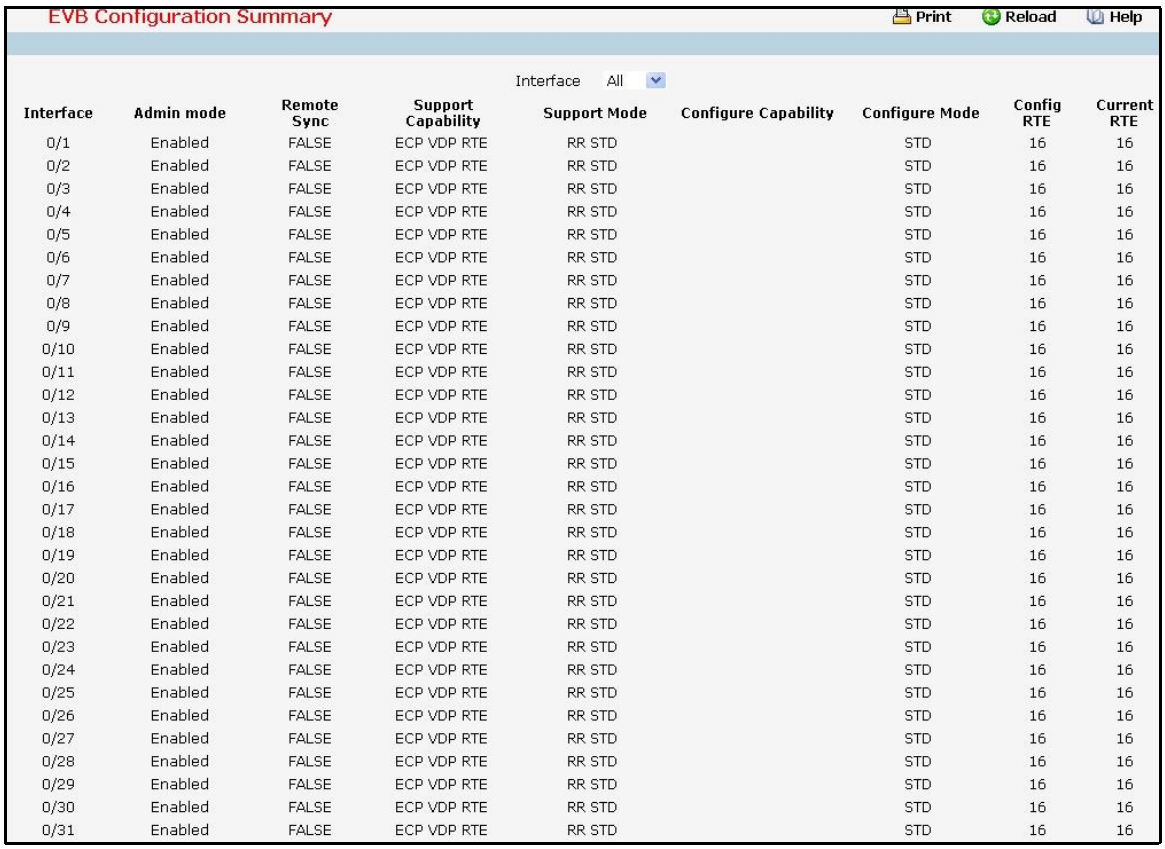
RTE - Get or Set Retransmission Exponent for a interface(s), Range From 16-31.

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.

