ECS4660-28F Layer 3 Gigabit Ethernet Switch

Management Guide

www.edge-core.com

Management Guide

ECS4660-28F Gigabit Ethernet Switch

Layer 3 Switch
with 24 Gigabit Ethernet Ports (SFP),
2 10G Ethernet Ports (XSFP), and
2 Slots for Optional 10G Modules

ECS4660-28F
E102013/ST-R03
149100000140A

About This Guide

Purpose This guide gives specific information on how to operate and use the management functions of the switch.

Audience The guide is intended for use by network administrators who are responsible for operating and maintaining network equipment; consequently, it assumes a basic working knowledge of general switch functions, the Internet Protocol (IP), and Simple Network Management Protocol (SNMP).

Conventions The following conventions are used throughout this guide to show information:

Note: Emphasizes important information or calls your attention to related features or instructions.

Caution: Alerts you to a potential hazard that could cause loss of data, or damage the system or equipment.

Warning: Alerts you to a potential hazard that could cause personal injury.

Related Publications The following publication details the hardware features of the switch, including the physical and performance-related characteristics, and how to install the switch:

The *Installation Guide*

Also, as part of the switch’s software, there is an online web-based help that describes all management related features.

REVISION HISTORY

This section summarizes the changes in each revision of this guide.

OCTOBER 2013 REVISION

This is the third release of this guide. This guide is valid for software release V1.2.2.0. It includes information on the following changes:

- Updated information in Parameters section under "Configuring the Console Port" on page 172.
- Updated information in Parameters section under "Configuring Telnet Settings" on page 174.
- Updated Command Usage and Parameters sections under "Configuring by Port List" on page 182.
- Updated descriptive text under "Configuring by Port Range" on page 184.
- Added "Configuring History Sampling" on page 196.
- Temporarily removed “Sampling Traffic Flows.”
- Updated Parameters section under "Enabling QinQ Tunneling on the Switch" on page 247.
- Added "Creating CVLAN to SPVLAN Mapping Entries" on page 248.
- Added "Mapping Ingress DSCP Values to Internal DSCP Values" on page 314.
- Updated Command Usage and Parameters sections under "Attaching a Policy Map to a Port" on page 339.
- Updated Parameters section under "Binding a Port to an Access Control List" on page 408.
- Updated Parameters section under "Configuring Global Settings for ARP Inspection" on page 411.
- Added "DoS Protection" on page 431.
- Added "IPv6 Source Guard" on page 438.
- Updated Table 34, "Supported Notification Messages," on page 490.
- Updated Parameters section under "Configuring IGMP Snooping and Query Parameters" on page 613.
- Updated Parameters section under "Configuring MVR Domain Settings" on page 660.
- Updated Parameters section under "Configuring MVR6 Domain Settings" on page 677.

- Updated Parameters section under "Using the Trace Route Function" on page 746.
- Added commands "show watchdog" on page 909 and "watchdog software" on page 909.
- Updated syntax for command "delete" on page 917.
- Updated range for command "exec-timeout" on page 925.
- Added the commands "clock summer-time (date)" on page 951, "clock summer-time (predefined)" on page 953, and "clock summer-time (recurring)" on page 954.
- Updated displayed data for the command "show snmp" on page 999.
- Updated syntax for "snmp-server enable traps" on page 1000.
- Added the command "snmp-server enable port-traps mac-notification" on page 1003 and "show snmp-server enable port-traps" on page 1004.
- Updated the command under "Flow Sampling Commands" on page 1025.
- Updated syntax for the command "ip source-guard binding" on page 1134, "ip source-guard max-binding" on page 1137, and "show ip source-guard binding" on page 1139.
- Added the commands "ip source-guard mode" on page 1138 and "clear ip source-guard binding blocked" on page 1138.
- Updated syntax for the command "ip arp inspection validate" on page 1149.
- Updated syntax for the command "traffic-segmentation uplink/downlink" on page 1159.
- Updated syntax for the command "ip access-group" on page 1168, "ipv6 access-group" on page 1174, and "mac access-group" on page 1179.
- Added the command "clear access-list hardware counters" on page 1184.
- Updated syntax for the command "show access-list" on page 1185.
- Updated syntax and command usage sections for the command "capabilities" on page 1189.
- Added the command "discard" on page 1191 and "show discard" on page 1197.
- Updated information for the command "media-type" on page 1193.

- Updated command usage section for the command "negotiation" on page 1194.
- Removed the command “speed-duplex.”
- Moved the switchport packet-rate command from Interface Commands chapter to Congestion Control Commands on page 1241.
- Added the commands "transceiver-threshold-auto" on page 1205, and "transceiver-threshold-monitor" on page 1206.
- Updated description of all other transceiver threshold command from page 1206 to page 1212.
- Added "Loopback Detection Commands" on page 1259.
- Added the command "spanning-tree tc-prop-stop" on page 1300.
- Updated introductory text and command usage section for the command "interface vlan" on page 1345.
- Updated syntax for the command "show queue mode" on page 1391.
- Updated syntax for the command "show qos map ip-port-dscp" on page 1403.
- Added the command "ip igmp snooping priority" on page 1428.
- Added the commands "ip igmp authentication" on page 1451 and "show ip igmp authentication" on page 1456.
- Added "MLD Filtering and Throttling" on page 1469.
- Added the command "mvr priority" on page 1482.
- Added the commands "clear mvr6 groups" on page 1506 and "clear mvr6 statistics" on page 1507.
- Updated TTL range for the command "ethernet cfm linktrace" on page 1592.
- Added command "clear efm oam event-log" on page 1608.
- Added information about configuring an address for tunnels in the command "ipv6 address" on page 1665, and "ipv6 address eui-64" on page 1667.
- Updated syntax for the command "traceroute6" on page 1681.
- Added the commands "ipv6 nd managed-config-flag" on page 1685, "ipv6 nd other-config-flag" on page 1686, "ipv6 nd prefix" on page 1690, "ipv6 nd ra interval" on page 1691, "ipv6 nd ra lifetime" on page 1692, "ipv6 nd ra router-preference" on page 1692, and "ipv6 nd ra suppress" on page 1693.

November 2012 Revision

This is the second release of this guide. This guide is valid for software release V1.2.0.0. It includes information on the following changes:

- Removed information on Option 43 in "Downloading a Configuration File Referenced by a DHCP Server" on page 115.
- Updated parameter description in "Displaying Hardware/Software Versions" on page 151.
- Updated web page for "Setting the Time Zone" on page 171.
- Updated parameter description in "Resetting the System" on page 177.
- Added "Configuring Remote Port Mirroring" on page 188.
- Added “Timeout Mode” under "Configuring a Dynamic Trunk" on page 207.
- Updated parameter list under "Configuring VLAN Groups" on page 228.
- Added "Configuring VLAN Translation" on page 259.
- Added parameters under "Configuring Loopback Detection" on page 274.
- Added parameters under "Configuring a Class Map" on page 326.
- Updated parameters under "Configuring AAA Authorization" on page 360.
- Added parameters under "DHCP Snooping Configuration" on page 446.
- Added parameter under "Configuring Ports for DHCP Snooping" on page 449.
- Added parameters under "Configuring LLDP Interface Attributes" on page 461.
- Added parameters under "Displaying LLDP Remote Device Information" on page 470.
- Added sfpThresholdAlarmWarnTrap to Table 34, "Supported Notification Messages," on page 490.
- Updated description for ERPS version 2 under "Ethernet Ring Protection Switching" on page 523.
- Added "PTP Configuration" on page 594.
- Added parameters under "Configuring MVR Global Settings" on page 658.

- Added parameters under "Configuring MVR6 Global Settings" on page 675.
- Added RA Mode under "Configuring IPv6 Interface Settings" on page 697.
- Updated Command Usage section under "Specifying a DHCP Client Identifier" on page 720.
- Added "Configuring the PPPoE Intermediate Agent" on page 735.
- Added IPv6 information under "Enabling Multicast Routing Globally" on page 828 and "Displaying the Multicast Routing Table" on page 829.
- Added information on PIM6-SM under "Configuring PIMv6 for IPv6" on page 849.
- Added information on PIM6-SM "Configuring PIMv6 Interface Settings" on page 850.
- Added "Configuring Global PIM6-SM Settings" on page 856.
- Added "Configuring a PIM6 BSR Candidate" on page 858.
- Added "Configuring a PIM6 Static Rendezvous Point" on page 859.
- Added "Configuring a PIM6 RP Candidate" on page 861.
- Added "Displaying the PIM6 BSR Router" on page 863.
- Added "Displaying RP Mapping" on page 865.
- Added "ptp e-latency" on page 962.
- Added "ptp in-latency" on page 963.
- Added "Synchronous Ethernet" on page 979.
- Added "DHCPv6 Snooping" on page 1126.
- Added "IPv6 Source Guard" on page 1140.
- Added "lacp timeout" on page 1223.
- Added "RSPAN Mirroring Commands" on page 1231.
- Updated command set for ERPS under "ERPS Commands" on page 1305.
- Added RSPAN parameter to "vlan" on page 1344.
- Added "Configuring VLAN Translation" on page 1364.

- Updated parameter description for "ethernet cfm cc ma interval" on page 1581.
- Updated Command Usage section for "ip dhcp client class-id" on page 1625.
- Added "ipv6 nd raguard" on page 1688.
- Added "IPv6 to IPv4 Tunnels" on page 1696.
- Updated parameter description for "show ip route" on page 1726.
- Added “tunnel” parameter to "ipv6 route" on page 1730.
- Added "Border Gateway Protocol (BGPv4)" on page 1818.
- Added "Policy-based Routing for BGP" on page 1897.
- Updated Command Usage section under "router pim6" on page 1951.
- Updated Command Usage section under "ipv6 pim" on page 1951.

MARCH 2012 REVISION

This is the first version of this guide. This guide is valid for software release V1.0.0.0.

CONTENTS

ABOUT THIS GUIDE 5

CONTENTS 13

FIGURES 65

TABLES 81

SECTION I GETTING STARTED 91

1 INTRODUCTION 93

Key Features 93

Description of Software Features 95

IP Routing 99

Equal-cost Multipath Load Balancing 100

Address Resolution Protocol 100

System Defaults 102

2 INITIAL SWITCH CONFIGURATION 105

Connecting to the Switch 105

Configuration Options 105

Required Connections 106

Remote Connections 107

Basic Configuration 108

Console Connection 108

Setting Passwords 108

Setting an IP Address 109

Downloading a Configuration File Referenced by a DHCP Server 115

Enabling SNMP Management Access 116

Managing System Files 119

Saving or Restoring Configuration Settings 119

SECTION II WEB CONFIGURATION 121

3 USING THE WEB INTERFACE 123

Connecting to the Web Interface 123

Navigating the Web Browser Interface 124

Home Page 124

Configuration Options 125

Panel Display 125

Main Menu 126

4 BASIC MANAGEMENT TASKS 149

Displaying System Information 149

Displaying Hardware/Software Versions 151

Configuring Support for Jumbo Frames 152

Displaying Bridge Extension Capabilities 153

Managing System Files 155

Copying Files via FTP/TFTP or HTTP 155

Saving the Running Configuration to a Local File 157

Setting The Start-Up File 158

Showing System Files 159

Automatic Operation Code Upgrade 160

Setting the System Clock 164

Setting the Time Manually 164

Setting the SNTP Polling Interval 165

Configuring NTP 166

Configuring Time Servers 167

Setting the Time Zone 171

Configuring the Console Port 172

Configuring Telnet Settings 174

Displaying CPU Utilization 175

Displaying Memory Utilization 176

Resetting the System 177

5 INTERFACE CONFIGURATION 181

Port Configuration 182

Configuring by Port List 182

Configuring by Port Range 184

Displaying Connection Status 185

Configuring Local Port Mirroring 186

Configuring Remote Port Mirroring 188

Showing Port or Trunk Statistics 192

Configuring History Sampling 196

Displaying Transceiver Data 200

Configuring Transceiver Thresholds 201

Trunk Configuration 204

Configuring a Static Trunk 205

Configuring a Dynamic Trunk 207

Displaying LACP Port Counters 213

Displaying LACP Settings and Status for the Local Side 214

Displaying LACP Settings and Status for the Remote Side 216

Configuring Load Balancing 217

Traffic Segmentation 219

Enabling Traffic Segmentation 219

Configuring Uplink and Downlink Ports 220

VLAN Trunking 222

6 VLAN CONFIGURATION 225

IEEE 802.1Q VLANs 225

Configuring VLAN Groups 228

Adding Static Members to VLANs 231

Configuring Dynamic VLAN Registration 235

Private VLANs 238

Creating Private VLANs 239

Associating Private VLANs 240

Configuring Private VLAN Interfaces 242

IEEE 802.1Q Tunneling 243

Enabling QinQ Tunneling on the Switch 247

Creating CVLAN to SPVLAN Mapping Entries 248

Adding an Interface to a QinQ Tunnel 250

Protocol VLANs 251

Configuring Protocol VLAN Groups 252

Mapping Protocol Groups to Interfaces 253

Configuring IP Subnet VLANs 256

Configuring MAC-based VLANs 258

Configuring VLAN Translation 259

7 ADDRESS TABLE SETTINGS 263

Configuring MAC Address Learning 263

Setting Static Addresses 265

Changing the Aging Time 267

Displaying the Dynamic Address Table 268

Clearing the Dynamic Address Table 269

8 SPANNING TREE ALGORITHM 271

Overview 271

Configuring Loopback Detection 274

Configuring Global Settings for STA 276

Displaying Global Settings for STA 281

Configuring Interface Settings for STA 282

Displaying Interface Settings for STA 286

Configuring Multiple Spanning Trees 289

Configuring Interface Settings for MSTP 293

9 CONGESTION CONTROL 295

Rate Limiting 295

Storm Control 296

Automatic Traffic Control 298

Setting the ATC Timers 300

Configuring ATC Thresholds and Responses 301

10 CLASS OF SERVICE 305

Layer 2 Queue Settings 305

Setting the Default Priority for Interfaces 305

Selecting the Queue Mode 306

Mapping CoS Values to Egress Queues 309

Layer 3/4 Priority Settings 312

Setting Priority Processing to IP Precedence/DSCP or CoS 312

Mapping Ingress DSCP Values to Internal DSCP Values 314

Mapping CoS Priorities to Internal DSCP Values 316

Mapping Internal DSCP Values to Egress CoS Values 318

Mapping IP Precedence Values to Internal DSCP Values 320

Mapping IP Port Priority to Internal DSCP Values 323

11 QUALITY OF SERVICE 325

Overview 325

Configuring a Class Map 326

Creating QoS Policies 329

Attaching a Policy Map to a Port 339

12 VOIP TRAFFIC CONFIGURATION 341

Overview 341

Configuring VoIP Traffic 342

Configuring Telephony OUI 343

Configuring VoIP Traffic Ports 345

13 SECURITY MEASURES 347

AAA Authorization and Accounting 348

Configuring Local/Remote Logon Authentication **349**

Configuring Remote Logon Authentication Servers 350

Configuring AAA Accounting 355

Configuring AAA Authorization 360

Configuring User Accounts 363

Web Authentication 365

Configuring Global Settings for Web Authentication 366

Configuring Interface Settings for Web Authentication 367

Network Access (MAC Address Authentication) 368

Configuring Global Settings for Network Access 371

Configuring Network Access for Ports 372

Configuring Port Link Detection 374

Configuring a MAC Address Filter 375

Displaying Secure MAC Address Information 377

Configuring HTTPS 378

Configuring Global Settings for HTTPS 378

Replacing the Default Secure-site Certificate 380

Configuring the Secure Shell 381

Configuring the SSH Server 384

Generating the Host Key Pair 385

Importing User Public Keys 387

Access Control Lists 389

Setting a Time Range 391

Showing TCAM Utilization 394

Setting the ACL Name and Type 395

Configuring a Standard IPv4 ACL 397

Configuring an Extended IPv4 ACL 398

Configuring a Standard IPv6 ACL 400
Configuring an Extended IPv6 ACL 402
Configuring a MAC ACL 404
Configuring an ARP ACL 406
Binding a Port to an Access Control List 408
Showing ACL Hardware Counters 409
ARP Inspection 410
Configuring Global Settings for ARP Inspection 411
Configuring VLAN Settings for ARP Inspection 413
Configuring Interface Settings for ARP Inspection 415
Displaying ARP Inspection Statistics 416
Displaying the ARP Inspection Log 417
Filtering IP Addresses for Management Access 418
Configuring Port Security 420
Configuring 802.1X Port Authentication 423
Configuring 802.1X Global Settings 424
Configuring Port Authenticator Settings for 802.1X 425
Displaying 802.1X Statistics 429
DoS Protection 431
IPv4 Source Guard 432
Configuring Ports for IP Source Guard 433
Configuring Static Bindings for IP Source Guard 435
Displaying Information for Dynamic IPv4 Source Guard Bindings 437
IPv6 Source Guard 438
Configuring Ports for IPv6 Source Guard 438
Configuring Static Bindings for IPv6 Source Guard 440
Displaying Information for Dynamic IPv6 Source Guard Bindings 443
DHCP Snooping 444
DHCP Snooping Configuration 446
DHCP Snooping VLAN Configuration 448
Configuring Ports for DHCP Snooping 449
Displaying DHCP Snooping Binding Information 450
14 BASIC ADMINISTRATION PROTOCOLS 453
Configuring Event Logging 454
System Log Configuration 454
Remote Log Configuration 456

Sending Simple Mail Transfer Protocol Alerts 457

Link Layer Discovery Protocol 458

Setting LLDP Timing Attributes 459

Configuring LLDP Interface Attributes 461

Configuring LLDP Interface Civic-Address 464

Displaying LLDP Local Device Information 466

Displaying LLDP Remote Device Information 470

Displaying Device Statistics 478

Simple Network Management Protocol 480

Configuring Global Settings for SNMP 482

Setting the Local Engine ID 483

Specifying a Remote Engine ID 484

Setting SNMPv3 Views 486

Configuring SNMPv3 Groups 489

Setting Community Access Strings 494

Configuring Local SNMPv3 Users 495

Configuring Remote SNMPv3 Users 497

Specifying Trap Managers 500

Creating SNMP Notification Logs 504

Showing SNMP Statistics 506

Remote Monitoring 508

Configuring RMON Alarms 509

Configuring RMON Events 511

Configuring RMON History Samples 513

Configuring RMON Statistical Samples 516

Switch Clustering 518

Configuring General Settings for Clusters 519

Cluster Member Configuration 520

Managing Cluster Members 522

Ethernet Ring Protection Switching 523

ERPS Global Configuration 527

ERPS Ring Configuration 528

ERPS Forced and Manual Mode Operations 544

Connectivity Fault Management 548

Configuring Global Settings for CFM 551

Configuring Interfaces for CFM 555

Configuring CFM Maintenance Domains 555
Configuring CFM Maintenance Associations 560
Configuring Maintenance End Points 565
Configuring Remote Maintenance End Points 567
Transmitting Link Trace Messages 569
Transmitting Loop Back Messages 571
Transmitting Delay-Measure Requests 572
Displaying Local MEPs 574
Displaying Details for Local MEPs 575
Displaying Local MIPs 577
Displaying Remote MEPs 578
Displaying Details for Remote MEPs 579
Displaying the Link Trace Cache 581
Displaying Fault Notification Settings 583
Displaying Continuity Check Errors 584
OAM Configuration 585
Enabling OAM on Local Ports 585
Displaying Statistics for OAM Messages 588
Displaying the OAM Event Log 589
Displaying the Status of Remote Interfaces 590
Configuring a Remote Loop Back Test 591
Displaying Results of Remote Loop Back Testing 593
PTP Configuration 594
Configuring Global Settings for PTP 595
Configuring Interface Settings for PTP 598
Showing PTP Information 602
Showing PTP Foreign Master 607
15 MULTICAST FILTERING 609
Overview 609
IGMP Protocol 611
Layer 2 IGMP (Snooping and Query for IPv4) 611
Configuring IGMP Snooping and Query Parameters 613
Specifying Static Interfaces for an IPv4 Multicast Router 617
Assigning Interfaces to IPv4 Multicast Services 619
Setting IGMP Snooping Status per Interface 621
Filtering IGMP Query Packets and Multicast Data 627

Displaying Multicast Groups Discovered by IGMP Snooping 628

Displaying IGMP Snooping Statistics 629

Filtering and Throttling IGMP Groups 633

Enabling IGMP Filtering and Throttling 633

Configuring IGMP Filter Profiles 634

Configuring IGMP Filtering and Throttling for Interfaces 636

MLD Snooping (Snooping and Query for IPv6) 638

Configuring MLD Snooping and Query Parameters 638

Setting Immediate Leave Status for MLD Snooping per Interface 640

Specifying Static Interfaces for an IPv6 Multicast Router 641

Assigning Interfaces to IPv6 Multicast Services 643

Showing MLD Snooping Groups and Source List 645

Layer 3 IGMP (Query used with Multicast Routing) 646

Configuring IGMP Proxy Routing 647

Configuring IGMP Interface Parameters 650

Configuring Static IGMP Group Membership 652

Displaying Multicast Group Information 654

Multicast VLAN Registration for IPv4 657

Configuring MVR Global Settings 658

Configuring MVR Domain Settings 660

Configuring MVR Group Address Profiles 662

Configuring MVR Interface Status 665

Assigning Static MVR Multicast Groups to Interfaces 667

Displaying MVR Receiver Groups 669

Displaying MVR Statistics 670

Multicast VLAN Registration for IPv6 674

Configuring MVR6 Global Settings 675

Configuring MVR6 Domain Settings 677

Configuring MVR6 Group Address Profiles 678

Configuring MVR6 Interface Status 681

Assigning Static MVR6 Multicast Groups to Interfaces 684

Displaying MVR6 Receiver Groups 685

Displaying MVR6 Statistics 686

16 IP CONFIGURATION 691

Setting the Switch’s IP Address (IP Version 4) 691

Setting the Switch’s IP Address (IP Version 6) 695

Configuring the IPv6 Default Gateway 696

Configuring IPv6 Interface Settings 697

Configuring an IPv6 Address 700

Showing IPv6 Addresses 703

Showing the IPv6 Neighbor Cache 705

Showing IPv6 Statistics 706

Showing the MTU for Responding Destinations 712

17 IP SERVICES 713

Domain Name Service 713

Configuring General DNS Service Parameters 713

Configuring a List of Domain Names 714

Configuring a List of Name Servers 716

Configuring Static DNS Host to Address Entries 717

Displaying the DNS Cache 718

Dynamic Host Configuration Protocol 719

Specifying a DHCP Client Identifier 720

Configuring DHCP Relay Service 721

Configuring the DHCP Server 723

Forwarding UDP Service Requests 730

Enabling the UDP Helper 731

Specifying UDP Destination Ports 731

Specifying The Target Server or Subnet 733

Configuring the PPPoE Intermediate Agent 735

Configuring PPPoE IA Global Settings 735

Configuring PPPoE IA Interface Settings 736

Showing PPPoE IA Statistics 738

18 GENERAL IP ROUTING 741

Overview 741

Initial Configuration 741

IP Routing and Switching 742

Routing Path Management 743

Routing Protocols 744

Configuring IP Routing Interfaces 744

Configuring Local and Remote Interfaces 744

Using the Ping Function 745

Using the Trace Route Function 746

Address Resolution Protocol 748

Basic ARP Configuration 748

Configuring Static ARP Addresses 750

Displaying Dynamic or Local ARP Entries 752

Displaying ARP Statistics 753

Configuring Static Routes 753

Displaying the Routing Table 755

Equal-cost Multipath Routing 757

19 CONFIGURING ROUTER REDUNDANCY 759

Configuring VRRP Groups 760

Displaying VRRP Global Statistics 766

Displaying VRRP Group Statistics 767

20 UNICAST ROUTING 769

Overview 769

Configuring the Routing Information Protocol 770

Configuring General Protocol Settings 771

Clearing Entries from the Routing Table 774

Specifying Network Interfaces 775

Specifying Passive Interfaces 777

Specifying Static Neighbors 778

Configuring Route Redistribution 779

Specifying an Administrative Distance 781

Configuring Network Interfaces for RIP 782

Displaying RIP Interface Settings 786

Displaying Peer Router Information 787

Resetting RIP Statistics 788

Configuring the Open Shortest Path First Protocol (Version 2) 788

Defining Network Areas Based on Addresses 790

Configuring General Protocol Settings 793

Displaying Administrative Settings and Statistics 796

Adding an NSSA or Stub 798

Configuring NSSA Settings 799

Configuring Stub Settings 802

Displaying Information on NSSA and Stub Areas 804

Configuring Area Ranges (Route Summarization for ABRs) 805

Redistributing External Routes 807
Configuring Summary Addresses (for External AS Routes) 809
Configuring OSPF Interfaces 811
Configuring Virtual Links 817
Displaying Link State Database Information 820
Displaying Information on Neighboring Routers 823
21 MULTICAST ROUTING 825
Overview 825
Configuring Global Settings for Multicast Routing 828
Enabling Multicast Routing Globally 828
Displaying the Multicast Routing Table 829
Configuring PIM for IPv4 833
Enabling PIM Globally 833
Configuring PIM Interface Settings 834
Displaying PIM Neighbor Information 839
Configuring Global PIM-SM Settings 840
Configuring a PIM BSR Candidate 842
Configuring a PIM Static Rendezvous Point 843
Configuring a PIM RP Candidate 845
Displaying the PIM BSR Router 847
Displaying PIM RP Mapping 848
Configuring PIMv6 for IPv6 849
Enabling PIMv6 Globally 849
Configuring PIMv6 Interface Settings 850
Displaying PIM6 Neighbor Information 856
Configuring Global PIM6-SM Settings 856
Configuring a PIM6 BSR Candidate 858
Configuring a PIM6 Static Rendezvous Point 859
Configuring a PIM6 RP Candidate 861
Displaying the PIM6 BSR Router 863
Displaying RP Mapping 865

SECTION III COMMAND LINE INTERFACE 867

22 USING THE COMMAND LINE INTERFACE 869

Accessing the CLI 869

Console Connection 869

Telnet Connection 870

Entering Commands 871

Keywords and Arguments 871

Minimum Abbreviation 871

Command Completion 871

Getting Help on Commands 872

Partial Keyword Lookup 874

Negating the Effect of Commands 874

Using Command History 874

Understanding Command Modes 874

Exec Commands 875

Configuration Commands 876

Command Line Processing 878

CLI Command Groups 879

23 GENERAL COMMANDS 883

prompt 883

reload (Global Configuration) 884

enable 885

quit 886

show history 886

configure 887

disable 888

reload (Privileged Exec) 888

show reload 889

end 889

exit 889

24 SYSTEM MANAGEMENT COMMANDS 891

Device Designation 891

hostname 892

Banner Information 892

banner configure 893

banner configure company 894

banner configure dc-power-info 895

banner configure department 895

banner configure equipment-info 896

banner configure equipment-location 897

banner configure ip-lan 897

banner configure lp-number 898

banner configure manager-info 899

banner configure mux 899

banner configure note 900

show banner 901

System Status 901

show access-list tcam-utilization 902

show alarm-status 902

show memory 903

show process cpu 904

show running-config 904

show startup-config 906

show system 906

show tech-support 907

show users 908

show version 909

show watchdog 909

watchdog software 909

Fan Control 910

fan-speed force-full 910

Frame Size 910

jumbo frame 911

File Management 912

General Commands 913

boot system 913

copy 914

delete 917

dir 918

umount usbdisk 919

whichboot 919

Automatic Code Upgrade Commands 920
upgrade opcode auto 920
upgrade opcode path 921
upgrade opcode reload 922
show upgrade 923
Line 923
line 924
databits 925
exec-timeout 925
login 926
parity 927
password 928
password-thresh 929
silent-time 929
speed 930
stopbits 931
timeout login response 931
disconnect 932
show line 932
Event Logging 933
logging facility 934
logging history 934
logging host 935
logging on 936
logging trap 936
clear log 937
show log 938
show logging 938
SMTP Alerts 940
logging sendmail 940
logging sendmail host 941
logging sendmail level 941
logging sendmail destination-email 942
logging sendmail source-email 943
show logging sendmail 943

Time 944
SNTP Commands 945
sntp client 945
sntp poll 946
sntp server 946
show sntp 947
NTP Commands 947
ntp authenticate 947
ntp authentication-key 948
ntp client 949
ntp server 950
show ntp 951
Manual Configuration Commands 951
clock summer-time (date) 951
clock summer-time (predefined) 953
clock summer-time (recurring) 954
clock timezone 955
calendar set 956
show calendar 957
Time Range 957
time-range 957
absolute 958
periodic 959
show time-range 960
Precision Time Protocol 960
ptp adjust 961
ptp domain-number 962
ptp e-latency 962
ptp in-latency 963
ptp mode 963
ptp priority1 965
ptp priority2 966
ptp announce-receipt-timeout 966
ptp delay-mechanism 967
ptp log-announce-interval 968
ptp log-min-delay-request-interval 969

ptp log-min-pdelay-request-interval 969

ptp log-sync-interval 970

ptp port-enable 971

ptp transport 971

ptp port-release 973

show ptp configuration 974

show ptp foreign-master 974

show ptp information 975

Synchronous Ethernet 979

synce 980

synce ethernet 981

synce ethernet clock-source 982

synce auto-clock-source-selecting 983

synce force-clock-source-selecting 984

synce ssm ethernet 985

synce clk-src-ssm 986

show synce 987

Switch Clustering 989

cluster 990

cluster commander 990

cluster ip-pool 991

cluster member 992

rcommand 992

show cluster 993

show cluster members 993

show cluster candidates 994

25 SNMP COMMANDS 995

General SNMP Commands 997

snmp-server 997

snmp-server community 997

snmp-server contact 998

snmp-server location 998

show snmp 999

SNMP Target Host Commands 1000

snmp-server enable traps 1000

snmp-server host 1001

snmp-server enable port-traps mac-notification 1003

show snmp-server enable port-traps 1004

SNMPv3 Commands 1004

snmp-server engine-id 1004

snmp-server group 1006

snmp-server user 1007

snmp-server view 1008

show snmp engine-id 1009

show snmp group 1010

show snmp user 1011

show snmp view 1012

Notification Log Commands 1012

nlm 1012

snmp-server notify-filter 1013

show nlm oper-status 1014

show snmp notify-filter 1015

Additional Trap Commands 1015

memory 1015

process cpu 1016

26 REMOTE MONITORING COMMANDS 1017

rmon alarm 1018

rmon event 1019

rmon collection history 1020

rmon collection rmon1 1021

show rmon alarms 1022

show rmon events 1022

show rmon history 1022

show rmon statistics 1023

27 FLOW SAMPLING COMMANDS 1025

sflow owner 1025

sflow sampling instance 1027

sflow polling instance 1028

show sflow 1029

28 AUTHENTICATION COMMANDS 1031

User Accounts 1032

enable password 1032

username 1033
Authentication Sequence 1034
authentication enable 1034
authentication login 1035
RADIUS Client 1036
radius-server acct-port 1036
radius-server auth-port 1037
radius-server host 1037
radius-server key 1038
radius-server retransmit 1039
radius-server timeout 1039
show radius-server 1040
TACACS+ Client 1040
tacacs-server host 1041
tacacs-server key 1041
tacacs-server port 1042
tacacs-server retransmit 1042
tacacs-server timeout 1043
show tacacs-server 1043
AAA 1044
aaa accounting dot1x 1044
aaa accounting exec 1045
aaa accounting update 1046
aaa authorization exec 1047
aaa group server 1048
server 1048
accounting dot1x 1049
accounting exec 1049
authorization exec 1050
show accounting 1050
Web Server 1051
ip http port 1052
ip http server 1052
ip http secure-port 1053
ip http secure-server 1053

Telnet Server 1055
ip telnet max-sessions 1055
ip telnet port 1056
ip telnet server 1056
show ip telnet 1057
Secure Shell 1057
ip ssh authentication-retries 1060
ip ssh server 1060
ip ssh server-key size 1061
ip ssh timeout 1062
delete public-key 1062
ip ssh crypto host-key generate 1063
ip ssh crypto zeroize 1064
ip ssh save host-key 1064
show ip ssh 1065
show public-key 1065
show ssh 1066
802.1X Port Authentication 1067
General Commands 1068
dot1x default 1068
dot1x eapol-pass-through 1068
dot1x system-auth-control 1069
Authenticator Commands 1069
dot1x intrusion-action 1069
dot1x max-reauth-req 1070
dot1x max-req 1070
dot1x operation-mode 1071
dot1x port-control 1072
dot1x re-authentication 1072
dot1x timeout quiet-period 1073
dot1x timeout re-authperiod 1073
dot1x timeout supp-timeout 1074
dot1x timeout tx-period 1074
dot1x re-authenticate 1075
Display Information Commands 1076
show dot1x 1076

Management IP Filter 1078

management 1079

show management 1080

PPPoE Intermediate Agent 1081

pppoe intermediate-agent 1081

pppoe intermediate-agent format-type 1082

pppoe intermediate-agent port-enable 1083

pppoe intermediate-agent port-format-type 1083

pppoe intermediate-agent trust 1084

pppoe intermediate-agent vendor-tag strip 1085

clear pppoe intermediate-agent statistics 1085

show pppoe intermediate-agent info 1086

show pppoe intermediate-agent statistics 1087

29 GENERAL SECURITY MEASURES 1089

Port Security 1090

mac-learning 1090

port security 1091

port security mac-address-as-permanent 1093

show port security 1093

Network Access (MAC Address Authentication) 1095

network-access aging 1096

network-access mac-filter 1097

mac-authentication reauth-time 1098

network-access dynamic-qos 1098

network-access dynamic-vlan 1100

network-access guest-vlan 1100

network-access link-detection 1101

network-access link-detection link-down 1102

network-access link-detection link-up 1102

network-access link-detection link-up-down 1103

network-access max-mac-count 1103

network-access mode mac-authentication 1104

network-access port-mac-filter 1105

mac-authentication intrusion-action 1106

mac-authentication max-mac-count 1106

clear network-access 1107

show network-access 1107
show network-access mac-address-table 1108
show network-access mac-filter 1109
Web Authentication 1109
web-auth login-attempts 1110
web-auth quiet-period 1111
web-auth session-timeout 1111
web-auth system-auth-control 1112
web-auth 1112
web-auth re-authenticate (Port) 1113
web-auth re-authenticate (IP) 1113
show web-auth 1114
show web-auth interface 1114
show web-auth summary 1115
DHCPv4 Snooping 1115
ip dhcp snooping 1116
ip dhcp snooping information option 1118
ip dhcp snooping information policy 1119
ip dhcp snooping verify mac-address 1120
ip dhcp snooping vlan 1121
ip dhcp snooping information option circuit-id 1122
ip dhcp snooping trust 1123
clear ip dhcp snooping binding 1124
clear ip dhcp snooping database flash 1124
ip dhcp snooping database flash 1125
show ip dhcp snooping 1125
show ip dhcp snooping binding 1126
DHCPv6 Snooping 1126
ipv6 dhcp snooping 1126
ipv6 dhcp snooping vlan 1129
ipv6 dhcp snooping max-binding 1130
ipv6 dhcp snooping trust 1130
clear ipv6 dhcp snooping binding 1131
clear ipv6 dhcp snooping statistics 1132
show ipv6 dhcp snooping 1132
show ipv6 dhcp snooping binding 1132

show ipv6 dhcp snooping statistics 1133

IPv4 Source Guard 1133

ip source-guard binding 1134

ip source-guard 1135

ip source-guard max-binding 1137

ip source-guard mode 1138

clear ip source-guard binding blocked 1138

show ip source-guard 1139

show ip source-guard binding 1139

IPv6 Source Guard 1140

ipv6 source-guard binding 1140

ipv6 source-guard 1142

ipv6 source-guard max-binding 1143

show ipv6 source-guard 1144

show ipv6 source-guard binding 1145

ARP Inspection 1145

ip arp inspection 1146

ip arp inspection filter 1147

ip arp inspection log-buffer logs 1148

ip arp inspection validate 1149

ip arp inspection vlan 1150

ip arp inspection limit 1151

ip arp inspection trust 1151

show ip arp inspection configuration 1152

show ip arp inspection interface 1152

show ip arp inspection log 1153

show ip arp inspection statistics 1153

show ip arp inspection vlan 1153

Denial of Service Protection 1154

dos-protection land 1154

dos-protection tcp-null-scan 1155

dos-protection tcp-syn-fin-scan 1155

dos-protection tcp-xmas-scan 1156

show dos-protection 1156

Configuring Port-based Traffic Segmentation 1157

traffic-segmentation 1157

traffic-segmentation session 1158
traffic-segmentation uplink/downlink 1159
traffic-segmentation uplink-to-uplink 1160
show traffic-segmentation 1161
30 ACCESS CONTROL LISTS 1163
IPv4 ACLs 1163
access-list ip 1164
permit, deny (Standard IP ACL) 1165
permit, deny (Extended IPv4 ACL) 1166
ip access-group 1168
show ip access-group 1169
show ip access-list 1169
IPv6 ACLs 1170
access-list ipv6 1170
permit, deny (Standard IPv6 ACL) 1171
permit, deny (Extended IPv6 ACL) 1172
ipv6 access-group 1174
show ipv6 access-group 1175
show ipv6 access-list 1175
MAC ACLs 1176
access-list mac 1176
permit, deny (MAC ACL) 1177
mac access-group 1179
show mac access-group 1180
show mac access-list 1180
ARP ACLs 1181
access-list arp 1181
permit, deny (ARP ACL) 1182
show access-list arp 1183
ACL Information 1184
clear access-list hardware counters 1184
show access-group 1184
show access-list 1185
31 INTERFACE COMMANDS 1187
Interface Configuration 1188
interface 1188

alias 1189
capabilities 1189
description 1190
discard 1191
flowcontrol 1191
history 1192
media-type 1193
negotiation 1194
shutdown 1194
switchport mtu 1195
clear counters 1196
show discard 1197
show interfaces brief 1197
show interfaces counters 1198
show interfaces history 1199
show interfaces status 1202
show interfaces switchport 1203
Transceiver Threshold Configuration 1205
transceiver-threshold-auto 1205
transceiver-threshold-monitor 1206
transceiver-threshold current 1206
transceiver-threshold rx-power 1207
transceiver-threshold temperature 1208
transceiver-threshold tx-power 1209
transceiver-threshold voltage 1210
show interfaces transceiver 1211
show interfaces transceiver-threshold 1212
32 LINK AGGREGATION COMMANDS 1215
Manual Configuration Commands 1216
port channel load-balance 1216
channel-group 1218
Dynamic Configuration Commands 1218
lacp 1218
lacp admin-key (Ethernet Interface) 1220
lacp port-priority 1221
lacp system-priority 1222

lacp admin-key (Port Channel) 1222

lacp timeout 1223

Trunk Status Display Commands 1224

show lacp 1224

show port-channel load-balance 1228

33 PORT MIRRORING COMMANDS 1229

Local Port Mirroring Commands 1229

port monitor 1229

show port monitor 1230

RSPAN Mirroring Commands 1231

rspan source 1233

rspan destination 1234

rspan remote vlan 1235

no rspan session 1236

show rspan 1236

34 CONGESTION CONTROL COMMANDS 1239

Rate Limit Commands 1239

rate-limit 1240

Storm Control Commands 1241

switchport packet-rate 1241

switchport block 1242

Automatic Traffic Control Commands 1243

Threshold Commands 1246

auto-traffic-control apply-timer 1246

auto-traffic-control release-timer 1246

auto-traffic-control 1247

auto-traffic-control action 1248

auto-traffic-control alarm-clear-threshold 1249

auto-traffic-control alarm-fire-threshold 1250

auto-traffic-control auto-control-release 1251

auto-traffic-control control-release 1251

SNMP Trap Commands 1252

snmp-server enable port-traps atc broadcast-alarm-clear 1252

snmp-server enable port-traps atc broadcast-alarm-fire 1252

snmp-server enable port-traps atc broadcast-control-apply 1253

snmp-server enable port-traps atc broadcast-control-release 1253 snmp-server enable port-traps atc multicast-alarm-clear 1254

snmp-server enable port-traps atc multicast-alarm-fire 1254

snmp-server enable port-traps atc multicast-control-apply 1255

snmp-server enable port-traps atc multicast-control-release 1255

ATC Display Commands 1256

show auto-traffic-control 1256

show auto-traffic-control interface 1256

35 LOOPBACK DETECTION COMMANDS 1259

loopback-detection 1260

loopback-detection action 1260

loopback-detection recover-time 1261

loopback-detection transmit-interval 1262

loopback detection trap 1262

loopback-detection release 1263

show loopback-detection 1263

36 UNIDIRECTIONAL LINK DETECTION COMMANDS 1265

udld message-interval 1265

udld aggressive 1266

udld port 1267

show udld 1268

37 ADDRESS TABLE COMMANDS 1271

mac-address-table aging-time 1271

mac-address-table static 1272

clear mac-address-table dynamic 1273

show mac-address-table 1273

show mac-address-table aging-time 1274

show mac-address-table count 1275

38 SPANNING TREE COMMANDS 1277

spanning-tree 1278

spanning-tree forward-time 1279

spanning-tree hello-time 1279

spanning-tree max-age 1280

spanning-tree mode 1281

spanning-tree pathcost method 1282

spanning-tree priority 1283

spanning-tree mst configuration 1283

spanning-tree system-bpdu-flooding 1284
spanning-tree transmission-limit 1284
max-hops 1285
mst priority 1286
mst vlan 1286
name 1287
revision 1288
spanning-tree bpdu-filter 1288
spanning-tree bpdu-guard 1289
spanning-tree cost 1290
spanning-tree edge-port 1291
spanning-tree link-type 1292
spanning-tree loopback-detection 1293
spanning-tree loopback-detection action 1293
spanning-tree loopback-detection release-mode 1294
spanning-tree loopback-detection trap 1295
spanning-tree mst cost 1295
spanning-tree mst port-priority 1296
spanning-tree port-bpdu-flooding 1297
spanning-tree port-priority 1298
spanning-tree root-guard 1298
spanning-tree spanning-disabled 1299
spanning-tree tc-prop-stop 1300
spanning-tree loopback-detection release 1300
spanning-tree protocol-migration 1301
show spanning-tree 1302
show spanning-tree mst configuration 1304
39 ERPS COMMANDS 1305
erps 1307
erps domain 1307
control-vlan 1308
enable 1309
guard-timer 1310
holdoff-timer 1310
major-domain 1311
meg-level 1312

mep-monitor 1312
node-id 1313
non-erps-dev-protect 1314
non-revertive 1315
propagate-tc 1319
raps-def-mac 1320
raps-without-vc 1320
ring-port 1322
rpl neighbor 1323
rpl owner 1324
version 1325
wtr-timer 1326
clear erps statistics 1326
erps clear 1327
erps forced-switch 1327
erps manual-switch 1329
show erps 1331
40 VLAN COMMANDS 1337
GVRP and Bridge Extension Commands 1338
bridge-ext gvrp 1338
garp timer 1339
switchport forbidden vlan 1340
switchport gvrp 1340
show bridge-ext 1341
show garp timer 1341
show gvrp configuration 1342
Editing VLAN Groups 1343
vlan database 1343
vlan 1344
Configuring VLAN Interfaces 1345
interface vlan 1345
switchport acceptable-frame-types 1346
switchport allowed vlan 1347
switchport ingress-filtering 1348
switchport mode 1349
switchport native vlan 1350

vlan-trunking 1350

Displaying VLAN Information 1352

show vlan 1352

Configuring IEEE 802.1Q Tunneling 1353

dot1q-tunnel system-tunnel-control 1354

switchport dot1q-tunnel mode 1355

switchport dot1q-tunnel service match cvid 1356

switchport dot1q-tunnel tpid 1358

show dot1q-tunnel 1359

Configuring L2CP Tunneling 1360

l2protocol-tunnel tunnel-dmac 1360

switchport l2protocol-tunnel 1363

show l2protocol-tunnel 1364

Configuring VLAN Translation 1364

switchport vlan-translation 1364

show vlan-translation 1366

Configuring Private VLANs 1366

private-vlan 1367

private vlan association 1368

switchport mode private-vlan 1369

switchport private-vlan host-association 1370

switchport private-vlan mapping 1370

show vlan private-vlan 1371

Configuring Protocol-based VLANs 1371

protocol-vlan protocol-group (Configuring Groups) 1372

protocol-vlan protocol-group (Configuring Interfaces) 1373

show protocol-vlan protocol-group 1374

show interfaces protocol-vlan protocol-group 1374

Configuring IP Subnet VLANs 1375

subnet-vlan 1376

show subnet-vlan 1377

Configuring MAC Based VLANs 1377

mac-vlan 1378

show mac-vlan 1378

Configuring Voice VLANs 1379

voice vlan 1379

voice vlan aging 1380

voice vlan mac-address 1381

switchport voice vlan 1382

switchport voice vlan priority 1383

switchport voice vlan rule 1383

switchport voice vlan security 1384

show voice vlan 1385

41 CLASS OF SERVICE COMMANDS 1387

Priority Commands (Layer 2) 1387

queue mode 1388

queue weight 1389

switchport priority default 1390

show queue mode 1391

show queue weight 1391

Priority Commands (Layer 3 and 4) 1392

qos map cos-dscp 1393

qos map default-drop-precedence 1394

qos map dscp-cos 1395

qos map dscp-mutation 1396

qos map ip-port-dscp 1398

qos map ip-prec-dscp 1398

qos map phb-queue 1399

qos map trust-mode 1400

show qos map cos-dscp 1401

show qos map dscp-cos 1402

show qos map dscp-mutation 1402

show qos map ip-port-dscp 1403

show qos map ip-prec-dscp 1404

show qos map phb-queue 1404

show qos map trust-mode 1405

42 QUALITY OF SERVICE COMMANDS 1407

class-map 1408

description 1409

match 1410

rename 1411

policy-map 1411

class 1412

police flow 1413

police srtcm-color 1415

police trtcm-color 1417

set cos 1419

set phb 1420

service-policy 1421

show class-map 1422

show policy-map 1422

show policy-map interface 1423

43 MULTICAST FILTERING COMMANDS 1425

IGMP Snooping 1426

ip igmp snooping 1427

ip igmp snooping priority 1428

ip igmp snooping proxy-reporting 1428

ip igmp snooping querier 1429

ip igmp snooping router-alert-option-check 1429

ip igmp snooping router-port-expire-time 1430

ip igmp snooping tcn-flood 1431

ip igmp snooping tcn-query-solicit 1432

ip igmp snooping unregistered-data-flood 1432

ip igmp snooping unsolicited-report-interval 1433

ip igmp snooping version 1434

ip igmp snooping version-exclusive 1434

ip igmp snooping vlan general-query-suppression 1435

ip igmp snooping vlan immediate-leave 1436

ip igmp snooping vlan last-memb-query-count 1437

ip igmp snooping vlan last-memb-query-intvl 1437

ip igmp snooping vlan mrd 1438

ip igmp snooping vlan proxy-address 1439

ip igmp snooping vlan query-interval 1440

ip igmp snooping vlan query-resp-intvl 1441

ip igmp snooping vlan static 1442

show ip igmp snooping 1442

show ip igmp snooping group 1443

show ip igmp snooping statistics 1444

Static Multicast Routing 1446
ip igmp snooping vlan mrouter 1447
show ip igmp snooping mrouter 1447
IGMP Filtering and Throttling 1448
ip igmp filter (Global Configuration) 1449
ip igmp profile 1450
permit, deny 1450
range 1451
ip igmp authentication 1451
ip igmp filter (Interface Configuration) 1453
ip igmp max-groups 1454
ip igmp max-groups action 1454
ip igmp query-drop 1455
ip multicast-data-drop 1455
show ip igmp authentication 1456
show ip igmp filter 1457
show ip igmp profile 1457
show ip igmp query-drop 1458
show ip igmp throttle interface 1458
show ip multicast-data-drop 1459
MLD Snooping 1460
ipv6 mld snooping 1461
ipv6 mld snooping querier 1461
ipv6 mld snooping query-interval 1462
ipv6 mld snooping query-max-response-time 1462
ipv6 mld snooping robustness 1463
ipv6 mld snooping router-port-expire-time 1463
ipv6 mld snooping unknown-multicast mode 1464
ipv6 mld snooping version 1465
ipv6 mld snooping vlan mrouter 1465
ipv6 mld snooping vlan static 1466
ipv6 mld snooping vlan immediate-leave 1466
show ipv6 mld snooping 1467
show ipv6 mld snooping group 1468
show ipv6 mld snooping group source-list 1468
show ipv6 mld snooping mrouter 1469

MLD Filtering and Throttling 1469
ipv6 mld filter (Global Configuration) 1470
ipv6 mld profile 1471
permit, deny 1471
range 1472
ipv6 mld filter (Interface Configuration) 1472
ipv6 mld max-groups 1473
ipv6 mld max-groups action 1474
ipv6 mld query-drop 1474
ipv6 multicast-data-drop 1475
show ipv6 mld filter 1475
show ipv6 mld profile 1476
show ipv6 mld query-drop 1476
show ipv6 mld throttle interface 1477
MVR for IPv4 1478
mvr 1479
mvr associated-profile 1479
mvr domain 1480
mvr profile 1481
mvr proxy-query-interval 1481
mvr priority 1482
mvr proxy-switching 1483
mvr robustness-value 1484
mvr source-port-mode dynamic 1484
mvr upstream-source-ip 1485
mvr vlan 1486
mvr immediate-leave 1486
mvr type 1487
mvr vlan group 1488
show mvr 1489
show mvr associated-profile 1490
show mvr interface 1491
show mvr members 1492
show mvr profile 1493
show mvr statistics 1494

MVR for IPv6 1496

mvr6 associated-profile 1497

mvr6 domain 1498

mvr6 profile 1498

mvr6 proxy-query-interval 1499

mvr6 proxy-switching 1500

mvr6 robustness-value 1501

mvr6 source-port-mode dynamic 1501

mvr6 upstream-source-ip 1502

mvr6 vlan 1503

mvr6 immediate-leave 1503

mvr6 type 1504

mvr6 vlan group 1505

clear mvr6 groups 1506

clear mvr6 statistics 1507

show mvr6 1507

show mvr6 associated-profile 1508

show mvr6 interface 1509

show mvr6 members 1510

show mvr6 profile 1511

show mvr6 statistics 1511

IGMP (Layer 3) 1513

ip igmp 1514

ip igmp last-member-query-interval 1515

ip igmp max-resp-interval 1515

ip igmp query-interval 1516

ip igmp robustval 1517

ip igmp static-group 1518

ip igmp version 1519

clear ip igmp group 1519

show ip igmp groups 1520

show ip igmp interface 1522

IGMP Proxy Routing 1523

ip igmp proxy 1523

ip igmp proxy unsolicited-report-interval 1524

MLD (Layer 3) 1525

ipv6 mld 1525

ipv6 mld last-member-query-response-interval 1526

ipv6 mld max-resp-interval 1527

ipv6 mld query-interval 1528

ipv6 mld robustval 1528

ipv6 mld static-group 1529

ipv6 mld version 1530

clear ipv6 mld group 1531

show ipv6 mld groups 1531

show ipv6 mld interface 1533

MLD Proxy Routing 1533

ipv6 mld proxy 1534

ipv6 mld proxy unsolicited-report-interval 1535

44 LLDP COMMANDS 1537

lldp 1539

lldp holdtime-multiplier 1539

lldp med-fast-start-count 1540

lldp notification-interval 1540

lldp refresh-interval 1541

lldp reinit-delay 1541

lldp tx-delay 1542

lldp admin-status 1543

lldp basic-tlv management-ip-address 1543

lldp basic-tlv port-description 1544

lldp basic-tlv system-capabilities 1545

lldp basic-tlv system-description 1545

lldp basic-tlv system-name 1546

lldp dot1-tlv proto-ident 1546

lldp dot1-tlv proto-vid 1547

lldp dot1-tlv pvid 1547

lldp dot1-tlv vlan-name 1548

lldp dot3-tlv link-agg 1548

lldp dot3-tlv mac-phy 1549

lldp dot3-tlv max-frame 1549

lldp med-location civic-addr 1550

lldp med-notification 1551
lldp med-tlv inventory 1552
lldp med-tlv location 1553
lldp med-tlv med-cap 1553
lldp med-tlv network-policy 1554
lldp notification 1554
show lldp config 1555
show lldp info local-device 1556
show lldp info remote-device 1557
show lldp info statistics 1560
45 CFM COMMANDS 1561
Defining CFM Structures 1564
ethernet cfm ais level 1564
ethernet cfm ais ma 1565
ethernet cfm ais period 1566
ethernet cfm ais suppress alarm 1566
ethernet cfm domain 1567
ethernet cfm enable 1569
ma index name 1570
ma index name-format 1571
ethernet cfm mep 1571
ethernet cfm port-enable 1572
clear ethernet cfm ais mpid 1573
show ethernet cfm configuration 1574
show ethernet cfm md 1575
show ethernet cfm ma 1576
show ethernet cfm maintenance-points local 1576
show ethernet cfm maintenance-points local detail mep 1577
show ethernet cfm maintenance-points remote detail 1579
Continuity Check Operations 1581
ethernet cfm cc ma interval 1581
ethernet cfm cc enable 1582
snmp-server enable traps ethernet cfm cc 1583
mep archive-hold-time 1584
clear ethernet cfm maintenance-points remote 1584
clear ethernet cfm errors 1585

show ethernet cfm errors 1585

Cross Check Operations 1586

ethernet cfm mep crosscheck start-delay 1586

snmp-server enable traps ethernet cfm crosscheck 1587

mep crosscheck mpid 1588

ethernet cfm mep crosscheck 1589

show ethernet cfm maintenance-points remote crosscheck 1590

Link Trace Operations 1590

ethernet cfm linktrace cache 1590

ethernet cfm linktrace cache hold-time 1591

ethernet cfm linktrace cache size 1591

ethernet cfm linktrace 1592

clear ethernet cfm linktrace-cache 1593

show ethernet cfm linktrace-cache 1594

Loopback Operations 1595

ethernet cfm loopback 1595

Fault Generator Operations 1596

mep fault-notify alarm-time 1596

mep fault-notify lowest-priority 1597

mep fault-notify reset-time 1598

show ethernet cfm fault-notify-generator 1599

Delay Measure Operations 1600

ethernet cfm delay-measure two-way 1600

46 OAM COMMANDS 1603

efm oam 1604

efm oam critical-link-event 1604

efm oam link-monitor frame 1605

efm oam link-monitor frame threshold 1605

efm oam link-monitor frame window 1606

efm oam mode **1607**

clear efm oam counters 1607

clear efm oam event-log 1608

efm oam remote-loopback 1608

efm oam remote-loopback test 1609

show efm oam counters interface 1610

show efm oam event-log interface 1611

show efm oam remote-loopback interface 1612

show efm oam status interface 1613

show efm oam status remote interface 1613

47 DOMAIN NAME SERVICE COMMANDS 1615

ip domain-list 1615

ip domain-lookup 1616

ip domain-name 1617

ip host 1618

ip name-server 1619

ipv6 host 1620

clear dns cache 1620

clear host 1621

show dns 1621

show dns cache 1622

show hosts 1622

48 DHCP COMMANDS 1625

DHCP Client 1625

DHCP for IPv4 1625

ip dhcp client class-id 1625

ip dhcp restart client 1627

DHCP for IPv6 1628

ipv6 dhcp client rapid-commit vlan 1628

DHCP Relay 1629

DHCP Relay for IPv4 1629

ip dhcp relay server 1629

ip dhcp restart relay 1630

DHCP Relay for IPv6 1631

ipv6 dhcp relay destination 1631

show ipv6 dhcp relay destination 1632

DHCP Server 1632

ip dhcp excluded-address 1633

ip dhcp pool 1634

service dhcp 1634

bootfile 1635

client-identifier 1635

default-router 1636

dns-server 1637
domain-name 1637
hardware-address 1638
host 1638
lease 1639
netbios-name-server 1640
netbios-node-type 1641
network 1641
next-server 1642
clear ip dhcp binding 1643
show ip dhcp 1644
show ip dhcp binding 1644
show ip dhcp pool 1644
49 IP INTERFACE COMMANDS 1647
IPv4 Interface 1647
Basic IPv4 Configuration 1648
ip address 1648
ip default-gateway 1650
show ip interface 1651
show ip traffic 1652
traceroute 1653
ping 1654
ARP Configuration 1655
arp 1655
arp timeout 1656
ip proxy-arp 1657
clear arp-cache 1658
show arp 1658
UDP Helper Configuration 1659
ip forward-protocol udp 1659
ip helper 1660
ip helper-address 1661
show ip helper 1662
IPv6 Interface 1663
Interface Address Configuration and Utilities 1664
ipv6 default-gateway 1664

ipv6 address 1665

ipv6 address eui-64 1667

ipv6 address link-local 1669

ipv6 enable 1670

ipv6 mtu 1671

show ipv6 interface 1672

show ipv6 mtu 1674

show ipv6 traffic 1675

clear ipv6 traffic 1679

ping6 1679

traceroute6 1681

Neighbor Discovery 1682

ipv6 hop-limit 1682

ipv6 neighbor 1683

ipv6 nd dad attempts 1684

ipv6 nd managed-config-flag 1685

ipv6 nd other-config-flag 1686

ipv6 nd ns-interval 1687

ipv6 nd raguard 1688

ipv6 nd reachable-time 1689

ipv6 nd prefix 1690

ipv6 nd ra interval 1691

ipv6 nd ra lifetime 1692

ipv6 nd ra router-preference 1692

ipv6 nd ra suppress 1693

clear ipv6 neighbors 1694

show ipv6 nd raguard 1694

show ipv6 neighbors 1694

IPv6 to IPv4 Tunnels 1696

interface tunnel 1697

tunnel destination 1698

tunnel mode ipv6ip 1699

tunnel source vlan 1701

tunnel ttl 1702

show ipv6 tunnel 1702

ND Snooping 1704

ipv6 nd snooping 1705

ipv6 nd snooping auto-detect 1706

ipv6 nd snooping auto-detect retransmit count 1707

ipv6 nd snooping auto-detect retransmit interval 1707

ipv6 nd snooping prefix timeout 1708

ipv6 nd snooping max-binding 1709

ipv6 nd snooping trust 1709

clear ipv6 nd snooping binding 1710

clear ipv6 nd snooping prefix 1710

show ipv6 nd snooping 1711

show ipv6 nd snooping binding 1711

show ipv6 nd snooping prefix 1711

50 VRRP COMMANDS 1713

vrrp authentication 1714

vrrp ip 1714

vrrp preempt 1715

vrrp priority 1716

vrrp timers advertise 1717

clear vrrp interface counters 1718

clear vrrp router counters 1718

show vrrp 1718

show vrrp interface 1720

show vrrp interface counters 1721

show vrrp router counters 1722

51 IP ROUTING COMMANDS 1723

Global Routing Configuration 1723

IPv4 Commands 1724

ip route 1724

maximum-paths 1725

show ip host-route 1726

show ip route 1726

show ip route database 1727

show ip route summary 1728

show ip traffic 1728

IPv6 Commands 1730

ipv6 route 1730

show ipv6 route 1731

Routing Information Protocol (RIP) 1733

router rip 1734

default-information originate 1734

default-metric 1735

distance 1736

maximum-prefix 1736

neighbor 1737

network 1738

passive-interface 1738

redistribute 1739

timers basic 1740

version 1741

ip rip authentication mode 1742

ip rip authentication string 1743

ip rip receive version 1744

ip rip receive-packet 1745

ip rip send version 1745

ip rip send-packet 1746

ip rip split-horizon 1747

clear ip rip route 1748

show ip protocols rip 1748

show ip rip 1749

Open Shortest Path First (OSPFv2) 1750

General Configuration 1751

router ospf 1751

compatible rfc1583 1752

default-information originate 1753

router-id 1754

timers spf 1755

clear ip ospf process 1756

Route Metrics and Summaries 1756

area default-cost 1756

area range 1757

auto-cost reference-bandwidth 1758
default-metric 1759
redistribute 1760
summary-address 1761
Area Configuration 1762
area nssa 1762
area stub 1764
area virtual-link 1765
network area 1768
Interface Configuration 1769
ip ospf authentication 1769
ip ospf authentication-key 1770
ip ospf cost 1771
ip ospf dead-interval 1772
ip ospf hello-interval 1772
ip ospf message-digest-key 1773
ip ospf priority 1774
ip ospf retransmit-interval 1775
ip ospf transmit-delay 1776
passive-interface 1777
Display Information 1777
show ip ospf 1777
show ip ospf border-routers 1779
show ip ospf database 1780
show ip ospf interface 1786
show ip ospf neighbor 1787
show ip ospf route 1788
show ip ospf virtual-links 1789
show ip protocols ospf 1790
Open Shortest Path First (OSPFv3) 1790
General Configuration 1792
router ipv6 ospf 1792
abr-type 1793
max-current-dd 1794
router-id 1795
timers spf 1796

Route Metrics and Summaries 1797
area default-cost 1797
area range 1798
default-metric 1799
redistribute 1799
Area Configuration 1801
area stub 1801
area virtual-link 1802
ipv6 router ospf area 1804
ipv6 router ospf tag area 1805
Interface Configuration 1806
ipv6 ospf cost 1806
ipv6 ospf dead-interval 1807
ipv6 ospf hello-interval 1808
ipv6 ospf priority 1808
ipv6 ospf retransmit-interval 1809
ipv6 ospf transmit-delay 1810
passive-interface 1811
Display Information 1812
show ipv6 ospf 1812
show ipv6 ospf database 1813
show ipv6 ospf interface 1814
show ipv6 ospf neighbor 1815
show ipv6 ospf route 1816
show ipv6 ospf virtual-links 1817
Border Gateway Protocol (BGPv4) 1818
BGP Overview 1818
External and Internal BGP 1818
BGP Routing Basics 1820
Internal BGP Scalability 1823
Route Flap Dampening 1827
BGP Command List 1828
General Configuration 1832
router bgp 1832
ip as-path access-list 1833
ip community-list 1834

ip extcommunity-list 1836
ip prefix-list 1838
aggregate-address 1839
bgp client-to-client reflection 1840
bgp cluster-id 1841
bgp confederation identifier 1842
bgp confederation peer 1843
bgp dampening 1844
bgp enforce-first-as 1845
bgp fast-external-failover 1845
bgp log-neighbor-changes 1846
bgp network import-check 1846
bgp router-id 1847
bgp scan-time 1848
network 1848
redistribute 1849
timers bgp 1850
clear ip bgp 1851
clear ip bgp dampening 1852
Route Metrics and Selection 1853
bgp always-compare-med 1853
bgp bestpath as-path ignore 1853
bgp bestpath compare-confed-aspath 1854
bgp bestpath compare-routerid 1854
bgp bestpath med 1855
bgp default local-preference 1855
bgp deterministic-med 1856
distance 1857
distance bgp 1858
Neighbor Configuration 1859
neighbor activate 1859
neighbor advertisement-interval 1859
neighbor allowas-in 1860
neighbor attribute-unchanged 1861
neighbor capability dynamic 1861
neighbor capability orf prefix-list 1862

neighbor default-originate 1863
neighbor description 1864
neighbor distribute-list 1864
neighbor dont-capability-negotiate 1865
neighbor ebgp-multihop 1866
neighbor enforce-multihop 1866
neighbor filter-list 1867
neighbor interface 1868
neighbor maximum-prefix 1868
neighbor next-hop-self 1869
neighbor override-capability 1870
neighbor passive 1870
neighbor peer-group (Creating) 1871
neighbor peer-group (Group Members) 1872
neighbor port 1872
neighbor prefix-list 1873
neighbor remote-as 1874
neighbor remove-private-as 1874
neighbor route-map 1875
neighbor route-reflector-client 1876
neighbor route-server-client 1877
neighbor send-community 1878
neighbor shutdown 1878
neighbor soft-reconfiguration inbound 1879
neighbor strict-capability-match 1880
neighbor timers 1880
neighbor timers connect 1881
neighbor unsuppress-map 1882
neighbor update-source 1883
neighbor weight 1883
Display Information 1884
show ip bgp 1884
show ip bgp attribute-info 1885
show ip bgp cidr-ony 1886
show ip bgp community 1886
show ip bgp community-info 1887

show ip bgp community-list 1888

show ip bgp dampening 1888

show ip bgp filter-list 1890

show ip bgp neighbors 1890

show ip bgp paths 1892

show ip bgp prefix-list 1892

show ip bgp regexp 1893

show ip bgp route-map 1893

show ip bgp scan 1894

show ip bgp summary 1894

show ip community-list 1895

show ip extcommunity-list 1895

show ip prefix-list 1896

show ip prefix-list detail 1896

show ip prefix-list summary 1897

Policy-based Routing for BGP 1897

route-map 1899

call 1900

continue 1901

description 1901

match as-path 1902

match community 1902

match extcommunity 1903

match ip address 1904

match ip next-hop 1904

match ip route-source 1905

match metric 1905

match origin 1906

match pathlimit as 1906

match peer 1907

on-match 1908

set aggregator as 1908

set as-path 1909

set atomic-aggregate 1910

set comm-list delete 1910

set community 1911

set extcommunity 1912

set ip next-hop 1913

set local-preference 1914

set metric 1914

set origin 1915

set originator-id 1916

set pathlimit ttl 1916

set weight 1917

show route-map 1917

52 MULTICAST ROUTING COMMANDS 1919

General Multicast Routing 1919

IPv4 Commands 1919

ip multicast-routing 1919

show ip mroute 1920

IPv6 Commands 1922

ipv6 multicast-routing 1922

show ipv6 mroute 1923

Static Multicast Routing 1925

ip igmp snooping vlan mrouter 1925

show ip igmp snooping mrouter 1926

PIM Multicast Routing 1927

IPv4 PIM Commands 1927

PIM Shared Mode Commands 1928

router pim 1928

ip pim 1929

ip pim hello-holdtime 1930

ip pim hello-interval 1931

ip pim join-prune-holdtime 1931

ip pim lan-prune-delay 1932

ip pim override-interval 1933

ip pim propagation-delay 1934

ip pim trigger-hello-delay 1934

show ip pim interface 1935

show ip pim neighbor 1936

PIM-DM Commands 1936

ip pim graft-retry-interval 1936

ip pim max-graft-retries 1937
ip pim state-refresh origination-interval 1937
PIM-SM Commands 1938
ip pim bsr-candidate 1938
ip pim register-rate-limit 1939
ip pim register-source 1940
ip pim rp-address 1941
ip pim rp-candidate 1942
ip pim spt-threshold 1944
ip pim dr-priority 1945
ip pim join-prune-interval 1946
clear ip pim bsr rp-set 1947
show ip pim bsr-router 1947
show ip pim rp mapping 1948
show ip pim rp-hash 1949
IPv6 PIM Commands 1950
PIM6 Shared Mode Commands 1951
router pim6 1951
ipv6 pim 1951
ipv6 pim hello-holdtime 1953
ipv6 pim hello-interval 1953
ipv6 pim join-prune-holdtime 1954
ipv6 pim lan-prune-delay 1954
ipv6 pim override-interval 1955
ipv6 pim propagation-delay 1956
ipv6 pim trigger-hello-delay 1957
show ipv6 pim interface 1957
show ipv6 pim neighbor 1958
PIM6-DM Commands 1959
ipv6 pim graft-retry-interval 1959
ipv6 pim max-graft-retries 1960
ipv6 pim state-refresh origination-interval 1960
PIM6-SM Commands 1961
ipv6 pim bsr-candidate 1961
ipv6 pim register-rate-limit 1962
ipv6 pim register-source 1963

ipv6 pim rp-address 1964
ipv6 pim rp-candidate 1965
ipv6 pim spt-threshold 1967
ipv6 pim dr-priority 1968
ipv6 pim join-prune-interval 1969
clear ipv6 pim bsr rp-set 1970
show ipv6 pim bsr-router 1970
show ipv6 pim rp mapping 1971
show ipv6 pim rp-hash 1972

SECTION IV APPENDICES 1973

A SOFTWARE SPECIFICATIONS 1975
Software Features 1975
Management Features 1977
Standards 1977
Management Information Bases 1978
B TROUBLESHOOTING 1981
Problems Accessing the Management Interface 1981
Using System Logs 1982
C LICENSE INFORMATION 1983
The GNU General Public License 1983
GLOSSARY 1987
COMMAND LIST 1995
INDEX 2007

Figures

Figure 1: Home Page 124

Figure 2: Front Panel Indicators 125

Figure 3: System Information 150

Figure 4: General Switch Information 152

Figure 5: Configuring Support for Jumbo Frames 153

Figure 6: Displaying Bridge Extension Configuration 154

Figure 7: Copy Firmware 157

Figure 8: Saving the Running Configuration 158

Figure 9: Setting Start-Up Files 159

Figure 10: Displaying System Files 159

Figure 11: Configuring Automatic Code Upgrade 163

Figure 12: Manually Setting the System Clock 165

Figure 13: Setting the Polling Interval for SNTP 166

Figure 14: Configuring NTP 167

Figure 15: Specifying SNTP Time Servers 168

Figure 16: Adding an NTP Time Server 169

Figure 17: Showing the NTP Time Server List 169

Figure 18: Adding an NTP Authentication Key 170

Figure 19: Showing the NTP Authentication Key List 170

Figure 20: Setting the Time Zone 171

Figure 21: Console Port Settings 173

Figure 22: Telnet Connection Settings 175

Figure 23: Displaying CPU Utilization 176

Figure 24: Displaying Memory Utilization 177

Figure 25: Restarting the Switch (Immediately) 179

Figure 26: Restarting the Switch (In) 179

Figure 27: Restarting the Switch (At) 180

Figure 28: Restarting the Switch (Regularly) 180

Figure 29: Configuring Connections by Port List 184

Figure 30: Configuring Connections by Port Range 185

Figure 31: Displaying Port Information 186

Figure 32: Configuring Local Port Mirroring 186
Figure 33: Configuring Local Port Mirroring 187
Figure 34: Displaying Local Port Mirror Sessions 188
Figure 35: Configuring Remote Port Mirroring 188
Figure 36: Configuring Remote Port Mirroring (Source) 191
Figure 37: Configuring Remote Port Mirroring (Intermediate) 192
Figure 38: Configuring Remote Port Mirroring (Destination) 192
Figure 39: Showing Port Statistics (Table) 195
Figure 40: Showing Port Statistics (Chart) 196
Figure 41: Configuring a History Sample 198
Figure 42: Showing Entries for History Sampling 198
Figure 43: Showing Status of Statistical History Sample 199
Figure 44: Showing Current Statistics for a History Sample 199
Figure 45: Showing Ingress Statistics for a History Sample 200
Figure 46: Displaying Transceiver Data 201
Figure 47: Configuring Transceiver Thresholds 203
Figure 48: Configuring Static Trunks 205
Figure 49: Creating Static Trunks 206
Figure 50: Adding Static Trunks Members 206
Figure 51: Configuring Connection Parameters for a Static Trunk 207
Figure 52: Showing Information for Static Trunks 207
Figure 53: Configuring Dynamic Trunks 207
Figure 54: Configuring the LACP Aggregator Admin Key 210
Figure 55: Enabling LACP on a Port 211
Figure 56: Configuring LACP Parameters on a Port 211
Figure 57: Showing Members of a Dynamic Trunk 212
Figure 58: Configuring Connection Settings for Dynamic Trunks 212
Figure 59: Displaying Connection Parameters for Dynamic Trunks 213
Figure 60: Displaying LACP Port Counters 214
Figure 61: Displaying LACP Port Internal Information 215
Figure 62: Displaying LACP Port Remote Information 217
Figure 63: Configuring Load Balancing 219
Figure 64: Enabling Traffic Segmentation 220
Figure 65: Configuring Members for Traffic Segmentation 221
Figure 66: Showing Traffic Segmentation Members 222
Figure 67: Configuring VLAN Trunking 222

Figure 68: Configuring VLAN Trunking 224
Figure 69: VLAN Compliant and VLAN Non-compliant Devices 226
Figure 70: Using GVRP 228
Figure 71: Creating Static VLANs 230
Figure 72: Modifying Settings for Static VLANs 230
Figure 73: Showing Static VLANs 231
Figure 74: Configuring Static Members by VLAN Index 234
Figure 75: Configuring Static VLAN Members by Interface 234
Figure 76: Configuring Static VLAN Members by Interface Range 235
Figure 77: Configuring Global Status of GVRP 237
Figure 78: Configuring GVRP for an Interface 237
Figure 79: Showing Dynamic VLANs Registered on the Switch 238
Figure 80: Showing the Members of a Dynamic VLAN 238
Figure 81: Configuring Private VLANs 240
Figure 82: Showing Private VLANs 240
Figure 83: Associating Private VLANs 241
Figure 84: Showing Associated VLANs 241
Figure 85: Configuring Interfaces for Private VLANs 243
Figure 86: QinQ Operational Concept 244
Figure 87: Enabling QinQ Tunneling 248
Figure 88: Configuring CVLAN to SPVLAN Mapping Entries 249
Figure 89: Showing CVLAN to SPVLAN Mapping Entries 249
Figure 90: Adding an Interface to a QinQ Tunnel 251
Figure 91: Configuring Protocol VLANs 253
Figure 92: Displaying Protocol VLANs 253
Figure 93: Assigning Interfaces to Protocol VLANs 255
Figure 94: Showing the Interface to Protocol Group Mapping 255
Figure 95: Configuring IP Subnet VLANs 257
Figure 96: Showing IP Subnet VLANs 257
Figure 97: Configuring MAC-Based VLANs 259
Figure 98: Showing MAC-Based VLANs 259
Figure 99: Configuring VLAN Translation 260
Figure 100: Configuring VLAN Translation 261
Figure 101: Showing the Entries for VLAN Translation 261
Figure 102: Configuring MAC Address Learning 264
Figure 103: Configuring Static MAC Addresses 266

Figure 104: Displaying Static MAC Addresses 266
Figure 105: Setting the Address Aging Time 267
Figure 106: Displaying the Dynamic MAC Address Table 269
Figure 107: Clearing Entries in the Dynamic MAC Address Table 270
Figure 108: STP Root Ports and Designated Ports 272
Figure 109: MSTP Region, Internal Spanning Tree, Multiple Spanning Tree 273
Figure 110: Common Internal Spanning Tree, Common Spanning Tree, Internal Spanning Tree 273
Figure 111: Configuring Port Loopback Detection 275
Figure 112: Configuring Global Settings for STA (STP) 280
Figure 113: Configuring Global Settings for STA (RSTP) 280
Figure 114: Configuring Global Settings for STA (MSTP) 281
Figure 115: Displaying Global Settings for STA 282
Figure 116: Configuring Interface Settings for STA 286
Figure 117: STA Port Roles 288
Figure 118: Displaying Interface Settings for STA 288
Figure 119: Creating an MST Instance 290
Figure 120: Displaying MST Instances 290
Figure 121: Modifying the Priority for an MST Instance 291
Figure 122: Displaying Global Settings for an MST Instance 291
Figure 123: Adding a VLAN to an MST Instance 292
Figure 124: Displaying Members of an MST Instance 292
Figure 125: Configuring MSTP Interface Settings 294
Figure 126: Displaying MSTP Interface Settings 294
Figure 127: Configuring Rate Limits 296
Figure 128: Configuring Storm Control 298
Figure 129: Storm Control by Limiting the Traffic Rate 298
Figure 130: Storm Control by Shutting Down a Port 299
Figure 131: Configuring ATC Timers 301
Figure 132: Configuring ATC Interface Attributes 303
Figure 133: Setting the Default Port Priority 306
Figure 134: Setting the Queue Mode (Strict) 308
Figure 135: Setting the Queue Mode (WRR) 308
Figure 136: Setting the Queue Mode (Strict and WRR) 309
Figure 137: Mapping CoS Values to Egress Queues 311
Figure 138: Showing CoS Values to Egress Queue Mapping 311
Figure 139: Setting the Trust Mode 313

Figure 140: Configuring DSCP to DSCP Internal Mapping 315
Figure 141: Showing DSCP to DSCP Internal Mapping 316
Figure 142: Configuring CoS to DSCP Internal Mapping 317
Figure 143: Showing CoS to DSCP Internal Mapping 318
Figure 144: Configuring DSCP to CoS Egress Mapping 319
Figure 145: Showing DSCP to CoS Egress Mapping 320
Figure 146: Configuring IP Precedence to DSCP Internal Mapping 322
Figure 147: Showing the IP Precedence to DSCP Internal Map 322
Figure 148: Configuring IP Port Number to DSCP Internal Mapping 324
Figure 149: Showing IP Port Number to DSCP Internal Mapping 324
Figure 150: Configuring a Class Map 327
Figure 151: Showing Class Maps 328
Figure 152: Adding Rules to a Class Map 328
Figure 153: Showing the Rules for a Class Map 329
Figure 154: Configuring a Policy Map 336
Figure 155: Showing Policy Maps 337
Figure 156: Adding Rules to a Policy Map 338
Figure 157: Showing the Rules for a Policy Map 338
Figure 158: Attaching a Policy Map to a Port 339
Figure 159: Configuring a Voice VLAN 343
Figure 160: Configuring an OUI Telephony List 344
Figure 161: Showing an OUI Telephony List 344
Figure 162: Configuring Port Settings for a Voice VLAN 346
Figure 163: Configuring the Authentication Sequence 350
Figure 164: Authentication Server Operation 350
Figure 165: Configuring Remote Authentication Server (RADIUS) 353
Figure 166: Configuring Remote Authentication Server (TACACS+) 354
Figure 167: Configuring AAA Server Groups 354
Figure 168: Showing AAA Server Groups 355
Figure 169: Configuring Global Settings for AAA Accounting 357
Figure 170: Configuring AAA Accounting Methods 358
Figure 171: Showing AAA Accounting Methods 358
Figure 172: Configuring AAA Accounting Service for 802.1X Service 359
Figure 173: Configuring AAA Accounting Service for Exec Service 359
Figure 174: Displaying a Summary of Applied AAA Accounting Methods 360
Figure 175: Displaying Statistics for AAA Accounting Sessions 360

Figure 176: Configuring AAA Authorization Methods 362

Figure 177: Showing AAA Authorization Methods 362

Figure 178: Configuring AAA Authorization Methods for Exec Service 363

Figure 179: Displaying the Applied AAA Authorization Method 363

Figure 180: Configuring User Accounts 365

Figure 181: Showing User Accounts 365

Figure 182: Configuring Global Settings for Web Authentication 367

Figure 183: Configuring Interface Settings for Web Authentication 368

Figure 184: Configuring Global Settings for Network Access 372

Figure 185: Configuring Interface Settings for Network Access 374

Figure 186: Configuring Link Detection for Network Access 375

Figure 187: Configuring a MAC Address Filter for Network Access 376

Figure 188: Showing the MAC Address Filter Table for Network Access 376

Figure 189: Showing Addresses Authenticated for Network Access 378

Figure 190: Configuring HTTPS 379

Figure 191: Downloading the Secure-Site Certificate 381

Figure 192: Configuring the SSH Server 385

Figure 193: Generating the SSH Host Key Pair 386

Figure 194: Showing the SSH Host Key Pair 387

Figure 195: Copying the SSH User’s Public Key 388

Figure 196: Showing the SSH User’s Public Key 389

Figure 197: Setting the Name of a Time Range 392

Figure 198: Showing a List of Time Ranges 392

Figure 199: Add a Rule to a Time Range 393

Figure 200: Showing the Rules Configured for a Time Range 393

Figure 201: Showing TCAM Utilization 395

Figure 202: Creating an ACL 396

Figure 203: Showing a List of ACLs 396

Figure 204: Configuring a Standard IPv4 ACL 398

Figure 205: Configuring an Extended IPv4 ACL 400

Figure 206: Configuring a Standard IPv6 ACL 402

Figure 207: Configuring an Extended IPv6 ACL 404

Figure 208: Configuring a MAC ACL 406

Figure 209: Configuring a ARP ACL 408

Figure 210: Binding a Port to an ACL 409

Figure 211: Showing ACL Statistics 410

Figure 212: Configuring Global Settings for ARP Inspection 413
Figure 213: Configuring VLAN Settings for ARP Inspection 415
Figure 214: Configuring Interface Settings for ARP Inspection 416
Figure 215: Displaying Statistics for ARP Inspection 417
Figure 216: Displaying the ARP Inspection Log 418
Figure 217: Creating an IP Address Filter for Management Access 420
Figure 218: Showing IP Addresses Authorized for Management Access 420
Figure 219: Configuring Port Security 422
Figure 220: Configuring Port Security 423
Figure 221: Configuring Global Settings for 802.1X Port Authentication 425
Figure 222: Configuring Interface Settings for 802.1X Port Authenticator 429
Figure 223: Showing Statistics for 802.1X Port Authenticator 431
Figure 224: Protecting Against DoS Attacks 432
Figure 225: Setting the Filter Type for IP Source Guard 434
Figure 226: Configuring Static Bindings for IP Source Guard 436
Figure 227: Displaying Static Bindings for IP Source Guard 436
Figure 228: Showing the IP Source Guard Binding Table 438
Figure 229: Setting the Filter Type for IPv6 Source Guard 440
Figure 230: Configuring Static Bindings for IPv6 Source Guard 442
Figure 231: Displaying Static Bindings for IPv6 Source Guard 442
Figure 232: Showing the IPv6 Source Guard Binding Table 443
Figure 233: Configuring Global Settings for DHCP Snooping 447
Figure 234: Configuring DHCP Snooping on a VLAN 448
Figure 235: Configuring the Port Mode for DHCP Snooping 450
Figure 236: Displaying the Binding Table for DHCP Snooping 451
Figure 237: Configuring Settings for System Memory Logs 455
Figure 238: Showing Error Messages Logged to System Memory 456
Figure 239: Configuring Settings for Remote Logging of Error Messages 457
Figure 240: Configuring SMTP Alert Messages 458
Figure 241: Configuring LLDP Timing Attributes 460
Figure 242: Configuring LLDP Interface Attributes 464
Figure 243: Configuring the Civic Address for an LLDP Interface 466
Figure 244: Displaying Local Device Information for LLDP (General) 469
Figure 245: Displaying Local Device Information for LLDP (Port) 469
Figure 246: Displaying Local Device Information for LLDP (Port Details) 469
Figure 247: Displaying Remote Device Information for LLDP (Port) 476

Figure 248: Displaying Remote Device Information for LLDP (Port Details) 477

Figure 249: Displaying Remote Device Information for LLDP (End Node) 478

Figure 250: Displaying LLDP Device Statistics (General) 480

Figure 251: Displaying LLDP Device Statistics (Port) 480

Figure 252: Configuring Global Settings for SNMP 483

Figure 253: Configuring the Local Engine ID for SNMP 484

Figure 254: Configuring a Remote Engine ID for SNMP 485

Figure 255: Showing Remote Engine IDs for SNMP 486

Figure 256: Creating an SNMP View 487

Figure 257: Showing SNMP Views 487

Figure 258: Adding an OID Subtree to an SNMP View 488

Figure 259: Showing the OID Subtree Configured for SNMP Views 488

Figure 260: Creating an SNMP Group 493

Figure 261: Showing SNMP Groups 493

Figure 262: Setting Community Access Strings 494

Figure 263: Showing Community Access Strings 495

Figure 264: Configuring Local SNMPv3 Users 496

Figure 265: Showing Local SNMPv3 Users 497

Figure 266: Configuring Remote SNMPv3 Users 499

Figure 267: Showing Remote SNMPv3 Users 499

Figure 268: Configuring Trap Managers (SNMPv1) 503

Figure 269: Configuring Trap Managers (SNMPv2c) 503

Figure 270: Configuring Trap Managers (SNMPv3) 504

Figure 271: Showing Trap Managers 504

Figure 272: Creating SNMP Notification Logs 506

Figure 273: Showing SNMP Notification Logs 506

Figure 274: Showing SNMP Statistics 508

Figure 275: Configuring an RMON Alarm 510

Figure 276: Showing Configured RMON Alarms 511

Figure 277: Configuring an RMON Event 513

Figure 278: Showing Configured RMON Events 513

Figure 279: Configuring an RMON History Sample 515

Figure 280: Showing Configured RMON History Samples 515

Figure 281: Showing Collected RMON History Samples 516

Figure 282: Configuring an RMON Statistical Sample 517

Figure 283: Showing Configured RMON Statistical Samples 517

Figure 284: Showing Collected RMON Statistical Samples 518
Figure 285: Configuring a Switch Cluster 520
Figure 286: Configuring a Cluster Members 521
Figure 287: Showing Cluster Members 521
Figure 288: Showing Cluster Candidates 522
Figure 289: Managing a Cluster Member 523
Figure 290: ERPS Ring Components 524
Figure 291: Ring Interconnection Architecture (Multi-ring/Ladder Network) 526
Figure 292: Setting ERPS Global Status 528
Figure 293: Sub-ring with Virtual Channel 537
Figure 294: Sub-ring without Virtual Channel 538
Figure 295: Creating an ERPS Ring 542
Figure 296: Creating an ERPS Ring 543
Figure 297: Showing Configured ERPS Rings 543
Figure 298: Blocking an ERPS Ring Port 548
Figure 299: Single CFM Maintenance Domain 549
Figure 300: Multiple CFM Maintenance Domains 550
Figure 301: Configuring Global Settings for CFM 554
Figure 302: Configuring Interfaces for CFM 555
Figure 303: Configuring Maintenance Domains 559
Figure 304: Showing Maintenance Domains 559
Figure 305: Configuring Detailed Settings for Maintenance Domains 560
Figure 306: Creating Maintenance Associations 563
Figure 307: Showing Maintenance Associations 564
Figure 308: Configuring Detailed Settings for Maintenance Associations 565
Figure 309: Configuring Maintenance End Points 566
Figure 310: Showing Maintenance End Points 567
Figure 311: Configuring Remote Maintenance End Points 568
Figure 312: Showing Remote Maintenance End Points 569
Figure 313: Transmitting Link Trace Messages 570
Figure 314: Transmitting Loopback Messages 572
Figure 315: Transmitting Delay-Measure Messages 574
Figure 316: Showing Information on Local MEPs 575
Figure 317: Showing Detailed Information on Local MEPs 577
Figure 318: Showing Information on Local MIPs 578
Figure 319: Showing Information on Remote MEPs 579

Figure 320: Showing Detailed Information on Remote MEPs 581
Figure 321: Showing the Link Trace Cache 583
Figure 322: Showing Settings for the Fault Notification Generator 584
Figure 323: Showing Continuity Check Errors 585
Figure 324: Enabling OAM for Local Ports 588
Figure 325: Displaying Statistics for OAM Messages 589
Figure 326: Displaying the OAM Event Log 590
Figure 327: Displaying Status of Remote Interfaces 591
Figure 328: Running a Remote Loop Back Test 593
Figure 329: Displaying the Results of Remote Loop Back Testing 594
Figure 330: Configuring Global Settings for PTP 598
Figure 331: Configuring Interface Settings for PTP 602
Figure 332: Displaying PTP Information (Default Data) 605
Figure 333: Displaying PTP Information (Current Data) 606
Figure 334: Displaying PTP Information (Parent Data) 606
Figure 335: Displaying PTP Information (Time Properties) 606
Figure 336: Displaying PTP Information (Port Data) 607
Figure 337: Displaying PTP Neighbor Information 608
Figure 338: Multicast Filtering Concept 610
Figure 339: IGMP Protocol 611
Figure 340: Configuring General Settings for IGMP Snooping 617
Figure 341: Configuring a Static Interface for an IPv4 Multicast Router 618
Figure 342: Showing Static Interfaces Attached an IPv4 Multicast Router 619
Figure 343: Showing Current Interfaces Attached an IPv4 Multicast Router 619
Figure 344: Assigning an Interface to an IPv4 Multicast Service 620
Figure 345: Showing Static Interfaces Assigned to an IPv4 Multicast Service 621
Figure 346: Configuring IGMP Snooping on a VLAN 626
Figure 347: Showing Interface Settings for IGMP Snooping 626
Figure 348: Dropping IGMP Query or Multicast Data Packets 627
Figure 349: Showing Multicast Groups Learned by IGMP Snooping 629
Figure 350: Displaying IGMP Snooping Statistics – Query 631
Figure 351: Displaying IGMP Snooping Statistics – VLAN 632
Figure 352: Displaying IGMP Snooping Statistics – Port 632
Figure 353: Enabling IGMP Filtering and Throttling 634
Figure 354: Creating an IGMP Filtering Profile 635
Figure 355: Showing the IGMP Filtering Profiles Created 635

Figure 356: Adding Multicast Groups to an IGMP Filtering Profile 636

Figure 357: Showing the Groups Assigned to an IGMP Filtering Profile 636

Figure 358: Configuring IGMP Filtering and Throttling Interface Settings 638

Figure 359: Configuring General Settings for MLD Snooping 640

Figure 360: Configuring Immediate Leave for MLD Snooping 641

Figure 361: Configuring a Static Interface for an IPv6 Multicast Router 642

Figure 362: Showing Static Interfaces Attached an IPv6 Multicast Router 642

Figure 363: Showing Current Interfaces Attached an IPv6 Multicast Router 642

Figure 364: Assigning an Interface to an IPv6 Multicast Service 644

Figure 365: Showing Static Interfaces Assigned to an IPv6 Multicast Service 644

Figure 366: Showing Current Interfaces Assigned to an IPv6 Multicast Service 645

Figure 367: Showing IPv6 Multicast Services and Corresponding Sources 646

Figure 368: IGMP Proxy Routing 647

Figure 369: Configuring IGMP Proxy Routing 649

Figure 370: Configuring IGMP Interface Settings 652

Figure 371: Configuring Static IGMP Groups 653

Figure 372: Showing Static IGMP Groups 654

Figure 373: Displaying Multicast Groups Learned from IGMP (Information) 656

Figure 374: Displaying Multicast Groups Learned from IGMP (Detail) 656

Figure 375: MVR Concept 657

Figure 376: Configuring Global Settings for MVR 660

Figure 377: Configuring Domain Settings for MVR 661

Figure 378: Configuring an MVR Group Address Profile 663

Figure 379: Displaying MVR Group Address Profiles 663

Figure 380: Assigning an MVR Group Address Profile to a Domain 664

Figure 381: Showing the MVR Group Address Profiles Assigned to a Domain 664

Figure 382: Configuring Interface Settings for MVR 667

Figure 383: Assigning Static MVR Groups to a Port 668

Figure 384: Showing the Static MVR Groups Assigned to a Port 668

Figure 385: Displaying MVR Receiver Groups 669

Figure 386: Displaying MVR Statistics – Query 672

Figure 387: Displaying MVR Statistics – VLAN 673

Figure 388: Displaying MVR Statistics – Port 674

Figure 389: Configuring Global Settings for MVR6 677

Figure 390: Configuring Domain Settings for MVR6 678

Figure 391: Configuring an MVR6 Group Address Profile 680

Figure 392: Displaying MVR6 Group Address Profiles 680
Figure 393: Assigning an MVR6 Group Address Profile to a Domain 681
Figure 394: Showing MVR6 Group Address Profiles Assigned to a Domain 681
Figure 395: Configuring Interface Settings for MVR6 683
Figure 396: Assigning Static MVR6 Groups to a Port 685
Figure 397: Showing the Static MVR6 Groups Assigned to a Port 685
Figure 398: Displaying MVR6 Receiver Groups 686
Figure 399: Displaying MVR6 Statistics – Query 688
Figure 400: Displaying MVR6 Statistics – VLAN 689
Figure 401: Displaying MVR6 Statistics – Port 690
Figure 402: Configuring a Static IPv4 Address 693
Figure 403: Configuring a Dynamic IPv4 Address 694
Figure 404: Showing the IPv4 Address for an Interface 695
Figure 405: Configuring the IPv6 Default Gateway 696
Figure 406: Configuring General Settings for an IPv6 Interface 700
Figure 407: Configuring RA Guard for an IPv6 Interface 700
Figure 408: Configuring an IPv6 Address 703
Figure 409: Showing Configured IPv6 Addresses 704
Figure 410: Showing IPv6 Neighbors 706
Figure 411: Showing IPv6 Statistics (IPv6) 710
Figure 412: Showing IPv6 Statistics (ICMPv6) 711
Figure 413: Showing IPv6 Statistics (UDP) 711
Figure 414: Showing Reported MTU Values 712
Figure 415: Configuring General Settings for DNS 714
Figure 416: Configuring a List of Domain Names for DNS 715
Figure 417: Showing the List of Domain Names for DNS 716
Figure 418: Configuring a List of Name Servers for DNS 717
Figure 419: Showing the List of Name Servers for DNS 717
Figure 420: Configuring Static Entries in the DNS Table 718
Figure 421: Showing Static Entries in the DNS Table 718
Figure 422: Showing Entries in the DNS Cache 719
Figure 423: Specifying A DHCP Client Identifier 721
Figure 424: Layer 3 DHCP Relay Service 722
Figure 425: Configuring DHCP Relay Service 723
Figure 426: DHCP Server 723
Figure 427: Enabling the DHCP Server 724

Figure 428: Configuring Excluded Addresses on the DHCP Server 725
Figure 429: Showing Excluded Addresses on the DHCP Server 725
Figure 430: Configuring DHCP Server Address Pools (Network) 728
Figure 431: Configuring DHCP Server Address Pools (Host) 729
Figure 432: Showing Configured DHCP Server Address Pools 729
Figure 433: Shows Addresses Assigned by the DHCP Server 730
Figure 434: Enabling the UDP Helper 731
Figure 435: Specifying UDP Destination Ports 732
Figure 436: Showing the UDP Destination Ports 733
Figure 437: Specifying the Target Server or Subnet for UDP Requests 734
Figure 438: Showing the Target Server or Subnet for UDP Requests 734
Figure 439: Configuring Global Settings for PPPoE Intermediate Agent 736
Figure 440: Configuring Interface Settings for PPPoE Intermediate Agent 738
Figure 441: Showing PPPoE Intermediate Agent Statistics 739
Figure 442: Virtual Interfaces and Layer 3 Routing 742
Figure 443: Pinging a Network Device 746
Figure 444: Tracing the Route to a Network Device 747
Figure 445: Proxy ARP 749
Figure 446: Configuring General Settings for ARP 750
Figure 447: Configuring Static ARP Entries 751
Figure 448: Displaying Static ARP Entries 751
Figure 449: Displaying Dynamic ARP Entries 752
Figure 450: Displaying Local ARP Entries 752
Figure 451: Displaying ARP Statistics 753
Figure 452: Configuring Static Routes 755
Figure 453: Displaying Static Routes 755
Figure 454: Displaying the Routing Table 757
Figure 455: Setting the Maximum ECMP Number 758
Figure 456: Master Virtual Router with Backup Routers 759
Figure 457: Several Virtual Master Routers Using Backup Routers 759
Figure 458: Several Virtual Master Routers Configured for Mutual Backup and Load Sharing 760
Figure 459: Configuring the VRRP Group ID 764
Figure 460: Showing Configured VRRP Groups 764
Figure 461: Setting the Virtual Router Address for a VRRP Group 765
Figure 462: Showing the Virtual Addresses Assigned to VRRP Groups 765
Figure 463: Configuring Detailed Settings for a VRRP Group 766

Figure 464: Showing Counters for Errors Found in VRRP Packets 767
Figure 465: Showing Counters for Errors Found in a VRRP Group 768
Figure 466: Configuring RIP 770
Figure 467: Configuring General Settings for RIP 774
Figure 468: Clearing Entries from the Routing Table 775
Figure 469: Adding Network Interfaces to RIP 776
Figure 470: Showing Network Interfaces Using RIP 777
Figure 471: Specifying a Passive RIP Interface 778
Figure 472: Showing Passive RIP Interfaces 778
Figure 473: Specifying a Static RIP Neighbor 779
Figure 474: Showing Static RIP Neighbors 779
Figure 475: Redistributing External Routes into RIP 780
Figure 476: Showing External Routes Redistributed into RIP 781
Figure 477: Setting the Distance Assigned to External Routes 782
Figure 478: Showing the Distance Assigned to External Routes 782
Figure 479: Configuring a Network Interface for RIP 785
Figure 480: Showing RIP Network Interface Settings 786
Figure 481: Showing RIP Interface Settings 787
Figure 482: Showing RIP Peer Information 787
Figure 483: Resetting RIP Statistics 788
Figure 484: Configuring OSPF 789
Figure 485: OSPF Areas 790
Figure 486: Defining OSPF Network Areas Based on Addresses 792
Figure 487: Showing OSPF Network Areas 792
Figure 488: Showing OSPF Process Identifiers 793
Figure 489: AS Boundary Router 795
Figure 490: Configure General Settings for OSPF 796
Figure 491: Showing General Settings for OSPF 797
Figure 492: Adding an NSSA or Stub 798
Figure 493: Showing NSSAs or Stubs 799
Figure 494: OSPF NSSA 799
Figure 495: Configuring Protocol Settings for an NSSA 802
Figure 496: OSPF Stub Area 802
Figure 497: Configuring Protocol Settings for a Stub 804
Figure 498: Displaying Information on NSSA and Stub Areas 805
Figure 499: Route Summarization for ABRs 805

Figure 500: Configuring Route Summaries for an Area Range 806
Figure 501: Showing Configured Route Summaries 807
Figure 502: Redistributing External Routes 807
Figure 503: Importing External Routes 809
Figure 504: Showing Imported External Route Types 809
Figure 505: Summarizing External Routes 810
Figure 506: Showing Summary Addresses for External Routes 811
Figure 507: Configuring Settings for All Interfaces Assigned to a VLAN 815
Figure 508: Configuring Settings for a Specific Area Assigned to a VLAN 816
Figure 509: Showing OSPF Interfaces 817
Figure 510: Showing MD5 Authentication Keys 817
Figure 511: OSPF Virtual Link 818
Figure 512: Adding a Virtual Link 819
Figure 513: Showing Virtual Links 819
Figure 514: Configuring Detailed Settings for a Virtual Link 820
Figure 515: Showing MD5 Authentication Keys 820
Figure 516: Displaying Information in the Link State Database 822
Figure 517: Displaying Neighbor Routers Stored in the Link State Database 824
Figure 518: Enabling IPv4 Multicast Routing 828
Figure 519: Enabling IPv6 Multicast Routing 829
Figure 520: Displaying the IPv4 Multicast Routing Table 831
Figure 521: Displaying Detailed Entries from IPv4 Multicast Routing Table 832
Figure 522: Displaying the IPv6 Multicast Routing Table 832
Figure 523: Displaying Detailed Entries from IPv6 Multicast Routing Table 833
Figure 524: Enabling PIM Multicast Routing 834
Figure 525: Configuring PIM Interface Settings (Dense Mode) 838
Figure 526: Configuring PIM Interface Settings (Sparse Mode) 839
Figure 527: Showing PIM Neighbors 840
Figure 528: Configuring Global Settings for PIM-SM 841
Figure 529: Configuring a PIM-SM BSR Candidate 843
Figure 530: Configuring a PIM Static Rendezvous Point 844
Figure 531: Showing PIM Static Rendezvous Points 845
Figure 532: Configuring a PIM RP Candidate 846
Figure 533: Showing Settings for a PIM RP Candidate 847
Figure 534: Showing Information About the PIM BSR 848
Figure 535: Showing PIM RP Mapping 849

Figure 536: Enabling PIMv6 Multicast Routing 850
Figure 537: Configuring PIMv6 Interface Settings (Dense Mode) 855
Figure 538: Configuring PIMv6 Interface Settings (Sparse Mode) 855
Figure 539: Showing PIMv6 Neighbors 856
Figure 540: Configuring Global Settings for PIM6-SM 858
Figure 541: Configuring a PIM6-SM BSR Candidate 859
Figure 542: Configuring a PIM6 Static Rendezvous Point 861
Figure 543: Showing PIM6 Static Rendezvous Points 861
Figure 544: Configuring a PIM6 RP Candidate 863
Figure 545: Showing Settings for a PIM6 RP Candidate 863
Figure 546: Showing Information About the PIM6 BSR 864
Figure 547: Showing PIM6 RP Mapping 865
Figure 548: Storm Control by Limiting the Traffic Rate 1244
Figure 549: Storm Control by Shutting Down a Port 1245
Figure 550: Sub-ring with Virtual Channel 1321
Figure 551: Sub-ring without Virtual Channel 1322
Figure 552: Configuring VLAN Trunking 1351
Figure 553: Mapping QinQ Service VLAN to Customer VLAN 1357
Figure 554: Configuring VLAN Translation 1365
Figure 555: Connections for Internal and External BGP 1819
Figure 556: Connections for Single Route Reflector 1824
Figure 557: Connections for Multiple Route Reflectors 1824
Figure 558: Connections for BGP Confederation 1826
Figure 559: Connections for Route Server 1827

TABLES

Table 1: Key Features 93

Table 2: System Defaults 102

Table 3: Options 60, 66 and 67 Statements 115

Table 4: Options 55 and 124 Statements 116

Table 5: Web Page Configuration Buttons 125

Table 6: Switch Main Menu 126

Table 7: Port Statistics 193

Table 8: LACP Port Counters 213

Table 9: LACP Internal Configuration Information 214

Table 10: LACP Remote Device Configuration Information 216

Table 11: Traffic Segmentation Forwarding 220

Table 12: Recommended STA Path Cost Range 283

Table 13: Default STA Path Costs 284

Table 14: IEEE 802.1p Egress Queue Priority Mapping 309

Table 15: CoS Priority Levels 310

Table 16: Mapping Internal Per-hop Behavior to Hardware Queues 310

Table 17: Default Mapping of DSCP Values to Internal PHB/Drop Values 315

Table 18: Default Mapping of CoS/CFI to Internal PHB/Drop Precedence 317

Table 19: Mapping Internal PHB/Drop Precedence to CoS/CFI Values 319

Table 20: Mapping IP Precedence 320

Table 21: Default Mapping of IP Precedence to Internal PHB/Drop Values 321

Table 22: Dynamic QoS Profiles 369

Table 23: HTTPS System Support 379

Table 24: ARP Inspection Statistics 416

Table 25: ARP Inspection Log 417

Table 26: 802.1X Statistics 429

Table 27: Logging Levels 454

Table 28: LLDP MED Location CA Types 465

Table 29: Chassis ID Subtype 466

Table 30: System Capabilities 467

Table 31: Port ID Subtype 468

Table 32: Remote Port Auto-Negotiation Advertised Capability 471
Table 33: SNMPv3 Security Models and Levels 481
Table 34: Supported Notification Messages 490
Table 35: ERPS Request/State Priority 545
Table 36: Remote MEP Priority Levels 557
Table 37: MEP Defect Descriptions 557
Table 38: OAM Operation State 586
Table 39: OAM Operation State 592
Table 40: Ethernet Multicast MAC Addresses 599
Table 41: UDP/IPv4 Destination Port Numbers 599
Table 42: UDP/IPv4 Multicast Addresses 599
Table 43: UDP/IPv6 Destination Port Numbers 600
Table 44: UDP/IPv6 Multicast Addresses 600
Table 45: Show IPv6 Neighbors - display description 705
Table 46: Show IPv6 Statistics - display description 707
Table 47: Show MTU - display description 712
Table 48: Options 60, 66 and 67 Statements 720
Table 49: Options 55 and 124 Statements 720
Table 50: Address Resolution Protocol 748
Table 51: ARP Statistics 753
Table 52: VRRP Group Statistics 767
Table 53: OSPF System Information 796
Table 54: General Command Modes 875
Table 55: Configuration Command Modes 877
Table 56: Keystroke Commands 878
Table 57: Command Group Index 879
Table 58: General Commands 883
Table 59: System Management Commands 891
Table 60: Device Designation Commands 891
Table 61: Banner Commands 892
Table 62: System Status Commands 901
Table 63: Fan Control Commands 910
Table 64: Frame Size Commands 910
Table 65: Flash/File Commands 912
Table 66: File Directory Information 918
Table 67: Line Commands 923

Table 68: Event Logging Commands 933

Table 69: Logging Levels 934

Table 70: show logging flash/ram - display description 939

Table 71: show logging trap - display description 939

Table 72: Event Logging Commands 940

Table 73: Time Commands 944

Table 74: Predefined Summer-Time Parameters 953

Table 75: Time Range Commands 957

Table 76: PTP Commands 960

Table 77: Ethernet Multicast MAC Addresses 972

Table 78: UDP/IPv4 Destination Port Numbers 972

Table 79: UDP/IPv4 Multicast Addresses 972

Table 80: UDP/IPv6 Destination Port Numbers 972

Table 81: UDP/IPv6 Multicast Addresses 973

Table 82: show ptp foreign-mater - display description 975

Table 83: show ptp information - display description for boundary clock 977

Table 84: show ptp information - display description for transparent clock 979

Table 85: Sync-E Commands 979

Table 86: Synchronous Ethernet Standards 980

Table 87: show sync - display description for sync 988

Table 88: Switch Cluster Commands 989

Table 89: SNMP Commands 995

Table 90: show snmp engine-id - display description 1009

Table 91: show snmp group - display description 1011

Table 92: show snmp user - display description 1011

Table 93: show snmp view - display description 1012

Table 94: RMON Commands 1017

Table 95: sFlow Commands 1025

Table 96: Authentication Commands 1031

Table 97: User Access Commands 1032

Table 98: Default Login Settings 1033

Table 99: Authentication Sequence Commands 1034

Table 100: RADIUS Client Commands 1036

Table 101: TACACS+ Client Commands 1040

Table 102: AAA Commands 1044

Table 103: Web Server Commands 1051

Table 104: HTTPS System Support 1054
Table 105: Telnet Server Commands 1055
Table 106: Secure Shell Commands 1057
Table 107: show ssh - display description 1066
Table 108: 802.1X Port Authentication Commands 1067
Table 109: Management IP Filter Commands 1078
Table 110: PPPoE Intermediate Agent Commands 1081
Table 111: show pppoe intermediate-agent statistics - display description 1087
Table 112: General Security Commands 1089
Table 113: Management IP Filter Commands 1090
Table 114: show port security - display description 1094
Table 115: Network Access Commands 1095
Table 116: Dynamic QoS Profiles 1099
Table 117: Web Authentication 1110
Table 118: DHCP Snooping Commands 1115
Table 119: Option 82 information 1122
Table 120: DHCP Snooping Commands 1126
Table 121: IPv4 Source Guard Commands 1133
Table 122: IPv6 Source Guard Commands 1140
Table 123: ARP Inspection Commands 1145
Table 124: DoS Protection Commands 1154
Table 125: Commands for Configuring Traffic Segmentation 1157
Table 126: Traffic Segmentation Forwarding 1158
Table 127: Access Control List Commands 1163
Table 128: IPv4 ACL Commands 1163
Table 129: IPv6 ACL Commands 1170
Table 130: MAC ACL Commands 1176
Table 131: ARP ACL Commands 1181
Table 132: ACL Information Commands 1184
Table 133: Interface Commands 1187
Table 134: show interfaces switchport - display description 1204
Table 135: Link Aggregation Commands 1215
Table 136: show lacp counters - display description 1225
Table 137: show lacp internal - display description 1225
Table 138: show lacp neighbors - display description 1226
Table 139: show lacp sysid - display description 1227

Table 140: Port Mirroring Commands 1229
Table 141: Mirror Port Commands 1229
Table 142: RSPAN Commands 1231
Table 143: Congestion Control Commands 1239
Table 144: Rate Limit Commands 1239
Table 145: Rate Limit Commands 1241
Table 146: ATC Commands 1243
Table 147: Loopback Detection Commands 1259
Table 148: UniDirectional Link Detection Commands 1265
Table 149: show udld - display description 1268
Table 150: Address Table Commands 1271
Table 151: Spanning Tree Commands 1277
Table 152: Recommended STA Path Cost Range 1290
Table 153: Default STA Path Costs 1291
Table 154: ERPS Commands 1305
Table 155: ERPS Request/State Priority 1328
Table 156: show erps - summary display description 1332
Table 157: show erps domain - detailed display description 1333
Table 158: show erps statistics - detailed display description 1334
Table 159: VLAN Commands 1337
Table 160: GVRP and Bridge Extension Commands 1338
Table 161: Commands for Editing VLAN Groups 1343
Table 162: Commands for Configuring VLAN Interfaces 1345
Table 163: Commands for Displaying VLAN Information 1352
Table 164: 802.1Q Tunneling Commands 1353
Table 165: L2 Protocol Tunnel Commands 1360
Table 166: VLAN Translation Commands 1364
Table 167: Private VLAN Commands 1367
Table 168: Protocol-based VLAN Commands 1372
Table 169: IP Subnet VLAN Commands 1375
Table 170: MAC Based VLAN Commands 1377
Table 171: Voice VLAN Commands 1379
Table 172: Priority Commands 1387
Table 173: Priority Commands (Layer 2) 1387
Table 174: Priority Commands (Layer 3 and 4) 1392
Table 175: Default Mapping of CoS/CFI to Internal PHB/Drop Precedence 1393

Table 176: Mapping Per-hop Behavior to Drop Precedence 1394
Table 177: Mapping Internal PHB/Drop Precedence to CoS/CFI Values 1395
Table 178: Default Mapping of DSCP Values to Internal PHB/Drop Values 1397
Table 179: Default Mapping of IP Precedence to Internal PHB/Drop Values 1399
Table 180: Mapping Internal Per-hop Behavior to Hardware Queues 1399
Table 181: Quality of Service Commands 1407
Table 182: Multicast Filtering Commands 1425
Table 183: IGMP Snooping Commands 1426
Table 184: show ip igmp snooping statistics input - display description 1445
Table 185: show ip igmp snooping statistics output - display description 1445
Table 186: show ip igmp snooping statistics vlan query - display description 1446
Table 187: Static Multicast Interface Commands 1446
Table 188: IGMP Filtering and Throttling Commands 1448
Table 189: IGMP Authentication RADIUS Attribute Value Pairs 1452
Table 190: MLD Snooping Commands 1460
Table 191: MLD Filtering and Throttling Commands 1469
Table 192: Multicast VLAN Registration for IPv4 Commands 1478
Table 193: show mvr - display description 1490
Table 194: show mvr interface - display description 1491
Table 195: show mvr members - display description 1493
Table 196: show mvr statistics input - display description 1494
Table 197: show mvr statistics output - display description 1495
Table 198: show mvr statistics query - display description 1495
Table 199: Multicast VLAN Registration for IPv6 Commands 1496
Table 200: show mvr6 - display description 1508
Table 201: show mvr6 interface - display description 1509
Table 202: show mvr6 members - display description 1511
Table 203: show mvr6 statistics input - display description 1512
Table 204: show mvr6 statistics output - display description 1513
Table 205: IGMP Commands (Layer 3) 1513
Table 206: show ip igmp groups - display description 1521
Table 207: show ip igmp groups detail - display description 1521
Table 208: IGMP Proxy Commands 1523
Table 209: MLD Commands (Layer 3) 1525
Table 210: show ipv6 mld groups - display description 1532
Table 211: IGMP Proxy Commands 1533

Table 212: LLDP Commands 1537
Table 213: LLDP MED Location CA Types 1550
Table 214: CFM Commands 1561
Table 215: show ethernet cfm configuration traps - display description 1575
Table 216: show ethernet cfm maintenance-points local detail mep - display 1578
Table 217: show ethernet cfm maintenance-points remote detail - display 1580
Table 218: show ethernet cfm errors - display description 1586
Table 219: show ethernet cfm linktrace-cache - display description 1594
Table 220: Remote MEP Priority Levels 1597
Table 221: MEP Defect Descriptions 1598
Table 222: show fault-notify-generator - display description 1599
Table 223: OAM Commands 1603
Table 224: Address Table Commands 1615
Table 225: show dns cache - display description 1622
Table 226: show hosts - display description 1623
Table 227: DHCP Commands 1625
Table 228: DHCP Client Commands 1625
Table 229: Options 60, 66 and 67 Statements 1626
Table 230: Options 55 and 124 Statements 1626
Table 231: DHCP Relay Commands 1629
Table 232: DHCP Server Commands 1632
Table 233: IP Interface Commands 1647
Table 234: IPv4 Interface Commands 1647
Table 235: Basic IP Configuration Commands 1648
Table 236: Address Resolution Protocol Commands 1655
Table 237: UDP Helper Commands 1659
Table 238: IPv6 Configuration Commands 1663
Table 239: show ipv6 interface - display description 1673
Table 240: show ipv6 mtu - display description 1674
Table 241: show ipv6 traffic - display description 1676
Table 242: show ipv6 neighbors - display description 1695
Table 243: IPv6 to IPv4 Tunnelling Commands 1696
Table 244: ND Snooping Commands 1704
Table 245: VRRP Commands 1713
Table 246: show vrrp - display description 1719
Table 247: show vrrp brief - display description 1720

Table 248: IP Routing Commands 1723
Table 249: Global Routing Configuration Commands 1723
Table 250: show ip host-route - display description 1726
Table 251: Routing Information Protocol Commands 1733
Table 252: Open Shortest Path First Commands 1750
Table 253: show ip ospf - display description 1778
Table 254: show ip ospf database - display description 1781
Table 255: show ip ospf database summary - display description 1782
Table 256: show ip ospf database external - display description 1783
Table 257: show ip ospf database network - display description 1784
Table 258: show ip ospf database router - display description 1784
Table 259: show ip ospf database summary - display description 1785
Table 260: show ip ospf interface - display description 1786
Table 261: show ip ospf neighbor - display description 1788
Table 262: show ip ospf virtual-links - display description 1789
Table 263: show ip protocols ospf - display description 1790
Table 264: Open Shortest Path First Commands (Version 3) 1790
Table 265: show ip ospf - display description 1812
Table 266: show ip ospf database - display description 1814
Table 267: show ip ospf interface - display description 1814
Table 268: show ipv6 ospf neighbor - display description 1816
Table 269: show ipv6 ospf virtual-links - display description 1817
Table 270: Border Gateway Protocol Commands – Version 4 1828
Table 271: show ip bgp - display description 1884
Table 272: show ip bgp community-info - display description 1887
Table 273: show ip bgp dampening parameters- display description 1889
Table 274: show ip bgp - display description 1891
Table 275: show ip bgp paths - display description 1892
Table 276: Policy-based Routing Configuration Commands 1898
Table 277: Multicast Routing Commands 1919
Table 278: General Multicast Routing Commands 1919
Table 279: show ip mroute - display description 1921
Table 280: show ip mroute - display description 1924
Table 281: Static Multicast Routing Commands 1925
Table 282: IPv4 and IPv6 PIM Commands 1927
Table 283: PIM-DM and PIM-SM Multicast Routing Commands 1927

Table 284: show ip pim neighbor - display description 1936
Table 285: show ip pim bsr-router - display description 1948
Table 286: show ip pim rp mapping - display description 1949
Table 287: show ip pim rp-hash - display description 1949
Table 288: PIM-DM and PIM-SM Multicast Routing Commands 1950
Table 289: show ipv6 pim neighbor - display description 1958
Table 290: show ip pim bsr-router - display description 1971
Table 291: show ip pim rp mapping - display description 1972
Table 292: show ip pim rp-hash - display description 1972
Table 293: Troubleshooting Chart 1981

SECTION I

GETTING STARTED

This section provides an overview of the switch, and introduces some basic concepts about network switches. It also describes the basic settings required to access the management interface.

This section includes these chapters:

- "Introduction" on page 93
- "Initial Switch Configuration" on page 105

1 Introduction

This switch provides a broad range of features for Layer 2 switching and Layer 3 routing. It includes a management agent that allows you to configure the features listed in this manual. The default configuration can be used for most of the features provided by this switch. However, there are many options that you should configure to maximize the switch's performance for your particular network environment.

Key Features

Table 1: Key Features

Feature	Description
Configuration Backup and Restore	Using management station or FTP/TFTP server
Authentication	Console, Telnet, web – user name/password, RADIUS, TACACS+ Port – IEEE 802.1X, MAC address filtering SNMP v1/2c - Community strings SNMP version 3 – MD5 or SHA password Telnet – SSH Web – HTTPS
General Security Measures	AAA ARP inspection DHCP Snooping (with Option 82 relay information) IP Source Guard PPPoE Intermediate Agent Private VLANs Port Authentication – IEEE 802.1X Port Security – MAC address filtering
Access Control Lists	Supports up to 256 ACLs, up to 96 rules per ACL
DHCP	Client, Relay, Server
DHCPv6	Client
DNS	Client and Proxy service
Port Configuration	Speed, duplex mode and flow control
Port Trunking	Supports up to 8 trunks – static or dynamic trunking (LACP)
Port Mirroring	28 sessions, one or more source ports to one analysis port
Congestion Control	Rate Limiting Throttling for broadcast, multicast, unknown unicast storms

Table 1: Key Features (Continued)

Feature	Description
Address Table	32K MAC addresses in forwarding table, 1K static MAC addresses; 8K entries in ARP cache,256 static ARP entries; 512 static IP routes, 512 IP interfaces; 12K IPv4 entries in host table; 8K IPv4 entries in routing table; 6K IPv6 entries in host table; 4K IPv6 entries in routing table 1K L2 IPv4 multicast groups; 1K L3 IPv4 multicast groups (shared with IPv6); 1K L3 IPv6 multicast groups (shared with IPv4)
IP Version 4 and 6	Supports IPv4 and IPv6 addressing, and management
IEEE 802.1D Bridge	Supports dynamic data switching and addresses learning
Store-and-Forward Switching	Supported to ensure wire-speed switching while eliminating bad frames
Spanning Tree Algorithm	Supports standard STP, Rapid Spanning Tree Protocol (RSTP), and Multiple Spanning Trees (MSTP)
Virtual LANs	Up to 4094 using IEEE 802.1Q, port-based, protocol-based, private VLANs, voice VLANs, and QinQ tunnel
Traffic Prioritization	Default port priority, traffic class map, queue scheduling, IP Precedence, or Differentiated Services Code Point (DSCP), and TCP/UDP Port
Qualify of Service	Supports Differentiated Services (DiffServ)
Link Layer Discovery Protocol	Used to discover basic information about neighboring devices
Switch Clustering	Supports up to 36 member switches in a cluster
Connectivity Fault Management	Connectivity monitoring using continuity check messages, fault verification through loop back messages, and fault isolation by examining end-to-end connections (IEEE 802.1ag)
ERPS	Supports Ethernet Ring Protection Switching for increased availability of Ethernet rings (G.8032)
Remote Device Management	Supports Ethernet OAM functions for attached CPEs (IEEE 802.3ah, ITU-T Y.1731)
Router Redundancy	Router backup is provided with the Virtual Router Redundancy Protocol (VRRP)
IP Routing	Routing Information Protocol (RIPv2), Open Shortest Path First (OSPFv2/v3), Border Gateway Protocol (BGPv4), policy-based routing for BGP, static routes, Equal-Cost Multipath Routing (ECMP)
ARP	Static and dynamic address configuration, proxy ARP
Multicast Filtering	Supports IGMP snooping and query for Layer 2, MLD snooping and query, IGMP for Layer 3, and Multicast VLAN Registration
Multicast Routing	Protocol-Independent Multicasting - Dense Mode and Sparse Mode (PIM-DM, PIM-SM, PIM6-DM, PIM6-SM)

DESCRIPTION OF SOFTWARE FEATURES

The switch provides a wide range of advanced performance enhancing features. Flow control eliminates the loss of packets due to bottlenecks caused by port saturation. Broadcast storm suppression prevents broadcast traffic storms from engulfing the network. Untagged (port-based), tagged, and protocol-based VLANs, plus support for automatic GVRP VLAN registration provide traffic security and efficient use of network bandwidth. CoS priority queueing ensures the minimum delay for moving real-time multimedia data across the network. While multicast filtering and routing provides support for real-time network applications.

Some of the management features are briefly described below.

CONFIGURATION BACKUP AND RESTORE

You can save the current configuration settings to a file on the management station (using the web interface) or an FTP/TFTP server (using the web or console interface), and later download this file to restore the switch configuration settings.

AUTHENTICATION

This switch authenticates management access via the console port, Telnet, or a web browser. User names and passwords can be configured locally or can be verified via a remote authentication server (i.e., RADIUS or TACACS+). Port-based authentication is also supported via the IEEE 802.1X protocol. This protocol uses Extensible Authentication Protocol over LANs (EAPOL) to request user credentials from the 802.1X client, and then uses the EAP between the switch and the authentication server to verify the client’s right to access the network via an authentication server (i.e., RADIUS or TACACS+ server).

Other authentication options include HTTPS for secure management access via the web, SSH for secure management access over a Telnet-equivalent connection, SNMP Version 3, IP address filtering for SNMP/Telnet/web management access. MAC address filtering and IP source guard also provide authenticated port access. While DHCP snooping is provided to prevent malicious attacks from insecure ports. While PPPoE Intermediate Agent supports authentication of a client for a service provider.

ACCESS CONTROL LISTS

ACLs provide packet filtering for IP frames (based on address, protocol, TCP/UDP port number or TCP control code) or any frames (based on MAC address or Ethernet type). ACLs can by used to improve performance by blocking unnecessary network traffic or to implement security controls by restricting access to specific network resources or protocols.

DHCP

A DHCP server is provided to assign IP addresses to host devices. Since DHCP uses a broadcast mechanism, a DHCP server and its client must physically reside on the same subnet. Since it is not practical to have a DHCP server on every subnet, DHCP Relay is also supported to allow dynamic configuration of local clients from a DHCP server located in a different network.

PORT CONFIGURATION

You can manually configure the speed, duplex mode, and flow control used on specific ports, or use auto-negotiation to detect the connection settings used by the attached device. Use full-duplex mode on ports whenever possible to double the throughput of switch connections. Flow control should also be enabled to control network traffic during periods of congestion and prevent the loss of packets when port buffer thresholds are exceeded. The switch supports flow control based on the IEEE 802.3x standard (now incorporated in IEEE 802.3-2002).

RATE LIMITING

This feature controls the maximum rate for traffic transmitted or received on an interface. Rate limiting is configured on interfaces at the edge of a network to limit traffic into or out of the network. Packets that exceed the acceptable amount of traffic are dropped.

PORT MIRRORING

The switch can unobtrusively mirror traffic from any port to a monitor port. You can then attach a protocol analyzer or RMON probe to this port to perform traffic analysis and verify connection integrity.

PORT TRUNKING

Ports can be combined into an aggregate connection. Trunks can be manually set up or dynamically configured using Link Aggregation Control Protocol (LACP – IEEE 802.3-2005). The additional ports dramatically increase the throughput across any connection, and provide redundancy by taking over the load if a port in the trunk should fail. The switch supports up to 8 trunks.

STORM CONTROL

Broadcast, multicast and unknown unicast storm suppression prevents traffic from overwhelming the network.When enabled on a port, the level of traffic passing through the port is restricted. If traffic rises above a pre-defined threshold, it will be throttled until the level falls back beneath the threshold.

STATIC MAC ADDRESSES

A static address can be assigned to a specific interface on this switch. Static addresses are bound to the assigned interface and will not be moved. When a static address is seen on another interface, the address will be ignored and will not be written to the address table. Static addresses can be used to provide network security by restricting access for a known host to a specific port.

IP ADDRESS FILTERING

Access to insecure ports can be controlled using DHCP Snooping which filters ingress traffic based on static IP addresses and addresses stored in the DHCP Snooping table. Traffic can also be restricted to specific source IP addresses or source IP/MAC address pairs based on static entries or entries stored in the DHCP Snooping table.

IEEE 802.1D BRIDGE

The switch supports IEEE 802.1D transparent bridging. The address table facilitates data switching by learning addresses, and then filtering or forwarding traffic based on this information. The address table supports up to 32K addresses.

STORE-AND-FORWARD SWITCHING

The switch copies each frame into its memory before forwarding them to another port. This ensures that all frames are a standard Ethernet size and have been verified for accuracy with the cyclic redundancy check (CRC). This prevents bad frames from entering the network and wasting bandwidth.

To avoid dropping frames on congested ports, the switch provides 3 Mbits for frame buffering. This buffer can queue packets awaiting transmission on congested networks.

SPANNING TREE ALGORITHM

The switch supports these spanning tree protocols:

- Spanning Tree Protocol (STP, IEEE 802.1D) – This protocol provides loop detection. When there are multiple physical paths between segments, this protocol will choose a single path and disable all others to ensure that only one route exists between any two stations on the network. This prevents the creation of network loops. However, if the chosen path should fail for any reason, an alternate path will be activated to maintain the connection.

- Rapid Spanning Tree Protocol (RSTP, IEEE 802.1w) – This protocol reduces the convergence time for network topology changes to about 3 to 5 seconds, compared to 30 seconds or more for the older IEEE 802.1D STP standard. It is intended as a complete replacement for STP, but can still interoperate with switches running the older standard by automatically reconfiguring ports to STP-compliant mode if they detect STP protocol messages from attached devices.

- Multiple Spanning Tree Protocol (MSTP, IEEE 802.1s) – This protocol is a direct extension of RSTP. It can provide an independent spanning tree for different VLANs. It simplifies network management, provides for even faster convergence than RSTP by limiting the size of each region, and prevents VLAN members from being segmented from the rest of the group (as sometimes occurs with IEEE 802.1D STP).

CONNECTIVITY FAULT MANAGEMENT

The switch provides connectivity fault monitoring for end-to-end connections within a designated service area by using continuity check messages which can detect faults in maintenance points, fault verification through loop back messages, and fault isolation with link trace messages.

VIRTUAL LANS

The switch supports up to 4094 VLANs. A Virtual LAN is a collection of network nodes that share the same collision domain regardless of their physical location or connection point in the network. The switch supports tagged VLANs based on the IEEE 802.1Q standard. Members of VLAN groups can be dynamically learned via GVRP, or ports can be manually assigned to a specific set of VLANs. This allows the switch to restrict traffic to the VLAN groups to which a user has been assigned. By segmenting your network into VLANs, you can:

- Eliminate broadcast storms which severely degrade performance in a flat network.
- Simplify network management for node changes/moves by remotely configuring VLAN membership for any port, rather than having to manually change the network connection.
- Provide data security by restricting all traffic to the originating VLAN, except where a connection is explicitly defined via the switch's routing service.
- Use private VLANs to restrict traffic to pass only between data ports and the uplink ports, thereby isolating adjacent ports within the same VLAN, and allowing you to limit the total number of VLANs that need to be configured.
- Use protocol VLANs to restrict traffic to specified interfaces based on protocol type.

IEEE 802.1Q TUNNELING (QINQ)

This feature is designed for service providers carrying traffic for multiple customers across their networks. QinQ tunneling is used to maintain customer-specific VLAN and Layer 2 protocol configurations even when different customers use the same internal VLAN IDs. This is accomplished by inserting Service Provider VLAN (SPVLAN) tags into the customer’s frames when they enter the service provider’s network, and then stripping the tags when the frames leave the network.

TRAFFIC PRIORITIZATION

This switch prioritizes each packet based on the required level of service, using eight priority queues with strict priority, Weighted Round Robin (WRR), or a combination of strict and weighted queuing. It uses IEEE 802.1p and 802.1Q tags to prioritize incoming traffic based on input from the end-station application. These functions can be used to provide independent priorities for delay-sensitive data and best-effort data.

This switch also supports several common methods of prioritizing layer 3/4 traffic to meet application requirements. Traffic can be prioritized based on the priority bits in the IP frame's Type of Service (ToS) octet using DSCP, or IP Precedence or TCP/UDP port numbers. When these services are enabled, the priorities are mapped to a Class of Service value by the switch, and the traffic then sent to the corresponding output queue.

QUALITY OF SERVICE

Differentiated Services (DiffServ) provides policy-based management mechanisms used for prioritizing network resources to meet the requirements of specific traffic types on a per-hop basis. Each packet is classified upon entry into the network based on access lists, IP Precedence or DSCP values, or VLAN lists. Using access lists allows you select traffic based on Layer 2, Layer 3, or Layer 4 information contained in each packet. Based on network policies, different kinds of traffic can be marked for different kinds of forwarding.

ETHERNET RING PROTECTION SWITCHING

ERPS can be used to increase the availability and robustness of Ethernet rings, such as those used in Metropolitan Area Networks (MAN). ERPS provides Layer 2 loop avoidance and fast reconvergence in Layer 2 ring topologies, supporting up to 255 nodes in the ring structure. It can also function with IEEE 802.1ag to support link monitoring when non-participating devices exist within the Ethernet ring.

OPERATION, ADMINISTRATION, AND MAINTENANCE

The switch provides OAM remote management tools required to monitor and maintain the links to subscriber CPEs (Customer Premise Equipment). This section describes functions including enabling OAM for selected ports, loopback testing, and displaying remote device information.

IP ROUTING

The switch provides Layer 3 IP routing. To maintain a high rate of throughput, the switch forwards all traffic passing within the same segment, and routes only traffic that passes between different subnetworks. The wire-speed routing provided by this switch lets you easily link network segments or VLANs together without having to deal with the bottlenecks or configuration hassles normally associated with conventional routers.

Routing for unicast traffic is supported with static routing, Routing Information Protocol (RIP), Open Shortest Path First (OSPF) protocol, and Border Gateway Protocol (BGP).

Static Routing – Traffic is automatically routed between any IP interfaces configured on the ECN430-switch. Routing to statically configured hosts or subnet addresses is provided based on next-hop entries specified in the static routing table.

RIP – This protocol uses a distance-vector approach to routing. Routes are determined on the basis of minimizing the distance vector, or hop count, which serves as a rough estimate of transmission cost.

OSPF – This approach uses a link state routing protocol to generate a shortest-path tree, then builds up its routing table based on this tree. OSPF produces a more stable network because the participating routers act on network changes predictably and simultaneously, converging on the best route more quickly than RIP.

BGP – This protocol uses a path vector approach to connect autonomous systems (AS) on the Internet. BGP maintains a table of IP network prefixes which designate network reachability among autonomous systems based the path of ASs to the destination, and next hop information. It makes routing decisions based on path, network policies and/or rule sets. For this reason, it is more appropriately termed a reachability protocol rather than a routing protocol.

Policy-based Routing for BGP – The next-hop behavior for ingress IP traffic can be determined based on matching criteria.

EQUAL-COST MULTIPATH LOAD BALANCING

When multiple paths to the same destination and with the same path cost are found in the routing table, the Equal-cost Multipath (ECMP) algorithm first checks if the cost is lower than that of any other routing entries. If the cost is the lowest in the table, the switch will use up to eight paths having the lowest path cost to balance traffic forwarded to the destination. ECMP uses either equal-cost unicast multipaths manually configured in the static routing table, or equal-cost multipaths dynamically detected by the Open Shortest Path Algorithm (OSPF). In other words, it uses either static or unicast routing entries, not both.

ROUTER REDUNDANCY

The Virtual Router Redundancy Protocol (VRRP) uses a virtual IP address to support a primary router and multiple backup routers. The backups can be configured to take over the workload if the master fails or to load share the traffic. The primary goal of this protocol is to allow a host device which has been configured with a fixed gateway to maintain network connectivity in case the primary gateway goes down.

ADDRESS RESOLUTION PROTOCOL

The switch uses ARP and Proxy ARP to convert between IP addresses and MAC (hardware) addresses. This switch supports conventional ARP, which locates the MAC address corresponding to a given IP address. This allows the switch to use IP addresses for routing decisions and the corresponding MAC addresses to forward packets from one hop to the next. Either static or dynamic entries can be configured in the ARP cache.

Proxy ARP allows hosts that do not support routing to determine the MAC address of a device on another network or subnet. When a host sends an ARP request for a remote network, the switch checks to see if it has the best route. If it does, it sends its own MAC address to the host. The host then sends traffic for the remote destination via the switch, which uses its own routing table to reach the destination on the other network.

MULTICAST FILTERING

Specific multicast traffic can be assigned to its own VLAN to ensure that it does not interfere with normal network traffic and to guarantee real-time delivery by setting the required priority level for the designated VLAN. The switch uses IGMP Snooping and Query for IPv4, MLD Snooping and Query for IPv6, and IGMP at Layer 3 to manage multicast group registration. It also supports Multicast VLAN Registration (MVR for IPv4 and MVR6 for IPv6) which allows common multicast traffic, such as television channels, to be transmitted across a single network-wide multicast VLAN shared by hosts residing in other standard or private VLAN groups, while preserving security and data isolation for normal traffic.

LINK LAYER DISCOVERY PROTOCOL

LLDP is used to discover basic information about neighboring devices within the local broadcast domain. LLDP is a Layer 2 protocol that advertises information about the sending device and collects information gathered from neighboring network nodes it discovers.

Advertised information is represented in Type Length Value (TLV) format according to the IEEE 802.1ab standard, and can include details such as device identification, capabilities and configuration settings. Media Endpoint Discovery (LLDP-MED) is an extension of LLDP intended for managing endpoint devices such as Voice over IP phones and network switches. The LLDP-MED TLVs advertise information such as network policy, power, inventory, and device location details. The LLDP and LLDP-MED information can be used by SNMP applications to simplify troubleshooting, enhance network management, and maintain an accurate network topology.

MULTICAST ROUTING

Routing for multicast packets is supported by the Protocol-Independent Multicasting - Dense Mode and Sparse Mode (PIM-DM, PIM-SM, PIM6-DM, PIM6-SM) protocols. These protocols work in conjunction with IGMP to filter and route multicast traffic. PIM is a very simple protocol that uses the routing table of the unicast routing protocol enabled on an interface. Dense Mode is designed for areas where the probability of multicast clients is relatively high, and the overhead of frequent flooding is justified. While Sparse mode is designed for network areas, such as the Wide Area Network, where the probability of multicast clients is low.

SYSTEM DEFAULTS

The switch's system defaults are provided in the configuration file "Factory_Default_Config.cfg." To reset the switch defaults, this file should be set as the startup configuration file.

The following table lists some of the basic system defaults.

Table 2: System Defaults

Function	Parameter	Default
Console Port Connection	Baud Rate	115200 bps
	Data bits	8
	Stop bits	1
	Parity	none
	Local Console Timeout	0 (disabled)
Authentication and Security Measures	Privileged Exec Level	Username "admin" Password "admin"
	Normal Exec Level	Username "guest" Password "guest"
	Enable Privileged Exec from Normal Exec Level	Password "super"
	RADIUS Authentication	Disabled
	TACACS+ Authentication	Disabled
	802.1X Port Authentication	Disabled
	MAC Authentication	Disabled
	PPPoE Intermediate Agent	Disabled
	HTTPS	Enabled
	SSH	Disabled
	Port Security	Disabled
	IP Filtering	Disabled
	DHCP Snooping	Disabled
Web Management	HTTP Server	Enabled
	HTTP Port Number	80
	HTTP Secure Server	Enabled
	HTTP Secure Server Port	443
SNMP	SNMP Agent	Enabled
	Community Strings	"public" (read only) "private" (read/write)
	Traps	Authentication traps: enabled Link-up-down events: enabled
	SNMP V3	View: defaultview Group: public (read only); private (read/write)

Table 2: System Defaults (Continued)

Function	Parameter	Default
Port Configuration	Admin Status	Enabled
	Auto-negotiation	Enabled
	Flow Control	Disabled
Port Trunking	Static Trunks	None
	LACP (all ports)	Disabled
Congestion Control	Rate Limiting	Disabled
	Storm Control	Broadcast: Enabled (500 packets/sec) Multicast: Disabled Unknown Unicast: Disabled
OAM	Status	Disabled
Address Table	Aging Time	300 seconds
Spanning Tree Algorithm	Status	Enabled, RSTP (Defaults: RSTP standard)
	Edge Ports	Disabled
ERPS	Status	Disabled
LLDP	Status	Enabled
Virtual LANs	Default VLAN	1
	PVID	1
	Acceptable Frame Type	All
	Ingress Filtering	Disabled
	Switchport Mode (Egress Mode)	Hybrid
	GVRP (global)	Disabled
	GVRP (port interface)	Disabled
	QinQ Tunneling	Disabled
Traffic Prioritization	Ingress Port Priority	0
	Queue Mode	WRR
	Queue Weight	Queue: 0 1 2 3 4 5 6 7 Weight: 1 2 4 6 8 10 12 14
	Class of Service	Enabled
	IP Precedence Priority	Disabled
	IP DSCP Priority	Disabled
	IP Port Priority	Disabled

Table 2: System Defaults (Continued)

Function	Parameter	Default
IP Settings	Management. VLAN	VLAN 1
	IP Address	DHCP assigned
	Subnet Mask	255.255.255.0
	Default Gateway	0.0.0.0
	DHCP	Client: Enabled
	DNS	Client/Proxy service: Disabled
	BOOTP	Disabled
	ARP	Enabled Cache Timeout: 20 minutes Proxy: Disabled
Unicast Routing	RIP	Disabled
	OSPF	Disabled
	OSPFv3	Disabled
	BGPv4	Disabled
Multicast Routing	PIMv4	Disabled
	PIMv6	Disabled
Router Redundancy	VRRP	Disabled
Multicast Filtering	IGMP Snooping (Layer 2)	Snooping: Enabled Querier: Disabled
	MLD Snooping (Layer 2 IPv6)	Snooping: Enabled Querier: Disabled
	Multicast VLAN Registration	Disabled
	IGMP Proxy Reporting	Enabled
	IGMP (Layer 3) IGMP Proxy (Layer 3)	Disabled Disabled
System Log	Status	Enabled
	Messages Logged to RAM	Levels 0-7 (all)
	Messages Logged to Flash	Levels 0-3
SMTP Email Alerts	Event Handler	Enabled (but no server defined)
SNTP	Clock Synchronization	Disabled
Switch Clustering	Status	Disabled
	Commander	Disabled

2 INITIAL SWITCH CONFIGURATION

This chapter includes information on connecting to the switch and basic configuration procedures.

CONNECTING TO THE SWITCH

The switch includes a built-in network management agent. The agent offers a variety of management options, including SNMP, RMON and a web-based interface. A PC may also be connected directly to the switch for configuration and monitoring via a command line interface (CLI).

NOTE: An IPv4 address for this switch is obtained via DHCP by default. To change this address, see "Setting an IP Address" on page 109.

CONFIGURATION OPTIONS

The switch's HTTP web agent allows you to configure switch parameters, monitor port connections, and display statistics using a standard web browser such as Internet Explorer 6, Mozilla Firefox 4, or Google Chrome 29, or more recent versions. The switch's web management interface can be accessed from any computer attached to the network.

The CLI program can be accessed by a direct connection to the RS-232 serial console port on the switch, or remotely by a Telnet connection over the network.

The switch's management agent also supports SNMP (Simple Network Management Protocol). This SNMP agent permits the switch to be managed from any system in the network using network management software.

The switch's web interface, console interface, and SNMP agent allow you to perform the following management functions:

- Set user names and passwords
- Set an IP interface for any VLAN
- Configure SNMP parameters
- Enable/disable any port
- Configure the bandwidth of any port by limiting input or output rates

- Control port access through IEEE 802.1X security or static address filtering
- Filter packets using Access Control Lists (ACLs)
- Configure up to 4094 IEEE 802.1Q VLANs
- Enable GVRP automatic VLAN registration
- Configure IP routing for unicast or multicast traffic
- Configure router redundancy
- Configure IGMP multicast filtering
- Upload and download system firmware or configuration files via HTTP (using the web interface) or FTP/TFTP (using the command line or web interface)
- Configure Spanning Tree parameters
- Configure Class of Service (CoS) priority queuing
- Configure static or LACP trunks (up to 8)
- Enable port mirroring
- Set storm control on any port for excessive broadcast, multicast, or unknown unicast traffic
- Display system information and statistics

REQUIRED CONNECTIONS

The switch provides an RS-232 serial port that enables a connection to a PC or terminal for monitoring and configuring the switch. A null-modem console cable is provided with the switch.

Attach a VT100-compatible terminal, or a PC running a terminal emulation program to the switch. You can use the console cable provided with this package, or use a null-modem cable that complies with the wiring assignments shown in the Installation Guide.

To connect a terminal to the console port, complete the following steps:

1. Connect the console cable to the serial port on a terminal, or a PC running terminal emulation software, and tighten the captive retaining screws on the DB-9 connector.
2. Connect the other end of the cable to the RS-232 serial port on the switch.

3. Make sure the terminal emulation software is set as follows:

   - Select the appropriate serial port (COM port 1 or COM port 2).
   - Set the baud rate to 115200 bps.
   - Set the data format to 8 data bits, 1 stop bit, and no parity.
   - Set flow control to none.
   - Set the emulation mode to VT100.
   - When using HyperTerminal, select Terminal keys, not Windows keys.

NOTE: Once you have set up the terminal correctly, the console login screen will be displayed.

For a description of how to use the CLI, see "Using the Command Line Interface" on page 869. For a list of all the CLI commands and detailed information on using the CLI, refer to "CLI Command Groups" on page 879.

REMOTE CONNECTIONS

Prior to accessing the switch's onboard agent via a network connection, you must first configure it with a valid IP address, subnet mask, and default gateway using a console connection, or DHCP protocol.

An IPv4 address for this switch is obtained via DHCP by default. To manually configure this address or enable dynamic address assignment via DHCP, see "Setting an IP Address" on page 109.

NOTE: This switch supports four Telnet sessions or four SSH sessions.

After configuring the switch's IP parameters, you can access the onboard configuration program from anywhere within the attached network. The onboard configuration program can be accessed using Telnet from any computer attached to the network. The switch can also be managed by any computer using a web browser (Internet Explorer 6, Mozilla Firefox 4, or Google Chrome 29, or more recent versions), or from a network computer using SNMP network management software.

The onboard program only provides access to basic configuration functions. To access the full range of SNMP management functions, you must use SNMP-based network management software.

NOTE: The switch also includes a Craft port on the front panel which provides a secure management connection that is isolated from all other ports on the switch. This interface is not configured with an IP address by default, but may be manually configured with an IPv4 or IPv6 address as described in the following sections. The Craft port can only be configured through the command line interface, and is specified with the name “craft” in the commands used to configure its IP address.

BASIC CONFIGURATION

CONSOLE CONNECTION

The CLI program provides two different command levels — normal access level (Normal Exec) and privileged access level (Privileged Exec). The commands available at the Normal Exec level are a limited subset of those available at the Privileged Exec level and allow you to only display information and use basic utilities. To fully configure the switch parameters, you must access the CLI at the Privileged Exec level.

Access to both CLI levels are controlled by user names and passwords. The switch has a default user name and password for each level. To log into the CLI at the Privileged Exec level using the default user name and password, perform these steps:

1. To initiate your console connection, press <Enter>. The “User Access Verification” procedure starts.

2. At the User Name prompt, enter “admin.”

3. At the Password prompt, also enter “admin.” (The password characters are not displayed on the console screen.)

4. The session is opened and the CLI displays the “Console#” prompt indicating you have access at the Privileged Exec level.

SETTING PASSWORDS

If this is your first time to log into the CLI program, you should define new passwords for both default user names using the “username” command, record them and put them in a safe place.

Passwords can consist of up to 32 alphanumeric characters and are case sensitive. To prevent unauthorized access to the switch, set the passwords as follows:

1. Open the console interface with the default user name and password “admin” to access the Privileged Exec level.

2. Type “configure” and press <Enter>.

3. Type “username guest password 0 *password*,” for the Normal Exec level, where *password* is your new password. Press <Enter>.

4. Type “username admin password 0 *password*,” for the Privileged Exec level, where *password* is your new password. Press <Enter>.

```
Username: admin
Password:

 CLI session with the ECS4660-28F is opened.
 To end the CLI session, enter [Exit].

Console#configure
Console(config)#username guest password 0 [password]
Console(config)#username admin password 0 [password]
Console(config)#
```

SETTING AN IP ADDRESS

You must establish IP address information for the switch to obtain management access through the network. This can be done in either of the following ways:

- **Manual** — You have to input the information, including IP address and subnet mask. If your management station is not in the same IP subnet as the switch, you will also need to specify the default gateway router.
- **Dynamic** — The switch can send IPv4 configuration requests to BOOTP or DHCP address allocation servers on the network, or can automatically generate a unique IPv6 host address based on the local subnet address prefix received in router advertisement messages. An IPv6 link local address for use in a local network can also be dynamically generated as described in "Obtaining an IPv6 Address" on page 114.

  The current software does not support DHCP for IPv6, so an IPv6 global unicast address for use in a network containing more than one subnet can only be manually configured as described in "Assigning an IPv6 Address" on page 110.

MANUAL CONFIGURATION

You can manually assign an IP address to the switch. You may also need to specify a default gateway that resides between this device and management stations that exist on another network segment. Valid IPv4 addresses consist of four decimal numbers, 0 to 255, separated by periods. Anything outside this format will not be accepted by the CLI program.

NOTE: The IPv4 address for VLAN 1 is obtained via DHCP by default.

Assigning an IPv4 Address

Before you can assign an IP address to the switch, you must obtain the following information from your network administrator:

- IP address for the switch
- Network mask for this network
- Default gateway for the network

To assign an IPv4 address to the switch, complete the following steps

1. From the Global Configuration mode prompt, type "interface vlan 1" to access the interface-configuration mode. Press <Enter>.
2. Type "ip address *ip-address netmask*," where "ip-address" is the switch IP address and "netmask" is the network mask for the network. Press <Enter>.
3. Type "exit" to return to the global configuration mode prompt. Press <Enter>.
4. To set the IP address of the default gateway for the network to which the switch belongs, type "ip default-gateway *gateway*," where "gateway" is the IP address of the default gateway. Press <Enter>.

```
Console(config)#interface vlan 1
Console(config-if)#ip address 192.168.1.5 255.255.255.0
Console(config-if)#exit
Console(config)#ip default-gateway 192.168.1.254
```

Assigning an IPv6 Address

This section describes how to configure a "link local" address for connectivity within the local subnet only, and also how to configure a "global unicast" address, including a network prefix for use on a multi-segment network and the host portion of the address.

An IPv6 prefix or address must be formatted according to RFC 2373 "IPv6 Addressing Architecture," using 8 colon-separated 16-bit hexadecimal values. One double colon may be used to indicate the appropriate number of zeros required to fill the undefined fields. For detailed information on the other ways to assign IPv6 addresses, see "Setting the Switch's IP Address (IP Version 6)" on page 695.

Link Local Address — All link-local addresses must be configured with a prefix in the range of FE80~FEBF. Remember that this address type makes the switch accessible over IPv6 for all devices attached to the same local subnet only. Also, if the switch detects that the address you configured conflicts with that in use by another device on the subnet, it will stop using the address in question, and automatically generate a link local address that does not conflict with any other devices on the local subnet.

To configure an IPv6 link local address for the switch, complete the following steps:

1. From the Global Configuration mode prompt, type “interface vlan 1” to access the interface-configuration mode. Press <Enter>.

2. Type “ipv6 address” followed by up to 8 colon-separated 16-bit hexadecimal values for the *ipv6-address* similar to that shown in the example, followed by the “link-local” command parameter. Then press <Enter>.

```
Console(config)#interface vlan 1
Console(config-if)#ipv6 address FE80::260:3EFF:FE11:6700 link-local
Console(config-if)#ipv6 enable
Console(config-if)#end
Console#show ipv6 interface
VLAN 1 is up
IPv6 is enabled
Link-local address:
  FE80::260:3EFF:FE11:6700/64
Global unicast address(es):
(None)
Joined group address(es):
FF02::1:FF11:6700
FF02::1
IPv6 link MTU is 1500 bytes
ND DAD is enabled, number of DAD attempts: 3.
ND retransmit interval is 1000 milliseconds
ND advertised retransmit interval is 0 milliseconds
ND reachable time is 30000 milliseconds
ND advertised reachable time is 0 milliseconds

Console#
```

Address for Multi-segment Network — Before you can assign an IPv6 address to the switch that will be used to connect to a multi-segment network, you must obtain the following information from your network administrator:

- Prefix for this network
- IP address for the switch
- Default gateway for the network

For networks that encompass several different subnets, you must define the full address, including a network prefix and the host address for the switch. You can specify either the full IPv6 address, or the IPv6 address and prefix length. The prefix length for an IPv6 network is the number of bits (from the left) of the prefix that form the network address, and is expressed as a decimal number. For example, all IPv6 addresses that start with the first byte of 73 (hexadecimal) could be expressed as 73:0:0:0:0:0:0:0/8 or 73::/8.

To generate an IPv6 global unicast address for the switch, complete the following steps:

1. From the global configuration mode prompt, type “interface vlan 1” to access the interface-configuration mode. Press <Enter>.

2. From the interface prompt, type “ipv6 address *ipv6-address*” or “ipv6 address *ipv6-address/prefix-length*,” where “prefix-length” indicates the address bits used to form the network portion of the address. (The network address starts from the left of the prefix and should encompass some of the ipv6-address bits.) The remaining bits are assigned to the host interface. Press <Enter>.

3. Type “exit” to return to the global configuration mode prompt. Press <Enter>.

4. To set the IP address of the IPv6 default gateway for the network to which the switch belongs, type “ipv6 default-gateway *gateway*,” where “gateway” is the IPv6 address of the default gateway. Press <Enter>.

```
Console(config)#interface vlan 1
Console(config-if)#ipv6 address 2001:DB8:2222:7272::/64
Console(config-if)#exit
Console(config)#ipv6 default-gateway 2001:DB8:2222:7272::254
Console(config)end
Console#show ipv6 interface
VLAN 1 is up
IPv6 is enabled
Link-local address:
  FE80::260:3EFF:FE11:6700/64
Global unicast address(es):
  2001:DB8:2222:7272::/64, subnet is 2001:DB8:2222:7272::/64
Joined group address(es):
ff02::2
ff02::1:ff00:0
ff02::1:ff00:fd
ff02::1:2
ff02::1
IPv6 link MTU is 1500 bytes
ND DAD is enabled, number of DAD attempts: 3.
ND retransmit interval is 1000 milliseconds
ND advertised retransmit interval is 0 milliseconds
ND reachable time is 30000 milliseconds
ND advertised reachable time is 0 milliseconds
ND advertised router lifetime is 1800 seconds

Console#show ipv6 route
Codes: C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
      i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default

S*     ::/0 [1/0] via 2001:db8:2222:7272::254, VLAN1
C      2001:db8:2222:7272::/64, VLAN1
C      fe80::/64, VLAN1

Console#
```

DYNAMIC CONFIGURATION

Obtaining an IPv4 Address

If you select the “bootp” or “dhcp” option, the system will immediately start broadcasting service requests. IP will be enabled but will not function until a BOOTP or DHCP reply has been received. Requests are broadcast every few minutes using exponential backoff until IP configuration information is obtained from a BOOTP or DHCP server. BOOTP and DHCP values can include the IP address, subnet mask, and default gateway. If the DHCP/BOOTP server is slow to respond, you may need to use the “ip dhcp restart client” command to re-start broadcasting service requests.

Note that the “ip dhcp restart client” command can also be used to start broadcasting service requests for all VLANs configured to obtain address assignments through BOOTP or DHCP. It may be necessary to use this command when DHCP is configured on a VLAN, and the member ports which were previously shut down are now enabled.

If the “bootp” or “dhcp” option is saved to the startup-config file (step 6), then the switch will start broadcasting service requests as soon as it is powered on.

To automatically configure the switch by communicating with BOOTP or DHCP address allocation servers on the network, complete the following steps:

1. From the Global Configuration mode prompt, type “interface vlan 1” to access the interface-configuration mode. Press <Enter>.

2. At the interface-configuration mode prompt, use one of the following commands:

   - To obtain IP settings via DHCP, type “ip address dhcp” and press <Enter>.

   - To obtain IP settings via BOOTP, type “ip address bootp” and press <Enter>.

3. Type “end” to return to the Privileged Exec mode. Press <Enter>.

4. Wait a few minutes, and then check the IP configuration settings by typing the “show ip interface” command. Press <Enter>.

5. Then save your configuration changes by typing "copy running-config startup-config." Enter the startup file name and press <Enter>.

```
Console(config)#interface vlan 1
Console(config-if)#ip address dhcp
Console(config-if)#end
Console#show ip interface
VLAN 1 is Administrative Up - Link Up
  Address is 00-E0-0C-00-00-FB
  Index: 1001, MTU: 1500
  Address Mode is DHCP
  IP Address: 192.168.0.2 Mask: 255.255.255.0
  Proxy ARP is disabled
Console#copy running-config startup-config
Startup configuration file name []: startup
\Write to FLASH Programming.
\Write to FLASH finish.
Success.
```

OBTAINING AN IPV6 ADDRESS

Link Local Address — There are several ways to configure IPv6 addresses. The simplest method is to automatically generate a "link local" address (identified by an address prefix of FE80). This address type makes the switch accessible over IPv6 for all devices attached to the same local subnet.

To generate an IPv6 link local address for the switch, complete the following steps:

1. From the Global Configuration mode prompt, type "interface vlan 1" to access the interface-configuration mode. Press <Enter>.

2. Type "ipv6 enable" and press <Enter>.

```
Console(config)#interface vlan 1
Console(config-if)#ipv6 enable
Console(config-if)#end
Console#show ipv6 interface
VLAN 1 is up
IPv6 is enabled
Link-local address:
  FE80::260:3EFF:FE11:6700/64
Global unicast address(es):
  2001:DB8:2222:7272::/64, subnet is 2001:DB8:2222:7272::/64
Joined group address(es):
ff02::2
ff02::1:ff00:0
ff02::1:ff00:fd
ff02::1:2
ff02::1
IPv6 link MTU is 1500 bytes
ND DAD is enabled, number of DAD attempts: 3.
ND retransmit interval is 1000 milliseconds
ND advertised retransmit interval is 0 milliseconds
ND reachable time is 30000 milliseconds
ND advertised reachable time is 0 milliseconds
ND advertised router lifetime is 1800 seconds
Console#
```

DOWNLOADING A CONFIGURATION FILE REFERENCED BY A DHCP SERVER

Information passed on to the switch from a DHCP server may also include a configuration file to be downloaded and the TFTP servers where that file can be accessed. If the Factory Default Configuration file is used to provision the switch at startup, in addition to requesting IP configuration settings from the DHCP server, it will also ask for the name of a bootup configuration file and TFTP servers where that file is stored.

If the switch receives information that allows it to download the remote bootup file, it will save this file to a local buffer, and then restart the provision process.

Note the following DHCP client behavior:

- The bootup configuration file received from a TFTP server is stored on the switch with the original file name. If this file name already exists in the switch, the file is overwritten.
- If the name of the bootup configuration file is the same as the Factory Default Configuration file, the download procedure will be terminated, and the switch will not send any further DHCP client requests.
- If the switch fails to download the bootup configuration file based on information passed by the DHCP server, it will not send any further DHCP client requests.
- If the switch does not receive a DHCP response prior to completing the bootup process, it will continue to send a DHCP client request once a minute. These requests will only be terminated if the switch's address is manually configured, but will resume if the address mode is set back to DHCP.

To successfully transmit a bootup configuration file to the switch the DHCP daemon (using a Linux based system for this example) must be configured with the following information:

- Options 60, 66 and 67 statements can be added to the daemon's configuration file.

Table 3: Options 60, 66 and 67 Statements

Option	Statement	
	Keyword	**Parameter**
60	vendor-class-identifier	a string indicating the vendor class identifier
66	tftp-server-name	a string indicating the tftp server name
67	bootfile-name	a string indicating the bootfile name

- By default, DHCP option 66/67 parameters are not carried in a DHCP server reply. To ask for a DHCP reply with option 66/67 information, the DHCP client request sent by this switch includes a "parameter request list" asking for this information. Besides, the client request also includes a "vendor class identifier" that allows the DHCP server to identify the device, and select the appropriate configuration file for download. This information is included in Option 55 and 124.

Table 4: Options 55 and 124 Statements

Option	Statement	
	Keyword	Parameter
55	dhcp-parameter-request-list	a list of parameters, separated by ','
124	vendor-class-identifier	a string indicating the vendor class identifier

The following configuration examples are provided for a Linux-based DHCP daemon (dhcpd.conf file). In the "Vendor class" section, the server will always send Option 66 and 67 to tell the switch to download the "test" configuration file from server 192.168.255.101.

```
ddns-update-style ad-hoc;

default-lease-time 600;
max-lease-time 7200;

log-facility local7;

server-name "Server1";
Server-identifier 192.168.255.250;
#option 66, 67
 option space dynamicProvision code width 1 length 1 hash size 2;
 option dynamicProvision.tftp-server-name code 66 = text;
 option dynamicProvision.bootfile-name code 67 = text;

subnet 192.168.255.0 netmask 255.255.255.0 {
  range 192.168.255.160 192.168.255.200;
  option routers 192.168.255.101;
  option tftp-server-name "192.168.255.100"; #Default Option 66
  option bootfile-name "bootfile";           #Default Option 67
}

class "Option66,67_1" {               #DHCP Option 60 Vendor class
two
  match if option vendor-class-identifier = "ecs4660-28f.cfg";
  option tftp-server-name "192.168.255.101";
  option bootfile-name "test";
}
```

NOTE: Use "ecs4660-28f.cfg" for the vendor-class-identifier in the dhcpd.conf file.

ENABLING SNMP MANAGEMENT ACCESS

The switch can be configured to accept management commands from Simple Network Management Protocol (SNMP) applications such as Edge-Core ECView Pro. You can configure the switch to respond to SNMP requests or generate SNMP traps.

When SNMP management stations send requests to the switch (either to return information or to set a parameter), the switch provides the requested data or sets the specified parameter. The switch can also be configured to send information to SNMP managers (without being requested by the managers) through trap messages, which inform the manager that certain events have occurred.

The switch includes an SNMP agent that supports SNMP version 1, 2c, and 3 clients. To provide management access for version 1 or 2c clients, you must specify a community string. The switch provides a default MIB View (i.e., an SNMPv3 construct) for the default “public” community string that provides read access to the entire MIB tree, and a default view for the “private” community string that provides read/write access to the entire MIB tree. However, you may assign new views to version 1 or 2c community strings that suit your specific security requirements (see "Setting SNMPv3 Views" on page 486).

Community Strings (for SNMP version 1 and 2c clients)

Community strings are used to control management access to SNMP version 1 and 2c stations, as well as to authorize SNMP stations to receive trap messages from the switch. You therefore need to assign community strings to specified users, and set the access level.

The default strings are:

- **public** - with read-only access. Authorized management stations are only able to retrieve MIB objects.
- **private** - with read/write access. Authorized management stations are able to both retrieve and modify MIB objects.

To prevent unauthorized access to the switch from SNMP version 1 or 2c clients, it is recommended that you change the default community strings.

To configure a community string, complete the following steps:

1. From the Privileged Exec level global configuration mode prompt, type “snmp-server community *string mode*,” where “string” is the community access string and “mode” is **rw** (read/write) or **ro** (read only). Press <Enter>. (Note that the default mode is read only.)
2. To remove an existing string, simply type “no snmp-server community *string*,” where “string” is the community access string to remove. Press <Enter>.

```
Console(config)#snmp-server community admin rw
Console(config)#snmp-server community private
Console(config)#
```

Note: If you do not intend to support access to SNMP version 1 and 2c clients, we recommend that you delete both of the default community strings. If there are no community strings, then SNMP management access from SNMP v1 and v2c clients is disabled.

TRAP RECEIVERS

You can also specify SNMP stations that are to receive traps from the switch. To configure a trap receiver, use the “snmp-server host” command. From the Privileged Exec level global configuration mode prompt, type:

> “snmp-server host *host-address community-string*
> [version {1 | 2c | 3 {auth | noauth | priv}}]”

where “host-address” is the IP address for the trap receiver, “community-string” specifies access rights for a version 1/2c host, or is the user name of a version 3 host, “version” indicates the SNMP client version, and “auth | noauth | priv” means that authentication, no authentication, or authentication and privacy is used for v3 clients. Then press <Enter>. For a more detailed description of these parameters, see "snmp-server host" on page 1001. The following example creates a trap host for each type of SNMP client.

```
Console(config)#snmp-server host 10.1.19.23 batman
Console(config)#snmp-server host 10.1.19.98 robin version 2c
Console(config)#snmp-server host 10.1.19.34 barbie version 3 auth
Console(config)#
```

CONFIGURING ACCESS FOR SNMP VERSION 3 CLIENTS

To configure management access for SNMPv3 clients, you need to first create a view that defines the portions of MIB that the client can read or write, assign the view to a group, and then assign the user to a group. The following example creates one view called “mib-2” that includes the entire MIB-2 tree branch, and then another view that includes the IEEE 802.1d bridge MIB. It assigns these respective read and read/write views to a group call “r&d” and specifies group authentication via MD5 or SHA. In the last step, it assigns a v3 user to this group, indicating that MD5 will be used for authentication, provides the password “greenpeace” for authentication, and the password “einstien” for encryption.

```
Console(config)#snmp-server view mib-2 1.3.6.1.2.1 included
Console(config)#snmp-server view 802.1d 1.3.6.1.2.1.17 included
Console(config)#snmp-server group r&d v3 auth mib-2 802.1d
Console(config)#snmp-server user steve group r&d v3 auth md5 greenpeace priv
  des56 einstien
Console(config)#
```

For a more detailed explanation on how to configure the switch for access from SNMP v3 clients, refer to "Simple Network Management Protocol" on page 480, or refer to the specific CLI commands for SNMP starting on page 995.

MANAGING SYSTEM FILES

The switch’s flash memory supports three types of system files that can be managed by the CLI program, web interface, or SNMP. The switch’s file system allows files to be uploaded and downloaded, copied, deleted, and set as a start-up file.

The types of files are:

- **Configuration** — This file type stores system configuration information and is created when configuration settings are saved. Saved configuration files can be selected as a system start-up file or can be uploaded via FTP/TFTP to a server for backup. The file named “Factory_Default_Config.cfg” contains all the system default settings and cannot be deleted from the system. If the system is booted with the factory default settings, the switch will also create a file named “startup1.cfg” that contains system settings for switch initialization, including information about the unit identifier, and MAC address for the switch. The configuration settings from the factory defaults configuration file are copied to this file, which is then used to boot the switch. See "Saving or Restoring Configuration Settings" on page 119 for more information.

- **Operation Code** — System software that is executed after boot-up, also known as run-time code. This code runs the switch operations and provides the CLI and web management interfaces. See "Managing System Files" on page 155 for more information.

- **Diagnostic Code** — Software that is run during system boot-up, also known as POST (Power On Self-Test).

Due to the size limit of the flash memory, the switch supports only two operation code files. However, you can have as many diagnostic code files and configuration files as available flash memory space allows. The switch has a total of 32 Mbytes of flash memory for system files.

In the system flash memory, one file of each type must be set as the start-up file. During a system boot, the diagnostic and operation code files set as the start-up file are run, and then the start-up configuration file is loaded.

Note that configuration files should be downloaded using a file name that reflects the contents or usage of the file settings. If you download directly to the running-config, the system will reboot, and the settings will have to be copied from the running-config to a permanent file.

SAVING OR RESTORING CONFIGURATION SETTINGS

Configuration commands only modify the running configuration file and are not saved when the switch is rebooted. To save all your configuration changes in nonvolatile storage, you must copy the running configuration file to the start-up configuration file using the “copy” command.

New startup configuration files must have a name specified. File names on the switch are case-sensitive, can be from 1 to 31 characters, must not contain slashes (\ or /), and the leading letter of the file name must not be a period (.). (Valid characters: A-Z, a-z, 0-9, ".", "-", "_")

There can be more than one user-defined configuration file saved in the switch's flash memory, but only one is designated as the "startup" file that is loaded when the switch boots. The **copy running-config startup-config** command always sets the new file as the startup file. To select a previously saved configuration file, use the **boot system config:**<*filename*> command.

The maximum number of saved configuration files depends on available flash memory. The amount of available flash memory can be checked by using the **dir** command.

To save the current configuration settings, enter the following command:

1. From the Privileged Exec mode prompt, type "copy running-config startup-config" and press <Enter>.

2. Enter the name of the start-up file. Press <Enter>.

```
Console#copy running-config startup-config
Startup configuration file name []: startup
\Write to FLASH Programming.

\Write to FLASH finish.
Success.

Console#
```

To restore configuration settings from a backup server, enter the following command:

1. From the Privileged Exec mode prompt, type "copy tftp startup-config" and press <Enter>.

2. Enter the address of the TFTP server. Press <Enter>.

3. Enter the name of the startup file stored on the server. Press <Enter>.

4. Enter the name for the startup file on the switch. Press <Enter>.

```
Console#copy file startup-config
Console#copy tftp startup-config
TFTP server IP address: 192.168.0.4
Source configuration file name: startup-rd.cfg
Startup configuration file name [startup1.cfg]:

Success.
Console#
```

SECTION II

WEB CONFIGURATION

This section describes the basic switch features, along with a detailed description of how to configure each feature via a web browser.

This section includes these chapters:

- "Using the Web Interface" on page 123
- "Basic Management Tasks" on page 149
- "Interface Configuration" on page 181
- "VLAN Configuration" on page 225
- "Address Table Settings" on page 263
- "Spanning Tree Algorithm" on page 271
- "Congestion Control" on page 295
- "Class of Service" on page 305
- "Quality of Service" on page 325
- "VoIP Traffic Configuration" on page 341
- "Security Measures" on page 347
- "Basic Administration Protocols" on page 453
- "Multicast Filtering" on page 609
- "IP Configuration" on page 691
- "IP Services" on page 713
- "General IP Routing" on page 741
- "Configuring Router Redundancy" on page 759
- "Unicast Routing" on page 769

- "Multicast Routing" on page 825

3 USING THE WEB INTERFACE

This switch provides an embedded HTTP web agent. Using a web browser you can configure the switch and view statistics to monitor network activity. The web agent can be accessed by any computer on the network using a standard web browser (Internet Explorer 6, Mozilla Firefox 4, or Google Chrome 29, or more recent versions).

NOTE: You can also use the Command Line Interface (CLI) to manage the switch over a serial connection to the console port or via Telnet. For more information on using the CLI, refer to "Using the Command Line Interface" on page 869.

CONNECTING TO THE WEB INTERFACE

Prior to accessing the switch from a web browser, be sure you have first performed the following tasks:

1. Configure the switch with a valid IP address, subnet mask, and default gateway using an out-of-band serial connection, BOOTP or DHCP protocol. (See "Setting an IP Address" on page 109.)

2. Set user names and passwords using an out-of-band serial connection. Access to the web agent is controlled by the same user names and passwords as the onboard configuration program. (See "Setting Passwords" on page 108.)

3. After you enter a user name and password, you will have access to the system configuration program.

NOTE: You are allowed three attempts to enter the correct password; on the third failed attempt the current connection is terminated.

NOTE: If you log into the web interface as guest (Normal Exec level), you can view the configuration settings or change the guest password. If you log in as “admin” (Privileged Exec level), you can change the settings on any page.

NOTE: If the path between your management station and this switch does not pass through any device that uses the Spanning Tree Algorithm, then you can set the switch port attached to your management station to fast forwarding (i.e., enable Admin Edge Port) to improve the switch’s response time to management commands issued through the web interface. See "Configuring Interface Settings for STA" on page 282.

NOTE: Connection to the web interface is not supported for HTTPS using an IPv6 link local address.

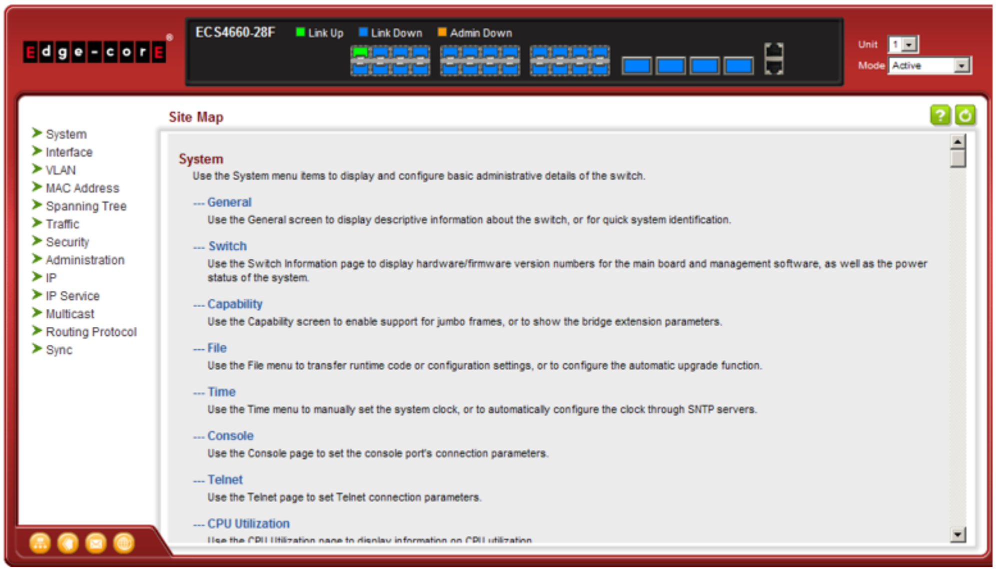
NAVIGATING THE WEB BROWSER INTERFACE

To access the web-browser interface you must first enter a user name and password. The administrator has Read/Write access to all configuration parameters and statistics. The default user name and password for the administrator is “admin.”

HOME PAGE

When your web browser connects with the switch’s web agent, the home page is displayed as shown below. The home page displays the Main Menu on the left side of the screen and System Information on the right side. The Main Menu links are used to navigate to other menus, and display configuration parameters and statistics.

Figure 1: Home Page



Site Map

System

Use the System menu items to display and configure basic administrative details of the switch.

--- General

Use the General screen to display descriptive information about the switch, or for quick system identification.

--- Switch

Use the Switch Information page to display hardware/firmware version numbers for the main board and management software, as well as the power status of the system.

--- Capability

Use the Capability screen to enable support for jumbo frames, or to show the bridge extension parameters.

--- File

Use the File menu to transfer runtime code or configuration settings, or to configure the automatic upgrade function.

--- Time

Use the Time menu to manually set the system clock, or to automatically configure the clock through SNTP servers.

--- Console

Use the Console page to set the console port's connection parameters.

--- Telnet

Use the Telnet page to set Telnet connection parameters.

--- CPU Utilization

Use the CPU Utilization page to display information on CPU utilization.

NOTE: You can open a connection to the vendor’s web site by clicking on the Edge-Core logo.

CONFIGURATION OPTIONS

Configurable parameters have a dialog box or a drop-down list. Once a configuration change has been made on a page, be sure to click on the Apply button to confirm the new setting. The following table summarizes the web page configuration buttons.

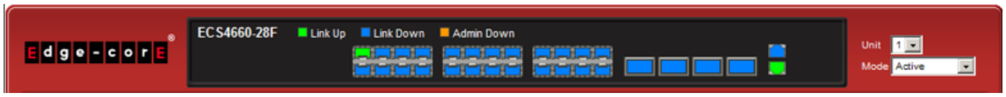
Table 5: Web Page Configuration Buttons

Button	Action
Apply	Sets specified values to the system.
Revert	Cancels specified values and restores current values prior to pressing "Apply."
?	Displays help for the selected page.
↻	Refreshes the current page.
🖧	Displays the site map.
◀	Logs out of the management interface.
✉	Sends mail to the vendor.
🌐	Links to the vendor's web site.

PANEL DISPLAY

The web agent displays an image of the switch's ports. The Mode can be set to display different information for the ports, including Active (i.e., up or down), Duplex (i.e., half or full duplex), or Flow Control (i.e., with or without flow control).

Figure 2: Front Panel Indicators



Unit 1
Mode Active

MAIN MENU

Using the onboard web agent, you can define system parameters, manage and control the switch, and all its ports, or monitor network conditions. The following table briefly describes the selections available from this program.

Table 6: Switch Main Menu

Menu	Description	Page
System		
General	Provides basic system description, including contact information	149
Switch	Shows the number of ports, hardware version, power status, and firmware version numbers	151
Capability	Enables support for jumbo frames; shows the bridge extension parameters	152, 153
File		155
Copy	Allows the transfer and copying files	155
Set Startup	Sets the startup file	158
Show	Shows the files stored in flash memory; allows deletion of files	159
Automatic Operation Code Upgrade	Automatically upgrades operation code if a newer version is found on the server	160
Time		164
Configure General		
Manual	Manually sets the current time	164
SNTP	Configures SNTP polling interval	165
NTP	Configures NTP authentication parameters	166
Configure Time Server	Configures a list of NTP or SNTP servers	167
Configure SNTP Server	Sets the IP address for SNTP time servers	167
Add NTP Server	Adds NTP time server and index of authentication key	168
Show NTP Server	Shows list of configured NTP time servers	168
Add NTP Authentication Key	Adds key index and corresponding MD5 key	169
Show NTP Authentication Key	Shows list of configured authentication keys	169
Configure Time Zone	Sets the local time zone for the system clock	171
Console	Sets console port connection parameters	172
Telnet	Sets Telnet connection parameters	174
CPU Utilization	Displays information on CPU utilization	175
Memory Status	Shows memory utilization parameters	176
Reset	Restarts the switch immediately, at a specified time, after a specified delay, or at a periodic interval	177
Interface		181
Port		182
General		
Configure by Port List	Configures connection settings per port	182
Configure by Port Range	Configures connection settings for a range of ports	184

Table 6: Switch Main Menu (Continued)

Menu	Description	Page
Show Information	Displays port connection status	185
Mirror		186
Add	Sets the source and target ports for mirroring	186
Show	Shows the configured mirror sessions	186
Statistics	Shows Interface, Etherlike, and RMON port statistics	192
Chart	Shows Interface, Etherlike, and RMON port statistics	192
History		196
Add	Configures a periodic sampling of statistics, specifying the sampling interval and number of samples	196
Show	Shows statistical history for the specified interface	196
Show Details	Shows detailed statistical history for the specified interface	196
Transceiver	Shows identifying information and operational parameters for optical transceivers which support Digital Diagnostic Monitoring (DDM), and configures thresholds for alarm and warning messages for optical transceivers which support DDM	200, 201
Trunk		
Static		205
Configure Trunk		205
Add	Creates a trunk, along with the first port member	205
Show	Shows the configured trunk identifiers	205
Add Member	Specifies ports to group into static trunks	205
Show Member	Shows the port members for the selected trunk	205
Configure General		205
Configure	Configures trunk connection settings	205
Show Information	Displays trunk connection settings	205
Dynamic		207
Configure Aggregator	Configures administration key and timeout for specific LACP groups	207
Configure Aggregation Port		205
Configure		205
General	Allows ports to dynamically join trunks	207
Actor	Configures parameters for link aggregation group members on the local side	207
Partner	Configures parameters for link aggregation group members on the remote side	207
Show Information		213
Counters	Displays statistics for LACP protocol messages	213
Internal	Displays configuration settings and operational state for the local side of a link aggregation	214
Neighbors	Displays configuration settings and operational state for the remote side of a link aggregation	216

Table 6: Switch Main Menu (Continued)

Menu	Description	Page
Configure Trunk		207
Configure	Configures connection settings	207
Show	Displays port connection status	207
Show Member	Shows the active members in a trunk	207
Statistics	Shows Interface, Etherlike, and RMON port statistics	192
Chart	Shows Interface, Etherlike, and RMON port statistics	192
Load Balance	Sets the load-distribution method among ports in aggregated links	217
History		196
Add	Configures a periodic sampling of statistics, specifying the sampling interval and number of samples	196
Show	Shows statistical history for the specified interface	196
RSPAN	Mirrors traffic from remote switches for analysis at a destination port on the local switch	188
Traffic Segmentation		219
Configure Global	Enables traffic segmentation globally	219
Configure Session	Configures the uplink and down-link ports for a segmented group of ports	220
Add	Assign the downlink and uplink ports to use in a segmented group	220
Show	Shows the assigned ports and direction (uplink/downlink)	220
VLAN Trunking	Allows unknown VLAN groups to pass through the specified interface	222
VLAN	Virtual LAN	225
Static		
Add	Creates VLAN groups	228
Show	Displays configured VLAN groups	228
Modify	Configures group name and administrative status	228
Edit Member by VLAN	Specifies VLAN attributes per VLAN	231
Edit Member by Interface	Specifies VLAN attributes per interface	231
Edit Member by Interface Range	Specifies VLAN attributes per interface range	231
Dynamic		
Configure General	Enables GVRP VLAN registration protocol globally	235
Configure Interface	Configures GVRP status and timers per interface	235
Show Dynamic VLAN		235
Show VLAN	Shows the VLANs this switch has joined through GVRP	235
Show VLAN Member	Shows the interfaces assigned to a VLAN through GVRP	235
Private		239
Configure VLAN		239
Add	Creates primary or community VLANs	239

Table 6: Switch Main Menu (Continued)

Menu	Description	Page
Show	Display configured primary and community VLANs	239
Add Community VLAN	Associates a community VLAN with a primary VLAN	240
Show Community VLAN	Shows the community VLANs associated with a primary VLAN	240
Configure Interface	Sets the private VLAN interface type, and associates the interfaces with a private VLAN	242
Tunnel	IEEE 802.1Q (QinQ) Tunneling	243
Configure Global	Sets tunnel mode for the switch	247
Configure Interface	Sets the tunnel mode for any participating interface	250
Protocol		251
Configure Protocol		252
Add	Creates a protocol group, specifying supported protocols	252
Show	Shows configured protocol groups	252
Configure Interface		253
Add	Maps a protocol group to a VLAN	253
Show	Shows the protocol groups mapped to each VLAN	253
IP Subnet		256
Add	Maps IP subnet traffic to a VLAN	256
Show	Shows IP subnet to VLAN mapping	256
MAC-Based		258
Add	Maps traffic with specified source MAC address to a VLAN	258
Show	Shows source MAC address to VLAN mapping	258
Translation		259
Add	Maps VLAN IDs between the customer and service provider	259
Show	Displays the configuration settings for VLAN translation	259
MAC Address		263
Learning Status	Enables MAC address learning on selected interfaces	263
Static		265
Add	Configures static entries in the address table	265
Show	Displays static entries in the address table	265
Dynamic		
Configure Aging	Sets timeout for dynamically learned entries	267
Show Dynamic MAC	Displays dynamic entries in the address table	268
Clear Dynamic MAC	Removes any learned entries from the forwarding database and clears the transmit and receive counts for any static or system configured entries	269
Spanning Tree		271
Loopback Detection	Configures Loopback Detection parameters	274

Table 6: Switch Main Menu (Continued)

Menu	Description	Page
STA	Spanning Tree Algorithm	
Configure Global		
Configure	Configures global bridge settings for STP, RSTP and MSTP	276
Show Information	Displays STA values used for the bridge	281
Configure Interface		
Configure	Configures interface settings for STA	282
Show Inform at on	Displays interface settings for STA	286
MSTP	Multiple Spanning Tree Algorithm	289
Configure Global		289
Add	Configures initial VLAN and priority for an MST instance	289
Show	Configures global settings for an MST instance	289
Modify	Configures the priority or an MST instance	289
Add Member	Adds VLAN members for an MST instance	289
Show Member	Adds or deletes VLAN members for an MST instance	289
Show Information	Displays MSTP values used for the bridge	
Configure Interface		293
Configure	Configures interface settings for an MST instance	293
Show Information	Displays interface settings for an MST instance	293
Traffic		
Rate Limit	Sets the input and output rate limits for a port	295
Storm Control	Sets the broadcast storm threshold for each interface	296
Auto Traffic Control	Sets thresholds for broadcast and multicast storms which can be used to trigger configured rate limits or to shut down a port	298
Configure Global	Sets the time to apply the control response after traffic has exceeded the upper threshold, and the time to release the control response after traffic has fallen beneath the lower threshold	300
Configure Interface	Sets the storm control mode (broadcast or multicast), the traffic thresholds, the control response, to automatically release a response of rate limiting, or to send related SNMP trap messages	301
Priority		
Default Priority	Sets the default priority for each port or trunk	305
Queue	Sets queue mode for the switch; sets the service weight for each queue that will use a weighted or hybrid mode	306
Trust Mode	Selects DSCP or CoS priority processing	312
DSCP to DSCP		314
Add	Maps DSCP values in incoming packets to per-hop behavior and drop precedence values for internal priority processing	314
Show	Shows the DSCP to DSCP mapping list	314
CoS to DSCP		316
Configure	Maps CoS/CFI values in incoming packets to per-hop behavior and drop precedence values for priority processing	316

Table 6: Switch Main Menu (Continued)

Menu	Description	Page
Show	Shows the CoS to DSCP mapping list	316
DSCP to CoS		318
Add	Maps internal per-hop behavior and drop precedence value pairs to CoS values used in tagged egress packets on a Layer 2 interface	318
Show	Shows the DSCP to CoS mapping list	318
IP Precedence to DSCP		320
Add	Maps IP precedence values in incoming packets to per-hop behavior and drop precedence values for priority processing	320
Show	Shows the IP Precedence to DSCP mapping list	320
IP Port to DSCP		323
Add	Sets TCP/UDP port priority, defining the socket number and associated per-hop behavior and drop precedence	323
Show	Shows the IP Port to DSCP mapping list	323
PHB to Queue		309
Configure	Maps internal per-hop behavior values to hardware queues	309
Show	Shows the PHB to Queue mapping list	309
DiffServ		325
Configure Class		326
Add	Creates a class map for a type of traffic	326
Show	Shows configured class maps	326
Modify	Modifies the name of a class map	326
Add Rule	Configures the criteria used to classify ingress traffic	326
Show Rule	Shows the traffic classification rules for a class map	326
Configure Policy		329
Add	Creates a policy map to apply to multiple interfaces	329
Show	Shows configured policy maps	329
Modify	Modifies the name of a policy map	329
Add Rule	Sets the boundary parameters used for monitoring inbound traffic, and the action to take for conforming and non-conforming traffic	329
Show Rule	Shows the rules used to enforce bandwidth policing for a policy map	329
Configure Interface	Applies a policy map to an ingress port	339
VoIP	Voice over IP	341
Configure Global	Configures auto-detection of VoIP traffic, sets the Voice VLAN, and VLAN aging time	342
Configure OUI		343
Add	Maps the OUI in the source MAC address of ingress packets to the VoIP device manufacturer	343
Show	Shows the OUI telephony list	343

Table 6: Switch Main Menu (Continued)

Menu	Description	Page
Configure Interface	Configures VoIP traffic settings for ports, including the way in which a port is added to the Voice VLAN, filtering of non-VoIP packets, the method of detecting VoIP traffic, and the priority assigned to the voice traffic	345
Security		347
AAA	Authentication, Authorization and Accounting	348
System Authentication	Configures authentication sequence – local, RADIUS, and TACACS	349
Server		350
Configure Server	Configures RADIUS and TACACS server message exchange settings	350
Configure Group		350
Add	Specifies a group of authentication servers and sets the priority sequence	350
Show	Shows the authentication server groups and priority sequence	350
Accounting	Enables accounting of requested services for billing or security purposes	355
Configure Global	Specifies the interval at which the local accounting service updates information to the accounting server	355
Configure Method		355
Add	Configures accounting for various service types	355
Show	Shows the accounting settings used for various service types	355
Configure Service	Sets the accounting method applied to specific interfaces for 802.1X, CLI command privilege levels for the console port, and for Telnet	355
Show Information		355
Summary	Shows the configured accounting methods, and the methods applied to specific interfaces	355
Statistics	Shows basic accounting information recorded for user sessions	355
Authorization	Enables authorization of requested services	360
Configure Method		360
Add	Configures authorization for various service types	360
Show	Shows the authorization settings used for various service types	360
Configure Service	Sets the authorization method applied used for the console port, and for Telnet	360
Show Information	Shows the configured authorization methods, and the methods applied to specific interfaces	360
User Accounts		363
Add	Configures user names, passwords, and access levels	363
Show	Shows authorized users	363
Modify	Modifies user attributes	363
Web Authentication	Allows authentication and access to the network when 802.1X or Network Access authentication are infeasible or impractical	365
Configure Global	Configures general protocol settings	366

Table 6: Switch Main Menu (Continued)

Menu	Description	Page
Configure Interface	Enables Web Authentication for individual ports	367
Network Access	MAC address-based network access authentication	368
Configure Global	Enables aging for authenticated MAC addresses, and sets the time period after which a connected MAC address must be reauthenticated	371
Configure Interface		372
General	Enables MAC authentication on a port; sets the maximum number of address that can be authenticated, the guest VLAN, dynamic VLAN and dynamic QoS	372
Link Detection	Configures detection of changes in link status, and the response (i.e., send trap or shut down port)	374
Configure MAC Filter		375
Add	Specifies MAC addresses exempt from authentication	375
Show	Shows the list of exempt MAC addresses	375
Show Information	Shows the authenticated MAC address list	377
HTTPS	Secure HTTP	378
Configure Global	Enables HTTPs, and specifies the UDP port to use	378
Copy Certificate	Replaces the default secure-site certificate	380
SSH	Secure Shell	381
Configure Global	Configures SSH server settings	384
Configure Host Key		385
Generate	Generates the host key pair (public and private)	385
Show	Displays RSA and DSA host keys; deletes host keys	385
Configure User Key		387
Copy	Imports user public keys from TFTP server	387
Show	Displays RSA and DSA user keys; deletes user keys	387
ACL	Access Control Lists	389
Configure Time Range	Configures the time to apply an ACL	391
Add	Specifies the name of a time range	391
Show	Shows the name of configured time ranges	391
Add Rule		391
Absolute	Sets exact time or time range	391
Periodic	Sets a recurrent time	391
Show Rule	Shows the time specified by a rule	391
Configure ACL		395
Show TCAM	Shows utilization parameters for TCAM	394
Add	Adds an ACL based on IP or MAC address filtering	395
Show	Shows the name and type of configured ACLs	395

Table 6: Switch Main Menu (Continued)

Menu	Description	Page
Add Rule	Configures packet filtering based on IP or MAC addresses and other packet attributes	395
Show Rule	Shows the rules specified for an ACL	395
Configure Interface		408
Configure	Binds a port to the specified ACL and time range	408
Show Hardware Counters	Shows statistics for ACL hardware counters	409
ARP Inspection		410
Configure General	Enables inspection globally, configures validation of additional address components, and sets the log rate for packet inspection	411
Configure VLAN	Enables ARP inspection on specified VLANs	413
Configure Interface	Sets the trust mode for ports, and sets the rate limit for packet inspection	415
Show Information		
Show Statistics	Displays statistics on the inspection process	416
Show Log	Shows the inspection log list	417
IP Filter		418
Add	Sets IP addresses of clients allowed management access via the web, SNMP, and Telnet	418
Show	Shows the addresses to be allowed management access	418
Port Security	Configures per port security, including status, response for security breach, and maximum allowed MAC addresses	420
Port Authentication	IEEE 802.1X	423
Configure Global	Enables authentication and EAPOL pass-through	424
Configure Interface	Sets authentication parameters for individual ports	425
Show Statistics	Displays protocol statistics for the selected port	429
DoS Protection	Protects against Denial-of-Service attacks	431
IP Source Guard	Filters IPv4 traffic based on static entries in the IP Source Guard table, or dynamic entries in the DHCPv4 Snooping table	432
Port Configuration	Enables IP source guard and selects filter type per port	433
Static Binding		435
Add	Adds a static addresses to the source-guard binding table	435
Show	Shows static addresses in the source-guard binding table	435
Dynamic Binding	Displays the source-guard binding table for a selected interface	437
IPv6 Source Guard	Filters IPv6 traffic based on static entries in the IP Source Guard table, or dynamic entries in the DHCP Snooping table	438
Port Configuration	Enables IPv6 source guard and selects filter type per port	438
Static Binding		440
Add	Adds a static addresses to the source-guard binding table	440
Show	Shows static addresses in the source-guard binding table	440
Dynamic Binding	Displays the source-guard binding table for a selected interface	443

Table 6: Switch Main Menu (Continued)

Menu	Description	Page
Administration		453
Log		454
System		454
Configure Global	Stores error messages in local memory	454
Show System Logs	Shows logged error messages	454
Remote	Configures the logging of messages to a remote logging process	456
SMTP	Sends an SMTP client message to a participating server	457
LLDP		458
Configure Global	Configures global LLDP timing parameters	459
Configure Interface	Sets the message transmission mode; enables SNMP notification; and sets the LLDP attributes to advertise	461
Show Local Device Information		466
General	Displays general information about the local device	466
Port/Trunk	Displays information about each interface	466
Show Remote Device Information		470
Port/Trunk	Displays information about a remote device connected to a port on this switch	470
Port/Trunk Details	Displays detailed information about a remote device connected to this switch	470
Show Device Statistics		478
General	Displays statistics for all connected remote devices	478
Port/Trunk	Displays statistics for remote devices on a selected port or trunk	478
SNMP	Simple Network Management Protocol	480
Configure Global	Enables SNMP agent status, and sets related trap functions	482
Configure Engine		483
Set Engine ID	Sets the SNMP v3 engine ID on this switch	483
Add Remote Engine	Sets the SNMP v3 engine ID for a remote device	484
Show Remote Engine	Shows configured engine ID for remote devices	484
Configure View		486
Add View	Adds an SNMP v3 view of the OID MIB	486
Show View	Shows configured SNMP v3 views	486
Add OID Subtree	Specifies a part of the subtree for the selected view	486
Show OID Subtree	Shows the subtrees assigned to each view	486
Configure Group		489
Add	Adds a group with access policies for assigned users	489
Show	Shows configured groups and access policies	489
Configure User		
Add Community	Configures community strings and access mode	494

Table 6: Switch Main Menu (Continued)

Menu	Description	Page
Show Community	Shows community strings and access mode	494
Add SNMPv3 Local User	Configures SNMPv3 users on this switch	495
Show SNMPv3 Local User	Shows SNMPv3 users configured on this switch	495
Change SNMPv3 Local User Group	Assign a local user to a new group	495
Add SNMPv3 Remote User	Configures SNMPv3 users from a remote device	497
Show SNMPv3 Remote User	Shows SNMPv3 users set from a remote device	495
Configure Trap		500
Add	Configures trap managers to receive messages on key events that occur this switch	500
Show	Shows configured trap managers	500
Configure Notify Filter		504
Add	Creates an SNMP notification log	504
Show	Shows the configured notification logs	504
Show Statistics	Shows the status of SNMP communications	506
RMON	Remote Monitoring	508
Configure Global		
Add		
Alarm	Sets threshold bounds for a monitored variable	509
Event	Creates a response event for an alarm	511
Show		
Alarm	Shows all configured alarms	509
Event	Shows all configured events	511
Configure Interface		
Add		
History	Periodically samples statistics on a physical interface	513
Statistics	Enables collection of statistics on a physical interface	516
Show		
History	Shows sampling parameters for each entry in the history group	513
Statistics	Shows sampling parameters for each entry in the statistics group	516
Show Details		
History	Shows sampled data for each entry in the history group	513
Statistics	Shows sampled data for each entry in the history group	516
Cluster		518
Configure Global	Globally enables clustering for the switch; sets Commander status	519
Configure Member	Adds switch members to the cluster	520
Add	Adds candidate members to the cluster	520
Show	Shows the cluster members	520

Table 6: Switch Main Menu (Continued)

Menu	Description	Page
Show Candidate	Shows candidate members	520
Show Member	Shows cluster switch member; managed switch members	522
ERPS	Ethernet Ring Protection Switching	523
Configure Global	Activates ERPS globally	527
Configure Domain		528
Add	Creates an ERPS ring	528
Show	Shows list of configured ERPS rings, status, and settings	528
Configure Details	Configures ring parameters	528
Configure Operation	Blocks a ring port using Forced Switch or Manual Switch commands	544
CFM	Connectivity Fault Management	548
Configure Global	Configures global settings, including administrative status, cross-check start delay, link trace, and SNMP traps	551
Configure Interface	Configures administrative status on an interface	555
Configure MD	Configure Maintenance Domains	555
Add	Defines a portion of the network for which connectivity faults can be managed, identified by an MD index, maintenance level, and the MIP creation method	555
Configure Details	Configures the archive hold time and fault notification settings	555
Show	Shows list of configured maintenance domains	555
Configure MA	Configure Maintenance Associations	560
Add	Defines a unique CFM service instance, identified by its parent MD, the MA index, the VLAN assigned to the MA, and the MIP creation method	560
Configure Details	Configures detailed settings, including continuity check status and interval level, cross-check status, and alarm indication signal parameters	560
Show	Shows list of configured maintenance associations	560
Configure MEP	Configures Maintenance End Points	565
Add	Configures MEPs at the domain boundary to provide management access for each maintenance association	565
Show	Shows list of configured maintenance end points	565
Configure Remote MEP	Configures Remote Maintenance End Points	567
Add	Configures a static list of remote MEPs for comparison against the MEPs learned through continuity check messages	567
Show	Shows list of configured remote maintenance end points	567
Transmit Link Trace	Sends link trace messages to isolate connectivity faults by tracing the path through a network to the designated target node	569
Transmit Loopback	Sends loopback messages to isolate connectivity faults by requesting a target node to echo the message back to the source	571
Transmit Delay Measure	Sends periodic delay-measure requests to a specified MEP within a maintenance association	572

Table 6: Switch Main Menu (Continued)

Menu	Description	Page
Show Information		
Show Local MEP	Shows the MEPs configured on this device	574
Show Local MEP Details	Displays detailed CFM information about a specified local MEP in the continuity check database	575
Show Local MIP	Shows the MIPs on this device discovered by the CFM protocol	577
Show Remote MEP	Shows MEPs located on other devices which have been discovered through continuity check messages, or statically configured in the MEP database	578
Show Remote MEP Details	Displays detailed CFM information about a specified remote MEP in the continuity check database	579
Show Link Trace Cache	Shows information about link trace operations launched from this device	581
Show Fault Notification Generator	Displays configuration settings for the fault notification generator	583
Show Continuity Check Error	Displays CFM continuity check errors logged on this device	584
OAM	Operation, Administration, and Maintenance	585
Interface	Enables OAM on specified port, sets the mode to active or passive, and enables the reporting of critical events or errored frame events	585
Counters	Displays statistics on OAM PDUs	588
Event Log	Displays the log for recorded link events	589
Remote Interface	Displays information about attached OAM-enabled devices	590
Remote Loopback	Performs a loopback test on the specified port	591
IP		
General		
Routing Interface		
Add Address	Configures an IP interface for a VLAN	691
Show Address	Shows the IP interfaces assigned to a VLAN	691
Ping	Sends ICMP echo request packets to another node on the network	745
Trace Route	Shows the route packets take to the specified destination	746
ARP	Address Resolution Protocol	748
Configure General	Sets the protocol timeout, and enables or disables proxy ARP for the specified VLAN	748
Configure Static Address		750
Add	Statically maps a physical address to an IP address	750
Show	Shows the MAC to IP address static table	750
Show Information		752
Dynamic Address	Shows dynamically learned entries in the IP routing table	752
Other Address	Shows internal addresses used by the switch	752
Statistics	Shows statistics on ARP requests sent and received	753

Table 6: Switch Main Menu (Continued)

Menu	Description	Page
Routing		
Static Routes		753
Add	Configures static routing entries	753
Show	Shows static routing entries	753
Routing Table		755
Show Information	Shows all routing entries, including local, static and dynamic routes	755
Configure ECMP Number	Sets the maximum number of equal-cost paths to the same destination that can be installed in the routing table	757
VRRP	Virtual Router Redundancy Protocol	759
Configure Group ID		760
Add	Adds a VRRP group identifier to a VLAN	760
Show	Shows the VRRP group identifier list	760
Add IP Address	Sets a virtual interface address for a VRRP group	760
Show IP Address	Shows the virtual interface address assigned to a VRRP group	760
Configure Detail	Configure detailed settings, such as advertisement interval, preemption, priority, and authentication	760
Show Statistics		
Global Statistics	Displays global statistics for VRRP protocol packet errors	766
Group Statistics	Displays statistics for VRRP protocol events and errors on the specified VRRP group and interface	767
IPv6 Configuration		695
Configure Global	Sets an IPv6 default gateway for traffic with no known next hop	696
Configure Interface		697
VLAN	Configures IPv6 interface address using auto-configuration or link-local address, and sets related protocol settings	697
RA Guard	Blocks incoming Router Advertisement and Router Redirect packets	697
Add IPv6 Address	Adds an global unicast, EUI-64, or link-local IPv6 address to an interface	700
Show IPv6 Address	Show the IPv6 addresses assigned to an interface	703
Show IPv6 Neighbor Cache	Displays information in the IPv6 neighbor discovery cache	705
Show Statistics		706
IPv6	Shows statistics about IPv6 traffic	706
ICMPv6	Shows statistics about ICMPv6 messages	706
UDP	Shows statistics about UDP messages	706
Show MTU	Shows the maximum transmission unit (MTU) cache for destinations that have returned an ICMP packet-too-big message along with an acceptable MTU to this switch	712

Table 6: Switch Main Menu (Continued)

Menu	Description	Page
IP Service		713
DNS	Domain Name Service	
General		713
Configure Global	Enables DNS lookup; defines the default domain name appended to incomplete host names	713
Add Domain Name	Defines a list of domain names that can be appended to incomplete host names	714
Show Domain Names	Shows the configured domain name list	714
Add Name Server	Specifies IP address of name servers for dynamic lookup	716
Show Name Servers	Shows the name server address list	716
Static Host Table		717
Add	Configures static entries for domain name to address mapping	717
Show	Shows the list of static mapping entries	717
Modify	Modifies the static address mapped to the selected host name	717
Cache	Displays cache entries discovered by designated name servers	718
DHCP	Dynamic Host Configuration Protocol	
Client	Specifies the DHCP client identifier for an interface	720
Relay	Specifies DHCP relay servers	721
Snooping		444
Configure Global	Enables DHCP snooping globally, MAC-address verification, information option; and sets the information policy	446
Configure VLAN	Enables DHCP snooping on a VLAN	448
Configure Interface	Sets the trust mode for an interface	449
Show Information	Displays the DHCP Snooping binding information	450
Server		723
Configure Global	Enables DHCP service on this switch	724
Configure Excluded Address		724
Add	Adds excluded addresses	724
Show	Shows excluded addresses	724
Configure Pool		726
Add		726
Network	Add address pool for network groups	726
Host	Add address entry for specified host	726
Show	Shows DHCP pool list	726
Modify	Modifies the specified pool entry	726
Show IP Binding	Displays addresses currently bound to DHCP clients	730

Table 6: Switch Main Menu (Continued)

Menu	Description	Page
UDP Helper		730
General	Enables UDP helper globally on the switch	731
Forwarding		731
Add	Specifies the UDP destination ports for which broadcast traffic will be forwarded	731
Show	Shows the list of UDP ports to which broadcast traffic will be forwarded	731
Address		733
Add	Specifies the servers to which designated UDP protocol packets are forwarded	733
Show	Shows the servers to which designated UDP protocol packets are forwarded	733
PPPoE Intermediate Agent		735
Configure Global	Enables PPPoE IA on the switch, sets access node identifier, sets generic error message	735
Configure Interface	Enables PPPoE IA on an interface, sets trust status, enables vendor tag stripping, sets circuit ID and remote ID	736
Show Statistics	Shows statistics on PPPoE IA protocol messages	738
Multicast		609
IGMP Snooping		611
General	Enables multicast filtering; configures parameters for IPv4 multicast snooping	613
Multicast Router		617
Add Static Multicast Router	Assigns ports that are attached to a neighboring multicast router	617
Show Static Multicast Router	Displays ports statically configured as attached to a neighboring multicast router	617
Show Current Multicast Router	Displays ports attached to a neighboring multicast router, either through static or dynamic configuration	617
IGMP Member		619
Add Static Member	Statically assigns multicast addresses to the selected VLAN	619
Show Static Member	Shows multicast addresses statically configured on the selected VLAN	619
Show Current Member	Shows multicast addresses associated with the selected VLAN, either through static or dynamic configuration	619
Interface		621
Configure VLAN	Configures IGMP snooping per VLAN interface	621
Show VLAN Information	Shows IGMP snooping settings per VLAN interface	621
Forwarding Entry	Displays the current multicast groups learned through IGMP Snooping	628
Filter		633
Configure General	Enables IGMP filtering for the switch	633
Configure Profile		634
Add	Adds IGMP filter profile; and sets access mode	634

Table 6: Switch Main Menu (Continued)

Menu	Description	Page
Show	Shows configured IGMP filter profiles	634
Add Multicast Group Range	Assigns multicast groups to selected profile	634
Show Multicast Group Range	Shows multicast groups assigned to a profile	634
Configure Interface	Assigns IGMP filter profiles to port interfaces and sets throttling action	636
Statistics		629
Show Query Statistics	Shows statistics for query-related messages	629
Show VLAN Statistics	Shows statistics for protocol messages and number of active groups	629
Show Port Statistics	Shows statistics for protocol messages and number of active groups	629
Show Trunk Statistics	Shows statistics for protocol messages and number of active groups	629
MLD Snooping		638
General	Enables multicast filtering; configures parameters for IPv6 multicast snooping	638
Interface	Configures Immediate Leave status for a VLAN	640
Multicast Router		641
Add Static Multicast Router	Assigns ports that are attached to a neighboring multicast router	641
Show Static Multicast Router	Displays ports statically configured as attached to a neighboring multicast router	641
Show Current Multicast Router	Displays ports attached to a neighboring multicast router, either through static or dynamic configuration	641
MLD Member		643
Add Static Member	Statically assigns multicast addresses to the selected VLAN	643
Show Static Member	Shows multicast addresses statically configured on the selected VLAN	643
Show Current Member	Shows multicast addresses associated with the selected VLAN, either through static or dynamic configuration	643
Group Information	Displays known multicast groups, member ports, the means by which each group was learned, and the corresponding source list	645
IGMP		646
Proxy	Configures IGMP proxy service for multicast routing	647
Interface	Configures Layer 3 IGMP settings for selected VLAN interface	650
Static Group		652
Add	Configures the router to be a static member of a multicast group on the specified VLAN interface	652
Show	Shows multicast group statically assigned to a VLAN interface	652
Group Information		654
Show Information	Shows the current multicast groups learned through IGMP for each VLAN	654
Show Detail	Shows detailed information on each multicast group associated with a VLAN interface	654

Table 6: Switch Main Menu (Continued)

Menu	Description	Page
Multicast Routing		825
General	Globally enables IPv4 multicast routing	828
Information		829
Show Summary	Shows each multicast route the switch has learned	829
Show Details	Shows additional information for each multicast route the switch has learned, including RP address, upstream router, and downstream interfaces	829
IPv6 Multicast Routing		825
General	Globally enables IPv6 multicast routing	828
Information		829
Show Summary	Shows each multicast route the switch has learned	829
Show Details	Shows additional information for each multicast route the switch has learned, including RP address, upstream router, and downstream interfaces	829
MVR	Multicast VLAN Registration	657
Configure Global	Configures proxy switching and robustness value	658
Configure Domain	Enables MVR for a domain, sets the MVR VLAN, forwarding priority, and upstream source IP	660
Configure Profile		662
Add	Configures multicast stream addresses	662
Show	Shows multicast stream addresses	662
Associate Profile		662
Add	Maps an address profile to a domain	662
Show	Shows addresses profile to domain mapping	662
Configure Interface	Configures MVR interface type and immediate leave mode; also displays MVR operational and active status	665
Configure Static Group Member		667
Add	Statically assigns MVR multicast streams to an interface	667
Show	Shows MVR multicast streams assigned to an interface	667
Show Member	Shows the multicast groups assigned to an MVR VLAN, the source address of the multicast services, and the interfaces with active subscribers	669
Show Statistics		670
Show Query Statistics	Shows statistics for query-related messages	670
Show VLAN Statistics	Shows statistics for protocol messages and number of active groups	670
Show Port Statistics	Shows statistics for protocol messages and number of active groups	670
Show Trunk Statistics	Shows statistics for protocol messages and number of active groups	670
MVR6	Multicast VLAN Registration for IPv6	674
Configure Global	Configures proxy switching and robustness value	675

Table 6: Switch Main Menu (Continued)

Menu	Description	Page
Configure Domain	Enables MVR for a domain, sets the MVR VLAN, forwarding priority, and upstream source IP	677
Configure Profile		678
Add	Configures multicast stream addresses	678
Show	Shows multicast stream addresses	678
Associate Profile		678
Add	Maps an address profile to a domain	678
Show	Shows addresses profile to domain mapping	678
Configure Interface	Configures MVR interface type and immediate leave mode; also displays MVR operational and active status	681
Configure Port	Configures MVR attributes for a port	681
Configure Trunk	Configures MVR attributes for a trunk	681
Configure Static Group Member		684
Add	Statically assigns MVR multicast streams to an interface	684
Show	Shows MVR multicast streams assigned to an interface	684
Show Member	Shows the multicast groups assigned to an MVR VLAN, the source address of the multicast services, and the interfaces with active subscribers	685
Show Statistics		686
Show Query Statistics	Shows statistics for query-related messages	686
Show VLAN Statistics	Shows statistics for protocol messages and number of active groups	686
Show Port Statistics	Shows statistics for protocol messages and number of active groups	686
Show Trunk Statistics	Shows statistics for protocol messages and number of active groups	686
Routing Protocol		769
RIP		770
General		771
Configure	Enables or disables RIP, sets the global RIP attributes and timer values	771
Clear Route	Clears the specified route type or network interface from the routing table	774
Network		775
Add	Sets the network interfaces that will use RIP	775
Show	Shows the network interfaces that will use RIP	775
Passive Interface		777
Add	Stops RIP broadcast and multicast messages from being sent on specified network interfaces	777
Show	Shows the configured passive interfaces	777

Table 6: Switch Main Menu (Continued)

Menu	Description	Page
Neighbor Address		778
Add	Configures the router to directly exchange routing information with a static neighbor	778
Show	Shows adjacent hosts or interfaces configured as a neighboring router	778
Redistribute		779
Add	Imports external routing information from other routing domains (that is, protocols) into the autonomous system	779
Show	Shows the external routing information to be imported from other routing domains	779
Distance		781
Add	Defines an administrative distance for external routes learned from other routing protocols	781
Show	Shows the administrative distances assigned to external routes learned from other routing protocols	781
Interface		782
Add	Configures RIP parameters for each interface, including send and receive versions, authentication, and method of loopback prevention	782
Show	Shows the RIP parameters set for each interface	782
Modify	Modifies RIP parameters for an interface	782
Statistics		
Show Interface Information	Shows RIP settings, and statistics on RIP protocol messages	786
Show Peer Information	Displays information on neighboring RIP routers	787
Reset Statistics	Clears statistics for RIP protocol messages	788
OSPF	Open Shortest Path First (Version 2)	788
Network Area		790
Add	Defines OSPF area address, area ID, and process ID	790
Show	Shows configured areas	790
Show Process	Show configured processes	790
System		793
Configure	Configures the Router ID, global settings, and default information	793
Show	Shows LSA statistics, administrative status, ABR/ASBR, area count, and version number	796
Area		
Configure Area		798
Add Area	Adds NSSA or stub	798
Show Area	Shows configured NSSA or stub	798
Configure NSSA Area	Configures settings for importing routes into or exporting routes out of not-so-stubby areas	799
Configure Stub Area	Configures default cost, and settings for importing routes into a stub	802

Table 6: Switch Main Menu (Continued)

Menu	Description	Page
Show Information	Shows statistics for each area, including SPF startups, ABR/ASBR count, LSA count, and LSA checksum	804
Area Range		805
Add	Configures route summaries to advertise at an area boundary	805
Show	Shows route summaries advertised at an area boundary	805
Modify	Modifies route summaries advertised at an area boundary	805
Redistribute		807
Add	Redistributes routes from one routing domain to another	807
Show	Shows route types redistributed to another domain	807
Modify	Modifies configuration settings for redistributed routes	807
Summary Address		809
Add	Aggregates routes learned from other protocols for advertising into other autonomous systems	809
Show	Shows configured summary addresses	809
Interface		811
Show	Shows area ID and designated router settings for each interface	811
Configure by VLAN	Configures OSPF protocol settings and authentication for specified VLAN	811
Configure by Address	Configures OSPF protocol settings and authentication for specified interface address	811
Show MD5 Key	Shows MD5 key ID used for each area	811
Virtual Link		817
Add	Configures a virtual link through a transit area to the backbone	817
Show	Shows virtual links, neighbor address, and state	817
Configure Detailed Settings	Configures detailed protocol and authentication settings	817
Show MD5 Key	Shows the MD5 key ID used for each neighbor	817
Information		820
LSDB	Shows information about different OSPF Link State Advertisements (LSAs)	820
Neighbor	Shows information about each OSPF neighbor	823
PIM		833
General	Enables PIM globally for the switch	833
Interface	Enables PIM per interface, and sets the mode to dense or sparse	834
Neighbor	Displays information neighboring PIM routers	839
SM		840
Configure Global	Configures settings for register messages, and use of the SPT	840
BSR Candidate	Configures the switch as a BSR candidate	842

Table 6: Switch Main Menu (Continued)

Menu	Description	Page
RP Address		843
Add	Sets a static address for an RP and the associated multicast group(s)	843
Show	Shows the static addresses configured for each RP and the associated multicast groups	843
RP Candidate		845
Add	Advertises the switch as an RP candidate to the BSR for the specified multicast groups	845
Show	Shows the multicast groups for which this switch is advertising itself as an RP candidate to the BSR	845
Show Information		847
Show BSR Router	Displays information about the BSR	847
Show RP Mapping	Displays the active RPs and associated multicast routing entries	848
PIM6	PIM for IPv6	849
General	Enables PIM globally for the switch	849
Interface	Enables PIM per interface, and sets the mode to dense or sparse	850
Neighbor	Displays information neighboring PIM routers	856
SM		856
Configure Global	Configures settings for register messages, and use of the SPT	856
BSR Candidate	Configures the switch as a BSR candidate	858
RP Address		859
Add	Sets a static address for an RP and the associated multicast group(s)	859
Show	Shows the static addresses configured for each RP and the associated multicast groups	859
RP Candidate		861
Add	Advertises the switch as an RP candidate to the BSR for the specified multicast groups	861
Show	Shows the multicast groups for which this switch is advertising itself as an RP candidate to the BSR	861
Show Information		863
Show BSR Router	Displays information about the BSR	863
Show RP Mapping	Displays the active RPs and associated multicast routing entries	865
Snyc		
PTP	Configures clock synchronization for the local network	594
Configure Global	Sets the PTP clock synchronization domain, and the preference level used in selecting the master clock; and adjusts the system time based information in received Sync messages	595
Configure Interface	Sets the timing parameters used in message exchange, and the transport method for protocol messages; and enabled PTP per port	598
Show PTP Information	Shows configured and protocol negotiated settings	602
Show Foreign Master	Shows PTP announcements from neighbors	607

4 Basic Management Tasks

This chapter describes the following topics:

- Displaying System Information – Provides basic system description, including contact information.
- Displaying Hardware/Software Versions – Shows the hardware version, power status, and firmware versions
- Configuring Support for Jumbo Frames – Enables support for jumbo frames.
- Displaying Bridge Extension Capabilities – Shows the bridge extension parameters.
- Managing System Files – Describes how to upgrade operating software or configuration files, and set the system start-up files.
- Setting the System Clock – Sets the current time manually or through specified NTP or SNTP servers.
- Configuring the Console Port – Sets console port connection parameters.
- Configuring Telnet Settings – Sets Telnet connection parameters.
- Displaying CPU Utilization – Displays information on CPU utilization.
- Displaying Memory Utilization – Shows memory utilization parameters.
- Resetting the System – Restarts the switch immediately, at a specified time, after a specified delay, or at a periodic interval.

Displaying System Information

Use the System > General page to identify the system by displaying information such as the device name, location and contact information.

CLI References

- "System Management Commands" on page 891
- "SNMP Commands" on page 995

PARAMETERS

These parameters are displayed:

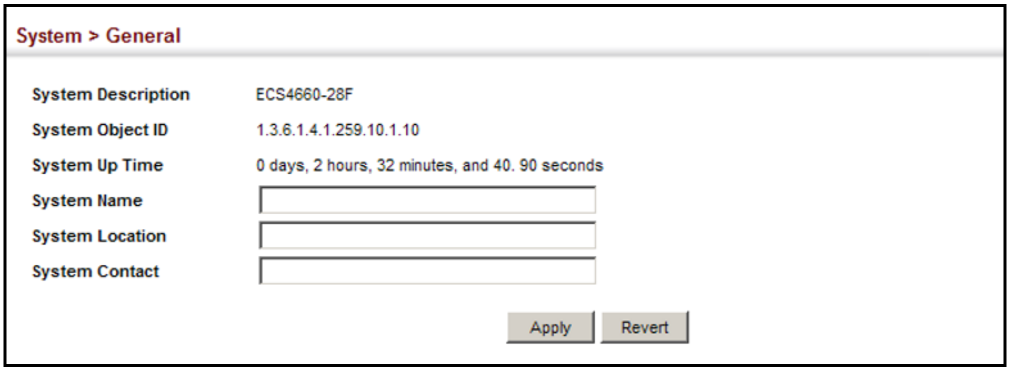
- **System Description** – Brief description of device type.
- **System Object ID** – MIB II object ID for switch's network management subsystem.
- **System Up Time** – Length of time the management agent has been up.
- **System Name** – Name assigned to the switch system.
- **System Location** – Specifies the system location.
- **System Contact** – Administrator responsible for the system.

WEB INTERFACE

To configure general system information:

1. Click System, General.
2. Specify the system name, location, and contact information for the system administrator.
3. Click Apply.

Figure 3: System Information



System > General

System Description ECS4660-28F
System Object ID 1.3.6.1.4.1.259.10.1.10
System Up Time 0 days, 2 hours, 32 minutes, and 40. 90 seconds
System Name
System Location
System Contact

DISPLAYING HARDWARE/SOFTWARE VERSIONS

Use the System > Switch page to display hardware/firmware version numbers for the main board and management software, as well as the power status of the system.

CLI REFERENCES

- "System Management Commands" on page 891

PARAMETERS

The following parameters are displayed:

Main Board Information

- **Serial Number** – The serial number of the switch.
- **Number of Ports** – Number of built-in ports.
- **Hardware Version** – Hardware version of the main board.
- **Main Power Status** – Displays the status of the internal power supply.
- **Redundant Power Status** – Displays the status of the redundant power supply.

Management Software Information

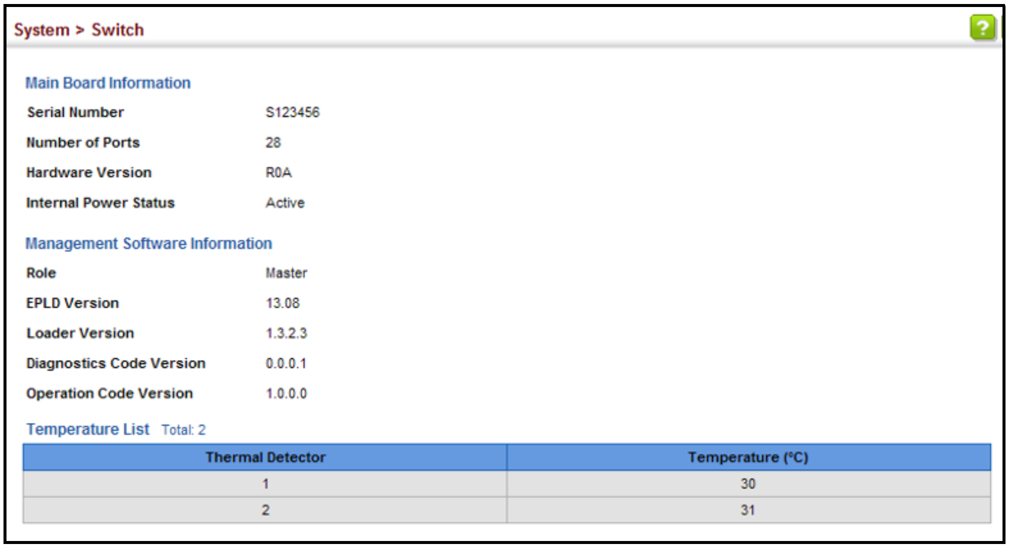
- **Role** – Shows that this switch is operating as Master or Slave.
- **EPLD Version** – Version number of EEPROM Programmable Logic Device.
- **Loader Version** – Version number of loader code.
- **Diagnostics Code Version** – Version of Power-On Self-Test (POST) and boot code.
- **Operation Code Version** – Version number of runtime code.
- **Thermal Detector** – The first detector is near the air flow intake vents. The second detector is near the switch ASIC and CPU.
- **Temperature** – Temperature at specified thermal detection point.

WEB INTERFACE

To view hardware and software version information.

1. Click System, then Switch.

Figure 4: General Switch Information



System > Switch

Main Board Information

Serial Number	S123456
Number of Ports	28
Hardware Version	R0A
Internal Power Status	Active

Management Software Information

Role	Master
EPLD Version	13.08
Loader Version	1.3.2.3
Diagnostics Code Version	0.0.0.1
Operation Code Version	1.0.0.0

Temperature List Total: 2

Thermal Detector	Temperature (°C)
1	30
2	31

CONFIGURING SUPPORT FOR JUMBO FRAMES

Use the System > Capability page to configure support for layer 2 jumbo frames. The switch provides more efficient throughput for large sequential data transfers by supporting jumbo frames of up to 9216 bytes for Gigabit and 10 Gigabit Ethernet ports or trunks. Compared to standard Ethernet frames that run only up to 1.5 KB, using jumbo frames significantly reduces the per-packet overhead required to process protocol encapsulation fields.

CLI REFERENCES

- "jumbo frame" on page 911
- "switchport mtu" on page 1195

USAGE GUIDELINES

- To use jumbo frames, both the source and destination end nodes (such as a computer or server) must support this feature. Also, when the connection is operating at full duplex, all switches in the network between the two end nodes must be able to accept the extended frame size. And for half-duplex connections, all devices in the collision domain would need to support jumbo frames.

- This command globally enables support for jumbo frames on all Gigabit and 10 Gigabit ports and trunks. To set the MTU for a specific interface, enable jumbo frames on this page, and then specify the required size of the MTU on the port or trunk interface configuration page (see "Port Configuration" on page 182 or "Trunk Configuration" on page 204).

PARAMETERS

The following parameters are displayed:

- **Jumbo Frame** – Configures support for jumbo frames. (Default: Disabled)

WEB INTERFACE

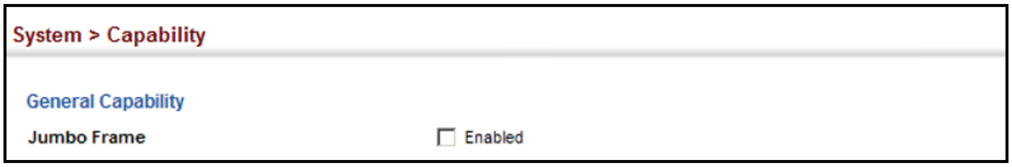
To configure support for jumbo frames:

1. Click System, then Capability.

2. Enable or disable support for jumbo frames.

3. Click Apply.

Figure 5: Configuring Support for Jumbo Frames



System > Capability

General Capability

Jumbo Frame ☐ Enabled

DISPLAYING BRIDGE EXTENSION CAPABILITIES

Use the System > Capability page to display settings based on the Bridge MIB. The Bridge MIB includes extensions for managed devices that support Multicast Filtering, Traffic Classes, and Virtual LANs. You can access these extensions to display default settings for the key variables.

CLI REFERENCES

- "GVRP and Bridge Extension Commands" on page 1338

PARAMETERS

The following parameters are displayed:

- **Extended Multicast Filtering Services** – This switch does not support the filtering of individual multicast addresses based on GMRP (GARP Multicast Registration Protocol).

- **Traffic Classes** – This switch provides mapping of user priorities to multiple traffic classes. (Refer to "Class of Service" on page 305.)

- **Static Entry Individual Port** – This switch allows static filtering for unicast and multicast addresses. (Refer to "Setting Static Addresses" on page 265.)

- **VLAN Version Number** – Based on IEEE 802.1Q, “1” indicates Bridges that support only single spanning tree (SST) operation, and “2” indicates Bridges that support multiple spanning tree (MST) operation.

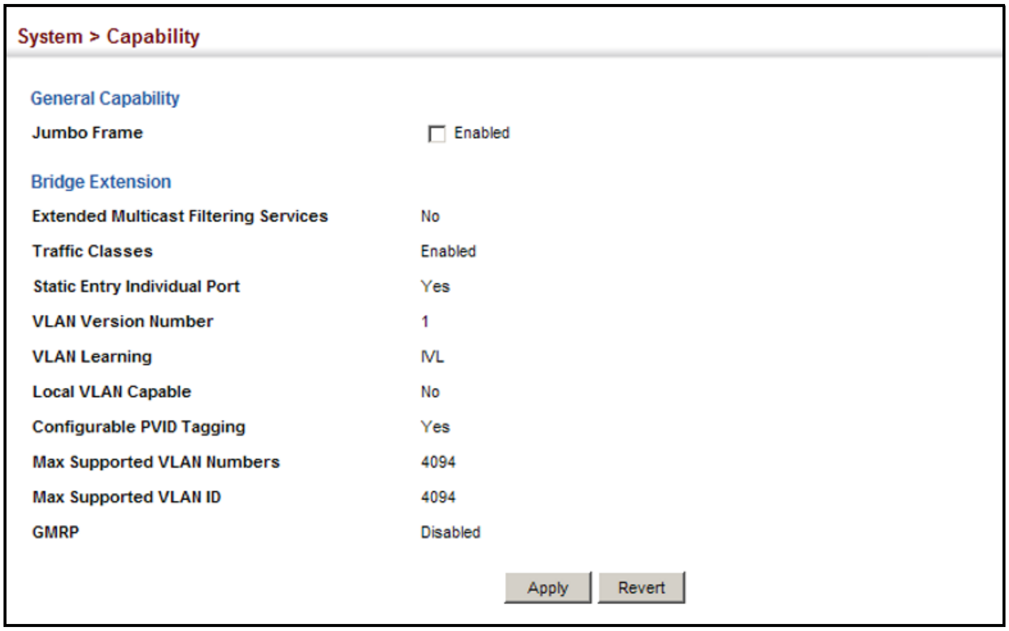
- **VLAN Learning** – This switch uses Independent VLAN Learning (IVL), where each port maintains its own filtering database.
- **Local VLAN Capable** – This switch does not support multiple local bridges outside of the scope of 802.1Q defined VLANs.
- **Configurable PVID Tagging** – This switch allows you to override the default Port VLAN ID (PVID used in frame tags) and egress status (VLAN-Tagged or Untagged) on each port. (Refer to "VLAN Configuration" on page 225.)
- **Max Supported VLAN Numbers** – The maximum number of VLANs supported on this switch.
- **Max Supported VLAN ID** – The maximum configurable VLAN identifier supported on this switch.
- **GMRP** – GARP Multicast Registration Protocol (GMRP) allows network devices to register end stations with multicast groups. This switch does not support GMRP; it uses the Internet Group Management Protocol (IGMP) to provide automatic multicast filtering.

WEB INTERFACE

To view Bridge Extension information:

1. Click System, then Capability.

Figure 6: Displaying Bridge Extension Configuration



System > Capability

General Capability

Jumbo Frame □ Enabled

Bridge Extension

Extended Multicast Filtering Services	No
Traffic Classes	Enabled
Static Entry Individual Port	Yes
VLAN Version Number	1
VLAN Learning	IVL
Local VLAN Capable	No
Configurable PVID Tagging	Yes
Max Supported VLAN Numbers	4094
Max Supported VLAN ID	4094
GMRP	Disabled

MANAGING SYSTEM FILES

This section describes how to upgrade the switch operating software or configuration files, and set the system start-up files.

COPYING FILES VIA FTP/TFTP OR HTTP

Use the System > File (Copy) page to upload/download firmware or configuration settings using FTP, TFTP or HTTP. By backing up a file to an FTP/TFTP server or management station, that file can later be downloaded to the switch to restore operation. Specify the method of file transfer, along with the file type and file names as required.

You can also set the switch to use new firmware or configuration settings without overwriting the current version. Just download the file using a different name from the current version, and then set the new file as the startup file.

CLI REFERENCES

- "copy" on page 914

COMMAND USAGE

When logging into an FTP server, the interface prompts for a user name and password configured on the remote server. Note that “Anonymous” is set as the default user name.

PARAMETERS

The following parameters are displayed:

- **Copy Type** – The firmware copy operation includes these options:
  - FTP Upload – Copies a file from an FTP server to the switch.
  - FTP Download – Copies a file from the switch to an FTP server.
  - HTTP Upload – Copies a file from a management station to the switch.
  - HTTP Download – Copies a file from the switch to a management station
  - TFTP Upload – Copies a file from a TFTP server to the switch.
  - TFTP Download – Copies a file from the switch to a TFTP server.
- **FTP/TFTP Server IP Address** – The IP address of an FTP/TFTP server.
- **User Name** – The user name for FTP server access.
- **Password** – The password for FTP server access.
- **File Type** – Specify Operation Code to copy firmware.

- **File Name** – The file name should not contain slashes (\ or /), the leading letter of the file name should not be a period (.), and the maximum length for file names is 32 characters for files on the switch or 128 characters for files on the server. (Valid characters: A-Z, a-z, 0-9, ".", "-", "_")

NOTE: Up to two copies of the system software (i.e., the runtime firmware) can be stored in the file directory on the switch.

NOTE: The maximum number of user-defined configuration files is limited only by available flash memory space.

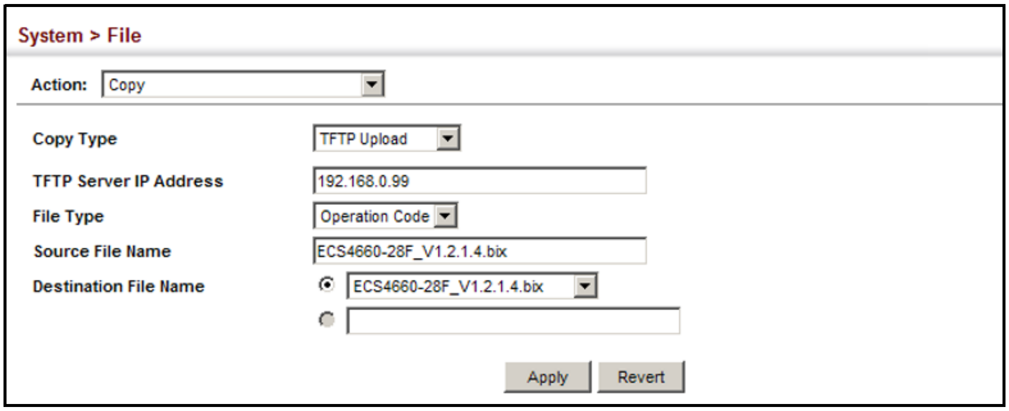
NOTE: The file "Factory_Default_Config.cfg" can be copied to a file server or management station, but cannot be used as the destination file name on the switch.

WEB INTERFACE

To copy firmware files:

1. Click System, then File.
2. Select Copy from the Action list.
3. Select FTP Upgrade, HTTP Upgrade, or TFTP Upgrade as the file transfer method.
4. If FTP or TFTP Upgrade is used, enter the IP address of the file server.
5. If FTP Upgrade is used, enter the user name and password for your account on the FTP server.
6. Set the file type to Operation Code.
7. Enter the name of the file to download.
8. Select a file on the switch to overwrite or specify a new file name.
9. Then click Apply.

Figure 7: Copy Firmware



System > File

Action: Copy

Copy Type: TFTP Upload

TFTP Server IP Address: 192.168.0.99

File Type: Operation Code

Source File Name: ECS4660-28F_V1.2.1.4.bix

Destination File Name: ● ECS4660-28F_V1.2.1.4.bix

○

If you replaced a file currently used for startup and want to start using the new file, reboot the system via the System > Reset menu.

SAVING THE RUNNING CONFIGURATION TO A LOCAL FILE

Use the System > File (Copy) page to save the current configuration settings to a local file on the switch. The configuration settings are not automatically saved by the system for subsequent use when the switch is rebooted. You must save these settings to the current startup file, or to another file which can be subsequently set as the startup file.

CLI REFERENCES

- "copy" on page 914

PARAMETERS

The following parameters are displayed:

- **Copy Type** – The copy operation includes this option:
  - Running-Config – Copies the current configuration settings to a local file on the switch.
- **Destination File Name** – Copy to the currently designated startup file, or to a new file. The file name should not contain slashes (\ or /), the leading letter of the file name should not be a period (.), and the maximum length for file names is 32 characters for files on the switch or 128 characters for files on the server. (Valid characters: A-Z, a-z, 0-9, ".", "-", "_")

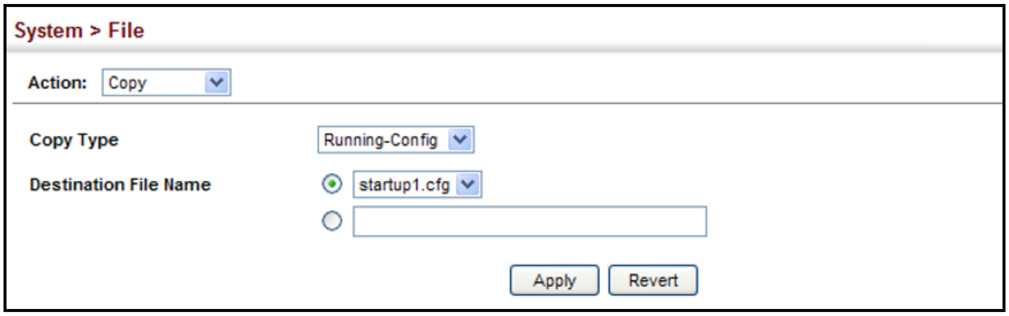
NOTE: The maximum number of user-defined configuration files is limited only by available flash memory space.

WEB INTERFACE

To save the running configuration file:

1. Click System, then File.
2. Select Copy from the Action list.
3. Select Running-Config from the Copy Type list.
4. Select the current startup file on the switch to overwrite or specify a new file name.
5. Then click Apply.

Figure 8: Saving the Running Configuration



System > File

Action: Copy

Copy Type: Running-Config

Destination File Name: ● startup1.cfg
○

If you replaced a file currently used for startup and want to start using the new file, reboot the system via the System > Reset menu.

SETTING THE START-UP FILE

Use the System > File (Set Start-Up) page to specify the firmware or configuration file to use for system initialization.

CLI REFERENCES

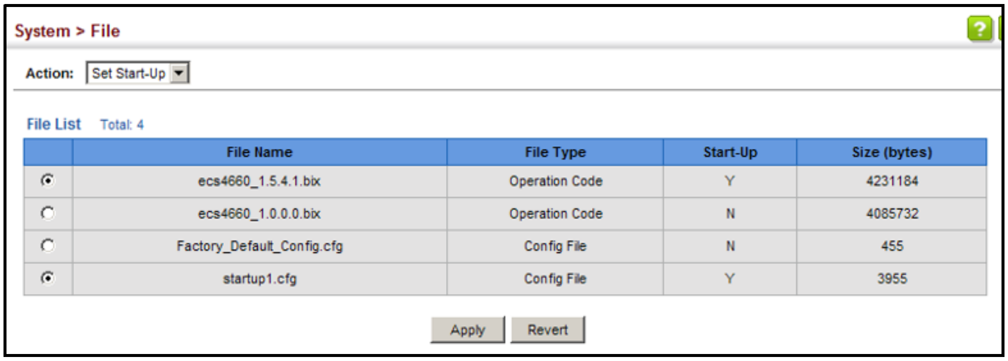
- "whichboot" on page 919
- "boot system" on page 913

WEB INTERFACE

To set a file to use for system initialization:

1. Click System, then File.
2. Select Set Start-Up from the Action list.
3. Mark the operation code or configuration file to be used at startup
4. Then click Apply.

Figure 9: Setting Start-Up Files



Action: Set Start-Up

File List Total: 4

	File Name	File Type	Start-Up	Size (bytes)
●	ecs4660_1.5.4.1.bix	Operation Code	Y	4231184
○	ecs4660_1.0.0.0.bix	Operation Code	N	4085732
○	Factory_Default_Config.cfg	Config File	N	455
●	startup1.cfg	Config File	Y	3955

To start using the new firmware or configuration settings, reboot the system via the System > Reset menu.

SHOWING SYSTEM FILES

Use the System > File (Show) page to show the files in the system directory, or to delete a file.

NOTE: Files designated for start-up, and the Factory_Default_Config.cfg file, cannot be deleted.

CLI REFERENCES

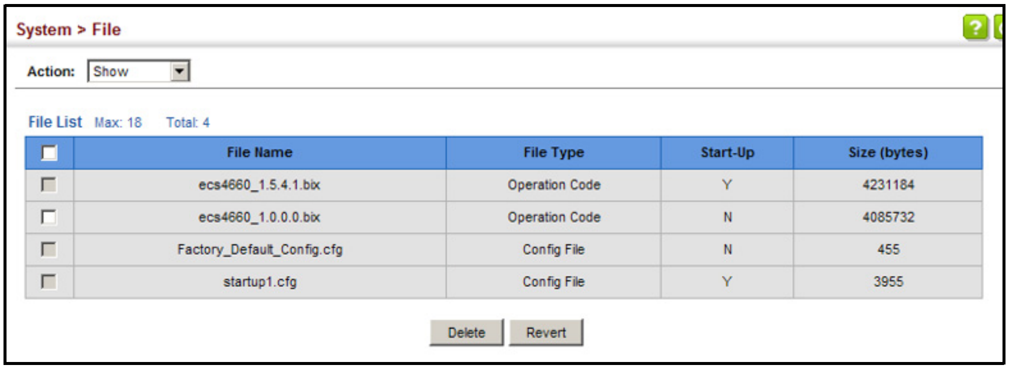
- "dir" on page 918
- "delete" on page 917

WEB INTERFACE

To show the system files:

1. Click System, then File.
2. Select Show from the Action list.
3. To delete a file, mark it in the File List and click Delete.

Figure 10: Displaying System Files



Action: Show

File List Max: 18 Total: 4

□	File Name	File Type	Start-Up	Size (bytes)
□	ecs4660_1.5.4.1.bix	Operation Code	Y	4231184
□	ecs4660_1.0.0.0.bix	Operation Code	N	4085732
□	Factory_Default_Config.cfg	Config File	N	455
□	startup1.cfg	Config File	Y	3955

AUTOMATIC OPERATION CODE UPGRADE

Use the System > File (Automatic Operation Code Upgrade) page to automatically download an operation code file when a file newer than the currently installed one is discovered on the file server. After the file is transferred from the server and successfully written to the file system, it is automatically set as the startup file, and the switch is rebooted.

CLI REFERENCES

- "upgrade opcode auto" on page 920
- "upgrade opcode path" on page 921

USAGE GUIDELINES

- If this feature is enabled, the switch searches the defined URL once during the bootup sequence.
- FTP (port 21) and TFTP (port 69) are both supported. Note that the TCP/UDP port bindings cannot be modified to support servers listening on non-standard ports.
- The host portion of the upgrade file location URL must be a valid IPv4 IP address. DNS host names are not recognized. Valid IP addresses consist of four numbers, 0 to 255, separated by periods.
- The path to the directory must also be defined. If the file is stored in the root directory for the FTP/TFTP service, then use the “/” to indicate this (e.g., ftp://192.168.0.1/).
- The file name must not be included in the upgrade file location URL. The file name of the code stored on the remote server must be ECS4660_28F.bix (using upper case and lower case letters exactly as indicated here). Enter the file name for other switches described in this manual exactly as shown on the web interface.
- The FTP connection is made with PASV mode enabled. PASV mode is needed to traverse some fire walls, even if FTP traffic is not blocked. PASV mode cannot be disabled.
- The switch-based search function is case-insensitive in that it will accept a file name in upper or lower case (i.e., the switch will accept *ECS4660_28F.BIX* from the server even though *ECS4660_28F.bix* was requested). However, keep in mind that the file systems of many operating systems such as Unix and most Unix-like systems (FreeBSD, NetBSD, OpenBSD, and most Linux distributions, etc.) are case-sensitive, meaning that two files in the same directory, *ecs4660-28f.bix* and *ECS4660-28F.BIX* are considered to be unique files. Thus, if the upgrade file is stored as *ECS4660-28F.BIX* (or even *Ecs4660-28f.bix*) on a case-sensitive server, then the switch (requesting *ECS4660-28F.bix*) will not be upgraded because the server does not recognize the requested file name and the stored file name as being equal. A notable exception in the list of case-sensitive Unix-like operating systems is Mac OS X, which by default is case-insensitive. Please check the documentation for your server’s operating system if you are unsure of its file system’s behavior.

- Note that the switch itself does not distinguish between upper and lower-case file names, and only checks to see if the file stored on the server is more recent than the current runtime image.

- If two operation code image files are already stored on the switch's file system, then the non-startup image is deleted before the upgrade image is transferred.

- The automatic upgrade process will take place in the background without impeding normal operations (data switching, etc.) of the switch.

- During the automatic search and transfer process, the administrator cannot transfer or update another operation code image, configuration file, public key, or HTTPS certificate (i.e., no other concurrent file management operations are possible).

- The upgrade operation code image is set as the startup image after it has been successfully written to the file system.

- The switch will send an SNMP trap and make a log entry upon all upgrade successes and failures.

- The switch will immediately restart after the upgrade file is successfully written to the file system and set as the startup image.

PARAMETERS

The following parameters are displayed:

- **Automatic Opcode Upgrade** – Enables the switch to search for an upgraded operation code file during the switch bootup process. (Default: Disabled)

- **Automatic Upgrade Location URL** – Defines where the switch should search for the operation code upgrade file. The last character of this URL must be a forward slash ("/"). The *ECS4660-28F.bix* filename must not be included since it is automatically appended by the switch. (Options: ftp, tftp)

  The following syntax must be observed:

  tftp://*host*[**/***filedir*]**/**

  - **tftp://** – Defines TFTP protocol for the server connection.
  - *host* – Defines the IP address of the TFTP server. Valid IP addresses consist of four numbers, 0 to 255, separated by periods. DNS host names are not recognized.
  - *filedir* – Defines the directory, relative to the TFTP server root, where the upgrade file can be found. Nested directory structures are accepted. The directory name must be separated from the host, and in nested directory structures, from the parent directory, with a prepended forward slash "/".
  - **/** – The forward slash must be the last character of the URL.

ftp://[*username*[**:***password***@**]]*host*[**/***filedir*]**/**

- **ftp://** – Defines FTP protocol for the server connection.
- *username* – Defines the user name for the FTP connection. If the user name is omitted, then "anonymous" is the assumed user name for the connection.
- *password* – Defines the password for the FTP connection. To differentiate the password from the user name and host portions of the URL, a colon (:) must precede the password, and an "at" symbol (@), must follow the password. If the password is omitted, then "" (an empty string) is the assumed password for the connection.
- *host* – Defines the IP address of the FTP server. Valid IP addresses consist of four numbers, 0 to 255, separated by periods. DNS host names are not recognized.
- *filedir* – Defines the directory, relative to the FTP server root, where the upgrade file can be found. Nested directory structures are accepted. The directory name must be separated from the host, and in nested directory structures, from the parent directory, with a prepended forward slash "/".
- **/** – The forward slash must be the last character of the URL.

Examples

The following examples demonstrate the URL syntax for a TFTP server at IP address 192.168.0.1 with the operation code image stored in various locations:

- tftp://192.168.0.1/

  The image file is in the TFTP root directory.

- tftp://192.168.0.1/switch-opcode/

  The image file is in the "switch-opcode" directory, relative to the TFTP root.

- tftp://192.168.0.1/switches/opcode/

  The image file is in the "opcode" directory, which is within the "switches" parent directory, relative to the TFTP root.

The following examples demonstrate the URL syntax for an FTP server at IP address 192.168.0.1 with various user name, password and file location options presented:

- ftp://192.168.0.1/

  The user name and password are empty, so "anonymous" will be the user name and the password will be blank. The image file is in the FTP root directory.

- ftp://switches:upgrade@192.168.0.1/

  The user name is "switches" and the password is "upgrade". The image file is in the FTP root.

- ftp://switches:upgrade@192.168.0.1/switches/opcode/

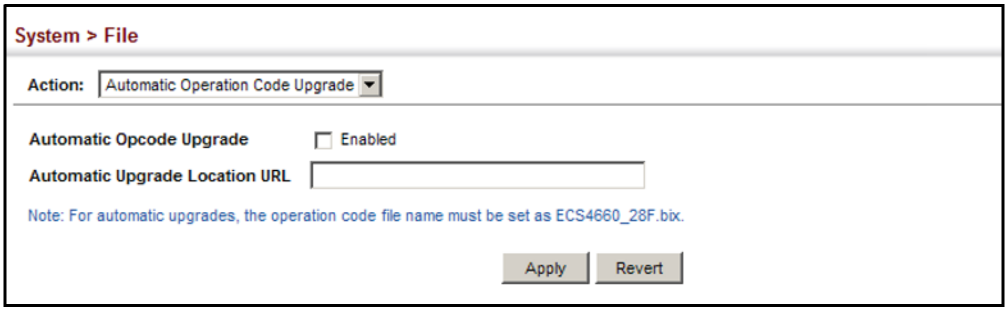
  The user name is “switches” and the password is “upgrade”. The image file is in the “opcode” directory, which is within the “switches” parent directory, relative to the FTP root.

WEB INTERFACE

To configure automatic code upgrade:

1. Click System, then File.
2. Select Automatic Operation Code Upgrade from the Action list.
3. Mark the check box to enable Automatic Opcode Upgrade.
4. Enter the URL of the FTP or TFTP server, and the path and directory containing the operation code.
5. Click Apply.

Figure 11: Configuring Automatic Code Upgrade



System > File

Action: Automatic Operation Code Upgrade

Automatic Opcode Upgrade □ Enabled

Automatic Upgrade Location URL

Note: For automatic upgrades, the operation code file name must be set as ECS4660_28F.bix.

If a new image is found at the specified location, the following type of messages will be displayed during bootup.

```
.
.
.
Automatic Upgrade is looking for a new image
New image detected: current version 1.1.1.0; new version 1.1.1.2
Image upgrade in progress
The switch will restart after upgrade succeeds
Downloading new image
Flash programming started
Flash programming completed
The switch will now restart
.
.
.
```

SETTING THE SYSTEM CLOCK

Simple Network Time Protocol (SNTP) allows the switch to set its internal clock based on periodic updates from a time server (SNTP or NTP). 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. If the clock is not set manually or via SNTP, the switch will only record the time from the factory default set at the last bootup.

When the SNTP client is enabled, the switch periodically sends a request for a time update to a configured time server. You can configure up to three time server IP addresses. The switch will attempt to poll each server in the configured sequence.

SETTING THE TIME MANUALLY

Use the System > Time (Configure General - Manual) page to set the system time on the switch manually without using SNTP.

CLI REFERENCES

- "calendar set" on page 956
- "show calendar" on page 957

PARAMETERS

The following parameters are displayed:

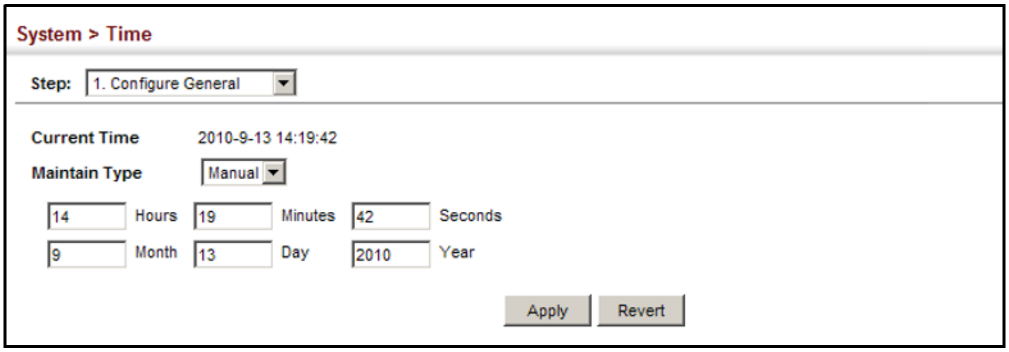
- **Current Time** – Shows the current time set on the switch.
- **Hours** – Sets the hour. (Range: 0-23)
- **Minutes** – Sets the minute value. (Range: 0-59)
- **Seconds** – Sets the second value. (Range: 0-59)
- **Month** – Sets the month. (Range: 1-12)
- **Day** – Sets the day of the month. (Range: 1-31)
- **Year** – Sets the year. (Range: 1970-2037)

WEB INTERFACE

To manually set the system clock:

1. Click System, then Time.
2. Select Configure General from the Step list.
3. Select Manual from the Maintain Type list.
4. Enter the time and date in the appropriate fields.
5. Click Apply

Figure 12: Manually Setting the System Clock



System > Time

Step: 1. Configure General

Current Time 2010-9-13 14:19:42

Maintain Type Manual

14 Hours 19 Minutes 42 Seconds

9 Month 13 Day 2010 Year

SETTING THE SNTP POLLING INTERVAL

Use the System > Time (Configure General - SNTP) page to set the polling interval at which the switch will query the specified time servers.

CLI REFERENCES

- "Time" on page 944

PARAMETERS

The following parameters are displayed:

- **Current Time** – Shows the current time set on the switch.

- **SNTP Polling Interval** – Sets the interval between sending requests for a time update from a time server. (Range: 16-16384 seconds; Default: 16 seconds)

WEB INTERFACE

To set the polling interval for SNTP:

1. Click System, then Time.

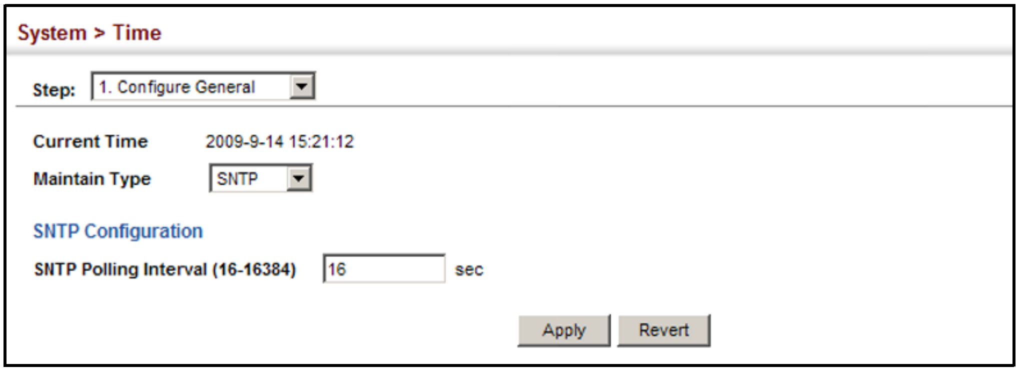
2. Select Configure General from the Step list.

3. Select SNTP from the Maintain Type list.

4. Modify the polling interval if required.

5. Click Apply

Figure 13: Setting the Polling Interval for SNTP



System > Time

Step: 1. Configure General

Current Time 2009-9-14 15:21:12

Maintain Type SNTP

SNTP Configuration

SNTP Polling Interval (16-16384) 16 sec

CONFIGURING NTP

Use the System > Time (Configure General - NTP) page to configure NTP authentication and show the polling interval at which the switch will query the specified time servers.

CLI REFERENCES

- "Time" on page 944

PARAMETERS

The following parameters are displayed:

- **Current Time** – Shows the current time set on the switch.
- **Authentication Status** – Enables authentication for time requests and updates between the switch and NTP servers. (Default: Disabled)

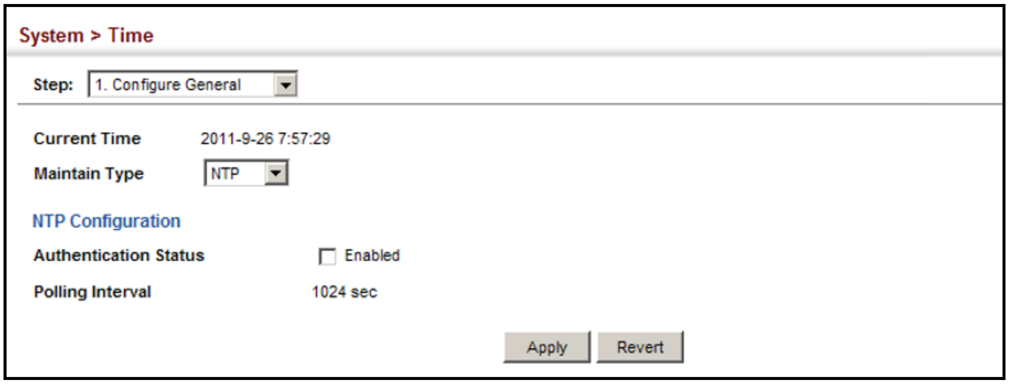
  You can enable NTP authentication to ensure that reliable updates are received from only authorized NTP servers. The authentication keys and their associated key number must be centrally managed and manually distributed to NTP servers and clients. The key numbers and key values must match on both the server and client.
- **Polling Interval** – Shows the interval between sending requests for a time update from NTP servers. (Fixed: 1024 seconds)

WEB INTERFACE

To set the clock maintenance type to NTP:

1. Click System, then Time.
2. Select Configure General from the Step list.
3. Select NTP from the Maintain Type list.
4. Enable authentication if required.
5. Click Apply

Figure 14: Configuring NTP



System > Time

Step: 1. Configure General

Current Time 2011-9-26 7:57:29

Maintain Type NTP

NTP Configuration

Authentication Status □ Enabled

Polling Interval 1024 sec

CONFIGURING TIME SERVERS

Use the System > Time (Configure Time Server) pages to specify the IP address for NTP/SNTP time servers, or to set the authentication key for NTP time servers.

SPECIFYING SNTP TIME SERVERS

Use the System > Time (Configure Time Server – Configure SNTP Server) page to specify the IP address for up to three SNTP time servers.

CLI REFERENCES

- "sntp server" on page 946

PARAMETERS

The following parameters are displayed:

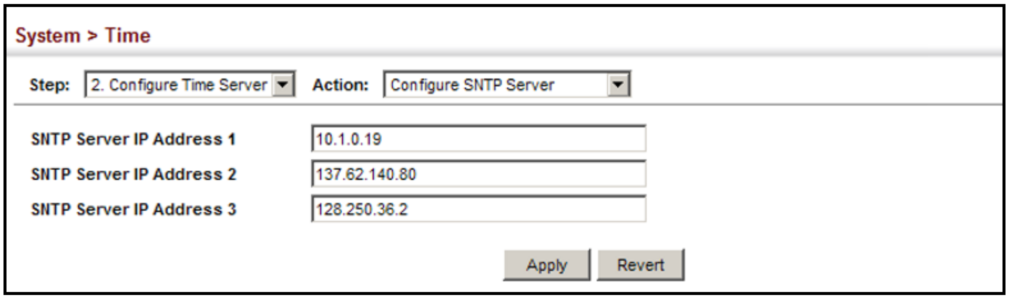
- **SNTP Server IP Address** – Sets the IPv4 or IPv6 address for up to three time servers. The switch attempts to update the time from the first server, if this fails it attempts an update from the next server in the sequence.

WEB INTERFACE

To set the SNTP time servers:

1. Click System, then Time.
2. Select Configure Time Server from the Step list.
3. Select Configure SNTP Server from the Action list.
4. Enter the IP address of up to three time servers.
5. Click Apply.

Figure 15: Specifying SNTP Time Servers



Step: 2. Configure Time Server
Action: Configure SNTP Server

SNTP Server IP Address 1: 10.1.0.19
SNTP Server IP Address 2: 137.62.140.80
SNTP Server IP Address 3: 128.250.36.2

SPECIFYING NTP TIME SERVERS

Use the System > Time (Configure Time Server – Add NTP Server) page to add the IP address for up to 50 NTP time servers.

CLI REFERENCES

- "ntp server" on page 950

PARAMETERS

The following parameters are displayed:

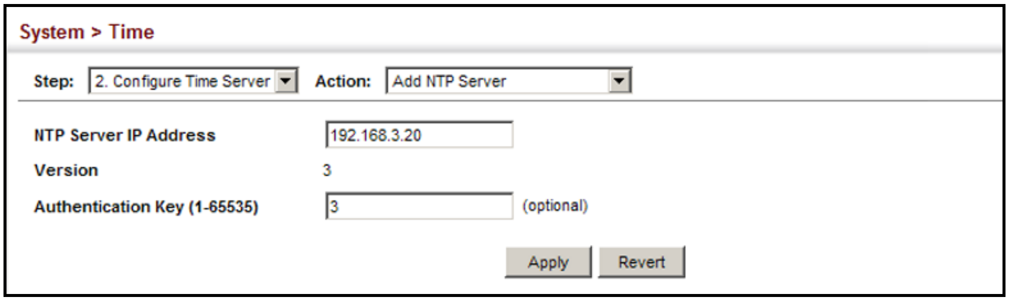
- **NTP Server IP Address** – Adds the IPv4 or IPv6 address for up to 50 time servers. The switch will poll the specified time servers for updates when the clock maintenance type is set to NTP on the System > Time (Configure General) page. It issues time synchronization requests at a fixed interval of 1024 seconds. The switch will poll all the time servers configured, the responses received are filtered and compared to determine the most reliable and accurate time update for the switch.
- **Version** – Specifies the NTP version supported by the server. (Fixed: Version 3)
- **Authentication Key** – Specifies the number of the key in the NTP Authentication Key List to use for authentication with the configured server. NTP authentication is optional. If enabled on the System > Time (Configure General) page, you must also configure at least one key on the System > Time (Add NTP Authentication Key) page. (Range: 1-65535)

WEB INTERFACE

To add an NTP time server to the server list:

1. Click System, then Time.
2. Select Configure Time Server from the Step list.
3. Select Add NTP Server from the Action list.
4. Enter the IP address of an NTP time server, and specify the index of the authentication key if authentication is required.
5. Click Apply.

Figure 16: Adding an NTP Time Server



System > Time

Step: 2. Configure Time Server Action: Add NTP Server

NTP Server IP Address: 192.168.3.20

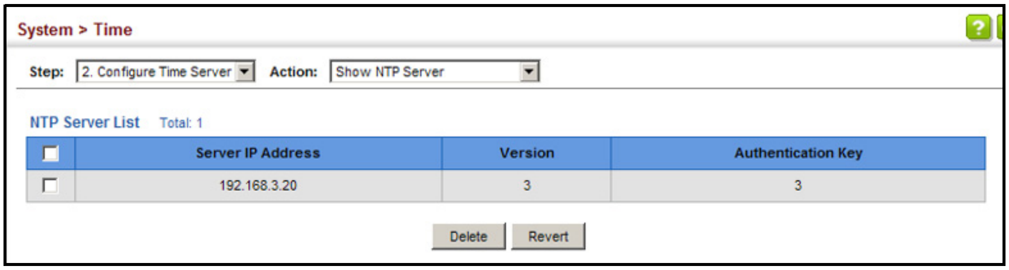
Version: 3

Authentication Key (1-65535): 3 (optional)

To show the list of configured NTP time servers:

1. Click System, then Time.
2. Select Configure Time Server from the Step list.
3. Select Show NTP Server from the Action list.

Figure 17: Showing the NTP Time Server List



System > Time

Step: 2. Configure Time Server Action: Show NTP Server

NTP Server List Total: 1

□	Server IP Address	Version	Authentication Key
□	192.168.3.20	3	3

SPECIFYING NTP AUTHENTICATION KEYS

Use the System > Time (Configure Time Server – Add NTP Authentication Key) page to add an entry to the authentication key list.

CLI REFERENCES

- "ntp authentication-key" on page 948

PARAMETERS

The following parameters are displayed:

- **Authentication Key** – Specifies the number of the key in the NTP Authentication Key List to use for authentication with a configured server. NTP authentication is optional. When enabled on the System > Time (Configure General) page, you must also configure at least one key on this page. Up to 255 keys can be configured on the switch. (Range: 1-65535)
- **Key Context** – An MD5 authentication key string. The key string can be up to 32 case-sensitive printable ASCII characters (no spaces).

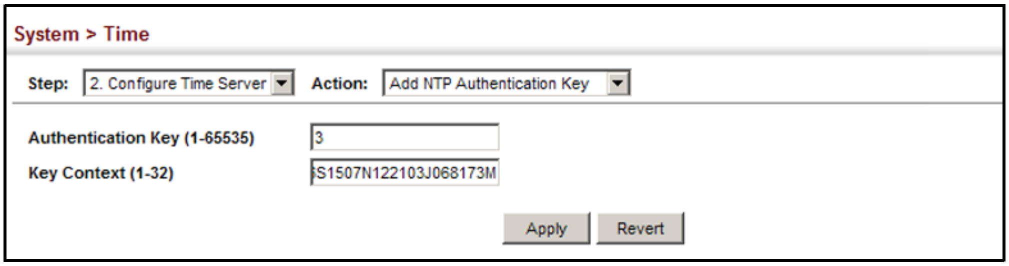
  NTP authentication key numbers and values must match on both the server and client.

WEB INTERFACE

To add an entry to NTP authentication key list:

1. Click System, then Time.
2. Select Configure Time Server from the Step list.
3. Select Add NTP Authentication Key from the Action list.
4. Enter the index number and MD5 authentication key string.
5. Click Apply.

Figure 18: Adding an NTP Authentication Key



System > Time

Step: 2. Configure Time Server

Action: Add NTP Authentication Key

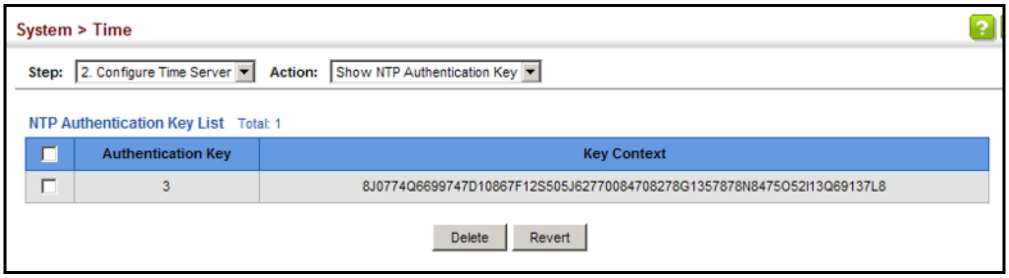
Authentication Key (1-65535): 3

Key Context (1-32): S1507N122103J068173M

To show the list of configured NTP authentication keys:

1. Click System, then Time.
2. Select Configure Time Server from the Step list.
3. Select Show NTP Authentication Key from the Action list.

Figure 19: Showing the NTP Authentication Key List



System > Time

Step: 2. Configure Time Server

Action: Show NTP Authentication Key

NTP Authentication Key List Total: 1

□	Authentication Key	Key Context
□	3	8J0774Q6699747D10867F12S505J62770084708278G1357878N8475052I13Q69137L8

SETTING THE TIME ZONE

Use the System > Time (Configure Time Zone) page to set the time zone. SNTP uses Coordinated Universal Time (or UTC, formerly Greenwich Mean Time, or GMT) based on the time at the Earth's prime meridian, zero degrees longitude, which passes through Greenwich, England. To display a time corresponding to your local time, you must indicate the number of hours and minutes your time zone is west (before) or east (after) of UTC. You can choose one of the 80 predefined time zone definitions, or your can manually configure the parameters for your local time zone.

CLI REFERENCES

- "clock timezone" on page 955

PARAMETERS

The following parameters are displayed:

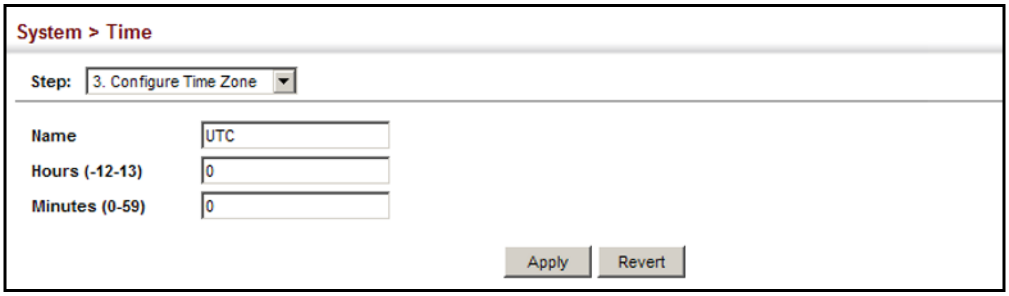
- **Name** – Assigns a name to the time zone. (Range: 1-30 characters)
- **Hours** (-12-13) – The number of hours before or after UTC. The maximum value before UTC is 12. The maximum value after UTC is 13.
- **Minutes** (0-59) – The number of minutes before/after UTC.

WEB INTERFACE

To set your local time zone:

1. Click System, then Time.
2. Select Configure Time Zone from the Step list.
3. Set the offset for your time zone relative to the UTC in hours and minutes.
4. Click Apply.

Figure 20: Setting the Time Zone



System > Time

Step: 3. Configure Time Zone

Name: UTC
Hours (-12-13): 0
Minutes (0-59): 0

CONFIGURING THE CONSOLE PORT

Use the System > Console menu to configure connection parameters for the switch’s console port. You can access the onboard configuration program by attaching a VT100 compatible device to the switch’s serial console port. Management access through the console port is controlled by various parameters, including a password (only configurable through the CLI), time outs, and basic communication settings. Note that these parameters can be configured via the web or CLI interface.

CLI REFERENCES

- "Line" on page 923

PARAMETERS

The following parameters are displayed:

- **Login Timeout** – Sets the interval that the system waits for a user to log into the CLI. If a login attempt is not detected within the timeout interval, the connection is terminated for the session. (Range: 10-300 seconds; Default: 300 seconds)

- **Exec Timeout** – Sets the interval that the system waits until user input is detected. If user input is not detected within the timeout interval, the current session is terminated. (Range: 60-65535 seconds; Default: 600 seconds)

- **Password Threshold** – Sets the password intrusion threshold, which limits the number of failed logon attempts. When the logon attempt threshold is reached, the system interface becomes silent for a specified amount of time (set by the Silent Time parameter) before allowing the next logon attempt. (Range: 1-120; Default: 3 attempts)

- **Silent Time** – Sets the amount of time the management console is inaccessible after the number of unsuccessful logon attempts has been exceeded. (Range: 1-65535 seconds; Default: Disabled)

- **Data Bits** – Sets the number of data bits per character that are interpreted and generated by the console port. If parity is being generated, specify 7 data bits per character. If no parity is required, specify 8 data bits per character. (Default: 8 bits)

- **Stop Bits** – Sets the number of the stop bits transmitted per byte. (Range: 1-2; Default: 1 stop bit)

- **Parity** – Defines the generation of a parity bit. Communication protocols provided by some terminals can require a specific parity bit setting. Specify Even, Odd, or None. (Default: None)

- **Speed** – Sets the terminal line’s baud rate for transmit (to terminal) and receive (from terminal). Set the speed to match the baud rate of the device connected to the serial port. (Range: 9600, 19200, 38400, 57600, or 115200 baud; Default: 115200 baud)

NOTE: The password for the console connection can only be configured through the CLI (see "password" on page 928).

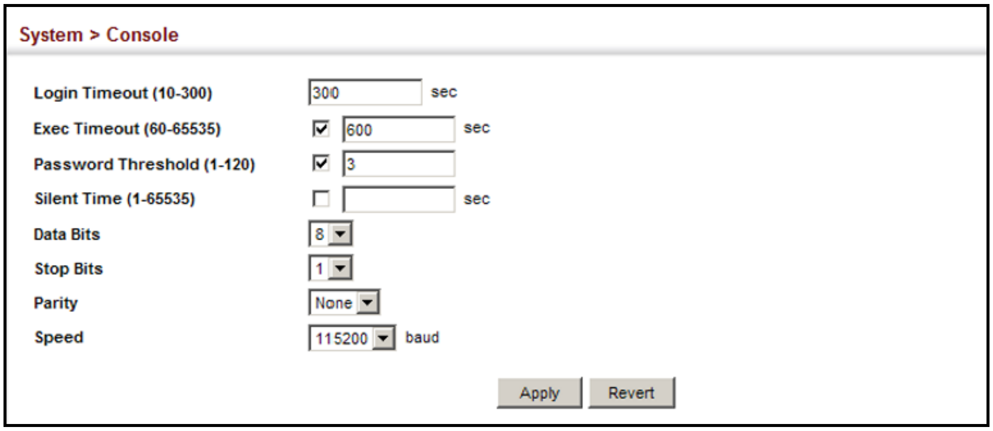
NOTE: Password checking can be enabled or disabled for logging in to the console connection (see "login" on page 926). You can select authentication by a single global password as configured for the password command, or by passwords set up for specific user-name accounts. The default is for local passwords configured on the switch.

WEB INTERFACE

To configure parameters for the console port:

1. Click System, then Console.
2. Specify the connection parameters as required.
3. Click Apply

Figure 21: Console Port Settings



System > Console

Login Timeout (10-300)	300	sec
Exec Timeout (60-65535)	☑ 600	sec
Password Threshold (1-120)	☑ 3	
Silent Time (1-65535)	☐	sec
Data Bits	8	
Stop Bits	1	
Parity	None	
Speed	115200	baud

CONFIGURING TELNET SETTINGS

Use the System > Telnet menu to configure parameters for accessing the CLI over a Telnet connection. You can access the onboard configuration program over the network using Telnet (i.e., a virtual terminal). Management access via Telnet can be enabled/disabled and other parameters set, including the TCP port number, time outs, and a password. Note that the password is only configurable through the CLI.) These parameters can be configured via the web or CLI interface.

CLI REFERENCES

- "Line" on page 923
- "Telnet Server" on page 1055

PARAMETERS

The following parameters are displayed:

- **Telnet Status** – Enables or disables Telnet access to the switch. (Default: Enabled)
- **TCP Port** – Sets the TCP port number for Telnet on the switch. (Range: 1-65535; Default: 23)
- **Max Sessions** – Sets the maximum number of Telnet sessions that can simultaneously connect to this system. (Range: 0-8; Default: 8)

  A maximum of eight sessions can be concurrently opened for Telnet and Secure Shell (i.e., both Telnet and SSH share a maximum number of eight sessions).
- **Login Timeout** – Sets the interval that the system waits for a user to log into the CLI. If a login attempt is not detected within the timeout interval, the connection is terminated for the session. (Range: 10-300 seconds; Default: 300 seconds)
- **Exec Timeout** – Sets the interval that the system waits until user input is detected. If user input is not detected within the timeout interval, the current session is terminated. (Range: 60-65535 seconds; Default: 600 seconds)
- **Password Threshold** – Sets the password intrusion threshold, which limits the number of failed logon attempts. When the logon attempt threshold is reached, the system interface becomes silent for a specified amount of time (set by the Silent Time parameter) before allowing the next logon attempt. (Range: 1-120; Default: 3 attempts)
- **Silent Time** – Sets the amount of time the management interface is inaccessible after the number of unsuccessful logon attempts has been exceeded. (Range: 1-65535 seconds; Default: Disabled)

NOTE: Password checking can be enabled or disabled for login to the console connection (see "login" on page 926). You can select authentication by a single global password as configured for the password command, or by passwords set up for specific user-name accounts. The default is for local passwords configured on the switch.

WEB INTERFACE

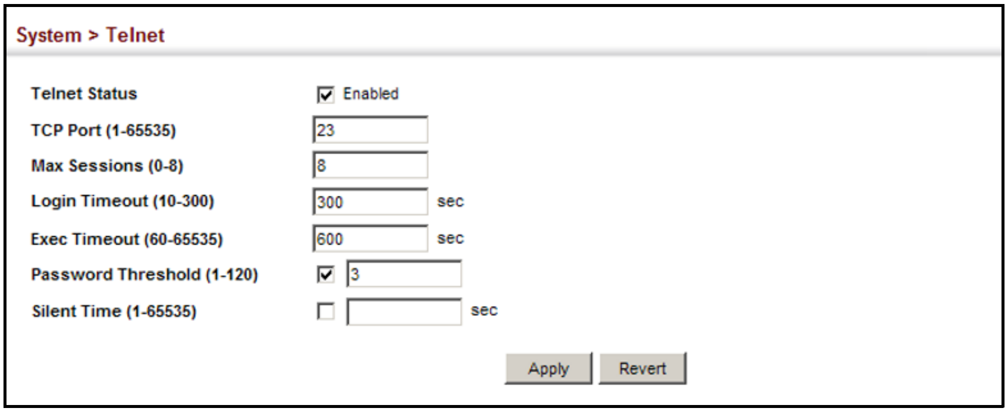
To configure parameters for the console port:

1. Click System, then Telnet.

2. Specify the connection parameters as required.

3. Click Apply

Figure 22: Telnet Connection Settings



System > Telnet

Telnet Status ☑ Enabled
TCP Port (1-65535) 23
Max Sessions (0-8) 8
Login Timeout (10-300) 300 sec
Exec Timeout (60-65535) 600 sec
Password Threshold (1-120) ☑ 3
Silent Time (1-65535) □ sec

DISPLAYING CPU UTILIZATION

Use the System > CPU Utilization page to display information on CPU utilization.

CLI REFERENCES

- "show process cpu" on page 904

PARAMETERS

The following parameters are displayed:

- **Time Interval** – The interval at which to update the displayed utilization rate. (Options: 1, 5, 10, 30, 60 seconds; Default: 1 second)

- **CPU Utilization** – CPU utilization over specified interval.

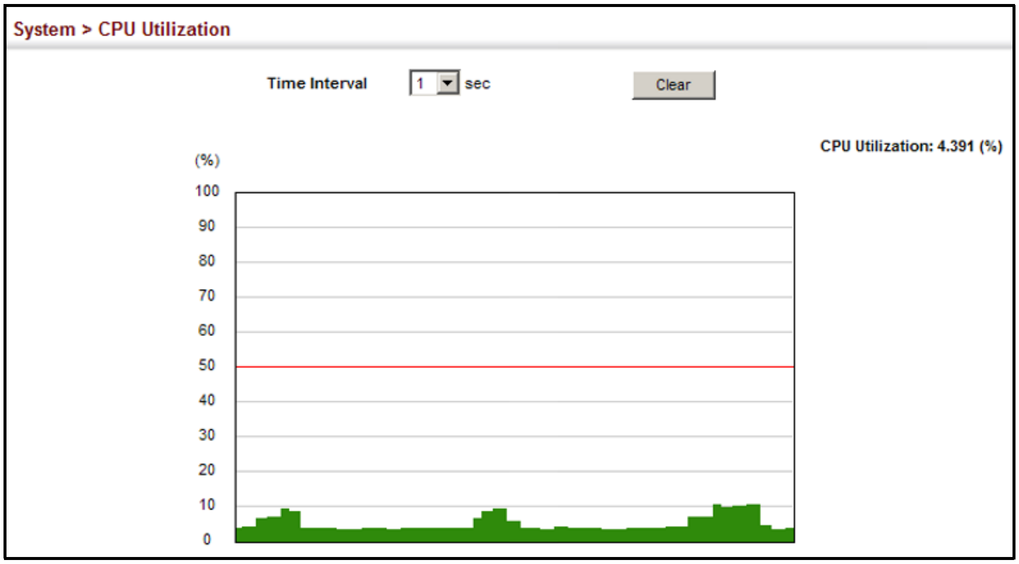
WEB INTERFACE

To display CPU utilization:

1. Click System, then CPU Utilization.

2. Change the update interval if required. Note that the interval is changed as soon as a new setting is selected.

Figure 23: Displaying CPU Utilization



System > CPU Utilization

Time Interval 1 sec

CPU Utilization: 4.391 (%)

DISPLAYING MEMORY UTILIZATION

Use the System > Memory Status page to display memory utilization parameters.

CLI REFERENCES

- "show memory" on page 903

PARAMETERS

The following parameters are displayed:

- **Free Size** – The amount of memory currently free for use.

- **Used Size** – The amount of memory allocated to active processes.

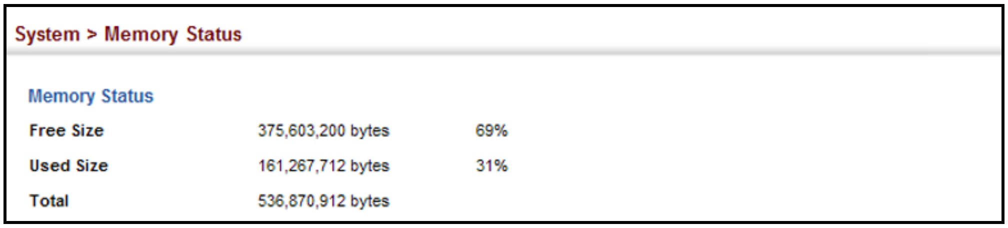
- **Total** – The total amount of system memory.

WEB INTERFACE

To display memory utilization:

1. Click System, then Memory Status.

Figure 24: Displaying Memory Utilization



System > Memory Status

Memory Status

Free Size	375,603,200 bytes	69%
Used Size	161,267,712 bytes	31%
Total	536,870,912 bytes	

RESETTING THE SYSTEM

Use the System > Reset menu to restart the switch immediately, at a specified time, after a specified delay, or at a periodic interval.

CLI REFERENCES

- "reload (Privileged Exec)" on page 888
- "reload (Global Configuration)" on page 884
- "show reload" on page 889

COMMAND USAGE

- This command resets the entire system.
- When the system is restarted, it will always run the Power-On Self-Test. It will also retain all configuration information stored in non-volatile memory by the copy running-config startup-config command (see "copy" on page 914).

PARAMETERS

The following parameters are displayed:

System Reload Information

- Reload Settings – Displays information on the next scheduled reload and selected reload mode as shown in the following example:

  "The switch will be rebooted at March 9 12:00:00 2012. Remaining
  Time: 0 days, 2 hours, 46 minutes, 5 seconds.
  Reloading switch regularly time: 12:00 everyday."

- **Refresh** – Refreshes reload information. Changes made through the console or to system time may need to be refreshed to display the current settings.
- **Cancel** – Cancels the current settings shown in this field.