11.10.6.2 Viewing EVB Configuration Summary

This menu will display an entry for EVB configuration of every interface



EVB Configuration Summary

Print Reload Help

Interface All

Interface	Admin mode	Remote Sync	Support Capability	Support Mode	Configure Capability	Configure Mode	Config RTE	Current RTE
0/1	Enabled	FALSE	ECP VDP RTE	RR STD		STD	16	16
0/2	Enabled	FALSE	ECP VDP RTE	RR STD		STD	16	16
0/3	Enabled	FALSE	ECP VDP RTE	RR STD		STD	16	16
0/4	Enabled	FALSE	ECP VDP RTE	RR STD		STD	16	16
0/5	Enabled	FALSE	ECP VDP RTE	RR STD		STD	16	16
0/6	Enabled	FALSE	ECP VDP RTE	RR STD		STD	16	16
0/7	Enabled	FALSE	ECP VDP RTE	RR STD		STD	16	16
0/8	Enabled	FALSE	ECP VDP RTE	RR STD		STD	16	16
0/9	Enabled	FALSE	ECP VDP RTE	RR STD		STD	16	16
0/10	Enabled	FALSE	ECP VDP RTE	RR STD		STD	16	16
0/11	Enabled	FALSE	ECP VDP RTE	RR STD		STD	16	16
0/12	Enabled	FALSE	ECP VDP RTE	RR STD		STD	16	16
0/13	Enabled	FALSE	ECP VDP RTE	RR STD		STD	16	16
0/14	Enabled	FALSE	ECP VDP RTE	RR STD		STD	16	16
0/15	Enabled	FALSE	ECP VDP RTE	RR STD		STD	16	16
0/16	Enabled	FALSE	ECP VDP RTE	RR STD		STD	16	16
0/17	Enabled	FALSE	ECP VDP RTE	RR STD		STD	16	16
0/18	Enabled	FALSE	ECP VDP RTE	RR STD		STD	16	16
0/19	Enabled	FALSE	ECP VDP RTE	RR STD		STD	16	16
0/20	Enabled	FALSE	ECP VDP RTE	RR STD		STD	16	16
0/21	Enabled	FALSE	ECP VDP RTE	RR STD		STD	16	16
0/22	Enabled	FALSE	ECP VDP RTE	RR STD		STD	16	16
0/23	Enabled	FALSE	ECP VDP RTE	RR STD		STD	16	16
0/24	Enabled	FALSE	ECP VDP RTE	RR STD		STD	16	16
0/25	Enabled	FALSE	ECP VDP RTE	RR STD		STD	16	16
0/26	Enabled	FALSE	ECP VDP RTE	RR STD		STD	16	16
0/27	Enabled	FALSE	ECP VDP RTE	RR STD		STD	16	16
0/28	Enabled	FALSE	ECP VDP RTE	RR STD		STD	16	16
0/29	Enabled	FALSE	ECP VDP RTE	RR STD		STD	16	16
0/30	Enabled	FALSE	ECP VDP RTE	RR STD		STD	16	16
0/31	Enabled	FALSE	ECP VDP RTE	RR STD		STD	16	16

Selection Criteria

Interface - You can use this to see EVB parameter for an interface.

Non-Configurable Data

Interface - Interface of EVB.

EVB Enable - Get administrative mode for EVB of an interface(s)

Remote Sync - Check if the interface is sync with remote party (ECP enabled)

Support Capability - Get EVB config capability for an interface(s)

Support Mode - Get EVB supported forwarding capability for an interface(s)

Configure Capability - Get EVB operational capability for an interface(s)

Configure Mode - Get EVB operational forwarding capability for an interface(s)

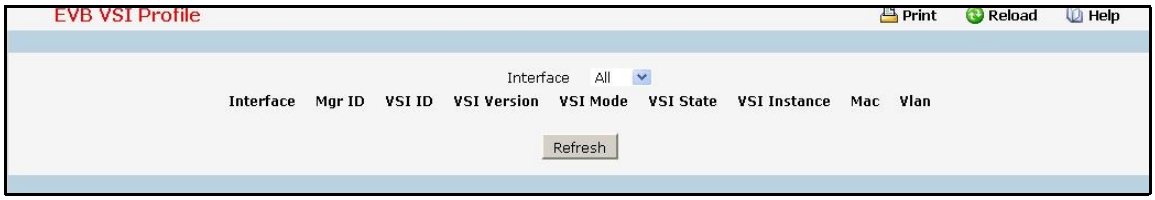
Config RTE - Get RTE for an interface(s)

Current RTE - Get ECP Retransmission Exponent (RTE)

Command Buttons

Refresh - Update the data.