System Reload Configuration

- **Reset Mode** – Restarts the switch immediately or at the specified time(s).
  - **Immediately** – Restarts the system immediately.
  - **In** – Specifies an interval after which to reload the switch. (The specified time must be equal to or less than 24 days.)
    - *hours* – The number of hours, combined with the minutes, before the switch resets. (Range: 0-576)
    - *minutes* – The number of minutes, combined with the hours, before the switch resets. (Range: 0-59)
  - **At** – Specifies a time at which to reload the switch.
    - DD - The day of the month at which to reload. (Range: 01-31)
    - MM - The month at which to reload. (Range: 01-12)
    - YYYY - The year at which to reload. (Range: 1970-2037)
    - HH - The hour at which to reload. (Range: 00-23)
    - MM - The minute at which to reload. (Range: 00-59)
  - **Regularly** – Specifies a periodic interval at which to reload the switch.

    Time

    - HH - The hour at which to reload. (Range: 00-23)
    - MM - The minute at which to reload. (Range: 00-59)

    Period

    - Daily - Every day.
    - Weekly - Day of the week at which to reload. (Range: Sunday ... Saturday)
    - Monthly - Day of the month at which to reload. (Range: 1-31)

WEB INTERFACE

To restart the switch:

1. Click System, then Reset.

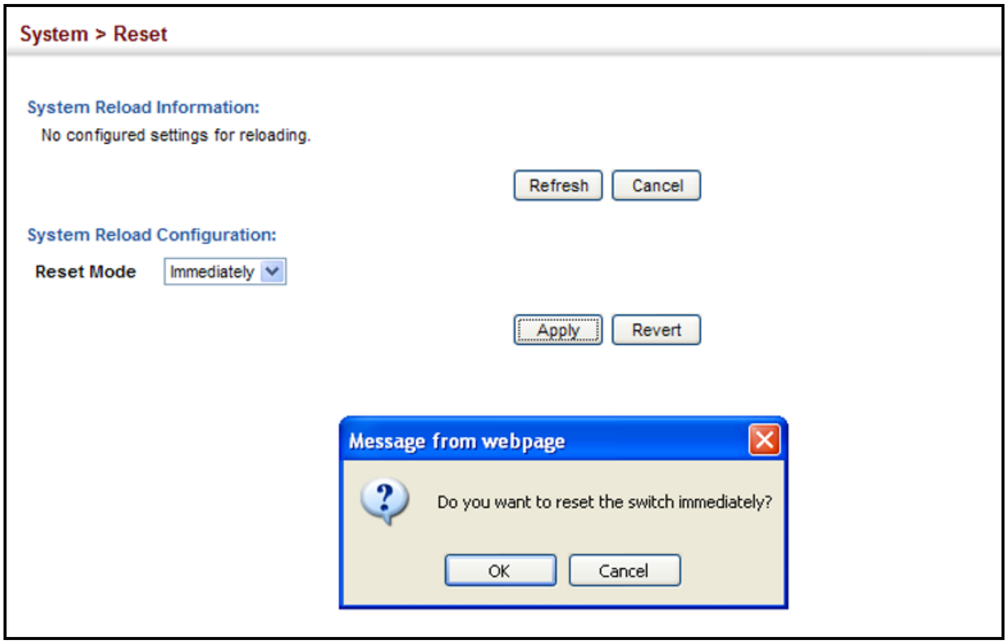
2. Select the required reset mode.

3. For any option other than to reset immediately, fill in the required parameters

4. Click Apply.

5. When prompted, confirm that you want reset the switch.

Figure 25: Restarting the Switch (Immediately)



System > Reset

System Reload Information:

No configured settings for reloading.

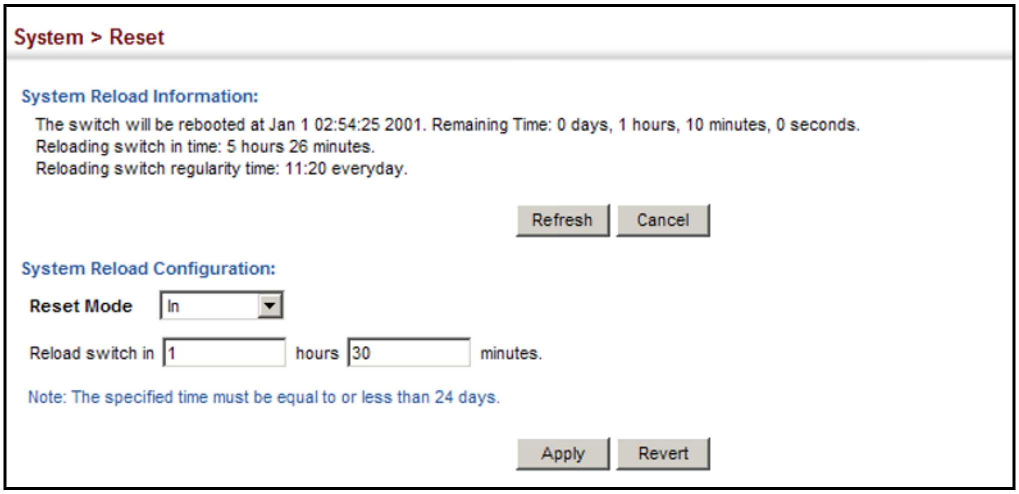
System Reload Configuration:

Reset Mode: Immediately

Message from webpage

Do you want to reset the switch immediately?

Figure 26: Restarting the Switch (In)



System > Reset

System Reload Information:

The switch will be rebooted at Jan 1 02:54:25 2001. Remaining Time: 0 days, 1 hours, 10 minutes, 0 seconds.
Reloading switch in time: 5 hours 26 minutes.
Reloading switch regularity time: 11:20 everyday.

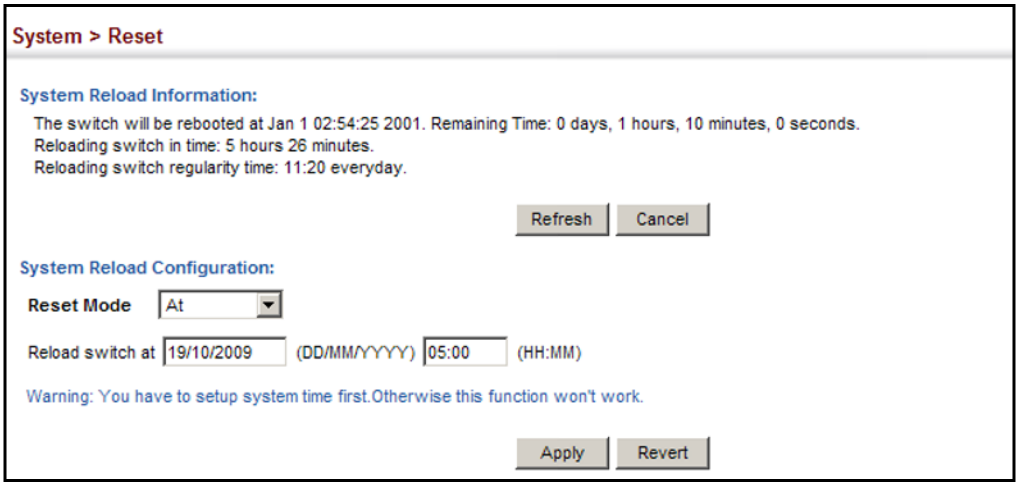
System Reload Configuration:

Reset Mode: In

Reload switch in 1 hours 30 minutes.

Note: The specified time must be equal to or less than 24 days.

Figure 27: Restarting the Switch (At)



System > Reset

System Reload Information:

The switch will be rebooted at Jan 1 02:54:25 2001. Remaining Time: 0 days, 1 hours, 10 minutes, 0 seconds.
Reloading switch in time: 5 hours 26 minutes.
Reloading switch regularity time: 11:20 everyday.

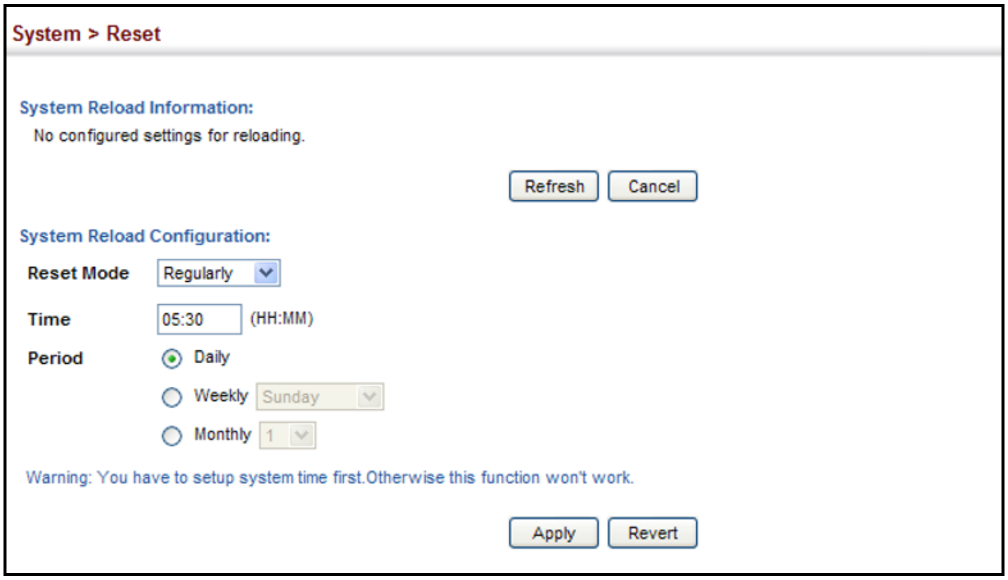
System Reload Configuration:

Reset Mode: At

Reload switch at 19/10/2009 (DD/MM/YYYY) 05:00 (HH:MM)

Warning: You have to setup system time first.Otherwise this function won't work.

Figure 28: Restarting the Switch (Regularly)



System > Reset

System Reload Information:

No configured settings for reloading.

System Reload Configuration:

Reset Mode: Regularly

Time: 05:30 (HH:MM)

Period: ● Daily
○ Weekly Sunday
○ Monthly 1

Warning: You have to setup system time first.Otherwise this function won't work.

5 Interface Configuration

This chapter describes the following topics:

- Port Configuration – Configures connection settings, including auto-negotiation, or manual setting of speed, duplex mode, and flow control.
- Local Port Mirroring – Sets the source and target ports for mirroring on the local switch.
- Remote Port Mirroring – Configures mirroring of traffic from remote switches for analysis at a destination port on the local switch.
- Displaying Statistics – Shows Interface, Etherlike, and RMON port statistics in table or chart form.
- Configuring History Sampling – Configures statistical sampling for the specified interfaces.
- Displaying Transceiver Data – Displays identifying information, and operational parameters for optical transceivers which support DDM.
- Configuring Transceiver Thresholds – Configures thresholds for alarm and warning messages for optical transceivers which support DDM.
- Trunk Configuration – Configures static or dynamic trunks.
- Traffic Segmentation – Configures the uplinks and down links to a segmented group of ports.
- VLAN Trunking – Configures a tunnel across one or more intermediate switches which pass traffic for VLAN groups to which they do not belong.

PORT CONFIGURATION

This section describes how to configure port connections, mirror traffic from one port to another, and run cable diagnostics.

CONFIGURING BY PORT LIST

Use the Interface > Port > General (Configure by Port List) page to enable/ disable an interface, set auto-negotiation and the interface capabilities to advertise, or manually fix the speed, duplex mode, and flow control.

CLI REFERENCES

- "Interface Commands" on page 1187

COMMAND USAGE

- Auto-negotiation must be disabled before you can configure or force an RJ-45 interface to use the Speed/Duplex mode or Flow Control options.

- When using auto-negotiation, the optimal settings will be negotiated between the link partners based on their advertised capabilities. To set the speed, duplex mode, or flow control under auto-negotiation, the required operation modes must be specified in the capabilities list for an interface.

- The Speed/Duplex mode is fixed at 1000full on the Gigabit SFP ports, and at 10Gfull on the 10 Gigabit ports. When auto-negotiation is enabled, the attributes which can be advertised include speed, duplex mode, flow control and symmetric pause frames.

Using Jumbo Frames

- Use the jumbo frame attribute on the System > Capability page to enable or disable jumbo frames for all Gigabit and 10 Gigabit Ethernet ports. Then specify the required MTU size for a specific interface on the port configuration page.

- The comparison of packet size against the configured port MTU considers only the incoming packet size, and is not affected by the fact that an ingress port is a tagged port or a QinQ ingress port. In other words, any additional size (for example, a tagged field of 4 bytes added by the chip) will not be considered when comparing the egress packet’s size against the configured MTU.

- When pinging the switch from an external device, information added for the Ethernet header can increase the packet size by at least 42 bytes for an untagged packet, and 46 bytes for a tagged packet. If the adjusted frame size exceeds the configured port MTU, the switch will not respond to the ping message.

- For other traffic types, calculation of overall frame size is basically the same, including the additional header fields SA(6) + DA(6) + Type(2) + VLAN-Tag(4) (for tagged packets, for untaqged packets, the 4-byte field will not be added by switch), and the payload. This should all be less than the configured port MTU, including the CRC at the end of the frame.

- For QinQ, the overall frame size is still calculated as described above, and does not add the length of the second tag to the frame.

PARAMETERS

These parameters are displayed:

- **Port** – Port identifier. (Range: 1-28)
- **Type** – Indicates the port type. (Options: 1000BASE SFP, 10GBASE XFP, 10GBASE SFP+)
- **Name** – Allows you to label an interface. (Range: 1-64 characters)
- **Admin** – Allows you to manually disable an interface. You can disable an interface due to abnormal behavior (e.g., excessive collisions), and then re-enable it after the problem has been resolved. You may also disable an interface for security reasons. (Default: Enabled)
- **Media Type** – Forces transceiver mode to use for SFP ports.
  - **None** - Mode is not forced. (This is the default for SFP ports.)
  - **SFP-Forced 100FX** - Always uses 1000BASE-FX mode.
  - **SFP-Forced 1000SFP** - Always uses 1000BASE SFP mode.
  - **SFP-Forced 10GSFP** - Always uses 10GBASE SFP mode.
- **Autonegotiation** (Port Capabilities) – Allows auto-negotiation to be enabled/disabled. When auto-negotiation is enabled, you need to specify the capabilities to be advertised. When auto-negotiation is disabled, you can force the settings for speed, mode, and flow control.The following capabilities are supported.
  - **1000f** (Gigabit ports only) - Supports 1000 Mbps full-duplex operation.
  - **10Gf** (10 Gigabit ports only) - Supports 10 Gbps full-duplex operation.
  - **Sym** (Gigabit ports only) - Check this item to transmit and receive pause frames.
  - **FC** (Gigabit ports only) - Flow control can eliminate frame loss by “blocking” traffic from end stations or segments connected directly to the switch when its buffers fill. When enabled, back pressure is used for half-duplex operation and IEEE 802.3-2005 (formally IEEE 802.3x) for full-duplex operation.

  Default: Autonegotiation enabled;
  Advertised capabilities for
  100Base-FX (SFP) – 100full

1000Base-SX/LX/LH (SFP) – 1000full
10GBase-SR/LR/ER (XFP/SFP+) - 10Gfull

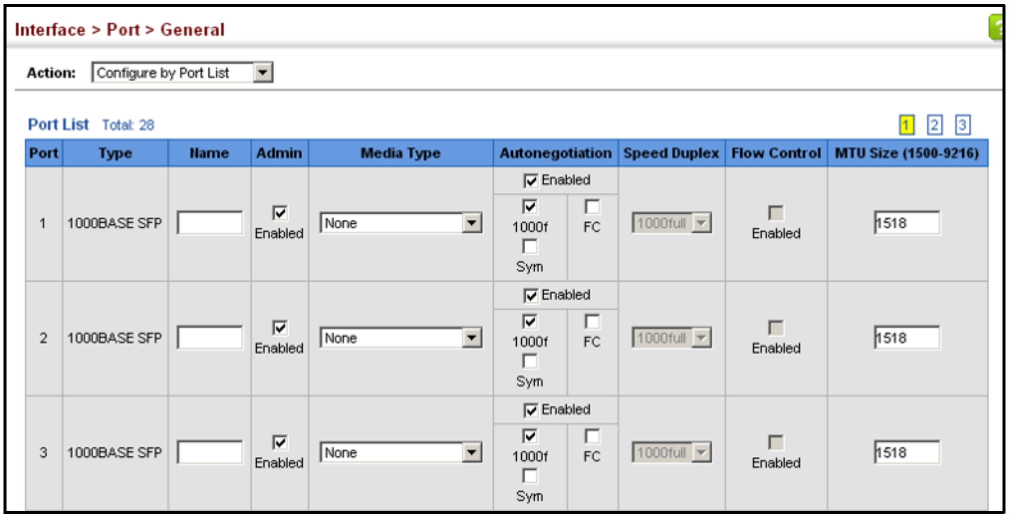
- **Speed/Duplex** – Allows you to manually set the port speed and duplex mode. (i.e., with auto-negotiation disabled)
- **Flow Control** – Allows automatic or manual selection of flow control.
- **MTU Size** – The maximum transfer unit (MTU) allowed for layer 2 packets crossing a Gigabit or 10 Gigabit Ethernet port or trunk. (Range: 1500-9216 bytes; Default: 1518 bytes)

WEB INTERFACE

To configure port connection parameters:

1. Click Interface, Port, General.
2. Select Configure by Port List from the Action List.
3. Modify the required interface settings.
4. Click Apply.

Figure 29: Configuring Connections by Port List



Interface > Port > General

Action: Configure by Port List

Port List Total: 28

Port	Type	Name	Admin	Media Type	Autonegotiation	Speed Duplex	Flow Control	MTU Size (1500-9216)
1	1000BASE SFP		☑ Enabled	None	☑ Enabled ☑ 1000f ☐ FC ☐ Sym	1000full	☐ Enabled	1518
2	1000BASE SFP		☑ Enabled	None	☑ Enabled ☑ 1000f ☐ FC ☐ Sym	1000full	☐ Enabled	1518
3	1000BASE SFP		☑ Enabled	None	☑ Enabled ☑ 1000f ☐ FC ☐ Sym	1000full	☐ Enabled	1518

CONFIGURING BY PORT RANGE

Use the Interface > Port > General (Configure by Port Range) page to enable/disable an interface, set auto-negotiation and the interface capabilities to advertise, or manually fix speed, duplex mode, and flow control.

For more information on command usage and a description of the parameters, refer to "Configuring by Port List" on page 182.

CLI REFERENCES

- "Interface Commands" on page 1187

WEB INTERFACE

To configure port connection parameters:

1. Click Interface, Port, General.

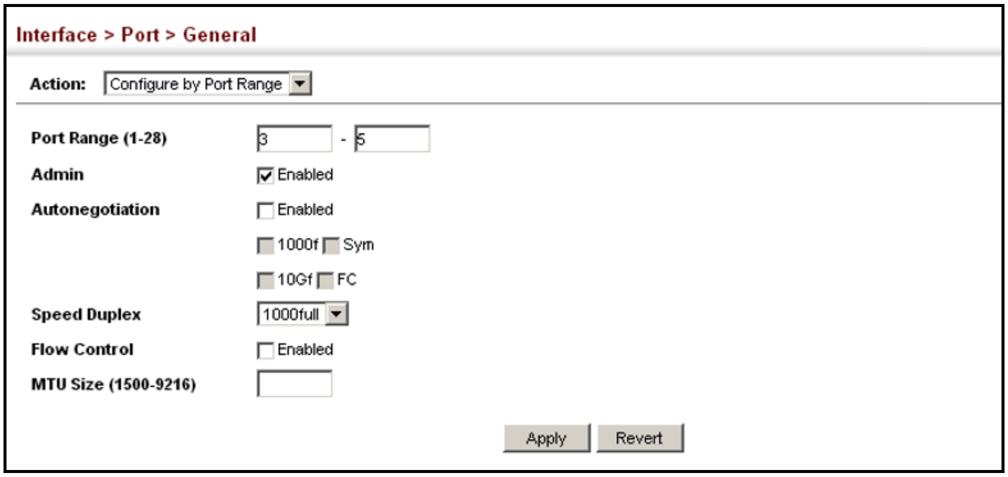
2. Select Configure by Port Range from the Action List.

3. Enter to range of ports to which your configuration changes apply.

4. Modify the required interface settings.

5. Click Apply.

Figure 30: Configuring Connections by Port Range



Interface > Port > General

Action: Configure by Port Range

Port Range (1-28) 3 - 5

Admin ☑ Enabled

Autonegotiation □ Enabled

□ 1000f □ Sym

□ 10Gf □ FC

Speed Duplex 1000full

Flow Control □ Enabled

MTU Size (1500-9216)

DISPLAYING CONNECTION STATUS

Use the Interface > Port > General (Show Information) page to display the current connection status, including link state, speed/duplex mode, flow control, and auto-negotiation.

CLI REFERENCES

- "show interfaces status" on page 1202

PARAMETERS

These parameters are displayed:

- **Port** – Port identifier.

- **Type** – Indicates the port type. (1000BASE SFP, 10GBASE XFP, 10GBASE SFP+)

- **Name** – Interface label.

- **Admin** – Shows if the port is enabled or disabled.

- **Oper Status** – Indicates if the link is Up or Down.

- **Media Type** – Media type used for combination ports.

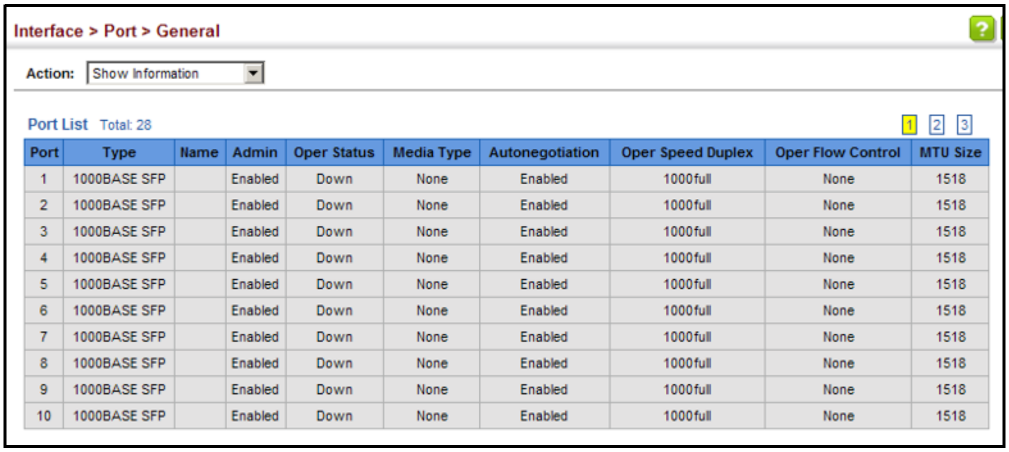
- **Autonegotiation** – Shows if auto-negotiation is enabled or disabled.
- **Oper Speed Duplex** – Shows the current speed and duplex mode.
- **Oper Flow Control** – Shows the flow control type used.
- **MTU Size** – The maximum transfer unit (MTU) allowed for layer 2 packets crossing a Gigabit or 10 Gigabit Ethernet port or trunk.

WEB INTERFACE

To display port connection parameters:

1. Click Interface, Port, General.
2. Select Show Information from the Action List.

Figure 31: Displaying Port Information



Interface > Port > General

Action: Show Information

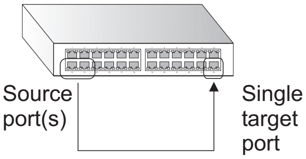
Port List Total: 28

Port	Type	Name	Admin	Oper Status	Media Type	Autonegotiation	Oper Speed Duplex	Oper Flow Control	MTU Size
1	1000BASE SFP		Enabled	Down	None	Enabled	1000full	None	1518
2	1000BASE SFP		Enabled	Down	None	Enabled	1000full	None	1518
3	1000BASE SFP		Enabled	Down	None	Enabled	1000full	None	1518
4	1000BASE SFP		Enabled	Down	None	Enabled	1000full	None	1518
5	1000BASE SFP		Enabled	Down	None	Enabled	1000full	None	1518
6	1000BASE SFP		Enabled	Down	None	Enabled	1000full	None	1518
7	1000BASE SFP		Enabled	Down	None	Enabled	1000full	None	1518
8	1000BASE SFP		Enabled	Down	None	Enabled	1000full	None	1518
9	1000BASE SFP		Enabled	Down	None	Enabled	1000full	None	1518
10	1000BASE SFP		Enabled	Down	None	Enabled	1000full	None	1518

CONFIGURING LOCAL PORT MIRRORING

Use the Interface > Port > Mirror page to mirror traffic from any source port to a target port for real-time analysis. You can then attach a logic analyzer or RMON probe to the target port and study the traffic crossing the source port in a completely unobtrusive manner.

Figure 32: Configuring Local Port Mirroring



CLI REFERENCES

- "Port Mirroring Commands" on page 1229

COMMAND USAGE

- Traffic can be mirrored from one or more source ports to a destination port on the same switch (local port mirroring as described in this section), or from one or more source ports on remote switches to a destination port on this switch (remote port mirroring as described in "Configuring Remote Port Mirroring" on page 188).

- Monitor port speed should match or exceed source port speed, otherwise traffic may be dropped from the monitor port.
- When mirroring port traffic, the target port must be included in the same VLAN as the source port when using MSTP (see "Spanning Tree Algorithm" on page 271).
- The destination port cannot be a trunk or trunk member port.
- Note that Spanning Tree BPDU packets are not mirrored to the target port.

PARAMETERS

These parameters are displayed:

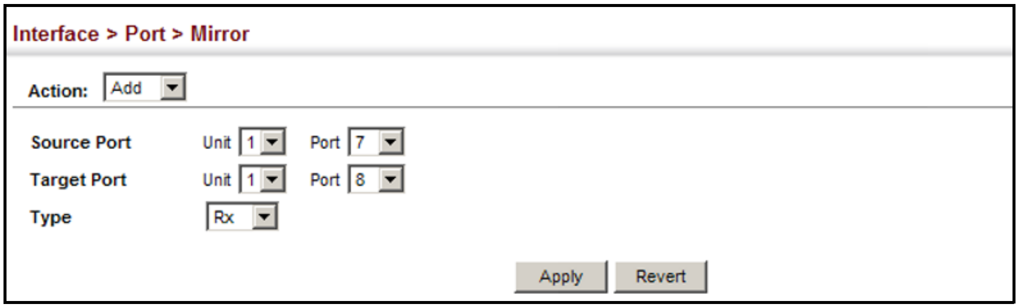
- **Source Port** – The port whose traffic will be monitored.
- **Target Port** – The port that will mirror the traffic on the source port.
- **Type** – Allows you to select which traffic to mirror to the target port, Rx (receive), Tx (transmit), or Both. (Default: Both)

WEB INTERFACE

To configure a local mirror session:

1. Click Interface, Port, Mirror.
2. Select Add from the Action List.
3. Specify the source port.
4. Specify the monitor port.
5. Specify the traffic type to be mirrored.
6. Click Apply.

Figure 33: Configuring Local Port Mirroring



Interface > Port > Mirror

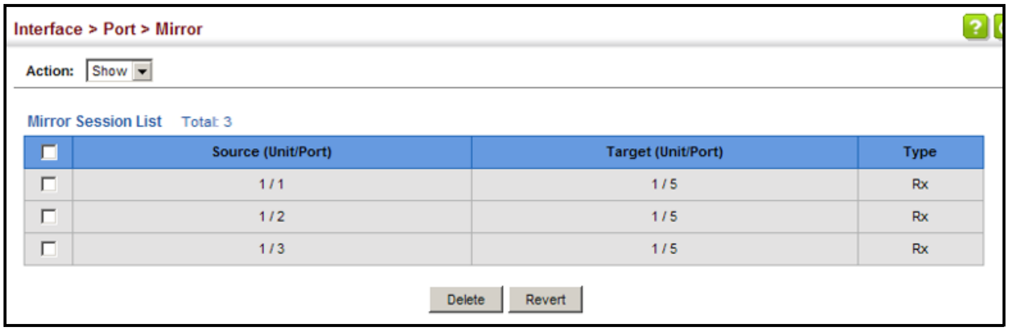
Action: Add

Source Port Unit 1 Port 7
Target Port Unit 1 Port 8
Type Rx

To display the configured mirror sessions:

1. Click Interface, Port, Mirror.
2. Select Show from the Action List.

Figure 34: Displaying Local Port Mirror Sessions



Interface > Port > Mirror

Action: Show

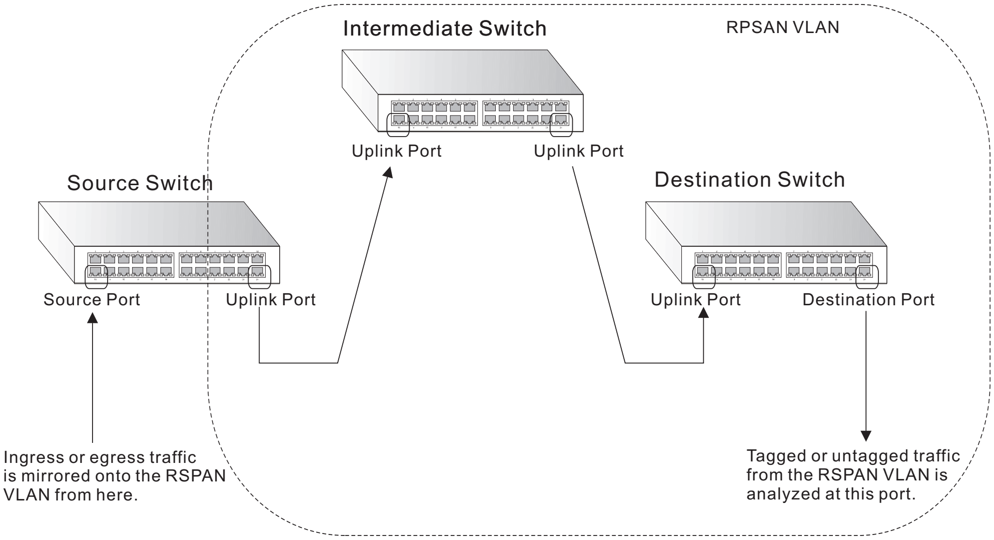
Mirror Session List Total: 3

□	Source (Unit/Port)	Target (Unit/Port)	Type
□	1 / 1	1 / 5	Rx
□	1 / 2	1 / 5	Rx
□	1 / 3	1 / 5	Rx

CONFIGURING REMOTE PORT MIRRORING

Use the Interface > RSPAN page to mirror traffic from remote switches for analysis at a destination port on the local switch. This feature, also called Remote Switched Port Analyzer (RSPAN), carries traffic generated on the specified source ports for each session over a user-specified VLAN dedicated to that RSPAN session in all participating switches. Monitored traffic from one or more sources is copied onto the RSPAN VLAN through IEEE 802.1Q trunk or hybrid ports that carry it to any RSPAN destination port monitoring the RSPAN VLAN as shown in the figure below.

Figure 35: Configuring Remote Port Mirroring



CLI REFERENCES

- "RSPAN Mirroring Commands" on page 1231

COMMAND USAGE

- Traffic can be mirrored from one or more source ports to a destination port on the same switch (local port mirroring as described in "Configuring Local Port Mirroring" on page 186), or from one or more source ports on remote switches to a destination port on this switch (remote port mirroring as described in this section).

- *Configuration Guidelines*

  Take the following step to configure an RSPAN session:

  1. Use the VLAN Static List (see "Configuring VLAN Groups" on page 228) to reserve a VLAN for use by RSPAN (marking the “Remote VLAN” field on this page. (Default VLAN 1 is prohibited.)

  2. Set up the source switch on the RSPAN configuration page by specifying the mirror session, the switch’s role (Source), the RSPAN VLAN, and the uplink port. Then specify the source port(s), and the traffic type to monitor (Rx, Tx or Both).

  3. Set up all intermediate switches on the RSPAN configuration page, entering the mirror session, the switch’s role (Intermediate), the RSPAN VLAN, and the uplink port(s).

  4. Set up the destination switch on the RSPAN configuration page by specifying the mirror session, the switch’s role (Destination), the destination port, whether or not the traffic exiting this port will be tagged or untagged, and the RSPAN VLAN. Then specify each uplink port where the mirrored traffic is being received.

- *RSPAN Limitations*

  The following limitations apply to the use of RSPAN on this switch:

  - *RSPAN Ports* – Only ports can be configured as an RSPAN source, destination, or uplink; static and dynamic trunks are not allowed. A port can only be configured as one type of RSPAN interface – source, destination, or uplink. Also, note that the source port and destination port cannot be configured on the same switch.

  - *Local/Remote Mirror* – The destination of a local mirror session (created on the Interface > Port > Mirror page) cannot be used as the destination for RSPAN traffic.

  - *Spanning Tree* – If the spanning tree is disabled, BPDUs will not be flooded onto the RSPAN VLAN.

  - MAC address learning is not supported on RSPAN uplink ports when RSPAN is enabled on the switch. Therefore, even if spanning tree is enabled after RSPAN has been configured, MAC address learning will still not be re-started on the RSPAN uplink ports.

  - *IEEE 802.1X* – RSPAN and 802.1X are mutually exclusive functions. When 802.1X is enabled globally, RSPAN uplink ports cannot be configured, even though RSPAN source and destination ports can still be configured. When RSPAN uplink ports are enabled on the switch, 802.1X cannot be enabled globally.

- *Port Security* – If port security is enabled on any port, that port cannot be set as an RSPAN uplink port, even though it can still be configured as an RSPAN source or destination port. Also, when a port is configured as an RSPAN uplink port, port security cannot be enabled on that port.

PARAMETERS

These parameters are displayed:

- **Session** – A number identifying this RSPAN session. (Range: 1-2)

  Only two mirror sessions are allowed, including both local and remote mirroring. If local mirroring is enabled (see page 186), then there is only one session available for RSPAN.

- **Operation Status** – Indicates whether or not RSPAN is currently functioning.

- **Switch Role** – Specifies the role this switch performs in mirroring traffic.

  - **None** – This switch will not participate in RSPAN.

  - **Source** - Specifies this device as the source of remotely mirrored traffic.

  - **Intermediate** - Specifies this device as an intermediate switch, transparently passing mirrored traffic from one or more sources to one or more destinations.

  - **Destination** - Specifies this device as a switch configured with a destination port which is to receive mirrored traffic for this session.

- **Remote VLAN** – The VLAN to which traffic mirrored from the source port will be flooded. The VLAN specified in this field must first be reserved for the RSPAN application using the VLAN > Static page (see page 228).

- **Uplink Port** – A port on any switch participating in RSPAN through which mirrored traffic is passed on to or received from the RSPAN VLAN.

  Only one uplink port can be configured on a source switch, but there is no limitation on the number of uplink ports configured on an intermediate or destination switch.

  Only destination and uplink ports will be assigned by the switch as members of the RSPAN VLAN. Ports cannot be manually assigned to an RSPAN VLAN through the VLAN > Static page. Nor can GVRP dynamically add port members to an RSPAN VLAN. Also, note that the VLAN > Static (Show) page will not display any members for an RSPAN VLAN, but will only show configured RSPAN VLAN identifiers.

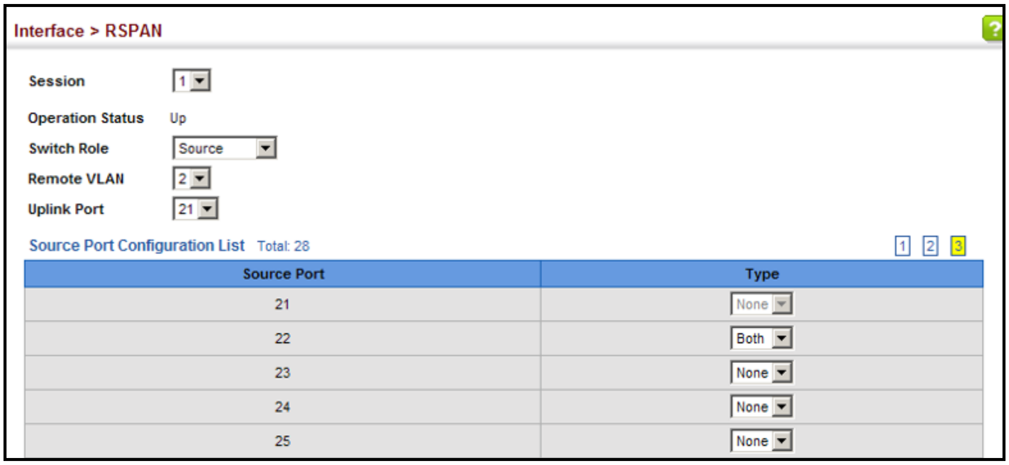
- **Type** – Specifies the traffic type to be mirrored remotely. (Options: Rx, Tx, Both)
- **Destination Port** – Specifies the destination port to monitor the traffic mirrored from the source ports. Only one destination port can be configured on the same switch per session, but a destination port can be configured on more than one switch for the same session. Also note that a destination port can still send and receive switched traffic, and participate in any Layer 2 protocols to which it has been assigned.
- **Tag** – Specifies whether or not the traffic exiting the destination port to the monitoring device carries the RSPAN VLAN tag.

WEB INTERFACE

To configure a remote mirror session:

1. Click Interface, RSPAN.
2. Set the Switch Role to None, Source, Intermediate, or Destination.
3. Configure the required settings for each switch participating in the RSPAN VLAN.
4. Click Apply.

Figure 36: Configuring Remote Port Mirroring (Source)



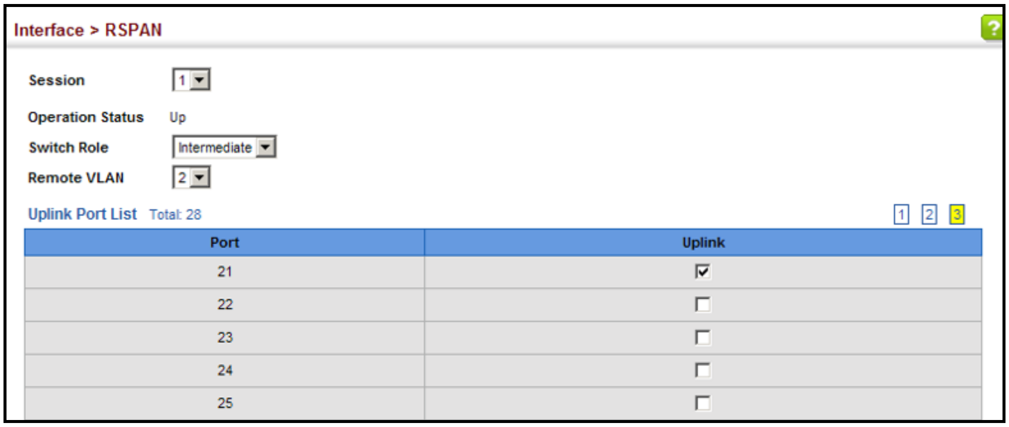
Interface > RSPAN

Session: 1
Operation Status: Up
Switch Role: Source
Remote VLAN: 2
Uplink Port: 21

Source Port Configuration List Total: 28

Source Port	Type
21	None
22	Both
23	None
24	None
25	None

Figure 37: Configuring Remote Port Mirroring (Intermediate)



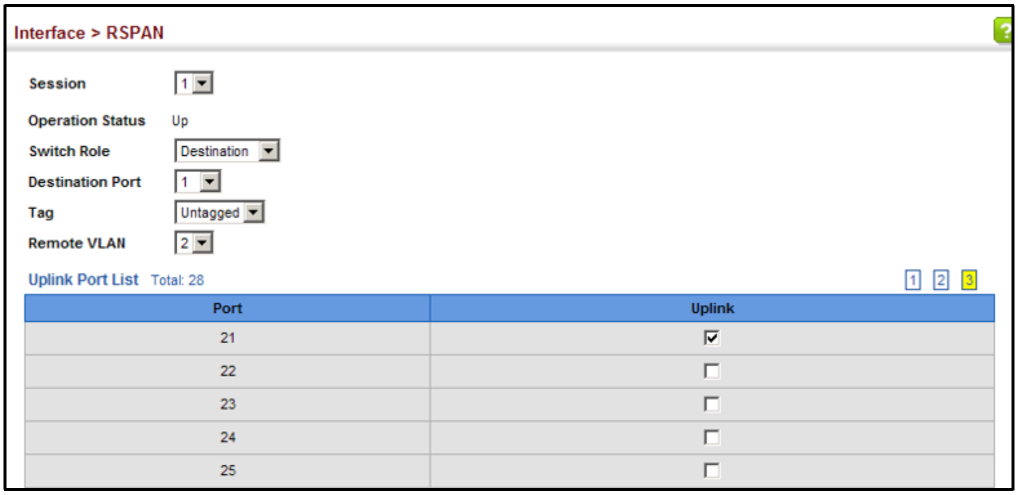
Interface > RSPAN

Session: 1
Operation Status: Up
Switch Role: Intermediate
Remote VLAN: 2

Uplink Port List Total: 28

Port	Uplink
21	☑
22	□
23	□
24	□
25	□

Figure 38: Configuring Remote Port Mirroring (Destination)



Interface > RSPAN

Session: 1
Operation Status: Up
Switch Role: Destination
Destination Port: 1
Tag: Untagged
Remote VLAN: 2

Uplink Port List Total: 28

Port	Uplink
21	☑
22	□
23	□
24	□
25	□

SHOWING PORT OR TRUNK STATISTICS

Use the Interface > Port/Trunk > Statistics or Chart page to display standard statistics on network traffic from the Interfaces Group and Ethernet-like MIBs, as well as a detailed breakdown of traffic based on the RMON MIB. Interfaces and Ethernet-like statistics display errors on the traffic passing through each port. This information can be used to identify potential problems with the switch (such as a faulty port or unusually heavy traffic). RMON statistics provide access to a broad range of statistics, including a total count of different frame types and sizes passing through each port. All values displayed have been accumulated since the last system reboot, and are shown as counts per second. Statistics are refreshed every 60 seconds by default.

NOTE: RMON groups 2, 3 and 9 can only be accessed using SNMP management software.

CLI REFERENCES

- "show interfaces counters" on page 1198

PARAMETERS

These parameters are displayed:

Table 7: Port Statistics

Parameter	Description
Interface Statistics	
Received Octets	The total number of octets received on the interface, including framing characters.
Transmitted Octets	The total number of octets transmitted out of the interface, including framing characters.
Received Errors	The number of inbound packets that contained errors preventing them from being deliverable to a higher-layer protocol.
Transmitted Errors	The number of outbound packets that could not be transmitted because of errors.
Received Unicast Packets	The number of subnetwork-unicast packets delivered to a higher-layer protocol.
Transmitted Unicast Packets	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.
Received Discarded Packets	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. One possible reason for discarding such a packet could be to free up buffer space.
Transmitted Discarded Packets	The number of outbound packets which were chosen to be discarded even though no errors had been detected to prevent their being transmitted. One possible reason for discarding such a packet could be to free up buffer space.
Received Multicast Packets	The number of packets, delivered by this sub-layer to a higher (sub-)layer, which were addressed to a multicast address at this sub-layer.
Transmitted Multicast Packets	The total number of packets that higher-level protocols requested be transmitted, and which were addressed to a multicast address at this sub-layer, including those that were discarded or not sent.
Received Broadcast Packets	The number of packets, delivered by this sub-layer to a higher (sub-)layer, which were addressed to a broadcast address at this sub-layer.
Transmitted Broadcast Packets	The total number of packets that higher-level protocols requested be transmitted, and which were addressed to a broadcast address at this sub-layer, including those that were discarded or not sent.
Received Unknown Packets	The number of packets received via the interface which were discarded because of an unknown or unsupported protocol.
Etherlike Statistics	
Single Collision Frames	The number of successfully transmitted frames for which transmission is inhibited by exactly one collision.
Multiple Collision Frames	A count of successfully transmitted frames for which transmission is inhibited by more than one collision.
Late Collisions	The number of times that a collision is detected later than 512 bit-times into the transmission of a packet.
Excessive Collisions	A count of frames for which transmission on a particular interface fails due to excessive collisions. This counter does not increment when the interface is operating in full-duplex mode.
Deferred Transmissions	A count of frames for which the first transmission attempt on a particular interface is delayed because the medium was busy.

Table 7: Port Statistics (Continued)

Parameter	Description
Frames Too Long	A count of frames received on a particular interface that exceed the maximum permitted frame size.
Alignment Errors	The number of alignment errors (missynchronized data packets).
FCS Errors	A count of frames received on a particular interface that are an integral number of octets in length but do not pass the FCS check. This count does not include frames received with frame-too-long or frame-too-short error.
SQE Test Errors	A count of times that the SQE TEST ERROR message is generated by the PLS sublayer for a particular interface.
Carrier Sense Errors	The number of times that the carrier sense condition was lost or never asserted when attempting to transmit a frame.
Internal MAC Receive Errors	A count of frames for which reception on a particular interface fails due to an internal MAC sublayer receive error.
Internal MAC Transmit Errors	A count of frames for which transmission on a particular interface fails due to an internal MAC sublayer transmit error.
RMON Statistics	
Drop Events	The total number of events in which packets were dropped due to lack of resources.
Jabbers	The total number of frames received that were longer than 1518 octets (excluding framing bits, but including FCS octets), and had either an FCS or alignment error.
Fragments	The total number of frames received that were less than 64 octets in length (excluding framing bits, but including FCS octets) and had either an FCS or alignment error.
Collisions	The best estimate of the total number of collisions on this Ethernet segment.
Received Octets	Total number of octets of data received on the network. This statistic can be used as a reasonable indication of Ethernet utilization.
Received Packets	The total number of packets (bad, broadcast and multicast) received.
Broadcast Packets	The total number of good packets received that were directed to the broadcast address. Note that this does not include multicast packets.
Multicast Packets	The total number of good packets received that were directed to this multicast address.
Undersize Packets	The total number of packets received that were less than 64 octets long (excluding framing bits, but including FCS octets) and were otherwise well formed.
Oversize Packets	The total number of packets received that were longer than 1518 octets (excluding framing bits, but including FCS octets) and were otherwise well formed.
64 Bytes Packets	The total number of packets (including bad packets) received and transmitted that were 64 octets in length (excluding framing bits but including FCS octets).
65-127 Byte Packets 128-255 Byte Packets 256-511 Byte Packets 512-1023 Byte Packets 1024-1518 Byte Packets 1519-1536 Byte Packets	The total number of packets (including bad packets) received and transmitted where the number of octets fall within the specified range (excluding framing bits but including FCS octets).

Table 7: Port Statistics (Continued)

Parameter	Description
Utilization Statistics	
Input Octets in kbits per second	Number of octets entering this interface in kbits/second.
Input Packets per second	Number of packets entering this interface per second.
Input Utilization	The input utilization rate for this interface.
Output Octets in kbits per second	Number of octets leaving this interface in kbits/second.
Output Packets per second	Number of packets leaving this interface per second.
Output Utilization	The output utilization rate for this interface.

WEB INTERFACE

To show a list of port statistics:

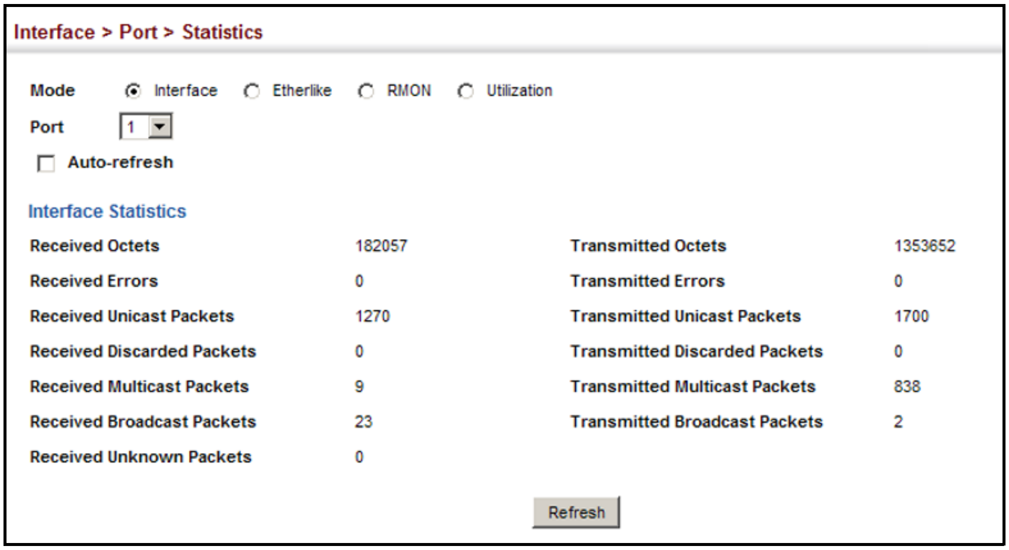
1. Click Interface, Port, Statistics.

2. Select the statistics mode to display (Interface, Etherlike, RMON or Utilization).

3. Select a port from the drop-down list.

4. Use the Refresh button at the bottom of the page if you need to update the screen.

Figure 39: Showing Port Statistics (Table)



Interface > Port > Statistics

Mode ● Interface ○ Etherlike ○ RMON ○ Utilization

Port 1

□ Auto-refresh

Interface Statistics

Received Octets	182057	Transmitted Octets	1353652
Received Errors	0	Transmitted Errors	0
Received Unicast Packets	1270	Transmitted Unicast Packets	1700
Received Discarded Packets	0	Transmitted Discarded Packets	0
Received Multicast Packets	9	Transmitted Multicast Packets	838
Received Broadcast Packets	23	Transmitted Broadcast Packets	2
Received Unknown Packets	0		

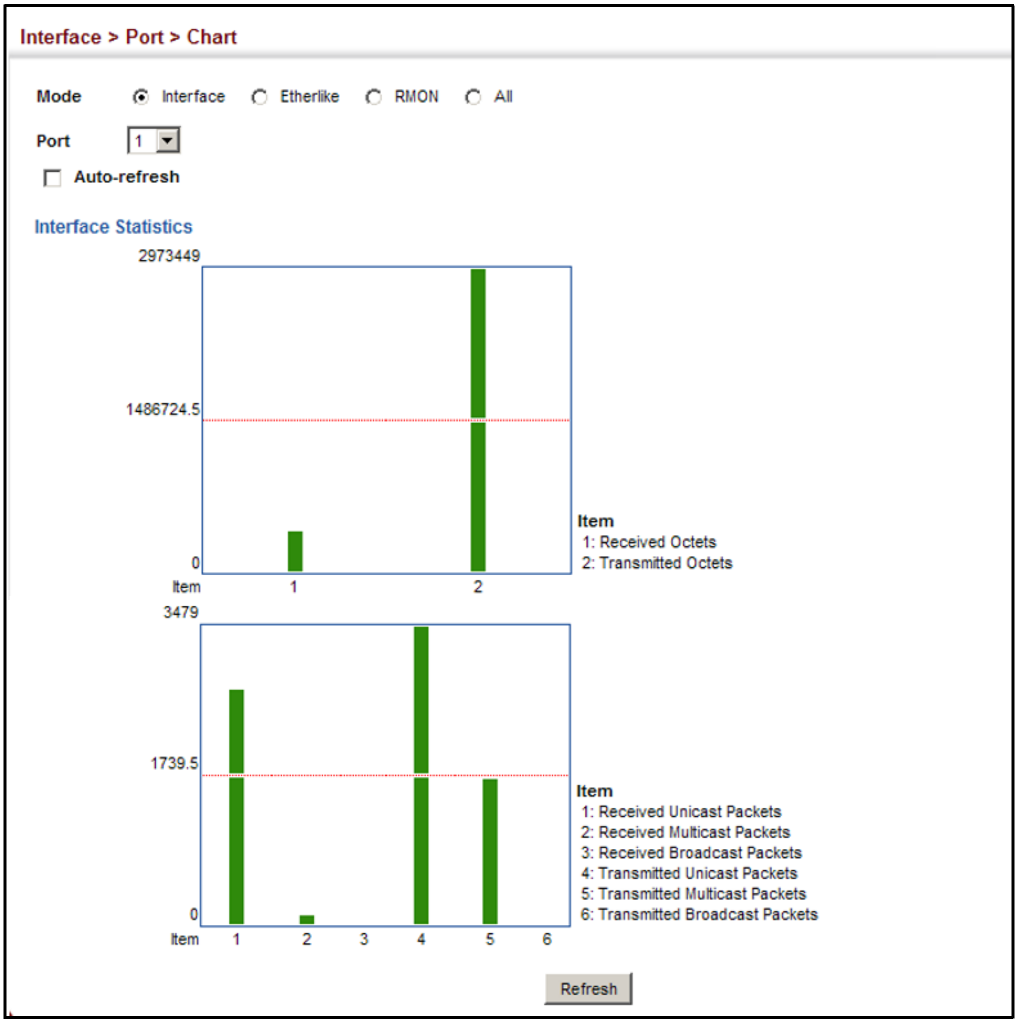
To show a chart of port statistics:

1. Click Interface, Port, Chart.

2. Select the statistics mode to display (Interface, Etherlike, RMON or All).

3. If Interface, Etherlike, RMON statistics mode is chosen, select a port from the drop-down list. If All (ports) statistics mode is chosen, select the statistics type to display.

Figure 40: Showing Port Statistics (Chart)



Interface > Port > Chart

Mode ● Interface ○ Etherlike ○ RMON ○ All

Port 1

□ Auto-refresh

Interface Statistics

2973449
1486724.5
0
Item
1
2
Item
1: Received Octets
2: Transmitted Octets
3479
1739.5
0
Item
1
2
3
4
5
6
Item
1: Received Unicast Packets
2: Received Multicast Packets
3: Received Broadcast Packets
4: Transmitted Unicast Packets
5: Transmitted Multicast Packets
6: Transmitted Broadcast Packets
Refresh

CONFIGURING HISTORY SAMPLING

Use the Interface > Port > History or Interface > Trunk > History page to configure a periodic sampling of statistics, specifying the sampling interval and number of samples.

CLI REFERENCES

- "history" on page 1192
- "show interfaces history" on page 1199

COMMAND USAGE

For a description of the statistics displayed on these pages, see "Showing Port or Trunk Statistics" on page 192.

PARAMETERS

These parameters are displayed:

Add

- **Port** – Port number. (Range: 1-28)
- **History Name** – Name of sample interval. (Range: 1-32 characters)
- **Interval** - The interval for sampling statistics. (Range: 1-86400 minutes)
- **Requested Buckets** - The number of samples to take. (Range: 1-96)

Show

- **Port** – Port number. (Range: 1-28)
- **History Name** – Name of sample interval. (Default settings: 15min, 1day)
- **Interval** - The interval for sampling statistics.
- **Requested Buckets** - The number of samples to take.

Show Details

- **Mode**
  - **Status** – Shows the sample parameters.
  - **Current Entry** – Shows current statistics for the specified port and named sample.
  - **Input Previous Entries** – Shows statistical history for ingress traffic.
  - **Output Previous Entries** – Shows statistical history for egress traffic.
- **Port** – Port number. (Range: 1-28)
- **Name** – Name of sample interval.

WEB INTERFACE

To configure a periodic sample of statistics:

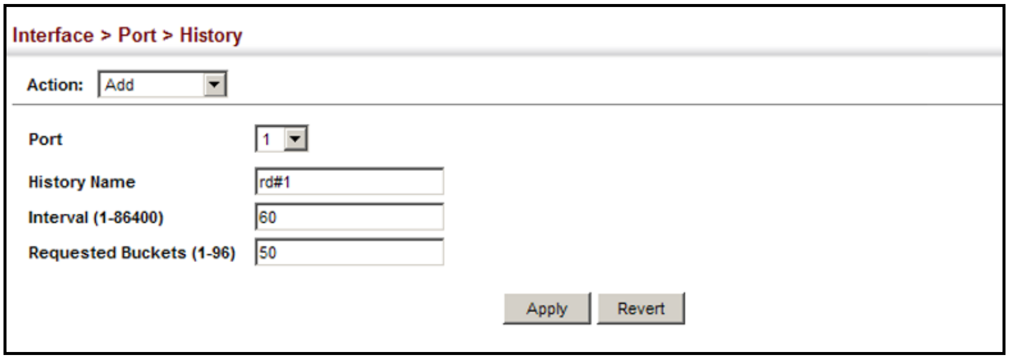
1. Click Interface, Port, Statistics, or Interface, Trunk, Statistics.
2. Select Add from the Action menu.

3. Select an interface from the Port or Trunk list.

4. Enter the sample name, the interval, and the number of buckets requested.

5. Click Apply.

Figure 41: Configuring a History Sample



Interface > Port > History

Action: Add

Port	1
History Name	rd#1
Interval (1-86400)	60
Requested Buckets (1-96)	50

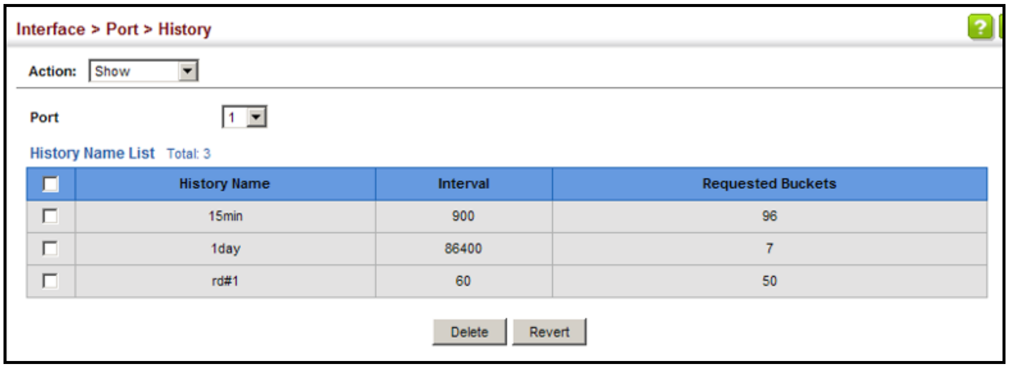
To show the configured entries for a history sample:

1. Click Interface, Port, Statistics, or Interface, Trunk, Statistics.

2. Select Show from the Action menu.

3. Select an interface from the Port or Trunk list.

Figure 42: Showing Entries for History Sampling



Interface > Port > History

Action: Show

Port 1

History Name List Total: 3

□	History Name	Interval	Requested Buckets
□	15min	900	96
□	1day	86400	7
□	rd#1	60	50

To show the configured parameters for a sampling entry:

1. Click Interface, Port, Statistics, or Interface, Trunk, Statistics.

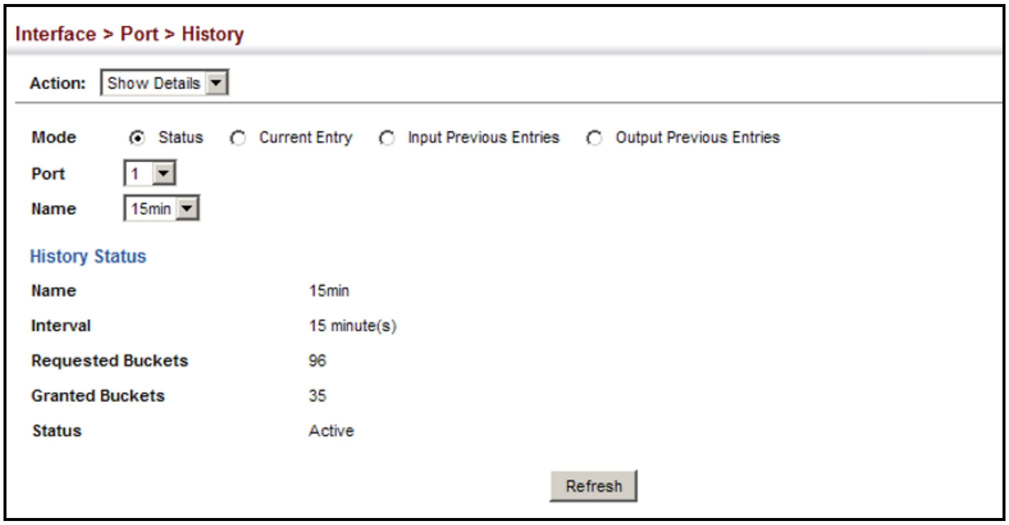
2. Select Show Details from the Action menu.

3. Select Status from the options for Mode.

4. Select an interface from the Port or Trunk list.

5. Select an sampling entry from the Name list.

Figure 43: Showing Status of Statistical History Sample



Interface > Port > History

Action: Show Details

Mode ● Status ○ Current Entry ○ Input Previous Entries ○ Output Previous Entries

Port 1

Name 15min

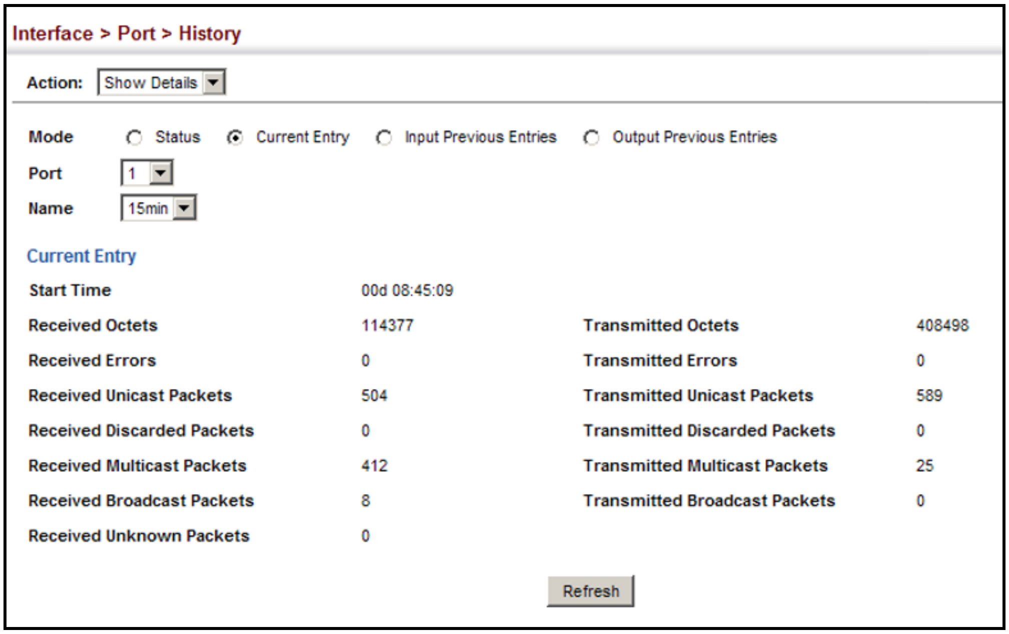
History Status

Name	15min
Interval	15 minute(s)
Requested Buckets	96
Granted Buckets	35
Status	Active

To show statistics for the current interval of a sample entry:

1. Click Interface, Port, Statistics, or Interface, Trunk, Statistics.
2. Select Show Details from the Action menu.
3. Select Current Entry from the options for Mode.
4. Select an interface from the Port or Trunk list.
5. Select an sampling entry from the Name list.

Figure 44: Showing Current Statistics for a History Sample



Interface > Port > History

Action: Show Details

Mode ○ Status ● Current Entry ○ Input Previous Entries ○ Output Previous Entries

Port 1

Name 15min

Current Entry

Start Time	00d 08:45:09		
Received Octets	114377	Transmitted Octets	408498
Received Errors	0	Transmitted Errors	0
Received Unicast Packets	504	Transmitted Unicast Packets	589
Received Discarded Packets	0	Transmitted Discarded Packets	0
Received Multicast Packets	412	Transmitted Multicast Packets	25
Received Broadcast Packets	8	Transmitted Broadcast Packets	0
Received Unknown Packets	0		

To show ingress or egress traffic statistics for a sample entry:

1. Click Interface, Port, Statistics, or Interface, Trunk, Statistics.

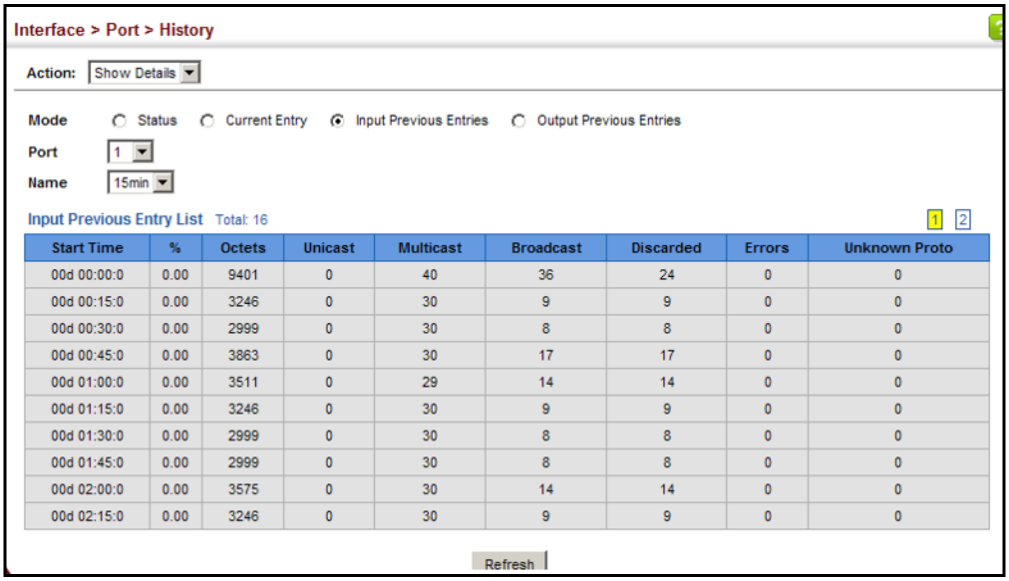
2. Select Show Details from the Action menu.

3. Select Input Previous Entry or Output Previous Entry from the options for Mode.

4. Select an interface from the Port or Trunk list.

5. Select an sampling entry from the Name list.

Figure 45: Showing Ingress Statistics for a History Sample



Interface > Port > History

Action: Show Details

Mode ○ Status ○ Current Entry ● Input Previous Entries ○ Output Previous Entries

Port 1

Name 15min

Input Previous Entry List Total: 16

Start Time	%	Octets	Unicast	Multicast	Broadcast	Discarded	Errors	Unknown Proto
00d 00:00:0	0.00	9401	0	40	36	24	0	0
00d 00:15:0	0.00	3246	0	30	9	9	0	0
00d 00:30:0	0.00	2999	0	30	8	8	0	0
00d 00:45:0	0.00	3863	0	30	17	17	0	0
00d 01:00:0	0.00	3511	0	29	14	14	0	0
00d 01:15:0	0.00	3246	0	30	9	9	0	0
00d 01:30:0	0.00	2999	0	30	8	8	0	0
00d 01:45:0	0.00	2999	0	30	8	8	0	0
00d 02:00:0	0.00	3575	0	30	14	14	0	0
00d 02:15:0	0.00	3246	0	30	9	9	0	0

DISPLAYING TRANSCEIVER DATA

Use the Interface > Port > Transceiver page to display identifying information, and operational for optical transceivers which support Digital Diagnostic Monitoring (DDM).

CLI REFERENCES

- "show interfaces transceiver" on page 1211

PARAMETERS

These parameters are displayed:

- **Port** – Port number. (Range: 1-28)

- **General** – Information on connector type and vendor-related parameters.

- **DDM Information** – Information on temperature, supply voltage, laser bias current, laser power, and received optical power.

  The switch can display diagnostic information for SFP modules which support the SFF-8472 Specification for Diagnostic Monitoring Interface for Optical Transceivers. This information allows administrators to remotely diagnose problems with optical devices. This feature, referred to as Digital Diagnostic Monitoring (DDM) provides information on transceiver parameters.

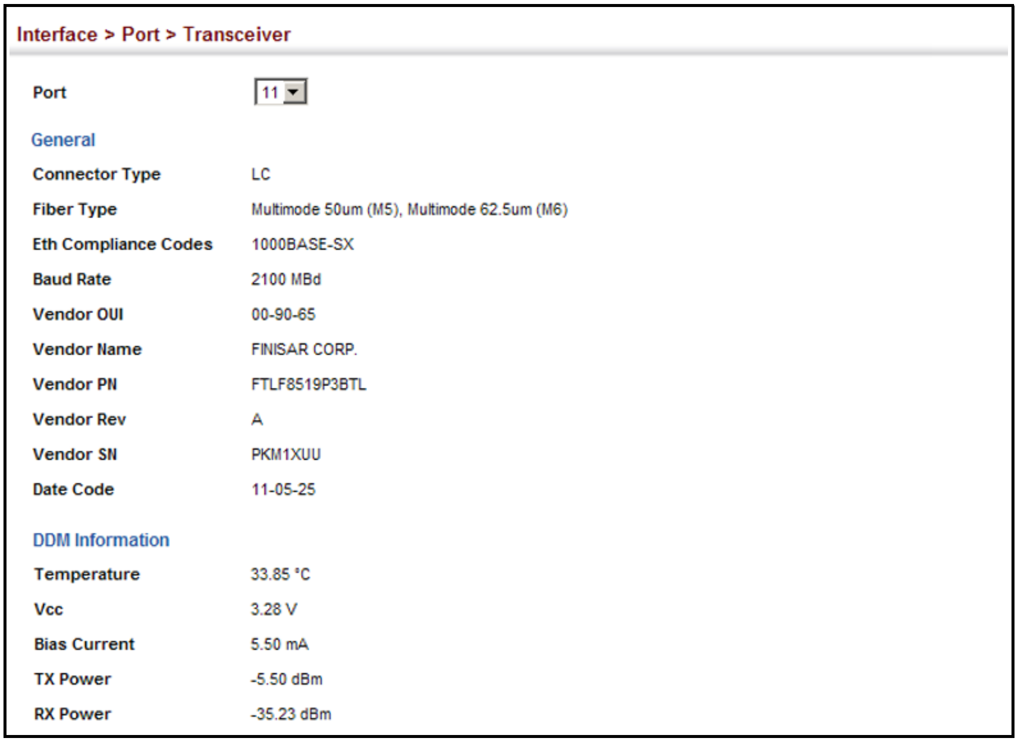
WEB INTERFACE

To display identifying information and functional parameters for optical transceivers:

1. Click Interface, Port, Transceiver.

2. Select a port from the scroll-down list.

Figure 46: Displaying Transceiver Data



Interface > Port > Transceiver

Port	11
General	
Connector Type	LC
Fiber Type	Multimode 50um (M5), Multimode 62.5um (M6)
Eth Compliance Codes	1000BASE-SX
Baud Rate	2100 MBd
Vendor OUI	00-90-65
Vendor Name	FINISAR CORP.
Vendor PN	FTLF8519P3BTL
Vendor Rev	A
Vendor SN	PKM1XUU
Date Code	11-05-25
DDM Information	
Temperature	33.85 °C
Vcc	3.28 V
Bias Current	5.50 mA
TX Power	-5.50 dBm
RX Power	-35.23 dBm

CONFIGURING TRANSCEIVER THRESHOLDS

Use the Interface > Port > Transceiver page to configure thresholds for alarm and warning messages for optical transceivers which support Digital Diagnostic Monitoring (DDM). This page also displays identifying information for supported transceiver types, and operational parameters for transceivers which support DDM.

CLI REFERENCES

- "transceiver-threshold-auto" on page 1205
- "transceiver-threshold-monitor" on page 1206
- "transceiver-threshold current" on page 1206
- "transceiver-threshold rx-power" on page 1207
- "transceiver-threshold temperature" on page 1208
- "transceiver-threshold tx-power" on page 1209

- "transceiver-threshold voltage" on page 1210
- "show interfaces transceiver-threshold" on page 1212

PARAMETERS

These parameters are displayed:

- **Port** – Port number. (Range: 1-28)

- **General** – Information on connector type and vendor-related parameters.

- **DDM Information** – Information on temperature, supply voltage, laser bias current, laser power, and received optical power.

  The switch can display diagnostic information for SFP modules which support the SFF-8472 Specification for Diagnostic Monitoring Interface for Optical Transceivers. This information allows administrators to remotely diagnose problems with optical devices. This feature, referred to as Digital Diagnostic Monitoring (DDM) provides information on transceiver parameters.

- **Trap** – Sends a trap when any of the transceiver's operation values falls outside of specified thresholds. (Default: Disabled)

- **Auto Mode** – Uses default threshold settings obtained from the transceiver to determine when an alarm or trap message should be sent. (Default: Enabled)

- **DDM Thresholds** – Information on alarm and warning thresholds. The switch can be configured to send a trap when the measured parameter falls outside of the specified thresholds.

  The following alarm and warning parameters are supported:

  - **High Alarm** – Sends an alarm message when the high threshold is crossed.
  - **High Warning** – Sends a warning message when the high threshold is crossed.
  - **Low Warning** – Sends a warning message when the low threshold is crossed.
  - **Low Alarm** – Sends an alarm message when the low threshold is crossed.

  The configurable ranges are:

  - **Temperature**: -200.00-200.00 °C
  - **Voltage**: 1.00-255.00 Volts
  - **Current**: 1.00-255.00 mA
  - **Power**: -99.99-99.99 dBm

    The threshold value for Rx and Tx power is calculated as the power ratio in decibels (dB) of the measured power referenced to one milliwatt (mW).

Threshold values for alarm and warning messages can be configured as described below.

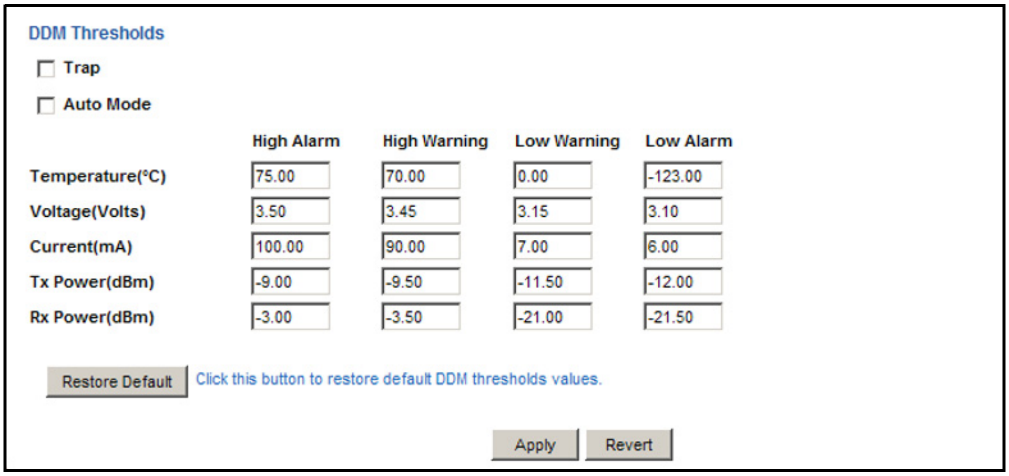
- A high-threshold alarm or warning message is sent if the current value is greater than or equal to the threshold, and the last sample value was less than the threshold. After a rising event has been generated, another such event will not be generated until the sampled value has fallen below the high threshold and reaches the low threshold.
- A low-threshold alarm or warning message is sent if the current value is less than or equal to the threshold, and the last sample value was greater than the threshold. After a falling event has been generated, another such event will not be generated until the sampled value has risen above the low threshold and reaches the high threshold.
- Threshold events are triggered as described above to avoid a hysteresis effect which would continuously trigger event messages if the power level were to fluctuate just above and below either the high threshold or the low threshold.
- Trap messages configured by this command are sent to any management station configured as an SNMP trap manager using the Administration > SNMP (Configure Trap) page.

WEB INTERFACE

To configure threshold values for optical transceivers:

1. Click Interface, Port, Transceiver.
2. Select a port from the scroll-down list.
3. Set the switch to send a trap based on default or manual settings.
4. Set alarm and warning thresholds if manual configuration is used.
5. Click Apply.

Figure 47: Configuring Transceiver Thresholds



DDM Thresholds

□ Trap

□ Auto Mode

	High Alarm	High Warning	Low Warning	Low Alarm
Temperature(°C)	75.00	70.00	0.00	-123.00
Voltage(Volts)	3.50	3.45	3.15	3.10
Current(mA)	100.00	90.00	7.00	6.00
Tx Power(dBm)	-9.00	-9.50	-11.50	-12.00
Rx Power(dBm)	-3.00	-3.50	-21.00	-21.50

Click this button to restore default DDM thresholds values.

TRUNK CONFIGURATION

This section describes how to configure static and dynamic trunks.

You can create multiple links between devices that work as one virtual, aggregate link. A port trunk offers a dramatic increase in bandwidth for network segments where bottlenecks exist, as well as providing a fault-tolerant link between two devices. You can create up to 6 trunks at a time on the switch.

The switch supports both static trunking and dynamic Link Aggregation Control Protocol (LACP). Static trunks have to be manually configured at both ends of the link, and the switches must comply with the Cisco EtherChannel standard. On the other hand, LACP configured ports can automatically negotiate a trunked link with LACP-configured ports on another device. You can configure any number of ports on the switch as LACP, as long as they are not already configured as part of a static trunk. If ports on another device are also configured as LACP, the switch and the other device will negotiate a trunk link between them. If an LACP trunk consists of more than eight ports, all other ports will be placed in standby mode. Should one link in the trunk fail, one of the standby ports will automatically be activated to replace it.

COMMAND USAGE

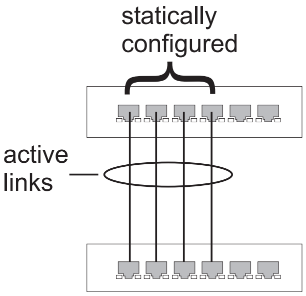
Besides balancing the load across each port in the trunk, the other ports provide redundancy by taking over the load if a port in the trunk fails. However, before making any physical connections between devices, use the web interface or CLI to specify the trunk on the devices at both ends. When using a port trunk, take note of the following points:

- Finish configuring port trunks before you connect the corresponding network cables between switches to avoid creating a loop.
- You can create up to 8 trunks on a switch, with up to eight ports per trunk.
- The ports at both ends of a connection must be configured as trunk ports.
- When configuring static trunks on switches of different types, they must be compatible with the Cisco EtherChannel standard.
- The ports at both ends of a trunk must be configured in an identical manner, including communication mode (i.e., speed, duplex mode and flow control), VLAN assignments, and CoS settings.
- Any of the Gigabit ports on the front panel can be trunked together, including ports of different media types.
- All the ports in a trunk have to be treated as a whole when moved from/to, added or deleted from a VLAN.
- STP, VLAN, and IGMP settings can only be made for the entire trunk.

CONFIGURING A STATIC TRUNK

Use the Interface > Trunk > Static page to create a trunk, assign member ports, and configure the connection parameters.

Figure 48: Configuring Static Trunks



CLI REFERENCES

- "Link Aggregation Commands" on page 1215
- "Interface Commands" on page 1187

COMMAND USAGE

- When configuring static trunks, you may not be able to link switches of different types, depending on the vendor's implementation. However, note that the static trunks on this switch are Cisco EtherChannel compatible.

- To avoid creating a loop in the network, be sure you add a static trunk via the configuration interface before connecting the ports, and also disconnect the ports before removing a static trunk via the configuration interface.

PARAMETERS

These parameters are displayed:

- **Trunk ID** – Trunk identifier. (Range: 1-8)

- **Member** – The initial trunk member. Use the Add Member page to configure additional members.

  - **Unit** – Unit identifier. (Range: 1)

  - **Port** – Port identifier. (Range: 1- 28)

WEB INTERFACE

To create a static trunk:

1. Click Interface, Trunk, Static.

2. Select Configure Trunk from the Step list.

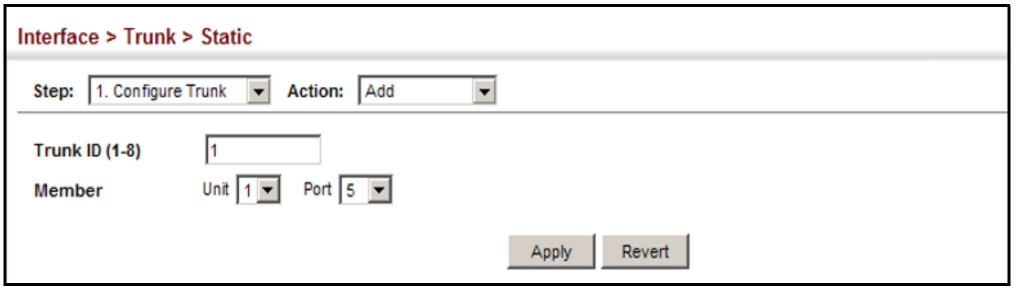
3. Select Add from the Action list.

4. Enter a trunk identifier.

5. Set the unit and port for the initial trunk member.

6. Click Apply.

Figure 49: Creating Static Trunks



Interface > Trunk > Static

Step: 1. Configure Trunk Action: Add

Trunk ID (1-8): 1

Member: Unit 1 Port 5

To add member ports to a static trunk:

1. Click Interface, Trunk, Static.

2. Select Configure Trunk from the Step list.

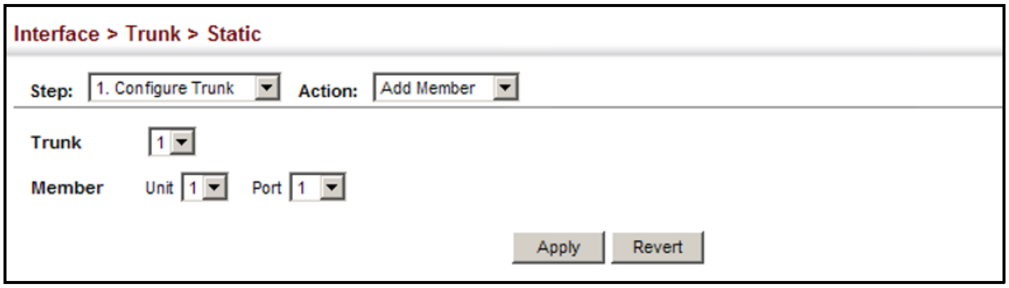
3. Select Add Member from the Action list.

4. Select a trunk identifier.

5. Set the unit and port for an additional trunk member.

6. Click Apply.

Figure 50: Adding Static Trunks Members



Interface > Trunk > Static

Step: 1. Configure Trunk Action: Add Member

Trunk: 1

Member: Unit 1 Port 1

To configure connection parameters for a static trunk:

1. Click Interface, Trunk, Static.

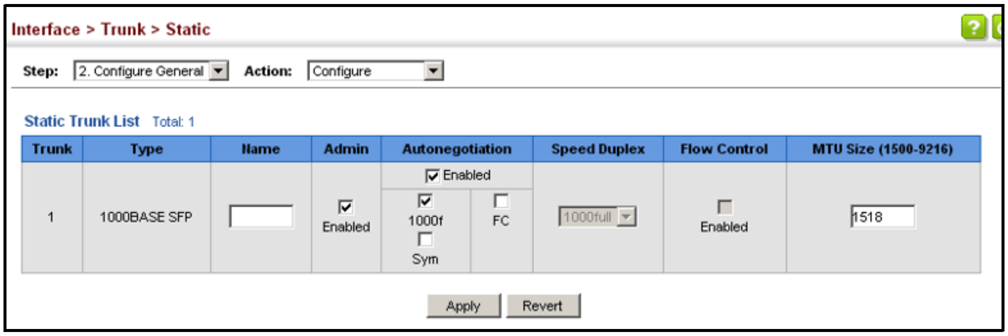
2. Select Configure General from the Step list.

3. Select Configure from the Action list.

4. Modify the required interface settings. (Refer to "Configuring by Port List" on page 182 for a description of the parameters.)

5. Click Apply.

Figure 51: Configuring Connection Parameters for a Static Trunk



Interface > Trunk > Static

Step: 2. Configure General Action: Configure

Static Trunk List Total: 1

Trunk	Type	Name	Admin	Autonegotiation		Speed Duplex	Flow Control	MTU Size (1500-9216)
				☑ Enabled				
1	1000BASE SFP		☑ Enabled	☑ 1000f ☐ Sym	☐ FC	1000full	☐ Enabled	1518

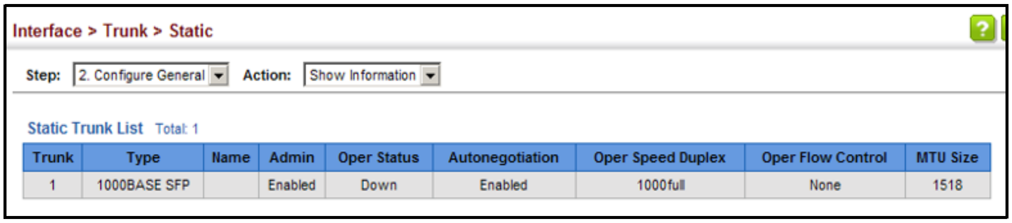
To display trunk connection parameters:

1. Click Interface, Trunk, Static.

2. Select Configure General from the Step list.

3. Select Show Information from the Action list.

Figure 52: Showing Information for Static Trunks



Interface > Trunk > Static

Step: 2. Configure General Action: Show Information

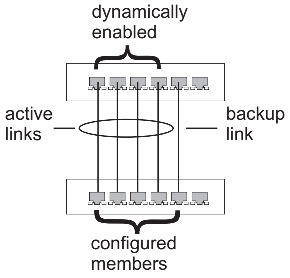
Static Trunk List Total: 1

Trunk	Type	Name	Admin	Oper Status	Autonegotiation	Oper Speed Duplex	Oper Flow Control	MTU Size
1	1000BASE SFP		Enabled	Down	Enabled	1000full	None	1518

CONFIGURING A DYNAMIC TRUNK

Use the Interface > Trunk > Dynamic pages to set the administrative key for an aggregation group, enable LACP on a port, and configure protocol parameters for local and partner ports, or to set Ethernet connection parameters.

Figure 53: Configuring Dynamic Trunks



CLI References

- "Link Aggregation Commands" on page 1215

Command Usage

- To avoid creating a loop in the network, be sure you enable LACP before connecting the ports, and also disconnect the ports before disabling LACP.
- If the target switch has also enabled LACP on the connected ports, the trunk will be activated automatically.
- A trunk formed with another switch using LACP will automatically be assigned the next available trunk ID.
- If more than eight ports attached to the same target switch have LACP enabled, the additional ports will be placed in standby mode, and will only be enabled if one of the active links fails.
- All ports on both ends of an LACP trunk must be configured for full duplex, and auto-negotiation.
- Ports are only allowed to join the same Link Aggregation Group (LAG) if (1) the LACP port system priority matches, (2) the LACP port admin key matches, and (3) the LAG admin key matches (if configured). However, if the LAG admin key is set, then the port admin key must be set to the same value for a port to be allowed to join that group.

NOTE: If the LACP admin key is not set when a channel group is formed (i.e., it has a null value of 0), the operational value of this key is set to the same value as the port admin key used by the interfaces that joined the group (see the show lacp internal command described on page 1224).

Parameters

These parameters are displayed:

Configure Aggregator

- **Admin Key** – LACP administration key is used to identify a specific link aggregation group (LAG) during local LACP setup on the switch. (Range: 0-65535)
- **Timeout Mode** – The timeout to wait for the next LACP data unit (LACPDU):
  - **Long Timeout** – Specifies a slow timeout of 90 seconds. (This is the default setting.)
  - **Short Timeout** – Specifies a fast timeout of 3 seconds.

    The timeout is set in the LACP timeout bit of the Actor State field in transmitted LACPDUs. When the partner switch receives an LACPDU set with a short timeout from the actor switch, the partner adjusts the transmit LACPDU interval to 1 second. When it receives an LACPDU set with a long timeout from the actor, it adjusts the transmit LACPDU interval to 30 seconds.

If the actor does not receive an LACPDU from its partner before the configured timeout expires, the partner port information will be deleted from the LACP group.

When a dynamic port-channel member leaves a port-channel, the default timeout value will be restored on that port.

When a dynamic port-channel is torn down, the configured timeout value will be retained. When the dynamic port-channel is constructed again, that timeout value will be used.

Configure Aggregation Port - General

- **Port** – Port identifier. (Range: 1-28)
- **LACP Status** – Enables or disables LACP on a port.

Configure Aggregation Port - Actor/Partner

- **Port** – Port number. (Range: 1-28)
- **Admin Key** – The LACP administration key must be set to the same value for ports that belong to the same LAG. (Range: 0-65535; Default – Actor: 1, Partner: 0)

  By default, the Actor Admin Key is determined by port's link speed, and copied to Oper Key. The Partner Admin Key is assigned to zero, and the Oper Key is set based upon LACP PDUs received from the Partner.
- **System Priority** – LACP system priority is used to determine link aggregation group (LAG) membership, and to identify this device to other switches during LAG negotiations. (Range: 0-65535; Default: 32768)

  System priority is combined with the switch’s MAC address to form the LAG identifier. This identifier is used to indicate a specific LAG during LACP negotiations with other systems.
- **Port Priority** – If a link goes down, LACP port priority is used to select a backup link. (Range: 0-65535; Default: 32768)
  - Setting a lower value indicates a higher effective priority.
  - If an active port link goes down, the backup port with the highest priority is selected to replace the downed link. However, if two or more ports have the same LACP port priority, the port with the lowest physical port number will be selected as the backup port.
  - If an LAG already exists with the maximum number of allowed port members, and LACP is subsequently enabled on another port using a higher priority than an existing member, the newly configured port will replace an existing port member that has a lower priority.

NOTE: Configuring LACP settings for a port only applies to its administrative state, not its operational state, and will only take effect the next time an aggregate link is established with that port.

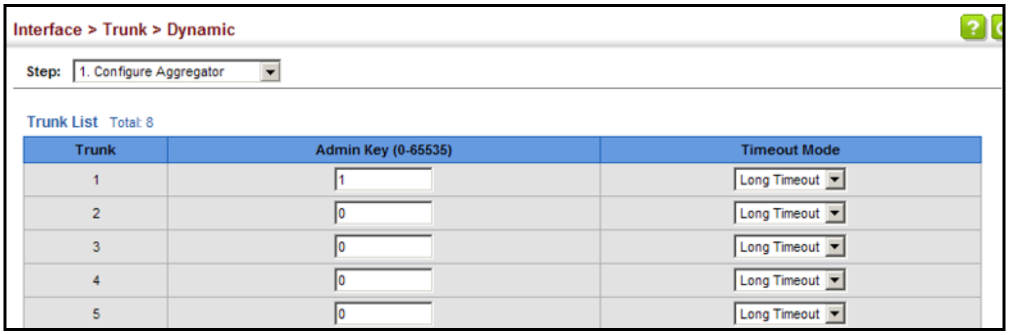
NOTE: Configuring the port partner sets the remote side of an aggregate link; i.e., the ports on the attached device. The command attributes have the same meaning as those used for the port actor.

WEB INTERFACE

To configure the admin key for a dynamic trunk:

1. Click Interface, Trunk, Dynamic.
2. Select Configure Aggregator from the Step list.
3. Set the Admin Key and timeout mode for the required LACP group.
4. Click Apply.

Figure 54: Configuring the LACP Aggregator Admin Key



Interface > Trunk > Dynamic

Step: 1. Configure Aggregator

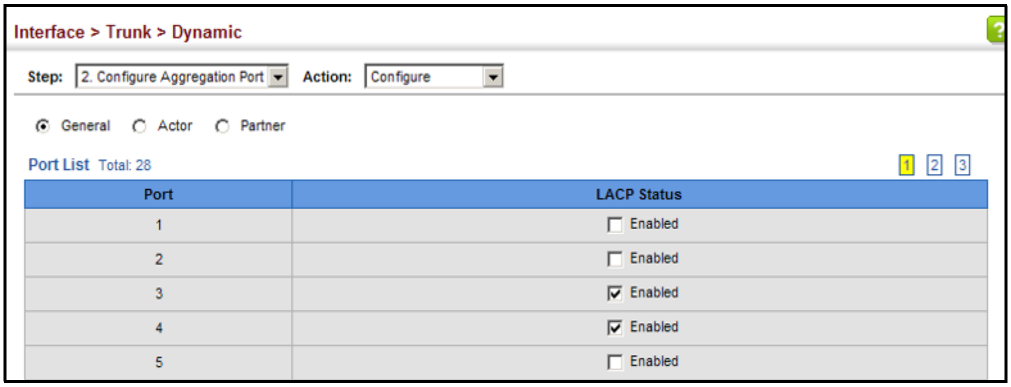
Trunk List Total: 8

Trunk	Admin Key (0-65535)	Timeout Mode
1	1	Long Timeout
2	0	Long Timeout
3	0	Long Timeout
4	0	Long Timeout
5	0	Long Timeout

To enable LACP for a port:

1. Click Interface, Trunk, Dynamic.
2. Select Configure Aggregation Port from the Step list.
3. Select Configure from the Action list.
4. Click General.
5. Enable LACP on the required ports.
6. Click Apply.

Figure 55: Enabling LACP on a Port



Interface > Trunk > Dynamic

Step: 2. Configure Aggregation Port   Action: Configure

● General   ○ Actor   ○ Partner

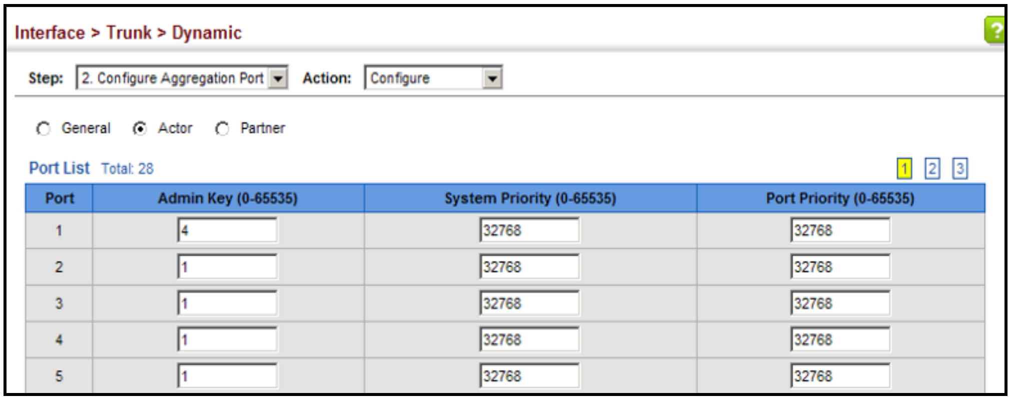
Port List Total: 28

Port	LACP Status
1	□ Enabled
2	□ Enabled
3	☑ Enabled
4	☑ Enabled
5	□ Enabled

To configure LACP parameters for group members:

1. Click Interface, Trunk, Dynamic.
2. Select Configure Aggregation Port from the Step list.
3. Select Configure from the Action list.
4. Click Actor or Partner.
5. Configure the required settings.
6. Click Apply.

Figure 56: Configuring LACP Parameters on a Port



Interface > Trunk > Dynamic

Step: 2. Configure Aggregation Port   Action: Configure

○ General   ● Actor   ○ Partner

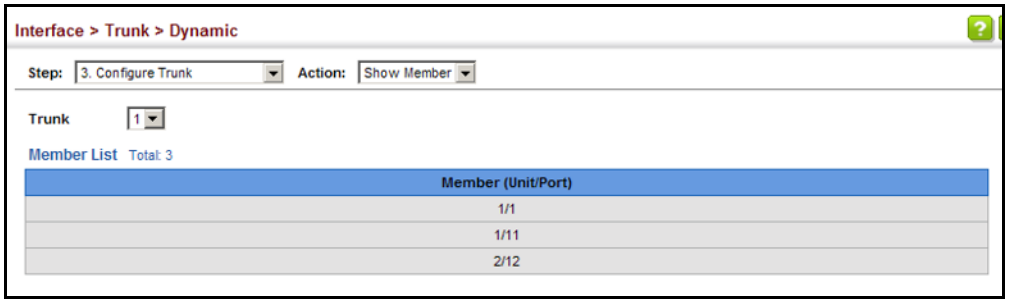
Port List Total: 28

Port	Admin Key (0-65535)	System Priority (0-65535)	Port Priority (0-65535)
1	4	32768	32768
2	1	32768	32768
3	1	32768	32768
4	1	32768	32768
5	1	32768	32768

To show the active members of a dynamic trunk:

1. Click Interface, Trunk, Dynamic.
2. Select Configure Trunk from the Step List.
3. Select Show Member from the Action List.
4. Select a Trunk.

Figure 57: Showing Members of a Dynamic Trunk



Interface > Trunk > Dynamic

Step: 3. Configure Trunk Action: Show Member

Trunk 1

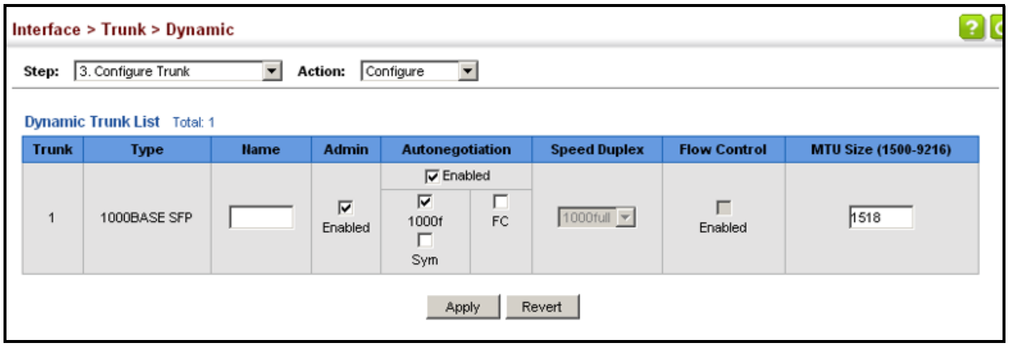
Member List Total: 3

Member (Unit/Port)
1/1
1/11
2/12

To configure connection parameters for a dynamic trunk:

1. Click Interface, Trunk, Dynamic.
2. Select Configure Trunk from the Step List.
3. Select Configure from the Action List.
4. Modify the required interface settings. (See "Configuring by Port List" on page 182 for a description of the interface settings.)
5. Click Apply.

Figure 58: Configuring Connection Settings for Dynamic Trunks



Interface > Trunk > Dynamic

Step: 3. Configure Trunk Action: Configure

Dynamic Trunk List Total: 1

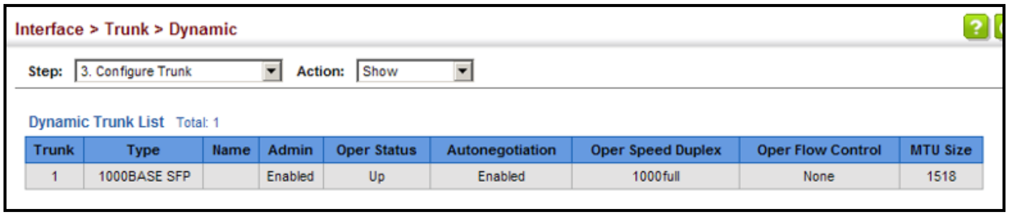
Trunk	Type	Name	Admin	Autonegotiation		Speed Duplex	Flow Control	MTU Size (1500-9216)
				☑ Enabled				
1	1000BASE SFP		☑ Enabled	☑ 1000f □ Sym	□ FC	1000full	□ Enabled	1518

To display connection parameters for a dynamic trunk:

1. Click Interface, Trunk, Dynamic.
2. Select Configure Trunk from the Step List.

3. Select Show from the Action List.

Figure 59: Displaying Connection Parameters for Dynamic Trunks



Interface > Trunk > Dynamic

Step: 3. Configure Trunk   Action: Show

Dynamic Trunk List Total: 1

Trunk	Type	Name	Admin	Oper Status	Autonegotiation	Oper Speed Duplex	Oper Flow Control	MTU Size
1	1000BASE SFP		Enabled	Up	Enabled	1000full	None	1518

DISPLAYING LACP PORT COUNTERS

Use the Interface > Trunk > Dynamic (Configure Aggregation Port - Show Information - Counters) page to display statistics for LACP protocol messages.

CLI REFERENCES

- "show lacp" on page 1224

PARAMETERS

These parameters are displayed:

Table 8: LACP Port Counters

Parameter	Description
LACPDUs Sent	Number of valid LACPDUs transmitted from this channel group.
LACPDUs Received	Number of valid LACPDUs received on this channel group.
Marker Sent	Number of valid Marker PDUs transmitted from this channel group.
Marker Received	Number of valid Marker PDUs received by this channel group.
Marker Unknown Pkts	Number of frames received that either (1) Carry the Slow Protocols Ethernet Type value, but contain an unknown PDU, or (2) are addressed to the Slow Protocols group MAC Address, but do not carry the Slow Protocols Ethernet Type.
Marker Illegal Pkts	Number of frames that carry the Slow Protocols Ethernet Type value, but contain a badly formed PDU or an illegal value of Protocol Subtype.

WEB INTERFACE

To display LACP port counters:

1. Click Interface, Trunk, Dynamic.

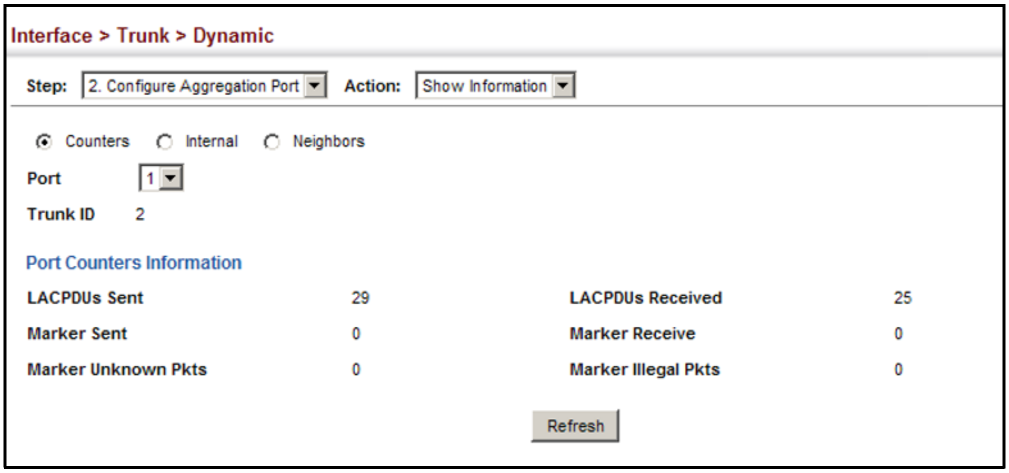
2. Select Configure Aggregation Port from the Step list.

3. Select Show Information from the Action list.

4. Click Counters.

5. Select a group member from the Port list.

Figure 60: Displaying LACP Port Counters



Interface > Trunk > Dynamic

Step: 2. Configure Aggregation Port   Action: Show Information

● Counters ○ Internal ○ Neighbors

Port 1

Trunk ID 2

Port Counters Information

LACPDUs Sent	29	LACPDUs Received	25
Marker Sent	0	Marker Receive	0
Marker Unknown Pkts	0	Marker Illegal Pkts	0

DISPLAYING LACP SETTINGS AND STATUS FOR THE LOCAL SIDE

Use the Interface > Trunk > Dynamic (Configure Aggregation Port - Show Information - Internal) page to display the configuration settings and operational state for the local side of a link aggregation.

CLI REFERENCES

- "show lacp" on page 1224

PARAMETERS

These parameters are displayed:

Table 9: LACP Internal Configuration Information

Parameter	Description
LACP System Priority	LACP system priority assigned to this port channel.
LACP Port Priority	LACP port priority assigned to this interface within the channel group.
Admin Key	Current administrative value of the key for the aggregation port.
Oper Key	Current operational value of the key for the aggregation port.
LACPDUs Interval	Number of seconds before invalidating received LACPDU information.
Admin State, Oper State	Administrative or operational values of the actor's state parameters: ◆ Expired – The actor's receive machine is in the expired state; ◆ Defaulted – The actor's receive machine is using defaulted operational partner information, administratively configured for the partner. ◆ Distributing – If false, distribution of outgoing frames on this link is disabled; i.e., distribution is currently disabled and is not expected to be enabled in the absence of administrative changes or changes in received protocol information. ◆ Collecting – Collection of incoming frames on this link is enabled; i.e., collection is currently enabled and is not expected to be disabled in the absence of administrative changes or changes in received protocol information. ◆ Synchronization – The System considers this link to be IN_SYNC; i.e., it has been allocated to the correct Link Aggregation Group, the group has been associated with a compatible Aggregator, and the identity of the Link Aggregation Group is consistent with the System ID and operational Key information transmitted.

Table 9: LACP Internal Configuration Information (Continued)

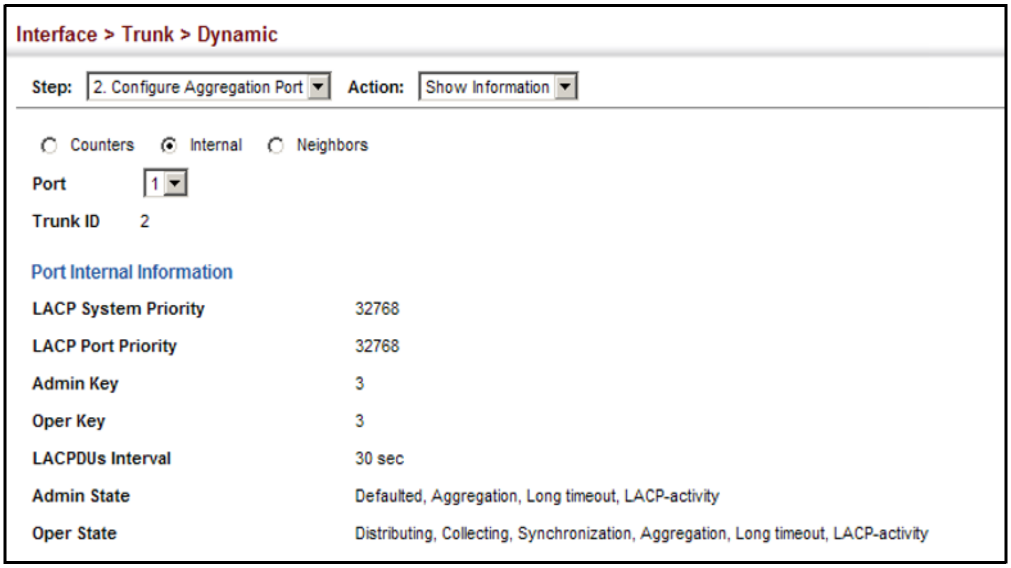
Parameter	Description
	◆ Aggregation – The system considers this link to be aggregatable; i.e., a potential candidate for aggregation. ◆ Long timeout – Periodic transmission of LACPDUs uses a slow transmission rate. ◆ LACP-Activity – Activity control value with regard to this link. (0: Passive; 1: Active)

WEB INTERFACE

To display LACP settings and status for the local side:

1. Click Interface, Trunk, Dynamic.
2. Select Configure Aggregation Port from the Step list.
3. Select Show Information from the Action list.
4. Click Internal.
5. Select a group member from the Port list.

Figure 61: Displaying LACP Port Internal Information



Interface > Trunk > Dynamic

Step: 2. Configure Aggregation Port Action: Show Information

○ Counters ● Internal ○ Neighbors

Port 1

Trunk ID 2

Port Internal Information

LACP System Priority	32768
LACP Port Priority	32768
Admin Key	3
Oper Key	3
LACPDUs Interval	30 sec
Admin State	Defaulted, Aggregation, Long timeout, LACP-activity
Oper State	Distributing, Collecting, Synchronization, Aggregation, Long timeout, LACP-activity

DISPLAYING LACP SETTINGS AND STATUS FOR THE REMOTE SIDE

Use the Interface > Trunk > Dynamic (Configure Aggregation Port - Show Information - Neighbors) page to display the configuration settings and operational state for the remote side of a link aggregation.

CLI REFERENCES

- "show lacp" on page 1224

PARAMETERS

These parameters are displayed:

Table 10: LACP Remote Device Configuration Information

Parameter	Description
Partner Admin System ID	LAG partner's system ID assigned by the user.
Partner Oper System ID	LAG partner's system ID assigned by the LACP protocol.
Partner Admin Port Number	Current administrative value of the port number for the protocol Partner.
Partner Oper Port Number	Operational port number assigned to this aggregation port by the port's protocol partner.
Port Admin Priority	Current administrative value of the port priority for the protocol partner.
Port Oper Priority	Priority value assigned to this aggregation port by the partner.
Admin Key	Current administrative value of the Key for the protocol partner.
Oper Key	Current operational value of the Key for the protocol partner.
Admin State	Administrative values of the partner's state parameters. (See preceding table.)
Oper State	Operational values of the partner's state parameters. (See preceding table.)

WEB INTERFACE

To display LACP settings and status for the remote side:

1. Click Interface, Trunk, Dynamic.

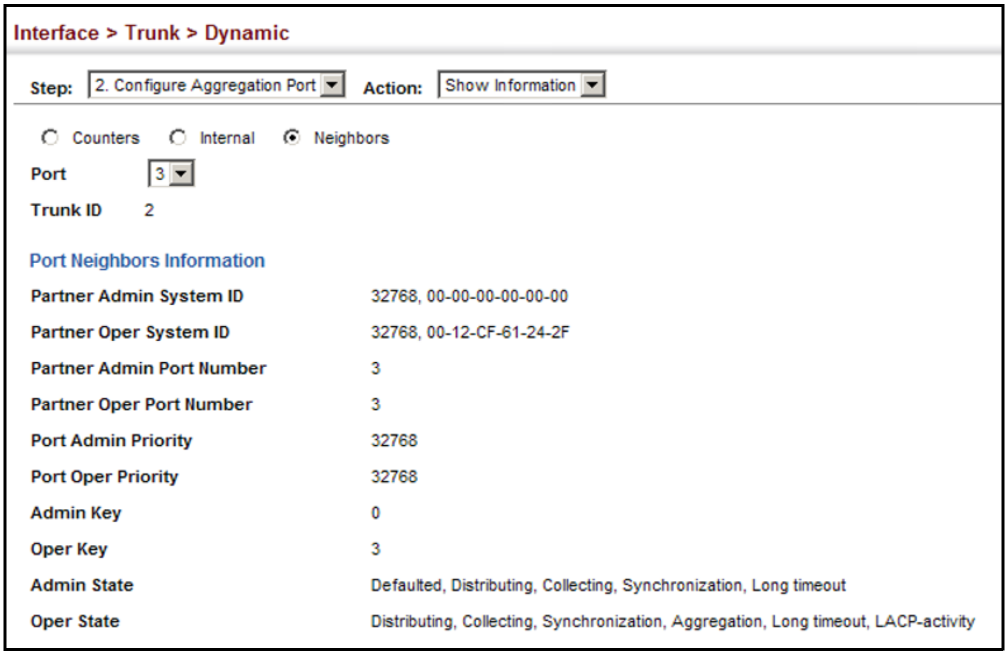
2. Select Configure Aggregation Port from the Step list.

3. Select Show Information from the Action list.

4. Click Neighbors.

5. Select a group member from the Port list.

Figure 62: Displaying LACP Port Remote Information



Interface > Trunk > Dynamic

Step: 2. Configure Aggregation Port Action: Show Information

○ Counters ○ Internal ● Neighbors

Port 3

Trunk ID 2

Port Neighbors Information

Partner Admin System ID	32768, 00-00-00-00-00-00
Partner Oper System ID	32768, 00-12-CF-61-24-2F
Partner Admin Port Number	3
Partner Oper Port Number	3
Port Admin Priority	32768
Port Oper Priority	32768
Admin Key	0
Oper Key	3
Admin State	Defaulted, Distributing, Collecting, Synchronization, Long timeout
Oper State	Distributing, Collecting, Synchronization, Aggregation, Long timeout, LACP-activity

CONFIGURING LOAD BALANCING

Use the Interface > Trunk > Load Balance page to set the load-distribution method used among ports in aggregated links.

CLI REFERENCES

- "port channel load-balance" on page 992

COMMAND USAGE

- This command applies to all static and dynamic trunks on the switch.
- To ensure that the switch traffic load is distributed evenly across all links in a trunk, select the source and destination addresses used in the load-balance calculation to provide the best result for trunk connections:
  - **Destination IP Address**: All traffic with the same destination IP address is output on the same link in a trunk. This mode works best for switch-to-router trunk links where traffic through the switch is destined for many different hosts. Do not use this mode for switch-to-server trunk links where the destination IP address is the same for all traffic.
  - **Destination MAC Address**: All traffic with the same destination MAC address is output on the same link in a trunk. This mode works best for switch-to-switch trunk links where traffic through the switch is destined for many different hosts. Do not use this mode for switch-to-router trunk links where the destination MAC address is the same for all traffic.
  - **Source and Destination IP Address**: All traffic with the same source and destination IP address is output on the same link in a

trunk. This mode works best for switch-to-router trunk links where traffic through the switch is received from and destined for many different hosts.

- **Source and Destination MAC Address**: All traffic with the same source and destination MAC address is output on the same link in a trunk. This mode works best for switch-to-switch trunk links where traffic through the switch is received from and destined for many different hosts.
- **Source IP Address**: All traffic with the same source IP address is output on the same link in a trunk. This mode works best for switch-to-router or switch-to-server trunk links where traffic through the switch is received from many different hosts.
- **Source MAC Address**: All traffic with the same source MAC address is output on the same link in a trunk. This mode works best for switch-to-switch trunk links where traffic through the switch is received from many different hosts.

PARAMETERS

These parameters are displayed for the load balance mode:

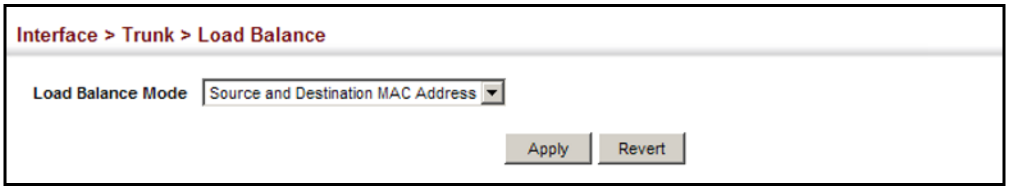
- **Destination IP Address** - Load balancing based on destination IP address.
- **Destination MAC Address** - Load balancing based on destination MAC address.
- **Source and Destination IP Address** - Load balancing based on source and destination IP address.
- **Source and Destination MAC Address** - Load balancing based on source and destination MAC address.
- **Source IP Address** - Load balancing based on source IP address.
- **Source MAC Address** - Load balancing based on source MAC address.

WEB INTERFACE

To display the load-distribution method used by ports in aggregated links:

1. Click Interface, Trunk, Load Balance.
2. Select the required method from the Load Balance Mode list.
3. Click Apply.

Figure 63: Configuring Load Balancing



Interface > Trunk > Load Balance

Load Balance Mode: Source and Destination MAC Address

TRAFFIC SEGMENTATION

If tighter security is required for passing traffic from different clients through downlink ports on the local network and over uplink ports to the service provider, port-based traffic segmentation can be used to isolate traffic for individual clients. Data traffic on downlink ports is only forwarded to, and from, uplink ports.

Traffic belonging to each client is isolated to the allocated downlink ports. But the switch can be configured to either isolate traffic passing across a client's allocated uplink ports from the uplink ports assigned to other clients, or to forward traffic through the uplink ports used by other clients, allowing different clients to share access to their uplink ports where security is less likely to be compromised.

ENABLING TRAFFIC SEGMENTATION

Use the Interface > Traffic Segmentation (Configure Global) page to enable traffic segmentation.

CLI REFERENCES

- "Configuring Port-based Traffic Segmentation" on page 1157

PARAMETERS

These parameters are displayed:

- **Status** – Enables port-based traffic segmentation. (Default: Disabled)
- **Uplink-to-Uplink Mode** – Specifies whether or not traffic can be forwarded between uplink ports assigned to different client sessions.
  - **Blocking** – Blocks traffic between uplink ports assigned to different sessions.
  - **Forwarding** – Forwards traffic between uplink ports assigned to different sessions.

WEB INTERFACE

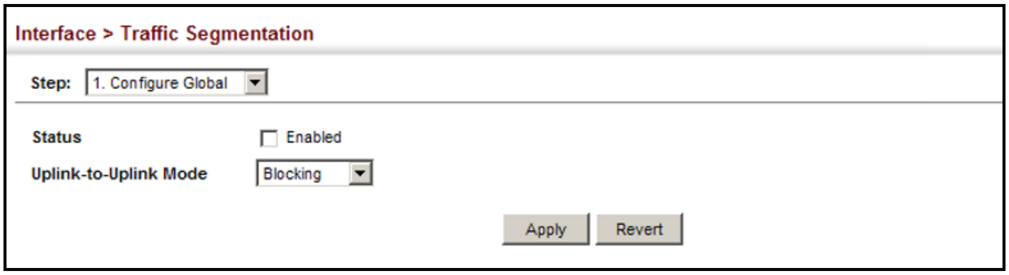
To enable traffic segmentation:

1. Click Interface, Traffic Segmentation.
2. Select Configure Global from the Step list.

3. Mark the Status check box, and set the required uplink-to-uplink mode.

4. Click Apply.

Figure 64: Enabling Traffic Segmentation



Interface > Traffic Segmentation

Step: 1. Configure Global

Status ☐ Enabled

Uplink-to-Uplink Mode: Blocking

CONFIGURING UPLINK AND DOWNLINK PORTS

Use the Interface > Traffic Segmentation (Configure Session) page to assign the downlink and uplink ports to use in the segmented group. Ports designated as downlink ports can not communicate with any other ports on the switch except for the uplink ports. Uplink ports can communicate with any other ports on the switch and with any designated downlink ports.

CLI REFERENCES

- "Configuring Port-based Traffic Segmentation" on page 1157

COMMAND USAGE

- When traffic segmentation is enabled, the forwarding state for the uplink and downlink ports assigned to different client sessions is shown below.

Table 11: Traffic Segmentation Forwarding

Destination Source	Session #1 Downlinks	Session #1 Uplinks	Session #2 Downlinks	Session #2 Uplinks	Normal Ports
Session #1 Downlink Ports	Blocking	Forwarding	Blocking	Blocking	Blocking
Session #1 Uplink Ports	Forwarding	Forwarding	Blocking	Blocking/ Forwarding*	Forwarding
Session #2 Downlink Ports	Blocking	Blocking	Blocking	Forwarding	Blocking
Session #2 Uplink Ports	Blocking	Blocking/ Forwarding*	Forwarding	Forwarding	Forwarding
Normal Ports	Forwarding	Forwarding	Forwarding	Forwarding	Forwarding

* The forwarding state for uplink-to-uplink ports is configured on the Configure Global page (see page 219).

- When traffic segmentation is disabled, all ports operate in normal forwarding mode based on the settings specified by other functions such as VLANs and spanning tree protocol.

- A port cannot be configured in both an uplink and downlink list.

- A port can only be assigned to one traffic-segmentation session.
- A downlink port can only communicate with an uplink port in the same session. Therefore, if an uplink port is not configured for a session, the assigned downlink ports will not be able to communicate with any other ports.
- If a downlink port is not configured for the session, the assigned uplink ports will operate as normal ports.

PARAMETERS

These parameters are displayed:

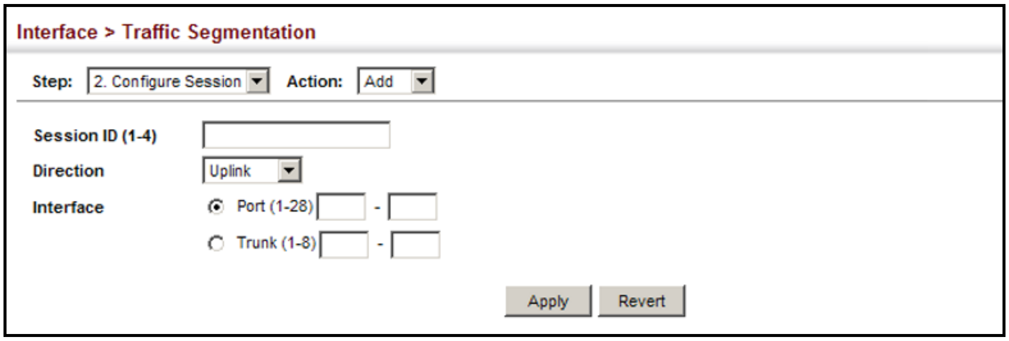
- **Session ID** – Traffic segmentation session. (Range: 1-4)
- **Direction** – Adds an interface to the segmented group by setting the direction to uplink or downlink. (Default: Uplink)
- **Interface** – Displays a list of ports or trunks.
- **Port** – Port Identifier. (Range: 1-28)
- **Trunk** – Trunk Identifier. (Range: 1-8)

WEB INTERFACE

To configure the members of the traffic segmentation group:

1. Click Interface, Traffic Segmentation.
2. Select Configure Session from the Step list.
3. Select Add from the Action list.
4. Enter the session ID, set the direction to uplink or downlink, and select the interface to add.
5. Click Apply.

Figure 65: Configuring Members for Traffic Segmentation



Interface > Traffic Segmentation

Step: 2. Configure Session Action: Add

Session ID (1-4)

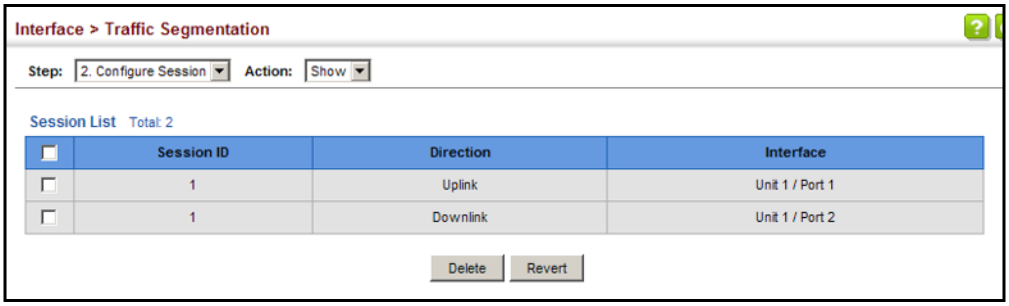
Direction Uplink

Interface ● Port (1-28) -
○ Trunk (1-8) -

To show the members of the traffic segmentation group:

1. Click Interface, Traffic Segmentation.
2. Select Configure Session from the Step list.
3. Select Show from the Action list.

Figure 66: Showing Traffic Segmentation Members



Interface > Traffic Segmentation

Step: 2. Configure Session Action: Show

Session List Total: 2

□	Session ID	Direction	Interface
□	1	Uplink	Unit 1 / Port 1
□	1	Downlink	Unit 1 / Port 2

VLAN TRUNKING

Use the Interface > VLAN Trunking page to allow unknown VLAN groups to pass through the specified interface.

CLI REFERENCES

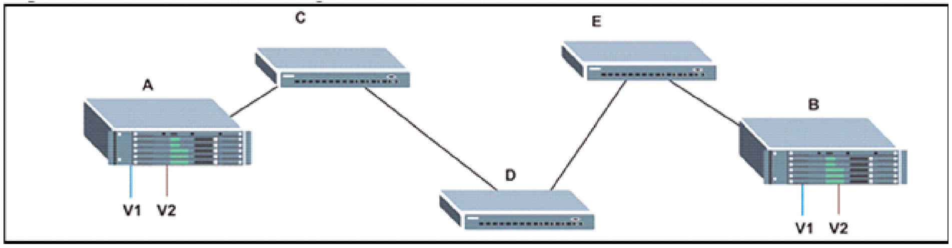
- "vlan-trunking" on page 1350

COMMAND USAGE

- Use this feature to configure a tunnel across one or more intermediate switches which pass traffic for VLAN groups to which they do not belong.

  The following figure shows VLANs 1 and 2 configured on switches A and B, with VLAN trunking being used to pass traffic for these VLAN groups across switches C, D and E.

  Figure 67: Configuring VLAN Trunking

  Without VLAN trunking, you would have to configure VLANs 1 and 2 on all intermediate switches – C, D and E; otherwise these switches would drop any frames with unknown VLAN group tags. However, by enabling VLAN trunking on the intermediate switch ports along the path connecting VLANs 1 and 2, you only need to create these VLAN groups in switches A and B. Switches C, D and E automatically allow frames with VLAN group tags 1 and 2 (groups that are unknown to those switches) to pass through their VLAN trunking ports.

- VLAN trunking is mutually exclusive with the “access” switchport mode (see "Adding Static Members to VLANs" on page 231). If VLAN trunking is enabled on an interface, then that interface cannot be set to access mode, and vice versa.

- To prevent loops from forming in the spanning tree, all unknown VLANs will be bound to a single instance (either STP/RSTP or an MSTP instance, depending on the selected STA mode).

- If both VLAN trunking and ingress filtering are disabled on an interface, packets with unknown VLAN tags will still be allowed to enter this interface and will be flooded to all other ports where VLAN trunking is enabled. (In other words, VLAN trunking will still be effectively enabled for the unknown VLAN).

PARAMETERS

These parameters are displayed:

- **Interface** – Displays a list of ports or trunks.

- **Port** – Port Identifier. (Range: 1-28)
- **Trunk** – Trunk Identifier. (Range: 1-8)

- **VLAN Trunking Status** – Enables VLAN trunking on the selected interface.

WEB INTERFACE

To enable VLAN trunking on a port or trunk:

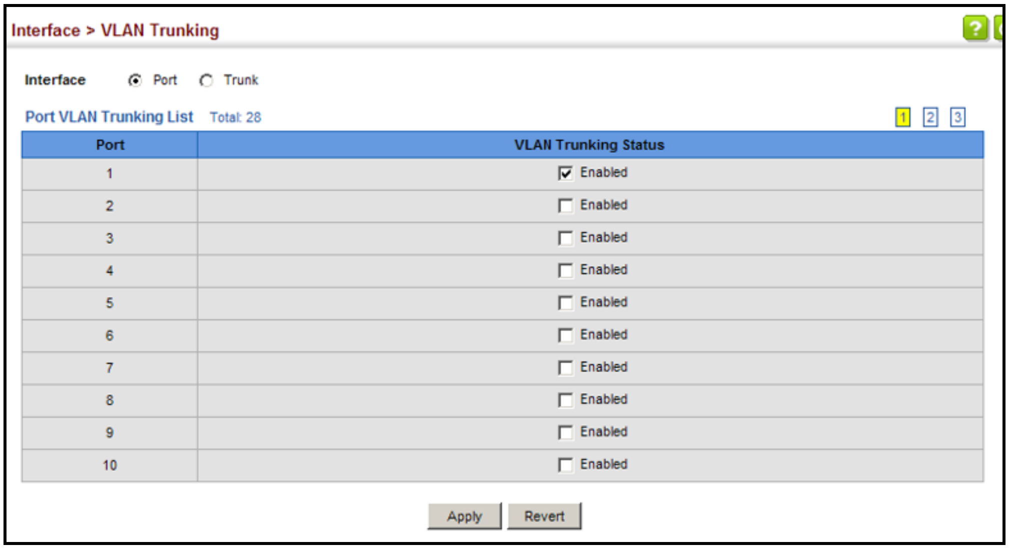
1. Click Interface, VLAN Trunking.

2. Click Port or Trunk to specify the interface type.

3. Enable VLAN trunking on any of the ports or on a trunk.

4. Click Apply.

Figure 68: Configuring VLAN Trunking



Interface > VLAN Trunking

Interface ● Port ○ Trunk

Port VLAN Trunking List Total: 28

Port	VLAN Trunking Status
1	☑ Enabled
2	□ Enabled
3	□ Enabled
4	□ Enabled
5	□ Enabled
6	□ Enabled
7	□ Enabled
8	□ Enabled
9	□ Enabled
10	□ Enabled

6 VLAN Configuration

This chapter includes the following topics:

- IEEE 802.1Q VLANs – Configures static and dynamic VLANs.
- Private VLANs – Configures private VLANs, using primary for unrestricted upstream access and community groups which are restricted to other local group members or to the ports in the associated primary group.
- IEEE 802.1Q Tunneling – Configures QinQ tunneling to maintain customer-specific VLAN and Layer 2 protocol configurations across a service provider network, even when different customers use the same internal VLAN IDs.
- Protocol VLANs – Configures VLAN groups based on specified protocols.
- IP Subnet VLANs – Maps untagged ingress frames to a specified VLAN if the source address is found in the IP subnet-to-VLAN mapping table.
- MAC-based VLANs – Maps untagged ingress frames to a specified VLAN if the source MAC address is found in the IP MAC address-to-VLAN mapping table.
- VLAN Translation – Maps VLAN IDs between the customer and the service provider.

IEEE 802.1Q VLANs

In large networks, routers are used to isolate broadcast traffic for each subnet into separate domains. This switch provides a similar service at Layer 2 by using VLANs to organize any group of network nodes into separate broadcast domains. VLANs confine broadcast traffic to the originating group, and can eliminate broadcast storms in large networks. This also provides a more secure and cleaner network environment.

An IEEE 802.1Q VLAN is a group of ports that can be located anywhere in the network, but communicate as though they belong to the same physical segment.

VLANs help to simplify network management by allowing you to move devices to a new VLAN without having to change any physical connections. VLANs can be easily organized to reflect departmental groups (such as Marketing or R&D), usage groups (such as e-mail), or multicast groups (used for multimedia applications such as video conferencing).

VLANs provide greater network efficiency by reducing broadcast traffic, and allow you to make network changes without having to update IP addresses or IP subnets. VLANs inherently provide a high level of network security since traffic must pass through a configured Layer 3 link to reach a different VLAN.

This switch supports the following VLAN features:

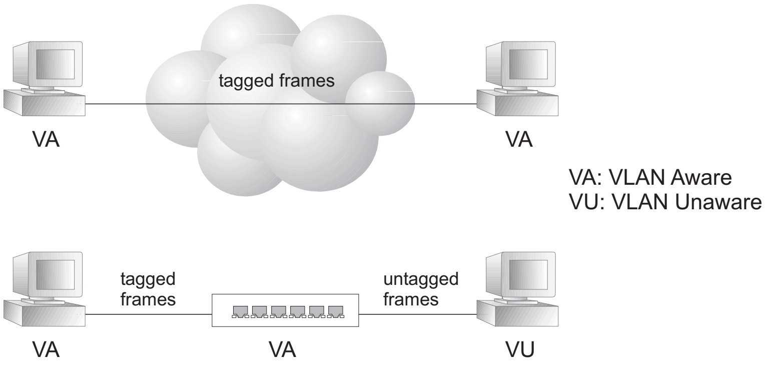
- Up to 4094 VLANs based on the IEEE 802.1Q standard
- Distributed VLAN learning across multiple switches using explicit or implicit tagging and GVRP protocol
- Port overlapping, allowing a port to participate in multiple VLANs
- End stations can belong to multiple VLANs
- Passing traffic between VLAN-aware and VLAN-unaware devices
- Priority tagging

Assigning Ports to VLANs

Before enabling VLANs for the switch, you must first assign each port to the VLAN group(s) in which it will participate. By default all ports are assigned to VLAN 1 as untagged ports. Add a port as a tagged port if you want it to carry traffic for one or more VLANs, and any intermediate network devices or the host at the other end of the connection supports VLANs. Then assign ports on the other VLAN-aware network devices along the path that will carry this traffic to the same VLAN(s), either manually or dynamically using GVRP. However, if you want a port on this switch to participate in one or more VLANs, but none of the intermediate network devices nor the host at the other end of the connection supports VLANs, then you should add this port to the VLAN as an untagged port.

NOTE: VLAN-tagged frames can pass through VLAN-aware or VLAN-unaware network interconnection devices, but the VLAN tags should be stripped off before passing it on to any end-node host that does not support VLAN tagging.

Figure 69: VLAN Compliant and VLAN Non-compliant Devices



VLAN Classification – When the switch receives a frame, it classifies the frame in one of two ways. If the frame is untagged, the switch assigns the frame to an associated VLAN (based on the default VLAN ID of the receiving port). But if the frame is tagged, the switch uses the tagged VLAN ID to identify the port broadcast domain of the frame.

Port Overlapping – Port overlapping can be used to allow access to commonly shared network resources among different VLAN groups, such as file servers or printers. Note that if you implement VLANs which do not overlap, but still need to communicate, you can connect them by enabled routing on this switch.

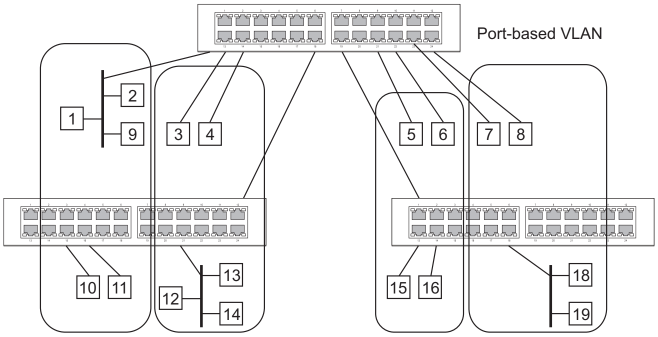
Untagged VLANs – Untagged (i.e., static) VLANs are typically used to reduce broadcast traffic and to increase security. A group of network users assigned to a VLAN form a broadcast domain that is separate from other VLANs configured on the switch. Packets are forwarded only between ports that are designated for the same VLAN. Untagged VLANs can be used to manually isolate user groups or subnets. However, you should use IEEE 802.3 tagged VLANs with GVRP whenever possible to fully automate VLAN registration.

Automatic VLAN Registration – GVRP (GARP VLAN Registration Protocol) defines a system whereby the switch can automatically learn the VLANs to which each end station should be assigned. If an end station (or its network adapter) supports the IEEE 802.1Q VLAN protocol, it can be configured to broadcast a message to your network indicating the VLAN groups it wants to join. When this switch receives these messages, it will automatically place the receiving port in the specified VLANs, and then forward the message to all other ports. When the message arrives at another switch that supports GVRP, it will also place the receiving port in the specified VLANs, and pass the message on to all other ports. VLAN requirements are propagated in this way throughout the network. This allows GVRP-compliant devices to be automatically configured for VLAN groups based solely on end station requests.

To implement GVRP in a network, first add the host devices to the required VLANs (using the operating system or other application software), so that these VLANs can be propagated onto the network. For both the edge switches attached directly to these hosts, and core switches in the network, enable GVRP on the links between these devices. You should also determine security boundaries in the network and disable GVRP on the boundary ports to prevent advertisements from being propagated, or forbid those ports from joining restricted VLANs.

NOTE: If you have host devices that do not support GVRP, you should configure static or untagged VLANs for the switch ports connected to these devices (as described in "Adding Static Members to VLANs" on page 231). But you can still enable GVRP on these edge switches, as well as on the core switches in the network.

Figure 70: Using GVRP



Forwarding Tagged/Untagged Frames

If you want to create a small port-based VLAN for devices attached directly to a single switch, you can assign ports to the same untagged VLAN. However, to participate in a VLAN group that crosses several switches, you should create a VLAN for that group and enable tagging on all ports.

Ports can be assigned to multiple tagged or untagged VLANs. Each port on the switch is therefore capable of passing tagged or untagged frames. When forwarding a frame from this switch along a path that contains any VLAN-aware devices, the switch should include VLAN tags. When forwarding a frame from this switch along a path that does not contain any VLAN-aware devices (including the destination host), the switch must first strip off the VLAN tag before forwarding the frame. When the switch receives a tagged frame, it will pass this frame onto the VLAN(s) indicated by the frame tag. However, when this switch receives an untagged frame from a VLAN-unaware device, it first decides where to forward the frame, and then inserts a VLAN tag reflecting the ingress port's default VID.

CONFIGURING VLAN GROUPS

Use the VLAN > Static (Add) page to create or remove VLAN groups, set administrative status, or specify Remote VLAN type (see "Configuring Remote Port Mirroring" on page 188). To propagate information about VLAN groups used on this switch to external network devices, you must specify a VLAN ID for each of these groups.

CLI REFERENCES

- "Editing VLAN Groups" on page 1343

PARAMETERS

These parameters are displayed:

Add

- **VLAN ID** – ID of VLAN or range of VLANs (1-4094).

  Up to 4094 VLAN groups can be defined. VLAN 1 is the default untagged VLAN.

- **Status** – Enables or disables the specified VLAN.

- **Remote VLAN** – Reserves this VLAN for RSPAN (see "Configuring Remote Port Mirroring" on page 188).

- **L3 Interface** – Sets the interface to support Layer 3 configuration, and reserves memory space required to maintain additional information about this interface type. This parameter must be enabled before you can assign an IP address to a VLAN (see "Setting the Switch's IP Address (IP Version 4)" on page 691).

Modify

- **VLAN ID** – ID of configured VLAN (1-4094).

- **VLAN Name** – Name of the VLAN (1 to 32 characters).

- **Status** – Enables or disables the specified VLAN.

- **L3 Interface** – Sets the interface to support Layer 3 configuration, and reserves memory space required to maintain additional information about this interface type. This parameter must be enabled before you can assign an IP address to a VLAN.

Show

- **VLAN ID** – ID of configured VLAN.

- **VLAN Name** – Name of the VLAN.

- **Status** – Operational status of configured VLAN.

- **Remote VLAN** – Shows if RSPAN is enabled on this VLAN (see "Configuring Remote Port Mirroring" on page 188).

- **L3 Interface** – Shows if the interface supports Layer 3 configuration.

WEB INTERFACE

To create VLAN groups:

1. Click VLAN, Static.

2. Select Add from the Action list.

3. Enter a VLAN ID or range of IDs.

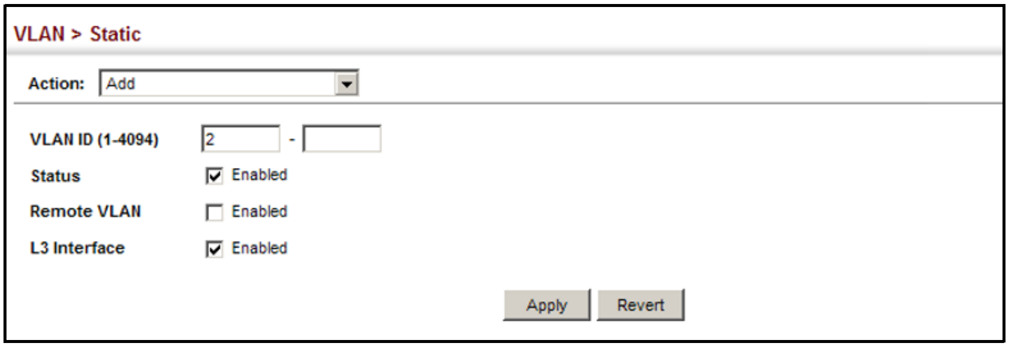
4. Enable the Status field to configure the VLAN as operational.

5. Specify whether the VLANs are to be used for remote port mirroring.

6. Enable the L3 Interface field to specify that a VLAN will be used as a Layer 3 interface.

7. Click Apply.

Figure 71: Creating Static VLANs



VLAN > Static

Action: Add

VLAN ID (1-4094) 2 -

Status ☑ Enabled

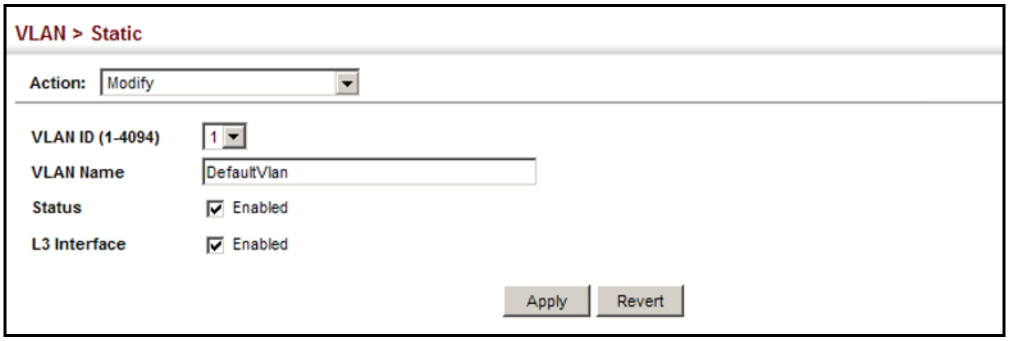
Remote VLAN □ Enabled

L3 Interface ☑ Enabled

To modify the configuration settings for VLAN groups:

1. Click VLAN, Static.
2. Select Modify from the Action list.
3. Select the identifier of a configured VLAN.
4. Modify the VLAN name, operational status, or Layer 3 Interface status as required.
5. Click Apply.

Figure 72: Modifying Settings for Static VLANs



VLAN > Static

Action: Modify

VLAN ID (1-4094) 1

VLAN Name DefaultVlan

Status ☑ Enabled

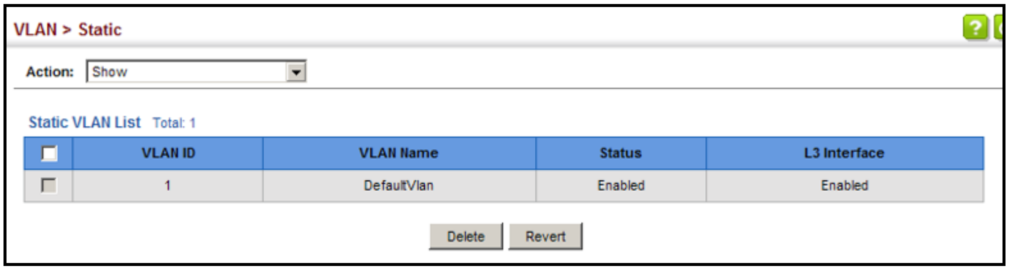
L3 Interface ☑ Enabled

To show the configuration settings for VLAN groups:

1. Click VLAN, Static.

2. Select Show from the Action list.

Figure 73: Showing Static VLANs



VLAN > Static

Action: Show

Static VLAN List Total: 1

□	VLAN ID	VLAN Name	Status	L3 Interface
□	1	DefaultVlan	Enabled	Enabled

ADDING STATIC MEMBERS TO VLANS

Use the VLAN > Static pages to configure port members for the selected VLAN index, interface, or a range of interfaces. Use the menus for editing port members to configure the VLAN behavior for specific interfaces, including the mode of operation (Hybrid or 1Q Trunk), the default VLAN identifier (PVID), accepted frame types, and ingress filtering. Assign ports as tagged if they are connected to 802.1Q VLAN compliant devices, or untagged they are not connected to any VLAN-aware devices. Or configure a port as forbidden to prevent the switch from automatically adding it to a VLAN via the GVRP protocol.

CLI REFERENCES

- "Configuring VLAN Interfaces" on page 1345
- "Displaying VLAN Information" on page 1352

PARAMETERS

These parameters are displayed:

Edit Member by VLAN

- **VLAN** – ID of configured VLAN (1-4094).

- **Interface** – Displays a list of ports or trunks.

- **Port** – Port Identifier. (Range: 1-28)

- **Trunk** – Trunk Identifier. (Range: 1-8)

- **Mode** – Indicates VLAN membership mode for an interface. (Default: Hybrid)

  - **Hybrid** – Specifies a hybrid VLAN interface. The port may transmit tagged or untagged frames.

  - **1Q Trunk** – Specifies a port as an end-point for a VLAN trunk. A trunk is a direct link between two switches, so the port transmits tagged frames that identify the source VLAN. Note that frames belonging to the port's default VLAN (i.e., associated with the PVID) are also transmitted as tagged frames.

- **PVID** – VLAN ID assigned to untagged frames received on the interface. (Default: 1)

  If an interface is not a member of VLAN 1 and you assign its PVID to this VLAN, the interface will automatically be added to VLAN 1 as an untagged member. For all other VLANs, the PVID must be defined first, then the status of the VLAN can be configured as a tagged or untagged member.

- **Acceptable Frame Type** – Sets the interface to accept all frame types, including tagged or untagged frames, or only tagged frames. When set to receive all frame types, any received frames that are untagged are assigned to the default VLAN. (Options: All, Tagged; Default: All)

- **Ingress Filtering** – Determines how to process frames tagged for VLANs for which the ingress port is not a member. (Default: Disabled)
  - Ingress filtering only affects tagged frames.
  - If ingress filtering is disabled and a port receives frames tagged for VLANs for which it is not a member, these frames will be flooded to all other ports (except for those VLANs explicitly forbidden on this port).
  - If ingress filtering is enabled and a port receives frames tagged for VLANs for which it is not a member, these frames will be discarded.
  - Ingress filtering does not affect VLAN independent BPDU frames, such as GVRP or STP. However, they do affect VLAN dependent BPDU frames, such as GMRP.

- **Membership Type** – Select VLAN membership for each interface by marking the appropriate radio button for a port or trunk:
  - **Tagged**: Interface is a member of the VLAN. All packets transmitted by the port will be tagged, that is, carry a tag and therefore carry VLAN or CoS information.
  - **Untagged**: Interface is a member of the VLAN. All packets transmitted by the port will be untagged, that is, not carry a tag and therefore not carry VLAN or CoS information. Note that an interface must be assigned to at least one group as an untagged port.
  - **Forbidden**: Interface is forbidden from automatically joining the VLAN via GVRP. For more information, see "Automatic VLAN Registration" on page 227.
  - **None**: Interface is not a member of the VLAN. Packets associated with this VLAN will not be transmitted by the interface.

NOTE: VLAN 1 is the default untagged VLAN containing all ports on the switch.

Edit Member by Interface

All parameters are the same as those described under the preceding section for Edit Member by VLAN.

Edit Member by Interface Range

All parameters are the same as those described under the earlier section for Edit Member by VLAN, except for the items shown below.

- **Port Range** – Displays a list of ports. (Range: 1-28)
- **Trunk Range** – Displays a list of ports. (Range: 1-8)

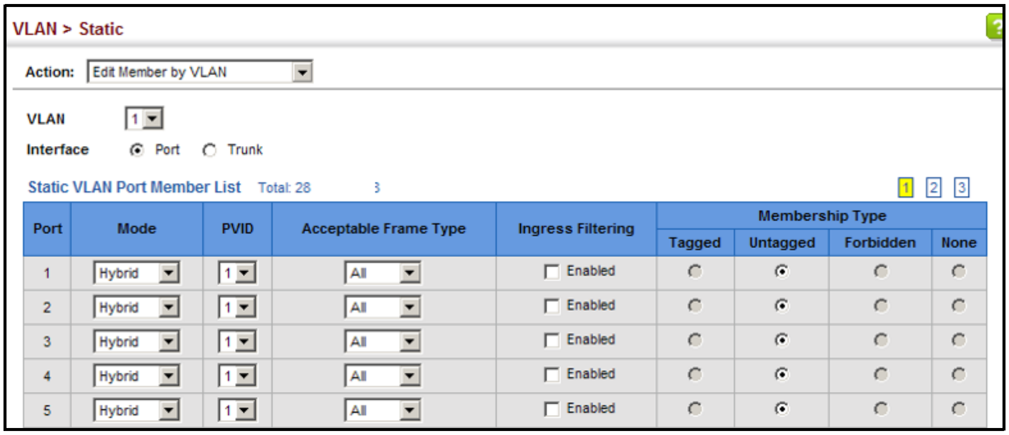
NOTE: The PVID, acceptable frame type, and ingress filtering parameters for each interface within the specified range must be configured on either the Edit Member by VLAN or Edit Member by Interface page.

WEB INTERFACE

To configure static members by the VLAN index:

1. Click VLAN, Static.
2. Select Edit Member by VLAN from the Action list.
3. Select a VLAN from the scroll-down list.
4. Set the Interface type to display as Port or Trunk.
5. Modify the settings for any interface as required.
6. Click Apply.

Figure 74: Configuring Static Members by VLAN Index



VLAN > Static

Action: Edit Member by VLAN

VLAN 1

Interface ● Port ○ Trunk

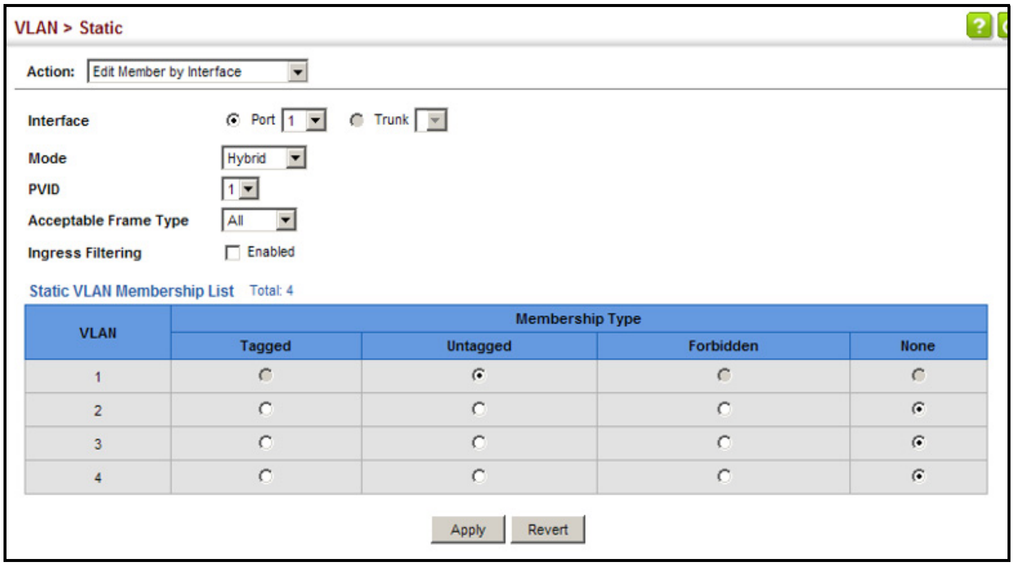
Static VLAN Port Member List Total: 28

Port	Mode	PVID	Acceptable Frame Type	Ingress Filtering	Membership Type			
					Tagged	Untagged	Forbidden	None
1	Hybrid	1	All	□ Enabled	○	●	○	○
2	Hybrid	1	All	□ Enabled	○	●	○	○
3	Hybrid	1	All	□ Enabled	○	●	○	○
4	Hybrid	1	All	□ Enabled	○	●	○	○
5	Hybrid	1	All	□ Enabled	○	●	○	○

To configure static members by interface:

1. Click VLAN, Static.
2. Select Edit Member by Interface from the Action list.
3. Select a port or trunk configure.
4. Modify the settings for any interface as required.
5. Click Apply.

Figure 75: Configuring Static VLAN Members by Interface



VLAN > Static

Action: Edit Member by Interface

Interface ● Port 1 ○ Trunk

Mode Hybrid

PVID 1

Acceptable Frame Type All

Ingress Filtering □ Enabled

Static VLAN Membership List Total: 4

VLAN	Membership Type			
	Tagged	Untagged	Forbidden	None
1	○	●	○	○
2	○	○	○	●
3	○	○	○	●
4	○	○	○	●

To configure static members by interface range:

1. Click VLAN, Static.
2. Select Edit Member by Interface Range from the Action list.

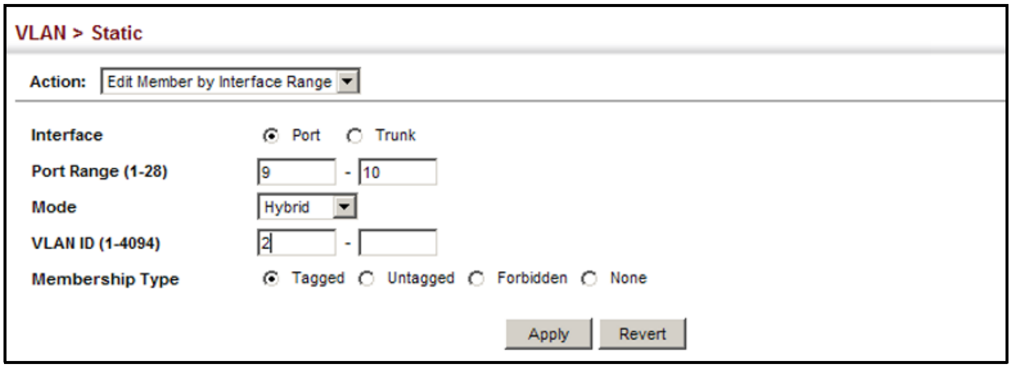
3. Set the Interface type to display as Port or Trunk.

4. Enter an interface range.

5. Modify the VLAN parameters as required. Remember that the PVID, acceptable frame type, and ingress filtering parameters for each interface within the specified range must be configured on either the Edit Member by VLAN or Edit Member by Interface page.

6. Click Apply.

Figure 76: Configuring Static VLAN Members by Interface Range



VLAN > Static

Action: Edit Member by Interface Range

Interface ● Port ○ Trunk

Port Range (1-28) 9 - 10

Mode Hybrid

VLAN ID (1-4094) 2 -

Membership Type ● Tagged ○ Untagged ○ Forbidden ○ None

Configuring Dynamic VLAN Registration

Use the VLAN > Dynamic page to enable GVRP globally on the switch, or to enable GVRP and adjust the protocol timers per interface.

CLI References

- "GVRP and Bridge Extension Commands" on page 1338
- "Configuring VLAN Interfaces" on page 1345

Parameters

These parameters are displayed:

Configure General

- **GVRP Status** – GVRP defines a way for switches to exchange VLAN information in order to register VLAN members on ports across the network. VLANs are dynamically configured based on join messages issued by host devices and propagated throughout the network. GVRP must be enabled to permit automatic VLAN registration, and to support VLANs which extend beyond the local switch. (Default: Disabled)

Configure Interface

- **Interface** – Displays a list of ports or trunks.

- **Port** – Port Identifier. (Range: 1-28)

- **Trunk** – Trunk Identifier. (Range: 1-8)

- **GVRP Status** – Enables/disables GVRP for the interface. GVRP must be globally enabled for the switch before this setting can take effect (using the Configure General page). When disabled, any GVRP packets received on this port will be discarded and no GVRP registrations will be propagated from other ports. (Default: Disabled)

- **GVRP Timers** – Timer settings must follow this rule:
  3 x (join timer) < leave timer < leaveAll timer

  - **Join** – The interval between transmitting requests/queries to participate in a VLAN group. (Range: 20-1000 centiseconds; Default: 20)

  - **Leave** – The interval a port waits before leaving a VLAN group. This time should be set to more than twice the join time. This ensures that after a Leave or LeaveAll message has been issued, the applicants can rejoin before the port actually leaves the group. (Range: 60-3000 centiseconds; Default: 60)

  - **LeaveAll** – The interval between sending out a LeaveAll query message for VLAN group participants and the port leaving the group. This interval should be considerably larger than the Leave Time to minimize the amount of traffic generated by nodes rejoining the group. (Range: 500-18000 centiseconds; Default: 1000)

Show Dynamic VLAN – Show VLAN

VLAN ID – Identifier of a VLAN this switch has joined through GVRP.

VLAN Name – Name of a VLAN this switch has joined through GVRP.

Status – Indicates if this VLAN is currently operational.
(Display Values: Enabled, Disabled)

Show Dynamic VLAN – Show VLAN Member

- **VLAN** – Identifier of a VLAN this switch has joined through GVRP.

- **Interface** – Displays a list of ports or trunks which have joined the selected VLAN through GVRP.

WEB INTERFACE

To configure GVRP on the switch:

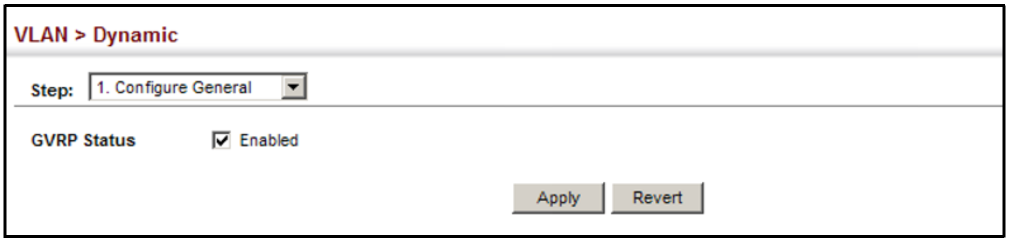
1. Click VLAN, Dynamic.

2. Select Configure General from the Step list.

3. Enable or disable GVRP.

4. Click Apply.

Figure 77: Configuring Global Status of GVRP



VLAN > Dynamic

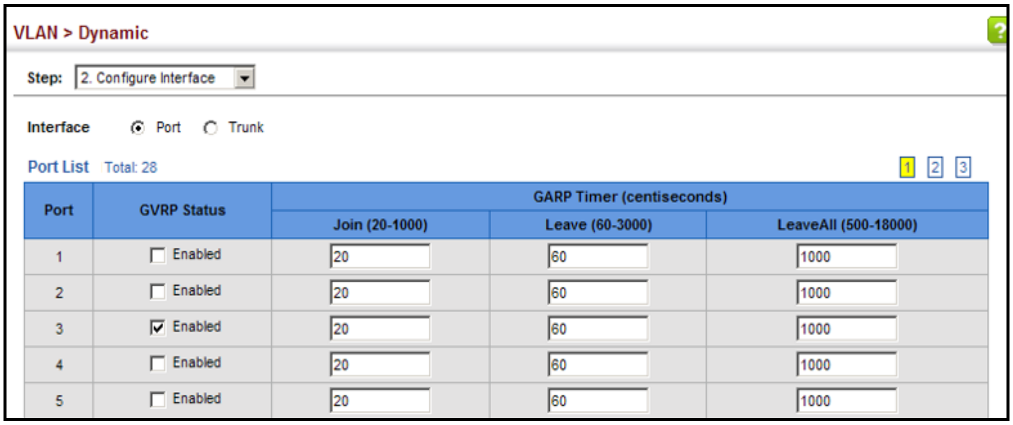
Step: 1. Configure General

GVRP Status ☑ Enabled

To configure GVRP status and timers on a port or trunk:

1. Click VLAN, Dynamic.
2. Select Configure Interface from the Step list.
3. Set the Interface type to display as Port or Trunk.
4. Modify the GVRP status or timers for any interface.
5. Click Apply.

Figure 78: Configuring GVRP for an Interface



VLAN > Dynamic

Step: 2. Configure Interface

Interface ● Port ○ Trunk

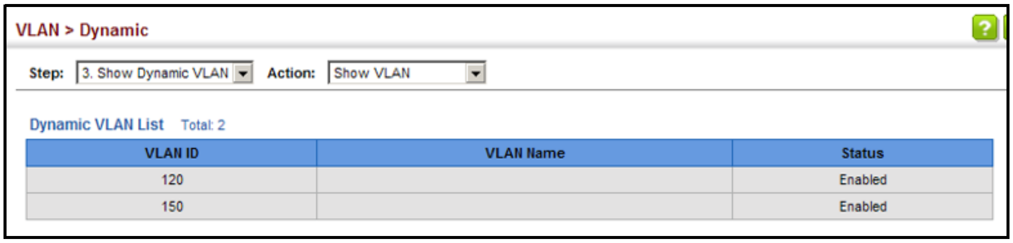
Port List Total: 28

Port	GVRP Status	GARP Timer (centiseconds)		
		Join (20-1000)	Leave (60-3000)	LeaveAll (500-18000)
1	□ Enabled	20	60	1000
2	□ Enabled	20	60	1000
3	☑ Enabled	20	60	1000
4	□ Enabled	20	60	1000
5	□ Enabled	20	60	1000

To show the dynamic VLAN joined by this switch:

1. Click VLAN, Dynamic.
2. Select Show Dynamic VLAN from the Step list.
3. Select Show VLAN from the Action list.

Figure 79: Showing Dynamic VLANs Registered on the Switch



VLAN > Dynamic

Step: 3. Show Dynamic VLAN Action: Show VLAN

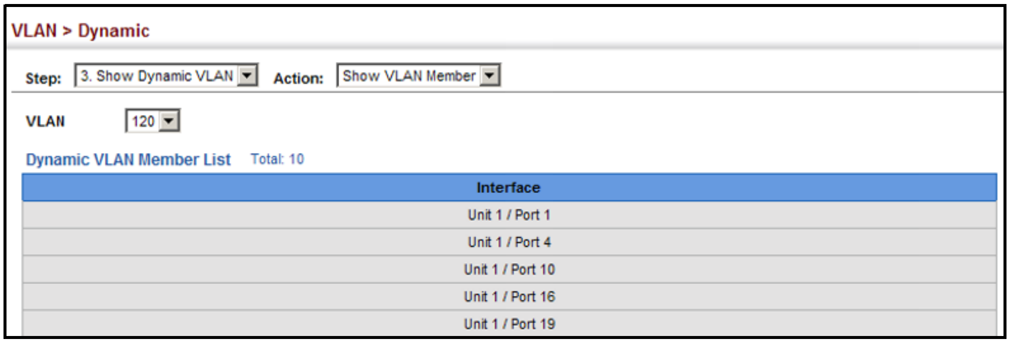
Dynamic VLAN List Total: 2

VLAN ID	VLAN Name	Status
120		Enabled
150		Enabled

To show the members of a dynamic VLAN:

1. Click VLAN, Dynamic.
2. Select Show Dynamic VLAN from the Step list.
3. Select Show VLAN Members from the Action list.

Figure 80: Showing the Members of a Dynamic VLAN



VLAN > Dynamic

Step: 3. Show Dynamic VLAN Action: Show VLAN Member

VLAN 120

Dynamic VLAN Member List Total: 10

Interface
Unit 1 / Port 1
Unit 1 / Port 4
Unit 1 / Port 10
Unit 1 / Port 16
Unit 1 / Port 19

PRIVATE VLANS

Private VLANs provide port-based security and isolation of local ports contained within different private VLAN groups. This switch supports two types of private VLANs – primary and community groups. A primary VLAN contains promiscuous ports that can communicate with all other ports in the associated private VLAN groups, while a community (or secondary) VLAN contains community ports that can only communicate with other hosts within the community VLAN and with any of the promiscuous ports in the associated primary VLAN. The promiscuous ports are designed to provide open access to an external network such as the Internet, while the community ports provide restricted access to local users.

Multiple primary VLANs can be configured on this switch, and multiple community VLANs can be associated with each primary VLAN. (Note that private VLANs and normal VLANs can exist simultaneously within the same switch.)

To configure primary/secondary associated groups, follow these steps:

1. Use the Configure VLAN (Add) page to designate one or more community VLANs, and the primary VLAN that will channel traffic outside of the VLAN groups.

2. Use the Configure VLAN (Add Community VLAN) page to map a community VLAN to the primary VLAN.

3. Use the Configure Interface page to set the port type to promiscuous (i.e., having access to all ports in the primary VLAN), or host (i.e., having access restricted to community VLAN members, and channeling all other traffic through promiscuous ports). Then assign any promiscuous ports to a primary VLAN and any host ports a community VLAN.

CREATING PRIVATE VLANS

Use the VLAN > Private (Configure VLAN - Add) page to create primary or community VLANs.

CLI REFERENCES

- "private-vlan" on page 1367

PARAMETERS

These parameters are displayed in the web interface:

- **VLAN ID** – ID of configured VLAN (1-4094).

- **Type** – There are two types of private VLANs:

  - **Primary** – Conveys traffic between promiscuous ports, and to community ports within secondary (or community) VLANs.

  - **Community** - Conveys traffic between community ports, and to their promiscuous ports in the associated primary VLAN.

WEB INTERFACE

To configure private VLANs in the web interface:

1. Click VLAN, Private.

2. Select Configure VLAN from the Step list.

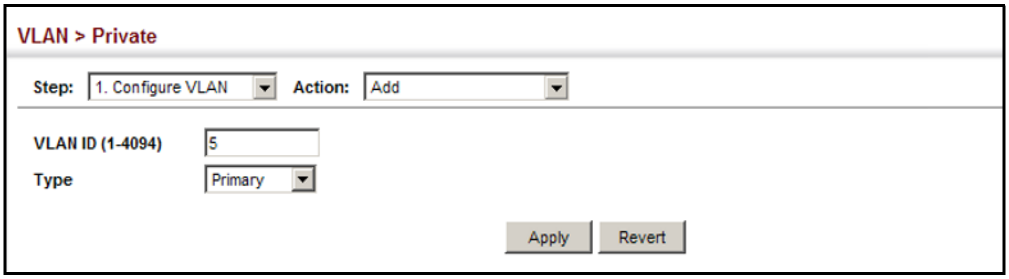
3. Select Add from the Action list.

4. Enter the VLAN ID to assign to the private VLAN.

5. Select Primary or Community from the Type list

6. Click Apply.

Figure 81: Configuring Private VLANs



VLAN > Private

Step: 1. Configure VLAN Action: Add

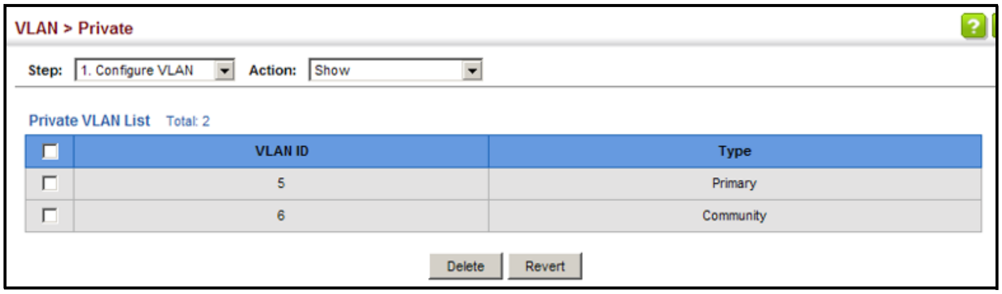
VLAN ID (1-4094) 5

Type Primary

To display a list of private VLANs in the web interface:

1. Click VLAN, Private.
2. Select Configure VLAN from the Step list.
3. Select Show from the Action list.

Figure 82: Showing Private VLANs



VLAN > Private

Step: 1. Configure VLAN Action: Show

Private VLAN List Total: 2

□	VLAN ID	Type
□	5	Primary
□	6	Community

NOTE: All member ports must be removed from the VLAN before it can be deleted.

ASSOCIATING PRIVATE VLANS

Use the VLAN > Private (Configure VLAN - Add Community VLAN) page to associate each community VLAN with a primary VLAN.

CLI REFERENCES

- "private vlan association" on page 1368

PARAMETERS

These parameters are displayed in the web interface:

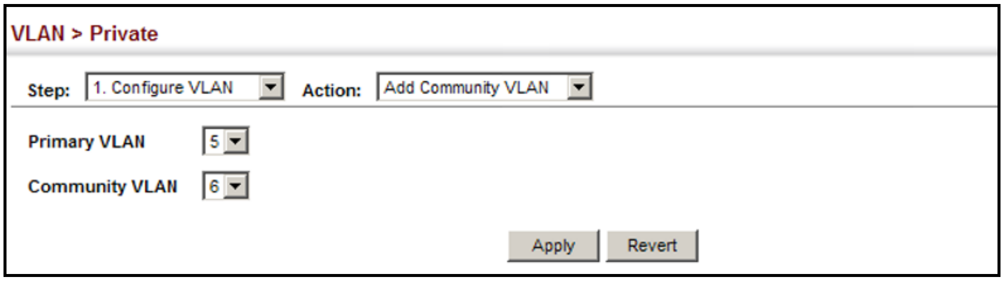
- **Primary VLAN** – ID of primary VLAN (2-4094).
- **Community VLAN** – VLAN associated with the selected primary VLAN.

WEB INTERFACE

To associate a community VLAN with a primary VLAN in the web interface:

1. Click VLAN, Private.
2. Select Configure VLAN from the Step list.
3. Select Add Community VLAN from the Action list.
4. Select an entry from the Primary VLAN list.
5. Select an entry from the Community VLAN list to associate it with the selected primary VLAN. Note that a community VLAN can only be associated with one primary VLAN.
6. Click Apply.

Figure 83: Associating Private VLANs



VLAN > Private

Step: 1. Configure VLAN Action: Add Community VLAN

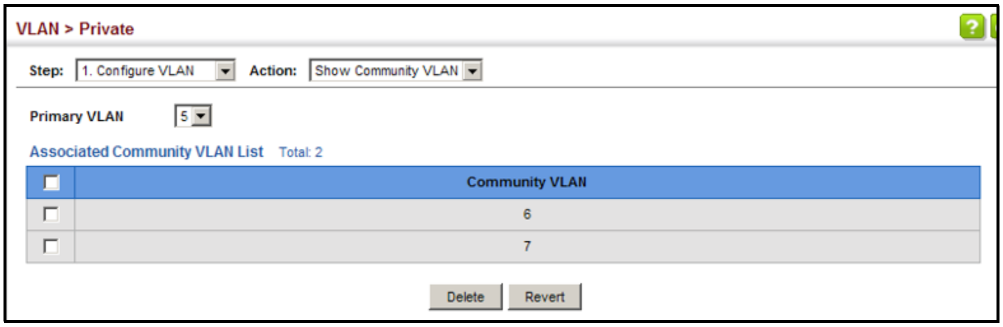
Primary VLAN: 5

Community VLAN: 6

To show a list of community VLANs associated with a primary VLAN in the web interface:

1. Click VLAN, Private.
2. Select Configure VLAN from the Step list.
3. Select Show Community VLAN from the Action list.
4. Select an entry from the Primary VLAN list.

Figure 84: Showing Associated VLANs



VLAN > Private

Step: 1. Configure VLAN Action: Show Community VLAN

Primary VLAN: 5

Associated Community VLAN List Total: 2

□	Community VLAN
□	6
□	7

CONFIGURING PRIVATE VLAN INTERFACES

Use the VLAN > Private (Configure Interface) page to set the private VLAN interface type, and assign the interfaces to a private VLAN.

CLI REFERENCES

- "switchport private-vlan mapping" on page 1370
- "switchport private-vlan host-association" on page 1370

PARAMETERS

These parameters are displayed in the web interface:

- **Interface** – Displays a list of ports or trunks.
- **Port** – Port Identifier. (Range: 1-28)
- **Trunk** – Trunk Identifier. (Range: 1-8)
- **Port/Trunk Mode** – Sets the private VLAN port types.
  - **Normal** – The port is not assigned to a private VLAN.
  - **Host** – The port is a community port. A community port can communicate with other ports in its own community VLAN and with designated promiscuous port(s).
  - **Promiscuous** – A promiscuous port can communicate with all interfaces within a private VLAN.
- **Primary VLAN** – Conveys traffic between promiscuous ports, and between promiscuous ports and community ports within the associated secondary VLANs. If Port Mode is “Promiscuous,” then specify the associated primary VLAN.
- **Community VLAN** – A community VLAN conveys traffic between community ports, and from community ports to their designated promiscuous ports. Set Port Mode to “Host,” and then specify the associated Community VLAN.

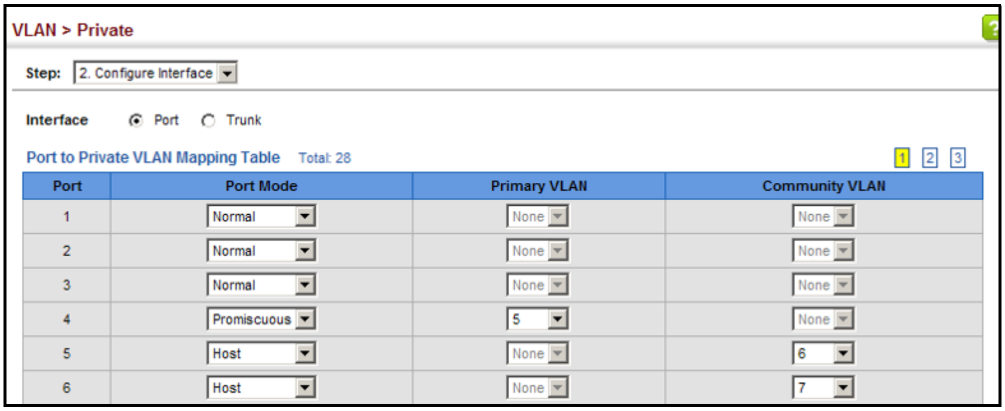
WEB INTERFACE

To configure a private VLAN port or trunk in the web interface:

1. Click VLAN, Private.
2. Select Configure Interface from the Step list.
3. Set the Interface type to display as Port or Trunk.
4. Set the Port Mode to Promiscuous.
5. For an interface set the Promiscuous mode, select an entry from the Primary VLAN list.
6. For an interface set the Host mode, select an entry from the Community VLAN list.

7. Click Apply.

Figure 85: Configuring Interfaces for Private VLANs



VLAN > Private

Step: 2. Configure Interface

Interface ● Port ○ Trunk

Port to Private VLAN Mapping Table Total: 28

Port	Port Mode	Primary VLAN	Community VLAN
1	Normal	None	None
2	Normal	None	None
3	Normal	None	None
4	Promiscuous	5	None
5	Host	None	6
6	Host	None	7

IEEE 802.1Q TUNNELING

IEEE 802.1Q Tunneling (QinQ) is designed for service providers carrying traffic for multiple customers across their networks. QinQ tunneling is used to maintain customer-specific VLAN and Layer 2 protocol configurations even when different customers use the same internal VLAN IDs. This is accomplished by inserting Service Provider VLAN (SPVLAN) tags into the customer's frames when they enter the service provider's network, and then stripping the tags when the frames leave the network.

A service provider's customers may have specific requirements for their internal VLAN IDs and number of VLANs supported. VLAN ranges required by different customers in the same service-provider network might easily overlap, and traffic passing through the infrastructure might be mixed. Assigning a unique range of VLAN IDs to each customer would restrict customer configurations, require intensive processing of VLAN mapping tables, and could easily exceed the maximum VLAN limit of 4096.

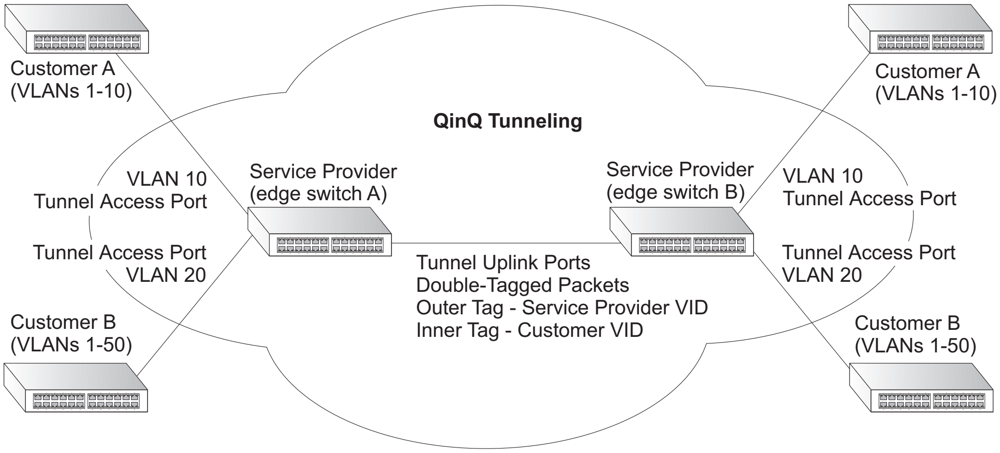
QinQ tunneling uses a single Service Provider VLAN (SPVLAN) for customers who have multiple VLANs. Customer VLAN IDs are preserved and traffic from different customers is segregated within the service provider's network even when they use the same customer-specific VLAN IDs. QinQ tunneling expands VLAN space by using a VLAN-in-VLAN hierarchy, preserving the customer's original tagged packets, and adding SPVLAN tags to each frame (also called double tagging).

A port configured to support QinQ tunneling must be set to tunnel port mode. The Service Provider VLAN (SPVLAN) ID for the specific customer must be assigned to the QinQ tunnel access port on the edge switch where the customer traffic enters the service provider's network. Each customer requires a separate SPVLAN, but this VLAN supports all of the customer's internal VLANs. The QinQ tunnel uplink port that passes traffic from the edge switch into the service provider's metro network must also be added to this SPVLAN. The uplink port can be added to multiple SPVLANs to carry inbound traffic for different customers onto the service provider's network.

When a double-tagged packet enters another trunk port in an intermediate or core switch in the service provider's network, the outer tag is stripped for packet processing. When the packet exits another trunk port on the same core switch, the same SPVLAN tag is again added to the packet.

When a packet enters the trunk port on the service provider's egress switch, the outer tag is again stripped for packet processing. However, the SPVLAN tag is not added when it is sent out the tunnel access port on the edge switch into the customer's network. The packet is sent as a normal IEEE 802.1Q-tagged frame, preserving the original VLAN numbers used in the customer's network.

Figure 86: QinQ Operational Concept



Layer 2 Flow for Packets Coming into a Tunnel Access Port

A QinQ tunnel port may receive either tagged or untagged packets. No matter how many tags the incoming packet has, it is treated as tagged packet.

The ingress process does source and destination lookups. If both lookups are successful, the ingress process writes the packet to memory. Then the egress process transmits the packet. Packets entering a QinQ tunnel port are processed in the following manner:

1. An SPVLAN tag is added to all outbound packets on the SPVLAN interface, no matter how many tags they already have. The switch constructs and inserts the outer tag (SPVLAN) into the packet based on the default VLAN ID and Tag Protocol Identifier (TPID, that is, the ether-type of the tag), unless otherwise defined as described under "Creating CVLAN to SPVLAN Mapping Entries" on page 248. The priority of the inner tag is copied to the outer tag if it is a tagged or priority tagged packet.

2. After successful source and destination lookup, the ingress process sends the packet to the switching process with two tags. If the incoming packet is untagged, the outer tag is an SPVLAN tag, and the inner tag is a dummy tag (8100 0000). If the incoming packet is tagged, the outer tag is an SPVLAN tag, and the inner tag is a CVLAN tag.

3. After packet classification through the switching process, the packet is written to memory with one tag (an outer tag) or with two tags (both an outer tag and inner tag).

4. The switch sends the packet to the proper egress port.

5. If the egress port is an untagged member of the SPVLAN, the outer tag will be stripped. If it is a tagged member, the outgoing packets will have two tags.

Layer 2 Flow for Packets Coming into a Tunnel Uplink Port

An uplink port receives one of the following packets:

- Untagged
- One tag (CVLAN or SPVLAN)
- Double tag (CVLAN + SPVLAN)

The ingress process does source and destination lookups. If both lookups are successful, the ingress process writes the packet to memory. Then the egress process transmits the packet. Packets entering a QinQ uplink port are processed in the following manner:

1. If incoming packets are untagged, the PVID VLAN native tag is added.

2. If the ether-type of an incoming packet (single or double tagged) is not equal to the TPID of the uplink port, the VLAN tag is determined to be a Customer VLAN (CVLAN) tag. The uplink port's PVID VLAN native tag is added to the packet. This outer tag is used for learning and switching packets within the service provider's network. The TPID must be configured on a per port basis, and the verification cannot be disabled.

3. If the ether-type of an incoming packet (single or double tagged) is equal to the TPID of the uplink port, no new VLAN tag is added. If the uplink port is not the member of the outer VLAN of the incoming packets, the packet will be dropped when ingress filtering is enabled. If ingress filtering is not enabled, the packet will still be forwarded. If the VLAN is not listed in the VLAN table, the packet will be dropped.

4. After successful source and destination lookups, the packet is double tagged. The switch uses the TPID of 0x8100 to indicate that an incoming packet is double-tagged. If the outer tag of an incoming double-tagged packet is equal to the port TPID and the inner tag is 0x8100, it is treated as a double-tagged packet. If a single-tagged packet has 0x8100 as its TPID, and port TPID is not 0x8100, a new VLAN tag is added and it is also treated as double-tagged packet.

5. If the destination address lookup fails, the packet is sent to all member ports of the outer tag's VLAN.

6. After packet classification, the packet is written to memory for processing as a single-tagged or double-tagged packet.

7. The switch sends the packet to the proper egress port.

8. If the egress port is an untagged member of the SPVLAN, the outer tag will be stripped. If it is a tagged member, the outgoing packet will have two tags.

Configuration Limitations for QinQ

- The native VLAN of uplink ports should not be used as the SPVLAN. If the SPVLAN is the uplink port's native VLAN, the uplink port must be an untagged member of the SPVLAN. Then the outer SPVLAN tag will be stripped when the packets are sent out. Another reason is that it causes non-customer packets to be forwarded to the SPVLAN.

- Static trunk port groups are compatible with QinQ tunnel ports as long as the QinQ configuration is consistent within a trunk port group.

- The native VLAN (VLAN 1) is not normally added to transmitted frames. Avoid using VLAN 1 as an SPVLAN tag for customer traffic to reduce the risk of misconfiguration. Instead, use VLAN 1 as a management VLAN instead of a data VLAN in the service provider network.

- There are some inherent incompatibilities between Layer 2 and Layer 3 switching:
  - Tunnel ports do not support IP Access Control Lists.
  - Layer 3 Quality of Service (QoS) and other QoS features containing Layer 3 information are not supported on tunnel ports.
  - Spanning tree bridge protocol data unit (BPDU) filtering is automatically disabled on a tunnel port.

General Configuration Guidelines for QinQ

1. Enable Tunnel Status, and set the Tag Protocol Identifier (TPID) value of the tunnel access port (in the Ethernet Type field). This step is required if the attached client is using a nonstandard 2-byte ethertype to identify 802.1Q tagged frames. The default ethertype value is 0x8100. (See "Enabling QinQ Tunneling on the Switch" on page 247.)

2. Create a Service Provider VLAN, also referred to as an SPVLAN (see "Configuring VLAN Groups" on page 228).

3. Configure the QinQ tunnel access port to Access mode (see "Adding an Interface to a QinQ Tunnel" on page 250).

4. Configure the QinQ tunnel access port to join the SPVLAN as an untagged member (see "Adding Static Members to VLANs" on page 231).

5. Configure the SPVLAN ID as the native VID on the QinQ tunnel access port (see "Adding Static Members to VLANs" on page 231).

6. Configure the QinQ tunnel uplink port to Uplink mode (see "Adding an Interface to a QinQ Tunnel" on page 250).

7. Configure the QinQ tunnel uplink port to join the SPVLAN as a tagged member (see "Adding Static Members to VLANs" on page 231).

ENABLING QINQ TUNNELING ON THE SWITCH

Use the VLAN > Tunnel (Configure Global) page to configure the switch to operate in IEEE 802.1Q (QinQ) tunneling mode, which is used for passing Layer 2 traffic across a service provider’s metropolitan area network. You can also globally set the Tag Protocol Identifier (TPID) value of the tunnel port if the attached client is using a nonstandard 2-byte ethertype to identify 802.1Q tagged frames.

CLI REFERENCES

- "Configuring IEEE 802.1Q Tunneling" on page 1353

PARAMETERS

These parameters are displayed:

- **Tunnel Status** – Sets the switch to QinQ mode. (Default: Disabled)

- **Ethernet Type** – The Tag Protocol Identifier (TPID) specifies the ethertype of incoming packets on a tunnel port. (Range: hexadecimal 8000-FFFF; Default: 8100)

  Use this field to set a custom 802.1Q ethertype value for the 802.1Q Tunnel TPID. This feature allows the switch to interoperate with third-party switches that do not use the standard 0x8100 ethertype to identify 802.1Q-tagged frames. For example, if 0x1234 is set as the custom 802.1Q ethertype on a trunk port, incoming frames containing that ethertype are assigned to the VLAN contained in the tag following the ethertype field, as they would be with a standard 802.1Q trunk. Frames arriving on the port containing any other ethertype are looked upon as untagged frames, and assigned to the native VLAN of that port.

  The specified ethertype only applies to ports configured in Uplink mode (see "Adding an Interface to a QinQ Tunnel" on page 250). If the port is in normal mode, the TPID is always 8100. If the port is in Access mode, received packets are processes as untagged packets.

WEB INTERFACE

To enable QinQ Tunneling on the switch:

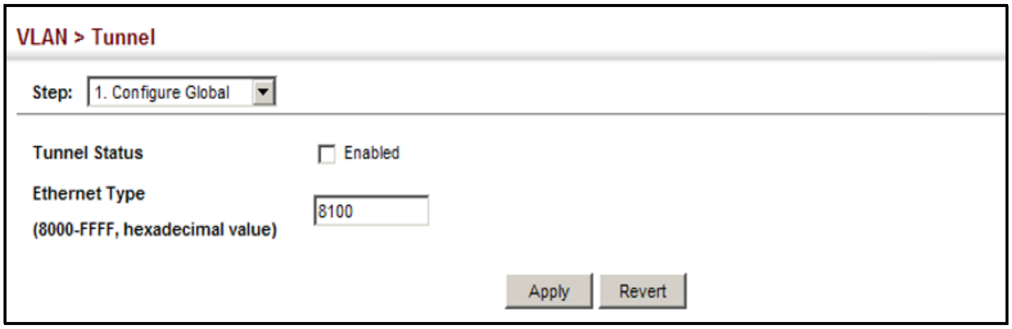
1. Click VLAN, Tunnel.

2. Select Configure Global from the Step list.

3. Enable Tunnel Status, and specify the TPID if a client attached to a tunnel port is using a non-standard ethertype to identify 802.1Q tagged frames.

4. Click Apply.

Figure 87: Enabling QinQ Tunneling



VLAN > Tunnel

Step: 1. Configure Global

Tunnel Status ☐ Enabled

Ethernet Type (8000-FFFF, hexadecimal value): 8100

CREATING CVLAN TO SPVLAN MAPPING ENTRIES

Use the VLAN > Tunnel (Configure Service) page to create a CVLAN to SPVLAN mapping entry.

CLI REFERENCES

- "switchport dot1q-tunnel service match cvid" on page 1356

COMMAND USAGE

- The inner VLAN tag of a customer packet entering the edge router of a service provider's network is mapped to an outer tag indicating the service provider VLAN that will carry this traffic across the 802.1Q tunnel. By default, the outer tag is based on the default VID of the edge router's ingress port. This process is performed in a transparent manner as described under "IEEE 802.1Q Tunneling" on page 243.

- When priority bits are found in the inner tag, these are also copied to the outer tag. This allows the service provider to differentiate service based on the indicated priority and appropriate methods of queue management at intermediate nodes across the tunnel.

- Rather than relying on standard service paths and priority queuing, QinQ VLAN mapping can be used to further enhance service by defining a set of differentiated service pathways to follow across the service provider's network for traffic arriving from specified inbound customer VLANs.

- Note that all customer interfaces should be configured as access interfaces (that is, a user-to-network interface) and service provider interfaces as uplink interfaces (that is, a network-to-network interface). Use the Configure Interface page described in the next section to set an interface to access or uplink mode.

PARAMETERS

These parameters are displayed:

- **Port** – Port identifier. (Range: 1-28)

- **Customer VLAN ID** – VLAN ID for the inner VLAN tag. (Range: 1-4094)

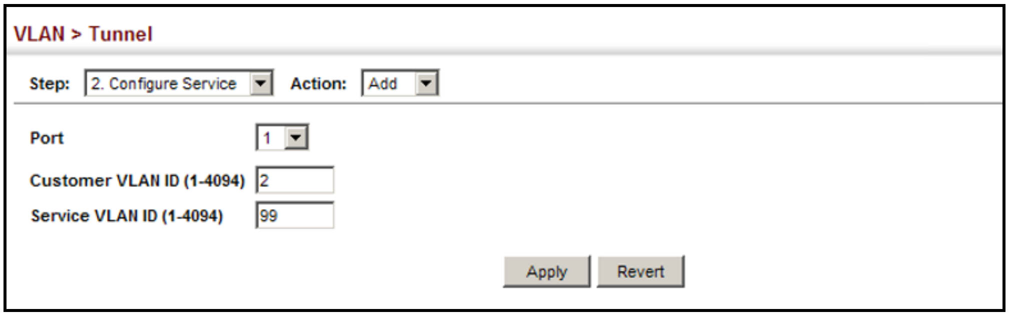
- **Service VLAN ID** – VLAN ID for the outer VLAN tag. (Range: 1-4094)

WEB INTERFACE

To configure a mapping entry:

1. Click VLAN, Tunnel.
2. Select Configure Service from the Step list.
3. Select Add from the Action list.
4. Select an interface from the Port list.
5. Specify the CVID to SVID mapping for packets exiting the specified port.
6. Click Apply.

Figure 88: Configuring CVLAN to SPVLAN Mapping Entries



VLAN > Tunnel

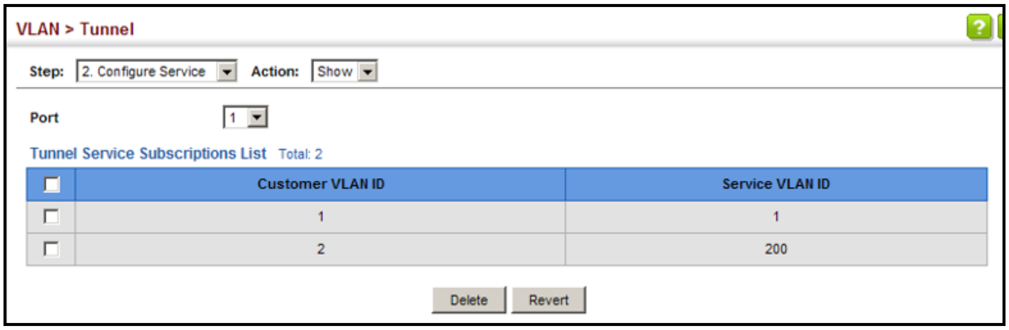
Step: 2. Configure Service Action: Add

Port	1
Customer VLAN ID (1-4094)	2
Service VLAN ID (1-4094)	99

To show the mapping table:

1. Click VLAN, Tunnel.
2. Select Configure Service from the Step list.
3. Select Show from the Action list.
4. Select an interface from the Port list.

Figure 89: Showing CVLAN to SPVLAN Mapping Entries



VLAN > Tunnel

Step: 2. Configure Service Action: Show

Port 1

Tunnel Service Subscriptions List Total: 2

□	Customer VLAN ID	Service VLAN ID
□	1	1
□	2	200

The preceding example sets the SVID to 99 in the outer tag for egress packets exiting port 1 when the packet's CVID is 2. For a more detailed example, see the switchport dot1q-tunnel service match cvid command.

ADDING AN INTERFACE TO A QINQ TUNNEL

Follow the guidelines in the preceding section to set up a QinQ tunnel on the switch. Then use the VLAN > Tunnel (Configure Interface) page to set the tunnel mode for any participating interface.

CLI REFERENCES

- "Configuring IEEE 802.1Q Tunneling" on page 1353

COMMAND USAGE

- Use the Configure Global page to set the switch to QinQ mode before configuring a tunnel access port or tunnel uplink port (see "Enabling QinQ Tunneling on the Switch" on page 247). Also set the Tag Protocol Identifier (TPID) value of the tunnel access port if the attached client is using a nonstandard 2-byte ethertype to identify 802.1Q tagged frames.

- Then use the Configure Interface page to set the access interface on the edge switch to Access mode, and set the uplink interface on the switch attached to the service provider network to Uplink mode.

PARAMETERS

These parameters are displayed:

- **Interface** – Displays a list of ports or trunks.

- **Port** – Port Identifier. (Range: 1-28)

- **Trunk** – Trunk Identifier. (Range: 1-8)

- **Mode** – Sets the VLAN membership mode of the port.
  - **None** – The port operates in its normal VLAN mode. (This is the default.)
  - **Access** – Configures QinQ tunneling for a client access port to segregate and preserve customer VLAN IDs for traffic crossing the service provider network.
  - **Uplink** – Configures QinQ tunneling for an uplink port to another device within the service provider network.

WEB INTERFACE

To add an interface to a QinQ tunnel:

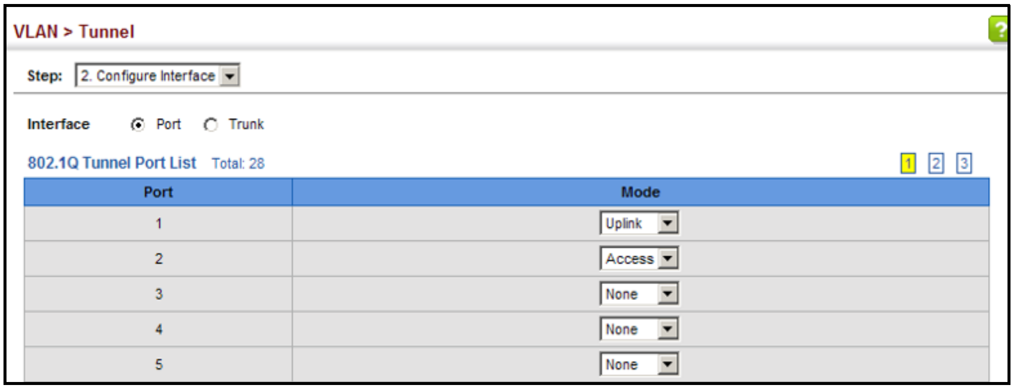
1. Click VLAN, Tunnel.

2. Select Configure Interface from the Step list.

3. Set the mode for any tunnel access port to Access and the tunnel uplink port to Uplink.

4. Click Apply.

Figure 90: Adding an Interface to a QinQ Tunnel



VLAN > Tunnel

Step: 2. Configure Interface

Interface ● Port ○ Trunk

802.1Q Tunnel Port List Total: 28

Port	Mode
1	Uplink
2	Access
3	None
4	None
5	None

PROTOCOL VLANS

The network devices required to support multiple protocols cannot be easily grouped into a common VLAN. This may require non-standard devices to pass traffic between different VLANs in order to encompass all the devices participating in a specific protocol. This kind of configuration deprives users of the basic benefits of VLANs, including security and easy accessibility.

To avoid these problems, you can configure this switch with protocol-based VLANs that divide the physical network into logical VLAN groups for each required protocol. When a frame is received at a port, its VLAN membership can then be determined based on the protocol type being used by the inbound packets.

COMMAND USAGE

- To configure protocol-based VLANs, follow these steps:

  1. First configure VLAN groups for the protocols you want to use (see "Configuring VLAN Groups" on page 228). Although not mandatory, we suggest configuring a separate VLAN for each major protocol running on your network. Do not add port members at this time.

  2. Create a protocol group for each of the protocols you want to assign to a VLAN using the Configure Protocol (Add) page.

  3. Then map the protocol for each interface to the appropriate VLAN using the Configure Interface (Add) page.

- When MAC-based, IP subnet-based, and protocol-based VLANs are supported concurrently, priority is applied in this sequence, and then port-based VLANs last.

CONFIGURING PROTOCOL VLAN GROUPS

Use the VLAN > Protocol (Configure Protocol - Add) page to create protocol groups.

CLI REFERENCES

- "protocol-vlan protocol-group (Configuring Groups)" on page 1372

PARAMETERS

These parameters are displayed:

- **Frame Type** – Choose either Ethernet, RFC 1042, or LLC Other as the frame type used by this protocol.
- **Protocol Type** – Specifies the protocol type to match. The available options are IP, ARP, RARP and IPv6. If LLC Other is chosen for the Frame Type, the only available Protocol Type is IPX Raw.
- **Protocol Group ID** – Protocol Group ID assigned to the Protocol VLAN Group. (Range: 1-2147483647)

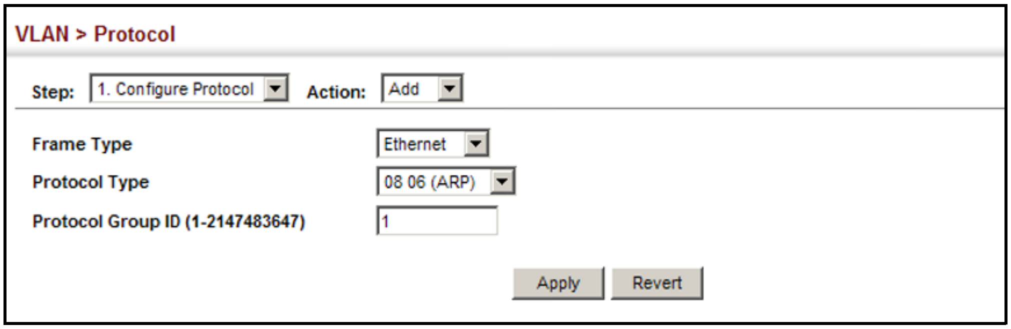
NOTE: Traffic which matches IP Protocol Ethernet Frames is mapped to the VLAN (VLAN 1) that has been configured with the switch's administrative IP. IP Protocol Ethernet traffic must not be mapped to another VLAN or you will lose administrative network connectivity to the switch. If lost in this manner, network access can be regained by removing the offending Protocol VLAN rule via the console. Alternately, the switch can be power-cycled, however all unsaved configuration changes will be lost.

WEB INTERFACE

To configure a protocol group:

1. Click VLAN, Protocol.
2. Select Configure Protocol from the Step list.
3. Select Add from the Action list.
4. Select an entry from the Frame Type list.
5. Select an entry from the Protocol Type list.
6. Enter an identifier for the protocol group.
7. Click Apply.

Figure 91: Configuring Protocol VLANs



VLAN > Protocol

Step: 1. Configure Protocol Action: Add

Frame Type: Ethernet

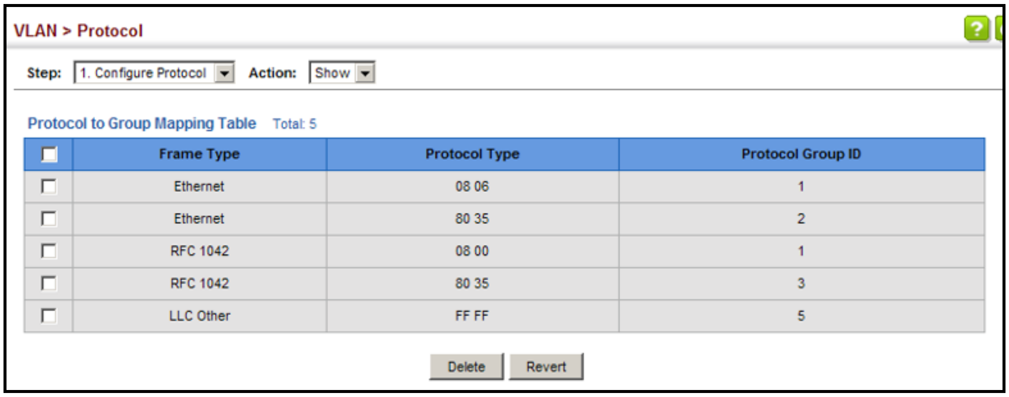
Protocol Type: 08 06 (ARP)

Protocol Group ID (1-2147483647): 1

To configure a protocol group:

1. Click VLAN, Protocol.
2. Select Configure Protocol from the Step list.
3. Select Show from the Action list.

Figure 92: Displaying Protocol VLANs



VLAN > Protocol

Step: 1. Configure Protocol Action: Show

Protocol to Group Mapping Table Total: 5

□	Frame Type	Protocol Type	Protocol Group ID
□	Ethernet	08 06	1
□	Ethernet	80 35	2
□	RFC 1042	08 00	1
□	RFC 1042	80 35	3
□	LLC Other	FF FF	5

MAPPING PROTOCOL GROUPS TO INTERFACES

Use the VLAN > Protocol (Configure Interface - Add) page to map a protocol group to a VLAN for each interface that will participate in the group.

CLI REFERENCES

- "protocol-vlan protocol-group (Configuring Interfaces)" on page 1373

COMMAND USAGE

- When creating a protocol-based VLAN, only assign interfaces using this configuration screen. If you assign interfaces using any of the other VLAN menus such as the VLAN Static table (page 231), these interfaces will admit traffic of any protocol type into the associated VLAN.

- When a frame enters a port that has been assigned to a protocol VLAN, it is processed in the following manner:
  - If the frame is tagged, it will be processed according to the standard rules applied to tagged frames.
  - If the frame is untagged and the protocol type matches, the frame is forwarded to the appropriate VLAN.
  - If the frame is untagged but the protocol type does not match, the frame is forwarded to the default VLAN for this interface.

PARAMETERS

These parameters are displayed:

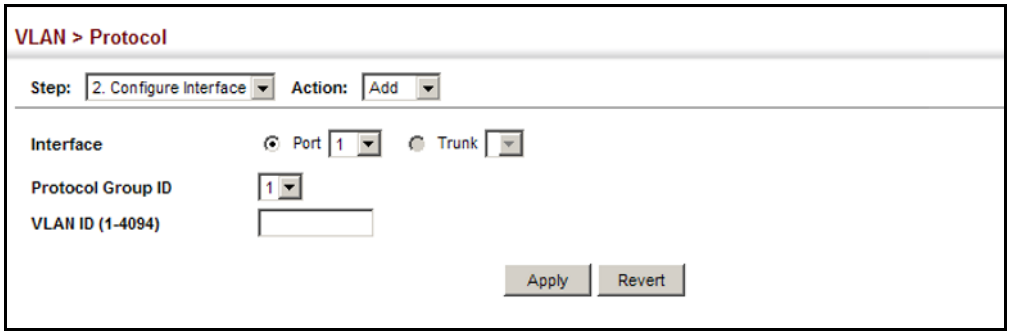
- **Interface** – Displays a list of ports or trunks.
- **Port** – Port Identifier. (Range: 1-28)
- **Trunk** – Trunk Identifier. (Range: 1-8)
- **Protocol Group ID** – Protocol Group ID assigned to the Protocol VLAN Group. (Range: 1-2147483647)
- **VLAN ID** – VLAN to which matching protocol traffic is forwarded. (Range: 1-4094)

WEB INTERFACE

To map a protocol group to a VLAN for a port or trunk:

1. Click VLAN, Protocol.
2. Select Configure Interface from the Step list.
3. Select Add from the Action list.
4. Select a port or trunk.
5. Enter the identifier for a protocol group.
6. Enter the corresponding VLAN to which the protocol traffic will be forwarded.
7. Click Apply.

Figure 93: Assigning Interfaces to Protocol VLANs



VLAN > Protocol

Step: 2. Configure Interface Action: Add

Interface ● Port 1 ○ Trunk

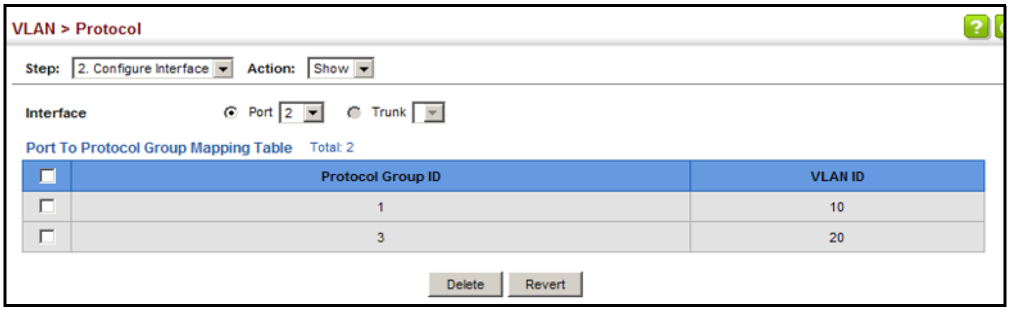
Protocol Group ID 1

VLAN ID (1-4094)

To show the protocol groups mapped to a port or trunk:

1. Click VLAN, Protocol.
2. Select Configure Interface from the Step list.
3. Select Show from the Action list.
4. Select a port or trunk.

Figure 94: Showing the Interface to Protocol Group Mapping



VLAN > Protocol

Step: 2. Configure Interface Action: Show

Interface ● Port 2 ○ Trunk

Port To Protocol Group Mapping Table Total: 2

□	Protocol Group ID	VLAN ID
□	1	10
□	3	20

CONFIGURING IP SUBNET VLANS

Use the VLAN > IP Subnet page to configure IP subnet-based VLANs.

When using port-based classification, all untagged frames received by a port are classified as belonging to the VLAN whose VID (PVID) is associated with that port.

When IP subnet-based VLAN classification is enabled, the source address of untagged ingress frames are checked against the IP subnet-to-VLAN mapping table. If an entry is found for that subnet, these frames are assigned to the VLAN indicated in the entry. If no IP subnet is matched, the untagged frames are classified as belonging to the receiving port's VLAN ID (PVID).

CLI REFERENCES

- "Configuring IP Subnet VLANs" on page 1375

COMMAND USAGE

- Each IP subnet can be mapped to only one VLAN ID. An IP subnet consists of an IP address and a mask. The specified VLAN need not be an existing VLAN.

- When an untagged frame is received by a port, the source IP address is checked against the IP subnet-to-VLAN mapping table, and if an entry is found, the corresponding VLAN ID is assigned to the frame. If no mapping is found, the PVID of the receiving port is assigned to the frame.

- The IP subnet cannot be a broadcast or multicast IP address.

- When MAC-based, IP subnet-based, and protocol-based VLANs are supported concurrently, priority is applied in this sequence, and then port-based VLANs last.

PARAMETERS

These parameters are displayed:

- **IP Address** – The IP address for a subnet. Valid IP addresses consist of four decimal numbers, 0 to 255, separated by periods.

- **Subnet Mask** – This mask identifies the host address bits of the IP subnet.

- **VLAN** – VLAN to which matching IP subnet traffic is forwarded. (Range: 1-4094)

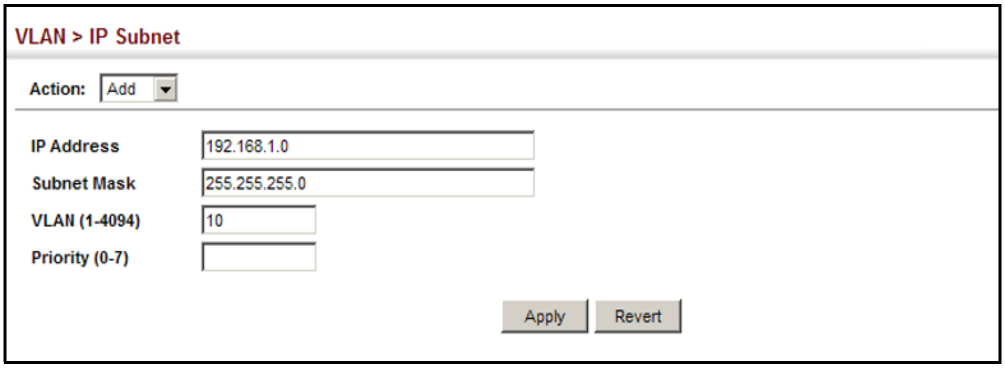
- **Priority** – The priority assigned to untagged ingress traffic. (Range: 0-7, where 7 is the highest priority; Default: 0)

WEB INTERFACE

To map an IP subnet to a VLAN:

1. Click VLAN, IP Subnet.
2. Select Add from the Action list.
3. Enter an address in the IP Address field.
4. Enter a mask in the Subnet Mask field.
5. Enter the identifier in the VLAN field. Note that the specified VLAN need not already be configured.
6. Enter a value to assign to untagged frames in the Priority field.
7. Click Apply.

Figure 95: Configuring IP Subnet VLANs



VLAN > IP Subnet

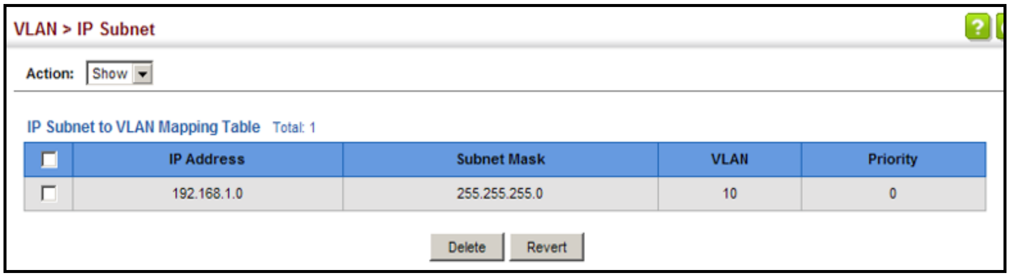
Action: Add

IP Address	192.168.1.0
Subnet Mask	255.255.255.0
VLAN (1-4094)	10
Priority (0-7)	

To show the configured IP subnet VLANs:

1. Click VLAN, IP Subnet.
2. Select Show from the Action list.

Figure 96: Showing IP Subnet VLANs



VLAN > IP Subnet

Action: Show

IP Subnet to VLAN Mapping Table Total: 1

□	IP Address	Subnet Mask	VLAN	Priority
□	192.168.1.0	255.255.255.0	10	0

CONFIGURING MAC-BASED VLANS

Use the VLAN > MAC-Based page to configure VLAN based on MAC addresses. The MAC-based VLAN feature assigns VLAN IDs to ingress untagged frames according to source MAC addresses.

When MAC-based VLAN classification is enabled, untagged frames received by a port are assigned to the VLAN which is mapped to the frame's source MAC address. When no MAC address is matched, untagged frames are assigned to the receiving port's native VLAN ID (PVID).

CLI REFERENCES

- "Configuring MAC Based VLANs" on page 1377

COMMAND USAGE

- The MAC-to-VLAN mapping applies to all ports on the switch.
- Source MAC addresses can be mapped to only one VLAN ID.
- Configured MAC addresses cannot be broadcast or multicast addresses.
- When MAC-based, IP subnet-based, and protocol-based VLANs are supported concurrently, priority is applied in this sequence, and then port-based VLANs last.

PARAMETERS

These parameters are displayed:

- **MAC Address** – A source MAC address which is to be mapped to a specific VLAN. The MAC address must be specified in the format xx-xx-xx-xx-xx-xx or xxxxxxxxxxxx.
- **VLAN** – VLAN to which ingress traffic matching the specified source MAC address is forwarded. (Range: 1-4094)
- **Priority** – The priority assigned to untagged ingress traffic. (Range: 0-7, where 7 is the highest priority; Default: 0)

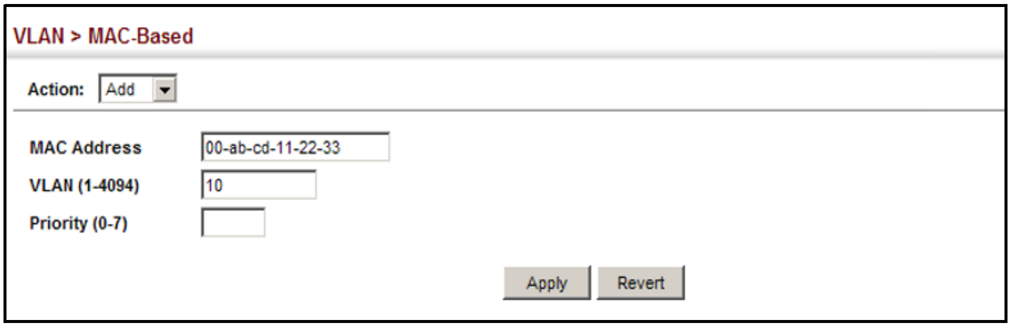
WEB INTERFACE

To map a MAC address to a VLAN:

1. Click VLAN, MAC-Based.
2. Select Add from the Action list.
3. Enter an address in the MAC Address field.
4. Enter an identifier in the VLAN field. Note that the specified VLAN need not already be configured.
5. Enter a value to assign to untagged frames in the Priority field.

6. Click Apply.

Figure 97: Configuring MAC-Based VLANs



VLAN > MAC-Based

Action: Add

MAC Address: 00-ab-cd-11-22-33

VLAN (1-4094): 10

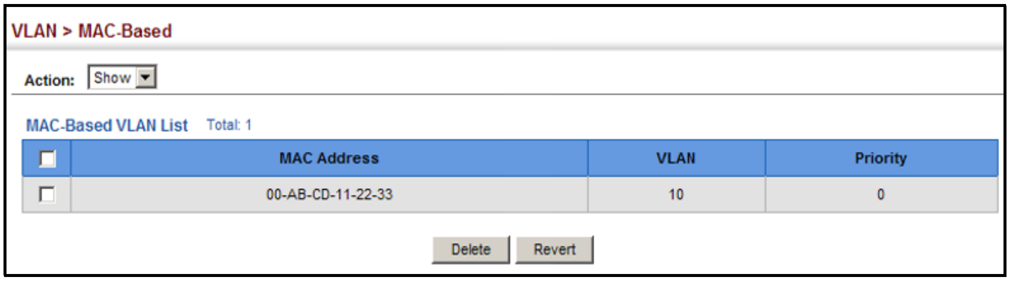
Priority (0-7):

To show the MAC addresses mapped to a VLAN:

1. Click VLAN, MAC-Based.

2. Select Show from the Action list.

Figure 98: Showing MAC-Based VLANs



VLAN > MAC-Based

Action: Show

MAC-Based VLAN List Total: 1

□	MAC Address	VLAN	Priority
□	00-AB-CD-11-22-33	10	0

CONFIGURING VLAN TRANSLATION

Use the VLAN > Translation (Add) page to map VLAN IDs between the customer and service provider for networks that do not support IEEE 802.1Q tunneling.

CLI REFERENCES

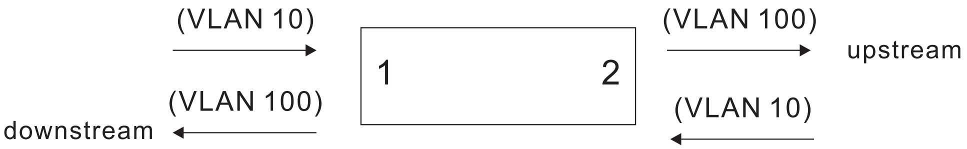
- "Configuring VLAN Translation" on page 1364

COMMAND USAGE

- QinQ tunneling uses double tagging to preserve the customer’s VLAN tags on traffic crossing the service provider’s network. However, if any switch in the path crossing the service provider’s network does not support this feature, then the switches directly connected to that device can be configured to swap the customer’s VLAN ID with the service provider’s VLAN ID for upstream traffic, or the service provider’s VLAN ID with the customer’s VLAN ID for downstream traffic.

  For example, assume that the upstream switch does not support QinQ tunneling. Select Port 1, and set the Old VLAN to 10 and the New VLAN to 100 to map VLAN 10 to VLAN 100 for upstream traffic entering port 1, and VLAN 100 to VLAN 10 for downstream traffic leaving port 1 as shown below.

Figure 99: Configuring VLAN Translation



- The maximum number of VLAN translation entries is 8 per port, and up to 96 for the system. However, note that configuring a large number of entries may degrade the performance of other processes that also use the TCAM, such as IP Source Guard filter rules, Quality of Service (QoS) processes, QinQ, MAC-based VLANs, VLAN translation, or traps.

- If VLAN translation is set on an interface, and the same interface is also configured as a QinQ access port on the VLAN > Tunnel (Configure Interface) page, VLAN tag assignments will be determined by the QinQ process, not by VLAN translation.

PARAMETERS

These parameters are displayed:

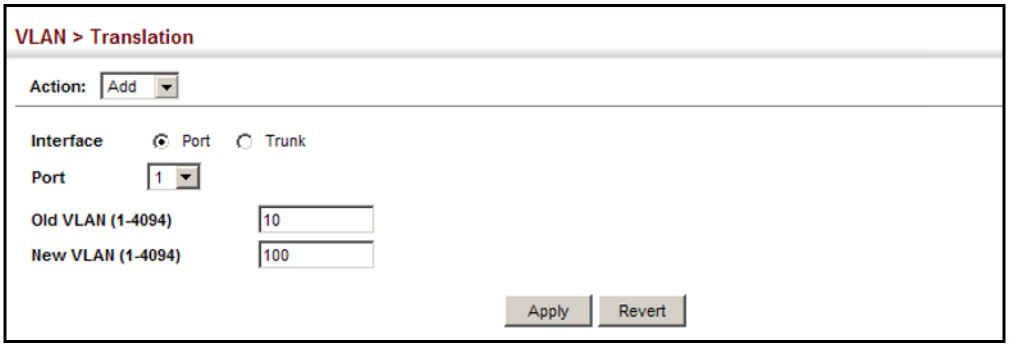
- **Interface** – Port or trunk identifier.
- **Old VLAN** – The original VLAN ID. (Range: 1-4094)
- **New VLAN** – The new VLAN ID. (Range: 1-4094)

WEB INTERFACE

To configure VLAN translation:

1. Click VLAN, Translation.
2. Select Add from the Action list.
3. Select a port, and enter the original and new VLAN IDs.
4. Click Apply.

Figure 100: Configuring VLAN Translation



VLAN > Translation

Action: Add

Interface ● Port ○ Trunk

Port 1

Old VLAN (1-4094) 10

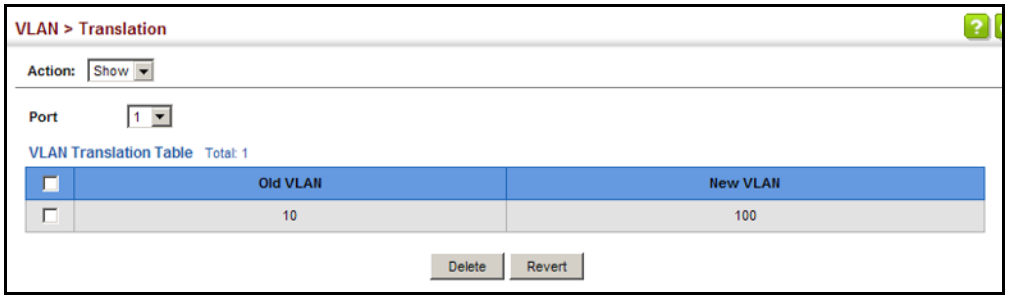
New VLAN (1-4094) 100

To show the mapping entries for VLANs translation:

1. Click VLAN, Translation.

2. Select Show from the Action list.

Figure 101: Showing the Entries for VLAN Translation



VLAN > Translation

Action: Show

Port 1

VLAN Translation Table Total: 1

□	Old VLAN	New VLAN
□	10	100

7 ADDRESS TABLE SETTINGS

Switches store the addresses for all known devices. This information is used to pass traffic directly between the inbound and outbound ports. All the addresses learned by monitoring traffic are stored in the dynamic address table. You can also manually configure static addresses that are bound to a specific port.

This chapter describes the following topics:

- MAC Address Learning – Enables or disables address learning on an interface.
- Static MAC Addresses – Configures static entries in the address table.
- Address Aging Time – Sets timeout for dynamically learned entries.
- Dynamic Address Cache – Shows dynamic entries in the address table.

CONFIGURING MAC ADDRESS LEARNING

Use the MAC Address > Learning Status page to enable or disable MAC address learning on an interface.

CLI REFERENCES

- "mac-learning" on page 1090

COMMAND USAGE

- When MAC address learning is disabled, the switch immediately stops learning new MAC addresses on the specified interface. Only incoming traffic with source addresses stored in the static address table (see "Setting Static Addresses" on page 265) will be accepted as authorized to access the network through that interface.
- Dynamic addresses stored in the address table when MAC address learning is disabled are flushed from the system, and no dynamic addresses are subsequently learned until MAC address learning has been re-enabled. Any device not listed in the static address table that attempts to use the interface after MAC learning has been disabled will be prevented from accessing the switch.

- Also note that MAC address learning cannot be disabled if any of the following conditions exist:
  - 802.1X Port Authentication has been globally enabled on the switch (see "Configuring 802.1X Global Settings" on page 424).
  - Security Status (see "Configuring Port Security" on page 420) is enabled on the same interface.

PARAMETERS

These parameters are displayed:

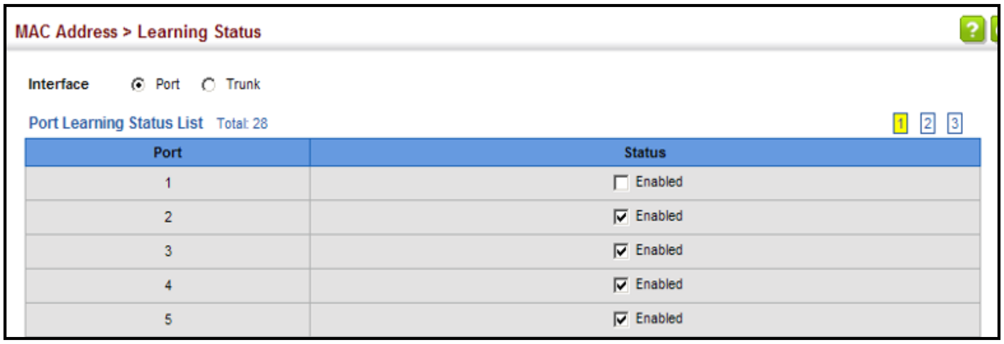
- **Interface** – Displays a list of ports or trunks.
- **Port** – Port Identifier. (Range: 1-28)
- **Trunk** – Trunk Identifier. (Range: 1-8)
- **Status** – The status of MAC address learning. (Default: Enabled)

WEB INTERFACE

To enable or disable MAC address learning:

1. Click MAC Address, Learning Status.
2. Set the learning status for any interface.
3. Click Apply.

Figure 102: Configuring MAC Address Learning



MAC Address > Learning Status

Interface ● Port ○ Trunk

Port Learning Status List Total: 28

Port	Status
1	☐ Enabled
2	☑ Enabled
3	☑ Enabled
4	☑ Enabled
5	☑ Enabled

SETTING STATIC ADDRESSES

Use the MAC Address > Static page to configure static MAC addresses. A static address can be assigned to a specific interface on this switch. Static addresses are bound to the assigned interface and will not be moved. When a static address is seen on another interface, the address will be ignored and will not be written to the address table.

CLI REFERENCES

- "mac-address-table static" on page 1272

COMMAND USAGE

The static address for a host device can be assigned to a specific port within a specific VLAN. Use this command to add static addresses to the MAC Address Table. Static addresses have the following characteristics:

- Static addresses are bound to the assigned interface and will not be moved. When a static address is seen on another interface, the address will be ignored and will not be written to the address table.
- Static addresses will not be removed from the address table when a given interface link is down.
- A static address cannot be learned on another port until the address is removed from the table.

PARAMETERS

These parameters are displayed:

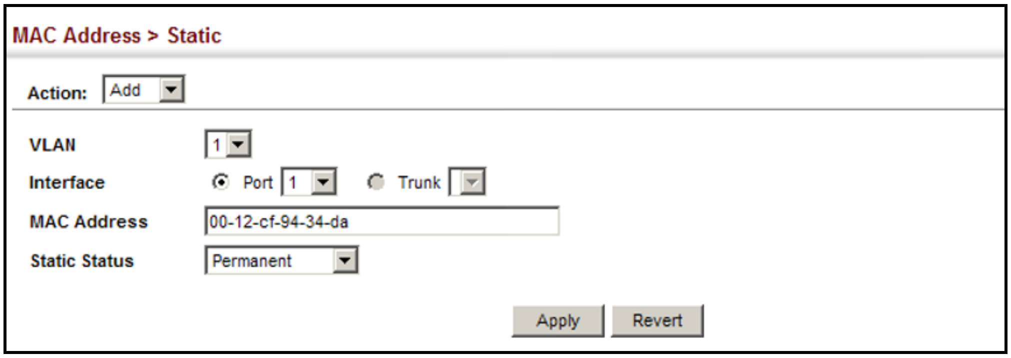
- **VLAN** – ID of configured VLAN. (Range: 1-4094)
- **Interface** – Port or trunk associated with the device assigned a static address.
- **MAC Address** – Physical address of a device mapped to this interface. Enter an address in the form of xx-xx-xx-xx-xx-xx or xxxxxxxxxxxx.
- **Static Status** – Sets the time to retain the specified address.
  - Delete-on-reset - Assignment lasts until the switch is reset.
  - Permanent - Assignment is permanent. (This is the default.)

WEB INTERFACE

To configure a static MAC address:

1. Click MAC Address, Static.
2. Select Add from the Action list.
3. Specify the VLAN, the port or trunk to which the address will be assigned, the MAC address, and the time to retain this entry.
4. Click Apply.

Figure 103: Configuring Static MAC Addresses



MAC Address > Static

Action: Add

VLAN: 1

Interface: ● Port 1 ○ Trunk

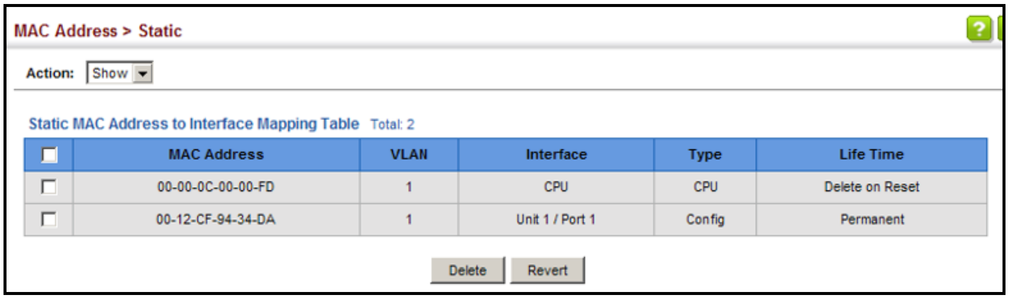
MAC Address: 00-12-cf-94-34-da

Static Status: Permanent

To show the static addresses in MAC address table:

1. Click MAC Address, Static.
2. Select Show from the Action list.

Figure 104: Displaying Static MAC Addresses



MAC Address > Static

Action: Show

Static MAC Address to Interface Mapping Table Total: 2

□	MAC Address	VLAN	Interface	Type	Life Time
□	00-00-0C-00-00-FD	1	CPU	CPU	Delete on Reset
□	00-12-CF-94-34-DA	1	Unit 1 / Port 1	Config	Permanent

CHANGING THE AGING TIME

Use the MAC Address > Dynamic (Configure Aging) page to set the aging time for entries in the dynamic address table. The aging time is used to age out dynamically learned forwarding information.

CLI REFERENCES

- "mac-address-table aging-time" on page 1271

PARAMETERS

These parameters are displayed:

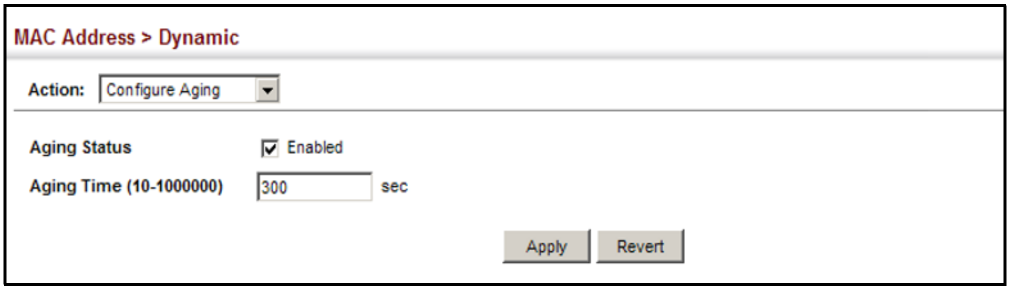
- **Aging Status** – Enables/disables the function.
- **Aging Time** – The time after which a learned entry is discarded. (Range: 10-1000000 seconds; Default: 300 seconds)

WEB INTERFACE

To set the aging time for entries in the dynamic address table:

1. Click MAC Address, Dynamic.
2. Select Configure Aging from the Action list.
3. Modify the aging status if required.
4. Specify a new aging time.
5. Click Apply.

Figure 105: Setting the Address Aging Time



MAC Address > Dynamic

Action: Configure Aging

Aging Status ☑ Enabled

Aging Time (10-1000000) 300 sec

DISPLAYING THE DYNAMIC ADDRESS TABLE

Use the MAC Address > Dynamic (Show Dynamic MAC) page to display the MAC addresses learned by monitoring the source address for traffic entering the switch. When the destination address for inbound traffic is found in the database, the packets intended for that address are forwarded directly to the associated port. Otherwise, the traffic is flooded to all ports.

CLI REFERENCES

- "show mac-address-table" on page 1273

PARAMETERS

These parameters are displayed:

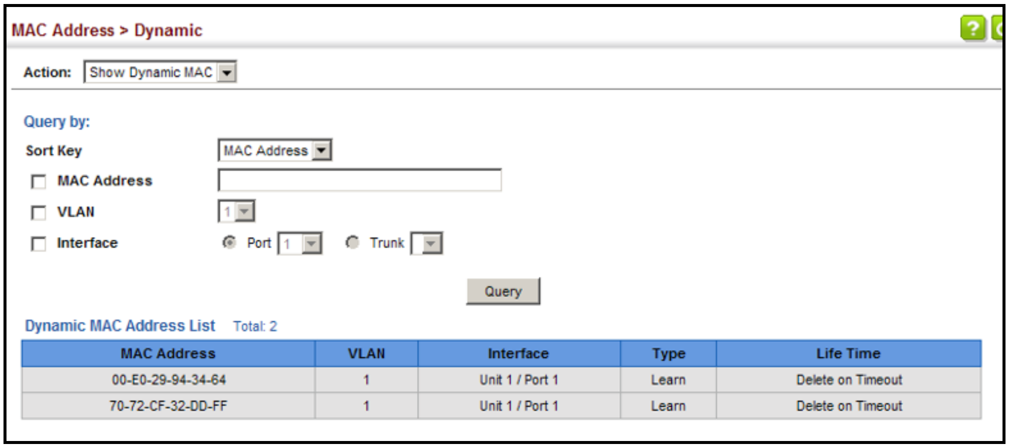
- **Sort Key** - You can sort the information displayed based on MAC address, VLAN or interface (port or trunk).
- **MAC Address** – Physical address associated with this interface.
- **VLAN** – ID of configured VLAN (1-4094).
- **Interface** – Indicates a port or trunk.
- **Type** – Shows that the entries in this table are learned.
- **Life Time** – Shows the time to retain the specified address.

WEB INTERFACE

To show the dynamic address table:

1. Click MAC Address, Dynamic.
2. Select Show Dynamic MAC from the Action list.
3. Select the Sort Key (MAC Address, VLAN, or Interface).
4. Enter the search parameters (MAC Address, VLAN, or Interface).
5. Click Query.

Figure 106: Displaying the Dynamic MAC Address Table



MAC Address > Dynamic

Action: Show Dynamic MAC

Query by:

Sort Key: MAC Address

□ MAC Address

□ VLAN: 1

□ Interface: ● Port 1 ○ Trunk

Dynamic MAC Address List Total: 2

MAC Address	VLAN	Interface	Type	Life Time
00-E0-29-94-34-64	1	Unit 1 / Port 1	Learn	Delete on Timeout
70-72-CF-32-DD-FF	1	Unit 1 / Port 1	Learn	Delete on Timeout

CLEARING THE DYNAMIC ADDRESS TABLE

Use the MAC Address > Dynamic (Clear Dynamic MAC) page to remove any learned entries from the forwarding database.

CLI REFERENCES

- "clear mac-address-table dynamic" on page 1273

PARAMETERS

These parameters are displayed:

- **Clear by** – All entries can be cleared; or you can clear the entries for a specific MAC address, all the entries in a VLAN, or all the entries associated with a port or trunk.

WEB INTERFACE

To clear the entries in the dynamic address table:

1. Click MAC Address, Dynamic.

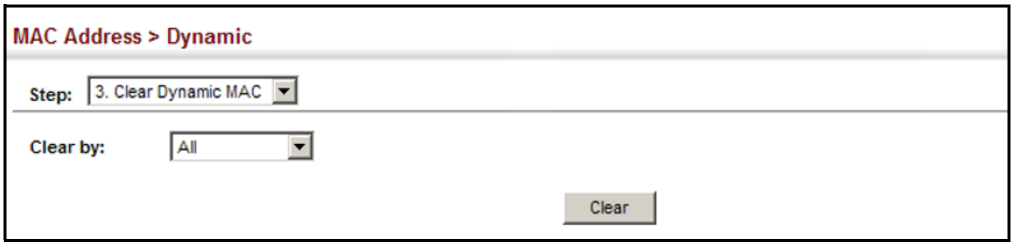
2. Select Clear Dynamic MAC from the Action list.

3. Select the method by which to clear the entries (i.e., All, MAC Address, VLAN, or Interface).

4. Enter information in the additional fields required for clearing entries by MAC Address, VLAN, or Interface.

5. Click Clear.

Figure 107: Clearing Entries in the Dynamic MAC Address Table



MAC Address > Dynamic

Step: 3. Clear Dynamic MAC

Clear by: All

8 Spanning Tree Algorithm

This chapter describes the following basic topics:

- Loopback Detection – Configures detection and response to loopback BPDUs.
- Global Settings for STA – Configures global bridge settings for STP, RSTP and MSTP.
- Interface Settings for STA – Configures interface settings for STA, including priority, path cost, link type, and designation as an edge port.
- Global Settings for MSTP – Sets the VLANs and associated priority assigned to an MST instance
- Interface Settings for MSTP – Configures interface settings for MSTP, including priority and path cost.

Overview

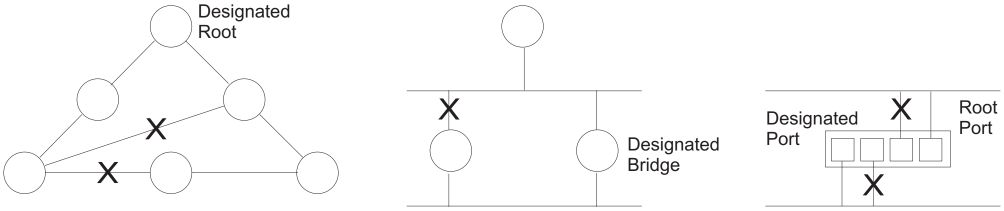
The Spanning Tree Algorithm (STA) can be used to detect and disable network loops, and to provide backup links between switches, bridges or routers. This allows the switch to interact with other bridging devices (that is, an STA-compliant switch, bridge or router) in your network to ensure that only one route exists between any two stations on the network, and provide backup links which automatically take over when a primary link goes down.

The spanning tree algorithms supported by this switch include these versions:

- STP – Spanning Tree Protocol (IEEE 802.1D)
- RSTP – Rapid Spanning Tree Protocol (IEEE 802.1w)
- MSTP – Multiple Spanning Tree Protocol (IEEE 802.1s)

STP – STP uses a distributed algorithm to select a bridging device (STP-compliant switch, bridge or router) that serves as the root of the spanning tree network. It selects a root port on each bridging device (except for the root device) which incurs the lowest path cost when forwarding a packet from that device to the root device. Then it selects a designated bridging device from each LAN which incurs the lowest path cost when forwarding a packet from that LAN to the root device. All ports connected to designated bridging devices are assigned as designated ports. After determining the lowest cost spanning tree, it enables all root ports and designated ports, and disables all other ports. Network packets are therefore only forwarded between root ports and designated ports, eliminating any possible network loops.

Figure 108: STP Root Ports and Designated Ports

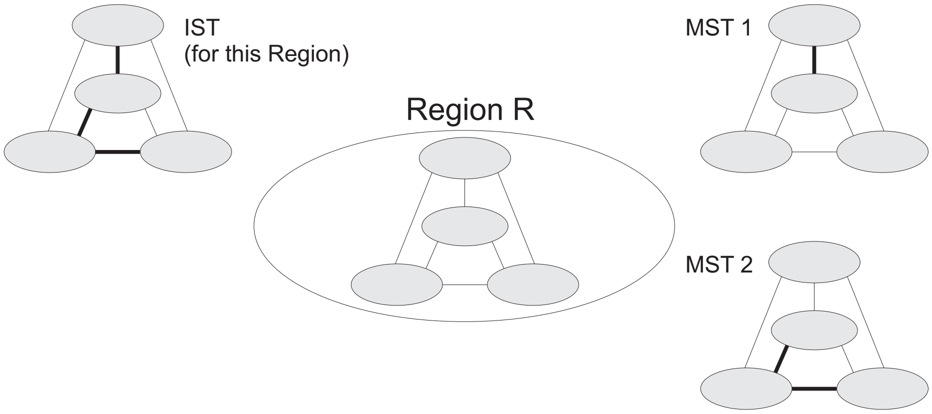


Once a stable network topology has been established, all bridges listen for Hello BPDUs (Bridge Protocol Data Units) transmitted from the Root Bridge. If a bridge does not get a Hello BPDU after a predefined interval (Maximum Age), the bridge assumes that the link to the Root Bridge is down. This bridge will then initiate negotiations with other bridges to reconfigure the network to reestablish a valid network topology.

RSTP – RSTP is designed as a general replacement for the slower, legacy STP. RSTP is also incorporated into MSTP. RSTP achieves much faster reconfiguration (i.e., around 1 to 3 seconds, compared to 30 seconds or more for STP) by reducing the number of state changes before active ports start learning, predefining an alternate route that can be used when a node or port fails, and retaining the forwarding database for ports insensitive to changes in the tree structure when reconfiguration occurs.

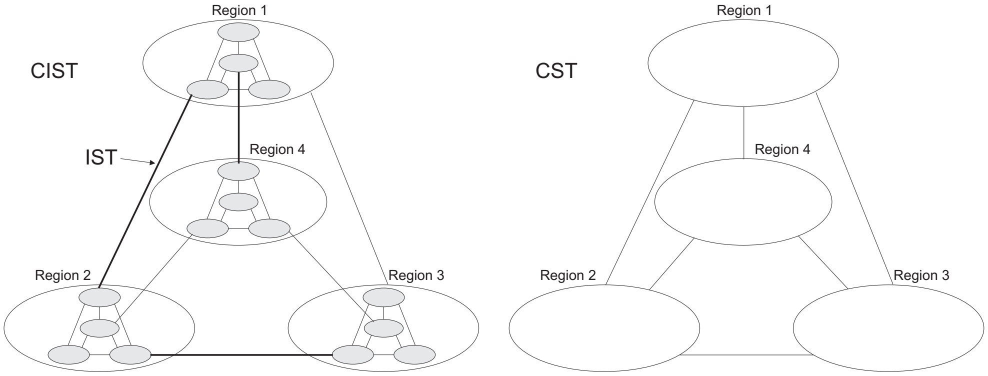
MSTP – When using STP or RSTP, it may be difficult to maintain a stable path between all VLAN members. Frequent changes in the tree structure can easily isolate some of the group members. MSTP (which is based on RSTP for fast convergence) is designed to support independent spanning trees based on VLAN groups. Using multiple spanning trees can provide multiple forwarding paths and enable load balancing. One or more VLANs can be grouped into a Multiple Spanning Tree Instance (MSTI). MSTP builds a separate Multiple Spanning Tree (MST) for each instance to maintain connectivity among each of the assigned VLAN groups. MSTP then builds a Internal Spanning Tree (IST) for the Region containing all commonly configured MSTP bridges.

Figure 109: MSTP Region, Internal Spanning Tree, Multiple Spanning Tree



An MST Region consists of a group of interconnected bridges that have the same MST Configuration Identifiers (including the Region Name, Revision Level and Configuration Digest – see "Configuring Multiple Spanning Trees" on page 289). An MST Region may contain multiple MSTP Instances. An Internal Spanning Tree (IST) is used to connect all the MSTP switches within an MST region. A Common Spanning Tree (CST) interconnects all adjacent MST Regions, and acts as a virtual bridge node for communications with STP or RSTP nodes in the global network.

Figure 110: Common Internal Spanning Tree, Common Spanning Tree, Internal Spanning Tree



MSTP connects all bridges and LAN segments with a single Common and Internal Spanning Tree (CIST). The CIST is formed as a result of the running spanning tree algorithm between switches that support the STP, RSTP, MSTP protocols.

Once you specify the VLANs to include in a Multiple Spanning Tree Instance (MSTI), the protocol will automatically build an MSTI tree to maintain connectivity among each of the VLANs. MSTP maintains contact with the global network because each instance is treated as an RSTP node in the Common Spanning Tree (CST).

CONFIGURING LOOPBACK DETECTION

Use the Spanning Tree > Loopback Detection page to configure loopback detection on an interface. When loopback detection is enabled and a port or trunk receives it's own BPDU, the detection agent drops the loopback BPDU, sends an SNMP trap, and places the interface in discarding mode. This loopback state can be released manually or automatically. If the interface is configured for automatic loopback release, then the port will only be returned to the forwarding state if one of the following conditions is satisfied:

- The interface receives any other BPDU except for it's own, or;
- The interfaces's link status changes to link down and then link up again, or;
- The interface ceases to receive it's own BPDUs in a forward delay interval.

NOTE: If loopback detection is not enabled and an interface receives it's own BPDU, then the interface will drop the loopback BPDU according to IEEE Standard 802.1w-2001 9.3.4 (Note 1).

NOTE: Loopback detection will not be active if Spanning Tree is disabled on the switch.

NOTE: When configured for manual release mode, then a link down/up event will not release the port from the discarding state.

CLI REFERENCES

- "Spanning Tree Commands" on page 1277

PARAMETERS

These parameters are displayed:

- **Interface** – Displays a list of ports or trunks.
- **Status** – Enables loopback detection on this interface. (Default: Enabled)
- **Trap** – Enables SNMP trap notification for loopback events on this interface. (Default: Disabled)
- **Release Mode** – Configures the interface for automatic or manual loopback release. (Default: Auto)
- **Release** – Allows an interface to be manually released from discard mode. This is only available if the interface is configured for manual release mode.
- **Action** – Sets the response for loopback detection to block user traffic or shut down the interface. (Default: Block)

- **Shutdown Interval** – The duration to shut down the interface. (Range: 60-86400 seconds; Default: 60 seconds)

  If an interface is shut down due to a detected loopback, and the release mode is set to "Auto," the selected interface will be automatically enabled when the shutdown interval has expired.

  If an interface is shut down due to a detected loopback, and the release mode is set to "Manual," the interface can be re-enabled using the Release button.

WEB INTERFACE

To configure loopback detection:

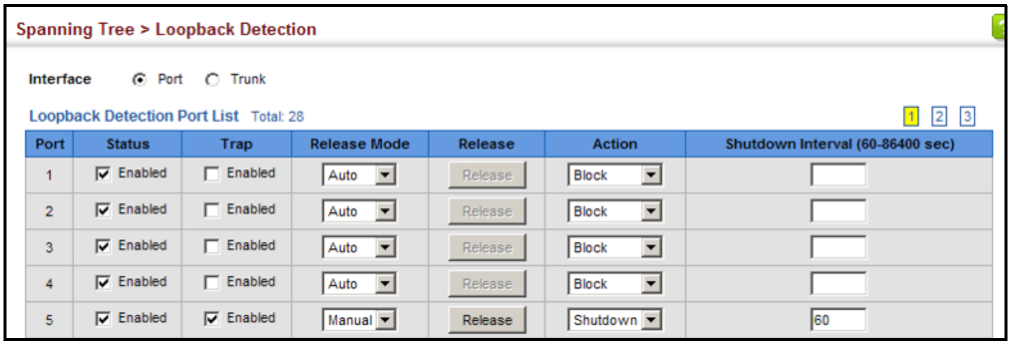
1. Click Spanning Tree, Loopback Detection.

2. Click Port or Trunk to display the required interface type.

3. Modify the required loopback detection attributes.

4. Click Apply

Figure 111: Configuring Port Loopback Detection



Spanning Tree > Loopback Detection

Interface ● Port ○ Trunk

Loopback Detection Port List Total: 28

1 2 3

Port	Status	Trap	Release Mode	Release	Action	Shutdown Interval (60-86400 sec)
1	☑ Enabled	□ Enabled	Auto	Release	Block	
2	☑ Enabled	□ Enabled	Auto	Release	Block	
3	☑ Enabled	□ Enabled	Auto	Release	Block	
4	☑ Enabled	□ Enabled	Auto	Release	Block	
5	☑ Enabled	☑ Enabled	Manual	Release	Shutdown	60

CONFIGURING GLOBAL SETTINGS FOR STA

Use the Spanning Tree > STA (Configure Global - Configure) page to configure global settings for the spanning tree that apply to the entire switch.

CLI REFERENCES

◆ "Spanning Tree Commands" on page 1277

COMMAND USAGE

◆ Spanning Tree Protocol[1]

  This option uses RSTP set to STP forced compatibility mode. It uses RSTP for the internal state machine, but sends only 802.1D BPDUs. This creates one spanning tree instance for the entire network. If multiple VLANs are implemented on a network, the path between specific VLAN members may be inadvertently disabled to prevent network loops, thus isolating group members. When operating multiple VLANs, we recommend selecting the MSTP option.

◆ Rapid Spanning Tree Protocol[1]

  RSTP supports connections to either STP or RSTP nodes by monitoring the incoming protocol messages and dynamically adjusting the type of protocol messages the RSTP node transmits, as described below:

  - STP Mode – If the switch receives an 802.1D BPDU (i.e., STP BPDU) after a port’s migration delay timer expires, the switch assumes it is connected to an 802.1D bridge and starts using only 802.1D BPDUs.

  - RSTP Mode – If RSTP is using 802.1D BPDUs on a port and receives an RSTP BPDU after the migration delay expires, RSTP restarts the migration delay timer and begins using RSTP BPDUs on that port.

◆ Multiple Spanning Tree Protocol

  MSTP generates a unique spanning tree for each instance. This provides multiple pathways across the network, thereby balancing the traffic load, preventing wide-scale disruption when a bridge node in a single instance fails, and allowing for faster convergence of a new topology for the failed instance.

  - To allow multiple spanning trees to operate over the network, you must configure a related set of bridges with the same MSTP configuration, allowing them to participate in a specific set of spanning tree instances.

  - A spanning tree instance can exist only on bridges that have compatible VLAN instance assignments.

[1] STP and RSTP BPDUs are transmitted as untagged frames, and will cross any VLAN boundaries.

- Be careful when switching between spanning tree modes. Changing modes stops all spanning-tree instances for the previous mode and restarts the system in the new mode, temporarily disrupting user traffic.

PARAMETERS

These parameters are displayed:

Basic Configuration of Global Settings

- **Spanning Tree Status** – Enables/disables STA on this switch. (Default: Enabled)

- **Spanning Tree Type** – Specifies the type of spanning tree used on this switch:

  - **STP**: Spanning Tree Protocol (IEEE 802.1D); i.e., when this option is selected, the switch will use RSTP set to STP forced compatibility mode).
  - **RSTP**: Rapid Spanning Tree (IEEE 802.1w); RSTP is the default.
  - **MSTP**: Multiple Spanning Tree (IEEE 802.1s)

- **Priority** – Bridge priority is used in selecting the root device, root port, and designated port. The device with the highest priority becomes the STA root device. However, if all devices have the same priority, the device with the lowest MAC address will then become the root device. (Note that lower numeric values indicate higher priority.)

  - Default: 32768
  - Range: 0-61440, in steps of 4096
  - Options: 0, 4096, 8192, 12288, 16384, 20480, 24576, 28672, 32768, 36864, 40960, 45056, 49152, 53248, 57344, 61440

- **BPDU Flooding** – Configures the system to flood BPDUs to all other ports on the switch or just to all other ports in the same VLAN when spanning tree is disabled globally on the switch or disabled on a specific port.

  - To VLAN: Floods BPDUs to all other ports within the receiving port’s native VLAN (i.e., as determined by port’s PVID). This is the default.
  - To All: Floods BPDUs to all other ports on the switch.

  The setting has no effect if BPDU flooding is disabled on a port (see "Configuring Interface Settings for STA").

Advanced Configuration Settings

The following attributes are based on RSTP, but also apply to STP since the switch uses a backwards-compatible subset of RSTP to implement STP, and also apply to MSTP which is based on RSTP according to the standard:

- **Path Cost Method** – The path cost is used to determine the best path between devices. The path cost method is used to determine the range of values that can be assigned to each interface.
  - Long: Specifies 32-bit based values that range from 1-200,000,000. (This is the default.)
  - Short: Specifies 16-bit based values that range from 1-65535.
- **Transmission Limit** – The maximum transmission rate for BPDUs is specified by setting the minimum interval between the transmission of consecutive protocol messages. (Range: 1-10; Default: 3)

When the Switch Becomes Root

- **Hello Time** – Interval (in seconds) at which the root device transmits a configuration message.
  - Default: 2
  - Minimum: 1
  - Maximum: The lower of 10 or [(Max. Message Age / 2) -1]
- **Maximum Age** – The maximum time (in seconds) a device can wait without receiving a configuration message before attempting to reconverge. All device ports (except for designated ports) should receive configuration messages at regular intervals. Any port that ages out STA information (provided in the last configuration message) becomes the designated port for the attached LAN. If it is a root port, a new root port is selected from among the device ports attached to the network. (References to "ports" in this section mean "interfaces," which includes both ports and trunks.)
  - Default: 20
  - Minimum: The higher of 6 or [2 x (Hello Time + 1)]
  - Maximum: The lower of 40 or [2 x (Forward Delay - 1)]
- **Forward Delay** – The maximum time (in seconds) this device will wait before changing states (i.e., discarding to learning to forwarding). This delay is required because every device must receive information about topology changes before it starts to forward frames. In addition, each port needs time to listen for conflicting information that would make it return to a discarding state; otherwise, temporary data loops might result.
  - Default: 15
  - Minimum: The higher of 4 or [(Max. Message Age / 2) + 1]
  - Maximum: 30

  RSTP does not depend on the forward delay timer in most cases. It is able to confirm that a port can transition to the forwarding state without having to rely on any timer configuration. To achieve fast convergence, RSTP relies on the use of edge ports, and automatic detection of point-to-point link types, both of which allow a port to directly transition to the forwarding state.

Configuration Settings for MSTP

- **Max Instance Numbers** – The maximum number of MSTP instances to which this switch can be assigned.

- **Configuration Digest** – An MD5 signature key that contains the VLAN ID to MST ID mapping table. In other words, this key is a mapping of all VLANs to the CIST.

- **Region Revision**[2] – The revision for this MSTI. (Range: 0-65535; Default: 0)

- **Region Name**[2] – The name for this MSTI. (Maximum length: 32 characters; switch's MAC address)

- **Max Hop Count** – The maximum number of hops allowed in the MST region before a BPDU is discarded. (Range: 1-40; Default: 20)

WEB INTERFACE

To configure global STA settings:

1. Click Spanning Tree, STA.

2. Select Configure Global from the Step list.

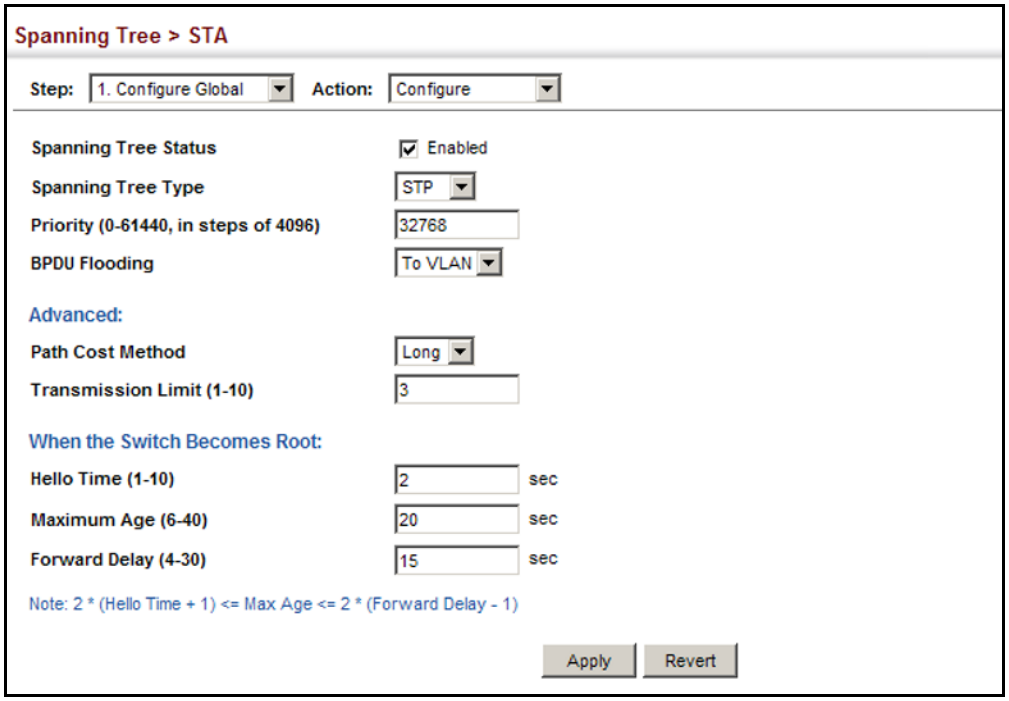
3. Select Configure from the Action list.

4. Modify any of the required attributes. Note that the parameters displayed for the spanning tree types (STP, RSTP, MSTP) varies as described in the preceding section.

5. Click Apply

[2] The MST name and revision number are both required to uniquely identify an MST region.

Figure 112: Configuring Global Settings for STA (STP)



Spanning Tree > STA

Step: 1. Configure Global Action: Configure

Spanning Tree Status ☑ Enabled

Spanning Tree Type STP

Priority (0-61440, in steps of 4096) 32768

BPDU Flooding To VLAN

Advanced:

Path Cost Method Long

Transmission Limit (1-10) 3

When the Switch Becomes Root:

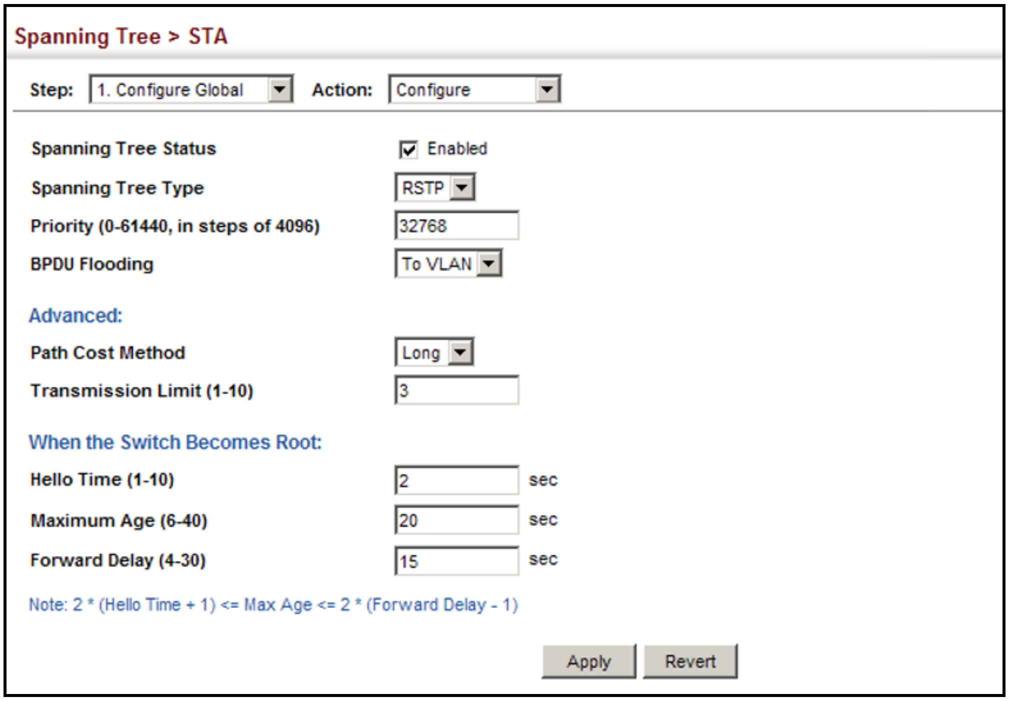
Hello Time (1-10) 2 sec

Maximum Age (6-40) 20 sec

Forward Delay (4-30) 15 sec

Note: 2 * (Hello Time + 1) <= Max Age <= 2 * (Forward Delay - 1)

Figure 113: Configuring Global Settings for STA (RSTP)



Spanning Tree > STA

Step: 1. Configure Global Action: Configure

Spanning Tree Status ☑ Enabled

Spanning Tree Type RSTP

Priority (0-61440, in steps of 4096) 32768

BPDU Flooding To VLAN

Advanced:

Path Cost Method Long

Transmission Limit (1-10) 3

When the Switch Becomes Root:

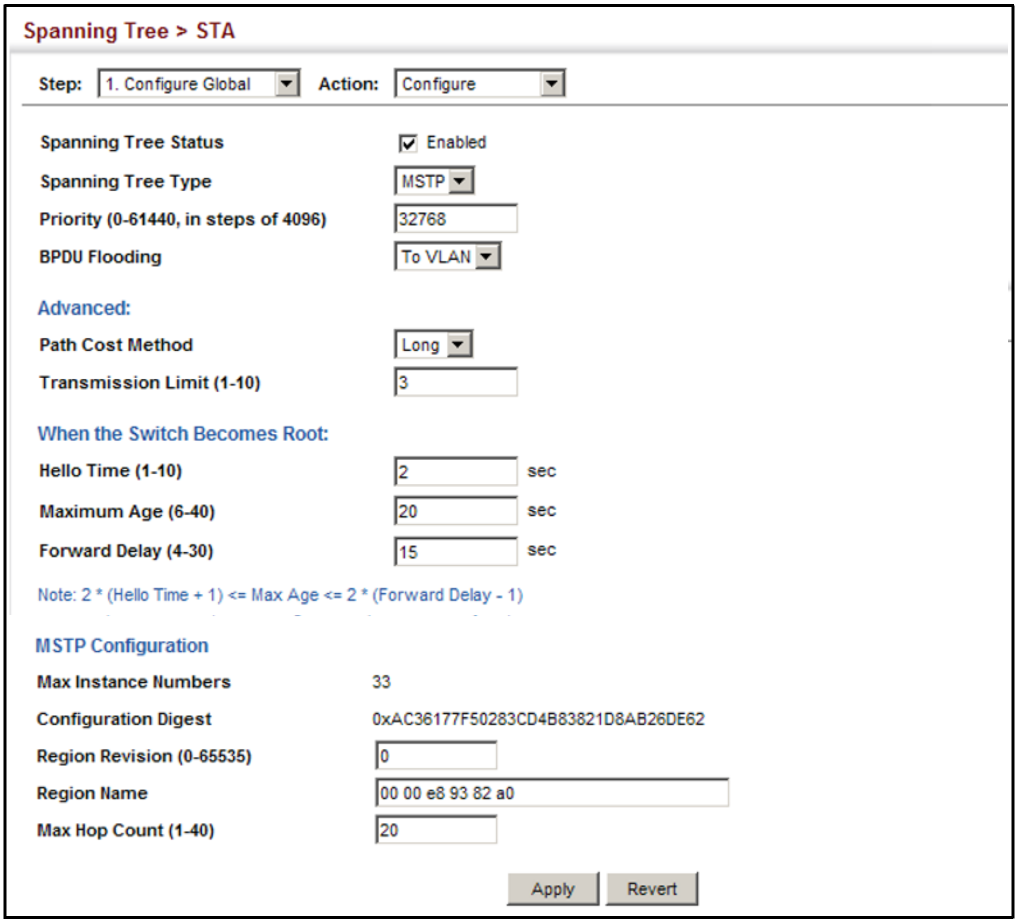
Hello Time (1-10) 2 sec

Maximum Age (6-40) 20 sec

Forward Delay (4-30) 15 sec

Note: 2 * (Hello Time + 1) <= Max Age <= 2 * (Forward Delay - 1)

Figure 114: Configuring Global Settings for STA (MSTP)



Spanning Tree > STA

Step: 1. Configure Global ▾ Action: Configure ▾

Spanning Tree Status ☑ Enabled

Spanning Tree Type MSTP ▾

Priority (0-61440, in steps of 4096) 32768

BPDU Flooding To VLAN ▾

Advanced:

Path Cost Method Long ▾

Transmission Limit (1-10) 3

When the Switch Becomes Root:

Hello Time (1-10) 2 sec

Maximum Age (6-40) 20 sec

Forward Delay (4-30) 15 sec

Note: 2 * (Hello Time + 1) <= Max Age <= 2 * (Forward Delay - 1)

MSTP Configuration

Max Instance Numbers 33

Configuration Digest 0xAC36177F50283CD4B83821D8AB26DE62

Region Revision (0-65535) 0

Region Name 00 00 e8 93 82 a0

Max Hop Count (1-40) 20

DISPLAYING GLOBAL SETTINGS FOR STA

Use the Spanning Tree > STA (Configure Global - Show Information) page to display a summary of the current bridge STA information that applies to the entire switch.

CLI REFERENCES

- "show spanning-tree" on page 1302
- "show spanning-tree mst configuration" on page 1304

PARAMETERS

The parameters displayed are described in the preceding section, except for the following items:

- **Bridge ID** – A unique identifier for this bridge, consisting of the bridge priority, the MST Instance ID 0 for the Common Spanning Tree when spanning tree type is set to MSTP, and MAC address (where the address is taken from the switch system).

- **Designated Root** – The priority and MAC address of the device in the Spanning Tree that this switch has accepted as the root device.

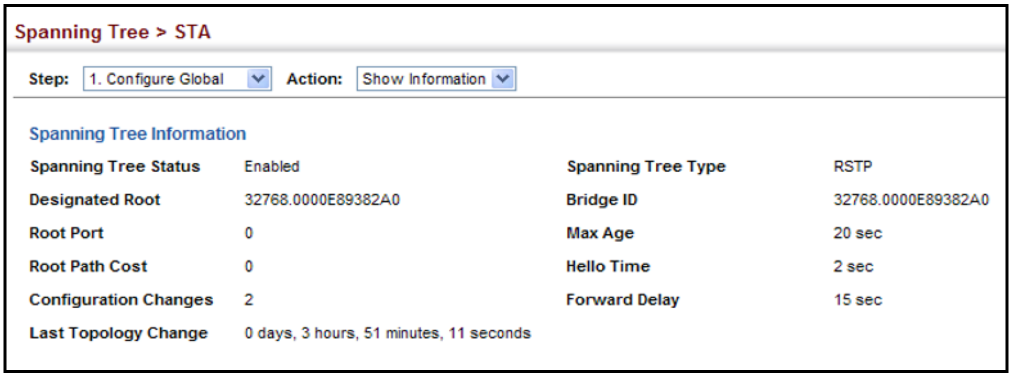
- **Root Port** – The number of the port on this switch that is closest to the root. This switch communicates with the root device through this port. If there is no root port, then this switch has been accepted as the root device of the Spanning Tree network.
- **Root Path Cost** – The path cost from the root port on this switch to the root device.
- **Configuration Changes** – The number of times the Spanning Tree has been reconfigured.
- **Last Topology Change** – Time since the Spanning Tree was last reconfigured.

WEB INTERFACE

To display global STA settings:

1. Click Spanning Tree, STA.
2. Select Configure Global from the Step list.
3. Select Show Information from the Action list.

Figure 115: Displaying Global Settings for STA



Spanning Tree > STA

Step: 1. Configure Global Action: Show Information

Spanning Tree Information

Spanning Tree Status	Enabled	Spanning Tree Type	RSTP
Designated Root	32768.0000E89382A0	Bridge ID	32768.0000E89382A0
Root Port	0	Max Age	20 sec
Root Path Cost	0	Hello Time	2 sec
Configuration Changes	2	Forward Delay	15 sec
Last Topology Change	0 days, 3 hours, 51 minutes, 11 seconds		

CONFIGURING INTERFACE SETTINGS FOR STA

Use the Spanning Tree > STA (Configure Interface - Configure) page to configure RSTP and MSTP attributes for specific interfaces, including port priority, path cost, link type, and edge port. You may use a different priority or path cost for ports of the same media type to indicate the preferred path, link type to indicate a point-to-point connection or shared-media connection, and edge port to indicate if the attached device can support fast forwarding. (References to “ports” in this section means “interfaces,” which includes both ports and trunks.)

CLI REFERENCES

- "Spanning Tree Commands" on page 1277

PARAMETERS

These parameters are displayed:

- **Interface** – Displays a list of ports or trunks.

- **Spanning Tree** – Enables/disables STA on this interface. (Default: Enabled)

- **BPDU Flooding** - Enables/disables the flooding of BPDUs to other ports when global spanning tree is disabled (page 276) or when spanning tree is disabled on specific port. When flooding is enabled, BPDUs are flooded to all other ports on the switch or to all other ports within the receiving port's native VLAN as specified by the Spanning Tree BPDU Flooding attribute (page 276). (Default: Enabled)

- **Priority** – Defines the priority used for this port in the Spanning Tree Protocol. If the path cost for all ports on a switch are the same, the port with the highest priority (i.e., lowest value) will be configured as an active link in the Spanning Tree. This makes a port with higher priority less likely to be blocked if the Spanning Tree Protocol is detecting network loops. Where more than one port is assigned the highest priority, the port with lowest numeric identifier will be enabled.
  - Default: 128
  - Range: 0-240, in steps of 16

- **Admin Path Cost** – This parameter is used by the STA to determine the best path between devices. Therefore, lower values should be assigned to ports attached to faster media, and higher values assigned to ports with slower media. Note that path cost takes precedence over port priority. (Range: 0 for auto-configuration, 1-65535 for the short path cost method[3], 1-200,000,000 for the long path cost method)

  By default, the system automatically detects the speed and duplex mode used on each port, and configures the path cost according to the values shown below. Path cost "0" is used to indicate auto-configuration mode. When the short path cost method is selected and the default path cost recommended by the IEEE 8021w standard exceeds 65,535, the default is set to 65,535.

Table 12: Recommended STA Path Cost Range

Port Type	IEEE 802.1D-1998	IEEE 802.1w-2001
Ethernet	50-600	200,000-20,000,000
Fast Ethernet	10-60	20,000-2,000,000
Gigabit Ethernet	3-10	2,000-200,000
10G Ethernet	1-5	200-20,000

[3] Refer to "Configuring Global Settings for STA" on page 276 for information on setting the path cost method.

Table 13: Default STA Path Costs

Port Type	Short Path Cost (IEEE 802.1D-1998)	Long Path Cost (802.1D-2004)
Ethernet	65,535	1,000,000
Fast Ethernet	65,535	100,000
Gigabit Ethernet	10,000	10,000
10G Ethernet	1,000	1,000

- **Admin Link Type** – The link type attached to this interface.
  - Point-to-Point – A connection to exactly one other bridge.
  - Shared – A connection to two or more bridges.
  - Auto – The switch automatically determines if the interface is attached to a point-to-point link or to shared media. (This is the default setting.)
- **Root Guard** – STA allows a bridge with a lower bridge identifier (or same identifier and lower MAC address) to take over as the root bridge at any time. Root Guard can be used to ensure that the root bridge is not formed at a suboptimal location. Root Guard should be enabled on any designated port connected to low-speed bridges which could potentially overload a slower link by taking over as the root port and forming a new spanning tree topology. It could also be used to form a border around part of the network where the root bridge is allowed. (Default: Disabled)
- **Admin Edge Port** – Since end nodes **cannot** cause forwarding loops, they can pass directly through to the spanning tree forwarding state. Specifying Edge Ports provides quicker convergence for devices such as workstations or servers, retains the current forwarding database to reduce the amount of frame flooding required to rebuild address tables during reconfiguration events, does not cause the spanning tree to initiate reconfiguration when the interface changes state, and also overcomes other STA-related timeout problems. However, remember that Edge Port should only be enabled for ports connected to an end-node device. (Default: Auto)
  - **Enabled** – Manually configures a port as an Edge Port.
  - **Disabled** – Disables the Edge Port setting.
  - **Auto** – The port will be automatically configured as an edge port if the edge delay time expires without receiving any RSTP or MSTP BPDUs. Note that edge delay time (802.1D-2004 17.20.4) equals the protocol migration time if a port's link type is point-to-point (which is 3 seconds as defined in IEEE 802.3D-2004 17.20.4); otherwise it equals the spanning tree’s maximum age for configuration messages (see maximum age under "Configuring Global Settings for STA" on page 276).

An interface cannot function as an edge port under the following conditions:

- If spanning tree mode is set to STP (page 276), edge-port mode cannot automatically transition to operational edge-port state using the automatic setting.
- If loopback detection is enabled (page 274) and a loopback BPDU is detected, the interface cannot function as an edge port until the loopback state is released.
- If an interface is in forwarding state and its role changes, the interface cannot continue to function as an edge port even if the edge delay time has expired.
- If the port does not receive any BPDUs after the edge delay timer expires, its role changes to designated port and it immediately enters forwarding state (see "Displaying Interface Settings for STA" on page 286).

- **BPDU Guard** – This feature protects edge ports from receiving BPDUs. It prevents loops by shutting down an edge port when a BPDU is received instead of putting it into the spanning tree discarding state. In a valid configuration, configured edge ports should not receive BPDUs. If an edge port receives a BPDU an invalid configuration exists, such as a connection to an unauthorized device. The BPDU guard feature provides a secure response to invalid configurations because an administrator must manually enable the port. (Default: Disabled)

- **BPDU Filter** – BPDU filtering allows you to avoid transmitting BPDUs on configured edge ports that are connected to end nodes. By default, STA sends BPDUs to all ports regardless of whether administrative edge is enabled on a port. BDPU filtering is configured on a per-port basis. (Default: Disabled)

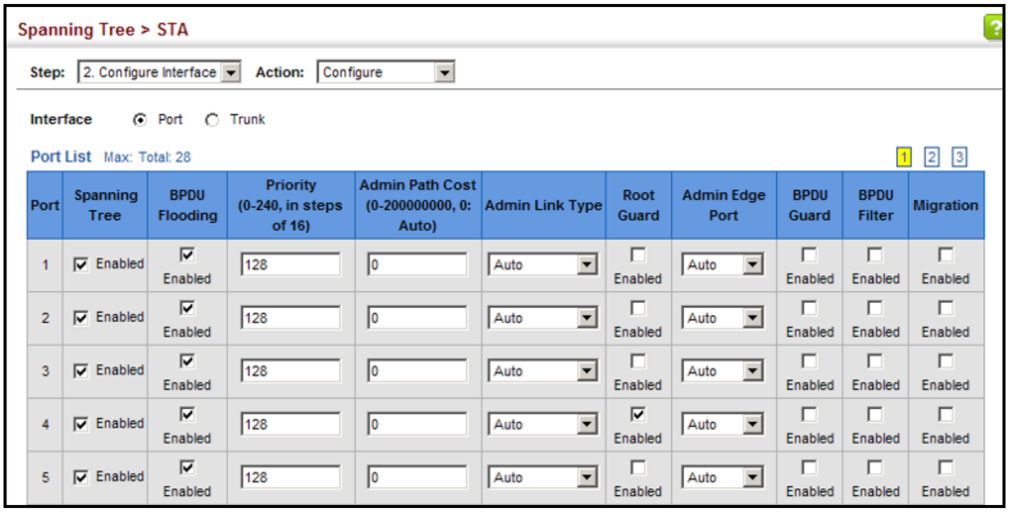
- **Migration** – If at any time the switch detects STP BPDUs, including Configuration or Topology Change Notification BPDUs, it will automatically set the selected interface to forced STP-compatible mode. However, you can also use the Protocol Migration button to manually re-check the appropriate BPDU format (RSTP or STP-compatible) to send on the selected interfaces. (Default: Disabled)

WEB INTERFACE

To configure interface settings for STA:

1. Click Spanning Tree, STA.
2. Select Configure Interface from the Step list.
3. Select Configure from the Action list.
4. Modify any of the required attributes.
5. Click Apply.

Figure 116: Configuring Interface Settings for STA



Spanning Tree > STA

Step: 2. Configure Interface Action: Configure

Interface ● Port ○ Trunk

Port List Max: Total: 28

1 2 3

Port	Spanning Tree	BPDU Flooding	Priority (0-240, in steps of 16)	Admin Path Cost (0-200000000, 0: Auto)	Admin Link Type	Root Guard	Admin Edge Port	BPDU Guard	BPDU Filter	Migration
1	☑ Enabled	☑ Enabled	128	0	Auto	□ Enabled	Auto	□ Enabled	□ Enabled	□ Enabled
2	☑ Enabled	☑ Enabled	128	0	Auto	□ Enabled	Auto	□ Enabled	□ Enabled	□ Enabled
3	☑ Enabled	☑ Enabled	128	0	Auto	□ Enabled	Auto	□ Enabled	□ Enabled	□ Enabled
4	☑ Enabled	☑ Enabled	128	0	Auto	☑ Enabled	Auto	□ Enabled	□ Enabled	□ Enabled
5	☑ Enabled	☑ Enabled	128	0	Auto	□ Enabled	Auto	□ Enabled	□ Enabled	□ Enabled

DISPLAYING INTERFACE SETTINGS FOR STA

Use the Spanning Tree > STA (Configure Interface - Show Information) page to display the current status of ports or trunks in the Spanning Tree.

CLI REFERENCES

- "show spanning-tree" on page 1302

PARAMETERS

These parameters are displayed:

- **Spanning Tree** – Shows if STA has been enabled on this interface.

- **BPDU Flooding** – Shows if BPDUs will be flooded to other ports when spanning tree is disabled globally on the switch or disabled on a specific port.

- **STA Status** – Displays current state of this port within the Spanning Tree:

  - **Discarding** - Port receives STA configuration messages, but does not forward packets.

  - **Learning** - Port has transmitted configuration messages for an interval set by the Forward Delay parameter without receiving contradictory information. Port address table is cleared, and the port begins learning addresses.

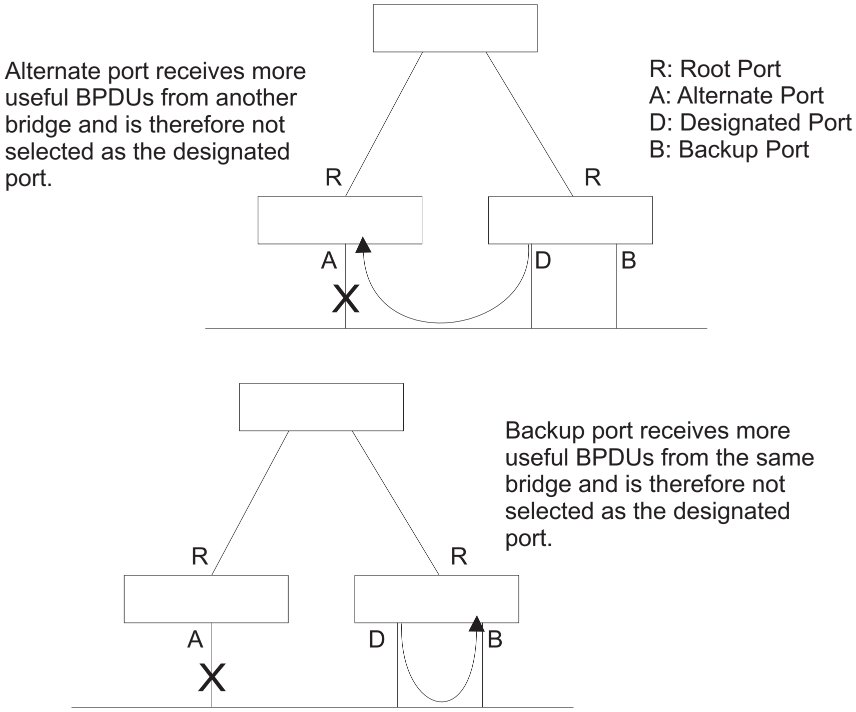
  - **Forwarding** - Port forwards packets, and continues learning addresses.