11.10.6.3 Viewing EVB VSI Profile



Selection Criteria

Interface - You can use this to see EVB VSI parameter for an interface

Non-Configurable Data

Interface- You can use this to set up EVB parameter for an interface.

Mgr ID - Get mgr id of the VSI profile

VSI ID - Get VSI ID of the VSI profile

VSI Version - Get version of the VSI profile

VSI Mode - Get VSI mode of the VSI profile

VSI State - Get VSI State of the VSI profile

VSI Instance - Get instance id of the VSI profile

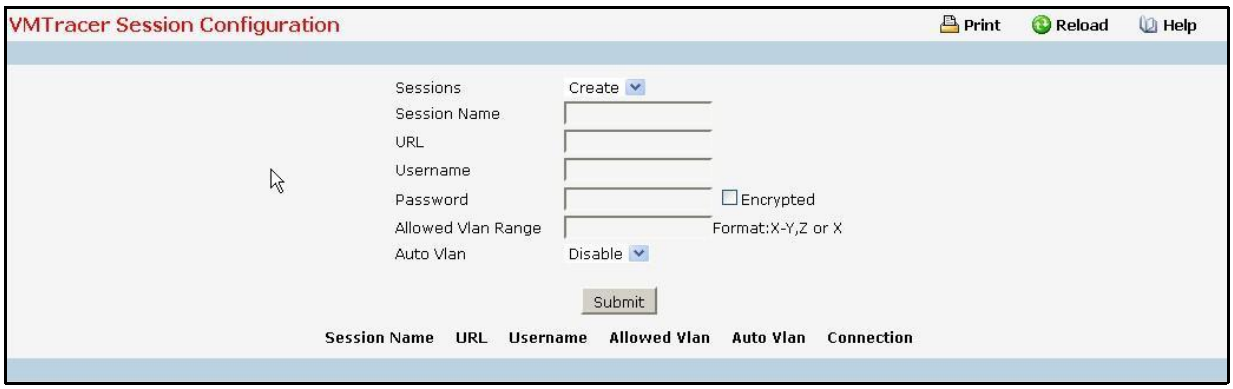
MAC VLAN - Get mac VALN list of the VSI profile

Command Buttons

Refresh - Update the data.

11.10.7 Managing VM Tracer

11.10.7.1 Configuring VM Tracer Session



Configurable Data

Sessions - Creates a new vmtracer session or loads an existing session for editing. The switch supports a maximum of four VM Tracer sessions.

Session Name - The label assigned to the VM Tracer session

URL - Location of the vCenter server. Valid formats include IP address (dotted decimal notation) and fully qualified domain name.

Username - The switch's account name on the vCenter server. The switch uses this user name to access vCenter information

Password - The token that authorizes the username to the vCenter associated with the VM Tracer mode session.

Auto Vlan - Disables auto provisioning, which prevents the creation or deletion of VLANs regardless of VM activity.

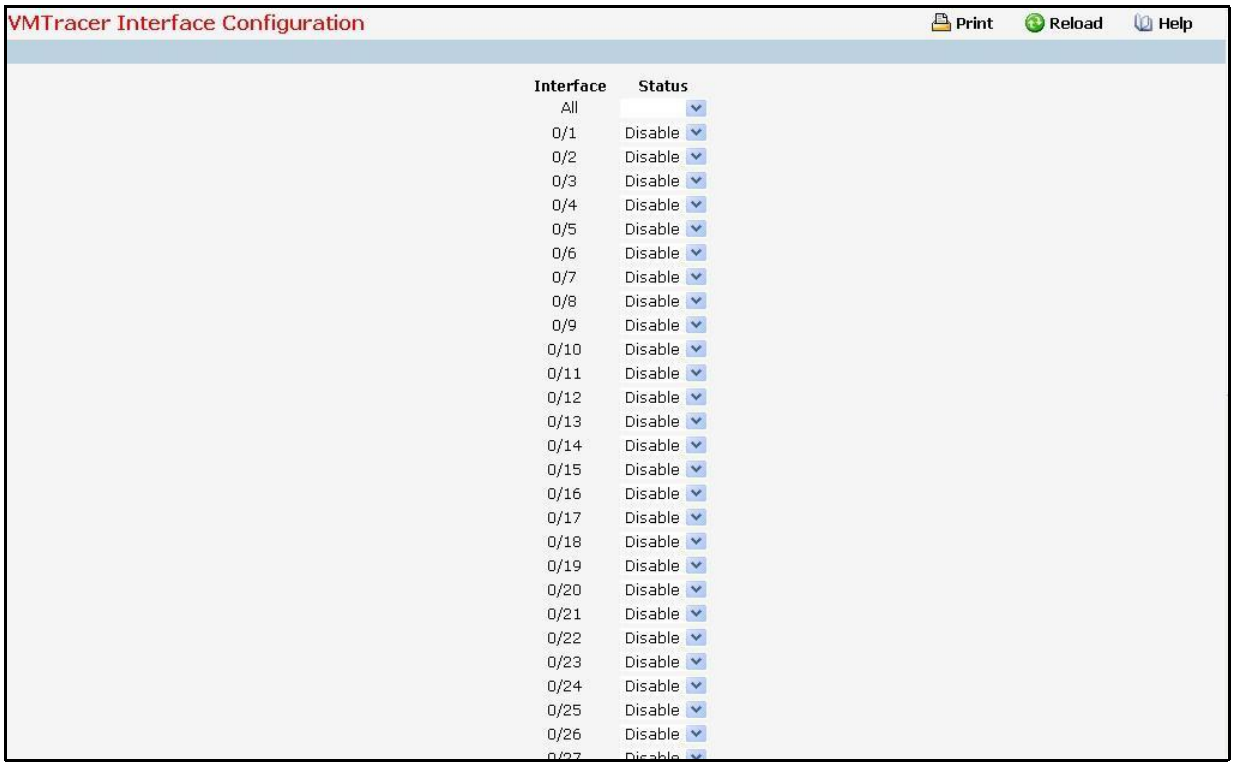
Allow-Vlan Range - The VLANs that may be added when a VM is added or moved from the hypervisor connected to the session specified by the vmtracer mode. By default, all VLANs are allowed.

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 VMTrace. You are not allowed to delete the default VLAN.

11.10.7.2 Configuring VM Tracer Interface



Configurable Data

Status - VM Tracer Interface administrate mode which are Enable and Disable.

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.

11.10.7.3 Viewing VM Tracer Summary

Configurable Data

VM Name - Name of the virtual machine

Interface - The switch's interface that connects to VM host

VM Adapter(vnic) - the vistual machine's interface

Mac - The MAC address associated to VM Adapter.

Port Group - The port group associated to VM host.

VLAN - The VLAN associated to portgroup that the VM use.

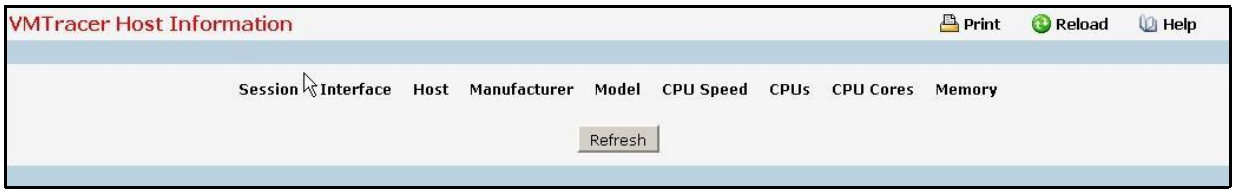
Switch - The name of the virtual switch associated to VM host

Host - The name of the VM host

Command Buttons

Refresh - 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.

11.10.7.4 Viewing VM Tracer Host Information



Non-Configurable Data

Session - Name of the vmtracer session

Interface - The switch's interface that connects to host

Host - The name of VM host

Manufacturer - Hardware vender identification of VM host.

Model - System model identification of VM host.

CPU Speed - The host's machine cpu speed

CPUs - The CPU speed of the VM host

CPU Cores - The number of physical cpu cores on the VM host

Memory - Total amount of physical memory on the VM host

Command Buttons

Refresh - 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.