The rules defining port status are:

- A port on a network segment with no other STA compliant bridging device is always forwarding.
- If two ports of a switch are connected to the same segment and there is no other STA device attached to this segment, the port with the smaller ID forwards packets and the other is discarding.
- All ports are discarding when the switch is booted, then some of them change state to learning, and then to forwarding.

- **Forward Transitions** – The number of times this port has transitioned from the Learning state to the Forwarding state.
- **Designated Cost** – The cost for a packet to travel from this port to the root in the current Spanning Tree configuration. The slower the media, the higher the cost.
- **Designated Bridge** – The bridge priority and MAC address of the device through which this port must communicate to reach the root of the Spanning Tree.
- **Designated Port** – The port priority and number of the port on the designated bridging device through which this switch must communicate with the root of the Spanning Tree.
- **Oper Path Cost** – The contribution of this port to the path cost of paths towards the spanning tree root which include this port.
- **Oper Link Type** – The operational point-to-point status of the LAN segment attached to this interface. This parameter is determined by manual configuration or by auto-detection, as described for Admin Link Type in STA Port Configuration on page 282.
- **Oper Edge Port** – This parameter is initialized to the setting for Admin Edge Port in STA Port Configuration on page 282 (i.e., true or false), but will be set to false if a BPDU is received, indicating that another bridge is attached to this port.
- **Port Role** – Roles are assigned according to whether the port is part of the active topology connecting a non-root bridge to the root bridge (i.e., **root** port), connecting a LAN through the bridge to the root bridge (i.e., **designated** port), is the MSTI regional root (i.e., **master** port), or is an **alternate** or **backup** port that may provide connectivity if other bridges, bridge ports, or LANs fail or are removed. The role is set to disabled (i.e., **disabled** port) if a port has no role within the spanning tree.

Figure 117: STA Port Roles

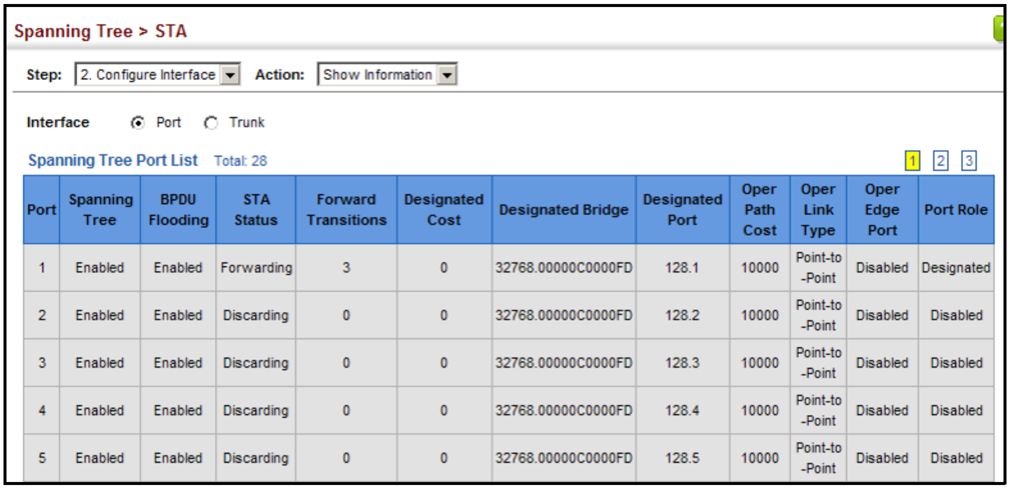

Alternate port receives more useful BPDUs from another bridge and is therefore not selected as the designated port.
R: Root Port
A: Alternate Port
D: Designated Port
B: Backup Port
R
R
A
D
B
X
Backup port receives more useful BPDUs from the same bridge and is therefore not selected as the designated port.
R
R
A
D
B
X

WEB INTERFACE

To display interface settings for STA:

1. Click Spanning Tree, STA.
2. Select Configure Interface from the Step list.
3. Select Show Information from the Action list.

Figure 118: Displaying Interface Settings for STA



Spanning Tree > STA

Step: 2. Configure Interface Action: Show Information

Interface ● Port ○ Trunk

Spanning Tree Port List Total: 28

Port	Spanning Tree	BPDU Flooding	STA Status	Forward Transitions	Designated Cost	Designated Bridge	Designated Port	Oper Path Cost	Oper Link Type	Oper Edge Port	Port Role
1	Enabled	Enabled	Forwarding	3	0	32768.00000C0000FD	128.1	10000	Point-to-Point	Disabled	Designated
2	Enabled	Enabled	Discarding	0	0	32768.00000C0000FD	128.2	10000	Point-to-Point	Disabled	Disabled
3	Enabled	Enabled	Discarding	0	0	32768.00000C0000FD	128.3	10000	Point-to-Point	Disabled	Disabled
4	Enabled	Enabled	Discarding	0	0	32768.00000C0000FD	128.4	10000	Point-to-Point	Disabled	Disabled
5	Enabled	Enabled	Discarding	0	0	32768.00000C0000FD	128.5	10000	Point-to-Point	Disabled	Disabled

CONFIGURING MULTIPLE SPANNING TREES

Use the Spanning Tree > MSTP (Configure Global) page to create an MSTP instance, or to add VLAN groups to an MSTP instance.

CLI REFERENCES

- "Spanning Tree Commands" on page 1277

COMMAND USAGE

MSTP generates a unique spanning tree for each instance. This provides multiple pathways across the network, thereby balancing the traffic load, preventing wide-scale disruption when a bridge node in a single instance fails, and allowing for faster convergence of a new topology for the failed instance.

By default all VLANs are assigned to the Internal Spanning Tree (MST Instance 0) that connects all bridges and LANs within the MST region. This switch supports up to 33 instances. You should try to group VLANs which cover the same general area of your network. However, remember that you must configure all bridges within the same MSTI Region (page 276) with the same set of instances, and the same instance (on each bridge) with the same set of VLANs. Also, note that RSTP treats each MSTI region as a single node, connecting all regions to the Common Spanning Tree.

To use multiple spanning trees:

1. Set the spanning tree type to MSTP (page 276).
2. Enter the spanning tree priority for the selected MST instance on the Spanning Tree > MSTP (Configure Global - Add) page.
3. Add the VLANs that will share this MSTI on the Spanning Tree > MSTP (Configure Global - Add Member) page.

NOTE: All VLANs are automatically added to the IST (Instance 0).

To ensure that the MSTI maintains connectivity across the network, you must configure a related set of bridges with the same MSTI settings.

PARAMETERS

These parameters are displayed:

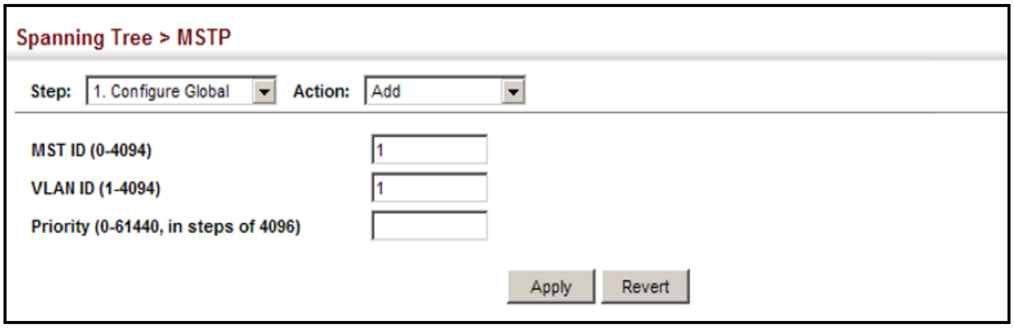
- **MST ID** – Instance identifier to configure. (Range: 0-4094)
- **VLAN ID** – VLAN to assign to this MST instance. (Range: 1-4094)
- **Priority** – The priority of a spanning tree instance. (Range: 0-61440 in steps of 4096; Options: 0, 4096, 8192, 12288, 16384, 20480, 24576, 28672, 32768, 36864, 40960, 45056, 49152, 53248, 57344, 61440; Default: 32768)

WEB INTERFACE

To create instances for MSTP:

1. Click Spanning Tree, MSTP.
2. Select Configure Global from the Step list.
3. Select Add from the Action list.
4. Specify the MST instance identifier and the initial VLAN member. Additional member can be added using the Spanning Tree > MSTP (Configure Global - Add Member) page. If the priority is not specified, the default value 32768 is used.
5. Click Apply.

Figure 119: Creating an MST Instance



Spanning Tree > MSTP

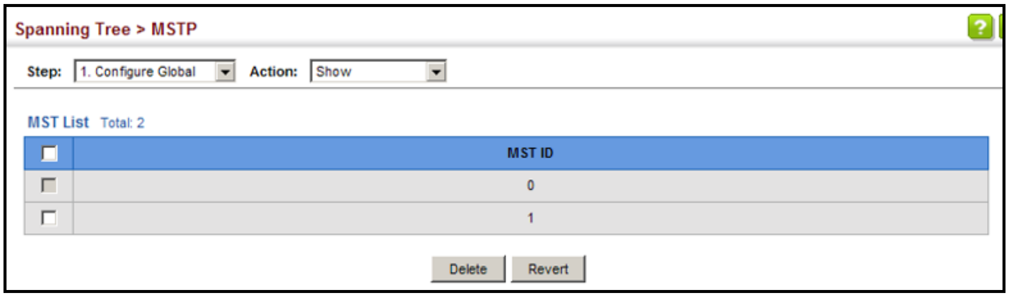
Step: 1. Configure Global   Action: Add

MST ID (0-4094): 1
VLAN ID (1-4094): 1
Priority (0-61440, in steps of 4096):

To show the MSTP instances:

1. Click Spanning Tree, MSTP.
2. Select Configure Global from the Step list.
3. Select Show from the Action list.

Figure 120: Displaying MST Instances



Spanning Tree > MSTP

Step: 1. Configure Global   Action: Show

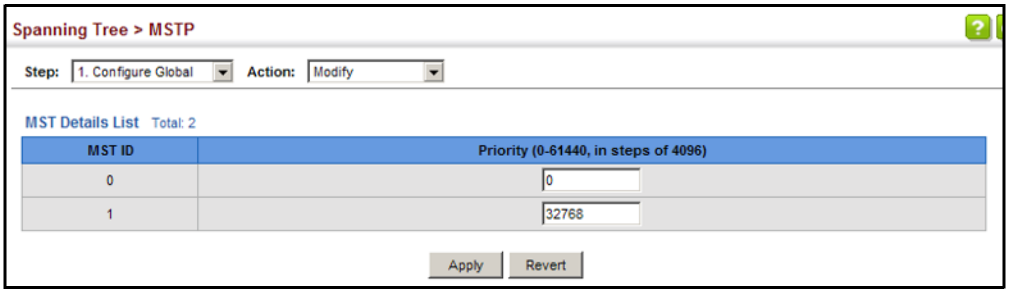
MST List Total: 2

□	MST ID
□	0
□	1

To modify the priority for an MST instance:

1. Click Spanning Tree, MSTP.
2. Select Configure Global from the Step list.
3. Select Modify from the Action list.
4. Modify the priority for an MSTP Instance.
5. Click Apply.

Figure 121: Modifying the Priority for an MST Instance



Spanning Tree > MSTP

Step: 1. Configure Global Action: Modify

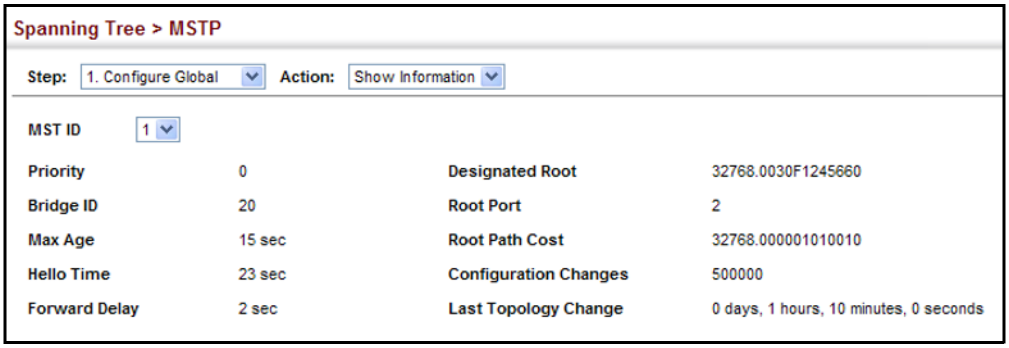
MST Details List Total: 2

MST ID	Priority (0-61440, in steps of 4096)
0	0
1	32768

To display global settings for MSTP:

1. Click Spanning Tree, MSTP.
2. Select Configure Global from the Step list.
3. Select Show Information from the Action list.
4. Select an MST ID. The attributes displayed on this page are described under "Displaying Global Settings for STA" on page 281.

Figure 122: Displaying Global Settings for an MST Instance



Spanning Tree > MSTP

Step: 1. Configure Global Action: Show Information

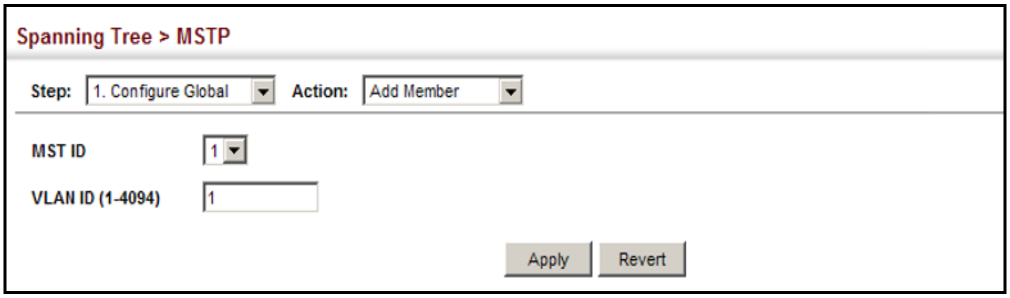
MST ID 1

Priority	0	Designated Root	32768.0030F1245660
Bridge ID	20	Root Port	2
Max Age	15 sec	Root Path Cost	32768.000001010010
Hello Time	23 sec	Configuration Changes	500000
Forward Delay	2 sec	Last Topology Change	0 days, 1 hours, 10 minutes, 0 seconds

To add additional VLAN groups to an MSTP instance:

1. Click Spanning Tree, MSTP.
2. Select Configure Global from the Step list.
3. Select Add Member from the Action list.
4. Select an MST instance from the MST ID list.
5. Enter the VLAN group to add to the instance in the VLAN ID field. Note that the specified member does not have to be a configured VLAN.
6. Click Apply

Figure 123: Adding a VLAN to an MST Instance



Spanning Tree > MSTP

Step: 1. Configure Global   Action: Add Member

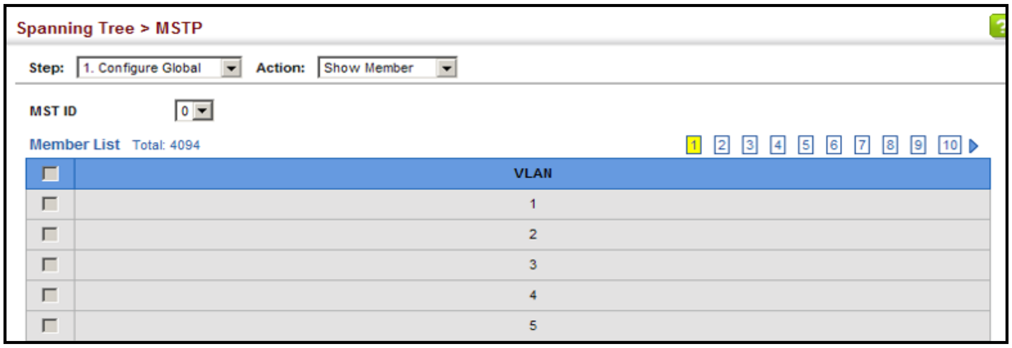
MST ID: 1

VLAN ID (1-4094): 1

To show the VLAN members of an MSTP instance:

1. Click Spanning Tree, MSTP.
2. Select Configure Global from the Step list.
3. Select Show Member from the Action list.

Figure 124: Displaying Members of an MST Instance



Spanning Tree > MSTP

Step: 1. Configure Global   Action: Show Member

MST ID: 0

Member List Total: 4094

□	VLAN
□	1
□	2
□	3
□	4
□	5

CONFIGURING INTERFACE SETTINGS FOR MSTP

Use the Spanning Tree > MSTP (Configure Interface - Configure) page to configure the STA interface settings for an MST instance.

CLI REFERENCES

- "Spanning Tree Commands" on page 1277

PARAMETERS

These parameters are displayed:

- **MST ID** – Instance identifier to configure. (Default: 0)

- **Interface** – Displays a list of ports or trunks.

- **STA Status** – Displays the current state of this interface within the Spanning Tree. (See "Displaying Interface Settings for STA" on page 286 for additional information.)

  - **Discarding** – Port receives STA configuration messages, but does not forward packets.

  - **Learning** – Port has transmitted configuration messages for an interval set by the Forward Delay parameter without receiving contradictory information. Port address table is cleared, and the port begins learning addresses.

  - **Forwarding** – Port forwards packets, and continues learning addresses.

- **Priority** – Defines the priority used for this port in the Spanning Tree Protocol. If the path cost for all ports on a switch are the same, the port with the highest priority (i.e., lowest value) will be configured as an active link in the Spanning Tree. This makes a port with higher priority less likely to be blocked if the Spanning Tree Protocol is detecting network loops. Where more than one port is assigned the highest priority, the port with lowest numeric identifier will be enabled. (Default: 128; Range: 0-240, in steps of 16)

- **Admin MST Path Cost** – This parameter is used by the MSTP to determine the best path between devices. Therefore, lower values should be assigned to ports attached to faster media, and higher values assigned to ports with slower media. (Path cost takes precedence over port priority.) Note that when the Path Cost Method is set to short (page 282), the maximum path cost is 65,535.

  By default, the system automatically detects the speed and duplex mode used on each port, and configures the path cost according to the values shown below. Path cost “0” is used to indicate auto-configuration mode. When the short path cost method is selected and the default path cost recommended by the IEEE 8021w standard exceeds 65,535, the default is set to 65,535.

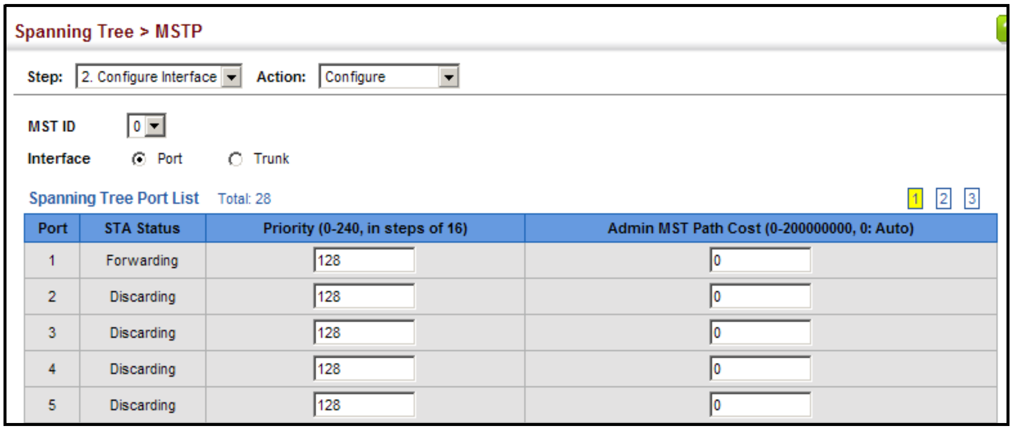
The recommended range is listed in Table 12 on page 283.
The default path costs are listed in Table 13 on page 284.

WEB INTERFACE

To configure MSTP parameters for a port or trunk:

1. Click Spanning Tree, MSTP.
2. Select Configure Interface from the Step list.
3. Select Configure from the Action list.
4. Enter the priority and path cost for an interface
5. Click Apply.

Figure 125: Configuring MSTP Interface Settings



Spanning Tree > MSTP

Step: 2. Configure Interface Action: Configure

MST ID 0

Interface ● Port ○ Trunk

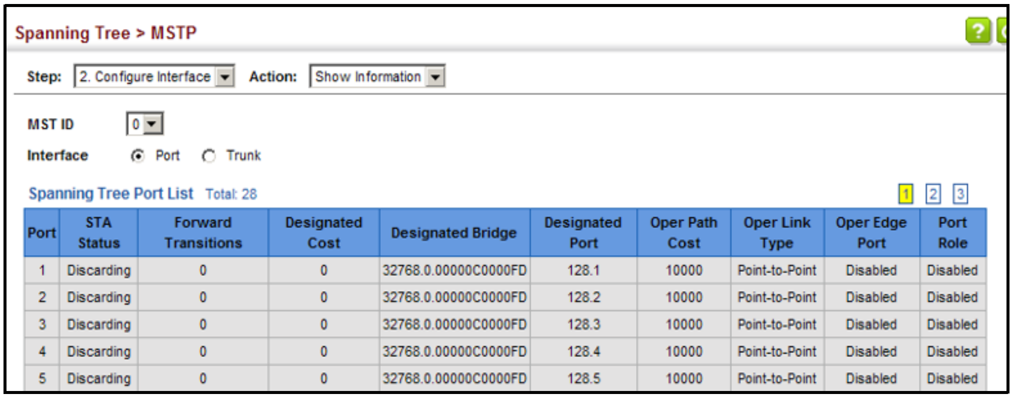
Spanning Tree Port List Total: 28

Port	STA Status	Priority (0-240, in steps of 16)	Admin MST Path Cost (0-200000000, 0: Auto)
1	Forwarding	128	0
2	Discarding	128	0
3	Discarding	128	0
4	Discarding	128	0
5	Discarding	128	0

To display MSTP parameters for a port or trunk:

1. Click Spanning Tree, MSTP.
2. Select Configure Interface from the Step list.
3. Select Show Information from the Action list.

Figure 126: Displaying MSTP Interface Settings



Spanning Tree > MSTP

Step: 2. Configure Interface Action: Show Information

MST ID 0

Interface ● Port ○ Trunk

Spanning Tree Port List Total: 28

Port	STA Status	Forward Transitions	Designated Cost	Designated Bridge	Designated Port	Oper Path Cost	Oper Link Type	Oper Edge Port	Port Role
1	Discarding	0	0	32768.0.00000C0000FD	128.1	10000	Point-to-Point	Disabled	Disabled
2	Discarding	0	0	32768.0.00000C0000FD	128.2	10000	Point-to-Point	Disabled	Disabled
3	Discarding	0	0	32768.0.00000C0000FD	128.3	10000	Point-to-Point	Disabled	Disabled
4	Discarding	0	0	32768.0.00000C0000FD	128.4	10000	Point-to-Point	Disabled	Disabled
5	Discarding	0	0	32768.0.00000C0000FD	128.5	10000	Point-to-Point	Disabled	Disabled

9 Congestion Control

The switch can set the maximum upload or download data transfer rate for any port. It can also control traffic storms by setting a maximum threshold for broadcast traffic or multicast traffic. It can also set bounding thresholds for broadcast and multicast storms which can be used to automatically trigger rate limits or to shut down a port.

Congestion Control includes following options:

- Rate Limiting – Sets the input and output rate limits for a port.
- Storm Control – Sets the traffic storm threshold for each interface.
- Automatic Traffic Control – Sets thresholds for broadcast and multicast storms which can be used to trigger configured rate limits or to shut down a port.

Rate Limiting

Use the Traffic > Rate Limit page to apply rate limiting to ingress or egress ports. This function allows the network manager to control the maximum rate for traffic received or transmitted on an interface. Rate limiting is configured on interfaces at the edge of a network to limit traffic into or out of the network. Packets that exceed the acceptable amount of traffic are dropped.

Rate limiting can be applied to individual ports or trunks. When an interface is configured with this feature, the traffic rate will be monitored by the hardware to verify conformity. Non-conforming traffic is dropped, conforming traffic is forwarded without any changes.

CLI References

- "Rate Limit Commands" on page 1205

Parameters

These parameters are displayed:

- **Interface** – Displays the switch’s ports or trunks.
- **Type** – Indicates the port type. (1000BASE SFP, 10GBASE XFP, 10GBASE SFP+)
- **Status** – Enables or disables the rate limit. (Default: Disabled)

- **Rate** – Sets the rate limit level.
  (Range: 64 - 1,000,000 kbits per second for Gigabit Ethernet ports; 64 - 10,000,000 kbits per second for 10 Gigabit Ethernet ports)

WEB INTERFACE

To configure rate limits:

1. Click Traffic, Rate Limit.

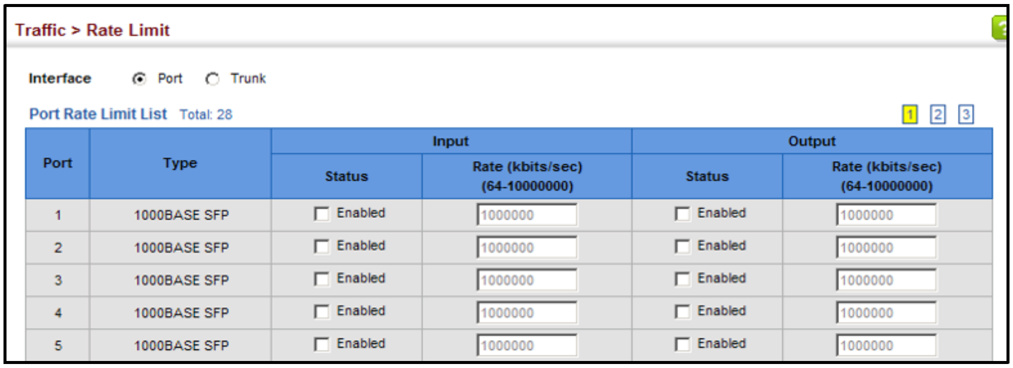
2. Set the interface type to Port or Trunk.

3. Enable the Rate Limit Status for the required interface.

4. Set the rate limit for the individual ports,.

5. Click Apply.

Figure 127: Configuring Rate Limits



Traffic > Rate Limit

Interface ● Port ○ Trunk

Port Rate Limit List Total: 28

Port	Type	Input		Output	
		Status	Rate (kbits/sec) (64-10000000)	Status	Rate (kbits/sec) (64-10000000)
1	1000BASE SFP	□ Enabled	1000000	□ Enabled	1000000
2	1000BASE SFP	□ Enabled	1000000	□ Enabled	1000000
3	1000BASE SFP	□ Enabled	1000000	□ Enabled	1000000
4	1000BASE SFP	□ Enabled	1000000	□ Enabled	1000000
5	1000BASE SFP	□ Enabled	1000000	□ Enabled	1000000

STORM CONTROL

Use the Traffic > Storm Control page to configure broadcast, multicast, and unknown unicast storm control thresholds. Traffic storms may occur when a device on your network is malfunctioning, or if application programs are not well designed or properly configured. If there is too much traffic on your network, performance can be severely degraded or everything can come to complete halt.

You can protect your network from traffic storms by setting a threshold for broadcast, multicast or unknown unicast traffic. Any packets exceeding the specified threshold will then be dropped.

CLI REFERENCES

- "switchport packet-rate" on page 1241

COMMAND USAGE

- Broadcast Storm Control is enabled by default.

- When traffic exceeds the threshold specified for broadcast and multicast or unknown unicast traffic, packets exceeding the threshold are dropped until the rate falls back down beneath the threshold.

- Traffic storms can be controlled at the hardware level using Storm Control or at the software level using Automatic Traffic Control which triggers various control responses. However, only one of these control types can be applied to a port. Enabling hardware-level storm control on a port will disable automatic storm control on that port.

- The rate limits set by this function are also used by automatic storm control when the control response is set to rate control on the Auto Traffic Control (Configure Interface) page.

- Using both rate limiting and storm control on the same interface may lead to unexpected results. It is therefore not advisable to use both of these commands on the same interface.

PARAMETERS

These parameters are displayed:

- **Interface** – Displays a list of ports or trunks.

- **Type** – Indicates interface type. (1000BASE SFP, 10GBASE XFP, 10GBASE SFP+)

- **Unknown Unicast** – Specifies storm control for unknown unicast traffic.

- **Multicast** – Specifies storm control for multicast traffic.

- **Broadcast** – Specifies storm control for broadcast traffic.

- **Status** – Enables or disables storm control. (Default: Enabled for broadcast storm control, disabled for multicast and unknown unicast storm control)

- **Rate** – Threshold level in packets per second.
  (Range: 500-14880000 pps; Default: Disabled for unknown unicast and multicast traffic, 500 pps for broadcast traffic)

WEB INTERFACE

To configure broadcast storm control:

1. Click Traffic, Storm Control.

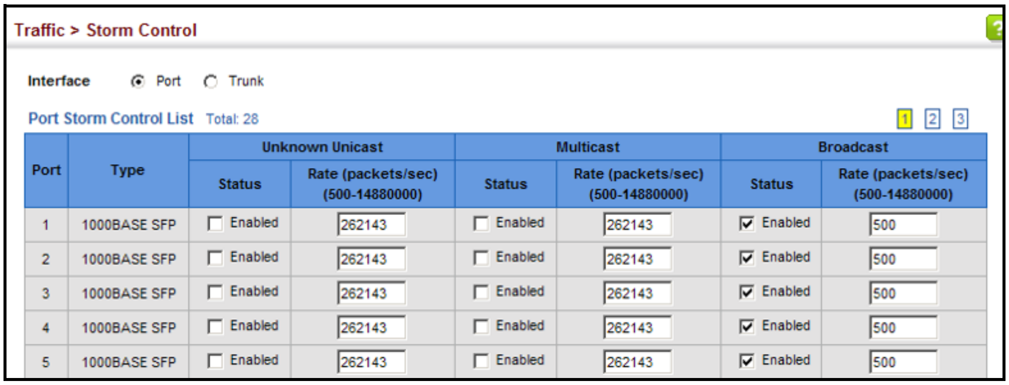
2. Set the interface type to Port or Trunk.

3. Set the Status field to enable or disable storm control.

4. Set the required threshold beyond which the switch will start dropping packets.

5. Click Apply.

Figure 128: Configuring Storm Control



Traffic > Storm Control

Interface ● Port ○ Trunk

Port Storm Control List Total: 28

Port	Type	Unknown Unicast		Multicast		Broadcast	
		Status	Rate (packets/sec) (500-14880000)	Status	Rate (packets/sec) (500-14880000)	Status	Rate (packets/sec) (500-14880000)
1	1000BASE SFP	□ Enabled	262143	□ Enabled	262143	☑ Enabled	500
2	1000BASE SFP	□ Enabled	262143	□ Enabled	262143	☑ Enabled	500
3	1000BASE SFP	□ Enabled	262143	□ Enabled	262143	☑ Enabled	500
4	1000BASE SFP	□ Enabled	262143	□ Enabled	262143	☑ Enabled	500
5	1000BASE SFP	□ Enabled	262143	□ Enabled	262143	☑ Enabled	500

AUTOMATIC TRAFFIC CONTROL

Use the Traffic > Congestion Control > Auto Traffic Control pages to configure bounding thresholds for broadcast and multicast storms which can automatically trigger rate limits or shut down a port.

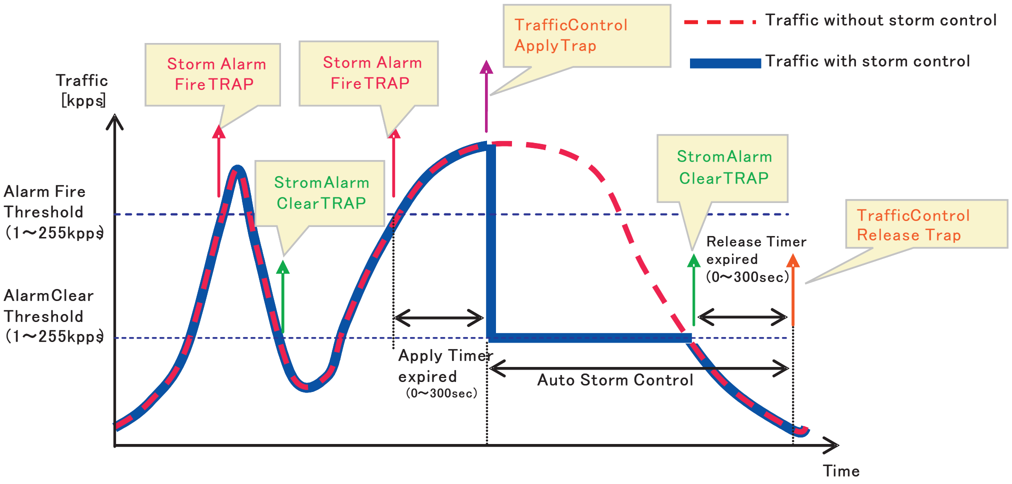
CLI REFERENCES

- "Automatic Traffic Control Commands" on page 1207

COMMAND USAGE

ATC includes storm control for broadcast or multicast traffic. The control response for either of these traffic types is the same, as shown in the following diagrams.

Figure 129: Storm Control by Limiting the Traffic Rate

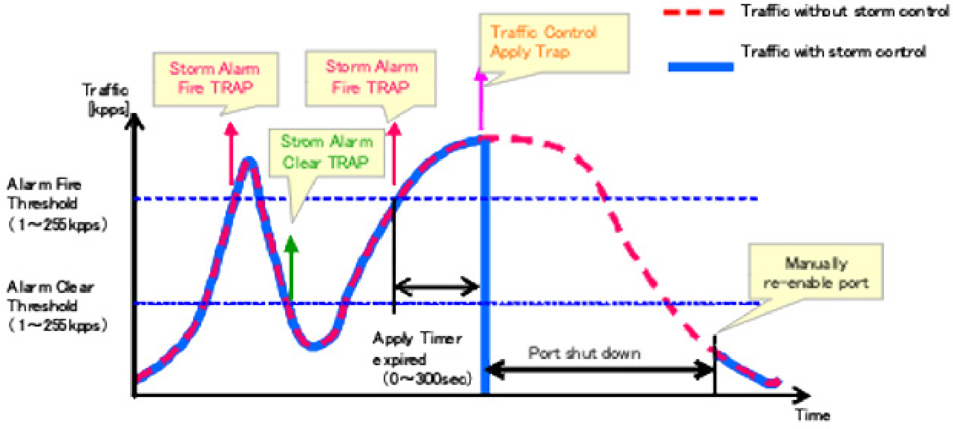


Traffic without storm control
Traffic with storm control
Traffic [kpps]
Storm Alarm Fire TRAP
Storm Alarm Fire TRAP
TrafficControl Apply Trap
StromAlarm Clear TRAP
StromAlarm Clear TRAP
TrafficControl Release Trap
Alarm Fire Threshold (1~255kpps)
AlarmClear Threshold (1~255kpps)
Apply Timer expired (0~300sec)
Auto Storm Control
Release Timer expired (0~300sec)
Time

The key elements of this diagram are described below:

- Alarm Fire Threshold – The highest acceptable traffic rate. When ingress traffic exceeds the threshold, ATC sends a Storm Alarm Fire Trap and logs it.
- When traffic exceeds the alarm fire threshold and the apply timer expires, a traffic control response is applied, and a Traffic Control Apply Trap is sent and logged.
- Alarm Clear Threshold – The lower threshold beneath which a control response can be automatically terminated after the release timer expires. When ingress traffic falls below this threshold, ATC sends a Storm Alarm Clear Trap and logs it.
- When traffic falls below the alarm clear threshold after the release timer expires, traffic control (for rate limiting) will be stopped and a Traffic Control Release Trap sent and logged. Note that if the control action has shut down a port, it can only be manually re-enabled using Manual Control Release (see page 301).
- The traffic control response of rate limiting can be released automatically or manually. The control response of shutting down a port can only be released manually.

Figure 130: Storm Control by Shutting Down a Port


Traffic without storm control
Traffic with storm control
Traffic Control Apply Trap
Storm Alarm Fire TRAP
Storm Alarm Fire TRAP
Strom Alarm Clear TRAP
Traffic [kpps]
Alarm Fire Threshold (1~255kpps)
Alarm Clear Threshold (1~255kpps)
Apply Timer expired (0~300sec)
Port shut down
Manually re-enable port
Time

The key elements of this diagram are the same as that described in the preceding diagram, except that automatic release of the control response is not provided. When traffic control is applied, you must manually re-enable the port.

Functional Limitations

Automatic storm control is a software level control function. Traffic storms can also be controlled at the hardware level using Port Broadcast Control or Port Multicast Control (as described on page 296). However, only one of these control types can be applied to a port. Enabling automatic storm control on a port will disable hardware-level storm control on that port.

SETTING THE ATC TIMERS

Use the Traffic > Auto Traffic Control (Configure Global) page to set the time at which to apply the control response after ingress traffic has exceeded the upper threshold, and the time at which to release the control response after ingress traffic has fallen beneath the lower threshold.

CLI REFERENCES

- "auto-traffic-control apply-timer" on page 1210
- "auto-traffic-control release-timer" on page 1210

COMMAND USAGE

- After the apply timer expires, the settings in the Traffic > Automatic Traffic Control (Configure Interface) page are used to determine if a control action will be triggered (as configured under the Action field) or a trap message sent (as configured under the Trap Storm Fire field).

- The release timer only applies to a Rate Control response set in the Action field of the ATC (Interface Configuration) page. When a port has been shut down by a control response, it must be manually re-enabled using the Manual Control Release (see page 301).

PARAMETERS

These parameters are displayed in the web interface:

- **Broadcast Apply Timer** – The interval after the upper threshold has been exceeded at which to apply the control response to broadcast storms. (Range: 1-300 seconds; Default: 300 seconds)

- **Broadcast Release Timer** – The time at which to release the control response after ingress traffic has fallen beneath the lower threshold for broadcast storms. (Range: 1-900 seconds; Default: 900 seconds)

- **Multicast Apply Timer** – The interval after the upper threshold has been exceeded at which to apply the control response to multicast storms. (Range: 1-300 seconds; Default: 300 seconds)

- **Multicast Release Timer** – The time at which to release the control response after ingress traffic has fallen beneath the lower threshold for multicast storms. (Range: 1-900 seconds; Default: 900 seconds)

WEB INTERFACE

To configure the response timers for automatic storm control:

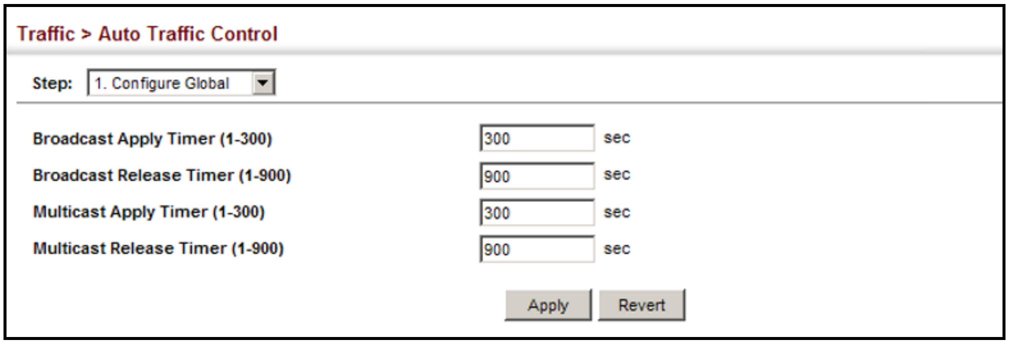
1. Click Traffic, Automatic Traffic Control.

2. Select Configure Global from the Step field.

3. Set the apply and release timers for broadcast and multicast storms.

4. Click Apply.

Figure 131: Configuring ATC Timers



Traffic > Auto Traffic Control

Step: 1. Configure Global

Broadcast Apply Timer (1-300): 300 sec

Broadcast Release Timer (1-900): 900 sec

Multicast Apply Timer (1-300): 300 sec

Multicast Release Timer (1-900): 900 sec

CONFIGURING ATC THRESHOLDS AND RESPONSES

Use the Traffic > Auto Traffic Control (Configure Interface) page to set the storm control mode (broadcast or multicast), the traffic thresholds, the control response, to automatically release a response of rate limiting, or to send related SNMP trap messages.

CLI REFERENCES

- "Automatic Traffic Control Commands" on page 1207

PARAMETERS

These parameters are displayed in the web interface:

- **Storm Control** – Specifies automatic storm control for broadcast traffic or multicast traffic.
- **Port** – Port identifier.
- **State** – Enables automatic traffic control for broadcast or multicast storms. (Default: Disabled)

  Automatic storm control is a software level control function. Traffic storms can also be controlled at the hardware level using the Storm Control menu. However, only one of these control types can be applied to a port. Enabling automatic storm control on a port will disable hardware-level storm control on that port.
- **Action** – When the Alarm Fire Threshold (upper threshold) is exceeded and the apply timer expires, one of the following control responses will be triggered.
  - **Rate Control** – The rate of ingress traffic is limited to the level set by the Alarm Clear Threshold. Rate limiting is discontinued only after the traffic rate has fallen beneath the Alarm Clear Threshold (lower threshold), and the release timer has expired. (This is the default response.)
  - **Shutdown** – The port is administratively disabled. A port disabled by automatic traffic control can only be manually re-enabled using the Manual Control Release attribute.

- **Auto Release Control** – Automatically stops a traffic control response of rate limiting when traffic falls below the alarm clear threshold and the release timer expires as illustrated in Figure 129 on page 298. When traffic control stops, the event is logged by the system and a Traffic Release Trap can be sent. (Default: Disabled)

  If automatic control release is not enabled and a control response of rate limiting has been triggered, you can manually stop the rate limiting response using the Manual Control Release attribute. If the control response has shut down a port, it can also be re-enabled using Manual Control Release.

- **Alarm Fire Threshold** – The upper threshold for ingress traffic beyond which a storm control response is triggered after the Apply Timer expires. (Range: 1-255 kilo-packets per second; Default: 128 Kpps)

  Once the traffic rate exceeds the upper threshold and the Apply Timer expires, a trap message will be sent if configured by the Trap Storm Fire attribute.

- **Alarm Clear Threshold** – The lower threshold for ingress traffic beneath which a control response for rate limiting will be released after the Release Timer expires, if so configured by the Auto Release Control attribute. (Range: 1-255 kilo-packets per second; Default: 128 Kpps)

  If rate limiting has been configured as a control response and Auto Control Release is enabled, rate limiting will be discontinued after the traffic rate has fallen beneath the lower threshold, and the Release Timer has expired. Note that if a port has been shut down by a control response, it will not be re-enabled by automatic traffic control. It can only be manually re-enabled using Manual Control Release.

  Once the traffic rate falls beneath the lower threshold and the Release Timer expires, a trap message will be sent if configured by the Trap Storm Clear attribute.

- **Trap Storm Fire** – Sends a trap when traffic exceeds the upper threshold for automatic storm control. (Default: Disabled)

- **Trap Storm Clear** – Sends a trap when traffic falls beneath the lower threshold after a storm control response has been triggered. (Default: Disabled)

- **Trap Traffic Apply** – Sends a trap when traffic exceeds the upper threshold for automatic storm control and the apply timer expires. (Default: Disabled)

- **Trap Traffic Release** – Sends a trap when traffic falls beneath the lower threshold after a storm control response has been triggered and the release timer expires. (Default: Disabled)

- **Manual Control Release** – Manually releases a control response of rate-limiting or port shutdown any time after the specified action has been triggered.

  If this function is enabled for any port, clicking Apply with manually release the control response, and clear the check box.

WEB INTERFACE

To configure the response timers for automatic storm control:

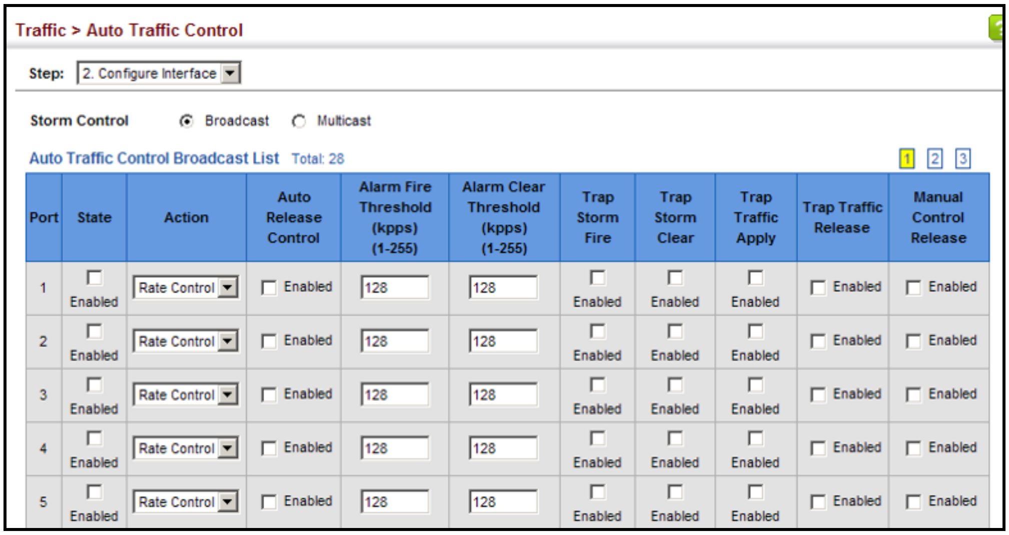
1. Click Traffic, Automatic Traffic Control.

2. Select Configure Interface from the Step field.

3. Enable or disable ATC as required, set the control response, specify whether or not to automatically release the control response of rate limiting, set the upper and lower thresholds, and specify which trap messages to send.

4. Click Apply.

Figure 132: Configuring ATC Interface Attributes



Traffic > Auto Traffic Control

Step: 2. Configure Interface ▾

Storm Control ● Broadcast ○ Multicast

Auto Traffic Control Broadcast List Total: 28

1 2 3

Port	State	Action	Auto Release Control	Alarm Fire Threshold (kpps) (1-255)	Alarm Clear Threshold (kpps) (1-255)	Trap Storm Fire	Trap Storm Clear	Trap Traffic Apply	Trap Traffic Release	Manual Control Release
1	□ Enabled	Rate Control ▾	□ Enabled	128	128	□ Enabled	□ Enabled	□ Enabled	□ Enabled	□ Enabled
2	□ Enabled	Rate Control ▾	□ Enabled	128	128	□ Enabled	□ Enabled	□ Enabled	□ Enabled	□ Enabled
3	□ Enabled	Rate Control ▾	□ Enabled	128	128	□ Enabled	□ Enabled	□ Enabled	□ Enabled	□ Enabled
4	□ Enabled	Rate Control ▾	□ Enabled	128	128	□ Enabled	□ Enabled	□ Enabled	□ Enabled	□ Enabled
5	□ Enabled	Rate Control ▾	□ Enabled	128	128	□ Enabled	□ Enabled	□ Enabled	□ Enabled	□ Enabled

10 CLASS OF SERVICE

Class of Service (CoS) allows you to specify which data packets have greater precedence when traffic is buffered in the switch due to congestion. This switch supports CoS with eight priority queues for each port. Data packets in a port's high-priority queue will be transmitted before those in the lower-priority queues. You can set the default priority for each interface, and configure the mapping of frame priority tags to the switch's priority queues.

This chapter describes the following basic topics:

- Layer 2 Queue Settings – Configures each queue, including the default priority, queue mode, queue weight, and mapping of packets to queues based on CoS tags.

- Layer 3/4 Priority Settings – Selects the method by which inbound packets are processed (DSCP or CoS), and sets the per-hop behavior and drop precedence for internal processing.

LAYER 2 QUEUE SETTINGS

This section describes how to configure the default priority for untagged frames, set the queue mode, set the weights assigned to each queue, and map class of service tags to queues.

SETTING THE DEFAULT PRIORITY FOR INTERFACES

Use the Traffic > Priority > Default Priority page to specify the default port priority for each interface on the switch. All untagged packets entering the switch are tagged with the specified default port priority, and then sorted into the appropriate priority queue at the output port.

CLI REFERENCES

- "switchport priority default" on page 1390

COMMAND USAGE

- This switch provides eight priority queues for each port. It uses Weighted Round Robin to prevent head-of-queue blockage, but can be configured to process each queue in strict order, or use a combination of strict and weighted queueing.

- The default priority applies for an untagged frame received on a port set to accept all frame types (i.e, receives both untagged and tagged frames). This priority does not apply to IEEE 802.1Q VLAN tagged frames. If the incoming frame is an IEEE 802.1Q VLAN tagged frame, the IEEE 802.1p User Priority bits will be used.

- If the output port is an untagged member of the associated VLAN, these frames are stripped of all VLAN tags prior to transmission.

PARAMETERS

These parameters are displayed:

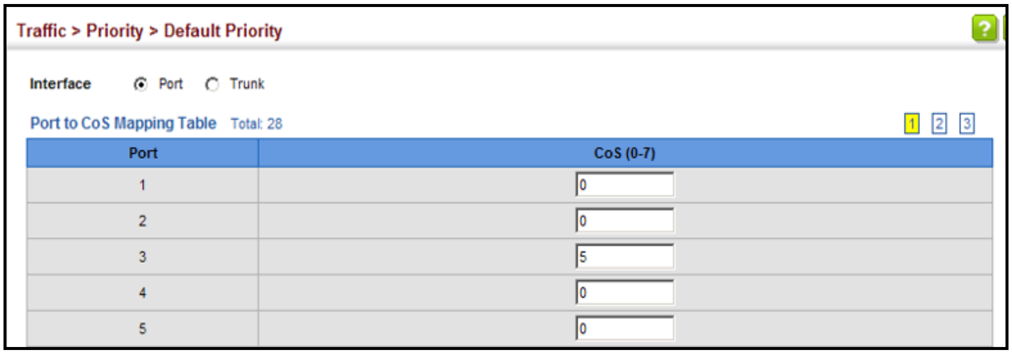
- **Interface** – Displays a list of ports or trunks.
- **CoS** – The priority that is assigned to untagged frames received on the specified interface. (Range: 0-7; Default: 0)

WEB INTERFACE

To configure the queue mode:

1. Click Traffic, Priority, Default Priority.
2. Select the interface type to display (Port or Trunk).
3. Modify the default priority for any interface.
4. Click Apply.

Figure 133: Setting the Default Port Priority



Traffic > Priority > Default Priority

Interface ● Port ○ Trunk

Port to CoS Mapping Table Total: 28

Port	CoS (0-7)
1	0
2	0
3	5
4	0
5	0

SELECTING THE QUEUE MODE

Use the Traffic > Priority > Queue page to set the queue mode for the egress queues on any interface. The switch can be set to service the queues based on a strict rule that requires all traffic in a higher priority queue to be processed before the lower priority queues are serviced, or Weighted Round-Robin (WRR) queuing which specifies a scheduling weight for each queue. It can also be configured to use a combination of strict and weighted queuing.

CLI REFERENCES

- "queue mode" on page 1388
- "show queue mode" on page 1391

COMMAND USAGE

- Strict priority requires all traffic in a higher priority queue to be processed before lower priority queues are serviced.

- WRR queuing specifies a relative weight for each queue. WRR uses a predefined relative weight for each queue that determines the percentage of service time the switch services each queue before moving on to the next queue. This prevents the head-of-line blocking that can occur with strict priority queuing.

- If Strict and WRR mode is selected, a combination of strict service is used for the high priority queues and weighted service for the remaining queues. The queues assigned to use strict priority should be specified using the Strict Mode field parameter.

- A weight can be assigned to each of the weighted queues (and thereby to the corresponding traffic priorities). This weight sets the frequency at which each queue is polled for service, and subsequently affects the response time for software applications assigned a specific priority value.

  Service time is shared at the egress ports by defining scheduling weights for WRR, or one of the queuing modes that use a combination of strict and weighted queuing.

- The specified queue mode applies to all interfaces.

- Protocols used to synchronize distributed switches use packets of 1588 bytes to control the synchronization process. This switch therefore assigns packets of this size to the highest priority queue to ensure quick passage.

PARAMETERS

These parameters are displayed:

- **Interface** – Port or trunk identifier.

- **Queue Mode**

  - **Strict** – Services the egress queues in sequential order, transmitting all traffic in the higher priority queues before servicing lower priority queues. This ensures that the highest priority packets are always serviced first, ahead of all other traffic.

  - **WRR** – Weighted Round-Robin shares bandwidth at the egress ports by using scheduling weights, and servicing each queue in a round-robin fashion. (This is the default setting.)

  - **Strict and WRR** – Uses strict priority on the high-priority queues and WRR on the rest of the queues.

- **Queue ID** – The ID of the priority queue. (Range: 0-7)

- **Strict Mode** – If “Strict and WRR” mode is selected, then a combination of strict service is used for the high priority queues and weighted service for the remaining queues. Use this parameter to specify the queues assigned to use strict priority. (Default: Disabled)

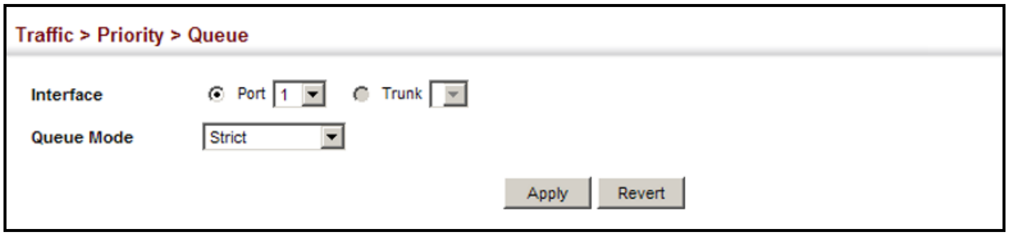
- **Weight** – Sets a weight for each queue which is used by the WRR scheduler. (Range: 1-15; Default: Weights 1, 2, 4, 6, 8, 10, 12 and 14 are assigned to queues 0 - 7 respectively)

WEB INTERFACE

To configure the queue mode:

1. Click Traffic, Priority, Queue.
2. Select a port or trunk.
3. Set the queue mode.
4. If the weighted queue mode is selected, the queue weight can be modified if required.
5. If the queue mode that uses a combination of strict and weighted queueing is selected, the queues which are serviced first must be specified by enabling strict mode parameter in the table.
6. Click Apply.

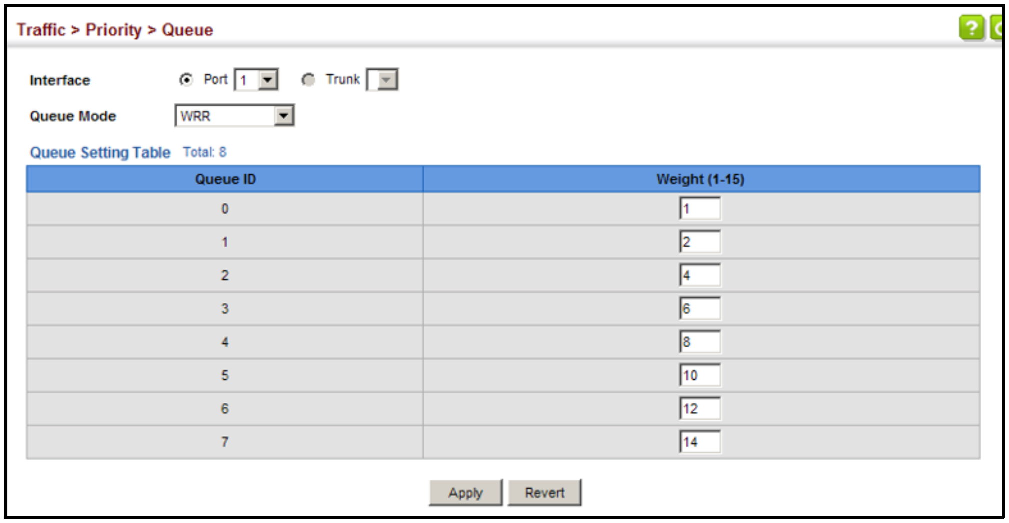
Figure 134: Setting the Queue Mode (Strict)



Interface ● Port 1 ○ Trunk

Queue Mode Strict

Figure 135: Setting the Queue Mode (WRR)



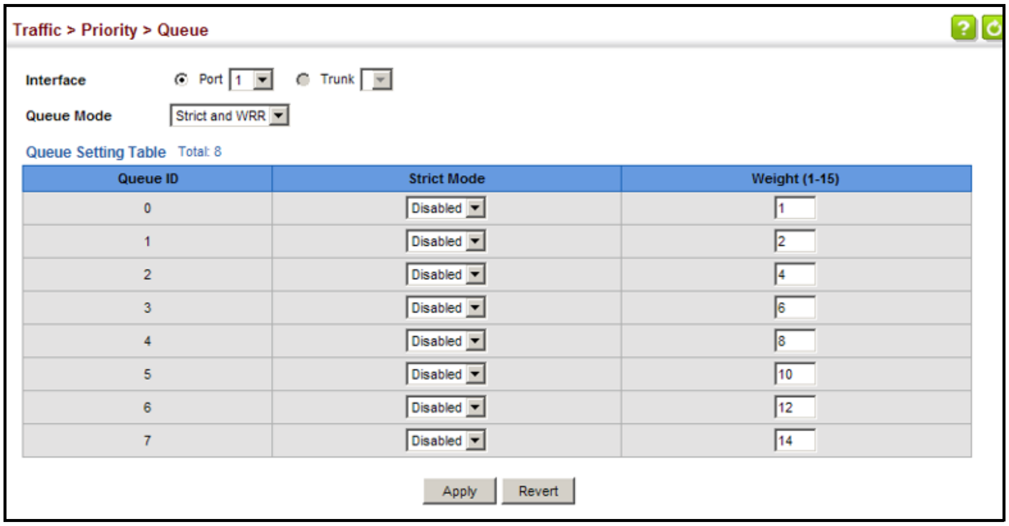
Interface ● Port 1 ○ Trunk

Queue Mode WRR

Queue Setting Table Total: 8

Queue ID	Weight (1-15)
0	1
1	2
2	4
3	6
4	8
5	10
6	12
7	14

Figure 136: Setting the Queue Mode (Strict and WRR)



Traffic > Priority > Queue

Interface ● Port 1 ○ Trunk

Queue Mode Strict and WRR

Queue Setting Table Total: 8

Queue ID	Strict Mode	Weight (1-15)
0	Disabled	1
1	Disabled	2
2	Disabled	4
3	Disabled	6
4	Disabled	8
5	Disabled	10
6	Disabled	12
7	Disabled	14

MAPPING COS VALUES TO EGRESS QUEUES

Use the Traffic > Priority > PHB to Queue page to specify the hardware output queues to use based on the internal per-hop behavior value. (For more information on exact manner in which the ingress priority tags are mapped to egress queues for internal processing, see "Mapping CoS Priorities to Internal DSCP Values" on page 316).

The switch processes Class of Service (CoS) priority tagged traffic by using eight priority queues for each port, with service schedules based on strict priority, Weighted Round-Robin (WRR), or a combination of strict and weighted queuing. Up to eight separate traffic priorities are defined in IEEE 802.1p. Default priority levels are assigned according to recommendations in the IEEE 802.1p standard as shown in Table 14. The following table indicates the default mapping of internal per-hop behavior to the hardware queues. The actual mapping may differ if the CoS priorities to internal DSCP values have been modified (page 316).

Table 14: IEEE 802.1p Egress Queue Priority Mapping

Priority	0	1	2	3	4	5	6	7
Queue	2	0	1	3	4	5	6	7

The priority levels recommended in the IEEE 802.1p standard for various network applications are shown in Table 15. However, priority levels can be mapped to the switch's output queues in any way that benefits application traffic for the network.

Table 15: CoS Priority Levels

Priority Level	Traffic Type
1	Background
2	(Spare)
0 (default)	Best Effort
3	Excellent Effort
4	Controlled Load
5	Video, less than 100 milliseconds latency and jitter
6	Voice, less than 10 milliseconds latency and jitter
7	Network Control

CLI References

- "qos map phb-queue" on page 1399

Command Usage

- Egress packets are placed into the hardware queues according to the mapping defined by this command.

- The default internal PHB to output queue mapping is shown below.

Table 16: Mapping Internal Per-hop Behavior to Hardware Queues

Per-hop Behavior	0	1	2	3	4	5	6	7
Hardware Queues	2	0	1	3	4	5	6	7

- The specified mapping applies to all interfaces.

Parameters

These parameters are displayed:

- **Port** – Specifies a port.

- **PHB** – Per-hop behavior, or the priority used for this router hop. (Range: 0-7, where 7 is the highest priority)

- **Queue** – Output queue buffer. (Range: 0-7, where 7 is the highest CoS priority queue)

Web Interface

To map internal PHB to hardware queues:

1. Click Traffic, Priority, PHB to Queue.

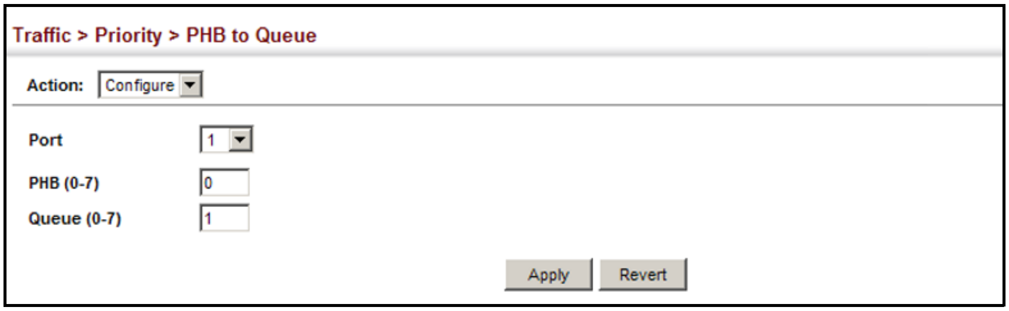
2. Select Configure from the Action list.

3. Select a port.

4. Map an internal PHB to a hardware queue. Depending on how an ingress packet is processed internally based on its CoS value, and the assigned output queue, the mapping done on this page can effectively determine the service priority for different traffic classes.

5. Click Apply.

Figure 137: Mapping CoS Values to Egress Queues


Traffic > Priority > PHB to Queue

Action: Configure

Port: 1

PHB (0-7): 0

Queue (0-7): 1

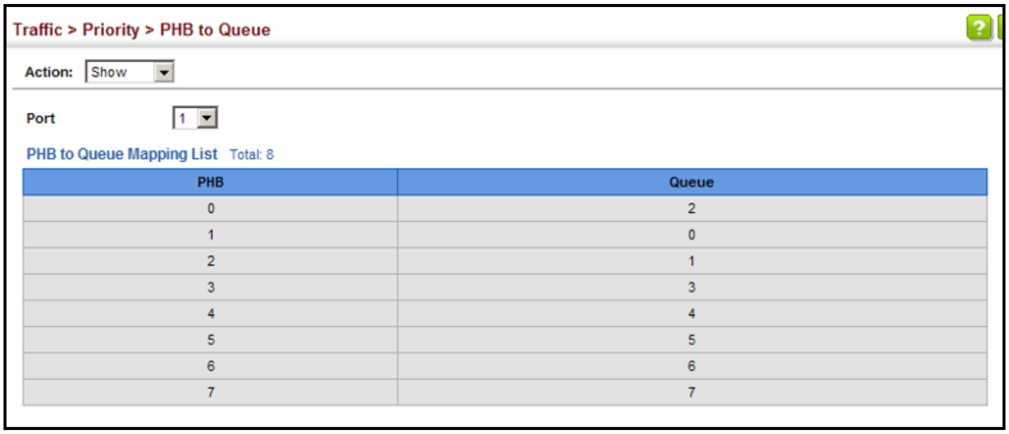
To show the internal PHB to hardware queue map:

1. Click Traffic, Priority, PHB to Queue.

2. Select Show from the Action list.

3. Select an interface.

Figure 138: Showing CoS Values to Egress Queue Mapping


Traffic > Priority > PHB to Queue

Action: Show

Port: 1

PHB to Queue Mapping List Total: 8

PHB	Queue
0	2
1	0
2	1
3	3
4	4
5	5
6	6
7	7

LAYER 3/4 PRIORITY SETTINGS

Mapping Layer 3/4 Priorities to CoS Values

The switch supports several common methods of prioritizing layer 3/4 traffic to meet application requirements. Traffic priorities can be specified in the IP header of a frame, using the priority bits in the Type of Service (ToS) octet, or the number of the TCP/UDP port. If priority bits are used, the ToS octet may contain three bits for IP Precedence or six bits for Differentiated Services Code Point (DSCP) service. When these services are enabled, the priorities are mapped to a Class of Service value by the switch, and the traffic then sent to the corresponding output queue.

Because different priority information may be contained in the traffic, this switch maps priority values to the output queues in the following manner – The precedence for priority mapping is DSCP Priority and then Default Port Priority.

NOTE: The default settings used for mapping priority values from ingress traffic to internal DSCP values are used to determine the hardware queues used for egress traffic, not to replace the priority values. These defaults are designed to optimize priority services for the majority of network applications. It should not be necessary to modify any of the default settings, unless a queuing problem occurs with a particular application.

SETTING PRIORITY PROCESSING TO IP PRECEDENCE/DSCP OR COS

The switch allows a choice between using IP Precedence, DSCP or CoS priority processing methods. Use the Priority > Trust Mode page to select the required processing method.

CLI REFERENCES

- "qos map trust-mode" on page 1400

COMMAND USAGE

- If the QoS mapping mode is set to IP Precedence, and the ingress packet type is IPv4, then priority processing will be based on the IP Precedence value in the ingress packet.

- If the QoS mapping mode is set to DSCP, and the ingress packet type is IPv4, then priority processing will be based on the DSCP value in the ingress packet.

- If the QoS mapping mode is set to either IP Precedence or DSCP, and a non-IP packet is received, the packet’s CoS and CFI (Canonical Format Indicator) values are used for priority processing if the packet is tagged. For an untagged packet, the default port priority (see page 305) is used for priority processing.

- If the QoS mapping mode is set to CoS, and the ingress packet type is IPv4, then priority processing will be based on the CoS and CFI values in the ingress packet.

  For an untagged packet, the default port priority (see page 305) is used for priority processing.

PARAMETERS

These parameters are displayed:

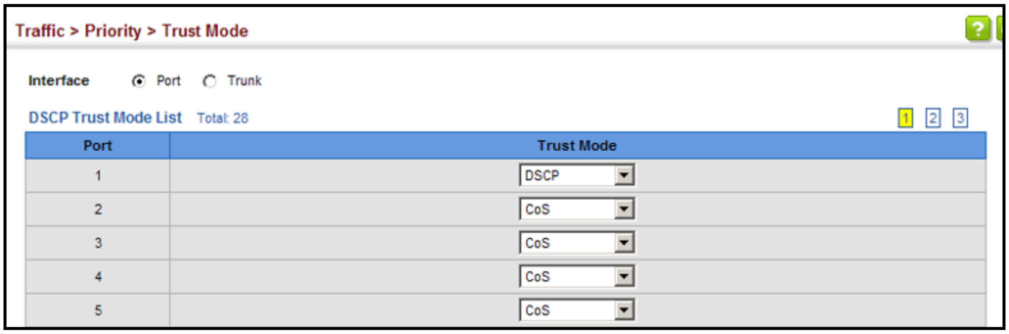
- **Interface** – Specifies a port or trunk.
- **Trust Mode**
  - **CoS** – Maps layer 3/4 priorities using Class of Service values. (This is the default setting.)
  - **DSCP** – Maps layer 3/4 priorities using Differentiated Services Code Point values.
  - **IP Precedence** – Maps layer 3/4 priorities using IP Precedence values.

WEB INTERFACE

To configure the trust mode:

1. Click Traffic, Priority, Trust Mode.
2. Select the interface type to display (Port or Trunk).
3. Set the trust mode.
4. Click Apply.

Figure 139: Setting the Trust Mode



Traffic > Priority > Trust Mode

Interface ● Port ○ Trunk

DSCP Trust Mode List Total: 28

Port	Trust Mode
1	DSCP
2	CoS
3	CoS
4	CoS
5	CoS

MAPPING INGRESS DSCP VALUES TO INTERNAL DSCP VALUES

Use the Traffic > Priority > DSCP to DSCP page to map DSCP values in incoming packets to per-hop behavior and drop precedence values for internal priority processing.

The DSCP is six bits wide, allowing coding for up to 64 different forwarding behaviors. The DSCP replaces the ToS bits, but it retains backward compatibility with the three precedence bits so that non-DSCP compliant, ToS-enabled devices, will not conflict with the DSCP mapping. Based on network policies, different kinds of traffic can be marked for different kinds of forwarding.

CLI REFERENCES

- "qos map dscp-mutation" on page 1396

COMMAND USAGE

- Enter per-hop behavior and drop precedence for any of the DSCP values 0 - 63.

- This map is only used when the priority mapping mode is set to DSCP (see page 312), and the ingress packet type is IPv4. Any attempt to configure the DSCP mutation map will not be accepted by the switch, unless the trust mode has been set to DSCP.

- Two QoS domains can have different DSCP definitions, so the DSCP-to-PHB/Drop Precedence mutation map can be used to modify one set of DSCP values to match the definition of another domain. The mutation map should be applied at the receiving port (ingress mutation) at the boundary of a QoS administrative domain.

- Random Early Detection starts dropping yellow and red packets when the buffer fills up to 0x60 packets, and then starts dropping any packets regardless of color when the buffer fills up to 0x80 packets.

PARAMETERS

These parameters are displayed:

- **Port** – Specifies a port.

- **DSCP** – DSCP value in ingress packets. (Range: 0-63)

- **PHB** – Per-hop behavior, or the priority used for this router hop. (Range: 0-7)

- **Drop Precedence** – Drop precedence used for Random Early Detection in controlling traffic congestion. (Range: 0 - Green, 3 - Yellow, 1 - Red)

Table 17: Default Mapping of DSCP Values to Internal PHB/Drop Values

ingress-dscp1	0	1	2	3	4	5	6	7	8	9
ingress-dscp10										
0	0,0	0,1	0,0	0,3	0,0	0,1	0,0	0,3	1,0	1,1
1	1,0	1,3	1,0	1,1	1,0	1,3	2,0	2,1	2,0	2,3
2	2,0	2,1	2,0	2,3	3,0	3,1	3,0	3,3	3.0	3,1
3	3,0	3,3	4,0	4,1	4,0	4,3	4,0	4,1	4.0	4,3
4	5,0	5,1	5,0	5,3	5,0	5,1	6,0	5,3	6,0	6,1
5	6,0	6,3	6,0	6,1	6,0	6,3	7,0	7,1	7.0	7,3
6	7,0	7,1	7,0	7,3						

The ingress DSCP is composed of ingress-dscp10 (most significant digit in the left column) and ingress-dscp1 (least significant digit in the top row (in other words, ingress-dscp = ingress-dscp10 * 10 + ingress-dscp1); and the corresponding internal-dscp is shown at the intersecting cell in the table.

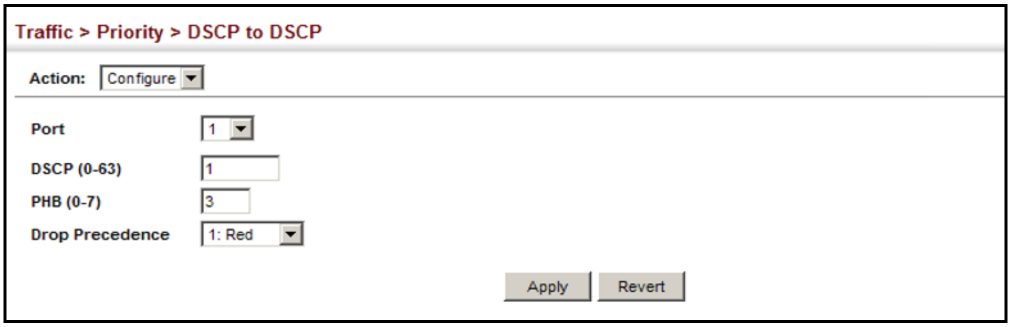
The ingress DSCP is bitwise ANDed with the binary value 11 to determine the drop precedence. If the resulting value is 10 binary, then the drop precedence is set to 0.

WEB INTERFACE

To map DSCP values to internal PHB/drop precedence:

1. Click Traffic, Priority, DSCP to DSCP.
2. Select Configure from the Action list.
3. Select a port.
4. Set the PHB and drop precedence for any DSCP value.
5. Click Apply.

Figure 140: Configuring DSCP to DSCP Internal Mapping



Traffic > Priority > DSCP to DSCP

Action: Configure

Port: 1

DSCP (0-63): 1

PHB (0-7): 3

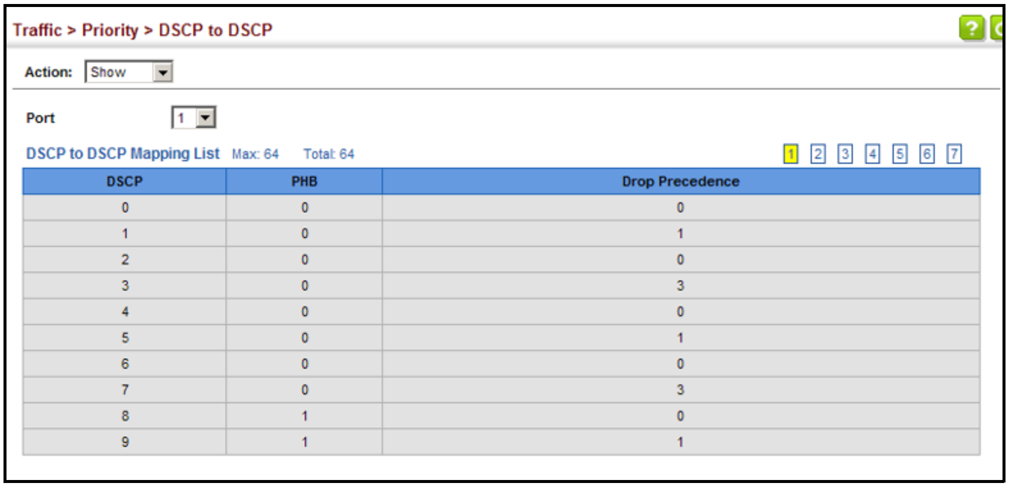
Drop Precedence: 1: Red

To show the DSCP to internal PHB/drop precedence map:

1. Click Traffic, Priority, DSCP to DSCP.
2. Select Show from the Action list.

3. Select a port.

Figure 141: Showing DSCP to DSCP Internal Mapping



Traffic > Priority > DSCP to DSCP

Action: Show

Port 1

DSCP to DSCP Mapping List Max: 64 Total: 64

DSCP	PHB	Drop Precedence
0	0	0
1	0	1
2	0	0
3	0	3
4	0	0
5	0	1
6	0	0
7	0	3
8	1	0
9	1	1

MAPPING COS PRIORITIES TO INTERNAL DSCP VALUES

Use the Traffic > Priority > CoS to DSCP page to maps CoS/CFI values in incoming packets to per-hop behavior and drop precedence values for priority processing.

CLI REFERENCES

- "qos map cos-dscp" on page 1393

COMMAND USAGE

- The default mapping of CoS to PHB values is shown in Table 18 on page 317.

- Enter up to eight CoS/CFI paired values, per-hop behavior and drop precedence.

- If a packet arrives with a 802.1Q header but it is not an IP packet, then the CoS/CFI-to-PHB/Drop Precedence mapping table is used to generate priority and drop precedence values for internal processing. Note that priority tags in the original packet are not modified by this command.

- The internal DSCP consists of three bits for per-hop behavior (PHB) which determines the queue to which a packet is sent; and two bits for drop precedence (namely color) which is used to control traffic congestion.

PARAMETERS

These parameters are displayed:

- **Port** – Specifies a port.

- **CoS** – CoS value in ingress packets. (Range: 0-7)

- **CFI** – Canonical Format Indicator. Set to this parameter to “0” to indicate that the MAC address information carried in the frame is in canonical format. (Range: 0-1)

- **PHB** – Per-hop behavior, or the priority used for this router hop. (Range: 0-7)

- **Drop Precedence** – Drop precedence used for controlling traffic congestion. (Range: 0 - Green, 3 - Yellow, 1 - Red)

Table 18: Default Mapping of CoS/CFI to Internal PHB/Drop Precedence

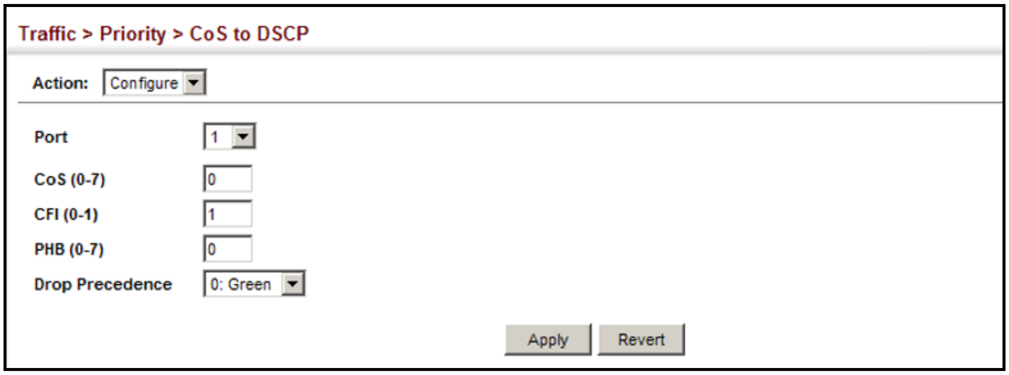
CoS \ CFI	0	1
0	(0,0)	(0,0)
1	(1,0)	(1,0)
2	(2,0)	(2,0)
3	(3,0)	(3,0)
4	(4,0)	(4,0)
5	(5,0)	(5,0)
6	(6,0)	(6,0)
7	(7,0)	(7,0)

WEB INTERFACE

To map CoS/CFI values to internal PHB/drop precedence:

1. Click Traffic, Priority, CoS to DSCP.
2. Select Configure from the Action list.
3. Select a port.
4. Set the PHB and drop precedence for any of the CoS/CFI combinations.
5. Click Apply.

Figure 142: Configuring CoS to DSCP Internal Mapping



Traffic > Priority > CoS to DSCP

Action: Configure

Port: 1

CoS (0-7): 0

CFI (0-1): 1

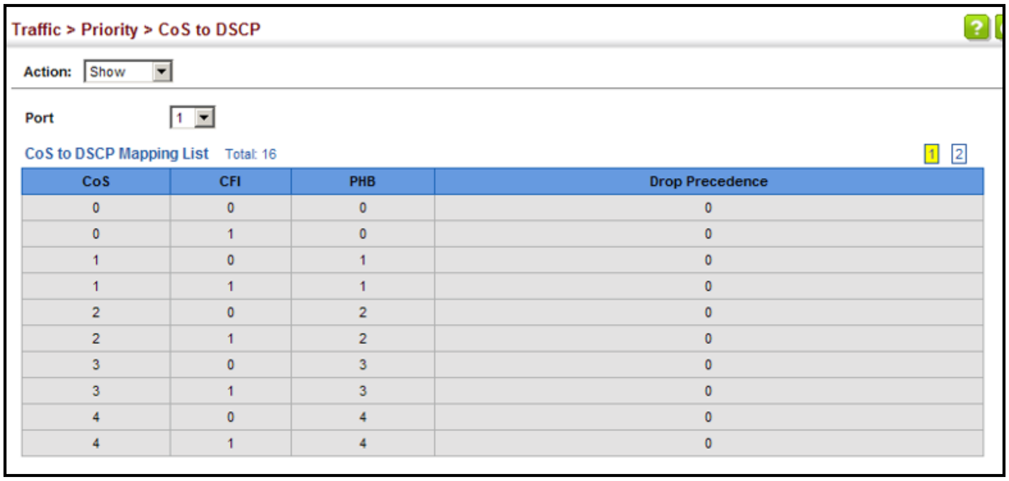
PHB (0-7): 0

Drop Precedence: 0: Green

To show the CoS/CFI to internal PHB/drop precedence map:

1. Click Traffic, Priority, CoS to DSCP.
2. Select Show from the Action list.
3. Select a port.

Figure 143: Showing CoS to DSCP Internal Mapping



Traffic > Priority > CoS to DSCP

Action: Show

Port 1

CoS to DSCP Mapping List Total: 16

CoS	CFI	PHB	Drop Precedence
0	0	0	0
0	1	0	0
1	0	1	0
1	1	1	0
2	0	2	0
2	1	2	0
3	0	3	0
3	1	3	0
4	0	4	0
4	1	4	0

MAPPING INTERNAL DSCP VALUES TO EGRESS COS VALUES

Use the Traffic > Priority > DSCP to CoS page to map internal per-hop behavior and drop precedence value pairs to CoS values used in tagged egress packets on a Layer 2 interface.

CLI REFERENCES

- "qos map dscp-cos" on page 1395

COMMAND USAGE

- Enter any per-hop behavior and drop precedence pair within the internal priority map, and then enter the corresponding CoS/CFI pair.
- If the packet is forwarded with an 8021.Q tag, the priority value in the egress packet is modified based on the default values shown in Table 19 on page 319, or on the values modified by this function.

PARAMETERS

These parameters are displayed in the web interface:

- **Port** – Specifies a port.
- **PHB** – Per-hop behavior, or the priority used for this router hop. (Range: 0-7)
- **Drop Precedence** – Drop precedence used for controlling traffic congestion. (Range: 0 - Green, 3 - Yellow, 1 - Red)

- **CoS** – Class-of-Service value. (Range: 0-7)
- **CFI** – Canonical Format Indicator. Set to this parameter to “0” to indicate that the MAC address information carried in the frame is in canonical format. (Range: 0-1)

Table 19: Mapping Internal PHB/Drop Precedence to CoS/CFI Values

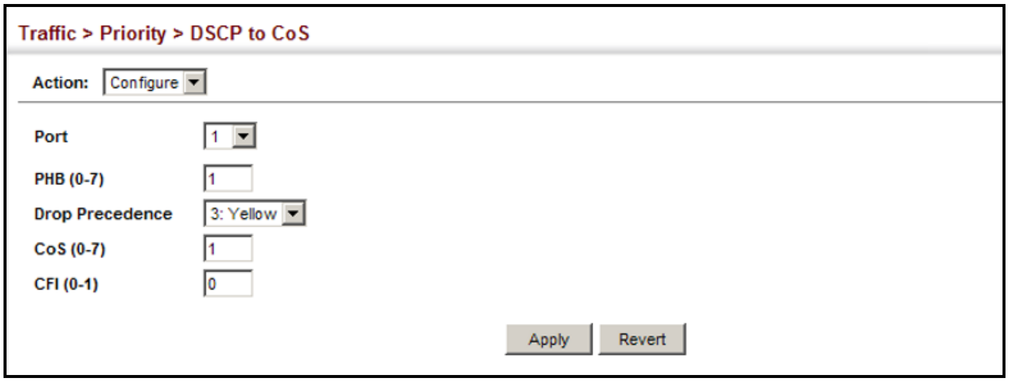
Drop Precedence	0 (green)	1 (red)	3 (yellow)
Per-hop Behavior			
0	(0,0)	(0,0)	(0,0)
1	(1,0)	(1,0)	(1,0)
2	(2,0)	(2,0)	(2,0)
3	(3,0)	(3,0)	(3,0)
4	(4,0)	(4,0)	(4,0)
5	(5,0)	(5,0)	(5,0)
6	(6,0)	(6,0)	(6,0)
7	(7,0)	(7,0)	(7,0)

WEB INTERFACE

To map internal per-hop behavior and drop precedence values to CoS values in the web interface:

1. Click Traffic, Priority, DSCP to CoS.
1. Select Configure from the Action list.
2. Select a port.
3. Select any PHB and drop precedence pair within the internal priority map, and then set the corresponding CoS/CFI pair.
4. Click Apply.

Figure 144: Configuring DSCP to CoS Egress Mapping



Traffic > Priority > DSCP to CoS

Action: Configure

Port: 1
PHB (0-7): 1
Drop Precedence: 3: Yellow
CoS (0-7): 1
CFI (0-1): 0

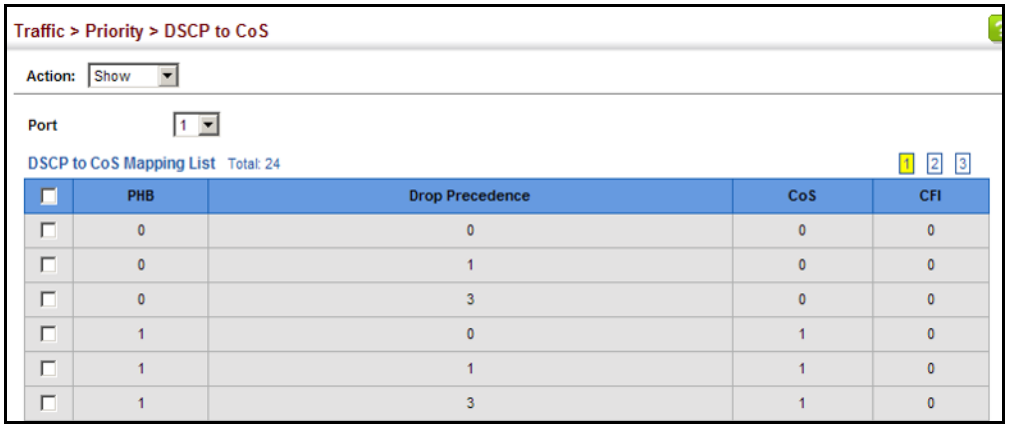
To show the DSCP to CoS egress map in the web interface:

1. Click Traffic, Priority, DSCP to CoS.

1. Select Show from the Action list.

2. Select a port.

Figure 145: Showing DSCP to CoS Egress Mapping



Traffic > Priority > DSCP to CoS

Action: Show

Port 1

DSCP to CoS Mapping List Total: 24

□	PHB	Drop Precedence	CoS	CFI
□	0	0	0	0
□	0	1	0	0
□	0	3	0	0
□	1	0	1	0
□	1	1	1	0
□	1	3	1	0

MAPPING IP PRECEDENCE VALUES TO INTERNAL DSCP VALUES

Use the Traffic > Priority > IP Precedence to DSCP page to map IP precedence values in incoming packets to per-hop behavior and drop precedence values for priority processing.

The Type of Service (ToS) octet in the IPv4 header includes three precedence bits defining eight different priority levels ranging from highest priority for network control packets to lowest priority for routine traffic. The default IP Precedence values map one-to-one to the Class of Service values (that is, Precedence value 0 maps to PHB value 0, and so forth). Bits 6 and 7 are used for network control, and the other bits for various application types. The ToS bits are defined in Table 20.

Table 20: Mapping IP Precedence

Priority Level	Traffic Type
7	Network Control
6	Internetwork Control
5	Critical
4	Flash Override
3	Flash
2	Immediate
1	Priority
0	Routine

CLI References

- "qos map ip-prec-dscp" on page 1398

Command Usage

- Enter per-hop behavior and drop precedence for any of the IP Precedence values 0 - 7.
- If the priority mapping mode is set the IP Precedence and the ingress packet type is IPv4, then the IP Precedence-to-PHB/Drop Precedence mapping table is used to generate priority and drop precedence values for internal processing.

Parameters

These parameters are displayed in the web interface:

- **Port** – Specifies a port.
- **IP Precedence** – IP Precedence value in ingress packets. (Range: 0-7)
- **PHB** – Per-hop behavior, or the priority used for this router hop. (Range: 0-7)
- **Drop Precedence** – Drop precedence used for controlling traffic congestion. (Range: 0 - Green, 3 - Yellow, 1 - Red)

Table 21: Default Mapping of IP Precedence to Internal PHB/Drop Values

IP Precedence Value	0	1	2	3	4	5	6	7
Per-hop Behavior	0	1	2	3	4	5	6	7
Drop Precedence	0	0	0	0	0	0	0	0

Web Interface

To map IP Precedence to internal PHB/drop precedence in the web interface:

1. Click Traffic, Priority, IP Precedence to DSCP.

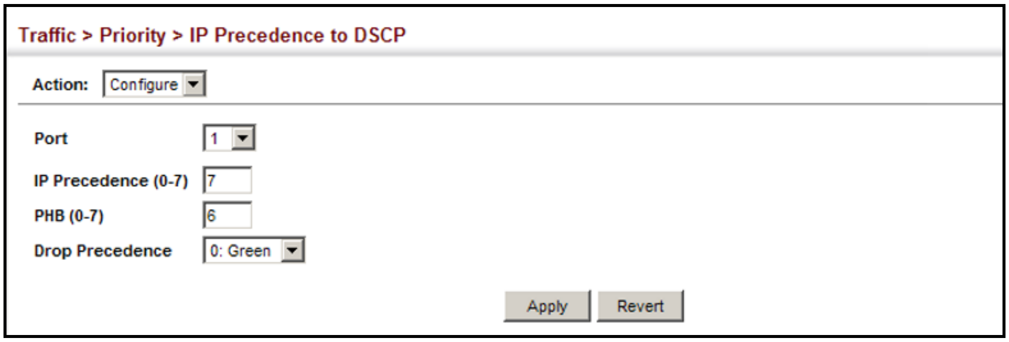
1. Select Configure from the Action list.

2. Select a port.

3. Set the PHB and drop precedence for any of the IP Precedence values.

4. Click Apply.

Figure 146: Configuring IP Precedence to DSCP Internal Mapping



Traffic > Priority > IP Precedence to DSCP

Action: Configure

Port: 1

IP Precedence (0-7): 7

PHB (0-7): 6

Drop Precedence: 0: Green

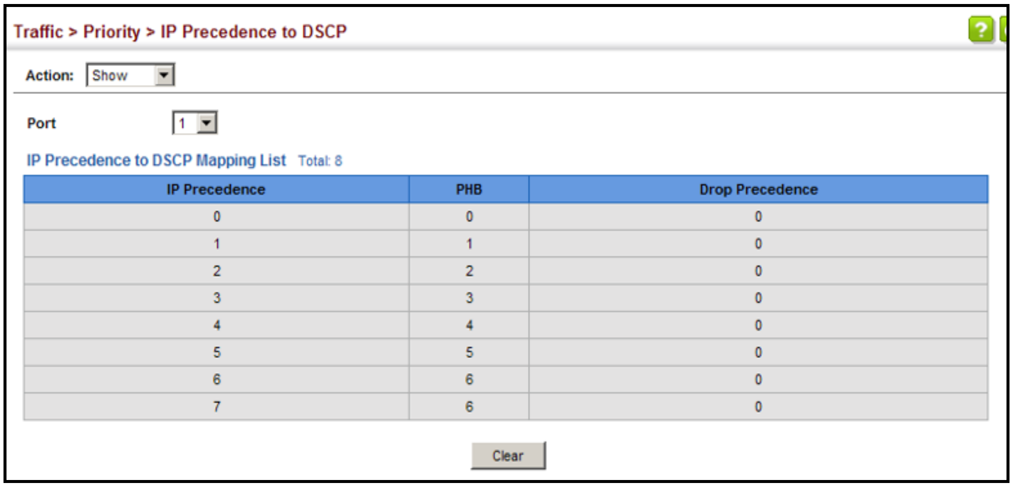
To show the IP Precedence to internal PHB/drop precedence map in the web interface:

1. Click Traffic, Priority, IP Precedence to DSCP.

2. Select Show from the Action list.

3. Select a port.

Figure 147: Showing the IP Precedence to DSCP Internal Map



Traffic > Priority > IP Precedence to DSCP

Action: Show

Port: 1

IP Precedence to DSCP Mapping List Total: 8

IP Precedence	PHB	Drop Precedence
0	0	0
1	1	0
2	2	0
3	3	0
4	4	0
5	5	0
6	6	0
7	6	0

MAPPING IP PORT PRIORITY TO INTERNAL DSCP VALUES

Use the Traffic > Priority > IP Port to DSCP page to map network applications designated by a TCP/UDP destination port number in the frame header to per-hop behavior and drop precedence values for internal priority processing.

CLI REFERENCES

- "qos map ip-port-dscp" on page 1398

COMMAND USAGE

- This mapping table is only used if the protocol type of the arriving packet is TCP or UDP. Some of the more common TCP service ports include: HTTP: 80, FTP: 21, Telnet: 23 and POP3: 110.

- No default mapping is defined for ingress TCP/UDP port types.

PARAMETERS

These parameters are displayed in the web interface:

- **Port** – Specifies a port.

- **IP Protocol**

  - **TCP** – Transport Control Protocol

  - **UDP** – User Datagram Protocol

- Destination Port Number – 16-bit TCP/UDP destination port number. (Range: 0-65535)

- PHB – Per-hop behavior, or the priority used for this router hop. (Range: 0-7)

- Drop Precedence – Drop precedence used for controlling traffic congestion. (Range: 0 - Green, 3 - Yellow, 1 - Red)

WEB INTERFACE

To map TCP/UDP port number to per-hop behavior and drop precedence in the web interface:

1. Click Traffic, Priority, IP Port to DSCP.

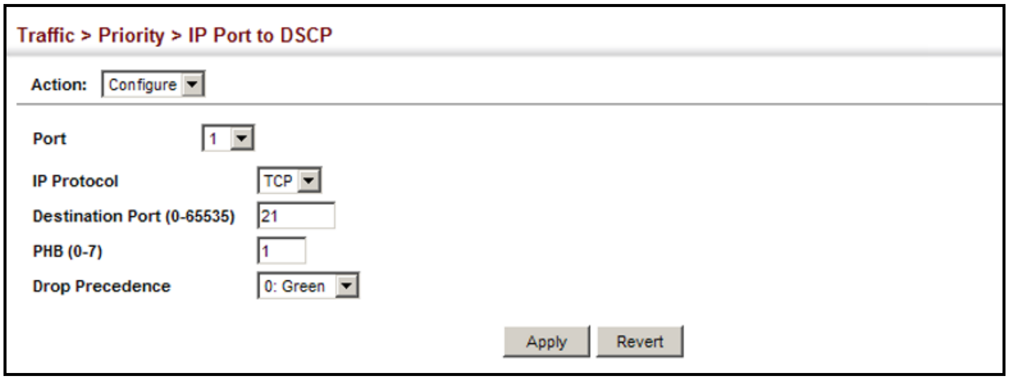
1. Select Configure from the Action list.

2. Select a port.

3. Set the PHB and drop precedence for any TCP or UDP port.

4. Click Apply.

Figure 148: Configuring IP Port Number to DSCP Internal Mapping



Traffic > Priority > IP Port to DSCP

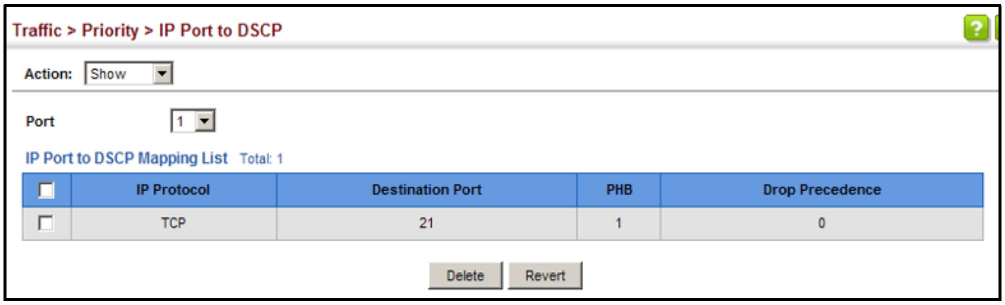
Action: Configure

Port	1
IP Protocol	TCP
Destination Port (0-65535)	21
PHB (0-7)	1
Drop Precedence	0: Green

To show the TCP/UDP port number to per-hop behavior and drop precedence map in the web interface:

1. Click Traffic, Priority, IP Port to DSCP.
2. Select Show from the Action list.
3. Select a port.

Figure 149: Showing IP Port Number to DSCP Internal Mapping



Traffic > Priority > IP Port to DSCP

Action: Show

Port 1

IP Port to DSCP Mapping List Total: 1

□	IP Protocol	Destination Port	PHB	Drop Precedence
□	TCP	21	1	0

11 QUALITY OF SERVICE

This chapter describes the following tasks required to apply QoS policies:

Class Map – Creates a map which identifies a specific class of traffic.

Policy Map – Sets the boundary parameters used for monitoring inbound traffic, and the action to take for conforming and non-conforming traffic.

Binding to a Port – Applies a policy map to an ingress port.

OVERVIEW

The commands described in this section are used to configure Quality of Service (QoS) classification criteria and service policies. Differentiated Services (DiffServ) provides policy-based management mechanisms used for prioritizing network resources to meet the requirements of specific traffic types on a per hop basis. Each packet is classified upon entry into the network based on access lists, IP Precedence, DSCP values, VLAN lists, or CoS values. Using access lists allows you select traffic based on Layer 2, Layer 3, or Layer 4 information contained in each packet. Based on configured network policies, different kinds of traffic can be marked for different kinds of forwarding.

All switches or routers that access the Internet rely on class information to provide the same forwarding treatment to packets in the same class. Class information can be assigned by end hosts, or switches or routers along the path. Priority can then be assigned based on a general policy, or a detailed examination of the packet. However, note that detailed examination of packets should take place close to the network edge so that core switches and routers are not overloaded.

Switches and routers along the path can use class information to prioritize the resources allocated to different traffic classes. The manner in which an individual device handles traffic in the DiffServ architecture is called per-hop behavior. All devices along a path should be configured in a consistent manner to construct a consistent end-to-end QoS solution.

NOTE: You can configure up to 16 rules per class map. You can also include multiple classes in a policy map.

NOTE: You should create a class map before creating a policy map. Otherwise, you will not be able to select a class map from the policy rule settings screen (see page 329).

COMMAND USAGE

To create a service policy for a specific category or ingress traffic, follow these steps:

1. Use the Configure Class (Add) page to designate a class name for a specific category of traffic.

2. Use the Configure Class (Add Rule) page to edit the rules for each class which specify a type of traffic based on an access list, a DSCP or IP Precedence value, a VLAN, or a CoS value.

3. Use the Configure Policy (Add) page to designate a policy name for a specific manner in which ingress traffic will be handled.

4. Use the Configure Policy (Add Rule) page to add one or more classes to the policy map. Assign policy rules to each class by "setting" the QoS value (CoS or PHB) to be assigned to the matching traffic class. The policy rule can also be configured to monitor the maximum throughput and burst rate. Then specify the action to take for conforming traffic, or the action to take for a policy violation.

5. Use the Configure Interface page to assign a policy map to a specific interface.

CONFIGURING A CLASS MAP

A class map is used for matching packets to a specified class. Use the Traffic > DiffServ (Configure Class) page to configure a class map.

CLI REFERENCES

- "Quality of Service Commands" on page 1407

COMMAND USAGE

- The class map is used with a policy map (page 329) to create a service policy (page 339) for a specific interface that defines packet classification, service tagging, and bandwidth policing. Note that one or more class maps can be assigned to a policy map.

- Up to 32 class maps can be configured.

PARAMETERS

These parameters are displayed:

Add

- **Class Name** – Name of the class map. (Range: 1-32 characters)

- **Type** – Only one match command is permitted per class map, so the match-any field refers to the criteria specified by the lone match command.

- **Description** – A brief description of a class map. (Range: 1-64 characters)

Add Rule

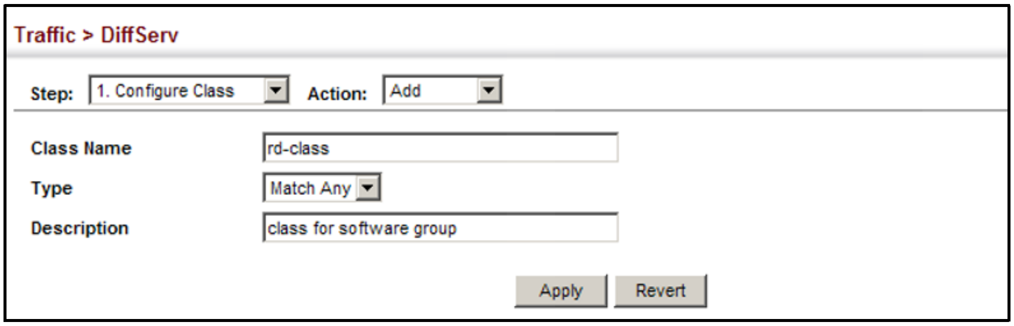
- **Class Name** – Name of the class map.
- **Type** – Only one match command is permitted per class map, so the match-any field refers to the criteria specified by the lone match command.
- **ACL** – Name of an access control list. Any type of ACL can be specified, including standard or extended IPv4/IPv6 ACLs and MAC ACLs.
- **IP DSCP** – A DSCP value. (Range: 0-63)
- **IP Precedence** – An IP Precedence value. (Range: 0-7)
- **IPv6 DSCP** – A DSCP value contained in an IPv6 packet. (Range: 0-63)
- **VLAN ID** – A VLAN. (Range:1-4094)
- **CoS** – A CoS value. (Range: 0-7)

WEB INTERFACE

To configure a class map:

1. Click Traffic, DiffServ.
2. Select Configure Class from the Step list.
3. Select Add from the Action list.
4. Enter a class name.
5. Enter a description.
6. Click Add.

Figure 150: Configuring a Class Map



Traffic > DiffServ

Step: 1. Configure Class
Action: Add

Class Name: rd-class
Type: Match Any
Description: class for software group

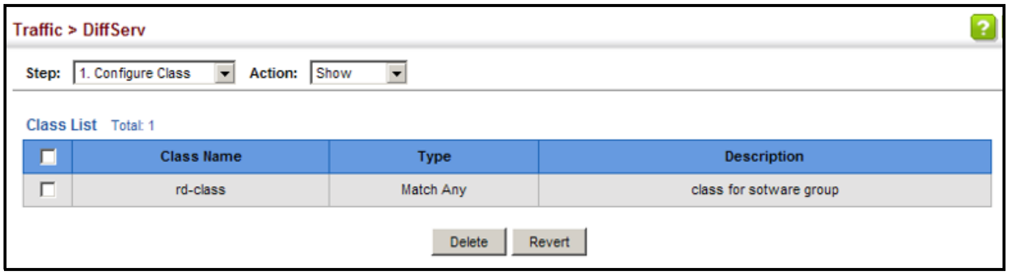
To show the configured class maps:

1. Click Traffic, DiffServ.

2. Select Configure Class from the Step list.

3. Select Show from the Action list.

Figure 151: Showing Class Maps



Traffic > DiffServ

Step: 1. Configure Class   Action: Show

Class List   Total: 1

□	Class Name	Type	Description
□	rd-class	Match Any	class for sotware group

To edit the rules for a class map:

1. Click Traffic, DiffServ.

2. Select Configure Class from the Step list.

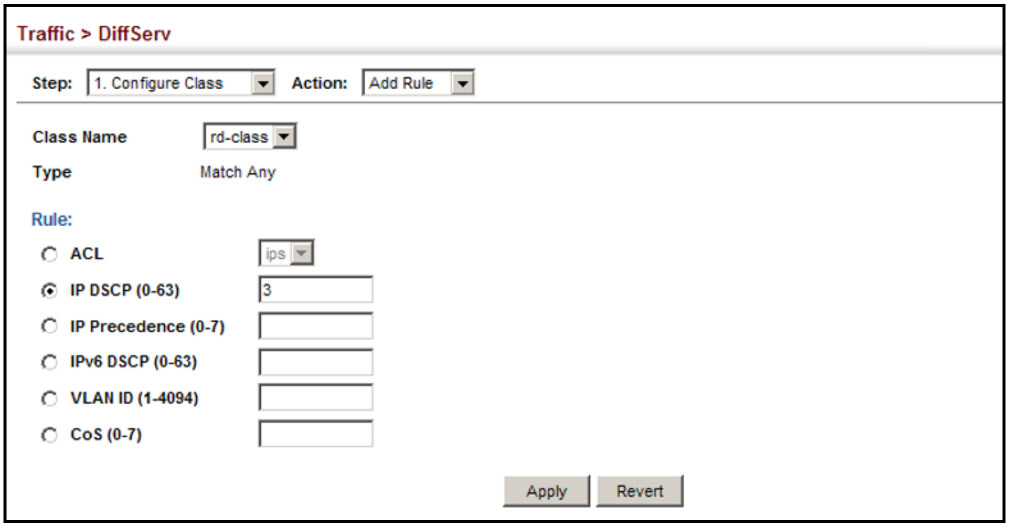
3. Select Add Rule from the Action list.

4. Select the name of a class map.

5. Specify type of traffic for this class based on an access list, a DSCP or IP Precedence value, a VLAN, or a CoS value. You can specify up to 16 items to match when assigning ingress traffic to a class map.

6. Click Apply.

Figure 152: Adding Rules to a Class Map



Traffic > DiffServ

Step: 1. Configure Class   Action: Add Rule

Class Name: rd-class

Type: Match Any

Rule:

- ○ ACL: ips
- ● IP DSCP (0-63): 3
- ○ IP Precedence (0-7):
- ○ IPv6 DSCP (0-63):
- ○ VLAN ID (1-4094):
- ○ CoS (0-7):

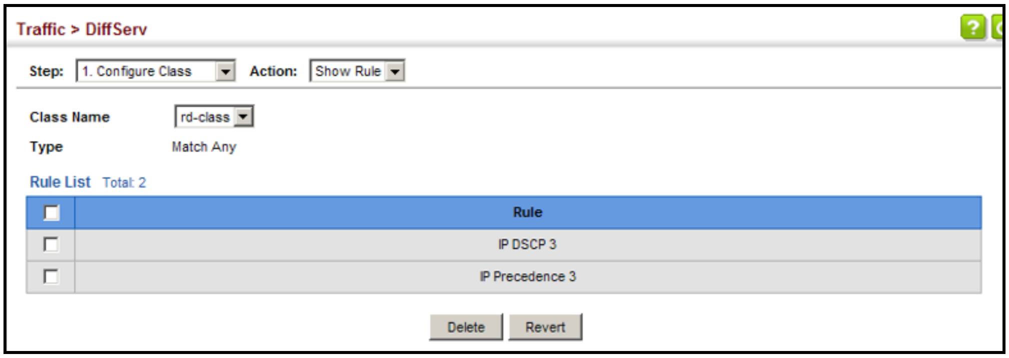
To show the rules for a class map:

1. Click Traffic, DiffServ.

2. Select Configure Class from the Step list.

3. Select Show Rule from the Action list.

Figure 153: Showing the Rules for a Class Map



Traffic > DiffServ

Step: 1. Configure Class Action: Show Rule

Class Name rd-class

Type Match Any

Rule List Total: 2

□	Rule
□	IP DSCP 3
□	IP Precedence 3

CREATING QOS POLICIES

Use the Traffic > DiffServ (Configure Policy) page to create a policy map that can be attached to multiple interfaces. A policy map is used to group one or more class map statements (page 326), modify service tagging, and enforce bandwidth policing. A policy map can then be bound by a service policy to one or more interfaces (page 339).

Configuring QoS policies requires several steps. A class map must first be configured which indicates how to match the inbound packets according to an access list, a DSCP or IP Precedence value, or a member of specific VLAN. A policy map is then configured which indicates the boundary parameters used for monitoring inbound traffic, and the action to take for conforming and non-conforming traffic. A policy map may contain one or more classes based on previously defined class maps.

The class of service or per-hop behavior (i.e., the priority used for internal queue processing) can be assigned to matching packets. In addition, the flow rate of inbound traffic can be monitored and the response to conforming and non-conforming traffic based by one of three distinct policing methods as described below.

Police Flow Meter – Defines the committed information rate (maximum throughput), committed burst size (burst rate), and the action to take for conforming and non-conforming traffic.

Policing is based on a token bucket, where bucket depth (that is, the maximum burst before the bucket overflows) is specified by the "burst" field (BC), and the average rate tokens are removed from the bucket is specified by the "rate" option (CIR). Action may be taken for traffic conforming to the maximum throughput, or exceeding the maximum throughput.

srTCM Police Meter – Defines an enforcer for classified traffic based on a single rate three color meter scheme defined in RFC 2697. This metering policy monitors a traffic stream and processes its packets according to the committed information rate (CIR, or maximum throughput), committed burst size (BC, or burst rate), and excess burst size (BE). Action may taken for traffic conforming to the maximum throughput, exceeding the maximum throughput, or exceeding the excess burst size.

- The PHB label is composed of five bits, three bits for per-hop behavior, and two bits for the color scheme used to control queue congestion. In addition to the actions defined by this command to transmit, remark the DSCP service value, or drop a packet, the switch will also mark the two color bits used to set the drop precedence of a packet. A packet is marked green if it doesn't exceed the committed information rate and committed burst size, yellow if it does exceed the committed information rate and committed burst size, but not the excess burst size, and red otherwise.

- The meter operates in one of two modes. In the color-blind mode, the meter assumes that the packet stream is uncolored. In color-aware mode the meter assumes that some preceding entity has pre-colored the incoming packet stream so that each packet is either green, yellow, or red. The marker (re)colors an IP packet according to the results of the meter. The color is coded in the DS field [RFC 2474] of the packet.

- The behavior of the meter is specified in terms of its mode and two token buckets, C and E, which both share the common rate CIR. The maximum size of the token bucket C is BC and the maximum size of the token bucket E is BE.

  The token buckets C and E are initially full, that is, the token count Tc(0) = BC and the token count Te(0) = BE. Thereafter, the token counts Tc and Te are updated CIR times per second as follows:

  - If Tc is less than BC, Tc is incremented by one, else
  - if Te is less then BE, Te is incremented by one, else
  - neither Tc nor Te is incremented.

  When a packet of size B bytes arrives at time t, the following happens if srTCM is configured to operate in Color-Blind mode:

  - If $Tc(t)-B \geq 0$, the packet is green and Tc is decremented by B down to the minimum value of 0, else
  - if $Te(t)-B \geq 0$, the packets is yellow and Te is decremented by B down to the minimum value of 0,
  - else the packet is red and neither Tc nor Te is decremented.

When a packet of size B bytes arrives at time t, the following happens if srTCM is configured to operate in Color-Aware mode:

- If the packet has been precolored as green and Tc(t)-B ≥ 0, the packet is green and Tc is decremented by B down to the minimum value of 0, else
- If the packet has been precolored as yellow or green and if Te(t)-B ≥ 0, the packets is yellow and Te is decremented by B down to the minimum value of 0, else
- the packet is red and neither Tc nor Te is decremented.

The metering policy guarantees a deterministic behavior where the volume of green packets is never smaller than what has been determined by the CIR and BC, that is, tokens of a given color are always spent on packets of that color. Refer to RFC 2697 for more information on other aspects of srTCM.

trTCM Police Meter – Defines an enforcer for classified traffic based on a two rate three color meter scheme defined in RFC 2698. This metering policy monitors a traffic stream and processes its packets according to the committed information rate (CIR, or maximum throughput), peak information rate (PIR), and their associated burst sizes – committed burst size (BC, or burst rate), and peak burst size (BP). Action may taken for traffic conforming to the maximum throughput, exceeding the maximum throughput, or exceeding the peak burst size.

- ◆ The PHB label is composed of five bits, three bits for per-hop behavior, and two bits for the color scheme used to control queue congestion. In addition to the actions defined by this command to transmit, remark the DSCP service value, or drop a packet, the switch will also mark the two color bits used to set the drop precedence of a packet. A packet is marked red if it exceeds the PIR. Otherwise it is marked either yellow or green depending on whether it exceeds or doesn't exceed the CIR.

  The trTCM is useful for ingress policing of a service, where a peak rate needs to be enforced separately from a committed rate.

- ◆ The meter operates in one of two modes. In the color-blind mode, the meter assumes that the packet stream is uncolored. In color-aware mode the meter assumes that some preceding entity has pre-colored the incoming packet stream so that each packet is either green, yellow, or red. The marker (re)colors an IP packet according to the results of the meter. The color is coded in the DS field [RFC 2474] of the packet.

- ◆ The behavior of the meter is specified in terms of its mode and two token buckets, P and C, which are based on the rates PIR and CIR, respectively. The maximum size of the token bucket P is BP and the maximum size of the token bucket C is BC.

  The token buckets P and C are initially (at time 0) full, that is, the token count Tp(0) = BP and the token count Tc(0) = BC. Thereafter, the token count Tp is incremented by one PIR times per second up to BP and the token count Tc is incremented by one CIR times per second up to BC.

When a packet of size B bytes arrives at time t, the following happens if trTCM is configured to operate in Color-Blind mode:

- If Tp(t)-B < 0, the packet is red, else
- if Tc(t)-B < 0, the packet is yellow and Tp is decremented by B, else
- the packet is green and both Tp and Tc are decremented by B.

When a packet of size B bytes arrives at time t, the following happens if trTCM is configured to operate in Color-Aware mode:

- If the packet has been precolored as red or if Tp(t)-B < 0, the packet is red, else
- if the packet has been precolored as yellow or if Tc(t)-B < 0, the packet is yellow and Tp is decremented by B, else
- the packet is green and both Tp and Tc are decremented by B.

- The trTCM can be used to mark a IP packet stream in a service, where different, decreasing levels of assurances (either absolute or relative) are given to packets which are green, yellow, or red. Refer to RFC 2698 for more information on other aspects of trTCM.

CLI REFERENCES

- "Quality of Service Commands" on page 1407

COMMAND USAGE

- A policy map can contain 1024 class statements that can be applied to the same interface (page 339). Up to 32 policy maps can be configured for ingress ports.
- After using the policy map to define packet classification, service tagging, and bandwidth policing, it must be assigned to a specific interface by a service policy (page 339) to take effect.

PARAMETERS

These parameters are displayed:

Add

- **Policy Name** – Name of policy map. (Range: 1-32 characters)
- **Description** – A brief description of a policy map. (Range: 1-256 characters)

Add Rule

- **Policy Name** – Name of policy map.

- **Class Name** – Name of a class map that defines a traffic classification upon which a policy can act.

- **Action** – This attribute is used to set an internal QoS value in hardware for matching packets. The PHB label is composed of five bits, three bits for per-hop behavior, and two bits for the color scheme used to control queue congestion with the srTCM and trTCM metering functions.

  - **Set CoS** – Configures the service provided to ingress traffic by setting an internal CoS value for a matching packet (as specified in rule settings for a class map). (Range: 0-7)

    See Table 18, "Default Mapping of CoS/CFI to Internal PHB/Drop Precedence," on page 317).

  - **Set PHB** – Configures the service provided to ingress traffic by setting the internal per-hop behavior for a matching packet (as specified in rule settings for a class map). (Range: 0-7)

    See Table 18, "Default Mapping of CoS/CFI to Internal PHB/Drop Precedence," on page 317).

- **Meter** – Check this to define the maximum throughput, burst rate, and the action that results from a policy violation.

- **Meter Mode** – Selects one of the following policing methods.

  - **Flow** (Police Flow) – Defines the committed information rate (CIR, or maximum throughput), committed burst size (BC, or burst rate), and the action to take for conforming and non-conforming traffic. Policing is based on a token bucket, where bucket depth (that is, the maximum burst before the bucket overflows) is specified by the "burst" field, and the average rate tokens are removed from the bucket is by specified by the "rate" option.

    - **Committed Information Rate** (CIR) – Rate in kilobits per second. (Range: 0-10000000 kbps or maximum port speed, whichever is lower)

      The rate cannot exceed the configured interface speed.

    - **Committed Burst Size** (BC) – Burst in bytes. (Range: 0-524288 bytes)

      The burst size cannot exceed 16 Mbytes.

    - **Conform** – Specifies that traffic conforming to the maximum rate (CIR) will be transmitted without any change to the DSCP service level.

      - **Transmit** – Transmits in-conformance traffic without any change to the DSCP service level.

    - **Violate** – Specifies whether the traffic that exceeds the maximum rate (CIR) will be dropped or the DSCP service level will be reduced.

- **Set IP DSCP** – Decreases DSCP priority for out of conformance traffic. (Range: 0-63)
- **Drop** – Drops out of conformance traffic.

- **srTCM** (Police Meter) – Defines the committed information rate (CIR, or maximum throughput), committed burst size (BC, or burst rate) and excess burst size (BE), and the action to take for traffic conforming to the maximum throughput, exceeding the maximum throughput but within the excess burst size, or exceeding the excess burst size. In addition to the actions defined by this command to transmit, remark the DSCP service value, or drop a packet, the switch will also mark the two color bits used to set the drop precedence of a packet.

  The color modes include "Color-Blind" which assumes that the packet stream is uncolored, and "Color-Aware" which assumes that the incoming packets are pre-colored. The functional differences between these modes is described at the beginning of this section under "srTCM Police Meter."

  - **Committed Information Rate** (CIR) – Rate in kilobits per second. (Range: 0-10000000 kbps or maximum port speed, whichever is lower)

    The rate cannot exceed the configured interface speed.

  - **Committed Burst Size** (BC) – Burst in bytes. (Range: 0-524288 bytes)

    The burst size cannot exceed 16 Mbytes.

  - **Excess Burst Size** (BE) – Burst in excess of committed burst size. (Range: 0-524288 bytes)

    The burst size cannot exceed 16 Mbytes.

  - **Conform** – Specifies that traffic conforming to the maximum rate (CIR) will be transmitted without any change to the DSCP service level.

    - **Transmit** – Transmits in-conformance traffic without any change to the DSCP service level.

  - **Exceed** – Specifies whether traffic that exceeds the maximum rate (CIR) but is within the excess burst size (BE) will be dropped or the DSCP service level will be reduced.

    - **Set IP DSCP** – Decreases DSCP priority for out of conformance traffic. (Range: 0-63)
    - **Drop** – Drops out of conformance traffic.

  - **Violate** – Specifies whether the traffic that exceeds the excess burst size (BE) will be dropped or the DSCP service level will be reduced.

    - **Set IP DSCP** – Decreases DSCP priority for out of conformance traffic. (Range: 0-63)

    - **Drop** – Drops out of conformance traffic.

- **trTCM** (Police Meter) – Defines the committed information rate (CIR, or maximum throughput), peak information rate (PIR), and their associated burst sizes – committed burst size (BC, or burst rate) and peak burst size (BP), and the action to take for traffic conforming to the maximum throughput, exceeding the maximum throughput but within the peak information rate, or exceeding the peak information rate. In addition to the actions defined by this command to transmit, remark the DSCP service value, or drop a packet, the switch will also mark the two color bits used to set the drop precedence of a packet.

  The color modes include "Color-Blind" which assumes that the packet stream is uncolored, and "Color-Aware" which assumes that the incoming packets are pre-colored. The functional differences between these modes is described at the beginning of this section under "trTCM Police Meter."

  - **Committed Information Rate** (CIR) – Rate in kilobits per second. (Range: 0-10000000 kbps or maximum port speed, whichever is lower)

    The rate cannot exceed the configured interface speed.

  - **Committed Burst Size** (BC) – Burst in bytes. (Range: 0-524288 bytes)

    The burst size cannot exceed 16 Mbytes.

  - **Peak Information Rate** (PIR) – Rate in kilobits per second. (Range: 0-1000000 kbps or maximum port speed, whichever is lower)

    The rate cannot exceed the configured interface speed.

  - **Peak Burst Size** (BP) – Burst size in bytes. (Range: 0-524288 bytes)

    The burst size cannot exceed 16 Mbytes.

  - **Conform** – Specifies that traffic conforming to the maximum rate (CIR) will be transmitted without any change to the DSCP service level.

    - **Transmit** – Transmits in-conformance traffic without any change to the DSCP service level.

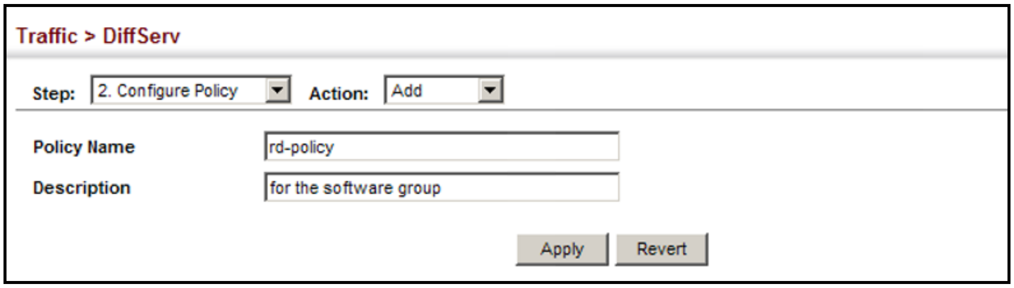
- **Exceed** – Specifies whether traffic that exceeds the maximum rate (CIR) but is within the peak information rate (PIR) will be dropped or the DSCP service level will be reduced.
  - **Set IP DSCP** – Decreases DSCP priority for out of conformance traffic. (Range: 0-63).
  - **Drop** – Drops out of conformance traffic.
- **Violate** – Specifies whether the traffic that exceeds the peak information rate (PIR) will be dropped or the DSCP service level will be reduced.
  - **Set IP DSCP** – Decreases DSCP priority for out of conformance traffic. (Range: 0-63).
  - **Drop** – Drops out of conformance traffic.

WEB INTERFACE

To configure a policy map:

1. Click Traffic, DiffServ.
2. Select Configure Policy from the Step list.
3. Select Add from the Action list.
4. Enter a policy name.
5. Enter a description.
6. Click Add.

Figure 154: Configuring a Policy Map



Traffic > DiffServ

Step: 2. Configure Policy Action: Add

Policy Name: rd-policy

Description: for the software group

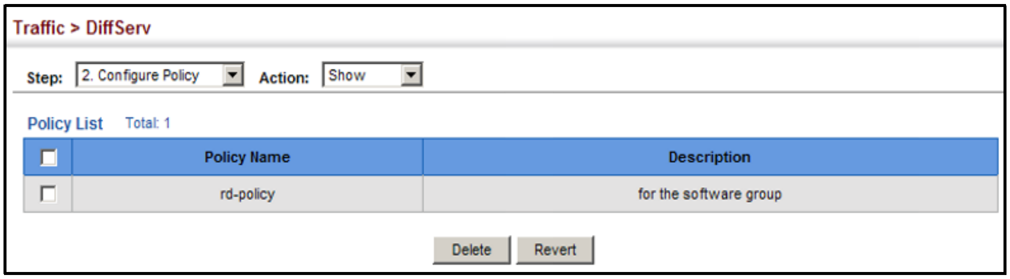
To show the configured policy maps:

1. Click Traffic, DiffServ.

2. Select Configure Policy from the Step list.

3. Select Show from the Action list.

Figure 155: Showing Policy Maps



Traffic > DiffServ

Step: 2. Configure Policy Action: Show

Policy List Total: 1

□	Policy Name	Description
□	rd-policy	for the software group

To edit the rules for a policy map:

1. Click Traffic, DiffServ.

2. Select Configure Policy from the Step list.

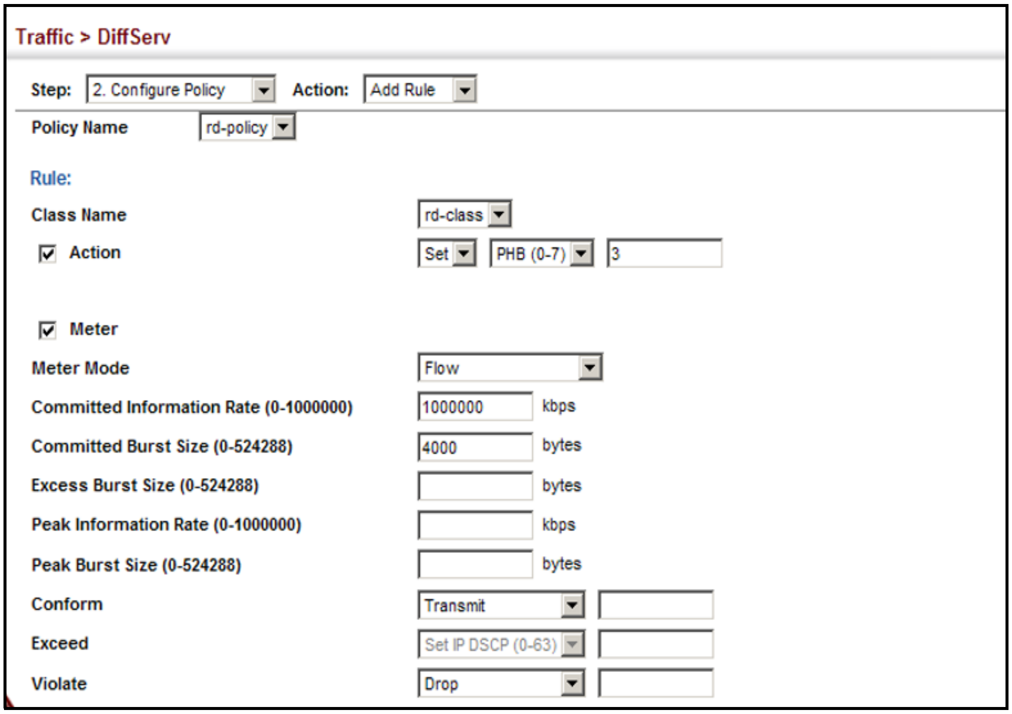
3. Select Add Rule from the Action list.

4. Select the name of a policy map.

5. Set the CoS or per-hop behavior for matching packets to specify the quality of service to be assigned to the matching traffic class. Use one of the metering options to define parameters such as the maximum throughput and burst rate. Then specify the action to take for conforming traffic, the action to tack for traffic in excess of the maximum rate but within the peak information rate, or the action to take for a policy violation.

6. Click Apply.

Figure 156: Adding Rules to a Policy Map



Traffic > DiffServ

Step: 2. Configure Policy Action: Add Rule

Policy Name rd-policy

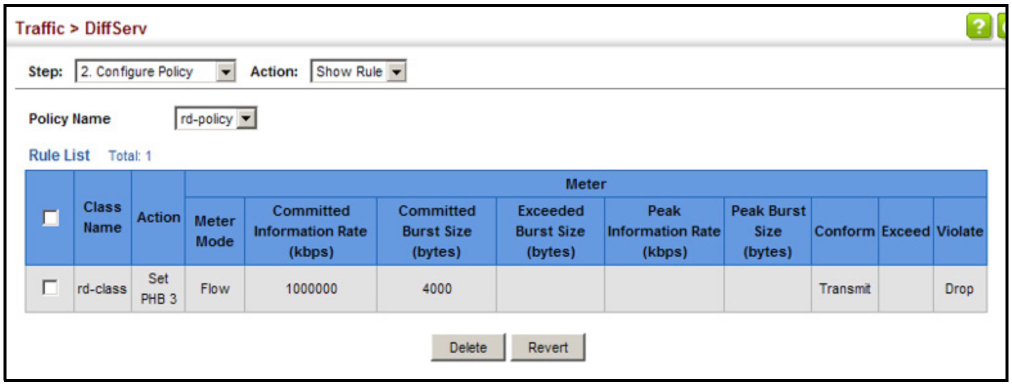
Rule:

Class Name	rd-class	
☑ Action	Set PHB (0-7) 3	
☑ Meter		
Meter Mode	Flow	
Committed Information Rate (0-1000000)	1000000	kbps
Committed Burst Size (0-524288)	4000	bytes
Excess Burst Size (0-524288)		bytes
Peak Information Rate (0-1000000)		kbps
Peak Burst Size (0-524288)		bytes
Conform	Transmit	
Exceed	Set IP DSCP (0-63)	
Violate	Drop	

To show the rules for a policy map:

1. Click Traffic, DiffServ.
2. Select Configure Policy from the Step list.
3. Select Show Rule from the Action list.

Figure 157: Showing the Rules for a Policy Map



Traffic > DiffServ

Step: 2. Configure Policy Action: Show Rule

Policy Name rd-policy

Rule List Total: 1

□	Class Name	Action	Meter								
			Meter Mode	Committed Information Rate (kbps)	Committed Burst Size (bytes)	Exceeded Burst Size (bytes)	Peak Information Rate (kbps)	Peak Burst Size (bytes)	Conform	Exceed	Violate
□	rd-class	Set PHB 3	Flow	1000000	4000				Transmit		Drop

ATTACHING A POLICY MAP TO A PORT

Use the Traffic > DiffServ (Configure Interface) page to bind a policy map to a port.

CLI REFERENCES

- "Quality of Service Commands" on page 1407

COMMAND USAGE

- First define a class map, define a policy map, and then bind the service policy to the required interface.

PARAMETERS

These parameters are displayed:

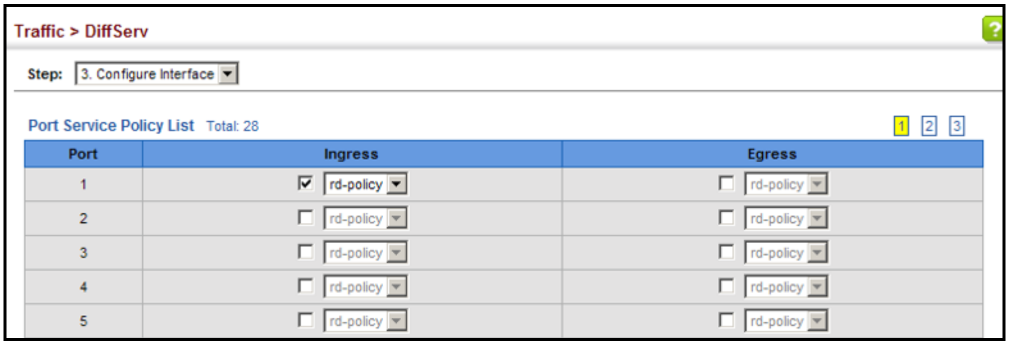
- **Port** – Specifies a port.
- **Ingress** – Applies the selected rule to ingress traffic.
- **Egress** – Applies the selected rule to egress traffic.

WEB INTERFACE

To bind a policy map to a port:

1. Click Traffic, DiffServ.
2. Select Configure Interface from the Step list.
3. Check the box under the Ingress or Egress field to enable a policy map for a port.
4. Select a policy map from the scroll-down box.
5. Click Apply.

Figure 158: Attaching a Policy Map to a Port



Traffic > DiffServ

Step: 3. Configure Interface

Port Service Policy List Total: 28

Port	Ingress	Egress
1	☑ rd-policy	☐ rd-policy
2	☐ rd-policy	☐ rd-policy
3	☐ rd-policy	☐ rd-policy
4	☐ rd-policy	☐ rd-policy
5	☐ rd-policy	☐ rd-policy

12 VoIP Traffic Configuration

This chapter covers the following topics:

- Global Settings – Enables VOIP globally, sets the Voice VLAN, and the aging time for attached ports.
- Telephony OUI List – Configures the list of phones to be treated as VOIP devices based on the specified Organization Unit Identifier (OUI).
- Port Settings – Configures the way in which a port is added to the Voice VLAN, the filtering of non-VoIP packets, the method of detecting VoIP traffic, and the priority assigned to voice traffic.

Overview

When IP telephony is deployed in an enterprise network, it is recommended to isolate the Voice over IP (VoIP) network traffic from other data traffic. Traffic isolation can provide higher voice quality by preventing excessive packet delays, packet loss, and jitter. This is best achieved by assigning all VoIP traffic to a single Voice VLAN.

The use of a Voice VLAN has several advantages. It provides security by isolating the VoIP traffic from other data traffic. End-to-end QoS policies and high priority can be applied to VoIP VLAN traffic across the network, guaranteeing the bandwidth it needs. VLAN isolation also protects against disruptive broadcast and multicast traffic that can seriously affect voice quality.

The switch allows you to specify a Voice VLAN for the network and set a CoS priority for the VoIP traffic. The VoIP traffic can be detected on switch ports by using the source MAC address of packets, or by using LLDP (IEEE 802.1AB) to discover connected VoIP devices. When VoIP traffic is detected on a configured port, the switch automatically assigns the port as a tagged member the Voice VLAN. Alternatively, switch ports can be manually configured.

CONFIGURING VOIP TRAFFIC

Use the Traffic > VoIP (Configure Global) page to configure the switch for VoIP traffic. First enable automatic detection of VoIP devices attached to the switch ports, then set the Voice VLAN ID for the network. The Voice VLAN aging time can also be set to remove a port from the Voice VLAN when VoIP traffic is no longer received on the port.

CLI REFERENCES

- "Configuring Voice VLANs" on page 1379

COMMAND USAGE

All ports are set to VLAN hybrid mode by default. Prior to enabling VoIP for a port (by setting the VoIP mode to Auto or Manual as described below), first ensure that VLAN membership is not set to access mode (see "Adding Static Members to VLANs" on page 231).

PARAMETERS

These parameters are displayed:

- **Auto Detection Status** – Enables the automatic detection of VoIP traffic on switch ports. (Default: Disabled)
- **Voice VLAN** – Sets the Voice VLAN ID for the network. Only one Voice VLAN is supported and it must already be created on the switch. (Range: 1-4094)
- **Voice VLAN Aging Time** – The time after which a port is removed from the Voice VLAN when VoIP traffic is no longer received on the port. (Range: 5-43200 minutes; Default: 1440 minutes)

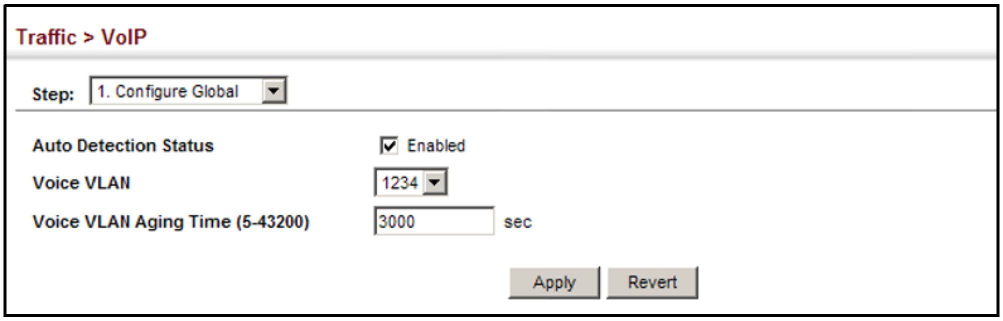
NOTE: The Voice VLAN ID cannot be modified when the global Auto Detection Status is enabled.

WEB INTERFACE

To configure global settings for a Voice VLAN:

1. Click Traffic, VoIP.
2. Select Configure Global from the Step list.
3. Enable Auto Detection.
4. Specify the Voice VLAN ID.
5. Adjust the Voice VLAN Aging Time if required.
6. Click Apply.

Figure 159: Configuring a Voice VLAN



Auto Detection Status ☑ Enabled

Voice VLAN 1234

Voice VLAN Aging Time (5-43200) 3000 sec

CONFIGURING TELEPHONY OUI

VoIP devices attached to the switch can be identified by the vendor's Organizational Unique Identifier (OUI) in the source MAC address of received packets. OUI numbers are assigned to vendors and form the first three octets of device MAC addresses. The MAC OUI numbers for VoIP equipment can be configured on the switch so that traffic from these devices is recognized as VoIP. Use the Traffic > VoIP (Configure OUI) page to configure this feature.

CLI REFERENCES

- "Configuring Voice VLANs" on page 1379

PARAMETERS

These parameters are displayed:

- **Telephony OUI** – Specifies a MAC address range to add to the list. Enter the MAC address in format 01-23-45-67-89-AB.
- **Mask** – Identifies a range of MAC addresses. Setting a mask of FF-FF-FF-00-00-00 identifies all devices with the same OUI (the first three octets). Other masks restrict the MAC address range. Setting FF-FF-FF-FF-FF-FF specifies a single MAC address. (Default: FF-FF-FF-00-00-00)
- **Description** – User-defined text that identifies the VoIP devices.

WEB INTERFACE

To configure MAC OUI numbers for VoIP equipment:

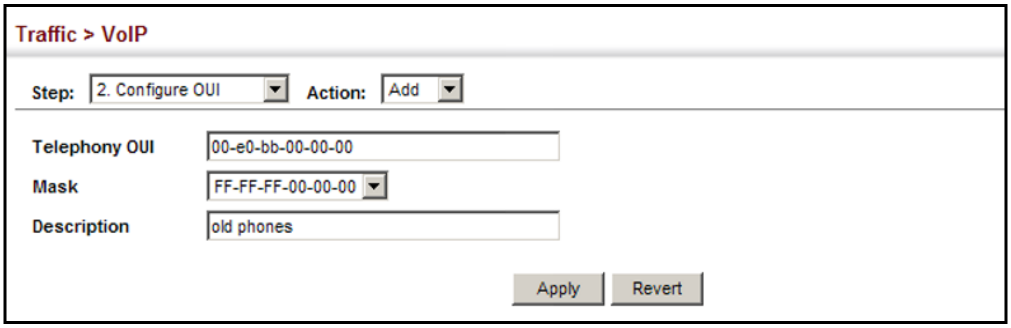
1. Click Traffic, VoIP.
2. Select Configure OUI from the Step list.
3. Select Add from the Action list.
4. Enter a MAC address that specifies the OUI for VoIP devices in the network.

5. Select a mask from the pull-down list to define a MAC address range.

6. Enter a description for the devices.

7. Click Apply.

Figure 160: Configuring an OUI Telephony List



Step: 2. Configure OUI Action: Add

Telephony OUI 00-e0-bb-00-00-00

Mask FF-FF-FF-00-00-00

Description old phones

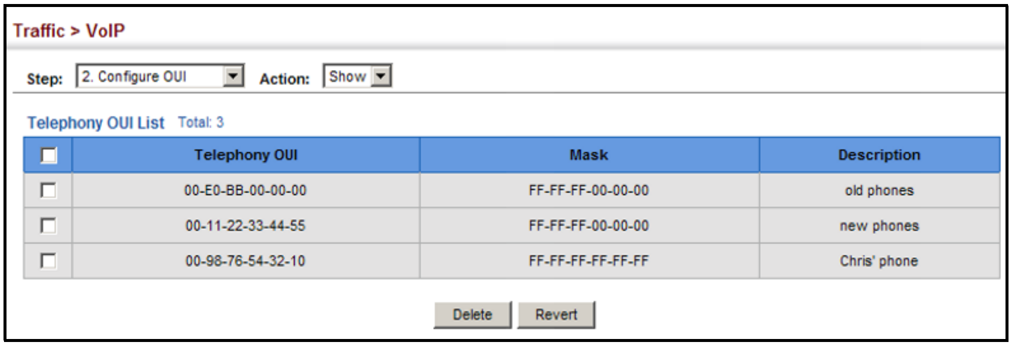
To show the MAC OUI numbers used for VoIP equipment:

1. Click Traffic, VoIP.

2. Select Configure OUI from the Step list.

3. Select Show from the Action list.

Figure 161: Showing an OUI Telephony List



Step: 2. Configure OUI Action: Show

Telephony OUI List Total: 3

□	Telephony OUI	Mask	Description
□	00-E0-BB-00-00-00	FF-FF-FF-00-00-00	old phones
□	00-11-22-33-44-55	FF-FF-FF-00-00-00	new phones
□	00-98-76-54-32-10	FF-FF-FF-FF-FF-FF	Chris' phone

CONFIGURING VOIP TRAFFIC PORTS

Use the Traffic > VoIP (Configure Interface) page to configure ports for VoIP traffic, you need to set the mode (Auto or Manual), specify the discovery method to use, and set the traffic priority. You can also enable security filtering to ensure that only VoIP traffic is forwarded on the Voice VLAN.

CLI REFERENCES

- "Configuring Voice VLANs" on page 1379

COMMAND USAGE

All ports are set to VLAN hybrid mode by default. Prior to enabling VoIP for a port (by setting the VoIP mode to Auto or Manual as described below), first ensure that VLAN membership is not set to access mode (see "Adding Static Members to VLANs" on page 231).

PARAMETERS

These parameters are displayed:

- **Mode** – Specifies if the port will be added to the Voice VLAN when VoIP traffic is detected. (Default: None)

  - **None** – The Voice VLAN feature is disabled on the port. The port will not detect VoIP traffic or be added to the Voice VLAN.

  - **Auto** – The port will be added as a tagged member to the Voice VLAN when VoIP traffic is detected on the port. You must select a method for detecting VoIP traffic, either OUI or 802.1ab (LLDP). When OUI is selected, be sure to configure the MAC address ranges in the Telephony OUI list.

  - **Manual** – The Voice VLAN feature is enabled on the port, but the port must be manually added to the Voice VLAN.

- **Security** – Enables security filtering that discards any non-VoIP packets received on the port that are tagged with the voice VLAN ID. VoIP traffic is identified by source MAC addresses configured in the Telephony OUI list, or through LLDP that discovers VoIP devices attached to the switch. Packets received from non-VoIP sources are dropped. (Default: Disabled)

- **Discovery Protocol** – Selects a method to use for detecting VoIP traffic on the port. (Default: OUI)

  - **OUI** – Traffic from VoIP devices is detected by the Organizationally Unique Identifier (OUI) of the source MAC address. OUI numbers are assigned to vendors and form the first three octets of a device MAC address. MAC address OUI numbers must be configured in the Telephony OUI list so that the switch recognizes the traffic as being from a VoIP device.

- **LLDP** – Uses LLDP (IEEE 802.1AB) to discover VoIP devices attached to the port. LLDP checks that the "telephone bit" in the system capability TLV is turned on. See "Link Layer Discovery Protocol" on page 458 for more information on LLDP.

- **Priority** – Defines a CoS priority for port traffic on the Voice VLAN. The priority of any received VoIP packet is overwritten with the new priority when the Voice VLAN feature is active for the port. (Range: 0-6; Default: 6)

- **Remaining Age** – Number of minutes before this entry is aged out.

  The Remaining Age starts to count down when the OUI's MAC address expires from the MAC address table. Therefore, the MAC address aging time should be added to the overall aging time. For example, if you configure the MAC address table aging time to 30 seconds, and the voice VLAN aging time to 5 minutes, then after 5.5 minutes, a port will be removed from voice VLAN when VoIP traffic is no longer received on the port. Alternatively, if you clear the MAC address table manually, then the switch will also start counting down the Remaining Age.

WEB INTERFACE

To configure VoIP traffic settings for a port:

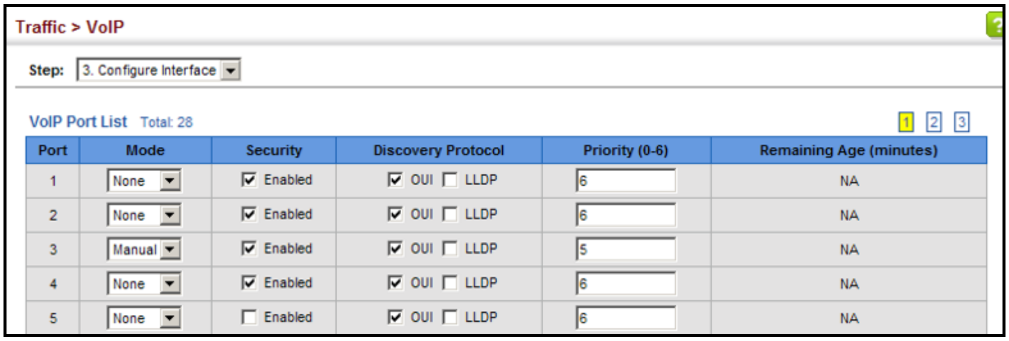
1. Click Traffic, VoIP.

2. Select Configure Interface from the Step list.

3. Configure any required changes to the VoIP settings each port.

4. Click Apply.

Figure 162: Configuring Port Settings for a Voice VLAN



Traffic > VoIP

Step: 3. Configure Interface

VoIP Port List Total: 28

Port	Mode	Security	Discovery Protocol	Priority (0-6)	Remaining Age (minutes)
1	None	☑ Enabled	☑ OUI ☐ LLDP	6	NA
2	None	☑ Enabled	☑ OUI ☐ LLDP	6	NA
3	Manual	☑ Enabled	☑ OUI ☐ LLDP	5	NA
4	None	☑ Enabled	☑ OUI ☐ LLDP	6	NA
5	None	☐ Enabled	☑ OUI ☐ LLDP	6	NA

13 Security Measures

You can configure this switch to authenticate users logging into the system for management access using local or remote authentication methods. Port-based authentication using IEEE 802.1X can also be configured to control either management access to the uplink ports or client access to the data ports. This switch provides secure network management access using the following options:

- AAA – Use local or remote authentication to configure access rights, specify authentication servers, configure remote authentication and accounting.
- User Accounts – Manually configure access rights on the switch for specified users.
- Web Authentication – Allows stations to authenticate and access the network in situations where 802.1X or Network Access authentication methods are infeasible or impractical.
- Network Access - Configure MAC authentication, intrusion response, dynamic VLAN assignment, and dynamic QoS assignment.
- HTTPS – Provide a secure web connection.
- SSH – Provide a secure shell (for secure Telnet access).
- ACL – Access Control Lists provide packet filtering for IP frames (based on address, protocol, Layer 4 protocol port number or TCP control code).
- ARP Inspection – Security feature that validates the MAC Address bindings for Address Resolution Protocol packets. Provides protection against ARP traffic with invalid MAC to IP Address bindings, which forms the basis for certain “man-in-the-middle” attacks.
- IP Filter – Filters management access to the web, SNMP or Telnet interface.
- Port Security – Configure secure addresses for individual ports.
- Port Authentication – Use IEEE 802.1X port authentication to control access to specific ports.
- DoS Protection – Protects against Denial-of-Service attacks.

- IPv4 Source Guard – Filters IPv4 traffic on insecure ports for which the source address cannot be identified via DHCPv4 snooping nor static source bindings.
- IPv6 Source Guard – Filters IPv6 traffic on insecure ports for which the source address cannot be identified via ND snooping, DHCPv6 snooping, nor static source bindings.
- DHCP Snooping – Filter IP traffic on insecure ports for which the source address cannot be identified via DHCP snooping.

NOTE: The priority of execution for the filtering commands is Port Security, Port Authentication, Network Access, Web Authentication, Access Control Lists, IP Source Guard, and then DHCP Snooping.

AAA AUTHORIZATION AND ACCOUNTING

The authentication, authorization, and accounting (AAA) feature provides the main framework for configuring access control on the switch. The three security functions can be summarized as follows:

- Authentication — Identifies users that request access to the network.
- Authorization — Determines if users can access specific services.
- Accounting — Provides reports, auditing, and billing for services that users have accessed on the network.

The AAA functions require the use of configured RADIUS or TACACS+ servers in the network. The security servers can be defined as sequential groups that are applied as a method for controlling user access to specified services. For example, when the switch attempts to authenticate a user, a request is sent to the first server in the defined group, if there is no response the second server will be tried, and so on. If at any point a pass or fail is returned, the process stops.

The switch supports the following AAA features:

- Accounting for IEEE 802.1X authenticated users that access the network through the switch.
- Accounting for users that access management interfaces on the switch through the console and Telnet.
- Accounting for commands that users enter at specific CLI privilege levels.
- Authorization of users that access management interfaces on the switch through the console and Telnet.

To configure AAA on the switch, you need to follow this general process:

1. Configure RADIUS and TACACS+ server access parameters. See "Configuring Local/Remote Logon Authentication" on page 349.
2. Define RADIUS and TACACS+ server groups to support the accounting and authorization of services.
3. Define a method name for each service to which you want to apply accounting or authorization and specify the RADIUS or TACACS+ server groups to use.
4. Apply the method names to port or line interfaces.

NOTE: This guide assumes that RADIUS and TACACS+ servers have already been configured to support AAA. The configuration of RADIUS and TACACS+ server software is beyond the scope of this guide, refer to the documentation provided with the RADIUS or TACACS+ server software.

CONFIGURING LOCAL/ REMOTE LOGON AUTHENTICATION

Use the Security > AAA > System Authentication page to specify local or remote authentication. Local authentication restricts management access based on user names and passwords manually configured on the switch. Remote authentication uses a remote access authentication server based on RADIUS or TACACS+ protocols to verify management access.

CLI REFERENCES

- "Authentication Sequence" on page 1034

COMMAND USAGE

- By default, management access is always checked against the authentication database stored on the local switch. If a remote authentication server is used, you must specify the authentication sequence. Then specify the corresponding parameters for the remote authentication protocol using the Security > AAA > Server page. Local and remote logon authentication control management access via the console port, web browser, or Telnet.

- You can specify up to three authentication methods for any user to indicate the authentication sequence. For example, if you select (1) RADIUS, (2) TACACS and (3) Local, the user name and password on the RADIUS server is verified first. If the RADIUS server is not available, then authentication is attempted using the TACACS+ server, and finally the local user name and password is checked.

PARAMETERS

These parameters are displayed:

- **Authentication Sequence** – Select the authentication, or authentication sequence required:

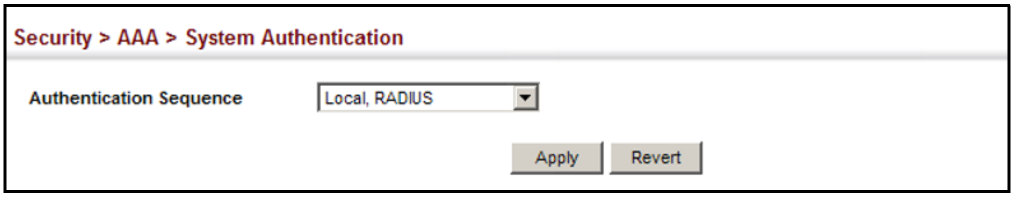
- **Local** – User authentication is performed only locally by the switch.
- **RADIUS** – User authentication is performed using a RADIUS server only.
- **TACACS** – User authentication is performed using a TACACS+ server only.
- [authentication sequence] – User authentication is performed by up to three authentication methods in the indicated sequence.

WEB INTERFACE

To configure the method(s) of controlling management access:

1. Click Security, AAA, System Authentication.
2. Specify the authentication sequence (i.e., one to three methods).
3. Click Apply.

Figure 163: Configuring the Authentication Sequence



Security > AAA > System Authentication

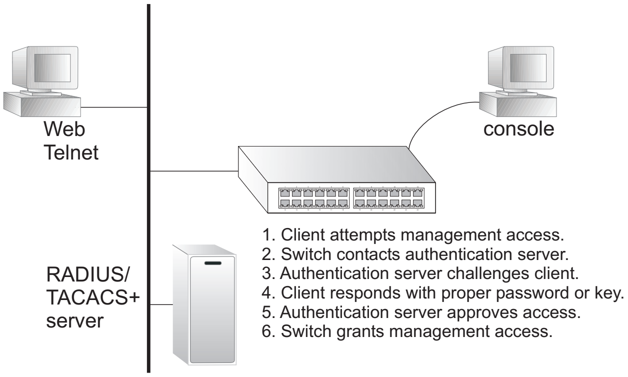
Authentication Sequence: Local, RADIUS

CONFIGURING REMOTE LOGON AUTHENTICATION SERVERS

Use the Security > AAA > Server page to configure the message exchange parameters for RADIUS or TACACS+ remote access authentication servers.

Remote Authentication Dial-in User Service (RADIUS) and Terminal Access Controller Access Control System Plus (TACACS+) are logon authentication protocols that use software running on a central server to control access to RADIUS-aware or TACACS-aware devices on the network. An authentication server contains a database of multiple user name/password pairs with associated privilege levels for each user that requires management access to the switch.

Figure 164: Authentication Server Operation



1. Client attempts management access.
2. Switch contacts authentication server.
3. Authentication server challenges client.
4. Client responds with proper password or key.
5. Authentication server approves access.
6. Switch grants management access.

RADIUS uses UDP while TACACS+ uses TCP. UDP only offers best effort delivery, while TCP offers a more reliable connection-oriented transport. Also, note that RADIUS encrypts only the password in the access-request packet from the client to the server, while TACACS+ encrypts the entire body of the packet.

CLI REFERENCES

- "RADIUS Client" on page 1036
- "TACACS+ Client" on page 1040
- "AAA" on page 1044

COMMAND USAGE

- If a remote authentication server is used, you must specify the message exchange parameters for the remote authentication protocol. Both local and remote logon authentication control management access via the console port, web browser, or Telnet.

- RADIUS and TACACS+ logon authentication assign a specific privilege level for each user name/password pair. The user name, password, and privilege level must be configured on the authentication server. The encryption methods used for the authentication process must also be configured or negotiated between the authentication server and logon client. This switch can pass authentication messages between the server and client that have been encrypted using MD5 (Message-Digest 5), TLS (Transport Layer Security), or TTLS (Tunneled Transport Layer Security).

PARAMETERS

These parameters are displayed:

Configure Server

- **RADIUS**

  - **Global** – Provides globally applicable RADIUS settings.

  - **Server Index** – Specifies one of five RADIUS servers that may be configured. The switch attempts authentication using the listed sequence of servers. The process ends when a server either approves or denies access to a user.

  - **Server IP Address** – Address of authentication server.
    (A Server Index entry must be selected to display this item.)

  - **Accounting Server UDP Port** – Network (UDP) port on authentication server used for accounting messages.
    (Range: 1-65535; Default: 1813)

  - **Authentication Server UDP Port** – Network (UDP) port on authentication server used for authentication messages.
    (Range: 1-65535; Default: 1812)

  - **Authentication Timeout** – The number of seconds the switch waits for a reply from the RADIUS server before it resends the request. (Range: 1-65535; Default: 5)
  - **Authentication Retries** – Number of times the switch tries to authenticate logon access via the authentication server. (Range: 1-30; Default: 2)
  - **Set Key** – Mark this box to set or modify the encryption key.
  - **Authentication Key** – Encryption key used to authenticate logon access for client. Do not use blank spaces in the string. (Maximum length: 48 characters)
  - **Confirm Authentication Key** – Re-type the string entered in the previous field to ensure no errors were made. The switch will not change the encryption key if these two fields do not match.

- **TACACS+**
  - **Global** – Provides globally applicable TACACS+ settings.
  - **Server Index** – Specifies the index number of the server to be configured. The switch currently supports only one TACACS+ server.
  - **Server IP Address** – Address of the TACACS+ server. (A Server Index entry must be selected to display this item.)
  - **Authentication Server TCP Port** – Network (TCP) port of TACACS+ server used for authentication messages. (Range: 1-65535; Default: 49)
  - **Authentication Timeout** – The number of seconds the switch waits for a reply from the RADIUS server before it resends the request. (Range: 1-65535; Default: 5)
  - **Authentication Retries** – Number of times the switch tries to authenticate logon access via the authentication server. (Range: 1-30; Default: 2)
  - **Set Key** – Mark this box to set or modify the encryption key.
  - **Authentication Key** – Encryption key used to authenticate logon access for client. Do not use blank spaces in the string. (Maximum length: 48 characters)
  - **Confirm Authentication Key** – Re-type the string entered in the previous field to ensure no errors were made. The switch will not change the encryption key if these two fields do not match.

Configure Group

- **Server Type** – Select RADIUS or TACACS+ server.
- **Group Name** - Defines a name for the RADIUS or TACACS+ server group. (Range: 1-64 characters)
- **Sequence at Priority** - Specifies the server and sequence to use for the group. (Range: 1-5 for RADIUS; 1 for TACACS)

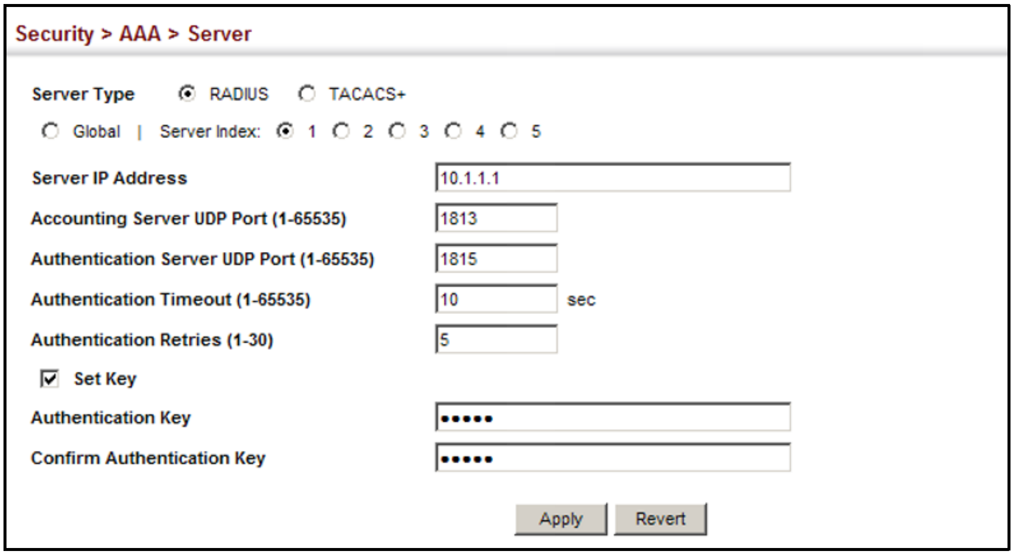
  When specifying the priority sequence for a sever, the server index must already be defined (see "Configuring Local/Remote Logon Authentication" on page 349).

WEB INTERFACE

To configure the parameters for RADIUS or TACACS+ authentication:

1. Click Security, AAA, Server.
2. Select Configure Server from the Step list.
3. Select RADIUS or TACACS+ server type.
4. Select Global to specify the parameters that apply globally to all specified servers, or select a specific Server Index to specify the parameters that apply to a specific server.
5. To set or modify the authentication key, mark the Set Key box, enter the key, and then confirm it
6. Click Apply.

Figure 165: Configuring Remote Authentication Server (RADIUS)



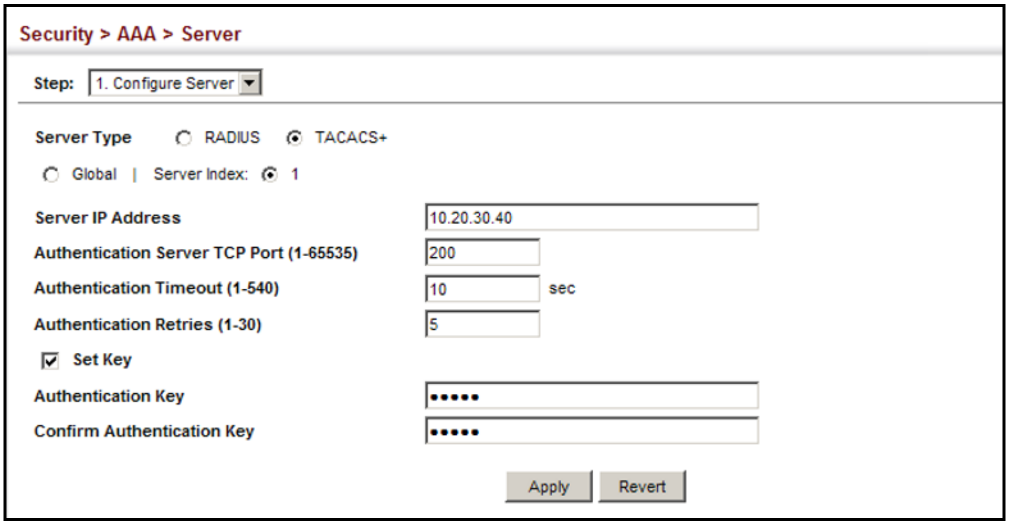
Security > AAA > Server

Server Type ● RADIUS ○ TACACS+

○ Global | Server Index: ● 1 ○ 2 ○ 3 ○ 4 ○ 5

Server IP Address	10.1.1.1
Accounting Server UDP Port (1-65535)	1813
Authentication Server UDP Port (1-65535)	1815
Authentication Timeout (1-65535)	10 sec
Authentication Retries (1-30)	5
☑ Set Key	
Authentication Key	•••••
Confirm Authentication Key	•••••

Figure 166: Configuring Remote Authentication Server (TACACS+)



Security > AAA > Server

Step: 1. Configure Server

Server Type ○ RADIUS ● TACACS+

○ Global | Server Index: ● 1

Server IP Address: 10.20.30.40

Authentication Server TCP Port (1-65535): 200

Authentication Timeout (1-540): 10 sec

Authentication Retries (1-30): 5

☑ Set Key

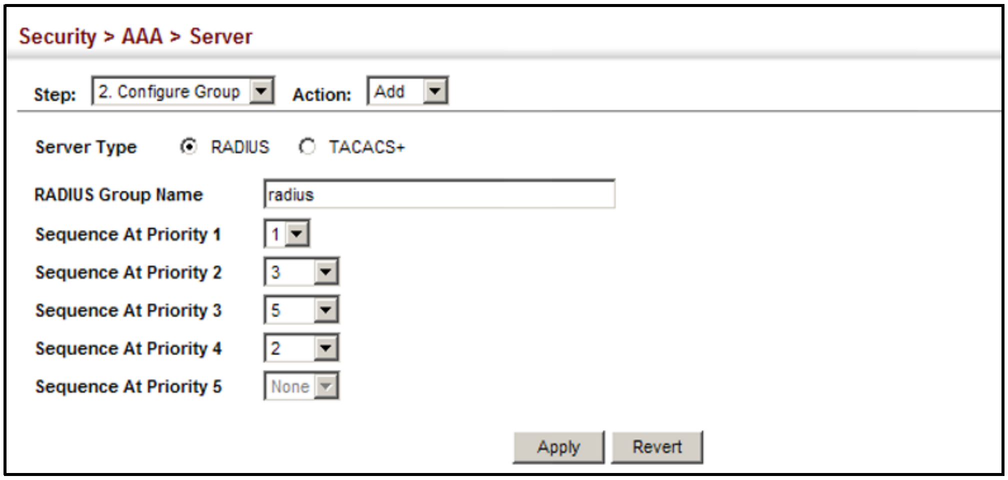
Authentication Key: •••••

Confirm Authentication Key: •••••

To configure the RADIUS or TACACS+ server groups to use for accounting and authorization:

1. Click Security, AAA, Server.
2. Select Configure Group from the Step list.
3. Select Add from the Action list.
4. Select RADIUS or TACACS+ server type.
5. Enter the group name, followed by the index of the server to use for each priority level.
6. Click Apply.

Figure 167: Configuring AAA Server Groups



Security > AAA > Server

Step: 2. Configure Group Action: Add

Server Type ● RADIUS ○ TACACS+

RADIUS Group Name: radius

Sequence At Priority 1: 1

Sequence At Priority 2: 3

Sequence At Priority 3: 5

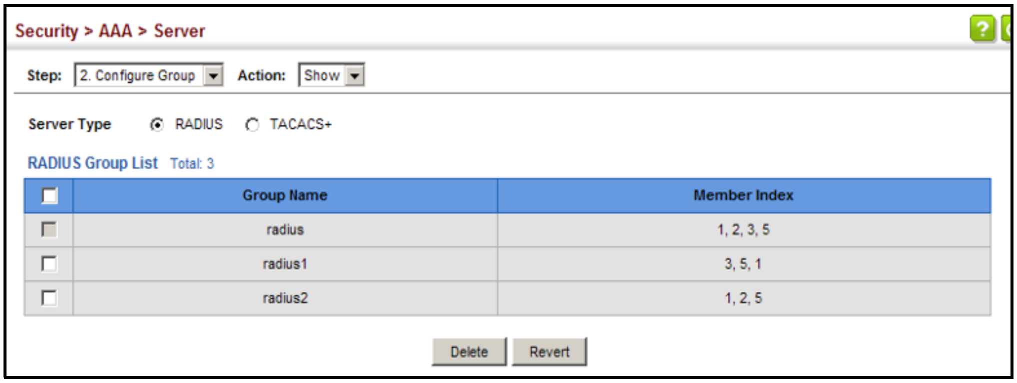
Sequence At Priority 4: 2

Sequence At Priority 5: None

To show the RADIUS or TACACS+ server groups used for accounting and authorization:

1. Click Security, AAA, Server.
2. Select Configure Group from the Step list.
3. Select Show from the Action list.

Figure 168: Showing AAA Server Groups



Security > AAA > Server

Step: 2. Configure Group Action: Show

Server Type ● RADIUS ○ TACACS+

RADIUS Group List Total: 3

□	Group Name	Member Index
□	radius	1, 2, 3, 5
□	radius1	3, 5, 1
□	radius2	1, 2, 5

CONFIGURING AAA ACCOUNTING

Use the Security > AAA > Accounting page to enable accounting of requested services for billing or security purposes, and also to display the configured accounting methods, the methods applied to specific interfaces, and basic accounting information recorded for user sessions.

CLI REFERENCES

- "AAA" on page 1044

COMMAND USAGE

AAA authentication through a RADIUS or TACACS+ server must be enabled before accounting is enabled.

PARAMETERS

These parameters are displayed:

Configure Global

- **Periodic Update** - Specifies the interval at which the local accounting service updates information for all users on the system to the accounting server. (Range: 1-2147483647 minutes)

Configure Method

- **Accounting Type** – Specifies the service as:
  - **802.1X** – Accounting for end users.
  - **Exec** – Administrative accounting for local console, Telnet, or SSH connections.

- **Method Name** – Specifies an accounting method for service requests. The "default" methods are used for a requested service if no other methods have been defined. (Range: 1-64 characters)

  Note that the method name is only used to describe the accounting method configured on the specified RADIUS or TACACS+ servers. No information is sent to the servers about the method to use.

- **Accounting Notice** – Records user activity from log-in to log-off point.

- **Server Group Name** - Specifies the accounting server group. (Range: 1-64 characters)

  The group names "radius" and "tacacs+" specifies all configured RADIUS and TACACS+ hosts (see "Configuring Local/Remote Logon Authentication" on page 349). Any other group name refers to a server group configured on the Security > AAA > Server (Configure Group) page.

Configure Service

- **Accounting Type** – Specifies the service as 802.1X, Command or Exec as described in the preceding section.

- **802.1X**

  - **Method Name** – Specifies a user defined accounting method to apply to an interface. This method must be defined in the Configure Method page. (Range: 1-64 characters)

- **Exec**

  - **Console Method Name** – Specifies a user defined method name to apply to console connections.

  - **VTY Method Name** – Specifies a user defined method name to apply to Telnet connections.

Show Information – Summary

- **Accounting Type** - Displays the accounting service.

- **Method Name** - Displays the user-defined or default accounting method.

- **Server Group Name** - Displays the accounting server group.

- **Interface** - Displays the port, console or Telnet interface to which these rules apply. (This field is null if the accounting method and associated server group has not been assigned to an interface.)

Show Information – Statistics

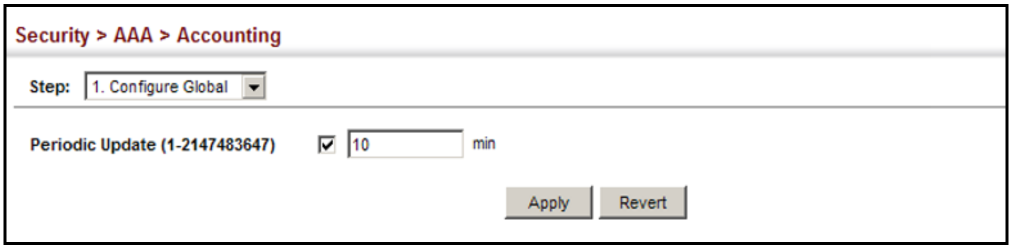
- **User Name** - Displays a registered user name.
- **Accounting Type** - Displays the accounting service.
- **Interface** - Displays the receive port number through which this user accessed the switch.
- **Time Elapsed** - Displays the length of time this entry has been active.

WEB INTERFACE

To configure global settings for AAA accounting:

1. Click Security, AAA, Accounting.
2. Select Configure Global from the Step list.
3. Enter the required update interval.
4. Click Apply.

Figure 169: Configuring Global Settings for AAA Accounting



Security > AAA > Accounting

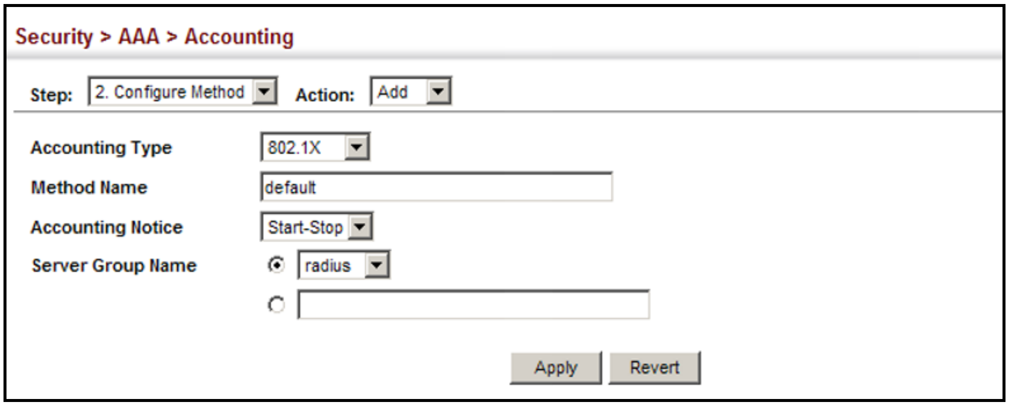
Step: 1. Configure Global

Periodic Update (1-2147483647) ☑ 10 min

To configure the accounting method applied to various service types and the assigned server group:

1. Click Security, AAA, Accounting.
2. Select Configure Method from the Step list.
3. Select Add from the Action list.
4. Select the accounting type (802.1X, Exec).
5. Specify the name of the accounting method and server group name.
6. Click Apply.

Figure 170: Configuring AAA Accounting Methods



Security > AAA > Accounting

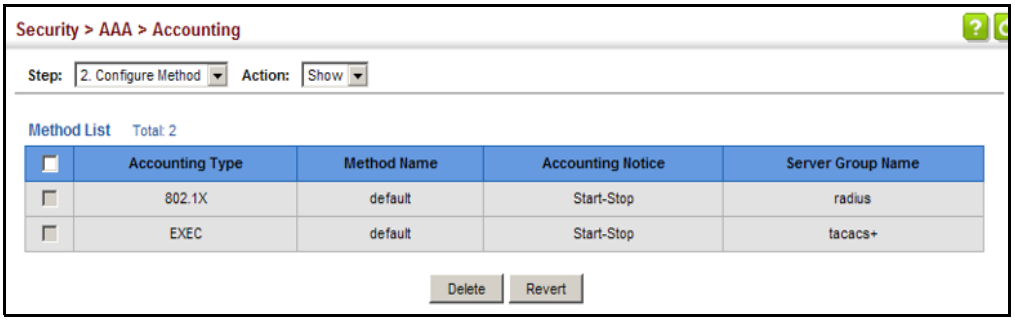
Step: 2. Configure Method Action: Add

Accounting Type	802.1X
Method Name	default
Accounting Notice	Start-Stop
Server Group Name	● radius ○

To show the accounting method applied to various service types and the assigned server group:

1. Click Security, AAA, Accounting.
2. Select Configure Method from the Step list.
3. Select Show from the Action list.

Figure 171: Showing AAA Accounting Methods



Security > AAA > Accounting

Step: 2. Configure Method Action: Show

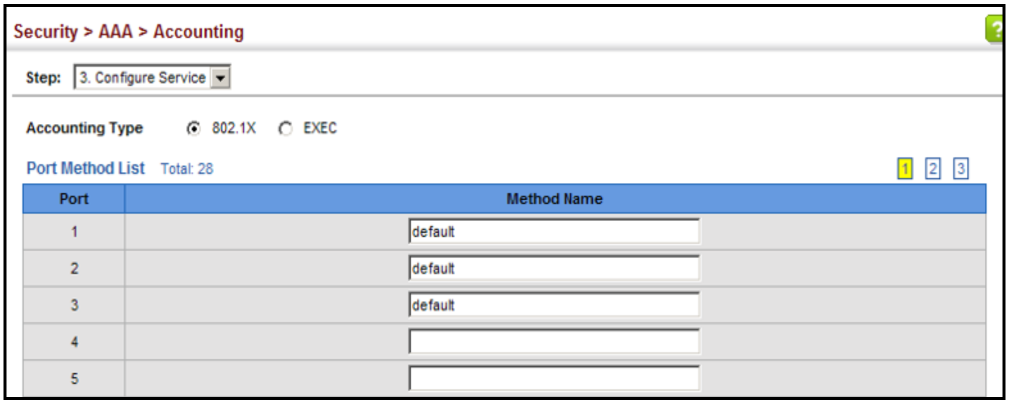
Method List Total: 2

□	Accounting Type	Method Name	Accounting Notice	Server Group Name
□	802.1X	default	Start-Stop	radius
□	EXEC	default	Start-Stop	tacacs+

To configure the accounting method applied to specific interfaces, console commands entered at specific privilege levels, and local console, Telnet, or SSH connections:

1. Click Security, AAA, Accounting.
2. Select Configure Service from the Step list.
3. Select the accounting type (802.1X, Exec).
4. Enter the required accounting method.
5. Click Apply.

Figure 172: Configuring AAA Accounting Service for 802.1X Service



Security > AAA > Accounting

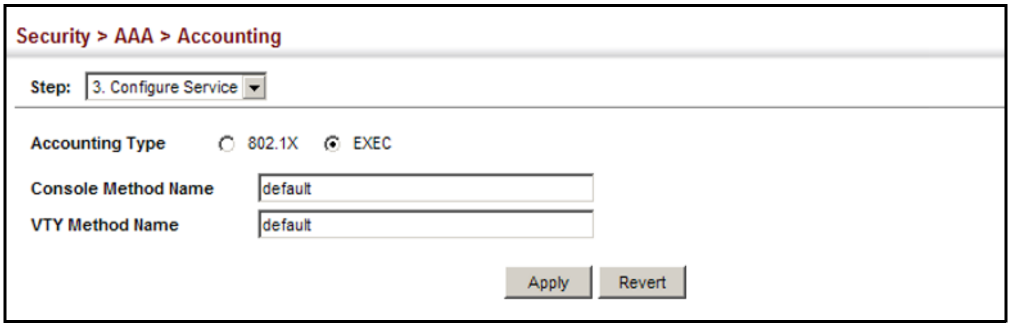
Step: 3. Configure Service

Accounting Type ● 802.1X ○ EXEC

Port Method List Total: 28

Port	Method Name
1	default
2	default
3	default
4	
5	

Figure 173: Configuring AAA Accounting Service for Exec Service



Security > AAA > Accounting

Step: 3. Configure Service

Accounting Type ○ 802.1X ● EXEC

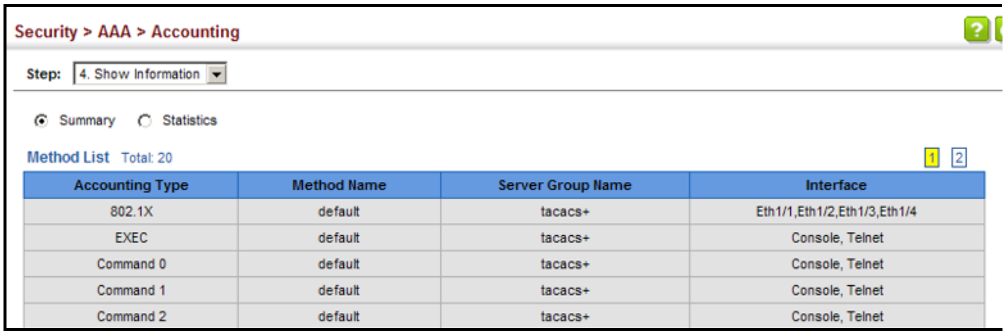
Console Method Name: default

VTY Method Name: default

To display a summary of the configured accounting methods and assigned server groups for specified service types:

1. Click Security, AAA, Accounting.
2. Select Show Information from the Step list.
3. Click Summary.

Figure 174: Displaying a Summary of Applied AAA Accounting Methods



Security > AAA > Accounting

Step: 4. Show Information

● Summary ○ Statistics

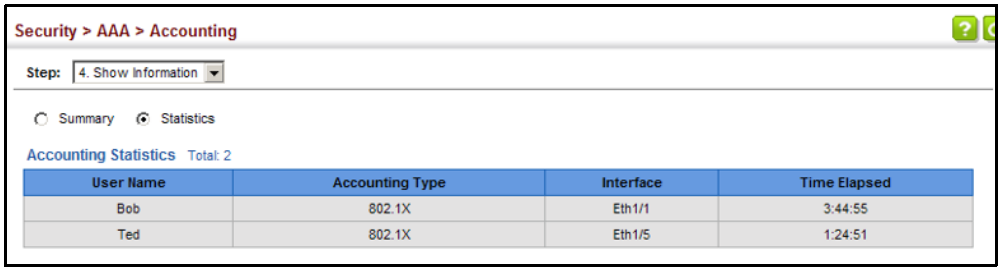
Method List Total: 20

Accounting Type	Method Name	Server Group Name	Interface
802.1X	default	tacacs+	Eth1/1,Eth1/2,Eth1/3,Eth1/4
EXEC	default	tacacs+	Console, Telnet
Command 0	default	tacacs+	Console, Telnet
Command 1	default	tacacs+	Console, Telnet
Command 2	default	tacacs+	Console, Telnet

To display basic accounting information and statistics recorded for user sessions:

1. Click Security, AAA, Accounting.
2. Select Show Information from the Step list.
3. Click Statistics.

Figure 175: Displaying Statistics for AAA Accounting Sessions



Security > AAA > Accounting

Step: 4. Show Information

○ Summary ● Statistics

Accounting Statistics Total: 2

User Name	Accounting Type	Interface	Time Elapsed
Bob	802.1X	Eth1/1	3:44:55
Ted	802.1X	Eth1/5	1:24:51

CONFIGURING AAA AUTHORIZATION

Use the Security > AAA > Authorization page to enable authorization of requested services, and also to display the configured authorization methods, and the methods applied to specific interfaces.

CLI REFERENCES

- "AAA" on page 1044

COMMAND USAGE

- This feature performs authorization to determine if a user is allowed to run an Exec shell.

- AAA authentication through a RADIUS or TACACS+ server must be enabled before authorization is enabled.

PARAMETERS

These parameters are displayed:

Configure Method

- **Authorization Type** – Specifies the service as Exec, indicating administrative authorization for local console, Telnet, or SSH connections.
- **Method Name** – Specifies an authorization method for service requests. The "default" method is used for a requested service if no other methods have been defined. (Range: 1-64 characters)
- **Server Group Name** - Specifies the authorization server group. (Range: 1-64 characters)

  The group name "tacacs+" specifies all configured TACACS+ hosts (see "Configuring Local/Remote Logon Authentication" on page 349). Any other group name refers to a server group configured on the TACACS+ Group Settings page. Authorization is only supported for TACACS+ servers.

Configure Service

- **Authorization Type** – Specifies the service as Exec, indicating administrative authorization for local console, Telnet, or SSH connections.
- **Console Method Name** – Specifies a user defined method name to apply to console connections.
- **VTY Method Name** – Specifies a user defined method name to apply to Telnet connections.

Show Information

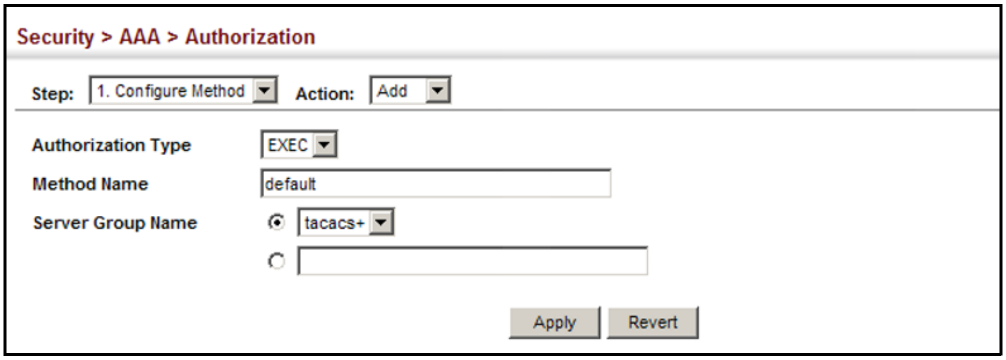
- **Authorization Type** - Displays the authorization service.
- **Method Name** - Displays the user-defined or default accounting method.
- **Server Group Name** - Displays the authorization server group.
- **Interface** - Displays the console or Telnet interface to which these rules apply. (This field is null if the authorization method and associated server group has not been assigned to an interface.)

WEB INTERFACE

To configure the authorization method applied to the Exec service type and the assigned server group:

1. Click Security, AAA, Authorization.
2. Select Configure Method from the Step list.
3. Specify the name of the authorization method and server group name.
4. Click Apply.

Figure 176: Configuring AAA Authorization Methods



Security > AAA > Authorization

Step: 1. Configure Method   Action: Add

Authorization Type: EXEC

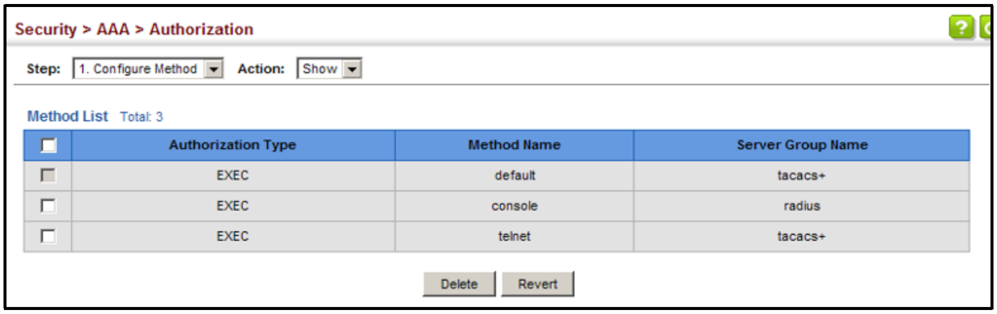
Method Name: default

Server Group Name: ● tacacs+
○

To show the authorization method applied to the EXEC service type and the assigned server group:

1. Click Security, AAA, Authorization.
2. Select Configure Method from the Step list.
3. Select Show from the Action list.

Figure 177: Showing AAA Authorization Methods



Security > AAA > Authorization

Step: 1. Configure Method   Action: Show

Method List Total: 3

□	Authorization Type	Method Name	Server Group Name
□	EXEC	default	tacacs+
□	EXEC	console	radius
□	EXEC	telnet	tacacs+

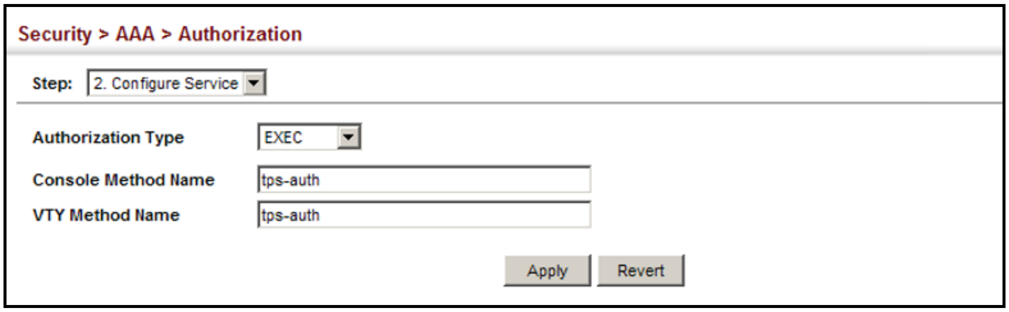
To configure the authorization method applied to local console, Telnet, or SSH connections:

1. Click Security, AAA, Authorization.
2. Select Configure Service from the Step list.

3. Enter the required authorization method.

4. Click Apply.

Figure 178: Configuring AAA Authorization Methods for Exec Service



Security > AAA > Authorization

Step: 2. Configure Service

Authorization Type: EXEC

Console Method Name: tps-auth

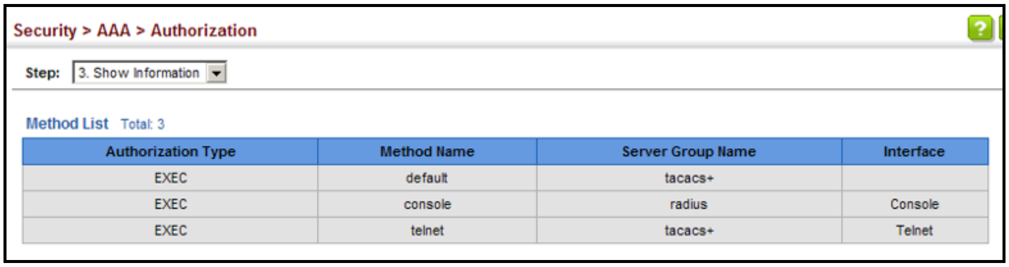
VTY Method Name: tps-auth

To display a the configured authorization method and assigned server groups for The Exec service type:

1. Click Security, AAA, Authorization.

2. Select Show Information from the Step list.

Figure 179: Displaying the Applied AAA Authorization Method



Security > AAA > Authorization

Step: 3. Show Information

Method List Total: 3

Authorization Type	Method Name	Server Group Name	Interface
EXEC	default	tacacs+	
EXEC	console	radius	Console
EXEC	telnet	tacacs+	Telnet

CONFIGURING USER ACCOUNTS

Use the Security > User Accounts page to control management access to the switch based on manually configured user names and passwords.

CLI REFERENCES

◆ "User Accounts" on page 1032

COMMAND USAGE

◆ The default guest name is “guest” with the password “guest.” The default administrator name is “admin” with the password “admin.”

◆ The guest only has read access for most configuration parameters. However, the administrator has write access for all parameters governing the onboard agent. You should therefore assign a new administrator password as soon as possible, and store it in a safe place.

PARAMETERS

These parameters are displayed:

- **User Name** – The name of the user.
  (Maximum length: 32 characters; maximum number of users: 16)

- **Access Level** – Specifies the user level. (Options: 0 - Normal, 15 - Privileged)

  The encrypted password is required for compatibility with legacy password settings (i.e., plain text or encrypted) when reading the configuration file during system bootup or when downloading the configuration file from a TFTP or FTP server. There is no need for you to manually configure encrypted passwords.

- **Password Type** – Specifies the following options:
  - **No Password** – No password is required for this user to log in.
  - **Plain Password** – Plain text unencrypted password.
  - **Encrypted Password** – Encrypted password.

    The encrypted password is required for compatibility with legacy password settings (i.e., plain text or encrypted) when reading the configuration file during system bootup. There is no need for you to manually configure encrypted passwords.

- **Password** – Specifies the user password.
  (Range: 0-32 characters, case sensitive)

- **Confirm Password** – Re-type the string entered in the previous field to ensure no errors were made. The switch will not change the password if these two fields do not match.

WEB INTERFACE

To configure user accounts:

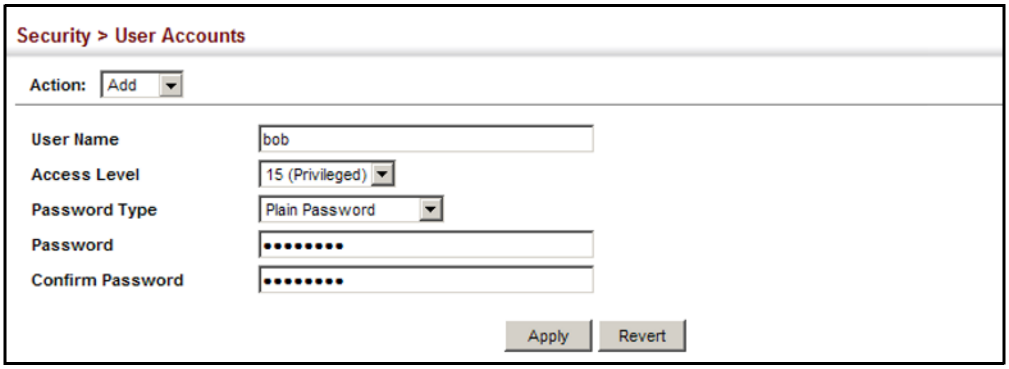
1. Click Security, User Accounts.

2. Select Add from the Action list.

3. Specify a user name, select the user's access level, then enter a password if required and confirm it.

4. Click Apply.

Figure 180: Configuring User Accounts



Security > User Accounts

Action: Add

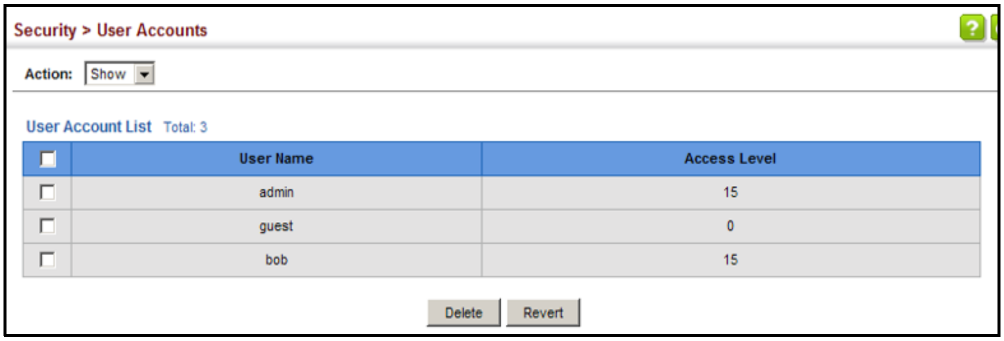
User Name: bob
Access Level: 15 (Privileged)
Password Type: Plain Password
Password: ••••••••
Confirm Password: ••••••••

To show user accounts:

1. Click Security, User Accounts.

2. Select Show from the Action list.

Figure 181: Showing User Accounts



Security > User Accounts

Action: Show

User Account List Total: 3

□	User Name	Access Level
□	admin	15
□	guest	0
□	bob	15

WEB AUTHENTICATION

Web authentication allows stations to authenticate and access the network in situations where 802.1X or Network Access authentication are infeasible or impractical. The web authentication feature allows unauthenticated hosts to request and receive a DHCP assigned IP address and perform DNS queries. All other traffic, except for HTTP protocol traffic, is blocked. The switch intercepts HTTP protocol traffic and redirects it to a switch-generated web page that facilitates user name and password authentication via RADIUS. Once authentication is successful, the web browser is forwarded on to the originally requested web page. Successful authentication is valid for all hosts connected to the port.

NOTE: RADIUS authentication must be activated and configured properly for the web authentication feature to work properly. (See "Configuring Local/Remote Logon Authentication" on page 349.)

NOTE: Web authentication cannot be configured on trunk ports.

CONFIGURING GLOBAL SETTINGS FOR WEB AUTHENTICATION

Use the Security > Web Authentication (Configure Global) page to edit the global parameters for web authentication.

CLI REFERENCES

- "Web Authentication" on page 1109

PARAMETERS

These parameters are displayed:

- **Web Authentication Status** – Enables web authentication for the switch. (Default: Disabled)

  Note that this feature must also be enabled for any port where required under the Configure Interface menu.

- **Session Timeout** – Configures how long an authenticated session stays active before it must re-authenticate itself. (Range: 300-3600 seconds; Default: 3600 seconds)

- **Quiet Period** – Configures how long a host must wait to attempt authentication again after it has exceeded the maximum allowable failed login attempts. (Range: 1-180 seconds; Default: 60 seconds)

- **Login Attempts** – Configures the amount of times a supplicant may attempt and fail authentication before it must wait the configured quiet period. (Range: 1-3 attempts; Default: 3 attempts)

WEB INTERFACE

To configure global parameters for web authentication:

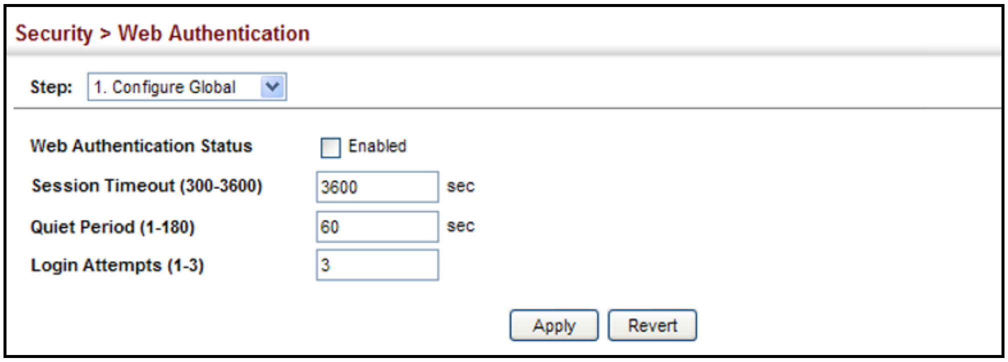
1. Click Security, Web Authentication.

2. Select Configure Global from the Step list.

3. Enable web authentication globally on the switch, and adjust any of the protocol parameters as required.

4. Click Apply.

Figure 182: Configuring Global Settings for Web Authentication



Security > Web Authentication

Step: 1. Configure Global

Web Authentication Status □ Enabled

Session Timeout (300-3600) 3600 sec

Quiet Period (1-180) 60 sec

Login Attempts (1-3) 3

CONFIGURING INTERFACE SETTINGS FOR WEB AUTHENTICATION

Use the Security > Web Authentication (Configure Interface) page to enable web authentication on a port, and display information for any connected hosts.

CLI REFERENCES

- "Web Authentication" on page 1109

PARAMETERS

These parameters are displayed:

- **Port** – Indicates the port being configured.
- **Status** – Configures the web authentication status for the port.
- **Host IP Address** – Indicates the IP address of each connected host.
- **Remaining Session Time** – Indicates the remaining time until the current authorization session for the host expires.
- **Apply** – Enables web authentication if the Status box is checked.
- **Revert** – Restores the previous configuration settings.
- **Re-authenticate** – Ends all authenticated web sessions for selected host IP addresses in the Authenticated Host List, and forces the users to re-authenticate.

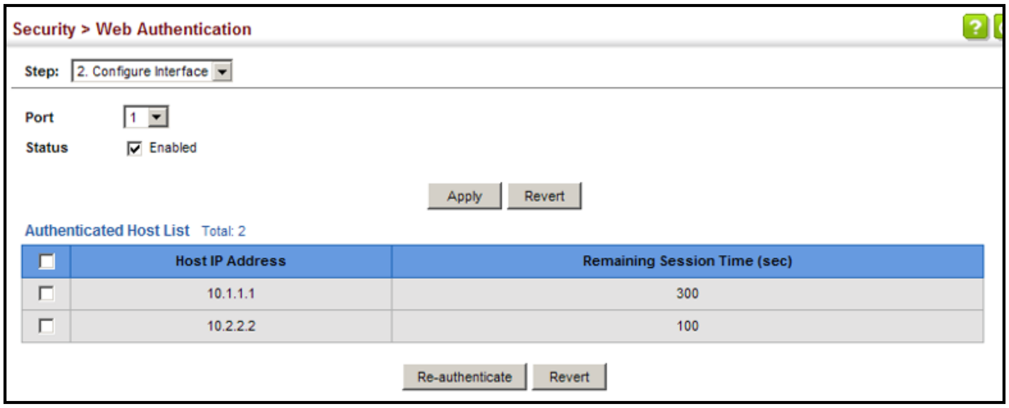
WEB INTERFACE

To enable web authentication for a port:

1. Click Security, Web Authentication.
2. Select Configure Interface from the Step list.
3. Set the status box to enabled for any port that requires web authentication, and click Apply.

4. Mark the check box for any host addresses that need to be re-authenticated, and click Re-authenticate.

Figure 183: Configuring Interface Settings for Web Authentication



Security > Web Authentication

Step: 2. Configure Interface

Port: 1

Status: ☑ Enabled

Authenticated Host List Total: 2

☐	Host IP Address	Remaining Session Time (sec)
☐	10.1.1.1	300
☐	10.2.2.2	100

NETWORK ACCESS (MAC ADDRESS AUTHENTICATION)

Some devices connected to switch ports may not be able to support 802.1X authentication due to hardware or software limitations. This is often true for devices such as network printers, IP phones, and some wireless access points. The switch enables network access from these devices to be controlled by authenticating device MAC addresses with a central RADIUS server.

NOTE: RADIUS authentication must be activated and configured properly for the MAC Address authentication feature to work properly. (See "Configuring Remote Logon Authentication Servers" on page 350.)

NOTE: MAC authentication cannot be configured on trunk ports.

CLI REFERENCES

- "Network Access (MAC Address Authentication)" on page 1095

COMMAND USAGE

- MAC address authentication controls access to the network by authenticating the MAC address of each host that attempts to connect to a switch port. Traffic received from a specific MAC address is forwarded by the switch only if the source MAC address is successfully authenticated by a central RADIUS server. While authentication for a MAC address is in progress, all traffic is blocked until authentication is completed. On successful authentication, the RADIUS server may optionally assign VLAN and quality of service settings for the switch port.

- When enabled on a port, the authentication process sends a Password Authentication Protocol (PAP) request to a configured RADIUS server. The user name and password are both equal to the MAC address being authenticated. On the RADIUS server, PAP user name and passwords must be configured in the MAC address format XX-XX-XX-XX-XX-XX (all in upper case).

- Authenticated MAC addresses are stored as dynamic entries in the switch secure MAC address table and are removed when the aging time expires. The maximum number of secure MAC addresses supported for the switch system is 1024.
- Configured static MAC addresses are added to the secure address table when seen on a switch port. Static addresses are treated as authenticated without sending a request to a RADIUS server.
- When port status changes to down, all MAC addresses mapped to that port are cleared from the secure MAC address table. Static VLAN assignments are not restored.
- The RADIUS server may optionally return a VLAN identifier list to be applied to the switch port. The following attributes need to be configured on the RADIUS server.
  - **Tunnel-Type** = VLAN
  - **Tunnel-Medium-Type** = 802
  - **Tunnel-Private-Group-ID** = 1u,2t   [*VLAN ID list*]

  The VLAN identifier list is carried in the RADIUS "Tunnel-Private-Group-ID" attribute. The VLAN list can contain multiple VLAN identifiers in the format "1u,2t,3u" where "u" indicates an untagged VLAN and "t" a tagged VLAN.
- The RADIUS server may optionally return dynamic QoS assignments to be applied to a switch port for an authenticated user. The "Filter-ID" attribute (attribute 11) can be configured on the RADIUS server to pass the following QoS information:

Table 22: Dynamic QoS Profiles

Profile	Attribute Syntax	Example
DiffServ	**service-policy-in**=*policy-map-name*	service-policy-in=p1
Rate Limit	**rate-limit-input**=*rate*	rate-limit-input=100 (in units of Kbps)
802.1p	**switchport-priority-default**=*value*	switchport-priority-default=2
IP ACL	**ip-access-group-in**=*ip-acl-name*	ip-access-group-in=ipv4acl
IPv6 ACL	**ipv6-access-group-in**=*ipv6-acl-name*	ipv6-access-group-in=ipv6acl
MAC ACL	**mac-access-group-in**=*mac-acl-name*	mac-access-group-in=macAcl

- Multiple profiles can be specified in the Filter-ID attribute by using a semicolon to separate each profile.

For example, the attribute "service-policy-in=pp1;rate-limit-input=100" specifies that the diffserv profile name is "pp1," and the ingress rate limit profile value is 100 kbps.

- If duplicate profiles are passed in the Filter-ID attribute, then only the first profile is used.

  For example, if the attribute is "service-policy-in=p1;service-policy-in=p2", then the switch applies only the DiffServ profile "p1."

- Any unsupported profiles in the Filter-ID attribute are ignored.

  For example, if the attribute is "map-ip-dscp=2:3;service-policy-in=p1," then the switch ignores the "map-ip-dscp" profile.

- When authentication is successful, the dynamic QoS information may not be passed from the RADIUS server due to one of the following conditions (authentication result remains unchanged):

  - The Filter-ID attribute cannot be found to carry the user profile.
  - The Filter-ID attribute is empty.
  - The Filter-ID attribute format for dynamic QoS assignment is unrecognizable (can not recognize the whole Filter-ID attribute).

- Dynamic QoS assignment fails and the authentication result changes from success to failure when the following conditions occur:

  - Illegal characters found in a profile value (for example, a non-digital character in an 802.1p profile value).
  - Failure to configure the received profiles on the authenticated port.

- When the last user logs off on a port with a dynamic QoS assignment, the switch restores the original QoS configuration for the port.

- When a user attempts to log into the network with a returned dynamic QoS profile that is different from users already logged on to the same port, the user is denied access.

- While a port has an assigned dynamic QoS profile, any manual QoS configuration changes only take effect after all users have logged off the port.

CONFIGURING GLOBAL SETTINGS FOR NETWORK ACCESS

MAC address authentication is configured on a per-port basis, however there are two configurable parameters that apply globally to all ports on the switch. Use the Security > Network Access (Configure Global) page to configure MAC address authentication aging and reauthentication time.

CLI REFERENCES

- "Network Access (MAC Address Authentication)" on page 1095

PARAMETERS

These parameters are displayed:

- **Aging Status** – Enables aging for authenticated MAC addresses stored in the secure MAC address table. (Default: Disabled)

  This parameter applies to authenticated MAC addresses configured by the MAC Address Authentication process described in this section, as well as to any secure MAC addresses authenticated by 802.1X, regardless of the 802.1X Operation Mode (Single-Host, Multi-Host, or MAC-Based authentication as described on page 425).

  Authenticated MAC addresses are stored as dynamic entries in the switch’s secure MAC address table and are removed when the aging time expires.

  The maximum number of secure MAC addresses supported for the switch system is 1024.

- **Reauthentication Time** – Sets the time period after which a connected host must be reauthenticated. When the reauthentication time expires for a secure MAC address, it is reauthenticated with the RADIUS server. During the reauthentication process traffic through the port remains unaffected. (Range: 120-1000000 seconds; Default: 1800 seconds)

WEB INTERFACE

To configure aging status and reauthentication time for MAC address authentication:

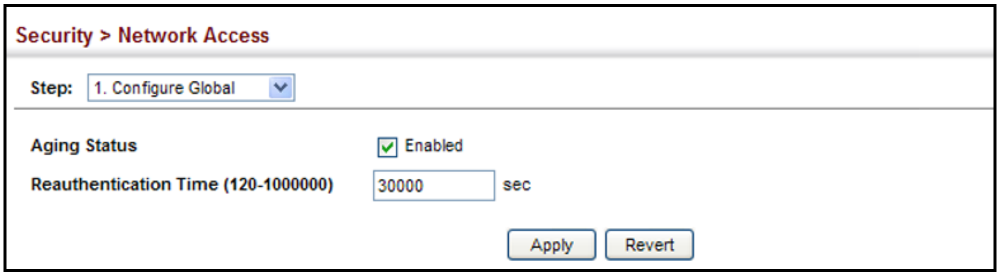
1. Click Security, Network Access.

2. Select Configure Global from the Step list.

3. Enable or disable aging for secure addresses, and modify the reauthentication time as required.

4. Click Apply.

Figure 184: Configuring Global Settings for Network Access



Security > Network Access

Step: 1. Configure Global

Aging Status ☑ Enabled

Reauthentication Time (120-1000000) 30000 sec

CONFIGURING NETWORK ACCESS FOR PORTS

Use the Security > Network Access (Configure Interface - General) page to configure MAC authentication on switch ports, including enabling address authentication, setting the maximum MAC count, and enabling dynamic VLAN or dynamic QoS assignments.

CLI REFERENCES

- "Network Access (MAC Address Authentication)" on page 1095

PARAMETERS

These parameters are displayed:

- **MAC Authentication**
  - **Status** – Enables MAC authentication on a port. (Default: Disabled)
  - **Intrusion** – Sets the port response to a host MAC authentication failure to either block access to the port or to pass traffic through. (Options: Block, Pass; Default: Block)
  - **Max MAC Count**[4] – Sets the maximum number of MAC addresses that can be authenticated on a port via MAC authentication; that is, the Network Access process described in this section.
    (Range: 1-1024; Default: 1024)
- **Network Access Max MAC Count**[4] – Sets the maximum number of MAC addresses that can be authenticated on a port interface via all forms of authentication (including Network Access and IEEE 802.1X). (Range: 1-1024; Default: 1024)
- **Guest VLAN** – Specifies the VLAN to be assigned to the port when 802.1X Authentication fails. (Range: 0-4094, where 0 means disabled; Default: Disabled)

  The VLAN must already be created and active (see "Configuring VLAN Groups" on page 228). Also, when used with 802.1X authentication, intrusion action must be set for “Guest VLAN” (see "Configuring Port Authenticator Settings for 802.1X" on page 425).

[4] The maximum number of MAC addresses per port is 1024, and the maximum number of secure MAC addresses supported for the switch system is 1024. When the limit is reached, all new MAC addresses are treated as authentication failures.

- **Dynamic VLAN** – Enables dynamic VLAN assignment for an authenticated port. When enabled, any VLAN identifiers returned by the RADIUS server through the 802.1X authentication process are applied to the port, providing the VLANs have already been created on the switch. (GVRP is not used to create the VLANs.) (Default: Enabled)

  The VLAN settings specified by the first authenticated MAC address are implemented for a port. Other authenticated MAC addresses on the port must have the same VLAN configuration, or they are treated as authentication failures.

  If dynamic VLAN assignment is enabled on a port and the RADIUS server returns no VLAN configuration, the authentication is still treated as a success, and the host is assigned to the default untagged VLAN.

  When the dynamic VLAN assignment status is changed on a port, all authenticated addresses mapped to that port are cleared from the secure MAC address table.

- **Dynamic QoS** – Enables dynamic QoS assignment for an authenticated port. (Default: Disabled)

- **MAC Filter ID** – Allows a MAC Filter to be assigned to the port. MAC addresses or MAC address ranges present in a selected MAC Filter are exempt from authentication on the specified port (as described under "Configuring a MAC Address Filter"). (Range: 1-64; Default: None)

WEB INTERFACE

To configure MAC authentication on switch ports:

1. Click Security, Network Access.

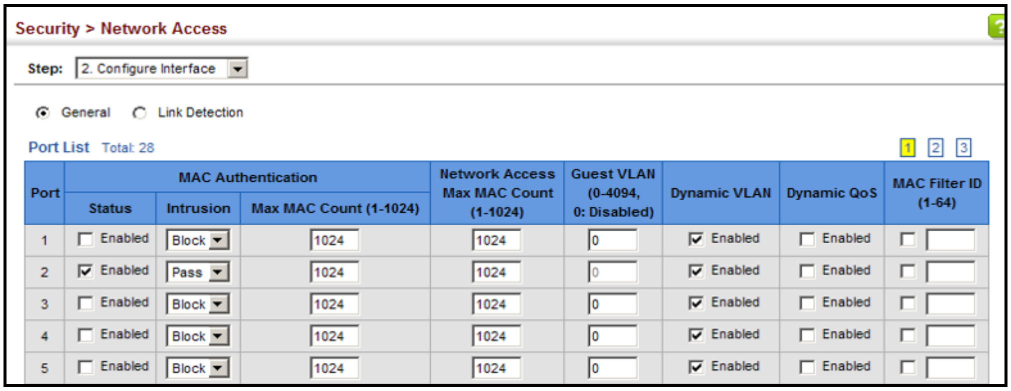
2. Select Configure Interface from the Step list.

3. Click the General button.

4. Make any configuration changes required to enable address authentication on a port, set the maximum number of secure addresses supported, the guest VLAN to use when MAC Authentication or 802.1X Authentication fails, and the dynamic VLAN and QoS assignments.

5. Click Apply.

Figure 185: Configuring Interface Settings for Network Access



Security > Network Access

Step: 2. Configure Interface

● General ○ Link Detection

Port List Total: 28 — 1 2 3

Port	MAC Authentication			Network Access Max MAC Count (1-1024)	Guest VLAN (0-4094, 0: Disabled)	Dynamic VLAN	Dynamic QoS	MAC Filter ID (1-64)
	Status	Intrusion	Max MAC Count (1-1024)					
1	☐ Enabled	Block	1024	1024	0	☑ Enabled	☐ Enabled	☐
2	☑ Enabled	Pass	1024	1024	0	☑ Enabled	☐ Enabled	☐
3	☐ Enabled	Block	1024	1024	0	☑ Enabled	☐ Enabled	☐
4	☐ Enabled	Block	1024	1024	0	☑ Enabled	☐ Enabled	☐
5	☐ Enabled	Block	1024	1024	0	☑ Enabled	☐ Enabled	☐

CONFIGURING PORT LINK DETECTION

Use the Security > Network Access (Configure Interface - Link Detection) page to send an SNMP trap and/or shut down a port when a link event occurs.

CLI REFERENCES

- "Network Access (MAC Address Authentication)" on page 1095

PARAMETERS

These parameters are displayed:

- **Link Detection Status** – Configures whether Link Detection is enabled or disabled for a port.
- **Condition** – The link event type which will trigger the port action.
  - **Link up** – Only link up events will trigger the port action.
  - **Link down** – Only link down events will trigger the port action.
  - **Link up and down** – All link up and link down events will trigger the port action.
- **Action** – The switch can respond in three ways to a link up or down trigger event.
  - **Trap** – An SNMP trap is sent.
  - **Trap and shutdown** – An SNMP trap is sent and the port is shut down.
  - **Shutdown** – The port is shut down.

WEB INTERFACE

To configure link detection on switch ports:

1. Click Security, Network Access.

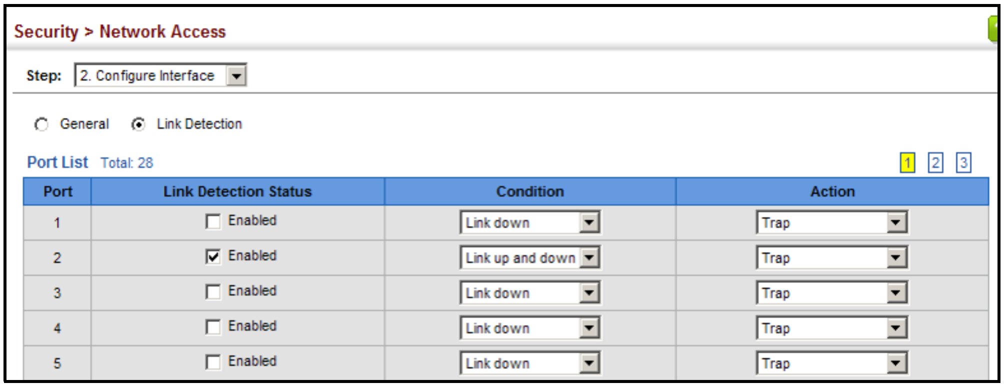
2. Select Configure Interface from the Step list.

3. Click the Link Detection button.

4. Modify the link detection status, trigger condition, and the response for any port.

5. Click Apply.

Figure 186: Configuring Link Detection for Network Access



Security > Network Access

Step: 2. Configure Interface

○ General ● Link Detection

Port List Total: 28 1 2 3

Port	Link Detection Status	Condition	Action
1	□ Enabled	Link down	Trap
2	☑ Enabled	Link up and down	Trap
3	□ Enabled	Link down	Trap
4	□ Enabled	Link down	Trap
5	□ Enabled	Link down	Trap

CONFIGURING A MAC ADDRESS FILTER

Use the Security > Network Access (Configure MAC Filter) page to designate specific MAC addresses or MAC address ranges as exempt from authentication. MAC addresses present in MAC Filter tables activated on a port are treated as pre-authenticated on that port.

CLI REFERENCES

- "Network Access (MAC Address Authentication)" on page 1095

COMMAND USAGE

- Specified MAC addresses are exempt from authentication.

- Up to 65 filter tables can be defined.

- There is no limitation on the number of entries used in a filter table.

PARAMETERS

These parameters are displayed:

- **Filter ID** – Adds a filter rule for the specified filter.

- **MAC Address** – The filter rule will check ingress packets against the entered MAC address or range of MAC addresses (as defined by the MAC Address Mask).

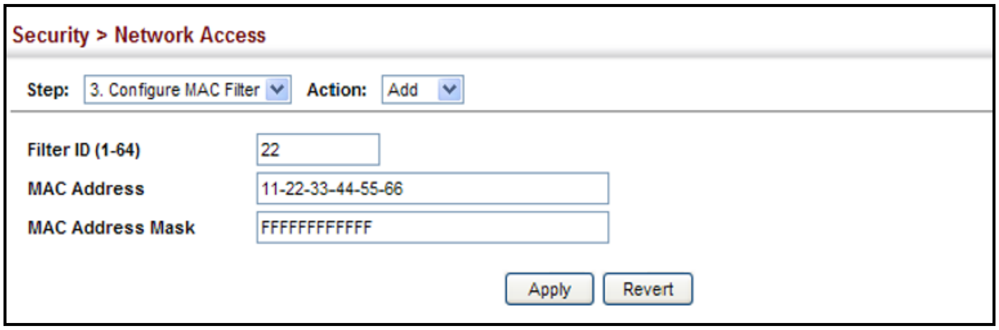
- **MAC Address Mask** – The filter rule will check for the range of MAC addresses defined by the MAC bit mask. If you omit the mask, the system will assign the default mask of an exact match.
(Range: 000000000000 - FFFFFFFFFFFF; Default: FFFFFFFFFFFF)

WEB INTERFACE

To add a MAC address filter for MAC authentication:

1. Click Security, Network Access.
2. Select Configure MAC Filter from the Step list.
3. Select Add from the Action list.
4. Enter a filter ID, MAC address, and optional mask.
5. Click Apply.

Figure 187: Configuring a MAC Address Filter for Network Access



Security > Network Access

Step: 3. Configure MAC Filter Action: Add

Filter ID (1-64): 22

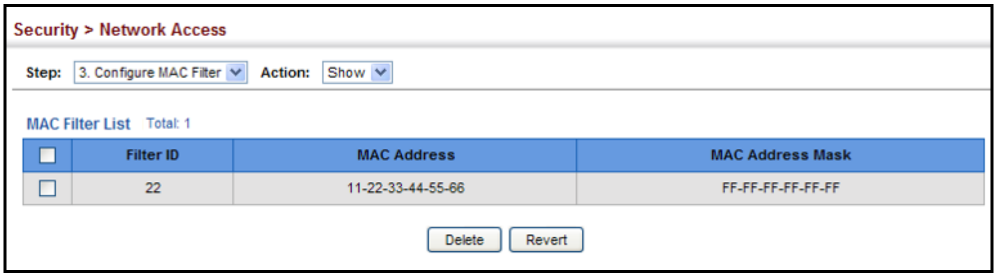
MAC Address: 11-22-33-44-55-66

MAC Address Mask: FFFFFFFFFFFF

To show the MAC address filter table for MAC authentication:

1. Click Security, Network Access.
2. Select Configure MAC Filter from the Step list.
3. Select Show from the Action list.

Figure 188: Showing the MAC Address Filter Table for Network Access



Security > Network Access

Step: 3. Configure MAC Filter Action: Show

MAC Filter List Total: 1

□	Filter ID	MAC Address	MAC Address Mask
□	22	11-22-33-44-55-66	FF-FF-FF-FF-FF-FF

DISPLAYING SECURE MAC ADDRESS INFORMATION

Use the Security > Network Access (Show Information) page to display the authenticated MAC addresses stored in the secure MAC address table. Information on the secure MAC entries can be displayed and selected entries can be removed from the table.

CLI REFERENCES

- "Network Access (MAC Address Authentication)" on page 1095

PARAMETERS

These parameters are displayed:

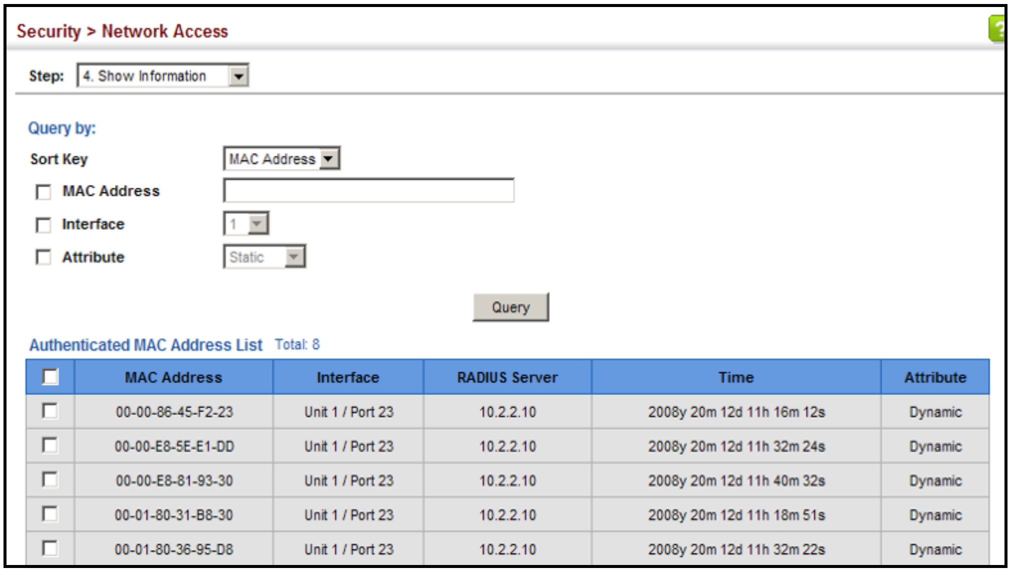
- **Query By** – Specifies parameters to use in the MAC address query.
  - **Sort Key** – Sorts the information displayed based on MAC address, port interface, or attribute.
  - **MAC Address** – Specifies a specific MAC address.
  - **Interface** – Specifies a port interface.
  - **Attribute** – Displays static or dynamic addresses.
- **Authenticated MAC Address List**
  - **MAC Address** – The authenticated MAC address.
  - **Interface** – The port interface associated with a secure MAC address.
  - **RADIUS Server** – The IP address of the RADIUS server that authenticated the MAC address.
  - **Time** – The time when the MAC address was last authenticated.
  - **Attribute** – Indicates a static or dynamic address.

WEB INTERFACE

To display the authenticated MAC addresses stored in the secure MAC address table:

1. Click Security, Network Access.
2. Select Show Information from the Step list.
3. Use the sort key to display addresses based MAC address, interface, or attribute.
4. Restrict the displayed addresses by entering a specific address in the MAC Address field, specifying a port in the Interface field, or setting the address type to static or dynamic in the Attribute field.
5. Click Query.

Figure 189: Showing Addresses Authenticated for Network Access



Security > Network Access

Step: 4. Show Information

Query by:

Sort Key: MAC Address

□ MAC Address

□ Interface: 1

□ Attribute: Static

Authenticated MAC Address List Total: 8

□	MAC Address	Interface	RADIUS Server	Time	Attribute
□	00-00-86-45-F2-23	Unit 1 / Port 23	10.2.2.10	2008y 20m 12d 11h 16m 12s	Dynamic
□	00-00-E8-5E-E1-DD	Unit 1 / Port 23	10.2.2.10	2008y 20m 12d 11h 32m 24s	Dynamic
□	00-00-E8-81-93-30	Unit 1 / Port 23	10.2.2.10	2008y 20m 12d 11h 40m 32s	Dynamic
□	00-01-80-31-B8-30	Unit 1 / Port 23	10.2.2.10	2008y 20m 12d 11h 18m 51s	Dynamic
□	00-01-80-36-95-D8	Unit 1 / Port 23	10.2.2.10	2008y 20m 12d 11h 32m 22s	Dynamic

CONFIGURING HTTPS

You can configure the switch to enable the Secure Hypertext Transfer Protocol (HTTPS) over the Secure Socket Layer (SSL), providing secure access (i.e., an encrypted connection) to the switch's web interface.

CONFIGURING GLOBAL SETTINGS FOR HTTPS

Use the Security > HTTPS (Configure Global) page to enable or disable HTTPS and specify the UDP port used for this service.

CLI REFERENCES

- "Web Server" on page 1051

COMMAND USAGE

- Both the HTTP and HTTPS service can be enabled independently on the switch. However, you cannot configure both services to use the same UDP port. (HTTP can only be configured through the CLI using the ip http server command described on page 1052.)

- If you enable HTTPS, you must indicate this in the URL that you specify in your browser: https://*device*[:*port_number*]

- When you start HTTPS, the connection is established in this way:
  - The client authenticates the server using the server's digital certificate.
  - The client and server negotiate a set of security protocols to use for the connection.
  - The client and server generate session keys for encrypting and decrypting data.

- The client and server establish a secure encrypted connection.

  A padlock icon should appear in the status bar for Internet Explorer 6, Mozilla Firefox 4, or Google Chrome 29, or more recent versions.

- The following web browsers and operating systems currently support HTTPS:

  Table 23: HTTPS System Support

Web Browser	Operating System
Internet Explorer 6.x or later	Windows 98,Windows NT (with service pack 6a), Windows 2000, XP, Vista, 7, 8
Mozilla Firefox 4 or later	Windows 2000, XP, Vista, 7, 8, Linux
Google Chrome 29 or later	Windows XP, Vista, 7, 8

- To specify a secure-site certificate, see "Replacing the Default Secure-site Certificate" on page 380.

NOTE: Connection to the web interface is not supported for HTTPS using an IPv6 link local address.

PARAMETERS

These parameters are displayed:

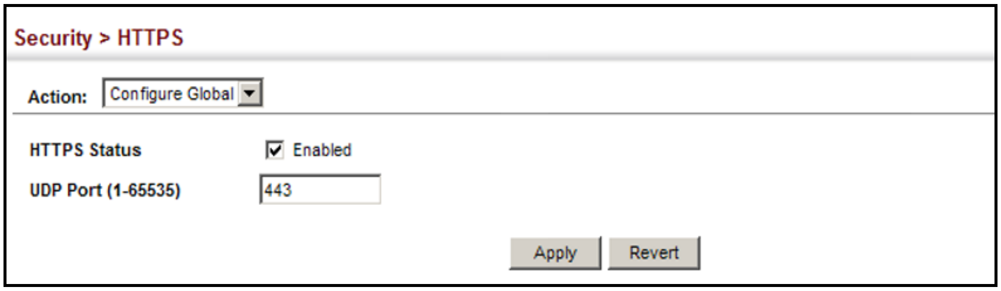
- **HTTPS Status** – Allows you to enable/disable the HTTPS server feature on the switch. (Default: Enabled)
- **HTTPS Port** – Specifies the UDP port number used for HTTPS connection to the switch's web interface. (Default: Port 443)

WEB INTERFACE

To configure HTTPS:

1. Click Security, HTTPS.
2. Select Configure Global from the Step list.
3. Enable HTTPS and specify the port number if required.
4. Click Apply.

Figure 190: Configuring HTTPS



Security > HTTPS

Action: Configure Global

HTTPS Status ☑ Enabled

UDP Port (1-65535) 443

REPLACING THE DEFAULT SECURE-SITE CERTIFICATE

Use the Security > HTTPS (Copy Certificate) page to replace the default secure-site certificate.

When you log onto the web interface using HTTPS (for secure access), a Secure Sockets Layer (SSL) certificate appears for the switch. By default, the certificate that the web browser displays will be associated with a warning that the site is not recognized as a secure site. This is because the certificate has not been signed by an approved certification authority. If you want this warning to be replaced by a message confirming that the connection to the switch is secure, you must obtain a unique certificate and a private key and password from a recognized certification authority.

CAUTION: For maximum security, we recommend you obtain a unique Secure Sockets Layer certificate at the earliest opportunity. This is because the default certificate for the switch is not unique to the hardware you have purchased.

When you have obtained these, place them on your TFTP server and transfer them to the switch to replace the default (unrecognized) certificate with an authorized one.

NOTE: The switch must be reset for the new certificate to be activated. To reset the switch, see "Resetting the System" on page 177 or type “reload” at the command prompt: `Console#reload`

CLI REFERENCES

- "Web Server" on page 1051

PARAMETERS

These parameters are displayed:

- **TFTP Server IP Address** – IP address of TFTP server which contains the certificate file.
- **Certificate Source File Name** – Name of certificate file stored on the TFTP server.
- **Private Key Source File Name** – Name of private key file stored on the TFTP server.
- **Private Password** – Password stored in the private key file. This password is used to verify authorization for certificate use, and is verified when downloading the certificate to the switch.
- **Confirm Password** – Re-type the string entered in the previous field to ensure no errors were made. The switch will not download the certificate if these two fields do not match.

WEB INTERFACE

To replace the default secure-site certificate:

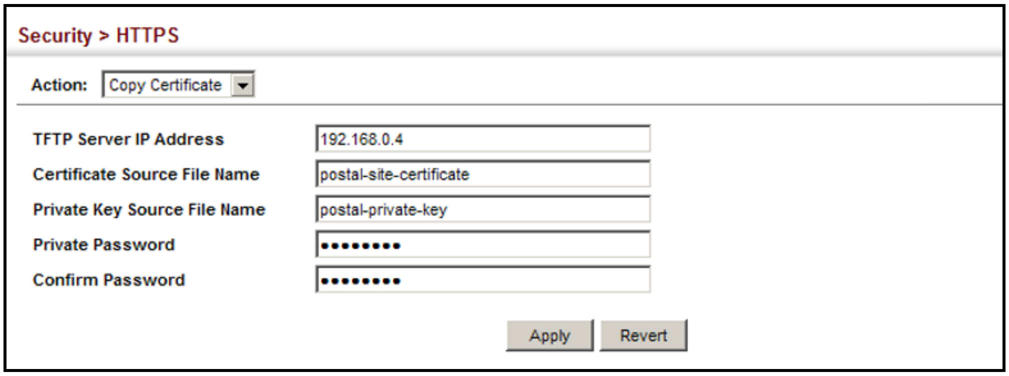
1. Click Security, HTTPS.

2. Select Copy Certificate from the Step list.

3. Fill in the TFTP server, certificate and private key file name, and private password.

4. Click Apply.

Figure 191: Downloading the Secure-Site Certificate



Security > HTTPS

Action: Copy Certificate

TFTP Server IP Address: 192.168.0.4
Certificate Source File Name: postal-site-certificate
Private Key Source File Name: postal-private-key
Private Password: ••••••••
Confirm Password: ••••••••

CONFIGURING THE SECURE SHELL

The Berkeley-standard includes remote access tools originally designed for Unix systems. Some of these tools have also been implemented for Microsoft Windows and other environments. These tools, including commands such as *rlogin* (remote login), *rsh* (remote shell), and *rcp* (remote copy), are not secure from hostile attacks.

Secure Shell (SSH) includes server/client applications intended as a secure replacement for the older Berkeley remote access tools. SSH can also provide remote management access to this switch as a secure replacement for Telnet. When the client contacts the switch via the SSH protocol, the switch generates a public-key that the client uses along with a local user name and password for access authentication. SSH also encrypts all data transfers passing between the switch and SSH-enabled management station clients, and ensures that data traveling over the network arrives unaltered.

NOTE: You need to install an SSH client on the management station to access the switch for management via the SSH protocol.

NOTE: The switch supports both SSH Version 1.5 and 2.0 clients.

COMMAND USAGE

The SSH server on this switch supports both password and public key authentication. If password authentication is specified by the SSH client, then the password can be authenticated either locally or via a RADIUS or TACACS+ remote authentication server, as specified on the System Authentication page (page 349). If public key authentication is specified by the client, then you must configure authentication keys on both the client and the switch as described in the following section. Note that regardless of whether you use public key or password authentication, you still have to generate authentication keys on the switch (SSH Host Key Settings) and enable the SSH server (Authentication Settings).

To use the SSH server, complete these steps:

1. *Generate a Host Key Pair* – On the SSH Host Key Settings page, create a host public/private key pair.

2. *Provide Host Public Key to Clients* – Many SSH client programs automatically import the host public key during the initial connection setup with the switch. Otherwise, you need to manually create a known hosts file on the management station and place the host public key in it. An entry for a public key in the known hosts file would appear similar to the following example:

   ```
   10.1.0.54 1024 35
   15684995401867669259333946775054617325313674890836547254
   15020245593199868544358361651999923329781766065830956
   10825913212890233 76546801726272571413428762941301196195566782
   59566410486957427888146206519417467729848654686157177393901647
   79355942303577413098022737087794545240839717526463580581767167
   09574804776117
   ```

3. *Import Client's Public Key to the Switch* – See "Importing User Public Keys" on page 387, or use the copy tftp public-key command to copy a file containing the public key for all the SSH client's granted management access to the switch. (Note that these clients must be configured locally on the switch via the User Accounts page as described on page 363.) The clients are subsequently authenticated using these keys. The current firmware only accepts public key files based on standard UNIX format as shown in the following example for an RSA Version 1 key:

   ```
   1024 35
   134108168560989392104094492015542534763164192187295892114317388
   800555361616310517759408386863110929123222682851925437460310093
   718772119969631781366277414168985132049117204830339254324101637
   997592371449011938006090253948408482717819437228840253311595
   2134861022902978982721353267131629432532818915045306393916643
   steve@192.168.1.19
   ```

4. *Set the Optional Parameters* – On the SSH Settings page, configure the optional parameters, including the authentication timeout, the number of retries, and the server key size.

5. *Enable SSH Service* – On the SSH Settings page, enable the SSH server on the switch.

6. Authentication – One of the following authentication methods is employed:

   Password Authentication (for SSH v1.5 or V2 Clients)

   a. The client sends its password to the server.
   b. The switch compares the client's password to those stored in memory.
   c. If a match is found, the connection is allowed.

NOTE: To use SSH with only password authentication, the host public key must still be given to the client, either during initial connection or manually entered into the known host file. However, you do not need to configure the client's keys.

Public Key Authentication – When an SSH client attempts to contact the switch, the SSH server uses the host key pair to negotiate a session key and encryption method. Only clients that have a private key corresponding to the public keys stored on the switch can access it. The following exchanges take place during this process:

Authenticating SSH v1.5 Clients

a. The client sends its RSA public key to the switch.
b. The switch compares the client's public key to those stored in memory.
c. If a match is found, the switch uses its secret key to generate a random 256-bit string as a challenge, encrypts this string with the user's public key, and sends it to the client.
d. The client uses its private key to decrypt the challenge string, computes the MD5 checksum, and sends the checksum back to the switch.
e. The switch compares the checksum sent from the client against that computed for the original string it sent. If the two checksums match, this means that the client's private key corresponds to an authorized public key, and the client is authenticated.

Authenticating SSH v2 Clients

a. The client first queries the switch to determine if DSA public key authentication using a preferred algorithm is acceptable.
b. If the specified algorithm is supported by the switch, it notifies the client to proceed with the authentication process. Otherwise, it rejects the request.
c. The client sends a signature generated using the private key to the switch.
d. When the server receives this message, it checks whether the supplied key is acceptable for authentication, and if so, it then

checks whether the signature is correct. If both checks succeed, the client is authenticated.

NOTE: The SSH server supports up to four client sessions. The maximum number of client sessions includes both current Telnet sessions and SSH sessions.

NOTE: The SSH server can be accessed using any configured IPv4 or IPv6 interface address on the switch.

CONFIGURING THE SSH SERVER

Use the Security > SSH (Configure Global) page to enable the SSH server and configure basic settings for authentication.

NOTE: A host key pair must be configured on the switch before you can enable the SSH server. See "Generating the Host Key Pair" on page 385.

CLI REFERENCES

- "Secure Shell" on page 1057

PARAMETERS

These parameters are displayed:

- **SSH Server Status** – Allows you to enable/disable the SSH server on the switch. (Default: Disabled)

- **Version** – The Secure Shell version number. Version 2.0 is displayed, but the switch supports management access via either SSH Version 1.5 or 2.0 clients.

- **Authentication Timeout** – Specifies the time interval in seconds that the SSH server waits for a response from a client during an authentication attempt. (Range: 1-120 seconds; Default: 120 seconds)

- **Authentication Retries** – Specifies the number of authentication attempts that a client is allowed before authentication fails and the client has to restart the authentication process. (Range: 1-5 times; Default: 3)

- **Server-Key Size** – Specifies the SSH server key size. (Range: 512-896 bits; Default:768)

  - The server key is a private key that is never shared outside the switch.

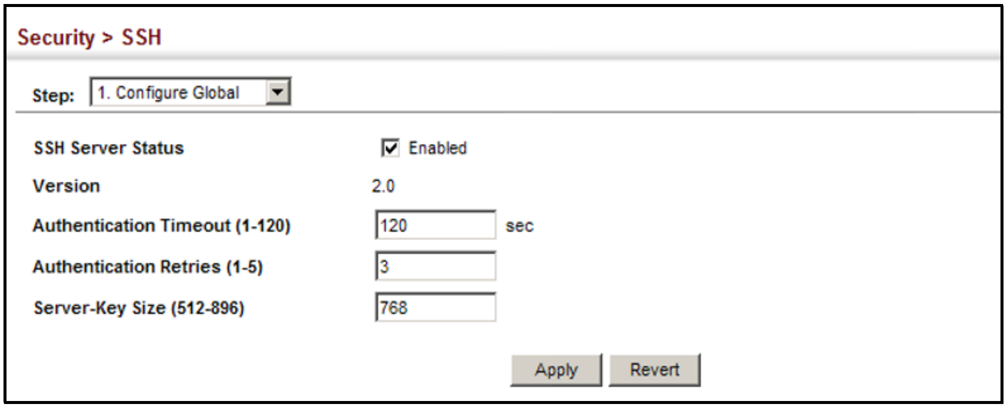
  - The host key is shared with the SSH client, and is fixed at 1024 bits.

WEB INTERFACE

To configure the SSH server:

1. Click Security, SSH.
2. Select Configure Global from the Step list.
3. Enable the SSH server.
4. Adjust the authentication parameters as required.
5. Click Apply.

Figure 192: Configuring the SSH Server



Security > SSH

Step: 1. Configure Global

SSH Server Status	☑ Enabled
Version	2.0
Authentication Timeout (1-120)	120 sec
Authentication Retries (1-5)	3
Server-Key Size (512-896)	768

GENERATING THE HOST KEY PAIR

Use the Security > SSH (Configure Host Key - Generate) page to generate a host public/private key pair used to provide secure communications between an SSH client and the switch. After generating this key pair, you must provide the host public key to SSH clients and import the client's public key to the switch as described in the section "Importing User Public Keys" on page 387.

NOTE: A host key pair must be configured on the switch before you can enable the SSH server. See "Configuring the SSH Server" on page 384.

CLI REFERENCES

- "Secure Shell" on page 1057

PARAMETERS

These parameters are displayed:

- **Host-Key Type** – The key type used to generate the host key pair (i.e., public and private keys). (Range: RSA (Version 1), DSA (Version 2), Both; Default: Both)

  The SSH server uses RSA or DSA for key exchange when the client first establishes a connection with the switch, and then negotiates with the client to select either DES (56-bit) or 3DES (168-bit) for data encryption.

NOTE: The switch uses only RSA Version 1 for SSHv1.5 clients and DSA Version 2 for SSHv2 clients.

- **Save Host-Key from Memory to Flash** – Saves the host key from RAM (i.e., volatile memory) to flash memory. Otherwise, the host key pair is stored to RAM by default. Note that you must select this item prior to generating the host-key pair. (Default: Disabled)

WEB INTERFACE

To generate the SSH host key pair:

1. Click Security, SSH.

2. Select Configure Host Key from the Step list.

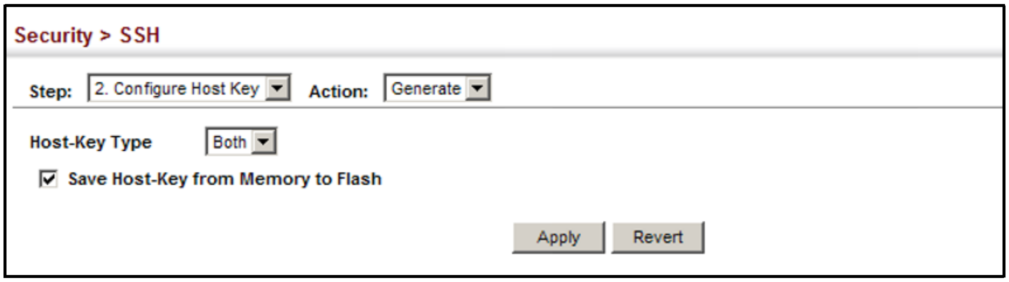
3. Select Generate from the Action list.

4. Select the host-key type from the drop-down box.

5. Select the option to save the host key from memory to flash if required.

6. Click Apply.

Figure 193: Generating the SSH Host Key Pair



Security > SSH

Step: 2. Configure Host Key Action: Generate

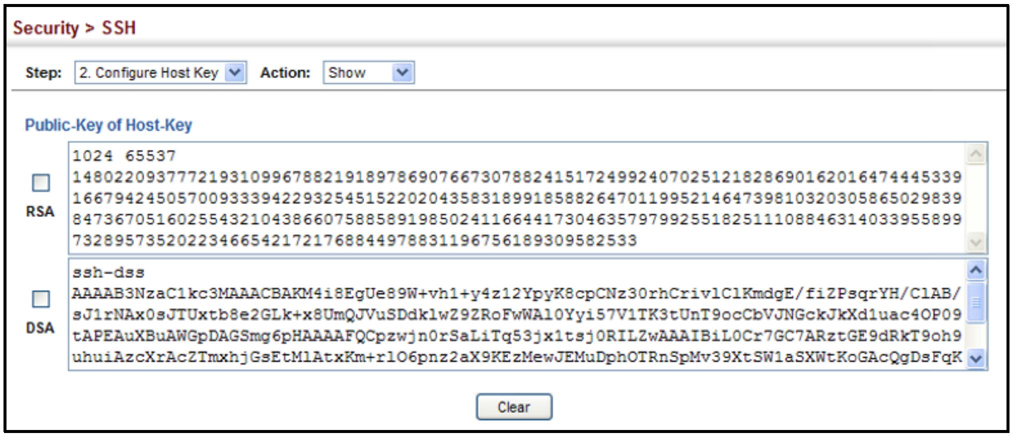
Host-Key Type: Both

☑ Save Host-Key from Memory to Flash

To display or clear the SSH host key pair:

1. Click Security, SSH.
2. Select Configure Host Key from the Step list.
3. Select Show from the Action list.
4. Select the host-key type to clear.
5. Click Clear.

Figure 194: Showing the SSH Host Key Pair



```
1024 65537
1480220937772193109967882191897869076673078824151724992407025121828690162016474445339
1667942450570093339422932545152202043583189918588264701199521464739810320305865029839
8473670516025543210438660758858919850241166441730463579799255182511108846314033955899
7328957352022346654217217688449788311967561893095825З3
```

```
ssh-dss
AAAAB3NzaC1kc3MAAACBAKM4i8EgUe89W+vh1+y4z12YpyK8cpCNz30rhCrivlClKmdgE/fiZPsqrYH/ClAB/
sJ1rNAx0sJTUxtb8e2GLk+x8UmQJVuSDdklwZ9ZRoFwWAl0Yyi57V1TK3tUnT9ocCbVJNGckJkXd1uac4OP09
tAPEAuXBuAWGpDAGSmg6pHAAAAFQCpzwjn0rSaLiTq53jx1tsj0RILZwAAAIBiL0Cr7GC7ARztGE9dRkT9oh9
uhuiAzcXrAcZTmxhjGsEtMlAtxKm+rl06pnz2aX9KEzMewJEMuDphOTRnSpMv39XtSW1aSXWtKoGAcQgDsFqK
```

IMPORTING USER PUBLIC KEYS

Use the Security > SSH (Configure User Key - Copy) page to upload a user's public key to the switch. This public key must be stored on the switch for the user to be able to log in using the public key authentication mechanism. If the user's public key does not exist on the switch, SSH will revert to the interactive password authentication mechanism to complete authentication.

CLI REFERENCES

- "Secure Shell" on page 1057

PARAMETERS

These parameters are displayed:

- **User Name** – This drop-down box selects the user who's public key you wish to manage. Note that you must first create users on the User Accounts page (see "Configuring User Accounts" on page 363).
- **User Key Type** – The type of public key to upload.
  - RSA: The switch accepts a RSA version 1 encrypted public key.
  - DSA: The switch accepts a DSA version 2 encrypted public key.

The SSH server uses RSA or DSA for key exchange when the client first establishes a connection with the switch, and then negotiates with the client to select either DES (56-bit) or 3DES (168-bit) for data encryption.

The switch uses only RSA Version 1 for SSHv1.5 clients and DSA Version 2 for SSHv2 clients.

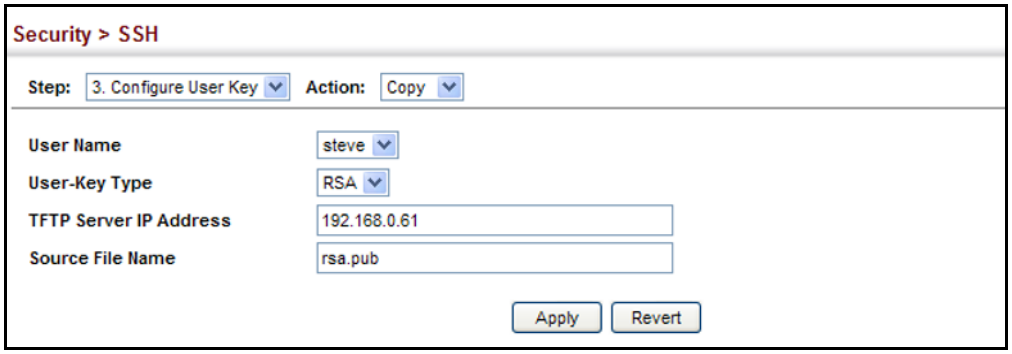
- **TFTP Server IP Address** – The IP address of the TFTP server that contains the public key file you wish to import.
- **Source File Name** – The public key file to upload.

WEB INTERFACE

To copy the SSH user's public key:

1. Click Security, SSH.
2. Select Configure User Key from the Step list.
3. Select Copy from the Action list.
4. Select the user name and the public-key type from the respective drop-down boxes, input the TFTP server IP address and the public key source file name.
5. Click Apply.

Figure 195: Copying the SSH User's Public Key



Security > SSH

Step: 3. Configure User Key Action: Copy

User Name: steve
User-Key Type: RSA
TFTP Server IP Address: 192.168.0.61
Source File Name: rsa.pub

To display or clear the SSH user's public key:

1. Click Security, SSH.

2. Select Configure User Key from the Step list.

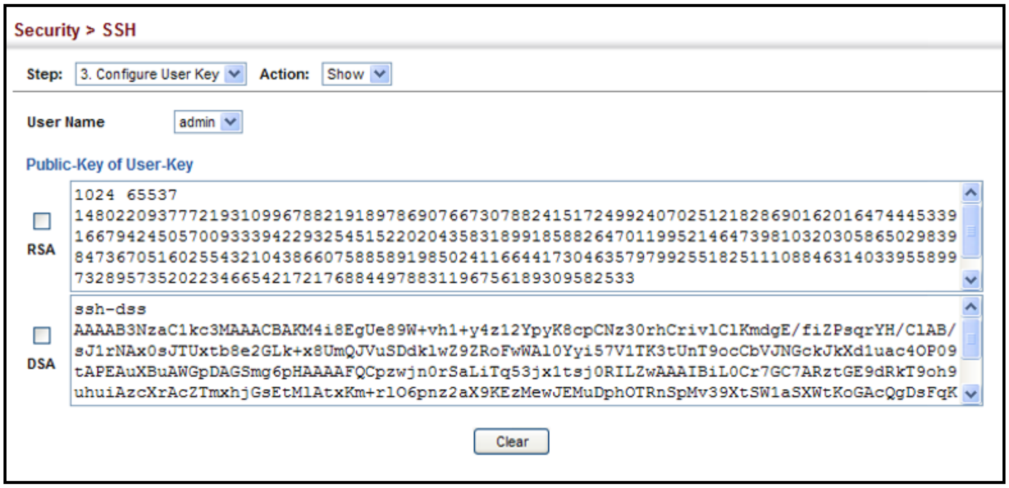
3. Select Show from the Action list.

4. Select a user from the User Name list.

5. Select the host-key type to clear.

6. Click Clear.

Figure 196: Showing the SSH User's Public Key



Step: 3. Configure User Key Action: Show

User Name: admin

□ RSA

```
1024 65537
1480220937772193109967882191897869076673078824151724992407025121828690162016474445339
1667942450570093339422932545152202043583189918588264701199521464739810320305865029839
8473670516025543210438660758858919850241166441730463579799255182511108846314033955899
732895735202234665421721768844978831196756189309582533
```

□ DSA

```
ssh-dss
AAAAB3NzaC1kc3MAAACBAKM4i8EgUe89W+vh1+y4z12YpyK8cpCNz30rhCrivlClKmdgE/fiZPsqrYH/ClAB/
sJ1rNAx0sJTUxtb8e2GLk+x8UmQJVuSDdklwZ9ZRoFwWAl0Yyi57V1TK3tUnT9ocCbVJNGckJkXd1uac4OP09
tAPEAuXBuAWGpDAGSmg6pHAAAAFQCpzwjn0rSaLiTq53jx1tsj0RILZwAAAIBiL0Cr7GC7ARztGE9dRkT9oh9
uhuiAzcXrAcZTmxhjGsEtMlAtxKm+rl06pnz2aX9KEzMewJEMuDphOTRnSpMv39XtSW1aSXWtKoGAcQgDsFqK
```

ACCESS CONTROL LISTS

Access Control Lists (ACL) provide packet filtering for IPv4 frames (based on address, protocol, Layer 4 protocol port number or TCP control code), IPv6 frames (based on address, DSCP, next header type, or flow label), or any frames (based on MAC address or Ethernet type). To filter incoming packets, first create an access list, add the required rules, and then bind the list to a specific port.

Configuring Access Control Lists –

An ACL is a sequential list of permit or deny conditions that apply to IP addresses, MAC addresses, or other more specific criteria. This switch tests ingress packets against the conditions in an ACL one by one. A packet will be accepted as soon as it matches a permit rule, or dropped as soon as it matches a deny rule. If no rules match, the packet is accepted.

COMMAND USAGE

The following restrictions apply to ACLs:

- The maximum number of ACLs is 256.
- The maximum number of rules per ACL is 96.
- An ACL can have up to 96 rules. However, due to resource restrictions, the average number of rules bound to the ports should not exceed 20.
- The maximum number of rules (Access Control Entries, or ACEs) stated above is the worst case scenario. In practice, the switch compresses the ACEs in TCAM (a hardware table used to store ACEs), but the actual maximum number of ACEs possible depends on too many factors to be precisely determined. It depends on the amount of hardware resources reserved at runtime for this purpose.

  Auto ACE Compression is a software feature used to compress all the ACEs of an ACL to utilize hardware resources more efficiency. Without compression, one ACE would occupy a fixed number of entries in TCAM. So if one ACL includes 25 ACEs, the ACL would need (25 * n) entries in TCAM, where "n" is the fixed number of TCAM entries needed for one ACE. When compression is employed, before writing the ACE into TCAM, the software compresses the ACEs to reduce the number of required TCAM entries. For example, one ACL may include 128 ACEs which classify a continuous IP address range like 192.168.1.0~255. If compression is disabled, the ACL would occupy (128*n) entries of TCAM, using up nearly all of the hardware resources. When using compression, the 128 ACEs are compressed into one ACE classifying the IP address as 192.168.1.0/24, which requires only "n" entries in TCAM. The above example is an ideal case for compression. The worst case would be if no any ACE can be compressed, in which case the used number of TCAM entries would be the same as without compression. It would also require more time to process the ACEs.

The order in which active ACLs are checked is as follows:

1. User-defined rules in IP and MAC ACLs for ingress ports are checked in parallel.
2. Rules within an ACL are checked in the configured order, from top to bottom.
3. If the result of checking an IP ACL is to permit a packet, but the result of a MAC ACL on the same packet is to deny it, the packet will be denied (because the decision to deny a packet has a higher priority for security reasons). A packet will also be denied if the IP ACL denies it and the MAC ACL accepts it.

SETTING A TIME RANGE

Use the Security > ACL (Configure Time Range) page to sets a time range during which ACL functions are applied.

CLI REFERENCES

- "Time Range" on page 957

COMMAND USAGE

If both an absolute rule and one or more periodic rules are configured for the same time range (i.e., named entry), that entry will only take effect if the current time is within the absolute time range and one of the periodic time ranges.

PARAMETERS

These parameters are displayed:

Add

- **Time-Range Name** – Name of a time range. (Range: 1-30 characters)

Add Rule

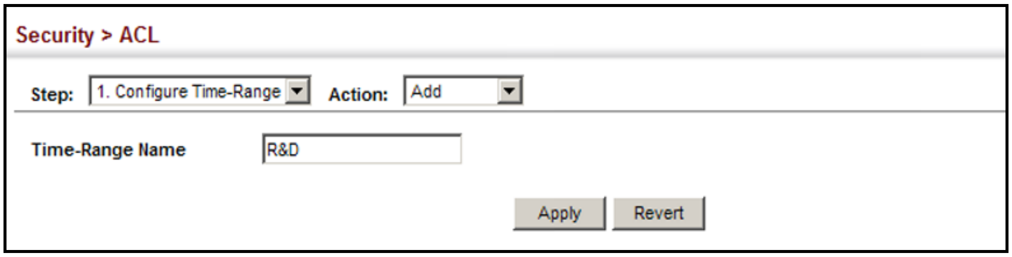
- **Time-Range** – Name of a time range.
- **Mode**
  - **Absolute** – Specifies a specific time or time range.
    - **Start/End** – Specifies the hours, minutes, month, day, and year at which to start or end.
  - **Periodic** – Specifies a periodic interval.
    - **Start/To** – Specifies the days of the week, hours, and minutes at which to start or end.

WEB INTERFACE

To configure a time range:

1. Click Security, ACL.
2. Select Configure Time Range from the Step list.
3. Select Add from the Action list.
4. Enter the name of a time range.
5. Click Apply.

Figure 197: Setting the Name of a Time Range



Security > ACL

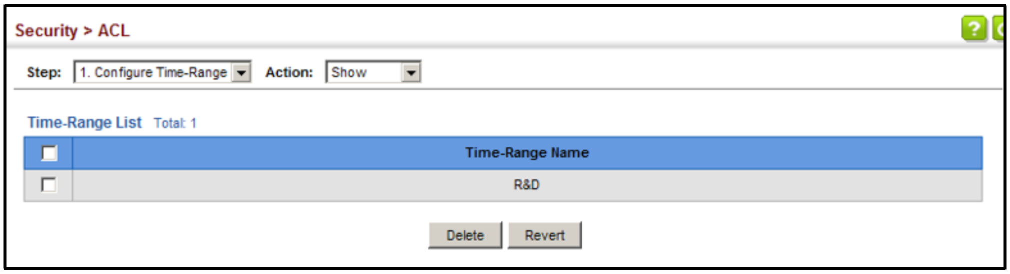
Step: 1. Configure Time-Range Action: Add

Time-Range Name: R&D

To show a list of time ranges:

1. Click Security, ACL.
2. Select Configure Time Range from the Step list.
3. Select Show from the Action list.

Figure 198: Showing a List of Time Ranges



Security > ACL

Step: 1. Configure Time-Range Action: Show

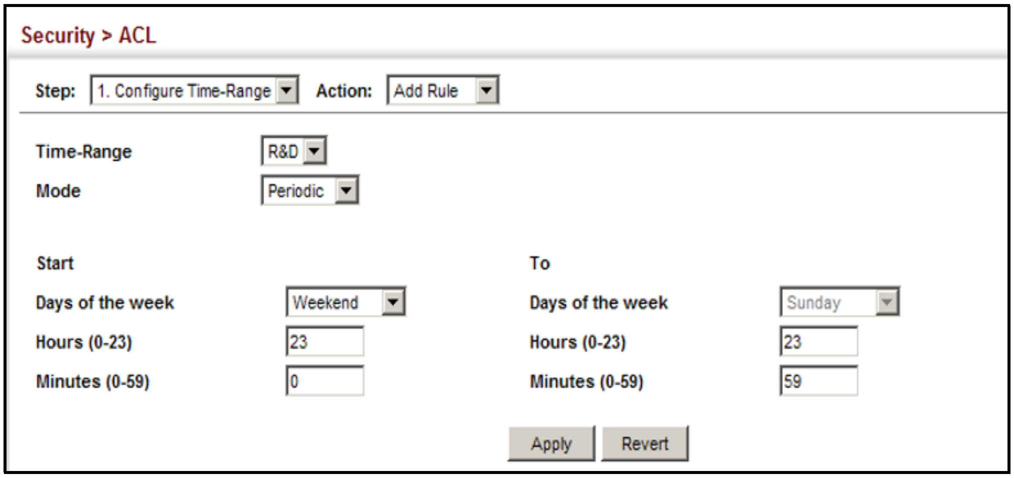
Time-Range List Total: 1

□	Time-Range Name
□	R&D

To configure a rule for a time range:

1. Click Security, ACL.
2. Select Configure Time Range from the Step list.
3. Select Add Rule from the Action list.
4. Select the name of time range from the drop-down list.
5. Select a mode option of Absolute or Periodic.
6. Fill in the required parameters for the selected mode.
7. Click Apply.

Figure 199: Add a Rule to a Time Range



Security > ACL

Step: 1. Configure Time-Range Action: Add Rule

Time-Range: R&D
Mode: Periodic

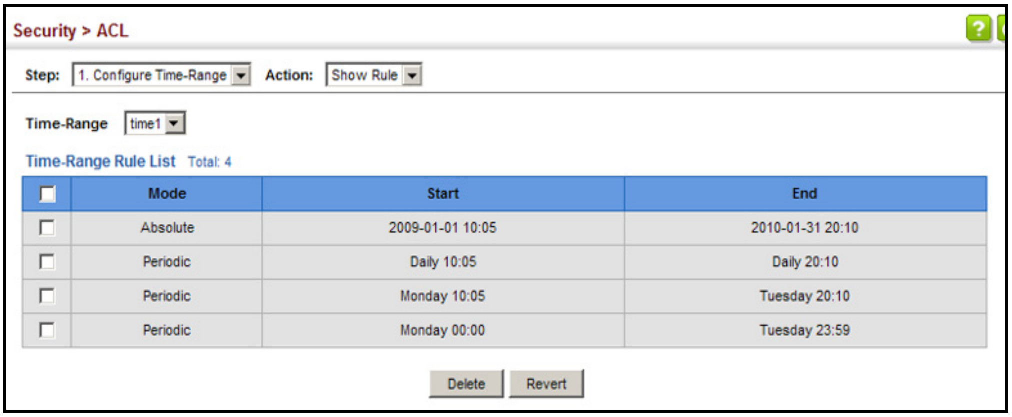
Start
Days of the week: Weekend
Hours (0-23): 23
Minutes (0-59): 0

To
Days of the week: Sunday
Hours (0-23): 23
Minutes (0-59): 59

To show the rules configured for a time range:

1. Click Security, ACL.
2. Select Configure Time Range from the Step list.
3. Select Show Rule from the Action list.

Figure 200: Showing the Rules Configured for a Time Range



Security > ACL

Step: 1. Configure Time-Range Action: Show Rule

Time-Range: time1

Time-Range Rule List Total: 4

□	Mode	Start	End
□	Absolute	2009-01-01 10:05	2010-01-31 20:10
□	Periodic	Daily 10:05	Daily 20:10
□	Periodic	Monday 10:05	Tuesday 20:10
□	Periodic	Monday 00:00	Tuesday 23:59

SHOWING TCAM UTILIZATION

Use the Security > ACL (Configure ACL - Show TCAM) page to show utilization parameters for TCAM (Ternary Content Addressable Memory), including the number policy control entries in use, the number of free entries, and the overall percentage of TCAM in use.

CLI REFERENCES

- "show access-list tcam-utilization" on page 902

COMMAND USAGE

Policy control entries (PCEs) are used by various system functions which rely on rule-based searches, including Access Control Lists (ACLs), IP Source Guard filter rules, Quality of Service (QoS) processes, QinQ, MAC-based VLANs, VLAN translation, or traps.

For example, when binding an ACL to a port, each rule in an ACL will use two PCEs; and when setting an IP Source Guard filter rule for a port, the system will also use two PCEs.

PARAMETERS

These parameters are displayed:

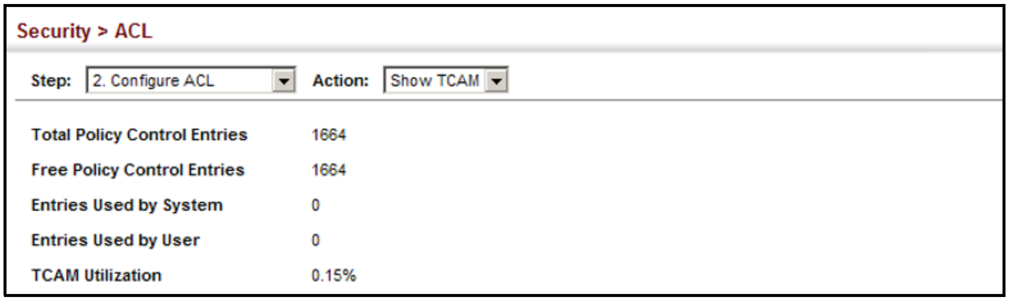
- **Total Policy Control Entries** – The number policy control entries in use.
- **Free Policy Control Entries** – The number of policy control entries available for use.
- **Entries Used by System** – The number of policy control entries used by the operating system.
- **Entries Used by User** – The number of policy control entries used by configuration settings, such as access control lists.
- **TCAM Utilization** – The overall percentage of TCAM in use.

WEB INTERFACE

To show information on TCAM utilization:

1. Click Security, ACL.
2. Select Configure ACL from the Step list.
3. Select Show TCAM from the Action list.

Figure 201: Showing TCAM Utilization



Security > ACL

Step: 2. Configure ACL Action: Show TCAM

Total Policy Control Entries 1664
Free Policy Control Entries 1664
Entries Used by System 0
Entries Used by User 0
TCAM Utilization 0.15%

SETTING THE ACL NAME AND TYPE

Use the Security > ACL (Configure ACL - Add) page to create an ACL.

CLI REFERENCES

- "access-list ip" on page 1164
- "show ip access-list" on page 1169

PARAMETERS

These parameters are displayed:

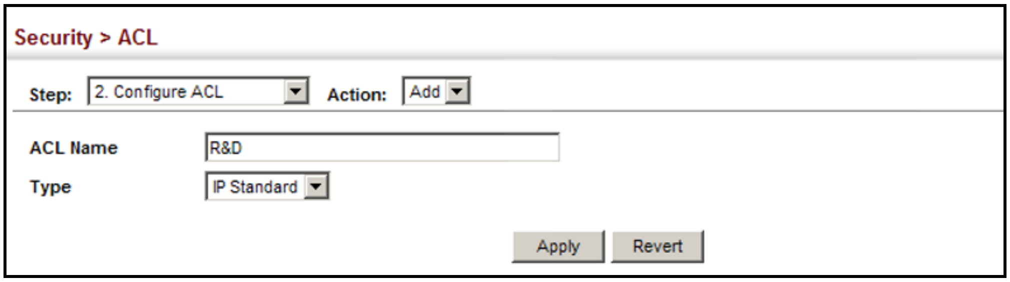
- **ACL Name** – Name of the ACL. (Maximum length: 32 characters)
- **Type** – The following filter modes are supported:
  - **IP Standard**: IPv4 ACL mode filters packets based on the source IPv4 address.
  - **IP Extended**: IPv4 ACL mode filters packets based on the source or destination IPv4 address, as well as the protocol type and protocol port number. If the “TCP” protocol is specified, then you can also filter packets based on the TCP control code.
  - **IPv6 Standard**: IPv6 ACL mode filters packets based on the source IPv6 address.
  - **IPv6 Extended**: IPv6 ACL mode filters packets based on the source or destination IP address, as well as DSCP, next header type, and the flow label (i.e., a request for special handling by IPv6 routers).
  - **MAC** – MAC ACL mode filters packets based on the source or destination MAC address and the Ethernet frame type (RFC 1060).
  - **ARP** – ARP ACL specifies static IP-to-MAC address bindings used for ARP inspection (see "ARP Inspection" on page 410).

WEB INTERFACE

To configure the name and type of an ACL:

1. Click Security, ACL.
2. Select Configure ACL from the Step list.
3. Select Add from the Action list.
4. Fill in the ACL Name field, and select the ACL type.
5. Click Apply.

Figure 202: Creating an ACL



Security > ACL

Step: 2. Configure ACL Action: Add

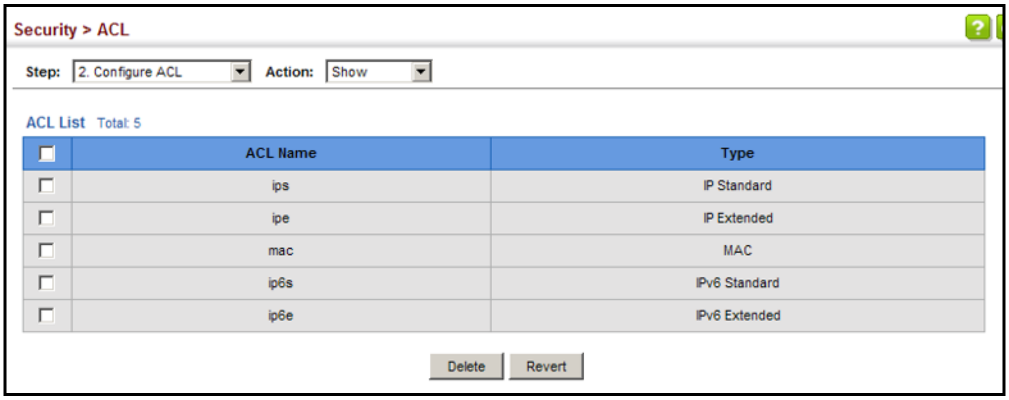
ACL Name: R&D

Type: IP Standard

To show a list of ACLs:

1. Click Security, ACL.
2. Select Configure ACL from the Step list.
3. Select Show from the Action list.

Figure 203: Showing a List of ACLs



Security > ACL

Step: 2. Configure ACL Action: Show

ACL List Total: 5

□	ACL Name	Type
□	ips	IP Standard
□	ipe	IP Extended
□	mac	MAC
□	ip6s	IPv6 Standard
□	ip6e	IPv6 Extended

CONFIGURING A STANDARD IPV4 ACL

Use the Security > ACL (Configure ACL - Add Rule - IP Standard) page to configure a Standard IPv4 ACL.

CLI REFERENCES

- "permit, deny (Standard IP ACL)" on page 1165
- "show ip access-list" on page 1169
- "Time Range" on page 957

PARAMETERS

These parameters are displayed:

- **Type** – Selects the type of ACLs to show in the Name list.
- **Name** – Shows the names of ACLs matching the selected type.
- **Action** – An ACL can contain any combination of permit or deny rules.
- **Address Type** – Specifies the source IP address. Use “Any” to include all possible addresses, “Host” to specify a specific host address in the Address field, or “IP” to specify a range of addresses with the Address and Subnet Mask fields. (Options: Any, Host, IP; Default: Any)
- **Source IP Address** – Source IP address.
- **Source Subnet Mask** – A subnet mask containing four integers from 0 to 255, each separated by a period. The mask uses 1 bits to indicate “match” and 0 bits to indicate “ignore.” The mask is bitwise ANDed with the specified source IP address, and compared with the address for each IP packet entering the port(s) to which this ACL has been assigned.
- **Time Range** – Name of a time range.

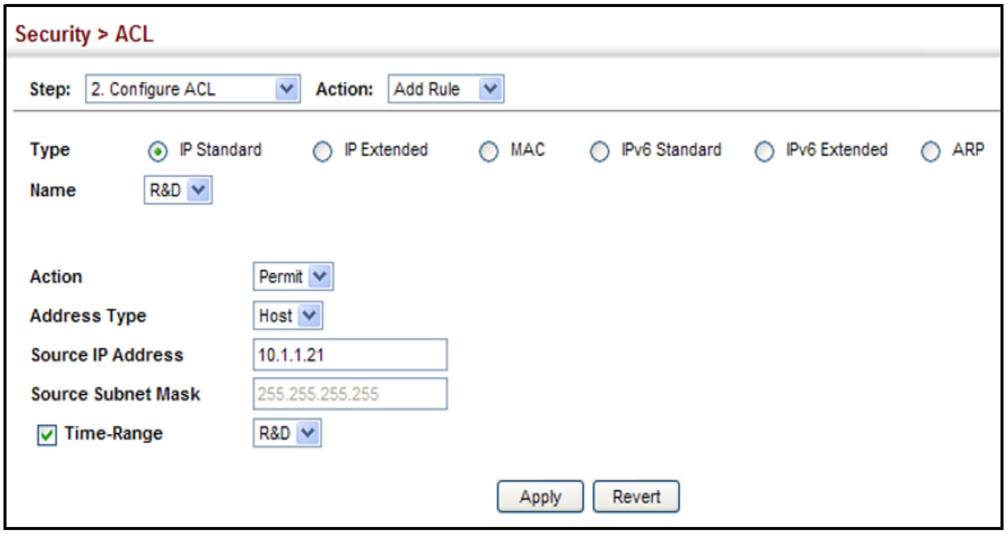
WEB INTERFACE

To add rules to a Standard IPv4 ACL:

1. Click Security, ACL.
2. Select Configure ACL from the Step list.
3. Select Add Rule from the Action list.
4. Select IP Standard from the Type list.
5. Select the name of an ACL from the Name list.
6. Specify the action (i.e., Permit or Deny).
7. Select the address type (Any, Host, or IP).
8. If you select “Host,” enter a specific address. If you select “IP,” enter a subnet address and the mask for an address range.

9. Click Apply.

Figure 204: Configuring a Standard IPv4 ACL



Security > ACL

Step: 2. Configure ACL Action: Add Rule

Type ● IP Standard ○ IP Extended ○ MAC ○ IPv6 Standard ○ IPv6 Extended ○ ARP

Name R&D

Action Permit

Address Type Host

Source IP Address 10.1.1.21

Source Subnet Mask 255.255.255.255

☑ Time-Range R&D

CONFIGURING AN EXTENDED IPV4 ACL

Use the Security > ACL (Configure ACL - Add Rule - IP Extended) page to configure an Extended IPv4 ACL.

CLI REFERENCES

- "permit, deny (Extended IPv4 ACL)" on page 1166
- "show ip access-list" on page 1169
- "Time Range" on page 957

PARAMETERS

These parameters are displayed:

- **Type** – Selects the type of ACLs to show in the Name list.
- **Name** – Shows the names of ACLs matching the selected type.
- **Action** – An ACL can contain any combination of permit or deny rules.
- **Source/Destination Address Type** – Specifies the source or destination IP address type. Use “Any” to include all possible addresses, “Host” to specify a specific host address in the Address field, or “IP” to specify a range of addresses with the Address and Subnet Mask fields. (Options: Any, Host, IP; Default: Any)
- **Source/Destination IP Address** – Source or destination IP address.
- **Source/Destination Subnet Mask** – Subnet mask for source or destination address. (See the description for Subnet Mask on page 397.)
- **Source/Destination Port** – Source/destination port number for the specified protocol type. (Range: 0-65535)

- **Source/Destination Port Bit Mask** – Decimal number representing the port bits to match. (Range: 0-65535)

- **Protocol** – Specifies the protocol type to match as TCP, UDP or Others, where others indicates a specific protocol number (0-255). (Options: TCP, UDP, Others; Default: Others)

- **Service Type** – Packet priority settings based on the following criteria:
  - **ToS** – Type of Service level. (Range: 0-15)
  - **Precedence** – IP precedence level. (Range: 0-7)
  - **DSCP** – DSCP priority level. (Range: 0-63)

- **Control Code** – Decimal number (representing a bit string) that specifies flag bits in byte 14 of the TCP header. (Range: 0-63)

- **Control Code Bit Mask** – Decimal number representing the code bits to match. (Range: 0-63)

  The control bit mask is a decimal number (for an equivalent binary bit mask) that is applied to the control code. Enter a decimal number, where the equivalent binary bit "1" means to match a bit and "0" means to ignore a bit. The following bits may be specified:

  - 1 (fin) – Finish
  - 2 (syn) – Synchronize
  - 4 (rst) – Reset
  - 8 (psh) – Push
  - 16 (ack) – Acknowledgement
  - 32 (urg) – Urgent pointer

  For example, use the code value and mask below to catch packets with the following flags set:

  - SYN flag valid, use control-code 2, control bit mask 2
  - Both SYN and ACK valid, use control-code 18, control bit mask 18
  - SYN valid and ACK invalid, use control-code 2, control bit mask 18

- **Time Range** – Name of a time range.

WEB INTERFACE

To add rules to an IPv4 Extended ACL:

1. Click Security, ACL.

2. Select Configure ACL from the Step list.

3. Select Add Rule from the Action list.

4. Select IP Extended from the Type list.

5. Select the name of an ACL from the Name list.

6. Specify the action (i.e., Permit or Deny).

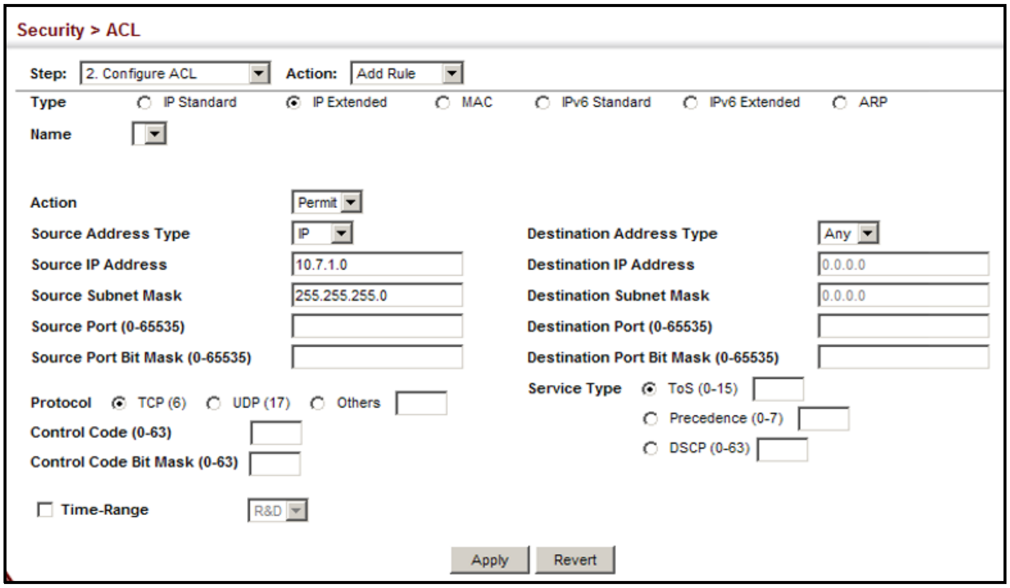
7. Select the address type (Any, Host, or IP).

8. If you select “Host,” enter a specific address. If you select “IP,” enter a subnet address and the mask for an address range.

9. Set any other required criteria, such as service type, protocol type, or control code.

10. Click Apply.

Figure 205: Configuring an Extended IPv4 ACL



Security > ACL

Step: 2. Configure ACL   Action: Add Rule

Type ○ IP Standard ● IP Extended ○ MAC ○ IPv6 Standard ○ IPv6 Extended ○ ARP

Name

Action: Permit

Source Address Type: IP   Destination Address Type: Any

Source IP Address: 10.7.1.0   Destination IP Address: 0.0.0.0

Source Subnet Mask: 255.255.255.0   Destination Subnet Mask: 0.0.0.0

Source Port (0-65535)   Destination Port (0-65535)

Source Port Bit Mask (0-65535)   Destination Port Bit Mask (0-65535)

Protocol ● TCP (6) ○ UDP (17) ○ Others   Service Type ● ToS (0-15) ○ Precedence (0-7) ○ DSCP (0-63)

Control Code (0-63)

Control Code Bit Mask (0-63)

□ Time-Range R&D

CONFIGURING A STANDARD IPV6 ACL

Use the Security > ACL (Configure ACL - Add Rule - IPv6 Standard) page to configure a Standard IPv6ACL.

CLI REFERENCES

- "permit, deny (Standard IPv6 ACL)" on page 1171
- "show ipv6 access-list" on page 1175
- "Time Range" on page 957

PARAMETERS

These parameters are displayed in the web interface:

- **Type** – Selects the type of ACLs to show in the Name list.
- **Name** – Shows the names of ACLs matching the selected type.
- **Action** – An ACL can contain any combination of permit or deny rules.

- **Source Address Type** – Specifies the source IP address. Use "Any" to include all possible addresses, "Host" to specify a specific host address in the Address field, or "IPv6-Prefix" to specify a range of addresses. (Options: Any, Host, IPv6-Prefix; Default: Any)

- **Source IPv6 Address** – An IPv6 source address or network class. The address must be formatted according to RFC 2373 "IPv6 Addressing Architecture," using 8 colon-separated 16-bit hexadecimal values. One double colon may be used in the address to indicate the appropriate number of zeros required to fill the undefined fields.

- **Source Prefix-Length** – A decimal value indicating how many contiguous bits (from the left) of the address comprise the prefix (i.e., the network portion of the address). (Range: 0-128 bits)

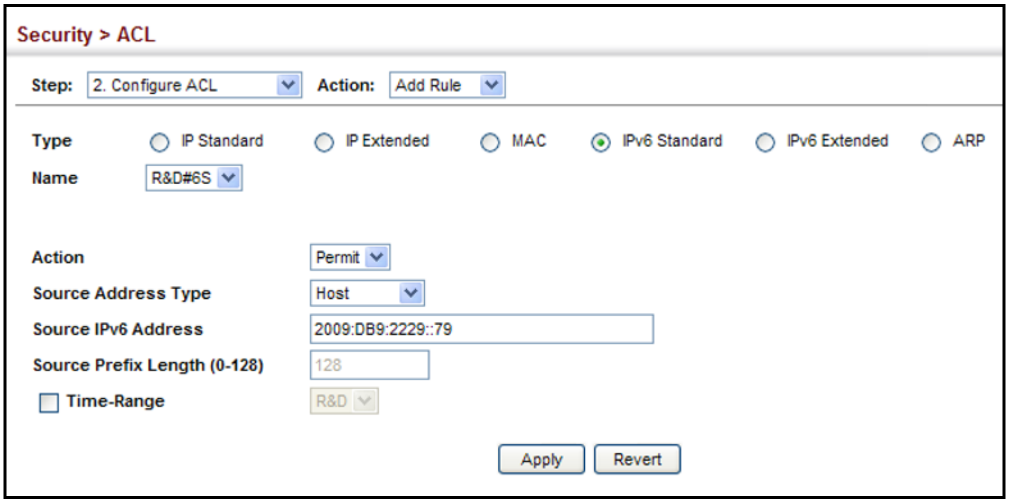
- **Time Range** – Name of a time range.

WEB INTERFACE

To add rules to a Standard IPv6 ACL:

1. Click Security, ACL.
2. Select Configure ACL from the Step list.
3. Select Add Rule from the Action list.
4. Select IPv6 Standard from the Type list.
5. Select the name of an ACL from the Name list.
6. Specify the action (i.e., Permit or Deny).
7. Select the source address type (Any, Host, or IPv6-prefix).
8. If you select "Host," enter a specific address. If you select "IPv6-prefix," enter a subnet address and the prefix length.
9. Click Apply.

Figure 206: Configuring a Standard IPv6 ACL



Security > ACL

Step: 2. Configure ACL Action: Add Rule

Type ○ IP Standard ○ IP Extended ○ MAC ● IPv6 Standard ○ IPv6 Extended ○ ARP

Name R&D#6S

Action Permit

Source Address Type Host

Source IPv6 Address 2009:DB9:2229::79

Source Prefix Length (0-128) 128

□ Time-Range R&D

Configuring an Extended IPv6 ACL

Use the Security > ACL (Configure ACL - Add Rule - IPv6 Extended) page to configure an Extended IPv6 ACL.

CLI References

- "permit, deny (Extended IPv6 ACL)" on page 1172
- "show ipv6 access-list" on page 1175
- "Time Range" on page 957

Parameters

These parameters are displayed in the web interface:

- **Type** – Selects the type of ACLs to show in the Name list.
- **Name** – Shows the names of ACLs matching the selected type.
- **Action** – An ACL can contain any combination of permit or deny rules.
- **Destination Address Type** – Specifies the destination IP address type. Use “Any” to include all possible addresses, or “IPv6-Prefix” to specify a range of addresses. (Options: Any, IPv6-Prefix; Default: Any)
- **Destination IPv6 Address** – An IPv6 address or network class. The address must be formatted according to RFC 2373 “IPv6 Addressing Architecture,” using 8 colon-separated 16-bit hexadecimal values. One double colon may be used in the address to indicate the appropriate number of zeros required to fill the undefined fields.
- **Destination Prefix-Length** – A decimal value indicating how many contiguous bits (from the left) of the address comprise the prefix; i.e., the network portion of the address. (Range: 0-64 bits)
- **DSCP** – DSCP traffic class. (Range: 0-63)

- **Next Header** – Identifies the type of header immediately following the IPv6 header. (Range: 0-255)

  Optional internet-layer information is encoded in separate headers that may be placed between the IPv6 header and the upper-layer header in a packet. There are a small number of such extension headers, each identified by a distinct Next Header value. IPv6 supports the values defined for the IPv4 Protocol field in RFC 1700, and includes these commonly used headers:

  0 : Hop-by-Hop Options (RFC 2460)
  6 : TCP Upper-layer Header (RFC 1700)
  17 : UDP Upper-layer Header (RFC 1700)
  43 : Routing (RFC 2460)
  44 : Fragment (RFC 2460)
  50 : Encapsulating Security Payload (RFC 2406)
  51 : Authentication (RFC 2402)
  60 : Destination Options (RFC 2460)

- **Flow Label** – A label for packets belonging to a particular traffic “flow” for which the sender requests special handling by IPv6 routers, such as non-default quality of service or “real-time” service (see RFC 2460). (Range: 0-1048575)

  A flow label is assigned to a flow by the flow's source node. New flow labels must be chosen pseudo-randomly and uniformly from the range 1 to FFFFF hexadecimal. The purpose of the random allocation is to make any set of bits within the Flow Label field suitable for use as a hash key by routers, for looking up the state associated with the flow.

  A flow identifies a sequence of packets sent from a particular source to a particular (unicast or multicast) destination for which the source desires special handling by the intervening routers. The nature of that special handling might be conveyed to the routers by a control protocol, such as a resource reservation protocol, or by information within the flow's packets themselves, e.g., in a hop-by-hop option. A flow is uniquely identified by the combination of a source address and a non-zero flow label. Packets that do not belong to a flow carry a flow label of zero.

  Hosts or routers that do not support the functions specified by the flow label must set the field to zero when originating a packet, pass the field on unchanged when forwarding a packet, and ignore the field when receiving a packet.

WEB INTERFACE

To add rules to an Extended IPv6 ACL:

1. Click Security, ACL.

2. Select Configure ACL from the Step list.

3. Select Add Rule from the Action list.

4. Select IPv6 Extended from the Type list.

5. Select the name of an ACL from the Name list.

6. Specify the action (i.e., Permit or Deny).

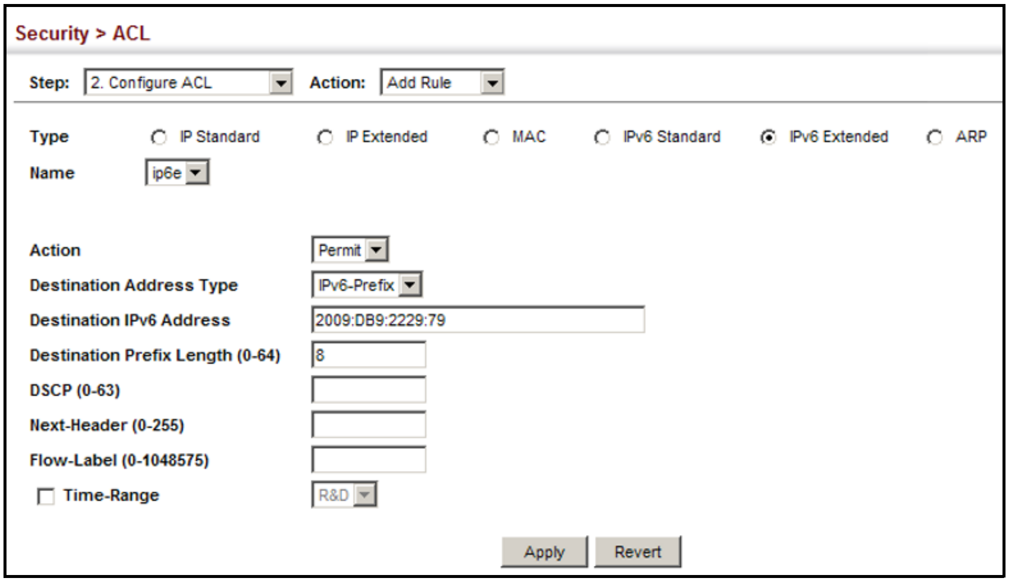
7. Select the address type (Any or IPv6-prefix).

8. If you select “Host,” enter a specific address. If you select “IPv6-prefix,” enter a subnet address and prefix length.

9. Set any other required criteria, such as DSCP, next header type, or flow label.

10. Click Apply.

Figure 207: Configuring an Extended IPv6 ACL



Security > ACL

Step: 2. Configure ACL Action: Add Rule

Type ○ IP Standard ○ IP Extended ○ MAC ○ IPv6 Standard ● IPv6 Extended ○ ARP

Name: ip6e

Action: Permit

Destination Address Type: IPv6-Prefix

Destination IPv6 Address: 2009:DB9:2229:79

Destination Prefix Length (0-64): 8

DSCP (0-63):

Next-Header (0-255):

Flow-Label (0-1048575):

□ Time-Range: R&D

CONFIGURING A MAC ACL

Use the Security > ACL (Configure ACL - Add Rule - MAC) page to configure a MAC ACL based on hardware addresses, packet format, and Ethernet type.

CLI REFERENCES

- "permit, deny (MAC ACL)" on page 1177
- "show ip access-list" on page 1169
- "Time Range" on page 957

PARAMETERS

These parameters are displayed:

- **Type** – Selects the type of ACLs to show in the Name list.
- **Name** – Shows the names of ACLs matching the selected type.
- **Action** – An ACL can contain any combination of permit or deny rules.

- **Source/Destination Address Type** – Use "Any" to include all possible addresses, "Host" to indicate a specific MAC address, or "MAC" to specify an address range with the Address and Bit Mask fields. (Options: Any, Host, MAC; Default: Any)

- **Source/Destination MAC Address** – Source or destination MAC address.

- **Source/Destination Bit Mask** – Hexadecimal mask for source or destination MAC address.

- **Packet Format** – This attribute includes the following packet types:
  - **Any** – Any Ethernet packet type.
  - **Untagged-eth2** – Untagged Ethernet II packets.
  - **Untagged-802.3** – Untagged Ethernet 802.3 packets.
  - **Tagged-eth2** – Tagged Ethernet II packets.
  - **Tagged-802.3** – Tagged Ethernet 802.3 packets.

- **VID** – VLAN ID. (Range: 1-4094)

- **VID Bit Mask** – VLAN bit mask. (Range: 0-4095)

- **Ethernet Type** – This option can only be used to filter Ethernet II formatted packets. (Range: 0-ffff hex.)

  A detailed listing of Ethernet protocol types can be found in RFC 1060. A few of the more common types include 0800 (IP), 0806 (ARP), 8137 (IPX).

- **Ethernet Type Bit Mask** – Protocol bit mask. (Range: 0-ffff hex.)

- **Time Range** – Name of a time range.

WEB INTERFACE

To add rules to a MAC ACL:

1. Click Security, ACL.

2. Select Configure ACL from the Step list.

3. Select Add Rule from the Action list.

4. Select MAC from the Type list.

5. Select the name of an ACL from the Name list.

6. Specify the action (i.e., Permit or Deny).

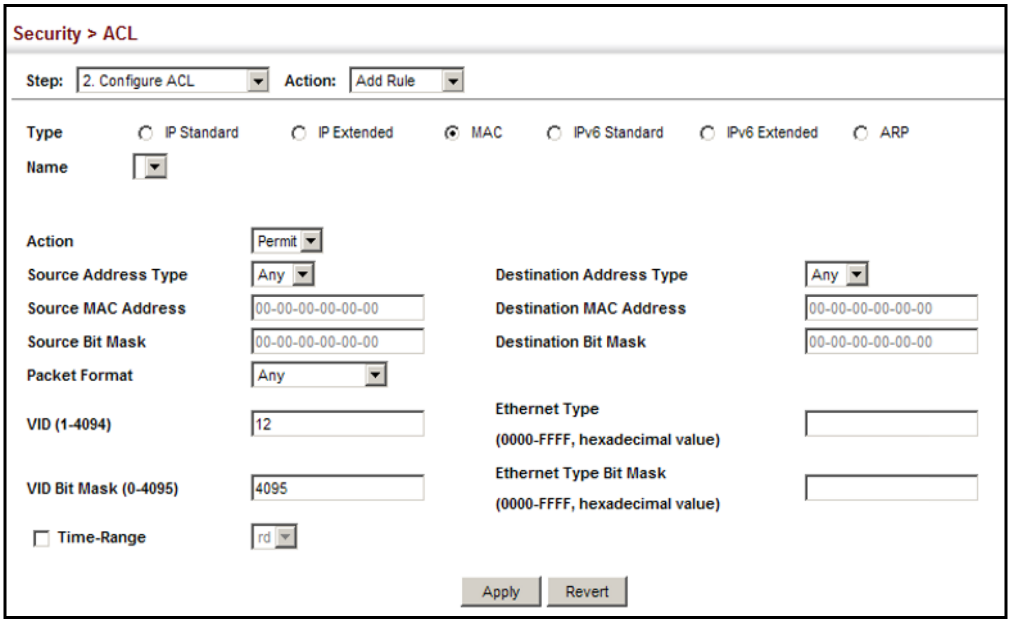
7. Select the address type (Any, Host, or MAC).

8. If you select "Host," enter a specific address (e.g., 11-22-33-44-55-66). If you select "MAC," enter a base address and a hexadecimal bit mask for an address range.

9. Set any other required criteria, such as VID, Ethernet type, or packet format.

10. Click Apply.

Figure 208: Configuring a MAC ACL



Security > ACL

Step: 2. Configure ACL Action: Add Rule

Type ○ IP Standard ○ IP Extended ● MAC ○ IPv6 Standard ○ IPv6 Extended ○ ARP

Name

Action	Permit		
Source Address Type	Any	Destination Address Type	Any
Source MAC Address	00-00-00-00-00-00	Destination MAC Address	00-00-00-00-00-00
Source Bit Mask	00-00-00-00-00-00	Destination Bit Mask	00-00-00-00-00-00
Packet Format	Any		
VID (1-4094)	12	Ethernet Type (0000-FFFF, hexadecimal value)	
VID Bit Mask (0-4095)	4095	Ethernet Type Bit Mask (0000-FFFF, hexadecimal value)	
□ Time-Range	rd		

CONFIGURING AN ARP ACL

Use the Security > ACL (Configure ACL - Add Rule - ARP) page to configure ACLs based on ARP message addresses. ARP Inspection can then use these ACLs to filter suspicious traffic (see "Configuring Global Settings for ARP Inspection" on page 411).

CLI REFERENCES

- "permit, deny (ARP ACL)" on page 1182
- "show ip access-list" on page 1169
- "Time Range" on page 957

PARAMETERS

These parameters are displayed:

- **Type** – Selects the type of ACLs to show in the Name list.

- **Name** – Shows the names of ACLs matching the selected type.

- **Action** – An ACL can contain any combination of permit or deny rules.

- **Packet Type** – Indicates an ARP request, ARP response, or either type. (Range: Request, Response, All; Default: Request)

- **Source/Destination IP Address Type** – Specifies the source or destination IPv4 address. Use “Any” to include all possible addresses, “Host” to specify a specific host address in the Address field, or “IP” to specify a range of addresses with the Address and Mask fields. (Options: Any, Host, IP; Default: Any)

- **Source/Destination IP Address** – Source or destination IP address.

- **Source/Destination IP Subnet Mask** – Subnet mask for source or destination address. (See the description for Subnet Mask on page 397.)

- **Source/Destination MAC Address Type** – Use “Any” to include all possible addresses, “Host” to indicate a specific MAC address, or “MAC” to specify an address range with the Address and Mask fields. (Options: Any, Host, MAC; Default: Any)

- **Source/Destination MAC Address** – Source or destination MAC address.

- **Source/Destination MAC Bit Mask** – Hexadecimal mask for source or destination MAC address.

- **Log** – Logs a packet when it matches the access control entry.

WEB INTERFACE

To add rules to an ARP ACL:

1. Click Security, ACL.

2. Select Configure ACL from the Step list.

3. Select Add Rule from the Action list.

4. Select ARP from the Type list.

5. Select the name of an ACL from the Name list.

6. Specify the action (i.e., Permit or Deny).

7. Select the packet type (Request, Response, All).

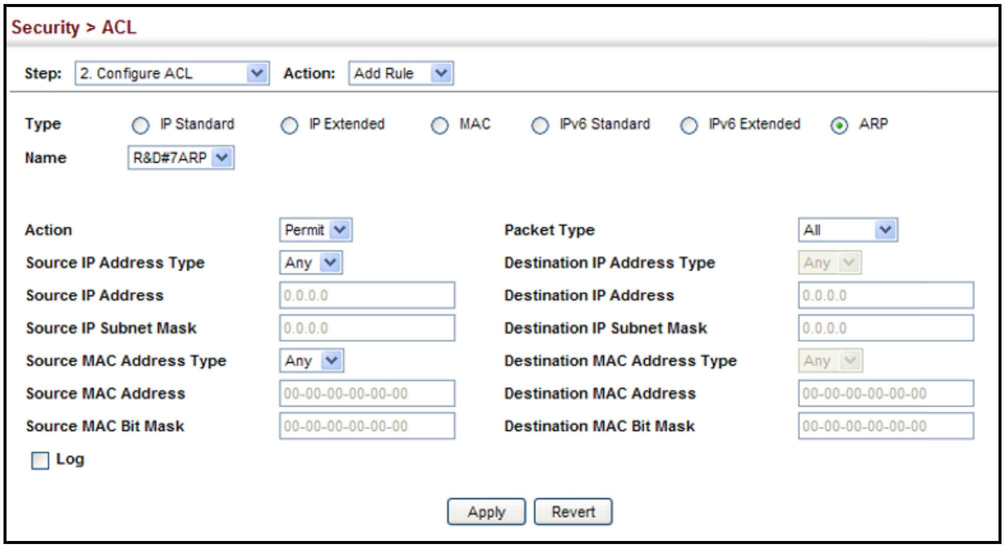
8. Select the address type (Any, Host, or IP).

9. If you select “Host,” enter a specific address (e.g., 11-22-33-44-55-66). If you select “IP,” enter a base address and a hexadecimal bit mask for an address range.

10. Enable logging if required.

11. Click Apply.

Figure 209: Configuring a ARP ACL



Security > ACL

Step: 2. Configure ACL Action: Add Rule

Type ○ IP Standard ○ IP Extended ○ MAC ○ IPv6 Standard ○ IPv6 Extended ● ARP

Name R&D#7ARP

Action	Permit	Packet Type	All
Source IP Address Type	Any	Destination IP Address Type	Any
Source IP Address	0.0.0.0	Destination IP Address	0.0.0.0
Source IP Subnet Mask	0.0.0.0	Destination IP Subnet Mask	0.0.0.0
Source MAC Address Type	Any	Destination MAC Address Type	Any
Source MAC Address	00-00-00-00-00-00	Destination MAC Address	00-00-00-00-00-00
Source MAC Bit Mask	00-00-00-00-00-00	Destination MAC Bit Mask	00-00-00-00-00-00

□ Log

BINDING A PORT TO AN ACCESS CONTROL LIST

After configuring ACLs, use the Security > ACL (Configure Interface) page to bind the ports that need to filter traffic to the appropriate ACLs. You can assign one IP access list and one MAC access list to any port.

CLI REFERENCES

- "ip access-group" on page 1168
- "show ip access-group" on page 1169
- "mac access-group" on page 1179
- "show mac access-group" on page 1180
- "Time Range" on page 957

PARAMETERS

These parameters are displayed:

- **Type** – Selects the type of ACLs to bind to a port.
- **Port** – Port identifier.
- **ACL** – ACL used for ingress or egress packets.
- **Time Range** – Name of a time range.
- **Counter** – Enables counter for ACL statistics.

WEB INTERFACE

To bind an ACL to a port:

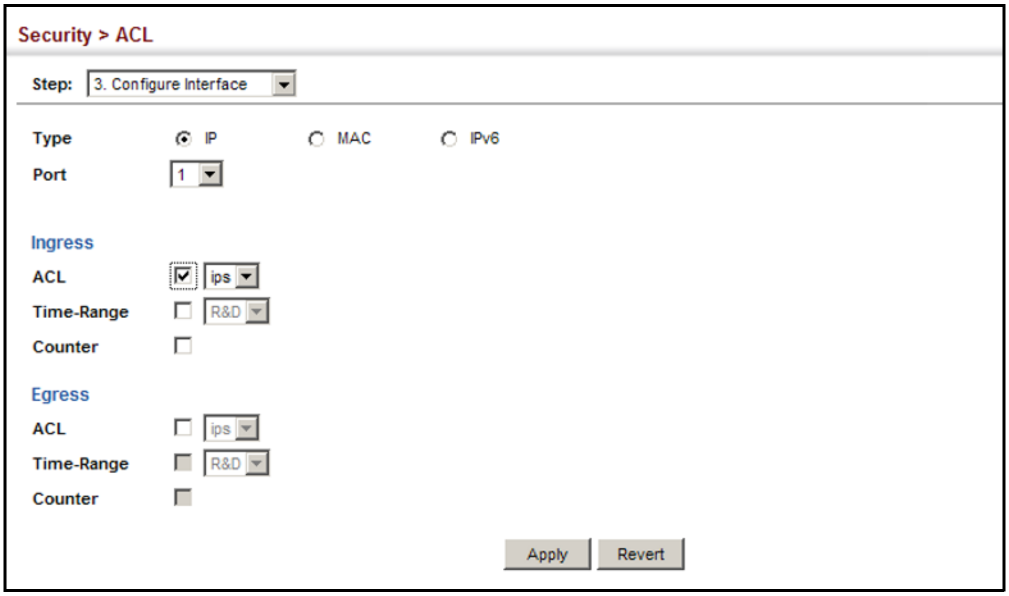
1. Click Security, ACL.
2. Select Configure Interface from the Step list.
3. Select IP, MAC or IPv6 from the Type list.

4. Select a port.

5. Select the name of an ACL from the ACL list.

6. Click Apply.

Figure 210: Binding a Port to an ACL



Security > ACL

Step: 3. Configure Interface

Type ● IP ○ MAC ○ IPv6

Port 1

Ingress

ACL ☑ ips

Time-Range □ R&D

Counter □

Egress

ACL □ ips

Time-Range □ R&D

Counter □

SHOWING ACL HARDWARE COUNTERS

Use the Security > ACL > Configure Interface (Show Hardware Counters) page to show statistics for ACL hardware counters.

CLI REFERENCES

- "show access-list" on page 1185

PARAMETERS

These parameters are displayed:

- **Port** – Port identifier. (Range: 1-12)

- **Type** – ACL type. (IP Standard, IP Extended, MAC, IPv6 Standard, or IPv6 Extended)

- **Direction** – Displays statistics for ingress or egress traffic.

- **ACL Name** – The ACL bound to this port.

- **Action** – Shows if action is to permit or deny specified packets.

- *Rules* – Shows the rules for the ACL bound to this port.

- **Time Range** – The time during which this ACL is applied.

- **Hit** – Shows the number of packets matching this ACL.[5]

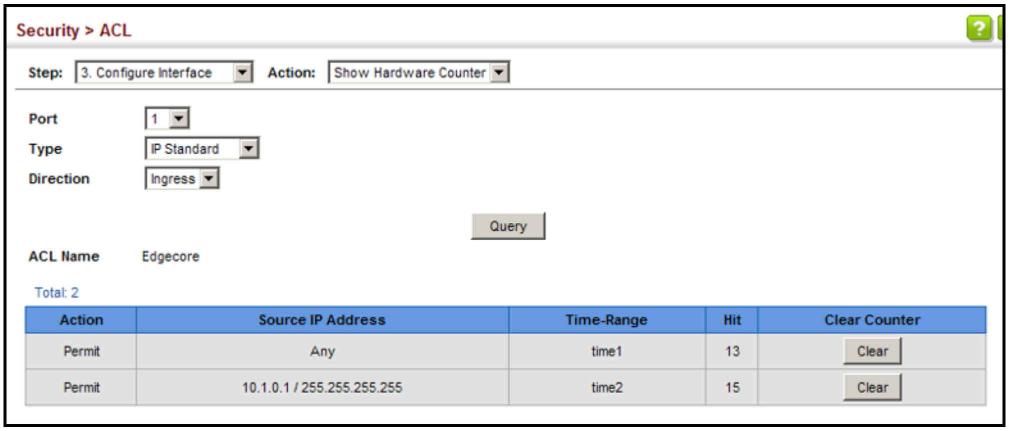
- **Clear Counter** – Clears hit counter for rules in specified ACL.

WEB INTERFACE

To show statistics for ACL hardware counters:

1. Click Security, ACL.
2. Select Configure Interface from the Step list.
3. Select Show Hardware Counters from the Action list.
4. Select a port.
5. Select ingress or egress traffic.

Figure 211: Showing ACL Statistics



Security > ACL

Step: 3. Configure Interface Action: Show Hardware Counter

Port: 1
Type: IP Standard
Direction: Ingress

ACL Name: Edgecore

Total: 2

Action	Source IP Address	Time-Range	Hit	Clear Counter
Permit	Any	time1	13	Clear
Permit	10.1.0.1 / 255.255.255.255	time2	15	Clear

ARP INSPECTION

ARP Inspection is a security feature that validates the MAC Address bindings for Address Resolution Protocol packets. It provides protection against ARP traffic with invalid MAC-to-IP address bindings, which forms the basis for certain "man-in-the-middle" attacks. This is accomplished by intercepting all ARP requests and responses and verifying each of these packets before the local ARP cache is updated or the packet is forwarded to the appropriate destination. Invalid ARP packets are dropped.

ARP Inspection determines the validity of an ARP packet based on valid IP-to-MAC address bindings stored in a trusted database – the DHCP snooping binding database (see "DHCP Snooping Configuration" on page 446). This database is built by DHCP snooping if it is enabled on globally on the switch and on the required VLANs. ARP Inspection can also validate ARP packets against user-configured ARP access control lists (ACLs) for hosts with statically configured addresses (see "Configuring an ARP ACL" on page 406).

[5] Due to a hardware limitation, statistics are only displayed for permit rules.

COMMAND USAGE

Enabling & Disabling ARP Inspection

- ARP Inspection is controlled on a global and VLAN basis.
- By default, ARP Inspection is disabled both globally and on all VLANs.
  - If ARP Inspection is globally enabled, then it becomes active only on the VLANs where it has been enabled.
  - When ARP Inspection is enabled globally, all ARP request and reply packets on inspection-enabled VLANs are redirected to the CPU and their switching behavior handled by the ARP Inspection engine.
  - If ARP Inspection is disabled globally, then it becomes inactive for all VLANs, including those where inspection is enabled.
  - When ARP Inspection is disabled, all ARP request and reply packets will bypass the ARP Inspection engine and their switching behavior will match that of all other packets.
  - Disabling and then re-enabling global ARP Inspection will not affect the ARP Inspection configuration of any VLANs.
  - When ARP Inspection is disabled globally, it is still possible to configure ARP Inspection for individual VLANs. These configuration changes will only become active after ARP Inspection is enabled globally again.
- The ARP Inspection engine in the current firmware version does not support ARP Inspection on trunk ports.

CONFIGURING GLOBAL SETTINGS FOR ARP INSPECTION

Use the Security > ARP Inspection (Configure General) page to enable ARP inspection globally for the switch, to validate address information in each packet, and configure logging.

CLI REFERENCES

- "ARP Inspection" on page 1145

COMMAND USAGE

ARP Inspection Validation

- By default, ARP Inspection Validation is disabled.
- Specifying at least one of the following validations enables ARP Inspection Validation globally. Any combination of the following checks can be active concurrently.
  - Destination MAC – Checks the destination MAC address in the Ethernet header against the target MAC address in the ARP body. This check is performed for ARP responses. When enabled, packets

with different MAC addresses are classified as invalid and are dropped.

- IP – Checks the ARP body for invalid and unexpected IP addresses. These addresses include 0.0.0.0, 255.255.255.255, and all IP multicast addresses. Sender IP addresses are checked in all ARP requests and responses, while target IP addresses are checked only in ARP responses.
- Source MAC – Checks the source MAC address in the Ethernet header against the sender MAC address in the ARP body. This check is performed on both ARP requests and responses. When enabled, packets with different MAC addresses are classified as invalid and are dropped.

ARP Inspection Logging

- By default, logging is active for ARP Inspection, and cannot be disabled.
- The administrator can configure the log facility rate.
- When the switch drops a packet, it places an entry in the log buffer, then generates a system message on a rate-controlled basis. After the system message is generated, the entry is cleared from the log buffer.
- Each log entry contains flow information, such as the receiving VLAN, the port number, the source and destination IP addresses, and the source and destination MAC addresses.
- If multiple, identical invalid ARP packets are received consecutively on the same VLAN, then the logging facility will only generate one entry in the log buffer and one corresponding system message.
- If the log buffer is full, the oldest entry will be replaced with the newest entry.

PARAMETERS

These parameters are displayed:

- **ARP Inspection Status** – Enables ARP Inspection globally. (Default: Disabled)
- **ARP Inspection Validation** – Enables extended ARP Inspection Validation if any of the following options are enabled. (Default: Disabled)
  - **Dst-MAC** – Validates the destination MAC address in the Ethernet header against the target MAC address in the body of ARP responses.
  - **IP** – Checks the ARP body for invalid and unexpected IP addresses. Sender IP addresses are checked in all ARP requests and responses, while target IP addresses are checked only in ARP responses.

- **Allow Zeros** – Allows sender IP address to be 0.0.0.0.
- **Src-MAC** – Validates the source MAC address in the Ethernet header against the sender MAC address in the ARP body. This check is performed on both ARP requests and responses.

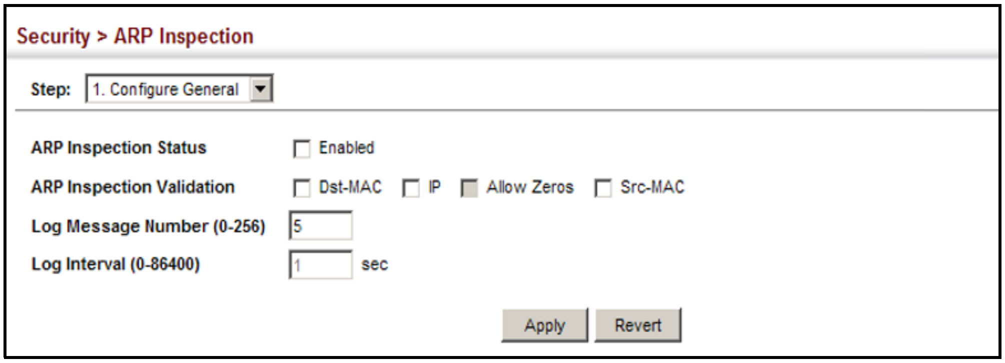
- **Log Message Number** – The maximum number of entries saved in a log message. (Range: 0-256; Default: 5)
- **Log Interval** – The interval at which log messages are sent. (Range: 0-86400 seconds; Default: 1 second)

WEB INTERFACE

To configure global settings for ARP Inspection:

1. Click Security, ARP Inspection.
2. Select Configure General from the Step list.
3. Enable ARP inspection globally, enable any of the address validation options, and adjust any of the logging parameters if required.
4. Click Apply.

Figure 212: Configuring Global Settings for ARP Inspection



Security > ARP Inspection

Step: 1. Configure General

ARP Inspection Status □ Enabled

ARP Inspection Validation □ Dst-MAC □ IP □ Allow Zeros □ Src-MAC

Log Message Number (0-256) 5

Log Interval (0-86400) 1 sec

CONFIGURING VLAN SETTINGS FOR ARP INSPECTION

Use the Security > ARP Inspection (Configure VLAN) page to enable ARP inspection for any VLAN and to specify the ARP ACL to use.

CLI REFERENCES

- "ARP Inspection" on page 1145

COMMAND USAGE

ARP Inspection VLAN Filters (ACLs)

- By default, no ARP Inspection ACLs are configured and the feature is disabled.

- ARP Inspection ACLs are configured within the ARP ACL configuration page (see page 406).

- ARP Inspection ACLs can be applied to any configured VLAN.

- ARP Inspection uses the DHCP snooping bindings database for the list of valid IP-to-MAC address bindings. ARP ACLs take precedence over entries in the DHCP snooping bindings database. The switch first compares ARP packets to any specified ARP ACLs.

- If *Static* is specified, ARP packets are only validated against the selected ACL – packets are filtered according to any matching rules, packets not matching any rules are dropped, and the DHCP snooping bindings database check is bypassed.

- If *Static* is not specified, ARP packets are first validated against the selected ACL; if no ACL rules match the packets, then the DHCP snooping bindings database determines their validity.

PARAMETERS

These parameters are displayed:

- **ARP Inspection VLAN ID** – Selects any configured VLAN. (Default: 1)

- **ARP Inspection VLAN Status** – Enables ARP Inspection for the selected VLAN. (Default: Disabled)

- **ARP Inspection ACL Name**

  - *ARP ACL* – Allows selection of any configured ARP ACLs. (Default: None)

  - **Static** – When an ARP ACL is selected, and static mode also selected, the switch only performs ARP Inspection and bypasses validation against the DHCP Snooping Bindings database. When an ARP ACL is selected, but static mode is not selected, the switch first performs ARP Inspection and then validation against the DHCP Snooping Bindings database. (Default: Disabled)

WEB INTERFACE

To configure VLAN settings for ARP Inspection:

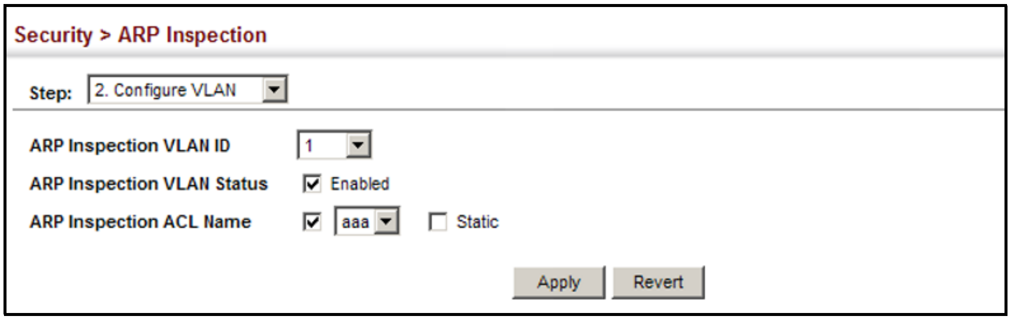
1. Click Security, ARP Inspection.

2. Select Configure VLAN from the Step list.

3. Enable ARP inspection for the required VLANs, select an ARP ACL filter to check for configured addresses, and select the Static option to bypass checking the DHCP snooping bindings database if required.

4. Click Apply.

Figure 213: Configuring VLAN Settings for ARP Inspection



Security > ARP Inspection

Step: 2. Configure VLAN

ARP Inspection VLAN ID: 1

ARP Inspection VLAN Status: ☑ Enabled

ARP Inspection ACL Name: ☑ aaa □ Static

CONFIGURING INTERFACE SETTINGS FOR ARP INSPECTION

Use the Security > ARP Inspection (Configure Interface) page to specify the ports that require ARP inspection, and to adjust the packet inspection rate.

CLI REFERENCES

- "ARP Inspection" on page 1145

PARAMETERS

These parameters are displayed:

- **Interface** – Port or trunk identifier.
- **Trust Status** – Configures the port as trusted or untrusted. (Default: Untrusted)

  By default, all untrusted ports are subject to ARP packet rate limiting, and all trusted ports are exempt from ARP packet rate limiting.

  Packets arriving on trusted interfaces bypass all ARP Inspection and ARP Inspection Validation checks and will always be forwarded, while those arriving on untrusted interfaces are subject to all configured ARP inspection tests.
- **Packet Rate Limit** – Sets the maximum number of ARP packets that can be processed by CPU per second on untrusted ports. (Range: 0-2048; Default: 15)

  Setting the rate limit to “0” means that there is no restriction on the number of ARP packets that can be processed by the CPU.

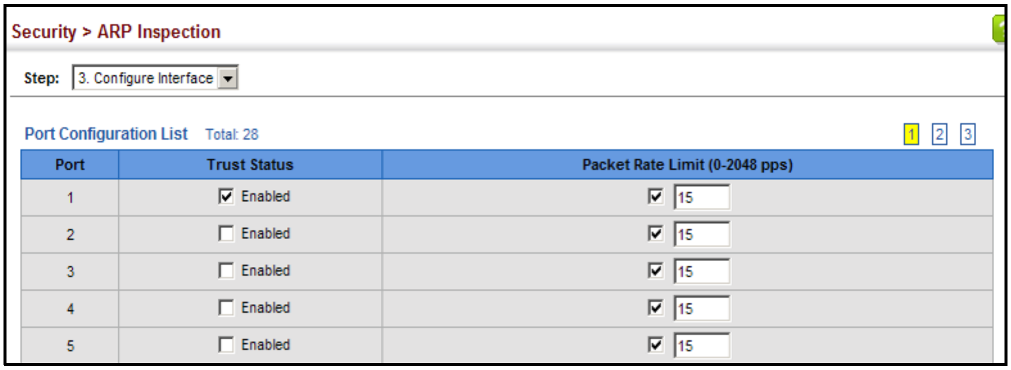
  The switch will drop all ARP packets received on a port which exceeds the configured ARP-packets-per-second rate limit.

WEB INTERFACE

To configure interface settings for ARP Inspection:

1. Click Security, ARP Inspection.
2. Select Configure Interface from the Step list.
3. Specify any untrusted ports which require ARP inspection, and adjust the packet inspection rate.
4. Click Apply.

Figure 214: Configuring Interface Settings for ARP Inspection



Security > ARP Inspection

Step: 3. Configure Interface

Port Configuration List Total: 28

Port	Trust Status	Packet Rate Limit (0-2048 pps)
1	☑ Enabled	☑ 15
2	□ Enabled	☑ 15
3	□ Enabled	☑ 15
4	□ Enabled	☑ 15
5	□ Enabled	☑ 15

DISPLAYING ARP INSPECTION STATISTICS

Use the Security > ARP Inspection (Show Information - Show Statistics) page to display statistics about the number of ARP packets processed, or dropped for various reasons.

CLI REFERENCES

- "show ip arp inspection statistics" on page 1153

PARAMETERS

These parameters are displayed:

Table 24: ARP Inspection Statistics

Parameter	Description
Received ARP packets before ARP inspection rate limit	Count of ARP packets received but not exceeding the ARP Inspection rate limit.
Dropped ARP packets in the process of ARP inspection rate limit	Count of ARP packets exceeding (and dropped by) ARP rate limiting.
Total ARP packets processed by ARP inspection	Count of all ARP packets processed by the ARP Inspection engine.
ARP packets dropped by additional validation (Src-MAC)	Count of packets that failed the source MAC address test.
ARP packets dropped by additional validation (Dst-MAC)	Count of packets that failed the destination MAC address test.

Table 24: ARP Inspection Statistics (Continued)

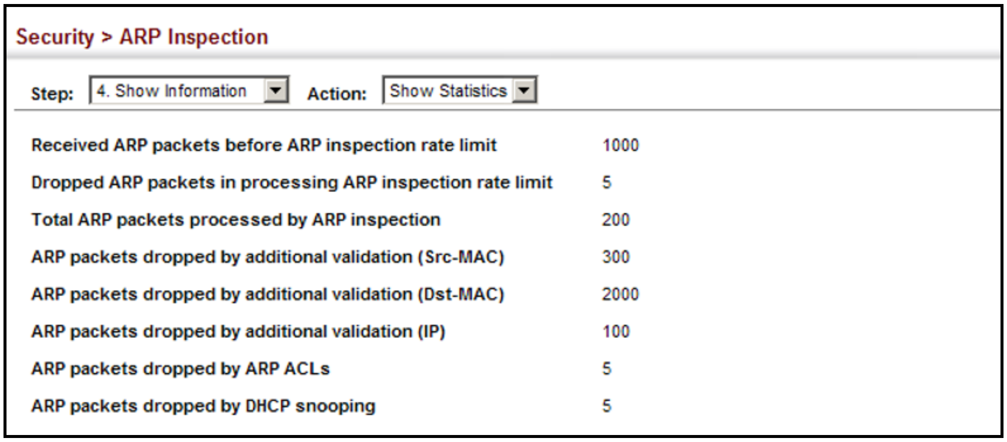
Parameter	Description
ARP packets dropped by additional validation (IP)	Count of ARP packets that failed the IP address test.
ARP packets dropped by ARP ACLs	Count of ARP packets that failed validation against ARP ACL rules.
ARP packets dropped by DHCP snooping	Count of packets that failed validation against the DHCP Snooping Binding database.

WEB INTERFACE

To display statistics for ARP Inspection:

1. Click Security, ARP Inspection.
2. Select Show Information from the Step list.
3. Select Show Statistics from the Action list.

Figure 215: Displaying Statistics for ARP Inspection



Security > ARP Inspection

Step: 4. Show Information Action: Show Statistics

Received ARP packets before ARP inspection rate limit	1000
Dropped ARP packets in processing ARP inspection rate limit	5
Total ARP packets processed by ARP inspection	200
ARP packets dropped by additional validation (Src-MAC)	300
ARP packets dropped by additional validation (Dst-MAC)	2000
ARP packets dropped by additional validation (IP)	100
ARP packets dropped by ARP ACLs	5
ARP packets dropped by DHCP snooping	5

DISPLAYING THE ARP INSPECTION LOG

Use the Security > ARP Inspection (Show Information - Show Log) page to show information about entries stored in the log, including the associated VLAN, port, and address components.

CLI REFERENCES

- "show ip arp inspection log" on page 1153

PARAMETERS

These parameters are displayed:

Table 25: ARP Inspection Log

Parameter	Description
VLAN ID	The VLAN where this packet was seen.
Port	The port where this packet was seen.

Table 25: ARP Inspection Log (Continued)

Parameter	Description
Src. IP Address	The source IP address in the packet.
Dst. IP Address	The destination IP address in the packet.
Src. MAC Address	The source MAC address in the packet.
Dst. MAC Address	The destination MAC address in the packet.

WEB INTERFACE

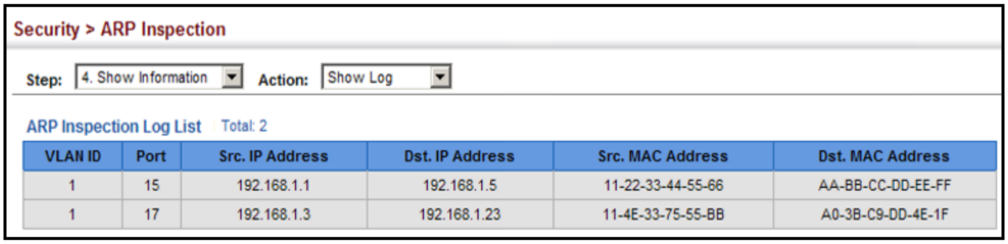
To display the ARP Inspection log:

1. Click Security, ARP Inspection.

2. Select Show Information from the Step list.

3. Select Show Log from the Action list.

Figure 216: Displaying the ARP Inspection Log



ARP Inspection Log List Total: 2

VLAN ID	Port	Src. IP Address	Dst. IP Address	Src. MAC Address	Dst. MAC Address
1	15	192.168.1.1	192.168.1.5	11-22-33-44-55-66	AA-BB-CC-DD-EE-FF
1	17	192.168.1.3	192.168.1.23	11-4E-33-75-55-BB	A0-3B-C9-DD-4E-1F

FILTERING IP ADDRESSES FOR MANAGEMENT ACCESS

Use the Security > IP Filter page to create a list of up to 15 IP addresses or IP address groups that are allowed management access to the switch through the web interface, SNMP, or Telnet.

CLI REFERENCES

- "Management IP Filter" on page 1078

COMMAND USAGE

- The management interfaces are open to all IP addresses by default. Once you add an entry to a filter list, access to that interface is restricted to the specified addresses.

- If anyone tries to access a management interface on the switch from an invalid address, the switch will reject the connection, enter an event message in the system log, and send a trap message to the trap manager.

- IP address can be configured for SNMP, web and Telnet access respectively. Each of these groups can include up to five different sets of addresses, either individual addresses or address ranges.

- When entering addresses for the same group (i.e., SNMP, web or Telnet), the switch will not accept overlapping address ranges. When entering addresses for different groups, the switch will accept overlapping address ranges.

- You cannot delete an individual address from a specified range. You must delete the entire range, and reenter the addresses.

- You can delete an address range just by specifying the start address, or by specifying both the start address and end address.

PARAMETERS

These parameters are displayed:

- **Mode**
  - **Web** – Configures IP address(es) for the web group.
  - **SNMP** – Configures IP address(es) for the SNMP group.
  - **Telnet** – Configures IP address(es) for the Telnet group.
  - **All** – Configures IP address(es) for all groups.

- **Start IP Address** – A single IP address, or the starting address of a range.

- **End IP Address** – The end address of a range.

WEB INTERFACE

To create a list of IP addresses authorized for management access:

1. Click Security, IP Filter.

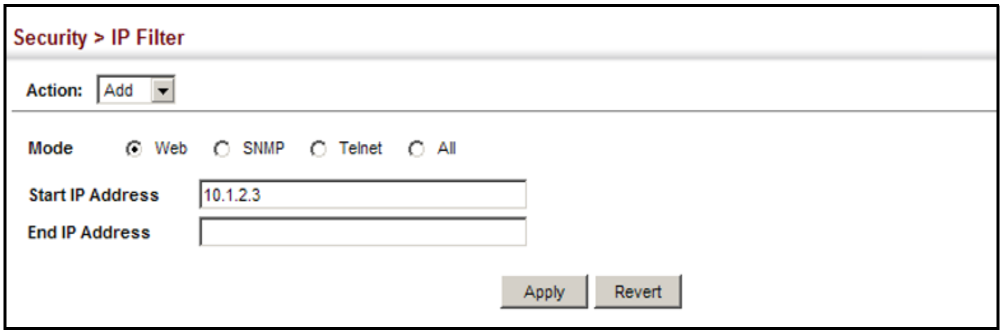
2. Select Add from the Action list.

3. Select the management interface to filter (Web, SNMP, Telnet).

4. Enter the IP addresses or range of addresses that are allowed management access to an interface.

5. Click Apply

Figure 217: Creating an IP Address Filter for Management Access



Security > IP Filter

Action: Add

Mode ● Web ○ SNMP ○ Telnet ○ All

Start IP Address: 10.1.2.3

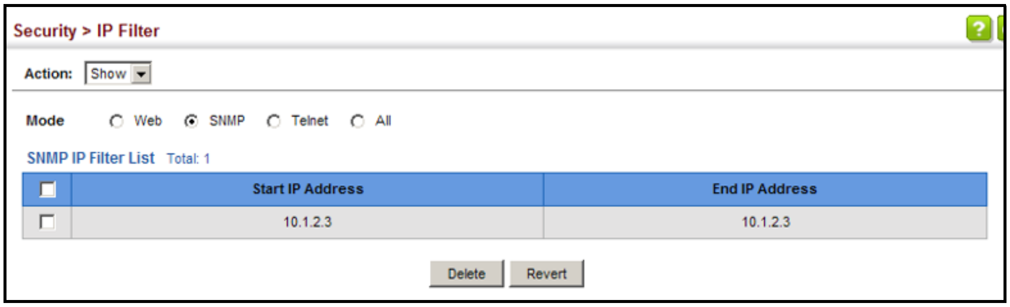
End IP Address:

To show a list of IP addresses authorized for management access:

1. Click Security, IP Filter.

2. Select Show from the Action list.

Figure 218: Showing IP Addresses Authorized for Management Access



Security > IP Filter

Action: Show

Mode ○ Web ● SNMP ○ Telnet ○ All

SNMP IP Filter List Total: 1

□	Start IP Address	End IP Address
□	10.1.2.3	10.1.2.3

CONFIGURING PORT SECURITY

Use the Security > Port Security page to configure the maximum number of device MAC addresses that can be learned by a switch port, stored in the address table, and authorized to access the network.

When port security is enabled on a port, the switch stops learning new MAC addresses on the specified port when it has reached a configured maximum number. Only incoming traffic with source addresses already stored in the address table will be authorized to access the network through that port. If a device with an unauthorized MAC address attempts to use the switch port, the intrusion will be detected and the switch can automatically take action by disabling the port and sending a trap message.

CLI REFERENCES

- "Port Security" on page 1090

COMMAND USAGE

- The default maximum number of MAC addresses allowed on a secure port is zero (that is, disabled). To use port security, you must configure the maximum number of addresses allowed on a port.

- To configure the maximum number of address entries which can be learned on a port, specify the maximum number of dynamic addresses allowed. The switch will learn up to the maximum number of allowed address pairs <source MAC address, VLAN> for frames received on the port. When the port has reached the maximum number of MAC addresses, the port will stop learning new addresses. The MAC addresses already in the address table will be retained and will not be aged out.

  Note that you can manually add additional secure addresses to a port using the Static Address Table (page 265).

- When the port security state is changed from enabled to disabled, all dynamically learned entries are cleared from the address table.

- If port security is enabled, and the maximum number of allowed addresses are set to a non-zero value, any device not in the address table that attempts to use the port will be prevented from accessing the switch.

- If a port is disabled (shut down) due to a security violation, it must be manually re-enabled from the Interface > Port > General page (page 182).

- A secure port has the following restrictions:
  - It cannot be used as a member of a static or dynamic trunk.
  - It should not be connected to a network interconnection device.

PARAMETERS

These parameters are displayed:

- **Port** – Port identifier.

- **Security Status** – Enables or disables port security on an interface. (Default: Disabled)

- **Port Status** – The operational status:

  - Secure/Down – Port security is disabled.

  - Secure/Up – Port security is enabled.

  - Shutdown – Port is shut down due to a response to a port security violation.

- **Action** – Indicates the action to be taken when a port security violation is detected:

  - **None**: No action should be taken. (This is the default.)

  - **Trap**: Send an SNMP trap message.

  - **Shutdown**: Disable the port.

  - **Trap and Shutdown**: Send an SNMP trap message and disable the port.

- **Max MAC Count** – The maximum number of MAC addresses that can be learned on a port. (Range: 0-1024, where 0 means disabled)

  The maximum address count is effective when port security is enabled or disabled.

- **Current MAC Count** – The number of MAC addresses currently associated with this interface.

- **MAC Filter** – Shows if MAC address filtering has been set under Security > Network Access (Configure MAC Filter) as described on page 375.

- **MAC Filter ID** – The identifier for a MAC address filter.

- **Last Intrusion MAC** – The last unauthorized MAC address detected.

- **Last Time Detected Intrusion MAC** – The last time an unauthorized MAC address was detected.

WEB INTERFACE

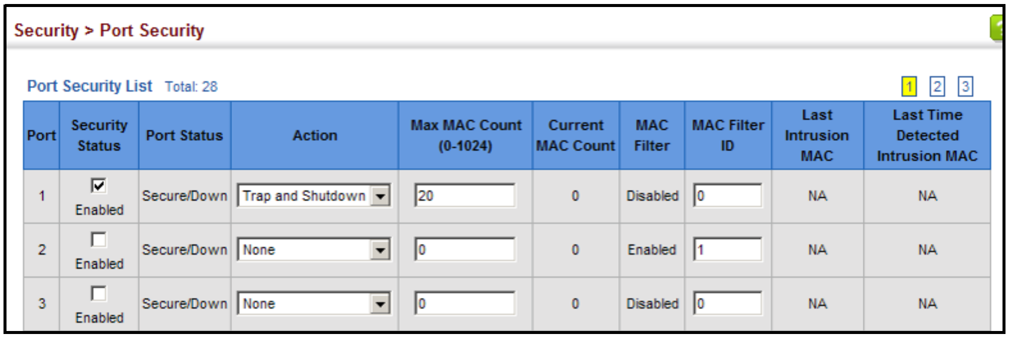
To configure port security:

1. Click Security, Port Security.

2. Mark the check box in the Security Status column to enable security, set the action to take when an invalid address is detected on a port, and set the maximum number of MAC addresses allowed on the port.

3. Click Apply.

Figure 219: Configuring Port Security



Security > Port Security

Port Security List Total: 28

1 2 3

Port	Security Status	Port Status	Action	Max MAC Count (0-1024)	Current MAC Count	MAC Filter	MAC Filter ID	Last Intrusion MAC	Last Time Detected Intrusion MAC
1	☑ Enabled	Secure/Down	Trap and Shutdown	20	0	Disabled	0	NA	NA
2	□ Enabled	Secure/Down	None	0	0	Enabled	1	NA	NA
3	□ Enabled	Secure/Down	None	0	0	Disabled	0	NA	NA

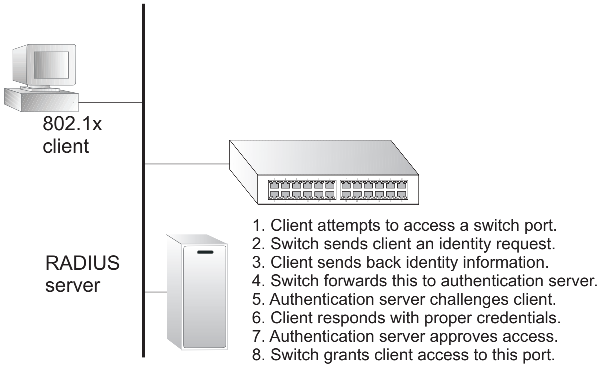
CONFIGURING 802.1X PORT AUTHENTICATION

Network switches can provide open and easy access to network resources by simply attaching a client PC. Although this automatic configuration and access is a desirable feature, it also allows unauthorized personnel to easily intrude and possibly gain access to sensitive network data.

The IEEE 802.1X (dot1X) standard defines a port-based access control procedure that prevents unauthorized access to a network by requiring users to first submit credentials for authentication. Access to all switch ports in a network can be centrally controlled from a server, which means that authorized users can use the same credentials for authentication from any point within the network.

This switch uses the Extensible Authentication Protocol over LANs (EAPOL) to exchange authentication protocol messages with the client, and a remote RADIUS authentication server to verify user identity and access rights. When a client (i.e., Supplicant) connects to a switch port, the switch (i.e., Authenticator) responds with an EAPOL identity request. The client provides its identity (such as a user name) in an EAPOL response to the switch, which it forwards to the RADIUS server. The RADIUS server verifies the client identity and sends an access challenge back to the client. The EAP packet from the RADIUS server contains not only the challenge, but the authentication method to be used. The client can reject the authentication method and request another, depending on the configuration of the client software and the RADIUS server. The encryption method used to pass authentication messages can be MD5 (Message-Digest 5), TLS (Transport Layer Security), PEAP (Protected Extensible Authentication Protocol), or TTLS (Tunneled Transport Layer Security). The client responds to the appropriate method with its credentials, such as a password or certificate. The RADIUS server verifies the client credentials and responds with an accept or reject packet. If authentication is successful, the switch allows the client to access the network. Otherwise, non-EAP traffic on the port is blocked or assigned to a guest VLAN based on the "intrusion-action" setting. In "multi-host" mode, only one host connected to a port needs to pass authentication for all other hosts to be granted network access. Similarly, a port can become unauthorized for all hosts if one attached host fails re-authentication or sends an EAPOL logoff message.

Figure 220: Configuring Port Security


802.1x
client
RADIUS
server
1. Client attempts to access a switch port.
2. Switch sends client an identity request.
3. Client sends back identity information.
4. Switch forwards this to authentication server.
5. Authentication server challenges client.
6. Client responds with proper credentials.
7. Authentication server approves access.
8. Switch grants client access to this port.

The operation of 802.1X on the switch requires the following:

- The switch must have an IP address assigned.
- RADIUS authentication must be enabled on the switch and the IP address of the RADIUS server specified.
- 802.1X must be enabled globally for the switch.
- Each switch port that will be used must be set to dot1X “Auto” mode.
- Each client that needs to be authenticated must have dot1X client software installed and properly configured.
- The RADIUS server and 802.1X client support EAP. (The switch only supports EAPOL in order to pass the EAP packets from the server to the client.)
- The RADIUS server and client also have to support the same EAP authentication type – MD5, PEAP, TLS, or TTLS. (Native support for these encryption methods is provided in Windows 7, Vista and XP. To support these encryption methods in Windows 95 and 98, you can use the AEGIS dot1x client or other comparable client software)

CONFIGURING 802.1X GLOBAL SETTINGS

Use the Security > Port Authentication (Configure Global) page to configure IEEE 802.1X port authentication. The 802.1X protocol must be enabled globally for the switch system before port settings are active.

CLI REFERENCES

- "802.1X Port Authentication" on page 1067

PARAMETERS

These parameters are displayed:

- **System Authentication Control** – Sets the global setting for 802.1X. (Default: Disabled)
- **EAPOL Pass Through** – Passes EAPOL frames through to all ports in STP forwarding state when dot1x is globally disabled.
  (Default: Disabled)

  When this device is functioning as intermediate node in the network and does not need to perform dot1x authentication, **EAPOL Pass Through** can be enabled to allow the switch to forward EAPOL frames from other switches on to the authentication servers, thereby allowing the authentication process to still be carried out by switches located on the edge of the network.

  When this device is functioning as an edge switch but does not require any attached clients to be authenticated, **EAPOL Pass Through** can be disabled to discard unnecessary EAPOL traffic.

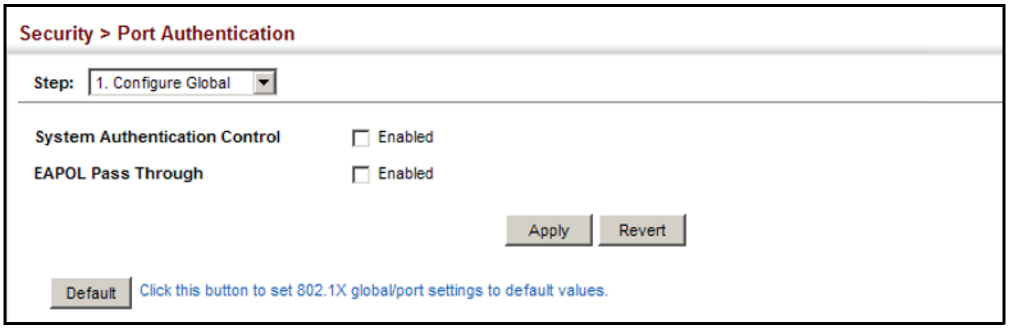
- **Default** – Sets all configurable 802.1X global and port settings to their default values.

WEB INTERFACE

To configure global settings for 802.1X:

1. Click Security, Port Authentication.
2. Select Configure Global from the Step list.
3. Enable 802.1X globally for the switch, and configure EAPOL Pass Through if required.
4. Click Apply

Figure 221: Configuring Global Settings for 802.1X Port Authentication



Security > Port Authentication

Step: 1. Configure Global

System Authentication Control □ Enabled

EAPOL Pass Through □ Enabled

Click this button to set 802.1X global/port settings to default values.

CONFIGURING PORT AUTHENTICATOR SETTINGS FOR 802.1X

Use the Security > Port Authentication (Configure Interface) page to configure 802.1X port settings for the switch as the local authenticator. When 802.1X is enabled, you need to configure the parameters for the authentication process that runs between the client and the switch (i.e., authenticator), as well as the client identity lookup process that runs between the switch and authentication server.

CLI REFERENCES

- "802.1X Port Authentication" on page 1067

COMMAND USAGE

- When the switch functions as a local authenticator between supplicant devices attached to the switch and the authentication server, configure the parameters for the exchange of EAP messages between the authenticator and clients on the Authenticator configuration page.
- This switch can be configured to serve as the authenticator on selected ports by setting the Control Mode to Auto on this configuration page.

PARAMETERS

These parameters are displayed:

- **Port** – Port number.
- **Status** – Indicates if authentication is enabled or disabled on the port. The status is disabled if the control mode is set to Force-Authorized.
- **Authorized** – Displays the 802.1X authorization status of connected clients.
  - **Yes** – Connected client is authorized.
  - **N/A** – Connected client is not authorized, or port is not connected.
- **Control Mode** – Sets the authentication mode to one of the following options:
  - **Auto** – Requires a dot1x-aware client to be authorized by the authentication server. Clients that are not dot1x-aware will be denied access.
  - **Force-Authorized** – Forces the port to grant access to all clients, either dot1x-aware or otherwise. (This is the default setting.)
  - **Force-Unauthorized** – Forces the port to deny access to all clients, either dot1x-aware or otherwise.
- **Operation Mode** – Allows single or multiple hosts (clients) to connect to an 802.1X-authorized port. (Default: Single-Host)
  - **Single-Host** – Allows only a single host to connect to this port.
  - **Multi-Host** – Allows multiple host to connect to this port.

    In this mode, only one host connected to a port needs to pass authentication for all other hosts to be granted network access. Similarly, a port can become unauthorized for all hosts if one attached host fails re-authentication or sends an EAPOL logoff message.
  - **MAC-Based** – Allows multiple hosts to connect to this port, with each host needing to be authenticated.

    In this mode, each host connected to a port needs to pass authentication. The number of hosts allowed access to a port operating in this mode is limited only by the available space in the secure address table (i.e., up to 1024 addresses).
- **Max Count** – The maximum number of hosts that can connect to a port when the Multi-Host operation mode is selected. (Range: 1-1024; Default: 5)

- **Max Request** – Sets the maximum number of times the switch port will retransmit an EAP request packet to the client before it times out the authentication session. (Range: 1-10; Default 2)

- **Quiet Period** – Sets the time that a switch port waits after the Max Request Count has been exceeded before attempting to acquire a new client. (Range: 1-65535 seconds; Default: 60 seconds)

- **Tx Period** – Sets the time period during an authentication session that the switch waits before re-transmitting an EAP packet. (Range: 1-65535; Default: 30 seconds)

- **Supplicant Timeout** – Sets the time that a switch port waits for a response to an EAP request from a client before re-transmitting an EAP packet. (Range: 1-65535; Default: 30 seconds)

  This command attribute sets the timeout for EAP-request frames other than EAP-request/identity frames. If dot1x authentication is enabled on a port, the switch will initiate authentication when the port link state comes up. It will send an EAP-request/identity frame to the client to request its identity, followed by one or more requests for authentication information. It may also send other EAP-request frames to the client during an active connection as required for reauthentication.

- **Server Timeout** – Sets the time that a switch port waits for a response to an EAP request from an authentication server before re-transmitting an EAP packet. (Default: 0 seconds)

  A RADIUS server must be set before the correct operational value of 10 seconds will be displayed in this field. (See "Configuring Remote Logon Authentication Servers" on page 350.)

- **Re-authentication Status** – Sets the client to be re-authenticated after the interval specified by the Re-authentication Period. Re-authentication can be used to detect if a new device is plugged into a switch port. (Default: Disabled)

- **Re-authentication Period** – Sets the time period after which a connected client must be re-authenticated. (Range: 1-65535 seconds; Default: 3600 seconds)

- **Re-authentication Max Retries** – The maximum number of times the switch port will retransmit an EAP request/identity packet to the client before it times out the authentication session. (Range: 1-10; Default: 2)

- **Intrusion Action** – Sets the port’s response to a failed authentication.

  - **Block Traffic** – Blocks all non-EAP traffic on the port. (This is the default setting.)

  - **Guest VLAN** – All traffic for the port is assigned to a guest VLAN. The guest VLAN must be separately configured (See "Configuring VLAN Groups" on page 228) and mapped on each port (See "Configuring Network Access for Ports" on page 372).

Supplicant List

- **Supplicant** – MAC address of authorized client.

Authenticator PAE State Machine

- **State** – Current state (including initialize, disconnected, connecting, authenticating, authenticated, aborting, held, force_authorized, force_unauthorized).
- **Reauth Count** – Number of times connecting state is re-entered.
- **Current Identifier** – Identifier sent in each EAP Success, Failure or Request packet by the Authentication Server.

Backend State Machine

- **State** – Current state (including request, response, success, fail, timeout, idle, initialize).
- **Request Count** – Number of EAP Request packets sent to the Supplicant without receiving a response.
- **Identifier (Server)** – Identifier carried in the most recent EAP Success, Failure or Request packet received from the Authentication Server.

Reauthentication State Machine

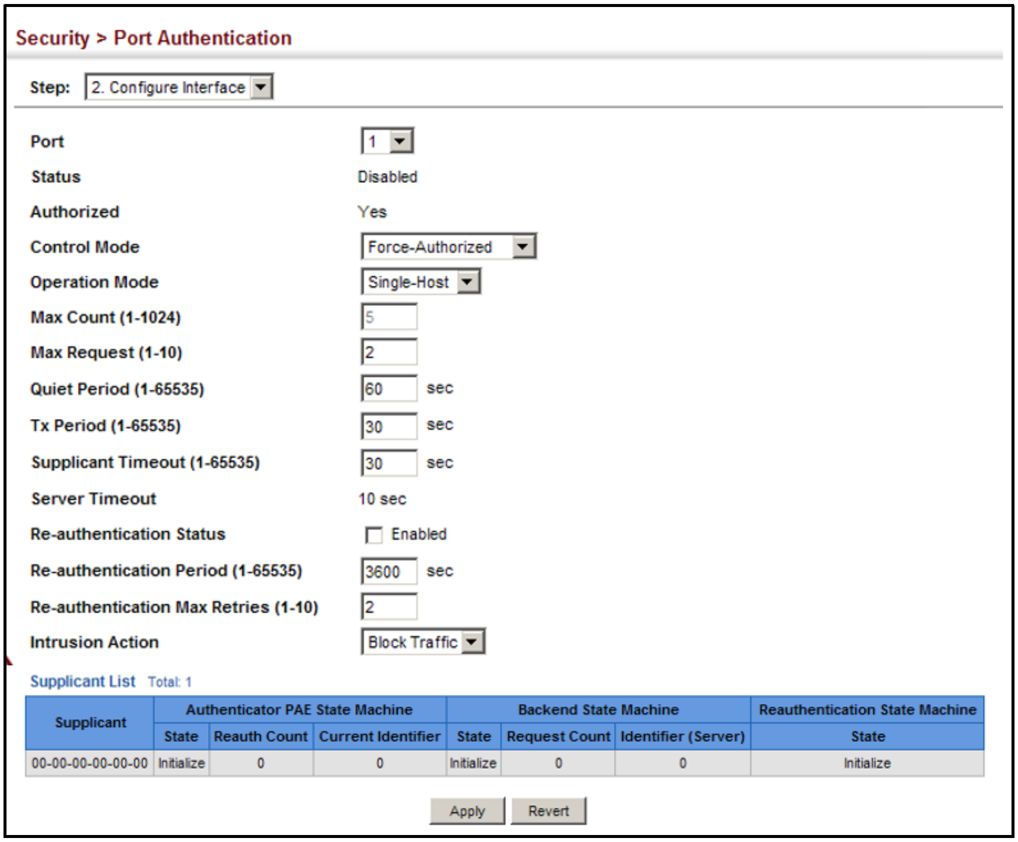
- **State** – Current state (including initialize, reauthenticate).

WEB INTERFACE

To configure port authenticator settings for 802.1X:

1. Click Security, Port Authentication.
2. Select Configure Interface from the Step list.
3. Modify the authentication settings for each port as required.
4. Click Apply

Figure 222: Configuring Interface Settings for 802.1X Port Authenticator



Security > Port Authentication

Step: 2. Configure Interface

Port	1
Status	Disabled
Authorized	Yes
Control Mode	Force-Authorized
Operation Mode	Single-Host
Max Count (1-1024)	5
Max Request (1-10)	2
Quiet Period (1-65535)	60 sec
Tx Period (1-65535)	30 sec
Supplicant Timeout (1-65535)	30 sec
Server Timeout	10 sec
Re-authentication Status	□ Enabled
Re-authentication Period (1-65535)	3600 sec
Re-authentication Max Retries (1-10)	2
Intrusion Action	Block Traffic

Supplicant List Total: 1

Supplicant	Authenticator PAE State Machine			Backend State Machine			Reauthentication State Machine
	State	Reauth Count	Current Identifier	State	Request Count	Identifier (Server)	State
00-00-00-00-00-00	Initialize	0	0	Initialize	0	0	Initialize

DISPLAYING 802.1X STATISTICS

Use the Security > Port Authentication (Show Statistics) page to display statistics for dot1x protocol exchanges for any port.

CLI REFERENCES

- "show dot1x" on page 1076

PARAMETERS

These parameters are displayed:

Table 26: 802.1X Statistics

Parameter	Description
Authenticator	
Rx EAPOL Start	The number of EAPOL Start frames that have been received by this Authenticator.
Rx EAPOL Logoff	The number of EAPOL Logoff frames that have been received by this Authenticator.
Rx EAPOL Invalid	The number of EAPOL frames that have been received by this Authenticator in which the frame type is not recognized.
Rx EAPOL Total	The number of valid EAPOL frames of any type that have been received by this Authenticator.
Rx Last EAPOLVer	The protocol version number carried in the most recent EAPOL frame received by this Authenticator.

Table 26: 802.1X Statistics (Continued)

Parameter	Description
Rx Last EAPOLSrc	The source MAC address carried in the most recent EAPOL frame received by this Authenticator.
Rx EAP Resp/Id	The number of EAP Resp/Id frames that have been received by this Authenticator.
Rx EAP Resp/Oth	The number of valid EAP Response frames (other than Resp/Id frames) that have been received by this Authenticator.
Rx EAP LenError	The number of EAPOL frames that have been received by this Authenticator in which the Packet Body Length field is invalid.
Tx EAP Req/Id	The number of EAP Req/Id frames that have been transmitted by this Authenticator.
Tx EAP Req/Oth	The number of EAP Request frames (other than Rq/Id frames) that have been transmitted by this Authenticator.
Tx EAPOL Total	The number of EAPOL frames of any type that have been transmitted by this Authenticator.
Supplicant	
Rx EAPOL Invalid	The number of EAPOL frames that have been received by this Supplicant in which the frame type is not recognized.
Rx EAPOL Total	The number of valid EAPOL frames of any type that have been received by this Supplicant.
Rx Last EAPOLVer	The protocol version number carried in the most recent EAPOL frame received by this Supplicant.
Rx Last EAPOLSrc	The source MAC address carried in the most recent EAPOL frame received by this Supplicant.
Rx EAP Resp/Id	The number of EAP Resp/Id frames that have been received by this Supplicant.
Rx EAP Resp/Oth	The number of valid EAP Response frames (other than Resp/Id frames) that have been received by this Supplicant.
Rx EAP LenError	The number of EAPOL frames that have been received by this Supplicant in which the Packet Body Length field is invalid.
Tx EAPOL Total	The number of EAPOL frames of any type that have been transmitted by this Supplicant.
Tx EAPOL Start	The number of EAPOL Start frames that have been transmitted by this Supplicant.
Tx EAPOL Logoff	The number of EAPOL Logoff frames that have been transmitted by this Supplicant.
Tx EAP Req/Id	The number of EAP Req/Id frames that have been transmitted by this Supplicant.
Tx EAP Req/Oth	The number of EAP Request frames (other than Req/Id frames) that have been transmitted by this Supplicant.

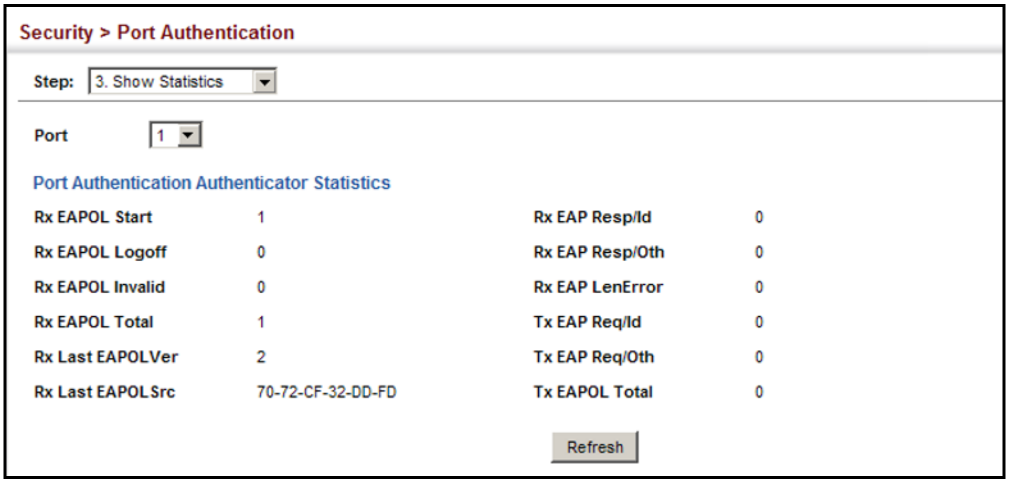
WEB INTERFACE

To display port authenticator statistics for 802.1X:

1. Click Security, Port Authentication.

2. Select Show Statistics from the Step list.

Figure 223: Showing Statistics for 802.1X Port Authenticator



Security > Port Authentication

Step: 3. Show Statistics

Port 1

Port Authentication Authenticator Statistics

Rx EAPOL Start	1	Rx EAP Resp/Id	0
Rx EAPOL Logoff	0	Rx EAP Resp/Oth	0
Rx EAPOL Invalid	0	Rx EAP LenError	0
Rx EAPOL Total	1	Tx EAP Req/Id	0
Rx Last EAPOLVer	2	Tx EAP Req/Oth	0
Rx Last EAPOLSrc	70-72-CF-32-DD-FD	Tx EAPOL Total	0

DOS PROTECTION

Use the Security > DoS Protection page to protect against denial-of-service (DoS) attacks. A DoS attack is an attempt to block the services provided by a computer or network resource. This kind of attack tries to prevent an Internet site or service from functioning efficiently or at all. In general, DoS attacks are implemented by either forcing the target to reset, to consume most of its resources so that it can no longer provide its intended service, or to obstruct the communication media between the intended users and the target so that they can no longer communicate adequately. This section describes how to protect against DoS attacks.

CLI REFERENCES

- "Denial of Service Protection" on page 947

PARAMETERS

These parameters are displayed:

- **LAND Attack** – Configures the switch to protect against DoS LAND (Local Area Network Denial) attacks in which hackers send spoofed-IP packets where the source and destination address are the same, thereby causing the target to reply to itself continuously.
(Default: Enabled)

- **TCP Null Scan** – A TCP NULL scan message is used to identify listening TCP ports. The scan uses a series of strangely configured TCP packets which contain a sequence number of 0 and no flags. If the target's TCP port is closed, the target replies with a TCP RST (reset) packet. If the target TCP port is open, it simply discards the TCP NULL scan. (Default: Enabled)

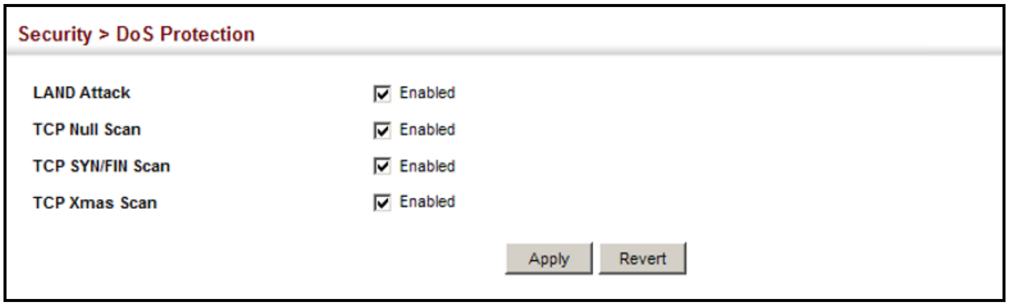
- **TCP SYN/FIN Scan** – A TCP SYN/FIN scan message is used to identify listening TCP ports. The scan uses a series of strangely configured TCP packets which contain SYN (synchronize) and FIN (finish) flags. If the target's TCP port is closed, the target replies with a TCP RST (reset) packet. If the target TCP port is open, it simply discards the TCP SYN FIN scan. (Default: Enabled)
- **TCP Xmas Scan** – A so-called TCP XMAS scan message is used to identify listening TCP ports. This scan uses a series of strangely configured TCP packets which contain a sequence number of 0 and the URG, PSH and FIN flags. If the target's TCP port is closed, the target replies with a TCP RST packet. If the target TCP port is open, it simply discards the TCP XMAS scan. (Default: Enabled)

WEB INTERFACE

To protect against DoS attacks:

1. Click Security, DoS Protection.
2. Enable protection for LAND attacks or TCP scan attacks.
3. Click Apply

Figure 224: Protecting Against DoS Attacks



Security > DoS Protection

LAND Attack ☑ Enabled
TCP Null Scan ☑ Enabled
TCP SYN/FIN Scan ☑ Enabled
TCP Xmas Scan ☑ Enabled

IPV4 SOURCE GUARD

IPv4 Source Guard is a security feature that filters IP traffic on network interfaces based on manually configured entries in the IP Source Guard table, or dynamic entries in the DHCP Snooping table when enabled (see "DHCP Snooping" on page 444). IP source guard can be used to prevent traffic attacks caused when a host tries to use the IP address of a neighbor to access the network. This section describes how to configure IP Source Guard.

CONFIGURING PORTS FOR IP SOURCE GUARD

Use the Security > IP Source Guard > Port Configuration page to set the filtering type based on source IP address, or source IP address and MAC address pairs.

IP Source Guard is used to filter traffic on an insecure port which receives messages from outside the network or fire wall, and therefore may be subject to traffic attacks caused by a host trying to use the IP address of a neighbor.

CLI REFERENCES

- "ip source-guard" on page 1135

COMMAND USAGE

- Setting source guard mode to SIP (Source IP) or SIP-MAC (Source IP and MAC) enables this function on the selected port. Use the SIP option to check the VLAN ID, source IP address, and port number against all entries in the binding table. Use the SIP-MAC option to check these same parameters, plus the source MAC address. If no matching entry is found, the packet is dropped.

NOTE: Multicast addresses cannot be used by IP Source Guard.

- When enabled, traffic is filtered based upon dynamic entries learned via DHCP snooping (see "DHCP Snooping" on page 444), or static addresses configured in the source guard binding table.

- If IP source guard is enabled, an inbound packet's IP address (SIP option) or both its IP address and corresponding MAC address (SIP-MAC option) will be checked against the binding table. If no matching entry is found, the packet will be dropped.

- Filtering rules are implemented as follows:

  - If DHCP snooping is disabled (see page 446), IP source guard will check the VLAN ID, source IP address, port number, and source MAC address (for the SIP-MAC option). If a matching entry is found in the binding table and the entry type is static IP source guard binding, the packet will be forwarded.

  - If DHCP snooping is enabled, IP source guard will check the VLAN ID, source IP address, port number, and source MAC address (for the SIP-MAC option). If a matching entry is found in the binding table and the entry type is static IP source guard binding, or dynamic DHCP snooping binding, the packet will be forwarded.

  - If IP source guard if enabled on an interface for which IP source bindings have not yet been configured (neither by static configuration in the IP source guard binding table nor dynamically learned from DHCP snooping), the switch will drop all IP traffic on that port, except for DHCP packets.

PARAMETERS

These parameters are displayed:

- **Filter Type** – Configures the switch to filter inbound traffic based source IP address, or source IP address and corresponding MAC address. (Default: None)
  - **None** – Disables IP source guard filtering on the port.
  - **SIP** – Enables traffic filtering based on IP addresses stored in the binding table.
  - **SIP-MAC** – Enables traffic filtering based on IP addresses and corresponding MAC addresses stored in the binding table.
- **Max Binding Entry** – The maximum number of entries that can be bound to an interface. (Range: 1-5; Default: 5)

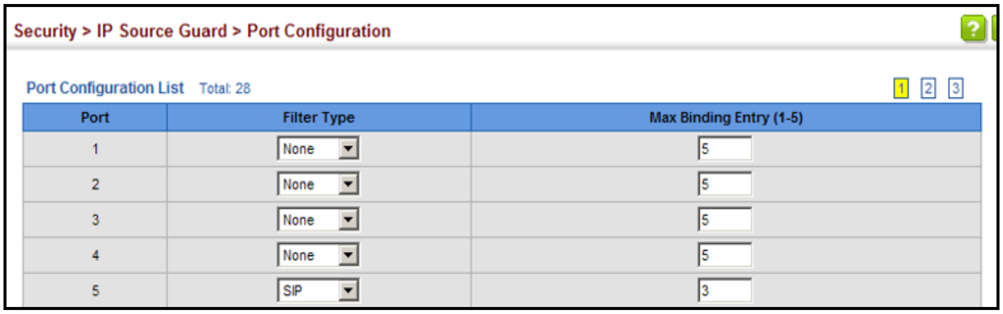
  This parameter sets the maximum number of address entries that can be mapped to an interface in the binding table, including both dynamic entries discovered by DHCP snooping (see "DHCP Snooping" on page 444) and static entries set by IP source guard (see "Configuring Static Bindings for IP Source Guard" on page 435).

WEB INTERFACE

To set the IP Source Guard filter for ports:

1. Click Security, IP Source Guard, Port Configuration.
2. Set the required filtering type for each port.
3. Click Apply

Figure 225: Setting the Filter Type for IP Source Guard



Security > IP Source Guard > Port Configuration

Port Configuration List Total: 28

Port	Filter Type	Max Binding Entry (1-5)
1	None	5
2	None	5
3	None	5
4	None	5
5	SIP	3

CONFIGURING STATIC BINDINGS FOR IP SOURCE GUARD

Use the Security > IP Source Guard > Static Configuration page to bind a static address to a port. Table entries include a MAC address, IP address, lease time, entry type (Static, Dynamic), VLAN identifier, and port identifier. All static entries are configured with an infinite lease time, which is indicated with a value of zero in the table.

CLI REFERENCES

- "ip source-guard binding" on page 1134

COMMAND USAGE

- Static addresses entered in the source guard binding table are automatically configured with an infinite lease time. Dynamic entries learned via DHCP snooping are configured by the DHCP server itself.

- Static bindings are processed as follows:

  - If there is no entry with the same VLAN ID and MAC address, a new entry is added to the binding table using the type “static IP source guard binding.”

  - If there is an entry with the same VLAN ID and MAC address, and the type of entry is static IP source guard binding, then the new entry will replace the old one.

  - If there is an entry with the same VLAN ID and MAC address, and the type of the entry is dynamic DHCP snooping binding, then the new entry will replace the old one and the entry type will be changed to static IP source guard binding.

  - Only unicast addresses are accepted for static bindings.

PARAMETERS

These parameters are displayed:

Add

- **Port** – The port to which a static entry is bound.

- **VLAN** – ID of a configured VLAN (Range: 1-4094)

- **MAC Address** – A valid unicast MAC address.

- **IP Address** – A valid unicast IP address, including classful types A, B or C.

Show

- **VLAN** – VLAN to which this entry is bound.

- **MAC Address** – Physical address associated with the entry.

- **Interface** – The port to which this entry is bound.

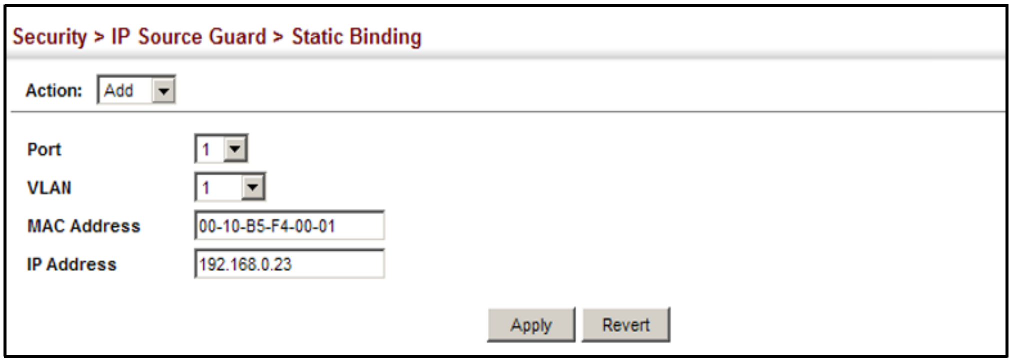
- **IP Address** – IP address corresponding to the client.
- **Lease Time** – The time for which this IP address is leased to the client. (This value is zero for all static addresses.)

WEB INTERFACE

To configure static bindings for IP Source Guard:

1. Click Security, IP Source Guard, Static Configuration.
2. Select Add from the Action list.
3. Enter the required bindings for each port.
4. Click Apply

Figure 226: Configuring Static Bindings for IP Source Guard



Security > IP Source Guard > Static Binding

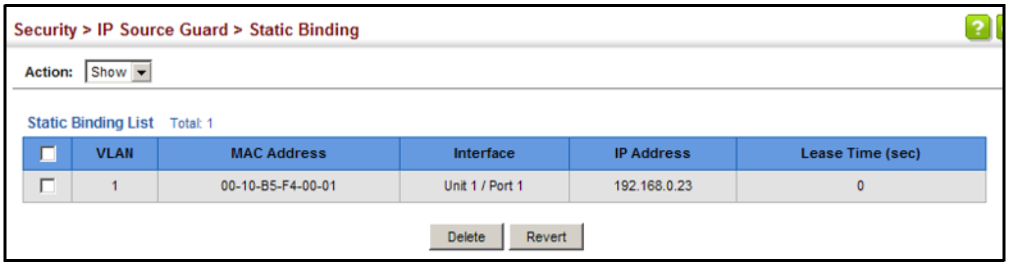
Action: Add

Port	1
VLAN	1
MAC Address	00-10-B5-F4-00-01
IP Address	192.168.0.23

To display static bindings for IP Source Guard:

1. Click Security, IP Source Guard, Static Configuration.
2. Select Show from the Action list.

Figure 227: Displaying Static Bindings for IP Source Guard



Security > IP Source Guard > Static Binding

Action: Show

Static Binding List Total: 1

□	VLAN	MAC Address	Interface	IP Address	Lease Time (sec)
□	1	00-10-B5-F4-00-01	Unit 1 / Port 1	192.168.0.23	0

DISPLAYING INFORMATION FOR DYNAMIC IPV4 SOURCE GUARD BINDINGS

Use the Security > IP Source Guard > Dynamic Binding page to display the source-guard binding table for a selected interface.

CLI REFERENCES

- "show ip dhcp snooping binding" on page 1126

PARAMETERS

These parameters are displayed:

Query by

- **Port** – A port on this switch.
- **VLAN** – ID of a configured VLAN (Range: 1-4094)
- **MAC Address** – A valid unicast MAC address.
- **IP Address** – A valid unicast IP address, including classful types A, B or C.

Dynamic Binding List

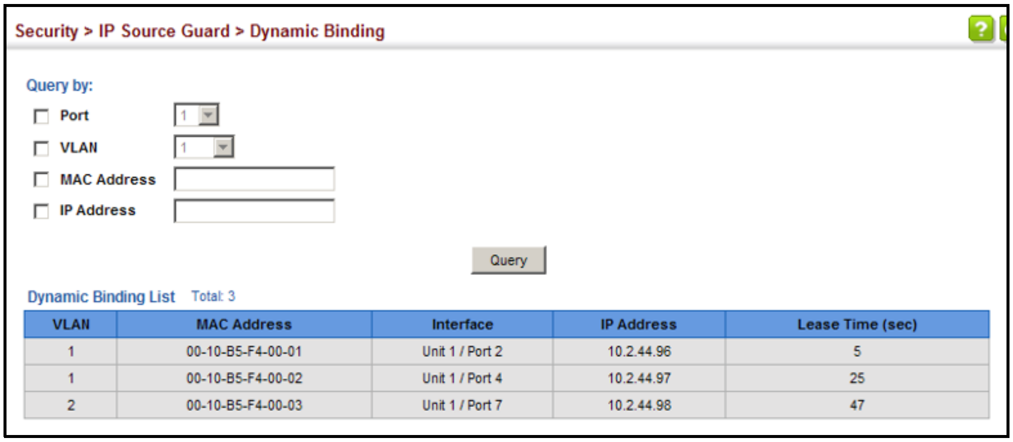
- **VLAN** – VLAN to which this entry is bound.
- **MAC Address** – Physical address associated with the entry.
- **Interface** – Port to which this entry is bound.
- **IP Address** – IP address corresponding to the client.
- **Lease Time** – The time for which this IP address is leased to the client.

WEB INTERFACE

To display the binding table for IP Source Guard:

1. Click Security, IP Source Guard, Dynamic Binding.
2. Mark the search criteria, and enter the required values.
3. Click Query

Figure 228: Showing the IP Source Guard Binding Table



Security > IP Source Guard > Dynamic Binding

Query by:

□ Port 1

□ VLAN 1

□ MAC Address

□ IP Address

Query

Dynamic Binding List Total: 3

VLAN	MAC Address	Interface	IP Address	Lease Time (sec)
1	00-10-B5-F4-00-01	Unit 1 / Port 2	10.2.44.96	5
1	00-10-B5-F4-00-02	Unit 1 / Port 4	10.2.44.97	25
2	00-10-B5-F4-00-03	Unit 1 / Port 7	10.2.44.98	47

IPv6 Source Guard

IPv6 Source Guard is a security feature that filters IPv6 traffic on non-routed, Layer 2 network interfaces based on manually configured entries in the IPv6 Source Guard table, or dynamic entries in the Neighbor Discovery Snooping table or DHCPv6 Snooping table when either snooping protocol is enabled (see the DHCPv6 Snooping commands on page 1126). IPv6 source guard can be used to prevent traffic attacks caused when a host tries to use the IPv6 address of a neighbor to access the network. This section describes how to configure IPv6 Source Guard.

Configuring Ports for IPv6 Source Guard

Use the Security > IPv6 Source Guard > Port Configuration page to filter inbound traffic based on the source IPv6 address stored in the binding table.

IPv6 Source Guard is used to filter traffic on an insecure port which receives messages from outside the network or fire wall, and therefore may be subject to traffic attacks caused by a host trying to use the IPv6 address of a neighbor.

CLI References

- "ipv6 source-guard" on page 1142

Command Usage

- Setting source guard mode to SIP (Source IP) enables this function on the selected port. Use the SIP option to check the VLAN ID, IPv6 global unicast source IP address, and port number against all entries in the binding table.

- After IPv6 source guard is enabled on an interface, the switch initially blocks all IPv6 traffic received on that interface, except for ND packets allowed by ND snooping and DHCPv6 packets allowed by DHCPv6 snooping. A port access control list (ACL) is applied to the interface. Traffic is then filtered based upon dynamic entries learned via ND snooping or DHCPv6 snooping, or static addresses configured in the source guard binding table. The port allows only IPv6 traffic with a matching entry in the binding table and denies all other IPv6 traffic.

- Table entries include a MAC address, IPv6 global unicast address, entry type (Static-IPv6-SG-Binding, Dynamic-ND-Binding, Dynamic-DHCPv6-Binding), VLAN identifier, and port identifier.

- Static addresses entered in the source guard binding table (using the Static Binding page) are automatically configured with an infinite lease time. Dynamic entries learned via DHCPv6 snooping are configured by the DHCPv6 server itself.

- If IPv6 source guard is enabled, an inbound packet's source IPv6 address will be checked against the binding table. If no matching entry is found, the packet will be dropped.

- Filtering rules are implemented as follows:

  - If ND snooping and DHCPv6 snooping are disabled, IPv6 source guard will check the VLAN ID, source IPv6 address, and port number. If a matching entry is found in the binding table and the entry type is static IPv6 source guard binding, the packet will be forwarded.

  - If ND snooping or DHCP snooping is enabled, IPv6 source guard will check the VLAN ID, source IP address, and port number. If a matching entry is found in the binding table and the entry type is static IPv6 source guard binding, dynamic ND snooping binding, or dynamic DHCPv6 snooping binding, the packet will be forwarded.

  - If IP source guard if enabled on an interface for which IPv6 source bindings (dynamically learned via ND snooping or DHCPv6 snooping, or manually configured) are not yet configured, the switch will drop all IPv6 traffic on that port, except for ND packets and DHCPv6 packets.

  - Only IPv6 global unicast addresses are accepted for static bindings.

PARAMETERS

These parameters are displayed:

- **Port** – Port identifier (Range: 1-28)

- **Filter Type** – Configures the switch to filter inbound traffic based on the following options. (Default: Disabled)

  - **Disabled** – Disables IPv6 source guard filtering on the port.

  - **SIP** – Enables traffic filtering based on IPv6 global unicast source IPv6 addresses stored in the binding table.

- **Max Binding Entry** – The maximum number of entries that can be bound to an interface. (Range: 1-5; Default: 5)

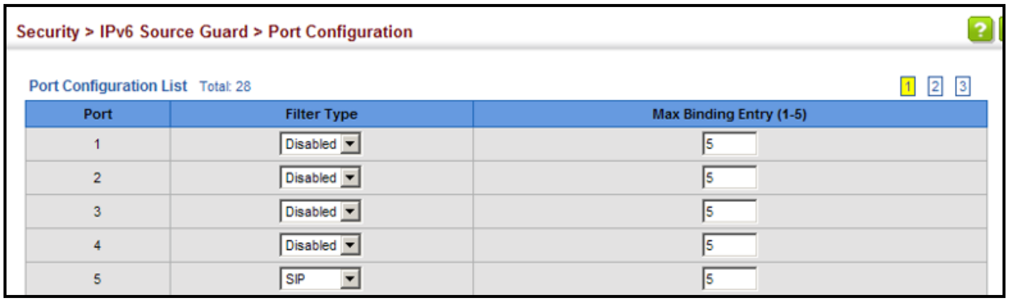
- This parameter sets the maximum number of IPv6 global unicast source IPv6 address entries that can be mapped to an interface in the binding table, including both dynamic entries discovered by ND snooping, DHCPv6 snooping (see the DHCPv6 Snooping commands), and static entries set by IPv6 Source Guard (see "Configuring Static Bindings for IPv6 Source Guard" on page 440).
- IPv6 source guard maximum bindings must be set to a value higher than DHCPv6 snooping maximum bindings and ND snooping maximum bindings.
- If IPv6 source guard, ND snooping, and DHCPv6 snooping are enabled on a port, the dynamic bindings used by ND snooping, DHCPv6 snooping, and IPv6 source guard static bindings cannot exceed the maximum allowed bindings set by this parameter. In other words, no new entries will be added to the IPv6 source guard binding table.
- If IPv6 source guard is enabled on a port, and the maximum number of allowed bindings is changed to a lower value, precedence is given to deleting entries learned through DHCPv6 snooping, ND snooping, and then manually configured IPv6 source guard static bindings, until the number of entries in the binding table reaches the newly configured maximum number of allowed bindings.

WEB INTERFACE

To set the IPv6 Source Guard filter for ports:

1. Click Security, IPv6 Source Guard, Port Configuration.
2. Set the required filtering type for each port.
3. Click Apply

Figure 229: Setting the Filter Type for IPv6 Source Guard



Security > IPv6 Source Guard > Port Configuration

Port Configuration List Total: 28

Port	Filter Type	Max Binding Entry (1-5)
1	Disabled	5
2	Disabled	5
3	Disabled	5
4	Disabled	5
5	SIP	5

CONFIGURING STATIC BINDINGS FOR IPV6 SOURCE GUARD

Use the Security > IPv6 Source Guard > Static Configuration page to bind a static address to a port. Table entries include a MAC address, IPv6 global unicast address, entry type (Static-IPv6-SG-Binding, Dynamic-ND-Binding, Dynamic-DHCPv6-Binding), VLAN identifier, and port identifier.

CLI REFERENCES

- ◆ "ipv6 source-guard binding" on page 1140

COMMAND USAGE

- Traffic filtering is based only on the source IPv6 address, VLAN ID, and port number.

- Static addresses entered in the source guard binding table are automatically configured with an infinite lease time.

- When source guard is enabled, traffic is filtered based upon dynamic entries learned via ND snooping, DHCPv6 snooping, or static addresses configured in the source guard binding table.

- Static bindings are processed as follows:

  - If there is no entry with same and MAC address and IPv6 address, a new entry is added to binding table using static IPv6 source guard binding.

  - If there is an entry with same MAC address and IPv6 address, and the type of entry is static IPv6 source guard binding, then the new entry will replace the old one.

  - If there is an entry with same MAC address and IPv6 address, and the type of the entry is either a dynamic ND snooping binding or DHCPv6 snooping binding, then the new entry will replace the old one and the entry type will be changed to static IPv6 source guard binding.

  - Only unicast addresses are accepted for static bindings.

PARAMETERS

These parameters are displayed:

Add

- **Port** – The port to which a static entry is bound.

- **VLAN** – ID of a configured VLAN (Range: 1-4094)

- **MAC Address** – A valid unicast MAC address.

- **IPv6 Address** – A valid global unicast IPv6 address. This address must be entered according to RFC 2373 “IPv6 Addressing Architecture,” using 8 colon-separated 16-bit hexadecimal values. One double colon may be used in the address to indicate the appropriate number of zeros required to fill the undefined fields.

Show

- **VLAN** – VLAN to which this entry is bound.

- **MAC Address** – Physical address associated with the entry.

- **Interface** – The port to which this entry is bound.

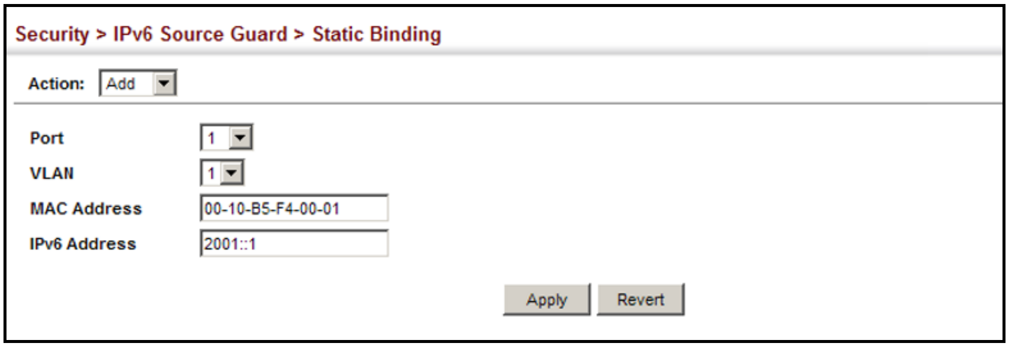
- **IPv6 Address** – IPv6 address corresponding to the client.
- **Type** – Shows the entry type:
  - **DHCP** – Dynamic DHCPv6 binding, stateful address.
  - **ND** – Dynamic Neighbor Discovery binding, stateless address.
  - **STA** – Static IPv6 Source Guard binding.

WEB INTERFACE

To configure static bindings for IPv6 Source Guard:

1. Click Security, IPv6 Source Guard, Static Configuration.
2. Select Add from the Action list.
3. Enter the required bindings for each port.
4. Click Apply

Figure 230: Configuring Static Bindings for IPv6 Source Guard



Security > IPv6 Source Guard > Static Binding

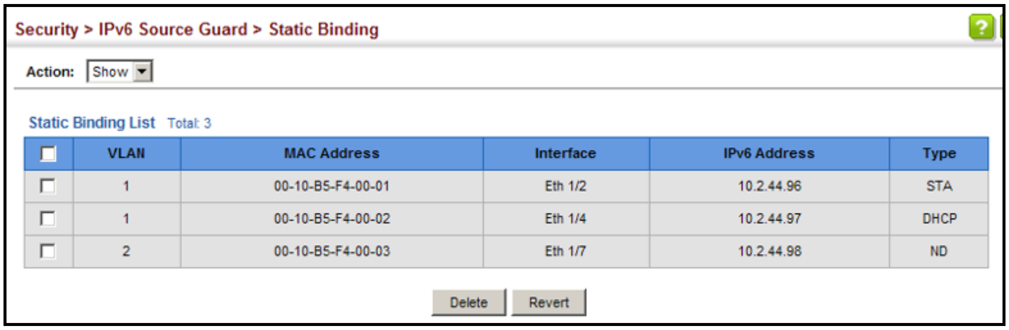
Action: Add

Port	1
VLAN	1
MAC Address	00-10-B5-F4-00-01
IPv6 Address	2001::1

To display static bindings for Iv6 Source Guard:

1. Click Security, IPv6 Source Guard, Static Configuration.
2. Select Show from the Action list.

Figure 231: Displaying Static Bindings for IPv6 Source Guard



Security > IPv6 Source Guard > Static Binding

Action: Show

Static Binding List Total: 3

□	VLAN	MAC Address	Interface	IPv6 Address	Type
□	1	00-10-B5-F4-00-01	Eth 1/2	10.2.44.96	STA
□	1	00-10-B5-F4-00-02	Eth 1/4	10.2.44.97	DHCP
□	2	00-10-B5-F4-00-03	Eth 1/7	10.2.44.98	ND

DISPLAYING INFORMATION FOR DYNAMIC IPV6 SOURCE GUARD BINDINGS

Use the Security > IPv6 Source Guard > Dynamic Binding page to display the source-guard binding table for a selected interface.

CLI REFERENCES

- "show ipv6 source-guard binding" on page 1145

PARAMETERS

These parameters are displayed:

Query by

- **Port** – A port on this switch.
- **VLAN** – ID of a configured VLAN (Range: 1-4094)
- **MAC Address** – A valid unicast MAC address.
- **IPv6 Address** – A valid global unicast IPv6 address.

Dynamic Binding List

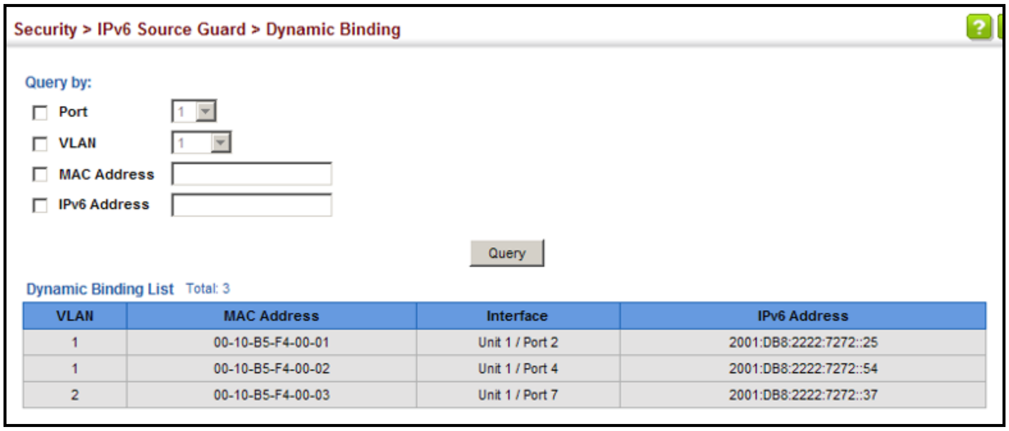
- **VLAN** – VLAN to which this entry is bound.
- **MAC Address** – Physical address associated with the entry.
- **Interface** – Port to which this entry is bound.
- **IPv6 Address** – IPv6 address corresponding to the client.

WEB INTERFACE

To display the binding table for IPv6 Source Guard:

1. Click Security, IPv6 Source Guard, Dynamic Binding.
2. Mark the search criteria, and enter the required values.
3. Click Query

Figure 232: Showing the IPv6 Source Guard Binding Table



Security > IPv6 Source Guard > Dynamic Binding

Query by:

□ Port	1
□ VLAN	1
□ MAC Address	
□ IPv6 Address	

Dynamic Binding List Total: 3

VLAN	MAC Address	Interface	IPv6 Address
1	00-10-B5-F4-00-01	Unit 1 / Port 2	2001:DB8:2222:7272::25
1	00-10-B5-F4-00-02	Unit 1 / Port 4	2001:DB8:2222:7272::54
2	00-10-B5-F4-00-03	Unit 1 / Port 7	2001:DB8:2222:7272::37

DHCP SNOOPING

The addresses assigned to DHCP clients on insecure ports can be carefully controlled using the dynamic bindings registered with DHCP Snooping (or using the static bindings configured with IP Source Guard). DHCP snooping allows a switch to protect a network from rogue DHCP servers or other devices which send port-related information to a DHCP server. This information can be useful in tracking an IP address back to a physical port.

COMMAND USAGE

DHCP Snooping Process

- Network traffic may be disrupted when malicious DHCP messages are received from an outside source. DHCP snooping is used to filter DHCP messages received on a non-secure interface from outside the network or fire wall. When DHCP snooping is enabled globally and enabled on a VLAN interface, DHCP messages received on an untrusted interface from a device not listed in the DHCP snooping table will be dropped.

- Table entries are only learned for trusted interfaces. An entry is added or removed dynamically to the DHCP snooping table when a client receives or releases an IP address from a DHCP server. Each entry includes a MAC address, IP address, lease time, VLAN identifier, and port identifier.

- The rate limit for the number of DHCP messages that can be processed by the switch is 100 packets per second. Any DHCP packets in excess of this limit are dropped.

- When DHCP snooping is enabled, DHCP messages entering an untrusted interface are filtered based upon dynamic entries learned via DHCP snooping.

- Filtering rules are implemented as follows:

  - If the global DHCP snooping is disabled, all DHCP packets are forwarded.

  - If DHCP snooping is enabled globally, and also enabled on the VLAN where the DHCP packet is received, all DHCP packets are forwarded for a *trusted* port. If the received packet is a DHCP ACK message, a dynamic DHCP snooping entry is also added to the binding table.

  - If DHCP snooping is enabled globally, and also enabled on the VLAN where the DHCP packet is received, but the port is *not trusted*, it is processed as follows:

    - If the DHCP packet is a reply packet from a DHCP server (including OFFER, ACK or NAK messages), the packet is dropped.

  - If the DHCP packet is from a client, such as a DECLINE or RELEASE message, the switch forwards the packet only if the corresponding entry is found in the binding table.

  - If the DHCP packet is from a client, such as a DISCOVER, REQUEST, INFORM, DECLINE or RELEASE message, the packet is forwarded if MAC address verification is disabled. However, if MAC address verification is enabled, then the packet will only be forwarded if the client's hardware address stored in the DHCP packet is the same as the source MAC address in the Ethernet header.

  - If the DHCP packet is not a recognizable type, it is dropped.

- If a DHCP packet from a client passes the filtering criteria above, it will only be forwarded to trusted ports in the same VLAN.

- If a DHCP packet is from server is received on a trusted port, it will be forwarded to both trusted and untrusted ports in the same VLAN.

- If the DHCP snooping is globally disabled, all dynamic bindings are removed from the binding table.

- *Additional considerations when the switch itself is a DHCP client* – The port(s) through which the switch submits a client request to the DHCP server must be configured as trusted. Note that the switch will not add a dynamic entry for itself to the binding table when it receives an ACK message from a DHCP server. Also, when the switch sends out DHCP client packets for itself, no filtering takes place. However, when the switch receives any messages from a DHCP server, any packets received from untrusted ports are dropped.

DHCP Snooping Option 82

- DHCP provides a relay mechanism for sending information about its DHCP clients or the relay agent itself to the DHCP server. Also known as DHCP Option 82, it allows compatible DHCP servers to use the information when assigning IP addresses, or to set other services or policies for clients. It is also an effective tool in preventing malicious network attacks from attached clients on DHCP services, such as IP Spoofing, Client Identifier Spoofing, MAC Address Spoofing, and Address Exhaustion.

- DHCP Snooping must be enabled for Option 82 information to be inserted into request packets.

- When the DHCP Snooping Information Option 82 is enabled, the requesting client (or an intermediate relay agent that has used the information fields to describe itself) can be identified in the DHCP request packets forwarded by the switch and in reply packets sent back from the DHCP server. This information may specify the MAC address or IP address of the requesting device (that is, the switch in this context).

  By default, the switch also fills in the Option 82 circuit-id field with information indicating the local interface over which the switch received the DHCP client request, including the port and VLAN ID. This allows DHCP client-server exchange messages to be forwarded between the server and client without having to flood them to the entire VLAN.

- If DHCP Snooping Information Option 82 is enabled on the switch, information may be inserted into a DHCP request packet received over any VLAN (depending on DHCP snooping filtering rules). The information inserted into the relayed packets includes the circuit-id and remote-id, as well as the gateway Internet address.

- When the switch receives DHCP packets from clients that already include DHCP Option 82 information, the switch can be configured to set the action policy for these packets. The switch can either drop the DHCP packets, keep the existing information, or replace it with the switch's relay information.

DHCP SNOOPING CONFIGURATION

Use the IP Service > DHCP > Snooping (Configure Global) page to enable DHCP Snooping globally on the switch, or to configure MAC Address Verification.

CLI REFERENCES

- "DHCPv4 Snooping" on page 1115

PARAMETERS

These parameters are displayed:

- **DHCP Snooping Status –** Enables DHCP snooping globally. (Default: Disabled)

- **DHCP Snooping MAC-Address Verification** – Enables or disables MAC address verification. If the source MAC address in the Ethernet header of the packet is not same as the client's hardware address in the DHCP packet, the packet is dropped. (Default: Enabled)

- **DHCP Snooping Information Option Status** – Enables or disables DHCP Option 82 information relay. (Default: Disabled)

- **DHCP Snooping Information Option Sub-option Format** – Enables or disables use of sub-type and sub-length fields in circuit-ID (CID) and remote-ID (RID) in Option 82 information.

- **DHCP Snooping Information Option Remote ID** – Specifies the MAC address, IP address, or arbitrary identifier of the requesting device (i.e., the switch in this context).

  - **MAC Address** – Inserts a MAC address in the remote ID sub-option for the DHCP snooping agent (i.e., the MAC address of the switch's CPU). This attribute can be encoded in Hexadecimal or ASCII.

  - **IP Address** – Inserts an IP address in the remote ID sub-option for the DHCP snooping agent (i.e., the IP address of the management interface). This attribute can be encoded in Hexadecimal or ASCII.

- *string* - An arbitrary string inserted into the remote identifier field. (Range: 1-32 characters)

◆ **DHCP Snooping Information Option Policy** – Specifies how to handle DHCP client request packets which already contain Option 82 information.

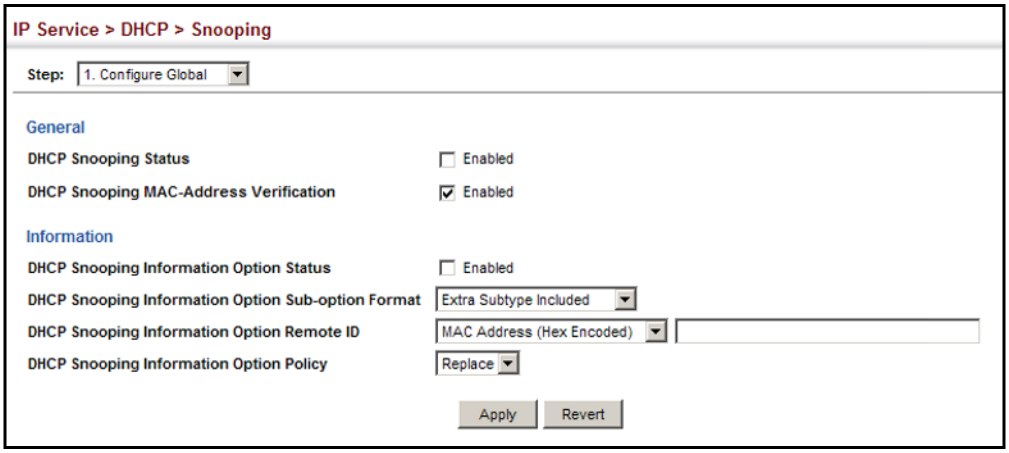
- **Drop** – Drops the client’s request packet instead of relaying it.
- **Keep** – Retains the Option 82 information in the client request, and forwards the packets to trusted ports.
- **Replace** – Replaces the Option 82 information circuit-id and remote-id fields in the client’s request with information about the relay agent itself, inserts the relay agent’s address (when DHCP snooping is enabled), and forwards the packets to trusted ports. (This is the default policy.)

WEB INTERFACE

To configure global settings for DHCP Snooping:

1. Click IP Service, DHCP, Snooping.
2. Select Configure Global from the Step list.
3. Select the required options for the general DHCP snooping process and for the DHCP Option 82 information policy.
4. Click Apply

Figure 233: Configuring Global Settings for DHCP Snooping



IP Service > DHCP > Snooping

Step: 1. Configure Global

General

DHCP Snooping Status □ Enabled

DHCP Snooping MAC-Address Verification ☑ Enabled

Information

DHCP Snooping Information Option Status □ Enabled

DHCP Snooping Information Option Sub-option Format: Extra Subtype Included

DHCP Snooping Information Option Remote ID: MAC Address (Hex Encoded)

DHCP Snooping Information Option Policy: Replace

DHCP SNOOPING VLAN CONFIGURATION

Use the IP Service > DHCP > Snooping (Configure VLAN) page to enable or disable DHCP snooping on specific VLANs.

CLI REFERENCES

- "ip dhcp snooping vlan" on page 1121

COMMAND USAGE

- When DHCP snooping is enabled globally on the switch, and enabled on the specified VLAN, DHCP packet filtering will be performed on any untrusted ports within the VLAN.

- When the DHCP snooping is globally disabled, DHCP snooping can still be configured for specific VLANs, but the changes will not take effect until DHCP snooping is globally re-enabled.

- When DHCP snooping is globally enabled, and DHCP snooping is then disabled on a VLAN, all dynamic bindings learned for this VLAN are removed from the binding table.

PARAMETERS

These parameters are displayed:

- **VLAN** – ID of a configured VLAN. (Range: 1-4094)

- **DHCP Snooping Status** – Enables or disables DHCP snooping for the selected VLAN. When DHCP snooping is enabled globally on the switch, and enabled on the specified VLAN, DHCP packet filtering will be performed on any untrusted ports within the VLAN. (Default: Disabled)

WEB INTERFACE

To configure global settings for DHCP Snooping:

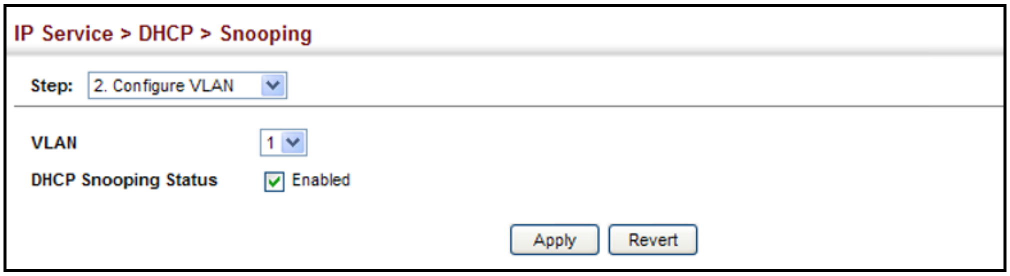
1. Click IP Service, DHCP, Snooping.

2. Select Configure VLAN from the Step list.

3. Enable DHCP Snooping on any existing VLAN.

4. Click Apply

Figure 234: Configuring DHCP Snooping on a VLAN



IP Service > DHCP > Snooping

Step: 2. Configure VLAN

VLAN 1

DHCP Snooping Status ☑ Enabled

CONFIGURING PORTS FOR DHCP SNOOPING

Use the IP Service > DHCP > Snooping (Configure Interface) page to configure switch ports as trusted or untrusted.

CLI REFERENCES

- "ip dhcp snooping trust" on page 1123

COMMAND USAGE

- A trusted interface is an interface that is configured to receive only messages from within the network. An untrusted interface is an interface that is configured to receive messages from outside the network or fire wall.
- When DHCP snooping is enabled both globally and on a VLAN, DHCP packet filtering will be performed on any untrusted ports within the VLAN.
- When an untrusted port is changed to a trusted port, all the dynamic DHCP snooping bindings associated with this port are removed.
- Set all ports connected to DHCP servers within the local network or fire wall to trusted state. Set all other ports outside the local network or fire wall to untrusted state.

PARAMETERS

These parameters are displayed:

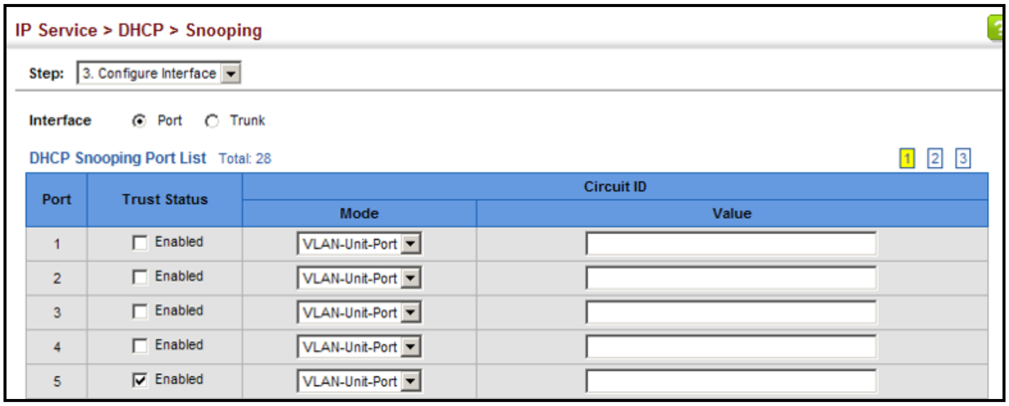
- **Trust Status** – Enables or disables a port as trusted. (Default: Disabled)
- **Circuit ID** – Specifies DHCP Option 82 circuit ID suboption information.
  - **Mode** – Specifies the default string “VLAN-Unit-Port” or an arbitrary string. (Default: VLAN-Unit-Port)
  - **Value** – An arbitrary string inserted into the circuit identifier field. (Range: 1-32 characters)

WEB INTERFACE

To configure global settings for DHCP Snooping:

1. Click IP Service, DHCP, Snooping.
2. Select Configure Interface from the Step list.
3. Set any ports within the local network or firewall to trusted.
4. Click Apply

Figure 235: Configuring the Port Mode for DHCP Snooping



IP Service > DHCP > Snooping

Step: 3. Configure Interface

Interface ● Port ○ Trunk

DHCP Snooping Port List Total: 28

1 2 3

Port	Trust Status	Circuit ID	
		Mode	Value
1	□ Enabled	VLAN-Unit-Port	
2	□ Enabled	VLAN-Unit-Port	
3	□ Enabled	VLAN-Unit-Port	
4	□ Enabled	VLAN-Unit-Port	
5	☑ Enabled	VLAN-Unit-Port	

DISPLAYING DHCP SNOOPING BINDING INFORMATION

Use the IP Service > DHCP > Snooping (Show Information) page to display entries in the binding table.

CLI REFERENCES

- "show ip dhcp snooping binding" on page 1126

PARAMETERS

These parameters are displayed:

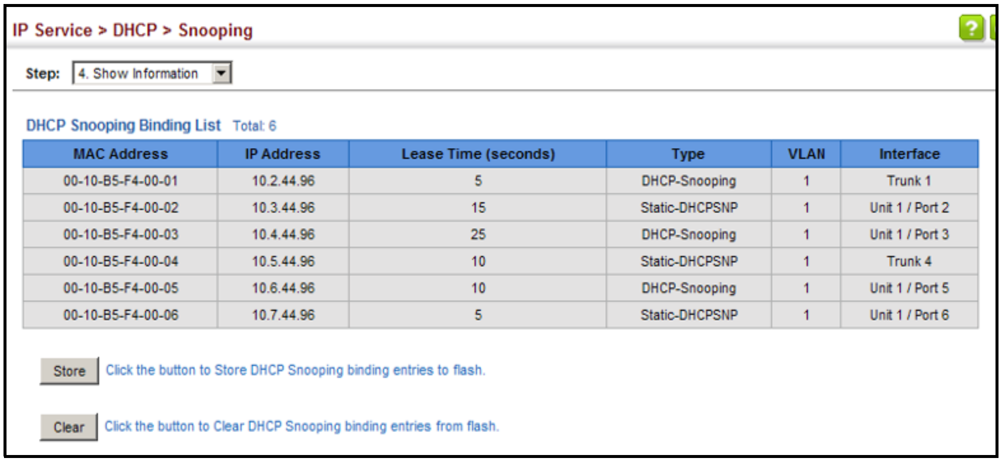
- **MAC Address** – Physical address associated with the entry.
- **IP Address** – IP address corresponding to the client.
- **Lease Time** – The time for which this IP address is leased to the client.
- **Type** – Entry types include:
  - **DHCP-Snooping** – Dynamically snooped.
  - **Static-DHCPSNP** – Statically configured.
- **VLAN** – VLAN to which this entry is bound.
- **Interface** – Port or trunk to which this entry is bound.
- **Store** – Writes all dynamically learned snooping entries to flash memory. This function can be used to store the currently learned dynamic DHCP snooping entries to flash memory. These entries will be restored to the snooping table when the switch is reset. However, note that the lease time shown for a dynamic entry that has been restored from flash memory will no longer be valid.
- **Clear** – Removes all dynamically learned snooping entries from flash memory.

WEB INTERFACE

To display the binding table for DHCP Snooping:

1. Click IP Service, DHCP, Snooping.
2. Select Show Information from the Step list.
3. Use the Store or Clear function if required.

Figure 236: Displaying the Binding Table for DHCP Snooping



IP Service > DHCP > Snooping

Step: 4. Show Information

DHCP Snooping Binding List Total: 6

MAC Address	IP Address	Lease Time (seconds)	Type	VLAN	Interface
00-10-B5-F4-00-01	10.2.44.96	5	DHCP-Snooping	1	Trunk 1
00-10-B5-F4-00-02	10.3.44.96	15	Static-DHCPSNP	1	Unit 1 / Port 2
00-10-B5-F4-00-03	10.4.44.96	25	DHCP-Snooping	1	Unit 1 / Port 3
00-10-B5-F4-00-04	10.5.44.96	10	Static-DHCPSNP	1	Trunk 4
00-10-B5-F4-00-05	10.6.44.96	10	DHCP-Snooping	1	Unit 1 / Port 5
00-10-B5-F4-00-06	10.7.44.96	5	Static-DHCPSNP	1	Unit 1 / Port 6

Click the button to Store DHCP Snooping binding entries to flash.

Click the button to Clear DHCP Snooping binding entries from flash.

14 Basic Administration Protocols

This chapter describes basic administration tasks including:

- Event Logging – Sets conditions for logging event messages to system memory or flash memory, configures conditions for sending trap messages to remote log servers, and configures trap reporting to remote hosts using Simple Mail Transfer Protocol (SMTP).
- Link Layer Discovery Protocol (LLDP) – Configures advertisement of basic information about the local switch, or discovery of information about neighboring devices on the local broadcast domain.
- Simple Network Management Protocol (SNMP) – Configures switch management through SNMPv1, SNMPv2c or SNMPv3.
- Remote Monitoring (RMON) – Configures local collection of detailed statistics or events which can be subsequently retrieved through SNMP.
- Switch Clustering – Configures centralized management by a single unit over a group of switches connected to the same local network.
- Ethernet Ring Protection Switching (ERPS) – Configures a protection switching mechanism and protocol for Ethernet layer network rings.
- Connectivity Fault Management (CFM) – This protocol provides proactive connectivity monitoring using continuity check messages, fault verification through loop back messages, and fault isolation by examining end-to-end connections between provider edge devices or between customer edge devices.
- Operation, Administration and Maintenance (OAM) – Provides remote management tools required to monitor and maintain the links to subscriber CPEs (Customer Premise Equipment).
- Precision Time Protocol (PTP) – Configures clock synchronization for the local network.

CONFIGURING EVENT LOGGING

The switch allows you to control the logging of error messages, including the type of events that are recorded in switch memory, logging to a remote System Log (syslog) server, and displays a list of recent event messages.

SYSTEM LOG CONFIGURATION

Use the Administration > Log > System (Configure Global) page to enable or disable event logging, and specify which levels are logged to RAM or flash memory.

Severe error messages that are logged to flash memory are permanently stored in the switch to assist in troubleshooting network problems. Up to 4096 log entries can be stored in the flash memory, with the oldest entries being overwritten first when the available log memory (256 kilobytes) has been exceeded.

The System Logs page allows you to configure and limit system messages that are logged to flash or RAM memory. The default is for event levels 0 to 3 to be logged to flash and levels 0 to 7 to be logged to RAM.

CLI REFERENCES

- "Event Logging" on page 933

PARAMETERS

These parameters are displayed:

- **System Log Status** – Enables/disables the logging of debug or error messages to the logging process. (Default: Enabled)

- **Flash Level** – Limits log messages saved to the switch’s permanent flash memory for all levels up to the specified level. For example, if level 3 is specified, all messages from level 0 to level 3 will be logged to flash. (Range: 0-7, Default: 3)

Table 27: Logging Levels

Level	Severity Name	Description
7	Debug	Debugging messages
6	Informational	Informational messages only
5	Notice	Normal but significant condition, such as cold start
4	Warning	Warning conditions (e.g., return false, unexpected return)
3	Error	Error conditions (e.g., invalid input, default used)
2	Critical	Critical conditions (e.g., memory allocation, or free memory error - resource exhausted)
1	Alert	Immediate action needed
0	Emergency	System unusable

* There are only Level 2, 5 and 6 error messages for the current firmware release.

- **RAM Level** – Limits log messages saved to the switch's temporary RAM memory for all levels up to the specified level. For example, if level 7 is specified, all messages from level 0 to level 7 will be logged to RAM. (Range: 0-7, Default: 7)

NOTE: The Flash Level must be equal to or less than the RAM Level.

NOTE: All log messages are retained in RAM and Flash after a warm restart (i.e., power is reset through the command interface).

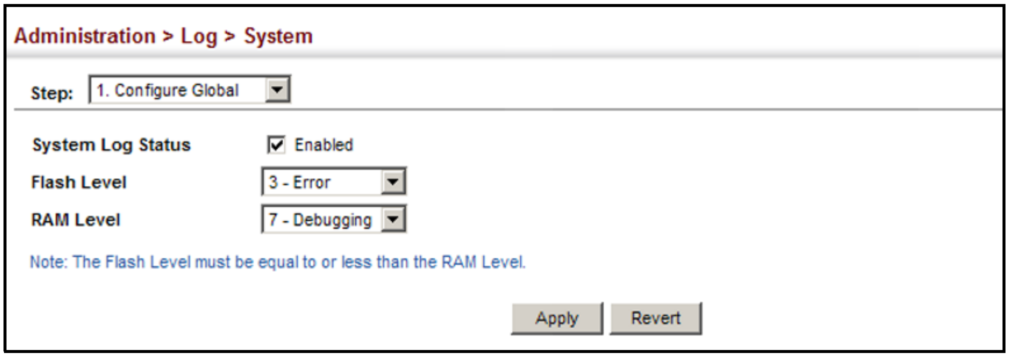
NOTE: All log messages are retained in Flash and purged from RAM after a cold restart (i.e., power is turned off and then on through the power source).

WEB INTERFACE

To configure the logging of error messages to system memory:

1. Click Administration, Log, System.
2. Select Configure Global from the Step list.
3. Enable or disable system logging, set the level of event messages to be logged to flash memory and RAM.
4. Click Apply.

Figure 237: Configuring Settings for System Memory Logs



Administration > Log > System

Step: 1. Configure Global

System Log Status ☑ Enabled

Flash Level 3 - Error

RAM Level 7 - Debugging

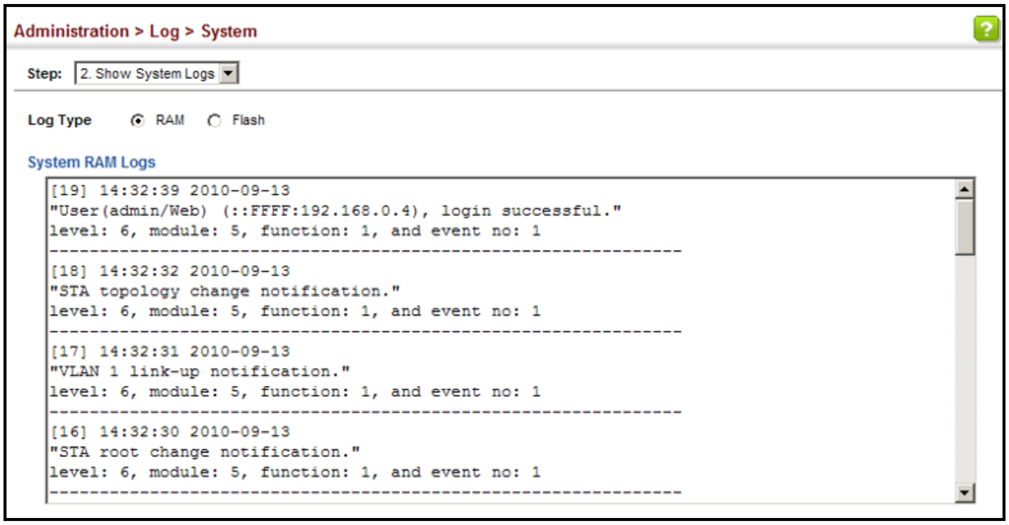
Note: The Flash Level must be equal to or less than the RAM Level.

To show the error messages logged to system or flash memory:

1. Click Administration, Log, System.
2. Select Show System Logs from the Step list.
3. Click RAM to display log messages stored in system memory, or Flash to display messages stored in flash memory.

   This page allows you to scroll through the logged system and event messages. The switch can store up to 2048 log entries in temporary random access memory (RAM; i.e., memory flushed on power reset) and up to 4096 entries in permanent flash memory.

Figure 238: Showing Error Messages Logged to System Memory



```
[19] 14:32:39 2010-09-13
"User(admin/Web) (::FFFF:192.168.0.4), login successful."
level: 6, module: 5, function: 1, and event no: 1
----------------------------------------------------------------
[18] 14:32:32 2010-09-13
"STA topology change notification."
level: 6, module: 5, function: 1, and event no: 1
----------------------------------------------------------------
[17] 14:32:31 2010-09-13
"VLAN 1 link-up notification."
level: 6, module: 5, function: 1, and event no: 1
----------------------------------------------------------------
[16] 14:32:30 2010-09-13
"STA root change notification."
level: 6, module: 5, function: 1, and event no: 1
----------------------------------------------------------------
```

REMOTE LOG CONFIGURATION

Use the Administration > Log > Remote page to send log messages to syslog servers or other management stations. You can also limit the event messages sent to only those messages below a specified level.

CLI REFERENCES

- "Event Logging" on page 933

PARAMETERS

These parameters are displayed:

- **Remote Log Status** – Enables/disables the logging of debug or error messages to the remote logging process. (Default: Disabled)
- **Logging Facility** – Sets the facility type for remote logging of syslog messages. There are eight facility types specified by values of 16 to 23. The facility type is used by the syslog server to dispatch log messages to an appropriate service.

  The attribute specifies the facility type tag sent in syslog messages (see RFC 3164). This type has no effect on the kind of messages reported by the switch. However, it may be used by the syslog server to process messages, such as sorting or storing messages in the corresponding database. (Range: 16-23, Default: 23)
- **Logging Trap Level** – Limits log messages that are sent to the remote syslog server for all levels up to the specified level. For example, if level 3 is specified, all messages from level 0 to level 3 will be sent to the remote server. (Range: 0-7, Default: 7)
- **Server IP Address** – Specifies the IPv4 or IPv6 address of a remote server which will be sent syslog messages.

WEB INTERFACE

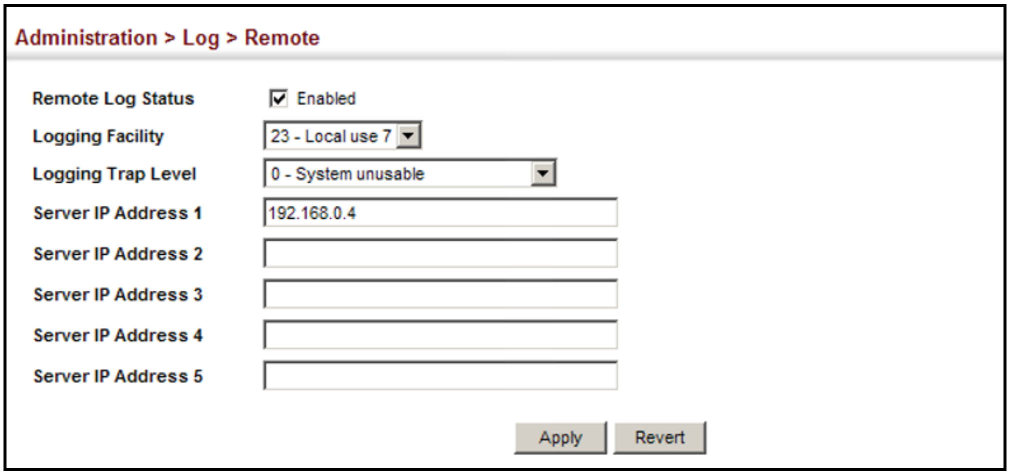
To configure the logging of error messages to remote servers:

1. Click Administration, Log, Remote.

2. Enable remote logging, specify the facility type to use for the syslog messages. and enter the IP address of the remote servers.

3. Click Apply.

Figure 239: Configuring Settings for Remote Logging of Error Messages



Administration > Log > Remote

Remote Log Status	☑ Enabled
Logging Facility	23 - Local use 7
Logging Trap Level	0 - System unusable
Server IP Address 1	192.168.0.4
Server IP Address 2	
Server IP Address 3	
Server IP Address 4	
Server IP Address 5	

SENDING SIMPLE MAIL TRANSFER PROTOCOL ALERTS

Use the Administration > Log > SMTP page to alert system administrators of problems by sending SMTP (Simple Mail Transfer Protocol) email messages when triggered by logging events of a specified level. The messages are sent to specified SMTP servers on the network and can be retrieved using POP or IMAP clients.

CLI REFERENCES

- "SMTP Alerts" on page 940

PARAMETERS

These parameters are displayed:

- **SMTP Status** – Enables/disables the SMTP function. (Default: Enabled)

- **Severity** – Sets the syslog severity threshold level (see table on page 454) used to trigger alert messages. All events at this level or higher will be sent to the configured email recipients. For example, using Level 7 will report all events from level 7 to level 0. (Default: Level 7)

- **Email Source Address** – Sets the email address used for the "From" field in alert messages. You may use a symbolic email address that identifies the switch, or the address of an administrator responsible for the switch.

- **Email Destination Address** – Specifies the email recipients of alert messages. You can specify up to five recipients.

- **Server IP Address** – Specifies a list of up to three recipient SMTP servers. IPv4 or IPv6 addresses may be specified. The switch attempts to connect to the listed servers in sequential order if the first server fails to respond.

WEB INTERFACE

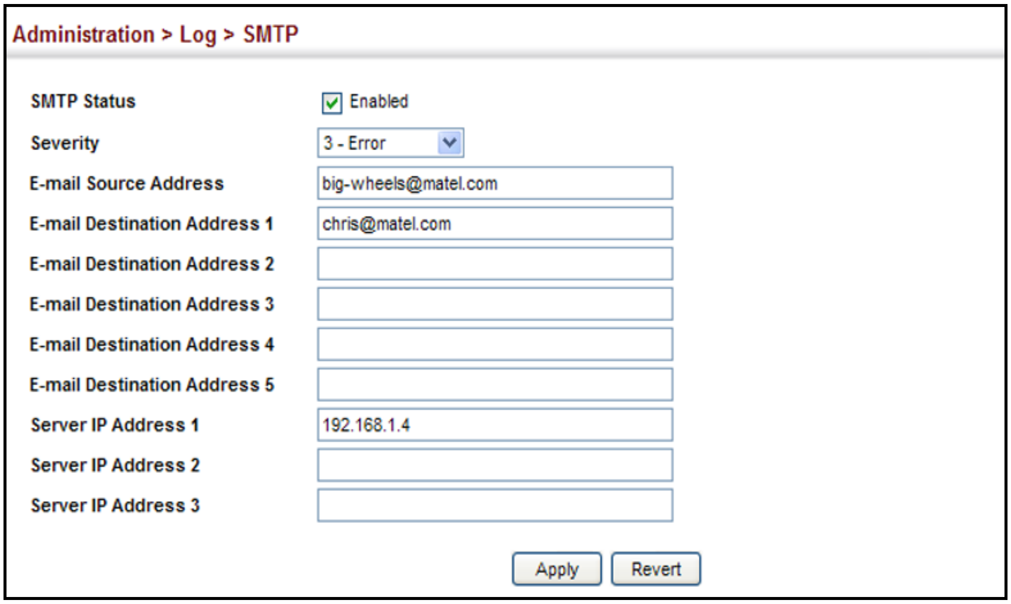
To configure SMTP alert messages:

1. Click Administration, Log, SMTP.

2. Enable SMTP, specify a source email address, and select the minimum severity level. Specify the source and destination email addresses, and one or more SMTP servers.

3. Click Apply.

Figure 240: Configuring SMTP Alert Messages



Administration > Log > SMTP

SMTP Status	☑ Enabled
Severity	3 - Error
E-mail Source Address	big-wheels@matel.com
E-mail Destination Address 1	chris@matel.com
E-mail Destination Address 2	
E-mail Destination Address 3	
E-mail Destination Address 4	
E-mail Destination Address 5	
Server IP Address 1	192.168.1.4
Server IP Address 2	
Server IP Address 3	

LINK LAYER DISCOVERY PROTOCOL

Link Layer Discovery Protocol (LLDP) is used to discover basic information about neighboring devices on the local broadcast domain. LLDP is a Layer 2 protocol that uses periodic broadcasts to advertise information about the sending device. Advertised information is represented in Type Length Value (TLV) format according to the IEEE 802.1ab standard, and can include details such as device identification, capabilities and configuration settings. LLDP also defines how to store and maintain information gathered about the neighboring network nodes it discovers.

Link Layer Discovery Protocol - Media Endpoint Discovery (LLDP-MED) is an extension of LLDP intended for managing endpoint devices such as Voice over IP phones and network switches. The LLDP-MED TLVs advertise information such as network policy, power, inventory, and device location details. LLDP and LLDP-MED information can be used by SNMP applications to simplify troubleshooting, enhance network management, and maintain an accurate network topology.

SETTING LLDP TIMING ATTRIBUTES

Use the Administration > LLDP (Configure Global) page to set attributes for general functions such as globally enabling LLDP on the switch, setting the message ageout time, and setting the frequency for broadcasting general advertisements or reports about changes in the LLDP MIB.

CLI REFERENCES

- "LLDP Commands" on page 1537

PARAMETERS

These parameters are displayed:

- **LLDP** – Enables LLDP globally on the switch. (Default: Enabled)

- **Transmission Interval** – Configures the periodic transmit interval for LLDP advertisements. (Range: 5-32768 seconds; Default: 30 seconds)

- **Hold Time Multiplier** – Configures the time-to-live (TTL) value sent in LLDP advertisements as shown in the formula below. (Range: 2-10; Default: 4)

  The time-to-live tells the receiving LLDP agent how long to retain all information pertaining to the sending LLDP agent if it does not transmit updates in a timely manner.

  TTL in seconds is based on the following rule:
  minimum value ((Transmission Interval * Holdtime Multiplier), or 65535)

  Therefore, the default TTL is 4*30 = 120 seconds.

- **Delay Interval** – Configures a delay between the successive transmission of advertisements initiated by a change in local LLDP MIB variables. (Range: 1-8192 seconds; Default: 2 seconds)

  The transmit delay is used to prevent a series of successive LLDP transmissions during a short period of rapid changes in local LLDP MIB objects, and to increase the probability that multiple, rather than single changes, are reported in each transmission.

  This attribute must comply with the rule:
  (4 * Delay Interval) ≤ Transmission Interval

- **Reinitialization Delay** – Configures the delay before attempting to re-initialize after LLDP ports are disabled or the link goes down. (Range: 1-10 seconds; Default: 2 seconds)

  When LLDP is re-initialized on a port, all information in the remote systems LLDP MIB associated with this port is deleted.

- **Notification Interval** – Configures the allowed interval for sending SNMP notifications about LLDP MIB changes. (Range: 5-3600 seconds; Default: 5 seconds)

  This parameter only applies to SNMP applications which use data stored in the LLDP MIB for network monitoring or management.

  Information about changes in LLDP neighbors that occur between SNMP notifications is not transmitted. Only state changes that exist at the time of a notification are included in the transmission. An SNMP agent should therefore periodically check the value of lldpStatsRemTableLastChangeTime to detect any lldpRemTablesChange notification-events missed due to throttling or transmission loss.

- **MED Fast Start Count** – Configures the amount of LLDP MED Fast Start LLDPDUs to transmit during the activation process of the LLDP-MED Fast Start mechanism. (Range: 1-10 packets; Default: 4 packets)

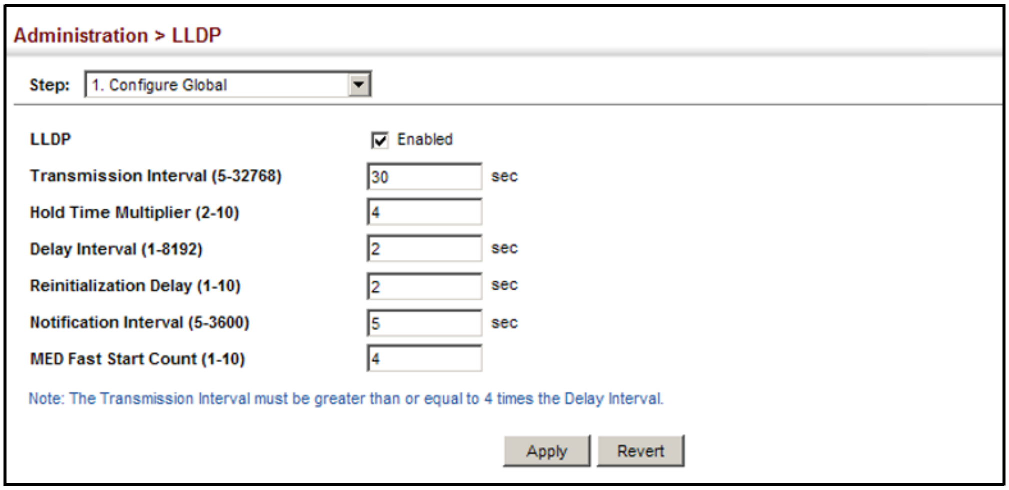
  The MED Fast Start Count parameter is part of the timer which ensures that the LLDP-MED Fast Start mechanism is active for the port. LLDP-MED Fast Start is critical to the timely startup of LLDP, and therefore integral to the rapid availability of Emergency Call Service.

WEB INTERFACE

To configure LLDP timing attributes:

1. Click Administration, LLDP.
2. Select Configure Global from the Step list.
3. Enable LLDP, and modify any of the timing parameters as required.
4. Click Apply.

Figure 241: Configuring LLDP Timing Attributes



Administration > LLDP

Step: 1. Configure Global

LLDP	☑ Enabled	
Transmission Interval (5-32768)	30	sec
Hold Time Multiplier (2-10)	4	
Delay Interval (1-8192)	2	sec
Reinitialization Delay (1-10)	2	sec
Notification Interval (5-3600)	5	sec
MED Fast Start Count (1-10)	4	

Note: The Transmission Interval must be greater than or equal to 4 times the Delay Interval.

CONFIGURING LLDP INTERFACE ATTRIBUTES

Use the Administration > LLDP (Configure Interface) page to specify the message attributes for individual interfaces, including whether messages are transmitted, received, or both transmitted and received, whether SNMP notifications are sent, and the type of information advertised.

CLI REFERENCES

- "LLDP Commands" on page 1537

PARAMETERS

These parameters are displayed:

- **Admin Status** – Enables LLDP message transmit and receive modes for LLDP Protocol Data Units. (Options: Tx only, Rx only, TxRx, Disabled; Default: TxRx)

- **SNMP Notification** – Enables the transmission of SNMP trap notifications about LLDP and LLDP-MED changes. (Default: Disabled)

  This option sends out SNMP trap notifications to designated target stations at the interval specified by the Notification Interval in the preceding section. Trap notifications include information about state changes in the LLDP MIB (IEEE 802.1AB), the LLDP-MED MIB (ANSI/TIA-1057), or vendor-specific LLDP-EXT-DOT1 and LLDP-EXT-DOT3 MIBs.

  For information on defining SNMP trap destinations, see "Specifying Trap Managers" on page 500.

  Information about additional changes in LLDP neighbors that occur between SNMP notifications is not transmitted. Only state changes that exist at the time of a trap notification are included in the transmission. An SNMP agent should therefore periodically check the value of lldpStatsRemTableLastChangeTime to detect any lldpRemTablesChange notification-events missed due to throttling or transmission loss.

- **MED Notification** – Enables the transmission of SNMP trap notifications about LLDP-MED changes. (Default: Disabled)

- **Basic Optional TLVs** – Configures basic information included in the TLV field of advertised messages.

  - **Management Address** – The management address protocol packet includes the IPv4 address of the switch. If no management address is available, the address should be the MAC address for the CPU or for the port sending this advertisement.

    The management address TLV may also include information about the specific interface associated with this address, and an object identifier indicating the type of hardware component or protocol entity associated with this address. The interface number and OID are included to assist SNMP applications in the performance of network discovery by indicating enterprise specific or other starting points for the search, such as the Interface or Entity MIB.

Since there are typically a number of different addresses associated with a Layer 3 device, an individual LLDP PDU may contain more than one management address TLV.

Every management address TLV that reports an address that is accessible on a port and protocol VLAN through the particular port should be accompanied by a port and protocol VLAN TLV that indicates the VLAN identifier (VID) associated with the management address reported by this TLV.

  - **Port Description** – The port description is taken from the ifDescr object in RFC 2863, which includes information about the manufacturer, the product name, and the version of the interface hardware/software.
  - **System Capabilities** – The system capabilities identifies the primary function(s) of the system and whether or not these primary functions are enabled. The information advertised by this TLV is described in IEEE 802.1AB.
  - **System Description** – The system description is taken from the sysDescr object in RFC 3418, which includes the full name and version identification of the system's hardware type, software operating system, and networking software.
  - **System Name** – The system name is taken from the sysName object in RFC 3418, which contains the system’s administratively assigned name. To configure the system name, see "Displaying System Information" on page 149.

- **802.1 Organizationally Specific TLVs** – Configures IEEE 802.1 information included in the TLV field of advertised messages.
  - **Protocol Identity** – The protocols that are accessible through this interface (see "Protocol VLANs" on page 251).
  - **VLAN ID** – The port’s default VLAN identifier (PVID) indicates the VLAN with which untagged or priority-tagged frames are associated (see "IEEE 802.1Q VLANs" on page 225).
  - **VLAN Name** – The name of all VLANs to which this interface has been assigned (see "IEEE 802.1Q VLANs" on page 225).
  - **Port and Protocol VLAN ID** – The port-based protocol VLANs configured on this interface (see "Protocol VLANs" on page 251).
- **802.3 Organizationally Specific TLVs** – Configures IEEE 802.3 information included in the TLV field of advertised messages.
  - **Link Aggregation** – The link aggregation capabilities, aggregation status of the link, and the IEEE 802.3 aggregated port identifier if this interface is currently a link aggregation member.

  - **Max Frame Size** – The maximum frame size. (See "Configuring Support for Jumbo Frames" on page 152 for information on configuring the maximum frame size for this switch

  - **MAC/PHY Configuration/Status** – The MAC/PHY configuration and status which includes information about auto-negotiation support/capabilities, and operational Multistation Access Unit (MAU) type.

- **MED TLVs** – Configures general information included in the MED TLV field of advertised messages.

  - **Capabilities** – This option advertises LLDP-MED TLV capabilities, allowing Media Endpoint and Connectivity Devices to efficiently discover which LLDP-MED related TLVs are supported on the switch.

  - **Inventory** – This option advertises device details useful for inventory management, such as manufacturer, model, software version and other pertinent information.

  - **Location** – This option advertises location identification details.

  - **Network Policy** – This option advertises network policy configuration information, aiding in the discovery and diagnosis of VLAN configuration mismatches on a port. Improper network policy configurations frequently result in voice quality degradation or complete service disruption.

- **MED-Location Civic Address** – Configures information for the location of the attached device included in the MED TLV field of advertised messages, including the country and the device type.

  - **Country** – The two-letter ISO 3166 country code in capital ASCII letters. (Example: DK, DE or US)

  - **Device entry refers to** – The type of device to which the location applies:

    - Location of DHCP server.
    - Location of network element closest to client.
    - Location of client. (This is the default.)

WEB INTERFACE

To configure LLDP interface attributes:

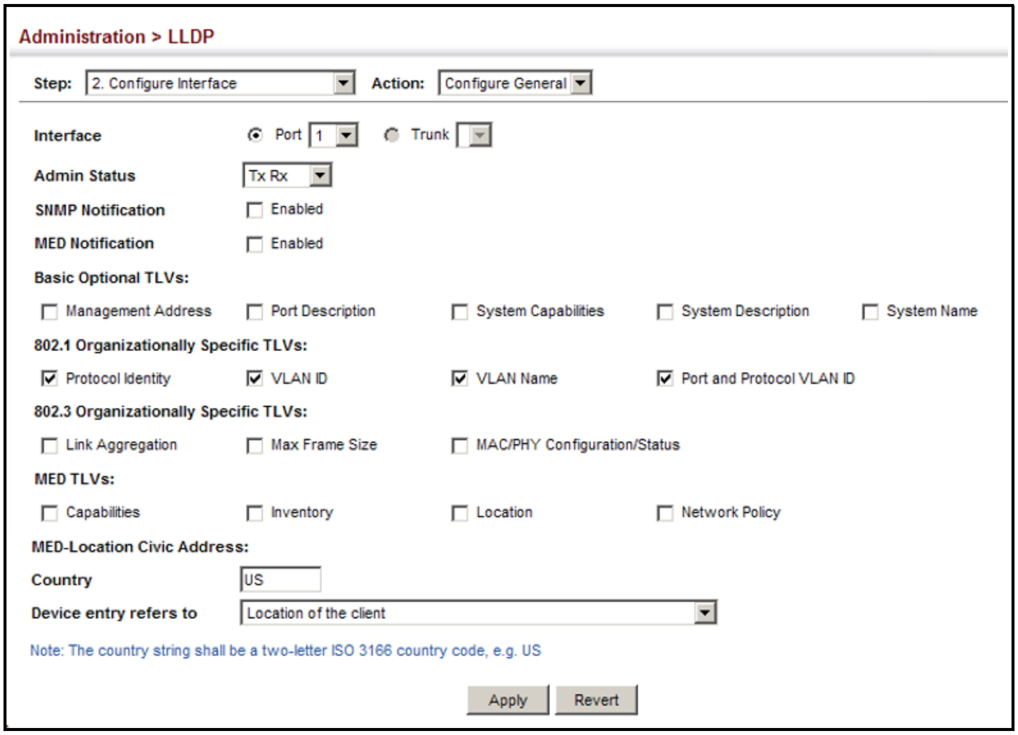
1. Click Administration, LLDP.

2. Select Configure Interface from the Step list.

3. Set the LLDP transmit/receive mode, specify whether or not to send SNMP trap messages, and select the information to advertise in LLDP messages.

4. Click Apply.

Figure 242: Configuring LLDP Interface Attributes



Administration > LLDP

Step: 2. Configure Interface Action: Configure General

Interface ● Port 1 ○ Trunk

Admin Status: Tx Rx

SNMP Notification: □ Enabled

MED Notification: □ Enabled

Basic Optional TLVs:

□ Management Address □ Port Description □ System Capabilities □ System Description □ System Name

802.1 Organizationally Specific TLVs:

☑ Protocol Identity ☑ VLAN ID ☑ VLAN Name ☑ Port and Protocol VLAN ID

802.3 Organizationally Specific TLVs:

□ Link Aggregation □ Max Frame Size □ MAC/PHY Configuration/Status

MED TLVs:

□ Capabilities □ Inventory □ Location □ Network Policy

MED-Location Civic Address:

Country: US

Device entry refers to: Location of the client

Note: The country string shall be a two-letter ISO 3166 country code, e.g. US

CONFIGURING LLDP INTERFACE CIVIC-ADDRESS

Use the Administration > LLDP (Configure Interface – Add CA-Type) page to specify the physical location of the device attached to an interface.

CLI REFERENCES

- "lldp med-location civic-addr" on page 1550

COMMAND USAGE

- Use the Civic Address type (CA-Type) to advertise the physical location of the device attached to an interface, including items such as the city, street number, building and room information. The address location is specified as a type and value pair, with the civic address type defined in RFC 4776. The following table describes some of the CA type numbers and provides examples.

Table 28: LLDP MED Location CA Types

CA Type	Description	CA Value Example
1	National subdivisions (state, canton, province)	California
2	County, parish	Orange
3	City, township	Irvine
4	City division, borough, city district	West Irvine
5	Neighborhood, block	Riverside
6	Group of streets below the neighborhood level	Exchange
18	Street suffix or type	Avenue
19	House number	320
20	House number suffix	A
21	Landmark or vanity address	Tech Center
26	Unit (apartment, suite)	Apt 519
27	Floor	5
28	Room	509B

- Any number of CA type and value pairs can be specified for the civic address location, as long as the total does not exceed 250 characters.

PARAMETERS

These parameters are displayed in the web interface:

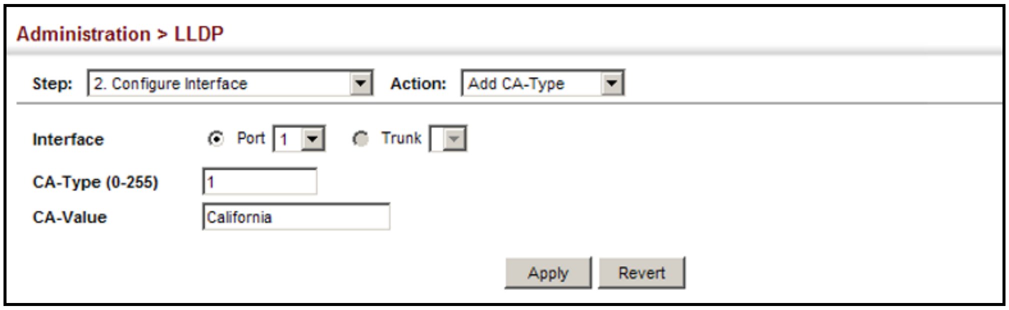
- **CA-Type** – Descriptor of the data civic address value. (Range: 0-255)
- **CA-Value** – Description of a location. (Range: 1-32 characters)

WEB INTERFACE

To specify the physical location of the attached device:

1. Click Administration, LLDP.
2. Select Configure Interface from the Step list.
3. Select Add CA-Type from the Action list.
4. Select an interface from the Port or Trunk list.
5. Specify a CA-Type and CA-Value pair.
6. Click Apply.

Figure 243: Configuring the Civic Address for an LLDP Interface



Administration > LLDP

Step: 2. Configure Interface Action: Add CA-Type

Interface ● Port 1 ○ Trunk

CA-Type (0-255) 1

CA-Value California

DISPLAYING LLDP LOCAL DEVICE INFORMATION

Use the Administration > LLDP (Show Local Device Information) page to display information about the switch, such as its MAC address, chassis ID, management IP address, and port information.

CLI REFERENCES

- "show lldp info local-device" on page 1556

PARAMETERS

These parameters are displayed:

Global Settings

- **Chassis Type** – Identifies the chassis containing the IEEE 802 LAN entity associated with the transmitting LLDP agent. There are several ways in which a chassis may be identified and a chassis ID subtype is used to indicate the type of component being referenced by the chassis ID field.

Table 29: Chassis ID Subtype

ID Basis	Reference
Chassis component	EntPhysicalAlias when entPhysClass has a value of 'chassis(3)' (IETF RFC 2737)
Interface alias	IfAlias (IETF RFC 2863)
Port component	EntPhysicalAlias when entPhysicalClass has a value 'port(10)' or 'backplane(4)' (IETF RFC 2737)
MAC address	MAC address (IEEE Std 802-2001)
Network address	networkAddress
Interface name	ifName (IETF RFC 2863)
Locally assigned	locally assigned

- **Chassis ID** – An octet string indicating the specific identifier for the particular chassis in this system.

- **System Name** – A string that indicates the system's administratively assigned name (see "Displaying System Information" on page 149).

- **System Description** – A textual description of the network entity. This field is also displayed by the **show system** command.

- **System Capabilities Supported** – The capabilities that define the primary function(s) of the system.

Table 30: System Capabilities

ID Basis	Reference
Other	—
Repeater	IETF RFC 2108
Bridge	IETF RFC 2674
WLAN Access Point	IEEE 802.11 MIB
Router	IETF RFC 1812
Telephone	IETF RFC 2011
DOCSIS cable device	IETF RFC 2669 and IETF RFC 2670
End Station Only	IETF RFC 2011

- **System Capabilities Enabled** – The primary function(s) of the system which are currently enabled. Refer to the preceding table.

- **Management Address** – The management address associated with the local system. If no management address is available, the address should be the MAC address for the CPU or for the port sending this advertisement.

Interface Settings

The attributes listed below apply to both port and trunk interface types. When a trunk is listed, the descriptions apply to the first port of the trunk.

- **Port/Trunk Description** – A string that indicates the port or trunk description. If RFC 2863 is implemented, the ifDescr object should be used for this field.

- **Port/Trunk ID** – A string that contains the specific identifier for the port or trunk from which this LLDPDU was transmitted.

Interface Details

The attributes listed below apply to both port and trunk interface types. When a trunk is listed, the descriptions apply to the first port of the trunk.

- **Local Port/Trunk** – Local interface on this switch.

- **Port/Trunk ID Type** – There are several ways in which a port may be identified. A port ID subtype is used to indicate how the port is being referenced in the Port ID TLV.

Table 31: Port ID Subtype

ID Basis	Reference
Interface alias	IfAlias (IETF RFC 2863)
Chassis component	EntPhysicalAlias when entPhysClass has a value of 'chassis(3)' (IETF RFC 2737)
Port component	EntPhysicalAlias when entPhysicalClass has a value 'port(10)' or 'backplane(4)' (IETF RFC 2737)
MAC address	MAC address (IEEE Std 802-2001)
Network address	networkAddress
Interface name	ifName (IETF RFC 2863)
Agent circuit ID	agent circuit ID (IETF RFC 3046)
Locally assigned	locally assigned

- **Port/Trunk ID** – A string that contains the specific identifier for the local interface based on interface subtype used by this switch.

- **Port/Trunk Description** – A string that indicates the port or trunk description. If RFC 2863 is implemented, the ifDescr object should be used for this field.

- **MED Capability** – The supported set of capabilities that define the primary function(s) of the interface:
  - LLDP-MED Capabilities
  - Network Policy
  - Location Identification
  - Extended Power via MDI – PSE
  - Extended Power via MDI – PD
  - Inventory

WEB INTERFACE

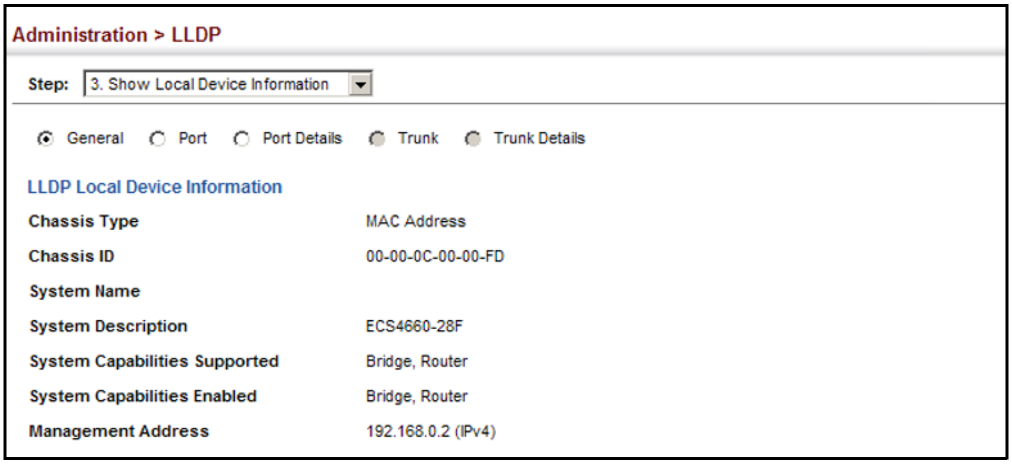
To display LLDP information for the local device:

1. Click Administration, LLDP.

2. Select Show Local Device Information from the Step list.

3. Select General, Port, Port Details, Trunk, or Trunk Details.

Figure 244: Displaying Local Device Information for LLDP (General)



Administration > LLDP

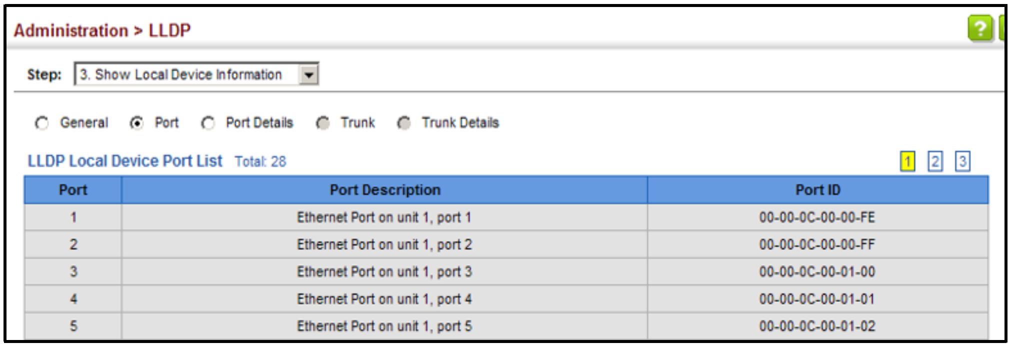
Step: 3. Show Local Device Information

● General ○ Port ○ Port Details ○ Trunk ○ Trunk Details

LLDP Local Device Information

Chassis Type	MAC Address
Chassis ID	00-00-0C-00-00-FD
System Name	
System Description	ECS4660-28F
System Capabilities Supported	Bridge, Router
System Capabilities Enabled	Bridge, Router
Management Address	192.168.0.2 (IPv4)

Figure 245: Displaying Local Device Information for LLDP (Port)



Administration > LLDP

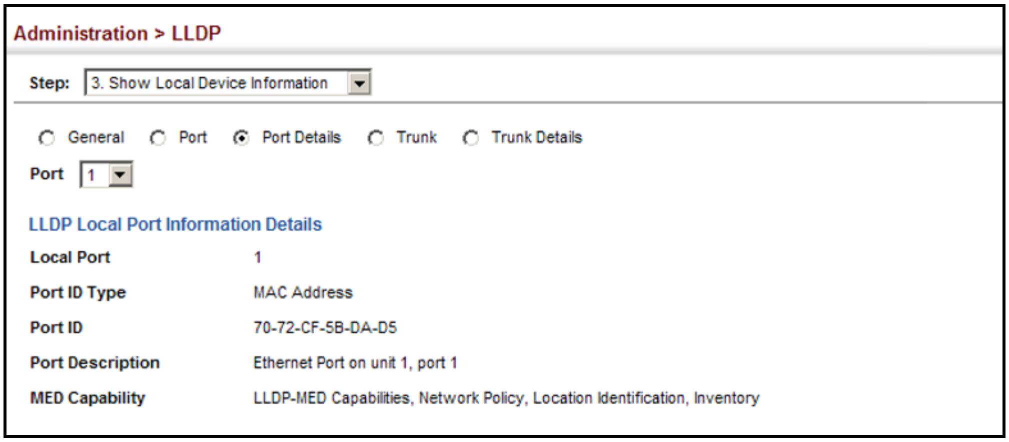
Step: 3. Show Local Device Information

○ General ● Port ○ Port Details ○ Trunk ○ Trunk Details

LLDP Local Device Port List Total: 28

Port	Port Description	Port ID
1	Ethernet Port on unit 1, port 1	00-00-0C-00-00-FE
2	Ethernet Port on unit 1, port 2	00-00-0C-00-00-FF
3	Ethernet Port on unit 1, port 3	00-00-0C-00-01-00
4	Ethernet Port on unit 1, port 4	00-00-0C-00-01-01
5	Ethernet Port on unit 1, port 5	00-00-0C-00-01-02

Figure 246: Displaying Local Device Information for LLDP (Port Details)



Administration > LLDP

Step: 3. Show Local Device Information

○ General ○ Port ● Port Details ○ Trunk ○ Trunk Details

Port 1

LLDP Local Port Information Details

Local Port	1
Port ID Type	MAC Address
Port ID	70-72-CF-5B-DA-D5
Port Description	Ethernet Port on unit 1, port 1
MED Capability	LLDP-MED Capabilities, Network Policy, Location Identification, Inventory

DISPLAYING LLDP REMOTE DEVICE INFORMATION

Use the Administration > LLDP (Show Remote Device Information) page to display information about devices connected directly to the switch's ports which are advertising information through LLDP, or to display detailed information about an LLDP-enabled device connected to a specific port on the local switch.

CLI REFERENCES

- "show lldp info remote-device" on page 1557

PARAMETERS

These parameters are displayed:

Port

- **Local Port** – The local port to which a remote LLDP-capable device is attached.
- **Chassis ID** – An octet string indicating the specific identifier for the particular chassis in this system.
- **Port ID** – A string that contains the specific identifier for the port from which this LLDPDU was transmitted.
- **System Name** – A string that indicates the system's administratively assigned name.

Port Details

- **Port** – Port identifier on local switch.
- **Remote Index** – Index of remote device attached to this port.
- **Local Port** – The local port to which a remote LLDP-capable device is attached.
- **Chassis Type** – Identifies the chassis containing the IEEE 802 LAN entity associated with the transmitting LLDP agent. There are several ways in which a chassis may be identified and a chassis ID subtype is used to indicate the type of component being referenced by the chassis ID field. (See Table 29, "Chassis ID Subtype," on page 466.)
- **Chassis ID** – An octet string indicating the specific identifier for the particular chassis in this system.
- **System Name** – A string that indicates the system's assigned name.
- **System Description** – A textual description of the network entity.
- **Port Type** – Indicates the basis for the identifier that is listed in the Port ID field. See Table 31, "Port ID Subtype," on page 468.
- **Port Description** – A string that indicates the port's description. If RFC 2863 is implemented, the ifDescr object should be used for this field.

- **Port ID** – A string that contains the specific identifier for the port from which this LLDPDU was transmitted.

- **System Capabilities Supported** – The capabilities that define the primary function(s) of the system. (See Table 30, "System Capabilities," on page 467.)

- **System Capabilities Enabled** – The primary function(s) of the system which are currently enabled. (See Table 30, "System Capabilities," on page 467.)

- **Management Address List** – The management addresses for this device. Since there are typically a number of different addresses associated with a Layer 3 device, an individual LLDP PDU may contain more than one management address TLV.

  If no management address is available, the address should be the MAC address for the CPU or for the port sending this advertisement.

Port Details – 802.1 Extension Information

- **Remote Port VID** – The port's default VLAN identifier (PVID) indicates the VLAN with which untagged or priority-tagged frames are associated.

- **Remote Port-Protocol VLAN List** – The port-based protocol VLANs configured on this interface, whether the given port (associated with the remote system) supports port-based protocol VLANs, and whether the port-based protocol VLANs are enabled on the given port associated with the remote system.

- **Remote VLAN Name List** – VLAN names associated with a port.

- **Remote Protocol Identity List** – Information about particular protocols that are accessible through a port. This object represents an arbitrary local integer value used by this agent to identify a particular protocol identity, and an octet string used to identify the protocols associated with a port of the remote system.

Port Details – 802.3 Extension Port Information

- **Remote Port Auto-Neg Supported** – Shows whether the given port (associated with remote system) supports auto-negotiation.

- **Remote Port Auto-Neg Adv-Capability** – The value (bitmap) of the ifMauAutoNegCapAdvertisedBits object (defined in IETF RFC 3636) which is associated with a port on the remote system.

Table 32: Remote Port Auto-Negotiation Advertised Capability

Bit	Capability
0	other or unknown
1	10BASE-T half duplex mode
2	10BASE-T full duplex mode

Table 32: Remote Port Auto-Negotiation Advertised Capability

Bit	Capability
3	100BASE-T4
4	100BASE-TX half duplex mode
5	100BASE-TX full duplex mode
6	100BASE-T2 half duplex mode
7	100BASE-T2 full duplex mode
8	PAUSE for full-duplex links
9	Asymmetric PAUSE for full-duplex links
10	Symmetric PAUSE for full-duplex links
11	Asymmetric and Symmetric PAUSE for full-duplex links
12	1000BASE-X, -LX, -SX, -CX half duplex mode
13	1000BASE-X, -LX, -SX, -CX full duplex mode
14	1000BASE-T half duplex mode
15	1000BASE-T full duplex mode

- **Remote Port Auto-Neg Status** – Shows whether port auto-negotiation is enabled on a port associated with the remote system.

- **Remote Port MAU Type** – An integer value that indicates the operational MAU type of the sending device. This object contains the integer value derived from the list position of the corresponding dot3MauType as listed in IETF RFC 3636 and is equal to the last number in the respective dot3MauType OID.

Port Details – 802.3 Extension Power Information

- **Remote Power Class** – The port Class of the given port associated with the remote system (PSE – Power Sourcing Equipment or PD – Powered Device).

- **Remote Power MDI Status** – Shows whether MDI power is enabled on the given port associated with the remote system.

- **Remote Power Pairs** – “Signal” means that the signal pairs only are in use, and “Spare” means that the spare pairs only are in use.

- **Remote Power MDI Supported** – Shows whether MDI power is supported on the given port associated with the remote system.

- **Remote Power Pair Controlable** – Indicates whether the pair selection can be controlled for sourcing power on the given port associated with the remote system.

- **Remote Power Classification** – This classification is used to tag different terminals on the Power over LAN network according to their power consumption. Devices such as IP telephones, WLAN access points and others, will be classified according to their power requirements.

Port Details – 802.3 Extension Trunk Information

- **Remote Link Aggregation Capable** – Shows if the remote port is not in link aggregation state and/or it does not support link aggregation.
- **Remote Link Aggregation Status** – The current aggregation status of the link.
- **Remote Link Port ID** – This object contains the IEEE 802.3 aggregated port identifier, aAggPortID (IEEE 802.3-2002, 30.7.2.1.1), derived from the ifNumber of the ifIndex for the port component associated with the remote system. If the remote port is not in link aggregation state and/or it does not support link aggregation, this value should be zero.

Port Details – 802.3 Extension Frame Information

- **Remote Max Frame Size** – An integer value indicating the maximum supported frame size in octets on the port component associated with the remote system.

Port Details – LLDP-MED Capability [6]

- **Device Class** – Any of the following categories of endpoint devices:
  - Class 1 – The most basic class of endpoint devices.
  - Class 2 – Endpoint devices that supports media stream capabilities.
  - Class 3 – Endpoint devices that directly supports end users of the IP communication systems.
  - Network Connectivity Device – Devices that provide access to the IEEE 802 based LAN infrastructure for LLDP-MED endpoint devices. These may be any LAN access device including LAN switch/router, IEEE 802.1 bridge, IEEE 802.3 repeater, IEEE 802.11 wireless access point, or any device that supports the IEEE 802.1AB and MED extensions defined by this Standard and can relay IEEE 802 frames via any method.
- **Supported Capabilities** – The supported set of capabilities that define the primary function(s) of the port:
  - LLDP-MED Capabilities
  - Network Policy
  - Location Identification
  - Extended Power via MDI – PSE
  - Extended Power via MDI – PD
  - Inventory

[6] These fields are only displayed for end-node devices advertising LLDP-MED TLVs.

- **Current Capabilities** – The set of capabilities that define the primary function(s) of the port which are currently enabled.

Port Details – Network Policy[6]

- **Application Type** – The primary application(s) defined for this network policy:
  - Voice
  - Voice Signaling
  - Guest Signaling
  - Guest Voice Signaling
  - Softphone Voice
  - Video Conferencing
  - Streaming Video
  - Video Signaling
- **Tagged Flag** – Indicates whether the specified application type is using a tagged or untagged VLAN.
- **Layer 2 Priority** – The Layer 2 priority to be used for the specified application type. This field may specify one of eight priority levels (0-7), where a value of 0 represents use of the default priority.
- **Unknown Policy Flag** – Indicates that an endpoint device wants to explicitly advertise that this policy is required by the device, but is currently unknown.
- **VLAN ID** – The VLAN identifier (VID) for the port as defined in IEEE 802.1Q. A value of zero indicates that the port is using priority tagged frames, meaning that only the IEEE 802.1D priority level is significant and the default PVID of the ingress port is used instead.
- **DSCP Value** – The DSCP value to be used to provide Diffserv node behavior for the specified application type. This field may contain one of 64 code point values (0-63). A value of 0 represents use of the default DSCP value as defined in RFC 2475.

Port Details – Location Identification[6]

- **Location Data Format** – Any of these location ID data formats:
  - Coordinate-based LCI[7] – Defined in RFC 3825, includes latitude resolution, latitude, longitude resolution, longitude, altitude type, altitude resolution, altitude, and datum.
  - Civic Address LCI[7] – Includes What, Country code, CA type, CA length and CA value. "What" is described as the field entry "Device entry refers to" under "Configuring LLDP Interface Attributes." The

[7] Location Configuration Information

  the other items and described under "Configuring LLDP Interface Civic-Address."

  - ECS ELIN – Emergency Call Service Emergency Location Identification Number supports traditional PSAP-based Emergency Call Service in North America.

- **Country Code** – The two-letter ISO 3166 country code in capital ASCII letters. (Example: DK, DE or US)

- **What** – The type of device to which the location applies as described for the field entry "Device entry refers to" under "Configuring LLDP Interface Attributes."

Port Details – Extended Power-via-MDI

- **Power Type** – Power Sourcing Entity (PSE) or Power Device (PD).

- **Power Priority** – Shows power priority for a port. (Unknown, Low, High, Critical)

- **Power Source** – Shows information based on the type of device:

  - **PD** – Unknown, PSE, Local, PSE and Local

  - **PSE** – Unknown, Primary Power Source, Backup Power Source - Power conservation mode

- **Power Value** – The total power in watts required by a PD device from a PSE device, or the total power a PSE device is capable of sourcing over a maximum length cable based on its current configuration. This parameter supports a maximum power required or available value of 102.3 Watts to allow for future expansion. (Range: 0 - 102.3 Watts)

Port Details – Inventory[6]

- **Hardware Revision** – The hardware revision of the end-point device.

- **Software Revision** – The software revision of the end-point device.

- **Manufacture Name** – The manufacturer of the end-point device.

- **Asset ID** – The asset identifier of the end-point device. End-point devices are typically assigned asset identifiers to facilitate inventory management and assets tracking.

- **Firmware Revision** – The firmware revision of the end-point device.

- **Serial Number** – The serial number of the end-point device.

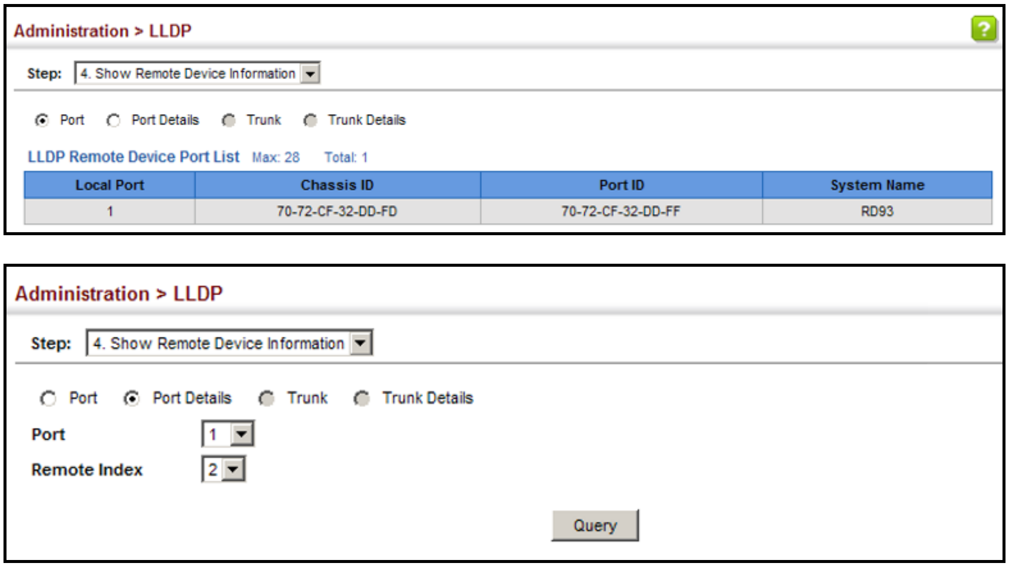
- **Model Name** – The model name of the end-point device.

WEB INTERFACE

To display LLDP information for a remote port:

1. Click Administration, LLDP.
2. Select Show Remote Device Information from the Step list.
3. Select Port, Port Details, Trunk, or Trunk Details.
4. When the next page opens, select a port on this switch and the index for a remote device attached to this port.
5. Click Query.

Figure 247: Displaying Remote Device Information for LLDP (Port)



Administration > LLDP

Step: 4. Show Remote Device Information

● Port ○ Port Details ○ Trunk ○ Trunk Details

LLDP Remote Device Port List Max: 28 Total: 1

Local Port	Chassis ID	Port ID	System Name
1	70-72-CF-32-DD-FD	70-72-CF-32-DD-FF	RD93

Administration > LLDP

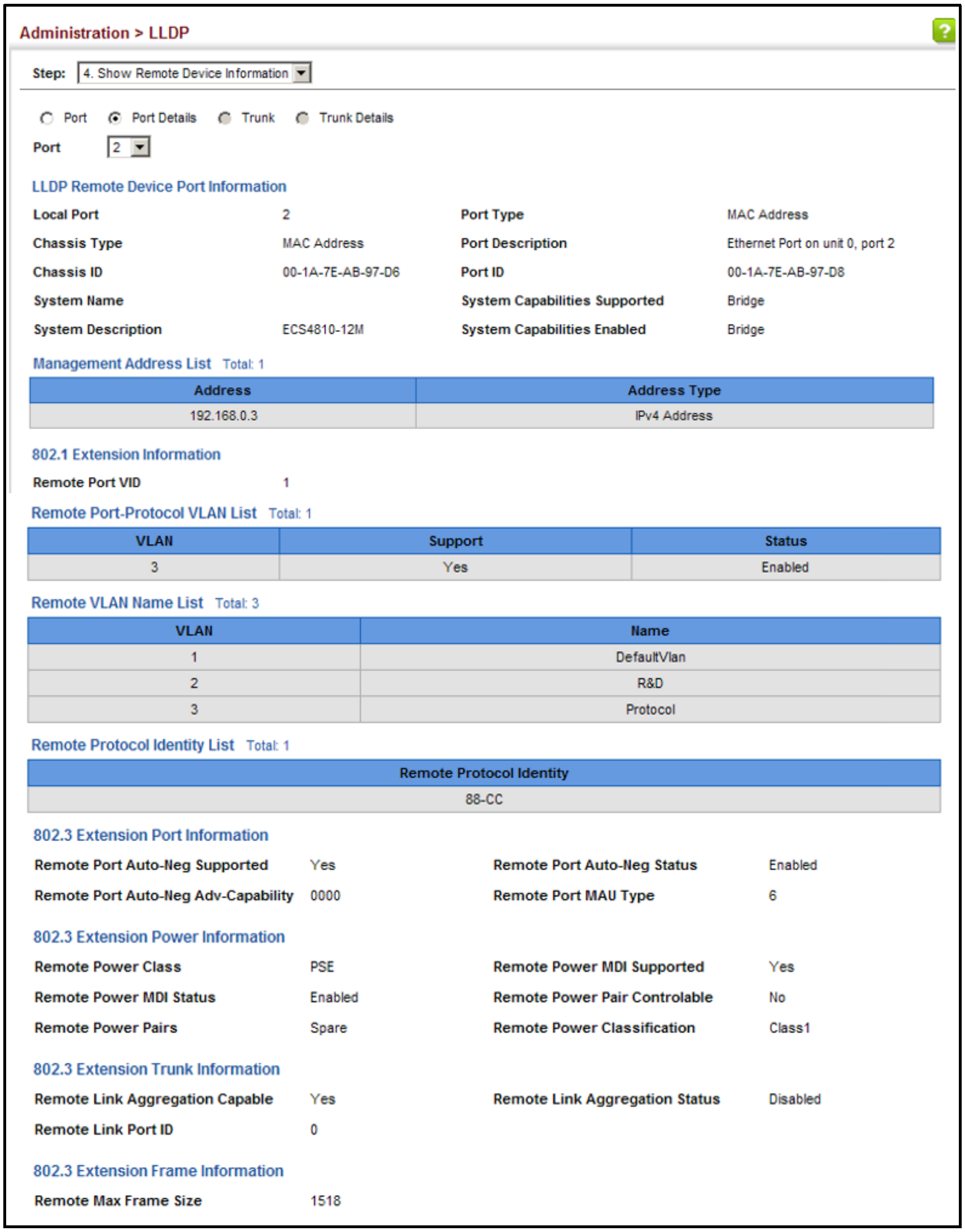
Step: 4. Show Remote Device Information

○ Port ● Port Details ○ Trunk ○ Trunk Details

Port: 1

Remote Index: 2

Figure 248: Displaying Remote Device Information for LLDP (Port Details)



Administration > LLDP

Step: 4. Show Remote Device Information

○ Port ● Port Details ○ Trunk ○ Trunk Details

Port 2

LLDP Remote Device Port Information

Local Port	2	Port Type	MAC Address
Chassis Type	MAC Address	Port Description	Ethernet Port on unit 0, port 2
Chassis ID	00-1A-7E-AB-97-D6	Port ID	00-1A-7E-AB-97-D8
System Name		System Capabilities Supported	Bridge
System Description	ECS4810-12M	System Capabilities Enabled	Bridge

Management Address List Total: 1

Address	Address Type
192.168.0.3	IPv4 Address

802.1 Extension Information

Remote Port VID	1

Remote Port-Protocol VLAN List Total: 1

VLAN	Support	Status
3	Yes	Enabled

Remote VLAN Name List Total: 3

VLAN	Name
1	DefaultVlan
2	R&D
3	Protocol

Remote Protocol Identity List Total: 1

Remote Protocol Identity
88-CC

802.3 Extension Port Information

Remote Port Auto-Neg Supported	Yes	Remote Port Auto-Neg Status	Enabled
Remote Port Auto-Neg Adv-Capability	0000	Remote Port MAU Type	6

802.3 Extension Power Information

Remote Power Class	PSE	Remote Power MDI Supported	Yes
Remote Power MDI Status	Enabled	Remote Power Pair Controlable	No
Remote Power Pairs	Spare	Remote Power Classification	Class1

802.3 Extension Trunk Information

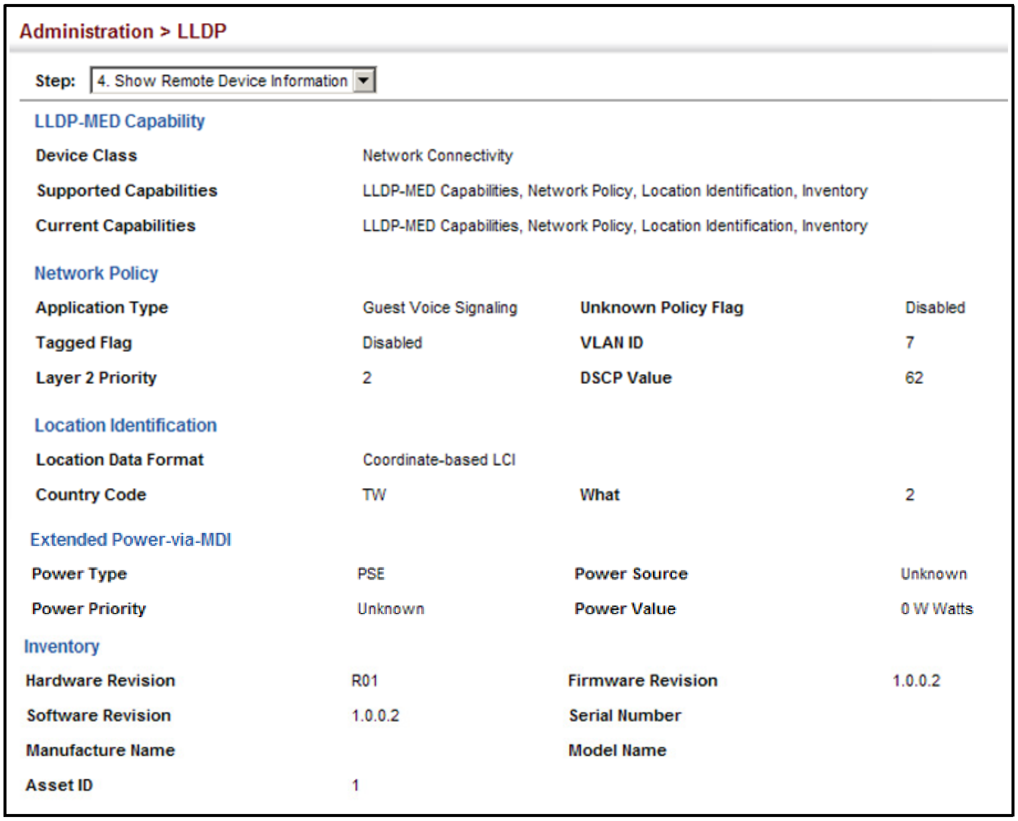
Remote Link Aggregation Capable	Yes	Remote Link Aggregation Status	Disabled
Remote Link Port ID	0		

802.3 Extension Frame Information

Remote Max Frame Size	1518

Additional information displayed by an end-point device which advertises LLDP-MED TLVs is shown in the following figure.

Figure 249: Displaying Remote Device Information for LLDP (End Node)



Administration > LLDP

Step: 4. Show Remote Device Information

LLDP-MED Capability

Device Class	Network Connectivity
Supported Capabilities	LLDP-MED Capabilities, Network Policy, Location Identification, Inventory
Current Capabilities	LLDP-MED Capabilities, Network Policy, Location Identification, Inventory

Network Policy

Application Type	Guest Voice Signaling	Unknown Policy Flag	Disabled
Tagged Flag	Disabled	VLAN ID	7
Layer 2 Priority	2	DSCP Value	62

Location Identification

Location Data Format	Coordinate-based LCI		
Country Code	TW	What	2

Extended Power-via-MDI

Power Type	PSE	Power Source	Unknown
Power Priority	Unknown	Power Value	0 W Watts

Inventory

Hardware Revision	R01	Firmware Revision	1.0.0.2
Software Revision	1.0.0.2	Serial Number	
Manufacture Name		Model Name	
Asset ID	1		

Displaying Device Statistics

Use the Administration > LLDP (Show Device Statistics) page to display statistics for LLDP-capable devices attached to the switch, and for LLDP protocol messages transmitted or received on all local interfaces.

CLI References

- "show lldp info statistics" on page 1560

Parameters

These parameters are displayed:

General Statistics on Remote Devices

- **Neighbor Entries List Last Updated** – The time the LLDP neighbor entry list was last updated.
- **New Neighbor Entries Count** – The number of LLDP neighbors for which the remote TTL has not yet expired.
- **Neighbor Entries Deleted Count** – The number of LLDP neighbors which have been removed from the LLDP remote systems MIB for any reason.

- **Neighbor Entries Dropped Count** – The number of times which the remote database on this switch dropped an LLDPDU because of insufficient resources.

- **Neighbor Entries Age-out Count** – The number of times that a neighbor's information has been deleted from the LLDP remote systems MIB because the remote TTL timer has expired.

Port/Trunk

- **Frames Discarded** – Number of frames discarded because they did not conform to the general validation rules as well as any specific usage rules defined for the particular TLV.

- **Frames Invalid** – A count of all LLDPDUs received with one or more detectable errors.

- **Frames Received** – Number of LLDP PDUs received.

- **Frames Sent** – Number of LLDP PDUs transmitted.

- **TLVs Unrecognized** – A count of all TLVs not recognized by the receiving LLDP local agent.

- **TLVs Discarded** – A count of all LLDPDUs received and then discarded due to insufficient memory space, missing or out-of-sequence attributes, or any other reason.

- **Neighbor Ageouts** – A count of the times that a neighbor's information has been deleted from the LLDP remote systems MIB because the remote TTL timer has expired.

WEB INTERFACE

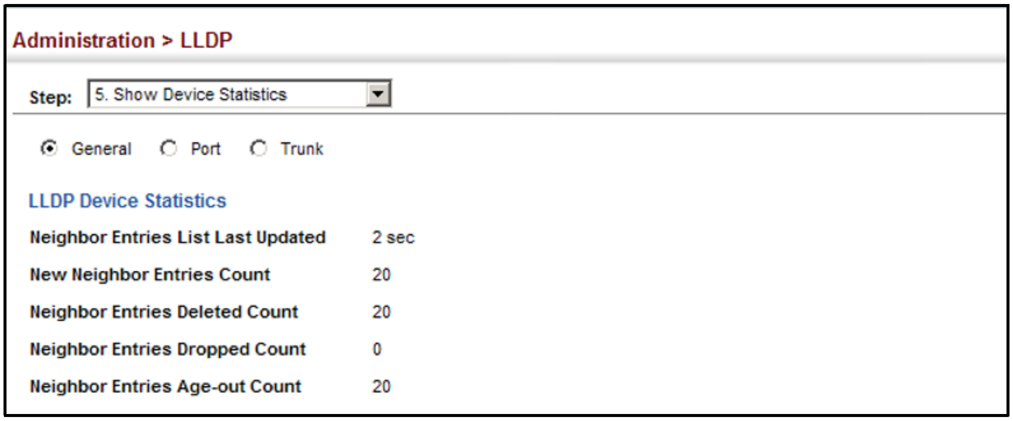
To display statistics for LLDP-capable devices attached to the switch:

1. Click Administration, LLDP.

2. Select Show Device Statistics from the Step list.

3. Select General, Port, or Trunk.

Figure 250: Displaying LLDP Device Statistics (General)



Administration > LLDP

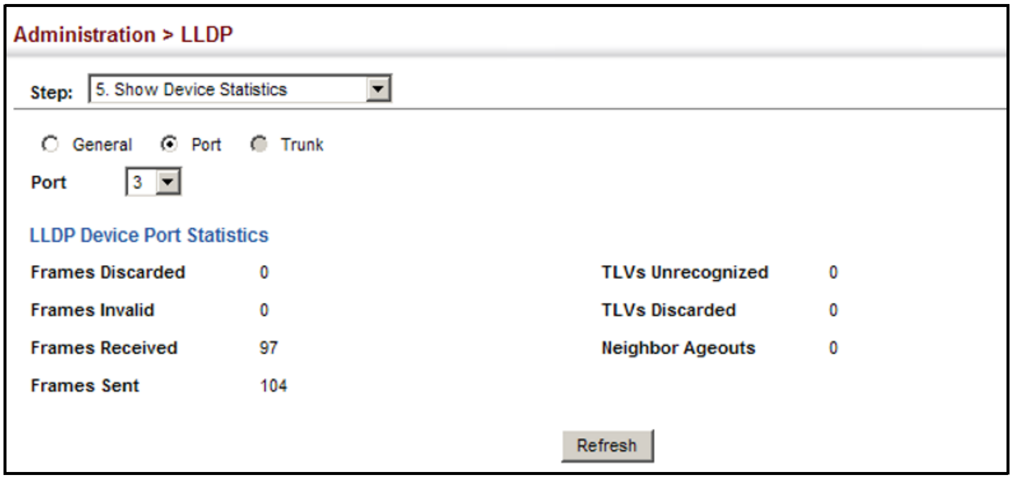
Step: 5. Show Device Statistics

● General ○ Port ○ Trunk

LLDP Device Statistics

Neighbor Entries List Last Updated	2 sec
New Neighbor Entries Count	20
Neighbor Entries Deleted Count	20
Neighbor Entries Dropped Count	0
Neighbor Entries Age-out Count	20

Figure 251: Displaying LLDP Device Statistics (Port)



Administration > LLDP

Step: 5. Show Device Statistics

○ General ● Port ○ Trunk

Port 3

LLDP Device Port Statistics

Frames Discarded	0	TLVs Unrecognized	0
Frames Invalid	0	TLVs Discarded	0
Frames Received	97	Neighbor Ageouts	0
Frames Sent	104		

SIMPLE NETWORK MANAGEMENT PROTOCOL

Simple Network Management Protocol (SNMP) is a communication protocol designed specifically for managing devices on a network. Equipment commonly managed with SNMP includes switches, routers and host computers. SNMP is typically used to configure these devices for proper operation in a network environment, as well as to monitor them to evaluate performance or detect potential problems.

Managed devices supporting SNMP contain software, which runs locally on the device and is referred to as an agent. A defined set of variables, known as managed objects, is maintained by the SNMP agent and used to manage the device. These objects are defined in a Management Information Base (MIB) that provides a standard presentation of the information controlled by the agent. SNMP defines both the format of the MIB specifications and the protocol used to access this information over the network.

The switch includes an onboard agent that supports SNMP versions 1, 2c, and 3. This agent continuously monitors the status of the switch hardware, as well as the traffic passing through its ports. A network management station can access this information using network management software. Access to the onboard agent from clients using SNMP v1 and v2c is controlled by community strings. To communicate with the switch, the management station must first submit a valid community string for authentication.

Access to the switch from clients using SNMPv3 provides additional security features that cover message integrity, authentication, and encryption; as well as controlling user access to specific areas of the MIB tree.

The SNMPv3 security structure consists of security models, with each model having it's own security levels. There are three security models defined, SNMPv1, SNMPv2c, and SNMPv3. Users are assigned to "groups" that are defined by a security model and specified security levels. Each group also has a defined security access to set of MIB objects for reading and writing, which are known as "views." The switch has a default view (all MIB objects) and default groups defined for security models v1 and v2c. The following table shows the security models and levels available and the system default settings.

Table 33: SNMPv3 Security Models and Levels

Model	Level	Group	Read View	Write View	Notify View	Security
v1	noAuthNoPriv	public (read only)	defaultview	none	none	Community string only
v1	noAuthNoPriv	private (read/write)	defaultview	defaultview	none	Community string only
v1	noAuthNoPriv	*user defined*	*user defined*	*user defined*	*user defined*	Community string only
v2c	noAuthNoPriv	public (read only)	defaultview	none	none	Community string only
v2c	noAuthNoPriv	private (read/write)	defaultview	defaultview	none	Community string only
v2c	noAuthNoPriv	*user defined*	*user defined*	*user defined*	*user defined*	Community string only
v3	noAuthNoPriv	*user defined*	*user defined*	*user defined*	*user defined*	A user name match only
v3	AuthNoPriv	*user defined*	*user defined*	*user defined*	*user defined*	Provides user authentication via MD5 or SHA algorithms
v3	AuthPriv	*user defined*	*user defined*	*user defined*	*user defined*	Provides user authentication via MD5 or SHA algorithms and data privacy using DES 56-bit encryption

NOTE: The predefined default groups and view can be deleted from the system. You can then define customized groups and views for the SNMP clients that require access.

COMMAND USAGE

Configuring SNMPv1/2c Management Access

To configure SNMPv1 or v2c management access to the switch, follow these steps:

1. Use the Administration > SNMP (Configure Global) page to enable SNMP on the switch, and to enable trap messages.

2. Use the Administration > SNMP (Configure User - Add Community) page to configure the community strings authorized for management access.

3. Use the Administration > SNMP (Configure Trap) page to specify trap managers so that key events are reported by this switch to your management station.

Configuring SNMPv3 Management Access

1. Use the Administration > SNMP (Configure Global) page to enable SNMP on the switch, and to enable trap messages.

2. Use the Administration > SNMP (Configure Trap) page to specify trap managers so that key events are reported by this switch to your management station.

3. Use the Administration > SNMP (Configure Engine) page to change the local engine ID. If you want to change the default engine ID, it must be changed before configuring other parameters.

4. Use the Administration > SNMP (Configure View) page to specify read and write access views for the switch MIB tree.

5. Use the Administration > SNMP (Configure User) page to configure SNMP user groups with the required security model (i.e., SNMP v1, v2c or v3) and security level (i.e., authentication and privacy).

6. Use the Administration > SNMP (Configure Group) page to assign SNMP users to groups, along with their specific authentication and privacy passwords.

CONFIGURING GLOBAL SETTINGS FOR SNMP

Use the Administration > SNMP (Configure Global) page to enable SNMPv3 service for all management clients (i.e., versions 1, 2c, 3), and to enable trap messages.

CLI REFERENCES

- "snmp-server" on page 997
- "snmp-server enable traps" on page 1000

PARAMETERS

These parameters are displayed:

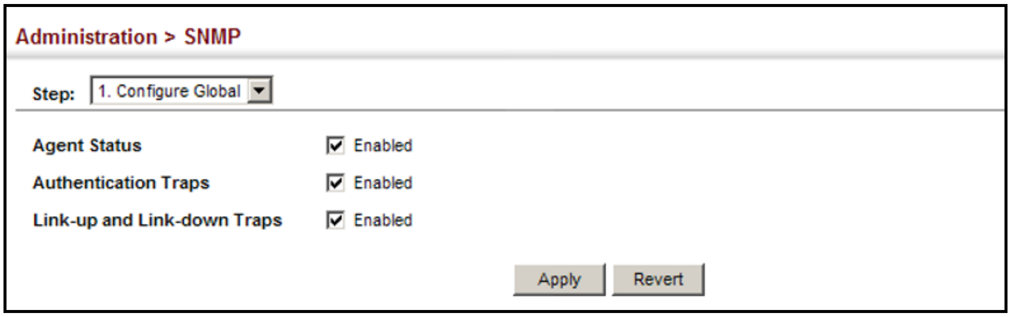
- **Agent Status** – Enables SNMP on the switch. (Default: Enabled)
- **Authentication Traps**[8] – Issues a notification message to specified IP trap managers whenever an invalid community string is submitted during the SNMP access authentication process. (Default: Enabled)
- **Link-up and Link-down Traps**[8] – Issues a notification message whenever a port link is established or broken. (Default: Enabled)

WEB INTERFACE

To configure global settings for SNMP:

1. Click Administration, SNMP.
2. Select Configure Global from the Step list.
3. Enable SNMP and the required trap types.
4. Click Apply

Figure 252: Configuring Global Settings for SNMP



Administration > SNMP

Step: 1. Configure Global

Agent Status ☑ Enabled

Authentication Traps ☑ Enabled

Link-up and Link-down Traps ☑ Enabled

SETTING THE LOCAL ENGINE ID

Use the Administration > SNMP (Configure Engine - Set Engine ID) page to change the local engine ID. An SNMPv3 engine is an independent SNMP agent that resides on the switch. This engine protects against message replay, delay, and redirection. The engine ID is also used in combination with user passwords to generate the security keys for authenticating and encrypting SNMPv3 packets.

CLI REFERENCES

- "snmp-server engine-id" on page 1004

COMMAND USAGE

- A local engine ID is automatically generated that is unique to the switch. This is referred to as the default engine ID. If the local engine

[8] These are legacy notifications and therefore when used for SNMPv3 hosts, they must be enabled in conjunction with the corresponding entries in the Notification View (page 486).

ID is deleted or changed, all SNMP users will be cleared. You will need to reconfigure all existing users.

PARAMETERS

These parameters are displayed:

- **Engine ID** – A new engine ID can be specified by entering 9 to 64 hexadecimal characters (5 to 32 octets in hexadecimal format). If an odd number of characters are specified, a trailing zero is added to the value to fill in the last octet. For example, the value “123456789” is equivalent to “1234567890”.

- **Engine Boots** – The number of times that the engine has (re-)initialized since the SNMP EngineID was last configured.

WEB INTERFACE

To configure the local SNMP engine ID:

1. Click Administration, SNMP.

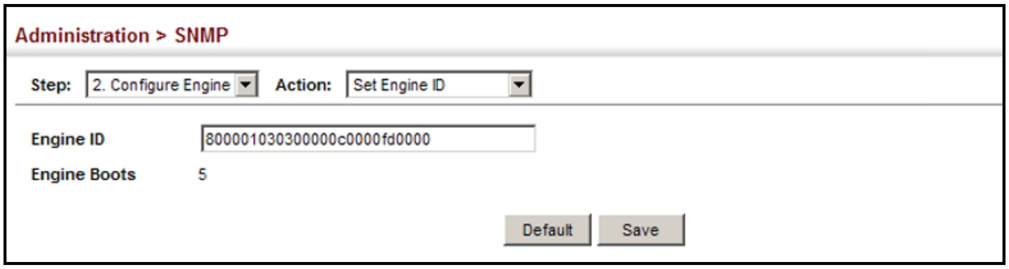
2. Select Configure Engine from the Step list.

3. Select Set Engine ID from the Action list.

4. Enter an ID of a least 9 hexadecimal characters.

5. Click Apply

Figure 253: Configuring the Local Engine ID for SNMP



Administration > SNMP

Step: 2. Configure Engine Action: Set Engine ID

Engine ID 800001030300000c0000fd0000

Engine Boots 5

SPECIFYING A REMOTE ENGINE ID

Use the Administration > SNMP (Configure Engine - Add Remote Engine) page to configure a engine ID for a remote management station. To allow management access from an SNMPv3 user on a remote device, you must first specify the engine identifier for the SNMP agent on the remote device where the user resides. The remote engine ID is used to compute the security digest for authentication and encryption of packets passed between the switch and a user on the remote host.

CLI REFERENCES

- "snmp-server engine-id" on page 1004

COMMAND USAGE

- SNMP passwords are localized using the engine ID of the authoritative agent. For informs, the authoritative SNMP agent is the remote agent. You therefore need to configure the remote agent's SNMP engine ID before you can send proxy requests or informs to it. (See "Configuring Remote SNMPv3 Users" on page 497.)

PARAMETERS

These parameters are displayed:

- **Remote Engine ID** – The engine ID can be specified by entering 9 to 64 hexadecimal characters (5 to 32 octets in hexadecimal format). If an odd number of characters are specified, a trailing zero is added to the value to fill in the last octet. For example, the value "123456789" is equivalent to "1234567890".

- **Remote IP Host** – The IP address of a remote management station which is using the specified engine ID.

WEB INTERFACE

To configure a remote SNMP engine ID:

1. Click Administration, SNMP.

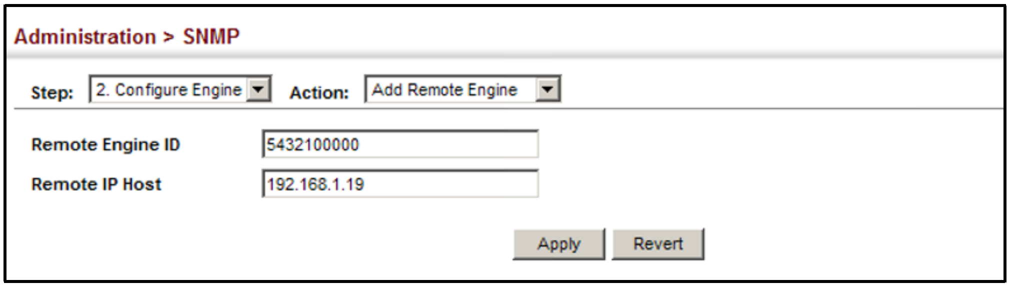
2. Select Configure Engine from the Step list.

3. Select Add Remote Engine from the Action list.

4. Enter an ID of a least 9 hexadecimal characters, and the IP address of the remote host.

5. Click Apply

Figure 254: Configuring a Remote Engine ID for SNMP



Administration > SNMP

Step: 2. Configure Engine Action: Add Remote Engine

Remote Engine ID: 5432100000

Remote IP Host: 192.168.1.19

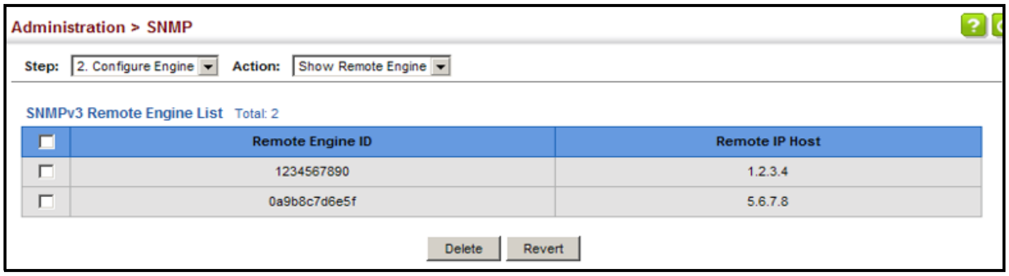
To show the remote SNMP engine IDs:

1. Click Administration, SNMP.

2. Select Configure Engine from the Step list.

3. Select Show Remote Engine from the Action list.

Figure 255: Showing Remote Engine IDs for SNMP



Administration > SNMP
Step: 2. Configure Engine
Action: Show Remote Engine
SNMPv3 Remote Engine List Total: 2

□	Remote Engine ID	Remote IP Host
□	1234567890	1.2.3.4
□	0a9b8c7d6e5f	5.6.7.8

SETTING SNMPv3 VIEWS

Use the Administration > SNMP (Configure View) page to configure SNMPv3 views which are used to restrict user access to specified portions of the MIB tree. The predefined view "defaultview" includes access to the entire MIB tree.

CLI REFERENCES

- "snmp-server view" on page 1008

PARAMETERS

These parameters are displayed:

Add View

- **View Name** – The name of the SNMP view. (Range: 1-64 characters)
- **OID Subtree** – Specifies the initial object identifier of a branch within the MIB tree. Wild cards can be used to mask a specific portion of the OID string. Use the Add OID Subtree page to configure additional object identifiers.
- **Type** – Indicates if the object identifier of a branch within the MIB tree is included or excluded from the SNMP view.

Add OID Subtree

- **View Name** – Lists the SNMP views configured in the Add View page.
- **OID Subtree** – Adds an additional object identifier of a branch within the MIB tree to the selected View. Wild cards can be used to mask a specific portion of the OID string.
- **Type** – Indicates if the object identifier of a branch within the MIB tree is included or excluded from the SNMP view.

WEB INTERFACE

To configure an SNMP view of the switch's MIB database:

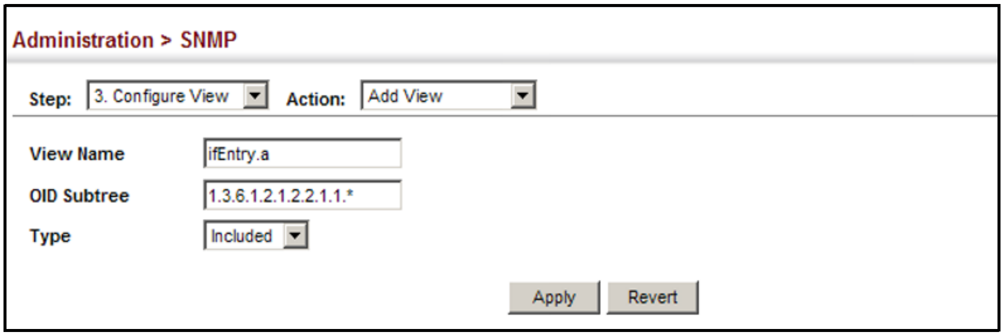
1. Click Administration, SNMP.
2. Select Configure View from the Step list.

3. Select Add View from the Action list.

4. Enter a view name and specify the initial OID subtree in the switch's MIB database to be included or excluded in the view. Use the Add OID Subtree page to add additional object identifier branches to the view.

5. Click Apply

Figure 256: Creating an SNMP View



Administration > SNMP

Step: 3. Configure View Action: Add View

View Name: ifEntry.a
OID Subtree: 1.3.6.1.2.1.2.2.1.1.*
Type: Included

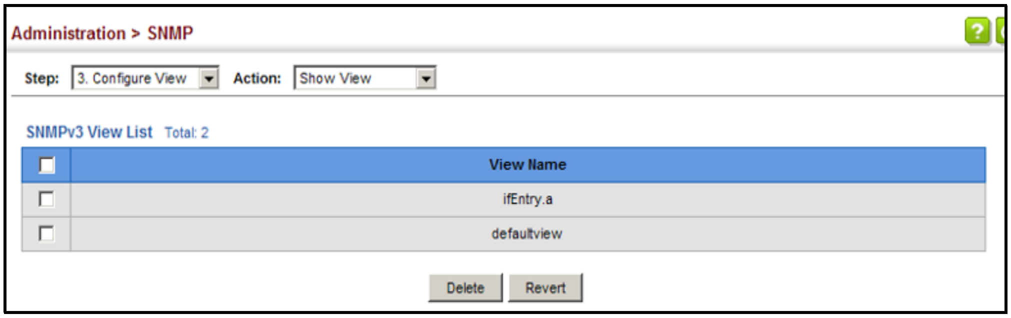
To show the SNMP views of the switch's MIB database:

1. Click Administration, SNMP.

2. Select Configure View from the Step list.

3. Select Show View from the Action list.

Figure 257: Showing SNMP Views



Administration > SNMP

Step: 3. Configure View Action: Show View

SNMPv3 View List Total: 2

□	View Name
□	ifEntry.a
□	defaultview

To add an object identifier to an existing SNMP view of the switch's MIB database:

1. Click Administration, SNMP.

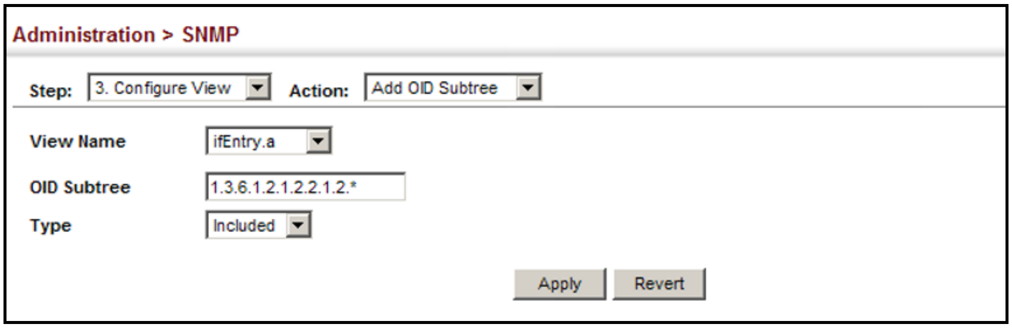
2. Select Configure View from the Step list.

3. Select Add OID Subtree from the Action list.

4. Select a view name from the list of existing views, and specify an additional OID subtree in the switch's MIB database to be included or excluded in the view.

5. Click Apply

Figure 258: Adding an OID Subtree to an SNMP View



Administration > SNMP

Step: 3. Configure View Action: Add OID Subtree

View Name: ifEntry.a

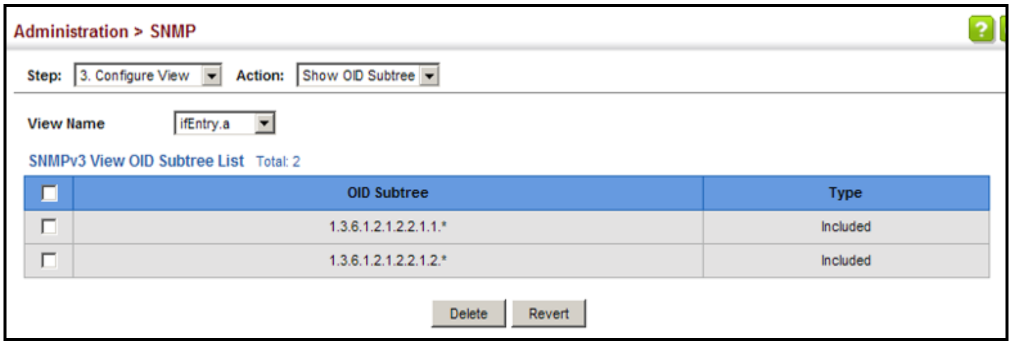
OID Subtree: 1.3.6.1.2.1.2.2.1.2.*

Type: Included

To show the OID branches configured for the SNMP views of the switch's MIB database:

1. Click Administration, SNMP.
2. Select Configure View from the Step list.
3. Select Show OID Subtree from the Action list.
4. Select a view name from the list of existing views.

Figure 259: Showing the OID Subtree Configured for SNMP Views



Administration > SNMP

Step: 3. Configure View Action: Show OID Subtree

View Name: ifEntry.a

SNMPv3 View OID Subtree List Total: 2

□	OID Subtree	Type
□	1.3.6.1.2.1.2.2.1.1.*	Included
□	1.3.6.1.2.1.2.2.1.2.*	Included

CONFIGURING SNMPV3 GROUPS

Use the Administration > SNMP (Configure Group) page to add an SNMPv3 group which can be used to set the access policy for its assigned users, restricting them to specific read, write, and notify views. You can use the pre-defined default groups or create new groups to map a set of SNMP users to SNMP views.

CLI REFERENCES

- "show snmp group" on page 1010

PARAMETERS

These parameters are displayed:

- **Group Name** – The name of the SNMP group to which the user is assigned. (Range: 1-32 characters)
- **Security Model** – The user security model; SNMP v1, v2c or v3.
- **Security Level** – The following security levels are only used for the groups assigned to the SNMP security model:
    - **noAuthNoPriv** – There is no authentication or encryption used in SNMP communications. (This is the default security level.)
    - **AuthNoPriv** – SNMP communications use authentication, but the data is not encrypted.
    - **AuthPriv** – SNMP communications use both authentication and encryption.
- **Read View** – The configured view for read access. (Range: 1-32 characters)
- **Write View** – The configured view for write access. (Range: 1-32 characters)
- **Notify View** – The configured view for notifications. (Range: 1-32 characters)

Table 34: Supported Notification Messages

Model	Level	Group
RFC 1493 Traps		
newRoot	1.3.6.1.2.1.17.0.1	The newRoot trap indicates that the sending agent has become the new root of the Spanning Tree; the trap is sent by a bridge soon after its election as the new root, e.g., upon expiration of the Topology Change Timer immediately subsequent to its election.
topologyChange	1.3.6.1.2.1.17.0.2	A topologyChange trap is sent by a bridge when any of its configured ports transitions from the Learning state to the Forwarding state, or from the Forwarding state to the Discarding state. The trap is not sent if a newRoot trap is sent for the same transition.
SNMPv2 Traps		
coldStart	1.3.6.1.6.3.1.1.5.1	A coldStart trap signifies that the SNMPv2 entity, acting in an agent role, is reinitializing itself and that its configuration may have been altered.
warmStart	1.3.6.1.6.3.1.1.5.2	A warmStart trap signifies that the SNMPv2 entity, acting in an agent role, is reinitializing itself such that its configuration is unaltered.
linkDown*	1.3.6.1.6.3.1.1.5.3	A linkDown trap signifies that the SNMP entity, acting in an agent role, has detected that the ifOperStatus object for one of its communication links is about to enter the down state from some other state (but not from the notPresent state). This other state is indicated by the included value of ifOperStatus.
linkUp*	1.3.6.1.6.3.1.1.5.4	A linkUp trap signifies that the SNMP entity, acting in an agent role, has detected that the ifOperStatus object for one of its communication links left the down state and transitioned into some other state (but not into the notPresent state). This other state is indicated by the included value of ifOperStatus.
authenticationFailure*	1.3.6.1.6.3.1.1.5.5	An authenticationFailure trap signifies that the SNMPv2 entity, acting in an agent role, has received a protocol message that is not properly authenticated. While all implementations of the SNMPv2 must be capable of generating this trap, the snmpEnableAuthenTraps object indicates whether this trap will be generated.
RMON Events (V2)		
risingAlarm	1.3.6.1.2.1.16.0.1	The SNMP trap that is generated when an alarm entry crosses its rising threshold and generates an event that is configured for sending SNMP traps.
fallingAlarm	1.3.6.1.2.1.16.0.2	The SNMP trap that is generated when an alarm entry crosses its falling threshold and generates an event that is configured for sending SNMP traps.
Private Traps[†]		
swPowerStatusChangeTrap	1.3.6.1.4.1.259.10.1.10.2.1.0.1	This trap is sent when the power state changes.
swFanFailureTrap	1.3.6.1.4.1.259.10.1.10.2.1.0.17	This trap is sent when the fan fails.
swFanRecoverTrap	1.3.6.1.4.1.259.10.1.10.2.1.0.18	This trap is sent when fan failure has recovered.
swPortSecurityTrap	1.3.6.1.4.1.259.10.1.10.2.1.0.36	This trap is sent when the port is being intruded. This trap will only be sent when the portSecActionTrap is enabled.

Table 34: Supported Notification Messages (Continued)

Model	Level	Group
swIpFilterRejectTrap	1.3.6.1.4.1.259.10.1.10.2.1.0.40	This trap is sent when an incorrect IP address is rejected by the IP Filter.
swSmtpConnFailureTrap	1.3.6.1.4.1.259.10.1.10.2.1.0.41	This trap is triggered if the SMTP system cannot open a connection to the mail server successfully.
swMainBoardVerMismatchNotificaiton	1.3.6.1.4.1.259.10.1.10.2.1.0.56	This trap is sent when the slave version is mismatched with the master version. This trap will bind two objects, the first object indicates the master version, whereas the second represents the slave version.
swThermalRisingNotification	1.3.6.1.4.1.259.10.1.10.2.1.0.58	This trap is sent when the temperature is over the switchThermalActionRisingThreshold.
swThermalFallingNotification	1.3.6.1.4.1.259.10.1.10.2.1.0.59	This trap is sent when the temperature is below the switchThermalActionFallingThreshold.
swAtcBcastStormAlarmFireTrap	1.3.6.1.4.1.259.10.1.10.2.1.0.70	When broadcast traffic is detected as a storm, this trap is fired.
swAtcBcastStormAlarmClearTrap	1.3.6.1.4.1.259.10.1.10.2.1.0.71	When a broadcast storm is detected as normal traffic, this trap is fired.
swAtcBcastStormTcApplyTrap	1.3.6.1.4.1.259.10.1.10.2.1.0.72	When ATC is activated, this trap is fired.
swAtcBcastStormTcReleaseTrap	1.3.6.1.4.1.259.10.1.10.2.1.0.73	When ATC is released, this trap is fired.
swAtcMcastStormAlarmFireTrap	1.3.6.1.4.1.259.10.1.10.2.1.0.74	When multicast traffic is detected as the storm, this trap is fired.
swAtcMcastStormAlarmClearTrap	1.3.6.1.4.1.259.10.1.10.2.1.0.75	When multicast storm is detected as normal traffic, this trap is fired.
swAtcMcastStormTcApplyTrap	1.3.6.1.4.1.259.10.1.10.2.1.0.76	When ATC is activated, this trap is fired.
swAtcMcastStormTcReleaseTrap	1.3.6.1.4.1.259.10.1.10.2.1.0.77	When ATC is released, this trap is fired.
swAlarmInput	1.3.6.1.4.1.259.10.1.10.2.1.0.90	This trap is fired when an alarm input event occurs.
stpBpduGuardPortShutdownTrap	1.3.6.1.4.1.259.10.1.10.2.1.0.91	This trap will be sent when an interface is shut down because of BPDU guard.
swLoopbackDetectionTrap	1.3.6.1.4.1.259.10.1.10.2.1.0.95	This trap is sent when loop back BPDUs have been detected.
networkAccessPortLinkDetectionTrap	1.3.6.1.4.1.259.10.1.10.2.1.0.96	This trap is sent when a networkAccessPortLinkDetection event is triggered.
dot1agCfmMepUpTrap	1.3.6.1.4.1.259.10.1.10.2.1.0.97	This trap is sent when a new remote MEP is discovered.
dot1agCfmMepDownTrap	1.3.6.1.4.1.259.10.1.10.2.1.0.98	This trap is sent when port status or interface status TLV received from a remote MEP indicates it is not up.
dot1agCfmConfigFailTrap	1.3.6.1.4.1.259.10.1.10.2.1.0.99	This trap is sent when a MEP receives a CCM with an MPID which already exists on the same MA in this switch.
dot1agCfmLoopFindTrap	1.3.6.1.4.1.259.10.1.10.2.1.0.100	This trap is sent when a MEP receives its own CCMs.
dot1agCfmMepUnknownTrap	1.3.6.1.4.1.259.10.1.10.2.1.0.101	This trap is sent when a CCM is received from an unexpected MEP.
dot1agCfmMepMissingTrap	1.3.6.1.4.1.259.10.1.10.2.1.0.102	This trap is sent when the cross-check enable timer expires and no CCMs were received from an expected (configured) MEP.
dot1agCfmMaUpTrap	1.3.6.1.4.1.259.10.1.10.2.1.0.103	This trap is sent when all expected remote MEPs are up.

Table 34: Supported Notification Messages (Continued)

Model	Level	Group
autoUpgradeTrap	1.3.6.1.4.1.259.10.1.10.2.1.0.104	This trap is sent when auto upgrade is executed.
swCpuUtiRisingNotification	1.3.6.1.4.1.259.10.1.10.2.1.0.107	This notification indicates that the CPU utilization has risen from cpuUtiFallingThreshold to cpuUtiRisingThreshold.
swCpuUtiFallingNotification	1.3.6.1.4.1.259.10.1.10.2.1.0.108	This notification indicates that the CPU utilization has fallen from cpuUtiRisingThreshold to cpuUtiFallingThreshold.
swMemoryUtiRisingThreshold Notification	1.3.6.1.4.1.259.10.1.10.2.1.0.109	This notification indicates that the memory utilization has risen from memoryUtiFallingThreshold to memoryUtiRisingThreshold.
swMemoryUtiFallingThreshold Notification	1.3.6.1.4.1.259.10.1.10.2.1.0.110	This notification indicates that the memory utilization has fallen from memoryUtiRisingThreshold to memoryUtiFallingThreshold.
dhcpRougeServerAttackTrap	1.3.6.1.4.1.259.10.1.10.2.1.0.114	This trap is sent when receiving a DHCP packet from a rouge server.
macNotificationTrap	1.3.6.1.4.1.259.10.1.10.2.1.0.138	This trap is sent when there are changes of the dynamic MAC addresses on the switch.
lbdDetectionTrap	1.3.6.1.4.1.259.10.1.10.2.1.0.141	This trap is sent when a loopback condition is detected by LBD.
lbdRecoveryTrap	1.3.6.1.4.1.259.10.1.10.2.1.0.142	This trap is sent when a recovery is done by LBD.
sfpThresholdAlarmWarnTrap	1.3.6.1.4.1.259.10.1.10.2.1.0.189	This trap is sent when the sfp's A/D quantity is not within alarm/warning thresholds.
syncEReceiveSSMTrap	1.3.6.1.4.1.259.10.1.10.2.1.0.196	This trap is sent when a port received SSM messages
syncEClockSource	1.3.6.1.4.1.259.10.1.10.2.1.0.197	This trap is sent when a port becomes clock source port
userAuthenticationFailureTrap	1.3.6.1.4.1.259.10.1.10.2.1.0.199	This trap will be triggered if authentication fails.
userAuthenticationSuccessTrap	1.3.6.1.4.1.259.10.1.10.2.1.0.200	This trap will be triggered if authentication is successful.
loginTrap	1.3.6.1.4.1.259.10.1.10.2.1.0.201	This trap is sent when user logs in.
logoutTrap	1.3.6.1.4.1.259.10.1.10.2.1.0.202	This trap is sent when user logs out.
swAlarmInputRecover	1.3.6.1.4.1.259.10.1.10.2.1.0.203	This trap is fired when the alarm input event has been recovered.
fileCopyTrap	1.3.6.1.4.1.259.10.1.10.2.1.0.208	This trap is sent when file copy is executed. If the copy action is triggered by system, the login user information(trapVarLoginUserName/ trapVarSessionType/ trapVarLoginInetAddressTypes/ trapVarLoginInetAddres) will be null value.

* These are legacy notifications and therefore must be enabled in conjunction with the corresponding traps on the SNMP Configuration menu.

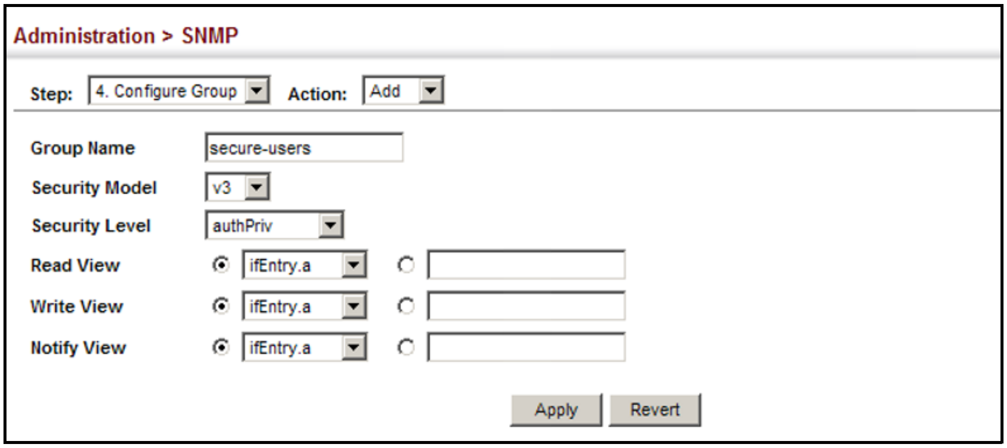
† The MIB OID for ECS4660-28F is 1.3.6.1.4.1.259.10.1.10.

WEB INTERFACE

To configure an SNMP group:

1. Click Administration, SNMP.
2. Select Configure Group from the Step list.
3. Select Add from the Action list.
4. Enter a group name, assign a security model and level, and then select read, write, and notify views.
5. Click Apply

Figure 260: Creating an SNMP Group



Administration > SNMP

Step: 4. Configure Group

Action: Add

Group Name: secure-users

Security Model: v3

Security Level: authPriv

Read View: ● ifEntry.a ○

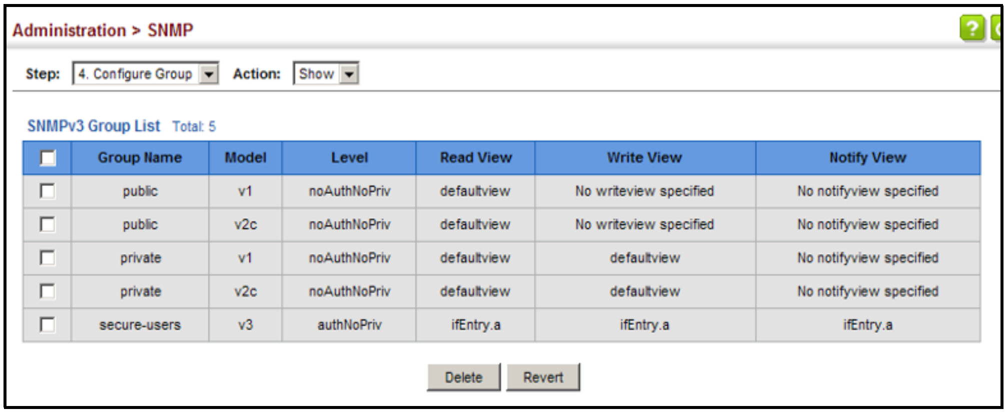
Write View: ● ifEntry.a ○

Notify View: ● ifEntry.a ○

To show SNMP groups:

1. Click Administration, SNMP.
2. Select Configure Group from the Step list.
3. Select Show from the Action list.

Figure 261: Showing SNMP Groups



Administration > SNMP

Step: 4. Configure Group

Action: Show

SNMPv3 Group List Total: 5

□	Group Name	Model	Level	Read View	Write View	Notify View
□	public	v1	noAuthNoPriv	defaultview	No writeview specified	No notifyview specified
□	public	v2c	noAuthNoPriv	defaultview	No writeview specified	No notifyview specified
□	private	v1	noAuthNoPriv	defaultview	defaultview	No notifyview specified
□	private	v2c	noAuthNoPriv	defaultview	defaultview	No notifyview specified
□	secure-users	v3	authNoPriv	ifEntry.a	ifEntry.a	ifEntry.a

SETTING COMMUNITY ACCESS STRINGS

Use the Administration > SNMP (Configure User - Add Community) page to configure up to five community strings authorized for management access by clients using SNMP v1 and v2c. For security reasons, you should consider removing the default strings.

CLI REFERENCES

- "snmp-server community" on page 997

PARAMETERS

These parameters are displayed:

- **Community String** – A community string that acts like a password and permits access to the SNMP protocol.

  Range: 1-32 characters, case sensitive
  Default strings: "public" (Read-Only), "private" (Read/Write)

- **Access Mode** – Specifies the access rights for the community string:

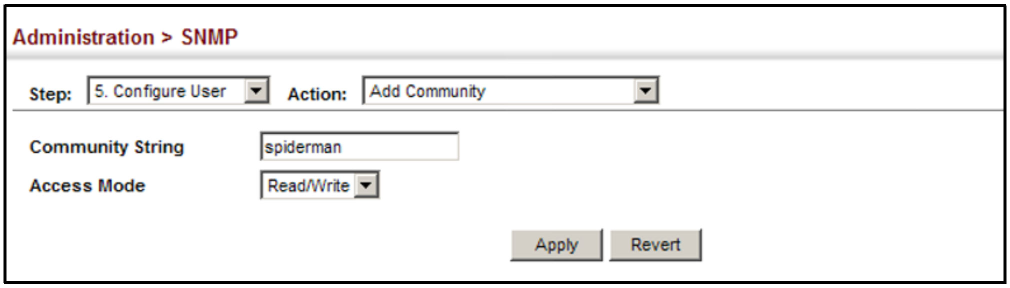
  - **Read-Only** – Authorized management stations are only able to retrieve MIB objects.
  - **Read/Write** – Authorized management stations are able to both retrieve and modify MIB objects.

WEB INTERFACE

To set a community access string:

1. Click Administration, SNMP.
2. Select Configure User from the Step list.
3. Select Add Community from the Action list.
4. Add new community strings as required, and select the corresponding access rights from the Access Mode list.
5. Click Apply

Figure 262: Setting Community Access Strings



Administration > SNMP

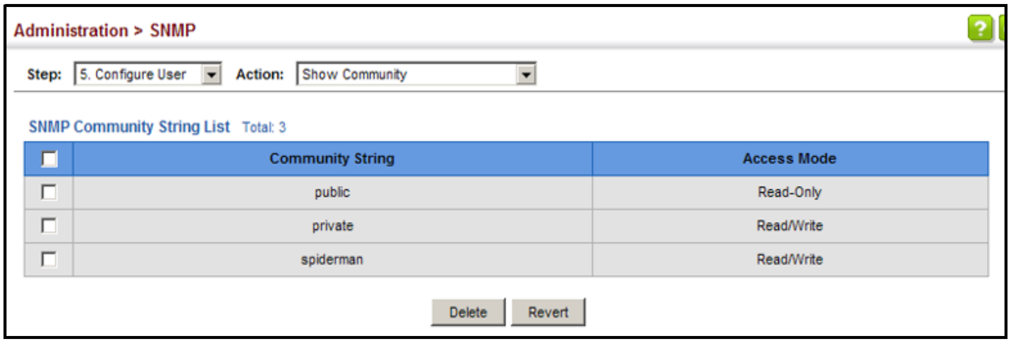
Step: 5. Configure User
Action: Add Community

Community String: spiderman
Access Mode: Read/Write

To show the community access strings:

1. Click Administration, SNMP.
2. Select Configure User from the Step list.
3. Select Show Community from the Action list.

Figure 263: Showing Community Access Strings



Administration > SNMP

Step: 5. Configure User Action: Show Community

SNMP Community String List Total: 3

☐	Community String	Access Mode
☐	public	Read-Only
☐	private	Read/Write
☐	spiderman	Read/Write

CONFIGURING LOCAL SNMPV3 USERS

Use the Administration > SNMP (Configure User - Add SNMPv3 Local User) page to authorize management access for SNMPv3 clients, or to identify the source of SNMPv3 trap messages sent from the local switch. Each SNMPv3 user is defined by a unique name. Users must be configured with a specific security level and assigned to a group. The SNMPv3 group restricts users to a specific read, write, and notify view.

CLI REFERENCES

- "snmp-server user" on page 1007

PARAMETERS

These parameters are displayed:

- **User Name** – The name of user connecting to the SNMP agent. (Range: 1-32 characters)
- **Group Name** – The name of the SNMP group to which the user is assigned. (Range: 1-32 characters)
- **Security Model** – The user security model; SNMP v1, v2c or v3.
- **Security Level** – The following security levels are only used for the groups assigned to the SNMP security model:
  - **noAuthNoPriv** – There is no authentication or encryption used in SNMP communications. (This is the default security level.)
  - **AuthNoPriv** – SNMP communications use authentication, but the data is not encrypted.

- **AuthPriv** – SNMP communications use both authentication and encryption.

- **Authentication Protocol** – The method used for user authentication. (Options: MD5, SHA; Default: MD5)

- **Authentication Password** – A minimum of eight plain text characters is required.

- **Privacy Protocol** – The encryption algorithm use for data privacy; only 56-bit DES is currently available.

- **Privacy Password** – A minimum of eight plain text characters is required.

WEB INTERFACE

To configure a local SNMPv3 user:

1. Click Administration, SNMP.

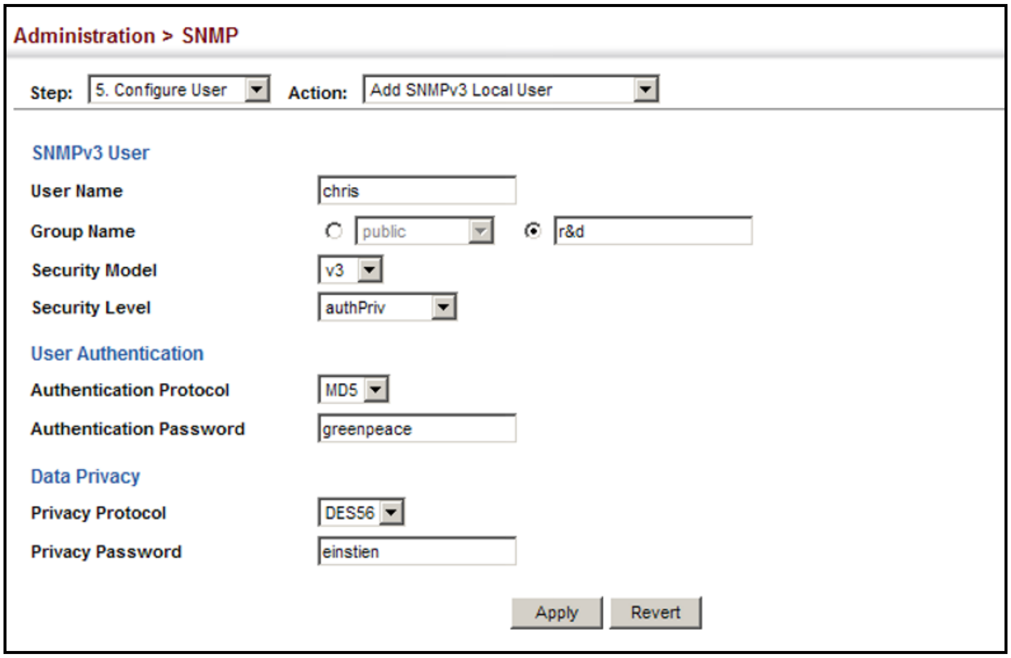
2. Select Configure User from the Step list.

3. Select Add SNMPv3 Local User from the Action list.

4. Enter a name and assign it to a group. If the security model is set to SNMPv3 and the security level is authNoPriv or authPriv, then an authentication protocol and password must be specified. If the security level is authPriv, a privacy password must also be specified.

5. Click Apply

Figure 264: Configuring Local SNMPv3 Users



Administration > SNMP

Step: 5. Configure User Action: Add SNMPv3 Local User

SNMPv3 User

User Name	chris
Group Name	○ public ● r&d
Security Model	v3
Security Level	authPriv

User Authentication

Authentication Protocol	MD5
Authentication Password	greenpeace

Data Privacy

Privacy Protocol	DES56
Privacy Password	einstien

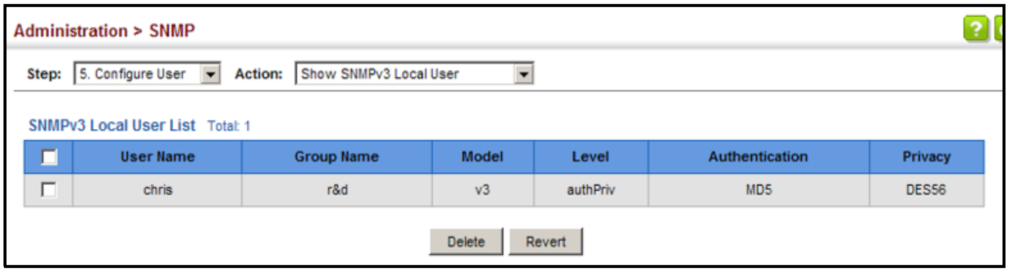
To show local SNMPv3 users:

1. Click Administration, SNMP.

2. Select Configure User from the Step list.

3. Select Show SNMPv3 Local User from the Action list.

Figure 265: Showing Local SNMPv3 Users



Step: 5. Configure User Action: Show SNMPv3 Local User

SNMPv3 Local User List Total: 1

□	User Name	Group Name	Model	Level	Authentication	Privacy
□	chris	r&d	v3	authPriv	MD5	DES56

CONFIGURING REMOTE SNMPV3 USERS

Use the Administration > SNMP (Configure User - Add SNMPv3 Remote User) page to identify the source of SNMPv3 inform messages sent from the local switch. Each SNMPv3 user is defined by a unique name. Users must be configured with a specific security level and assigned to a group. The SNMPv3 group restricts users to a specific read, write, and notify view.

CLI REFERENCES

- "snmp-server user" on page 1007

COMMAND USAGE

- To grant management access to an SNMPv3 user on a remote device, you must first specify the engine identifier for the SNMP agent on the remote device where the user resides. The remote engine ID is used to compute the security digest for authentication and encryption of packets passed between the switch and the remote user. (See "Specifying Trap Managers" on page 500 and "Specifying a Remote Engine ID" on page 484.)

PARAMETERS

These parameters are displayed:

- **User Name** – The name of user connecting to the SNMP agent. (Range: 1-32 characters)

- **Group Name** – The name of the SNMP group to which the user is assigned. (Range: 1-32 characters)

- **Remote IP** – The Internet address of the remote device where the user resides.

- **Security Model** – The user security model; SNMP v1, v2c or v3. (Default: v3)

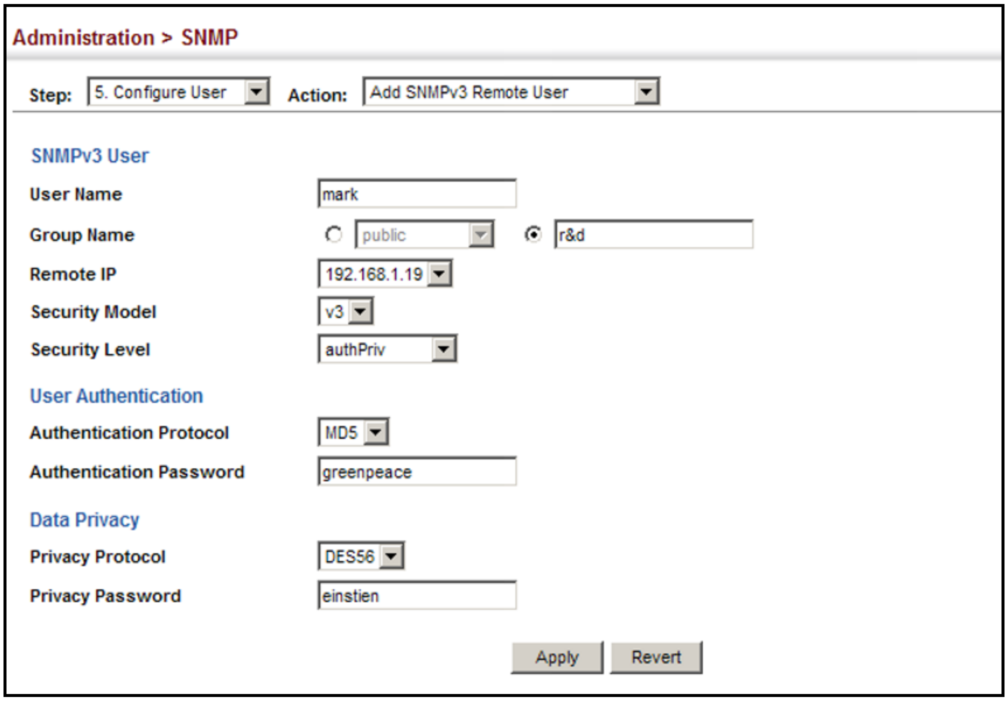
- **Security Level** – The following security levels are only used for the groups assigned to the SNMP security model:
  - **noAuthNoPriv** – There is no authentication or encryption used in SNMP communications. (This is the default security level.)
  - **AuthNoPriv** – SNMP communications use authentication, but the data is not encrypted.
  - **AuthPriv** – SNMP communications use both authentication and encryption.
- **Authentication Protocol** – The method used for user authentication. (Options: MD5, SHA; Default: MD5)
- **Authentication Password** – A minimum of eight plain text characters is required.
- **Privacy Protocol** – The encryption algorithm use for data privacy; only 56-bit DES is currently available.
- **Privacy Password** – A minimum of eight plain text characters is required.

WEB INTERFACE

To configure a remote SNMPv3 user:

1. Click Administration, SNMP.
2. Select Configure User from the Step list.
3. Select Add SNMPv3 Remote User from the Action list.
4. Enter a name and assign it to a group. Enter the IP address to identify the source of SNMPv3 inform messages sent from the local switch. If the security model is set to SNMPv3 and the security level is authNoPriv or authPriv, then an authentication protocol and password must be specified. If the security level is authPriv, a privacy password must also be specified.
5. Click Apply

Figure 266: Configuring Remote SNMPv3 Users



Administration > SNMP

Step: 5. Configure User Action: Add SNMPv3 Remote User

SNMPv3 User

User Name	mark
Group Name	○ public ● r&d
Remote IP	192.168.1.19
Security Model	v3
Security Level	authPriv

User Authentication

Authentication Protocol	MD5
Authentication Password	greenpeace

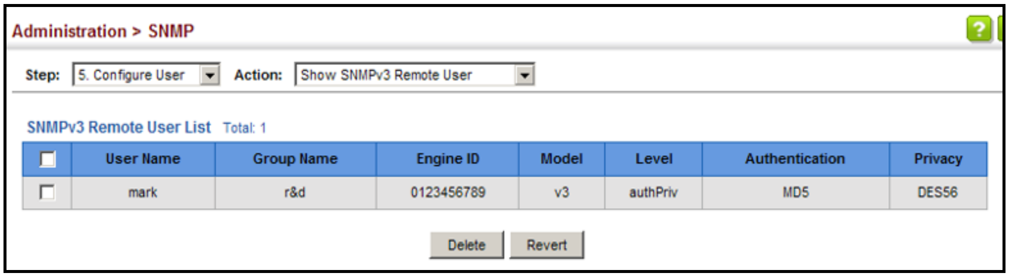
Data Privacy

Privacy Protocol	DES56
Privacy Password	einstien

To show remote SNMPv3 users:

1. Click Administration, SNMP.
2. Select Configure User from the Step list.
3. Select Show SNMPv3 Remote User from the Action list.

Figure 267: Showing Remote SNMPv3 Users



Administration > SNMP

Step: 5. Configure User Action: Show SNMPv3 Remote User

SNMPv3 Remote User List Total: 1

□	User Name	Group Name	Engine ID	Model	Level	Authentication	Privacy
□	mark	r&d	0123456789	v3	authPriv	MD5	DES56

SPECIFYING TRAP MANAGERS

Use the Administration > SNMP (Configure Trap) page to specify the host devices to be sent traps and the types of traps to send. Traps indicating status changes are issued by the switch to the specified trap managers. You must specify trap managers so that key events are reported by this switch to your management station (using network management software). You can specify up to five management stations that will receive authentication failure messages and other trap messages from the switch.

CLI REFERENCES

- "snmp-server host" on page 1001
- "snmp-server enable traps" on page 1000

COMMAND USAGE

- Notifications are issued by the switch as trap messages by default. The recipient of a trap message does not send a response to the switch. Traps are therefore not as reliable as inform messages, which include a request for acknowledgement of receipt. Informs can be used to ensure that critical information is received by the host. However, note that informs consume more system resources because they must be kept in memory until a response is received. Informs also add to network traffic. You should consider these effects when deciding whether to issue notifications as traps or informs.

  To send an inform to a SNMPv2c host, complete these steps:

  1. Enable the SNMP agent (page 482).
  2. Create a view with the required notification messages (page 486).
  3. Configure the group (matching the community string specified on the Configure Trap - Add page) to include the required notify view (page 489).
  4. Enable trap informs as described in the following pages.

  To send an inform to a SNMPv3 host, complete these steps:

  1. Enable the SNMP agent (page 482).
  2. Create a local SNMPv3 user to use in the message exchange process (page 495). If the user specified in the trap configuration page does not exist, an SNMPv3 group will be automatically created using the name of the specified local user, and default settings for the read, write, and notify view.
  3. Create a view with the required notification messages (page 486).
  4. Create a group that includes the required notify view (page 489).
  5. Enable trap informs as described in the following pages.

PARAMETERS

These parameters are displayed:

SNMP Version 1

- **IP Address** – IPv4 or IPv6 address of a new management station to receive notification message (i.e., the targeted recipient).
- **Version** – Specifies whether to send notifications as SNMP v1, v2c, or v3 traps. (Default: v1)
- **Community String** – Specifies a valid community string for the new trap manager entry. (Range: 1-32 characters, case sensitive)

  Although you can set this string in the Configure Trap – Add page, we recommend defining it in the Configure User – Add Community page.
- **UDP Port** – Specifies the UDP port number used by the trap manager. (Default: 162)

SNMP Version 2c

- **IP Address** – IPv4 or IPv6 address of a new management station to receive notification message (i.e., the targeted recipient).
- **Version** – Specifies whether to send notifications as SNMP v1, v2c, or v3 traps.
- **Notification Type**
  - **Traps** – Notifications are sent as trap messages.
  - **Inform** – Notifications are sent as inform messages. Note that this option is only available for version 2c and 3 hosts. (Default: traps are used)
    - **Timeout** – The number of seconds to wait for an acknowledgment before resending an inform message. (Range: 0-2147483647 centiseconds; Default: 1500 centiseconds)
    - **Retry times** – The maximum number of times to resend an inform message if the recipient does not acknowledge receipt. (Range: 0-255; Default: 3)
- **Community String** – Specifies a valid community string for the new trap manager entry. (Range: 1-32 characters, case sensitive)

  Although you can set this string in the Configure Trap – Add page, we recommend defining it in the Configure User – Add Community page.
- **UDP Port** – Specifies the UDP port number used by the trap manager. (Default: 162)

SNMP Version 3

- **IP Address** – IPv4 or IPv6 address of a new management station to receive notification message (i.e., the targeted recipient).
- **Version** – Specifies whether to send notifications as SNMP v1, v2c, or v3 traps.
- **Notification Type**
  - **Traps** – Notifications are sent as trap messages.
  - **Inform** – Notifications are sent as inform messages. Note that this option is only available for version 2c and 3 hosts. (Default: traps are used)
    - **Timeout** – The number of seconds to wait for an acknowledgment before resending an inform message. (Range: 0-2147483647 centiseconds; Default: 1500 centiseconds)
    - **Retry times** – The maximum number of times to resend an inform message if the recipient does not acknowledge receipt. (Range: 0-255; Default: 3)
- **Local User Name** – The name of a local user which is used to identify the source of SNMPv3 trap messages sent from the local switch. (Range: 1-32 characters)

  If an account for the specified user has not been created (page 495), one will be automatically generated.
- **Remote User Name** – The name of a remote user which is used to identify the source of SNMPv3 inform messages sent from the local switch. (Range: 1-32 characters)

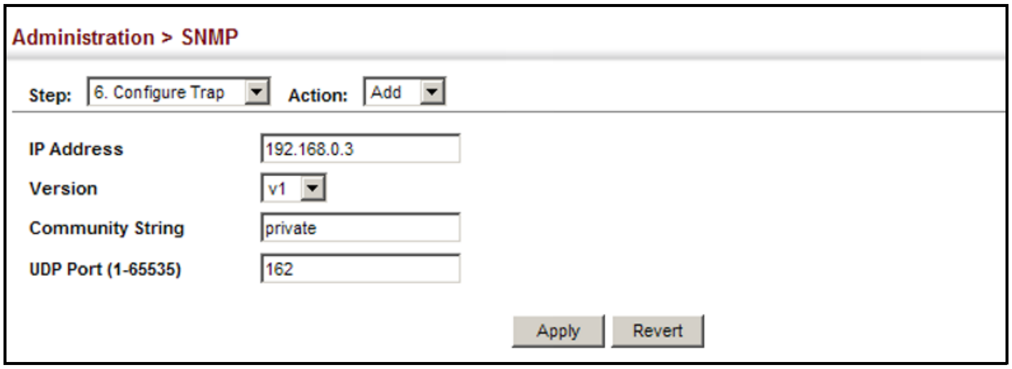
  If an account for the specified user has not been created (page 497), one will be automatically generated.
- **UDP Port** – Specifies the UDP port number used by the trap manager. (Default: 162)
- **Security Level** – When trap version 3 is selected, you must specify one of the following security levels. (Default: noAuthNoPriv)
  - **noAuthNoPriv** – There is no authentication or encryption used in SNMP communications.
  - **AuthNoPriv** – SNMP communications use authentication, but the data is not encrypted.
  - **AuthPriv** – SNMP communications use both authentication and encryption.

WEB INTERFACE

To configure trap managers:

1. Click Administration, SNMP.
2. Select Configure Trap from the Step list.
3. Select Add from the Action list.
4. Fill in the required parameters based on the selected SNMP version.
5. Click Apply

Figure 268: Configuring Trap Managers (SNMPv1)



Administration > SNMP

Step: 6. Configure Trap Action: Add

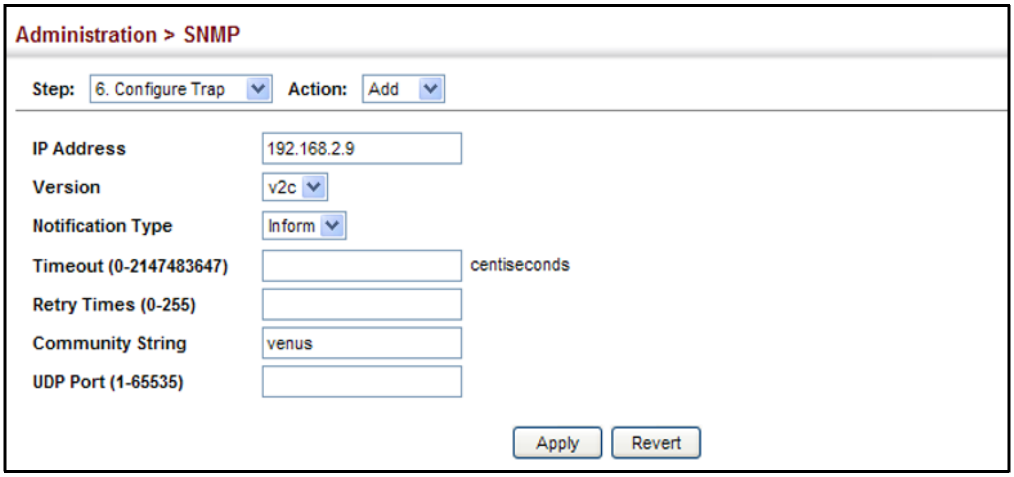
IP Address 192.168.0.3

Version v1

Community String private

UDP Port (1-65535) 162

Figure 269: Configuring Trap Managers (SNMPv2c)



Administration > SNMP

Step: 6. Configure Trap Action: Add

IP Address 192.168.2.9

Version v2c

Notification Type Inform

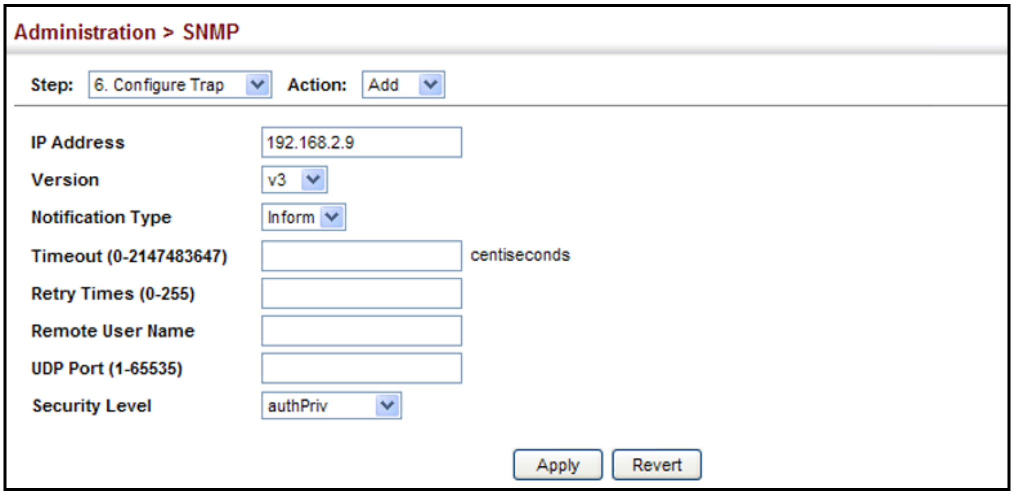
Timeout (0-2147483647) centiseconds

Retry Times (0-255)

Community String venus

UDP Port (1-65535)

Figure 270: Configuring Trap Managers (SNMPv3)



Administration > SNMP

Step: 6. Configure Trap Action: Add

IP Address: 192.168.2.9

Version: v3

Notification Type: Inform

Timeout (0-2147483647): centiseconds

Retry Times (0-255):

Remote User Name:

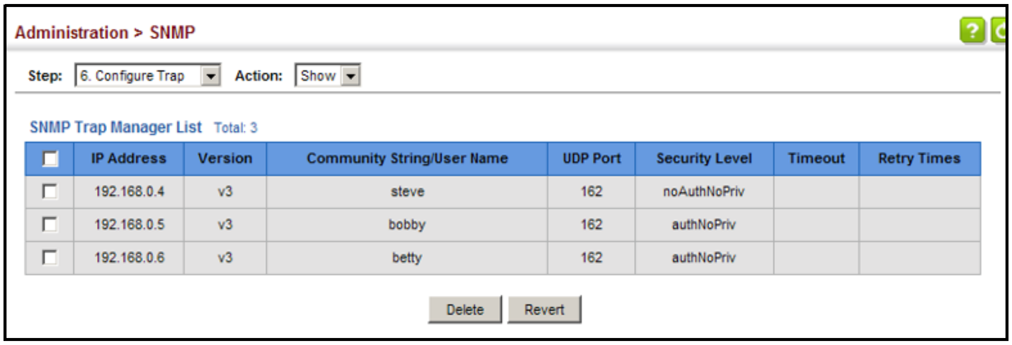
UDP Port (1-65535):

Security Level: authPriv

To show configured trap managers:

1. Click Administration, SNMP.
2. Select Configure Trap from the Step list.
3. Select Show from the Action list.

Figure 271: Showing Trap Managers



Administration > SNMP

Step: 6. Configure Trap Action: Show

SNMP Trap Manager List Total: 3

□	IP Address	Version	Community String/User Name	UDP Port	Security Level	Timeout	Retry Times
□	192.168.0.4	v3	steve	162	noAuthNoPriv		
□	192.168.0.5	v3	bobby	162	authNoPriv		
□	192.168.0.6	v3	betty	162	authNoPriv		

CREATING SNMP NOTIFICATION LOGS

Use the Administration > SNMP (Configure Notify Filter - Add) page to create an SNMP notification log.

CLI REFERENCES

- "nlm" on page 1012
- "snmp-server notify-filter" on page 1013
- "show nlm oper-status" on page 1014
- "show snmp notify-filter" on page 1015

COMMAND USAGE

- Systems that support SNMP often need a mechanism for recording Notification information as a hedge against lost notifications, whether there are Traps or Informs that may be exceeding retransmission limits.

The Notification Log MIB (NLM, RFC 3014) provides an infrastructure in which information from other MIBs may be logged.

- Given the service provided by the NLM, individual MIBs can now bear less responsibility to record transient information associated with an event against the possibility that the Notification message is lost, and applications can poll the log to verify that they have not missed any important Notifications.
- If notification logging is not configured, when the switch reboots, some SNMP traps (such as warm start) cannot be logged.
- To avoid this problem, notification logging should be configured as described in this section, and these commands stored in the startup configuration file using the System > File (Copy – Running-Config) page as described on page 157. Then when the switch reboots, SNMP traps (such as warm start) can now be logged.
- Based on the default settings used in RFC 3014, a notification log can contain up to 256 entries, and the entry aging time is 1440 minutes. Information recorded in a notification log, and the entry aging time can only be configured using SNMP from a network management station.
- When a trap host is created using the Administration > SNMP (Configure Trap – Add) page described on page 500, a default notify filter will be created.

PARAMETERS

These parameters are displayed:

- **IP Address** – The Internet address of a remote device. The specified target host must already have been configured using the Administration > SNMP (Configure Trap – Add) page.

  The notification log is stored locally. It is not sent to a remote device. This remote host parameter is only required to complete mandatory fields in the SNMP Notification MIB.
- **Filter Profile Name** – Notification log profile name. (Range: 1-32 characters)

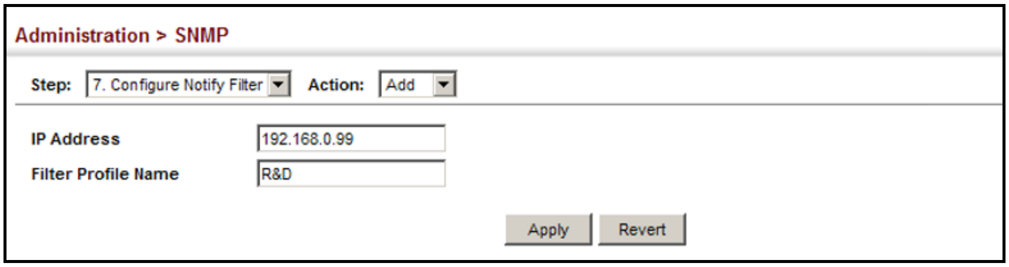
WEB INTERFACE

To create an SNMP notification log:

1. Click Administration, SNMP.
2. Select Configure Notify Filter from the Step list.
3. Select Add from the Action list.
4. Fill in the IP address of a configured trap manager and the filter profile name.

5. Click Apply

Figure 272: Creating SNMP Notification Logs



Administration > SNMP

Step: 7. Configure Notify Filter Action: Add

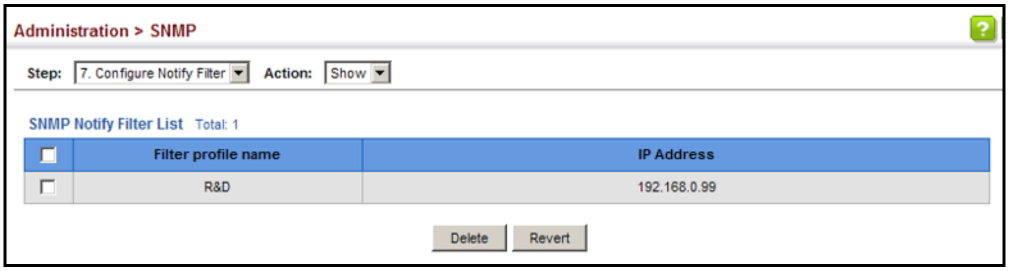
IP Address: 192.168.0.99

Filter Profile Name: R&D

To show configured SNMP notification logs:

1. Click Administration, SNMP.
2. Select Configure Notify Filter from the Step list.
3. Select Show from the Action list.

Figure 273: Showing SNMP Notification Logs



Administration > SNMP

Step: 7. Configure Notify Filter Action: Show

SNMP Notify Filter List Total: 1

□	Filter profile name	IP Address
□	R&D	192.168.0.99

SHOWING SNMP STATISTICS

Use the Administration > SNMP (Show Statistics) page to show counters for SNMP input and output protocol data units.

CLI REFERENCES

- "show snmp" on page 999

PARAMETERS

The following counters are displayed:

- **SNMP packets input** – The total number of messages delivered to the SNMP entity from the transport service.
- **Bad SNMP version errors** – The total number of SNMP messages which were delivered to the SNMP entity and were for an unsupported SNMP version.
- **Unknown community name** – The total number of SNMP messages delivered to the SNMP entity which used a SNMP community name not known to said entity.

- **Illegal operation for community name supplied** – The total number of SNMP messages delivered to the SNMP entity which represented an SNMP operation which was not allowed by the SNMP community named in the message.

- **Encoding errors** – The total number of ASN.1 or BER errors encountered by the SNMP entity when decoding received SNMP messages.

- **Number of requested variables** – The total number of MIB objects which have been retrieved successfully by the SNMP protocol entity as the result of receiving valid SNMP Get-Request and Get-Next PDUs.

- **Number of altered variables** – The total number of MIB objects which have been altered successfully by the SNMP protocol entity as the result of receiving valid SNMP Set-Request PDUs.

- **Get-request PDUs** – The total number of SNMP Get-Request PDUs which have been accepted and processed, or generated, by the SNMP protocol entity.

- **Get-next PDUs** – The total number of SNMP Get-Next PDUs which have been accepted and processed, or generated, by the SNMP protocol entity.

- **Set-request PDUs** – The total number of SNMP Set-Request PDUs which have been accepted and processed, or generated, by the SNMP protocol entity.

- **SNMP packets output** – The total number of SNMP Messages which were passed from the SNMP protocol entity to the transport service.

- **Too big errors** – The total number of SNMP PDUs which were generated by the SNMP protocol entity and for which the value of the error-status field is "tooBig."

- **No such name errors** – The total number of SNMP PDUs which were delivered to, or generated by, the SNMP protocol entity and for which the value of the error-status field is "noSuchName."

- **Bad values errors** – The total number of SNMP PDUs which were delivered to, or generated by, the SNMP protocol entity and for which the value of the error-status field is "badValue."

- **General errors** – The total number of SNMP PDUs which were delivered to, or generated by, the SNMP protocol entity and for which the value of the error-status field is "genErr."

- **Response PDUs** – The total number of SNMP Get-Response PDUs which have been accepted and processed by, or generated by, the SNMP protocol entity.

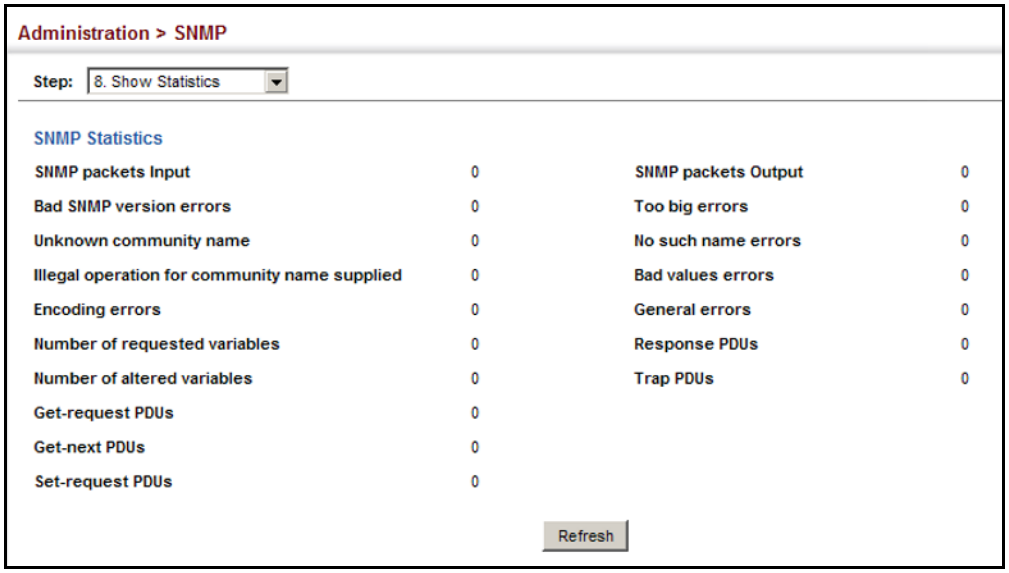
- **Trap PDUs** – The total number of SNMP Trap PDUs which have been accepted and processed by, or generated by, the SNMP protocol entity.

To show SNMP statistics:

1. Click Administration, SNMP.

2. Select Show Statistics from the Step list.

Figure 274: Showing SNMP Statistics



Administration > SNMP

Step: 8. Show Statistics

SNMP Statistics

SNMP packets Input	0	SNMP packets Output	0
Bad SNMP version errors	0	Too big errors	0
Unknown community name	0	No such name errors	0
Illegal operation for community name supplied	0	Bad values errors	0
Encoding errors	0	General errors	0
Number of requested variables	0	Response PDUs	0
Number of altered variables	0	Trap PDUs	0
Get-request PDUs	0		
Get-next PDUs	0		
Set-request PDUs	0		

REMOTE MONITORING

Remote Monitoring allows a remote device to collect information or respond to specified events on an independent basis. This switch is an RMON-capable device which can independently perform a wide range of tasks, significantly reducing network management traffic. It can continuously run diagnostics and log information on network performance. If an event is triggered, it can automatically notify the network administrator of a failure and provide historical information about the event. If it cannot connect to the management agent, it will continue to perform any specified tasks and pass data back to the management station the next time it is contacted.

The switch supports mini-RMON, which consists of the Statistics, History, Event and Alarm groups. When RMON is enabled, the system gradually builds up information about its physical interfaces, storing this information in the relevant RMON database group. A management agent then periodically communicates with the switch using the SNMP protocol. However, if the switch encounters a critical event, it can automatically send a trap message to the management agent which can then respond to the event if so configured.

CONFIGURING RMON ALARMS

Use the Administration > RMON (Configure Global - Add - Alarm) page to define specific criteria that will generate response events. Alarms can be set to test data over any specified time interval, and can monitor absolute or changing values (such as a statistical counter reaching a specific value, or a statistic changing by a certain amount over the set interval). Alarms can be set to respond to rising or falling thresholds. (However, note that after an alarm is triggered it will not be triggered again until the statistical value crosses the opposite bounding threshold and then back across the trigger threshold.

CLI REFERENCES

- "Remote Monitoring Commands" on page 1017

COMMAND USAGE

- If an alarm is already defined for an index, the entry must be deleted before any changes can be made.

PARAMETERS

These parameters are displayed:

- **Index** – Index to this entry. (Range: 1-65535)
- **Variable** – The object identifier of the MIB variable to be sampled. Only variables of the type etherStatsEntry.n.n may be sampled.

  Note that etherStatsEntry.n uniquely defines the MIB variable, and etherStatsEntry.n.n defines the MIB variable, plus the etherStatsIndex. For example, 1.3.6.1.2.1.16.1.1.1.6.1 denotes etherStatsBroadcastPkts, plus the etherStatsIndex of 1.
- **Interval** – The polling interval. (Range: 1-31622400 seconds)
- **Sample Type** – Tests for absolute or relative changes in the specified variable.
  - **Absolute** – The variable is compared directly to the thresholds at the end of the sampling period.
  - **Delta** – The last sample is subtracted from the current value and the difference is then compared to the thresholds.
- **Rising Threshold** – If the current value is greater than or equal to the rising threshold, and the last sample value was less than this threshold, then an alarm will be generated. After a rising event has been generated, another such event will not be generated until the sampled value has fallen below the rising threshold, reaches the falling threshold, and again moves back up to the rising threshold. (Range: 0-2147483647)
- **Rising Event Index** – The index of the event to use if an alarm is triggered by monitored variables reaching or crossing above the rising threshold. If there is no corresponding entry in the event control table, then no event will be generated. (Range: 0-65535)

- **Falling Threshold** – If the current value is less than or equal to the falling threshold, and the last sample value was greater than this threshold, then an alarm will be generated. After a falling event has been generated, another such event will not be generated until the sampled value has risen above the falling threshold, reaches the rising threshold, and again moves back down to the failing threshold. (Range: 0-2147483647)

- **Falling Event Index** – The index of the event to use if an alarm is triggered by monitored variables reaching or crossing below the falling threshold. If there is no corresponding entry in the event control table, then no event will be generated. (Range: 0-65535)

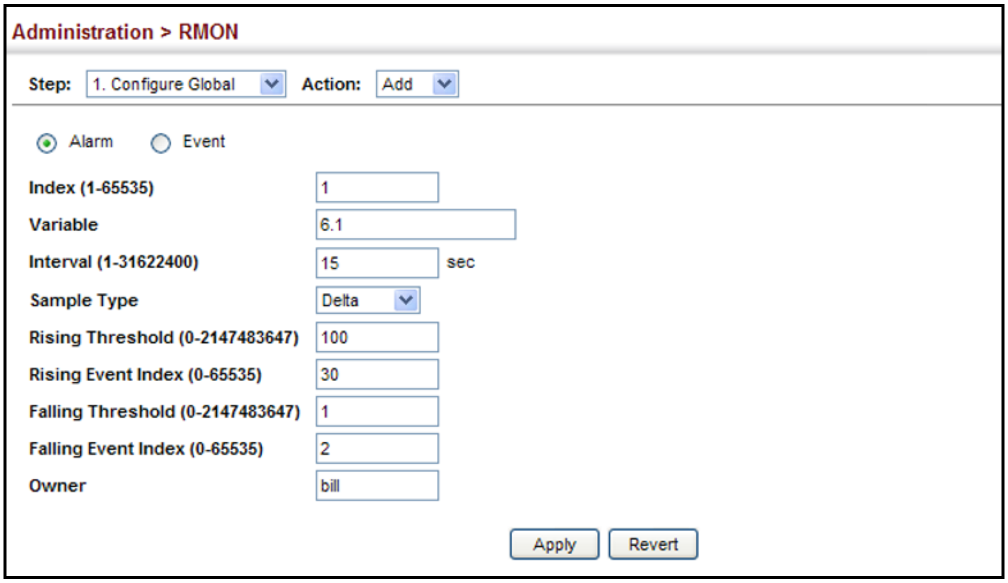
- **Owner** – Name of the person who created this entry. (Range: 1-127 characters)

WEB INTERFACE

To configure an RMON alarm:

1. Click Administration, RMON.
2. Select Configure Global from the Step list.
3. Select Add from the Action list.
4. Click Alarm.
5. Enter an index number, the MIB object to be polled (etherStatsEntry.n.n), the polling interval, the sample type, the thresholds, and the event to trigger.
6. Click Apply

Figure 275: Configuring an RMON Alarm



Administration > RMON

Step: 1. Configure Global Action: Add

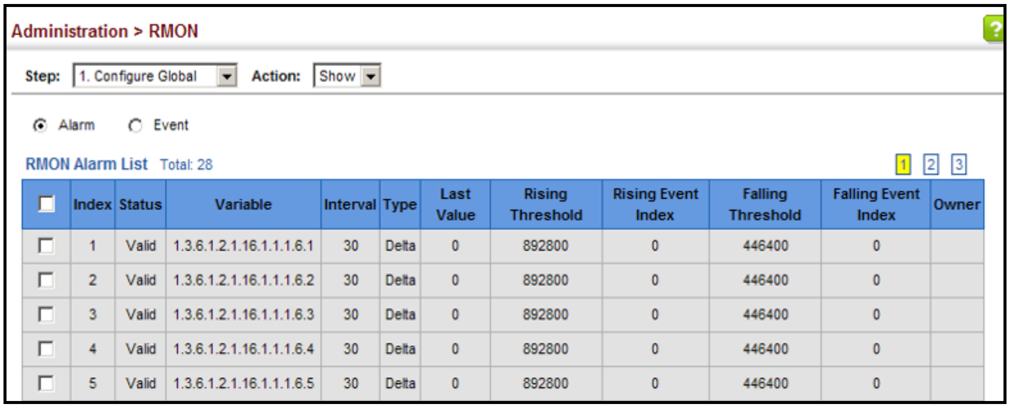
● Alarm ○ Event

Index (1-65535)	1
Variable	6.1
Interval (1-31622400)	15 sec
Sample Type	Delta
Rising Threshold (0-2147483647)	100
Rising Event Index (0-65535)	30
Falling Threshold (0-2147483647)	1
Falling Event Index (0-65535)	2
Owner	bill

To show configured RMON alarms:

1. Click Administration, RMON.
2. Select Configure Global from the Step list.
3. Select Show from the Action list.
4. Click Alarm.

Figure 276: Showing Configured RMON Alarms



Administration > RMON

Step: 1. Configure Global Action: Show

● Alarm ○ Event

RMON Alarm List Total: 28

1 2 3

□	Index	Status	Variable	Interval	Type	Last Value	Rising Threshold	Rising Event Index	Falling Threshold	Falling Event Index	Owner
□	1	Valid	1.3.6.1.2.1.16.1.1.1.6.1	30	Delta	0	892800	0	446400	0	
□	2	Valid	1.3.6.1.2.1.16.1.1.1.6.2	30	Delta	0	892800	0	446400	0	
□	3	Valid	1.3.6.1.2.1.16.1.1.1.6.3	30	Delta	0	892800	0	446400	0	
□	4	Valid	1.3.6.1.2.1.16.1.1.1.6.4	30	Delta	0	892800	0	446400	0	
□	5	Valid	1.3.6.1.2.1.16.1.1.1.6.5	30	Delta	0	892800	0	446400	0	

CONFIGURING RMON EVENTS

Use the Administration > RMON (Configure Global - Add - Event) page to set the action to take when an alarm is triggered. The response can include logging the alarm or sending a message to a trap manager. Alarms and corresponding events provide a way of immediately responding to critical network problems.

CLI REFERENCES

- "Remote Monitoring Commands" on page 1017

COMMAND USAGE

- If an alarm is already defined for an index, the entry must be deleted before any changes can be made.
- One default event is configured as follows:

  event Index = 1
  Description: RMON_TRAP_LOG
  Event type: log & trap
  Event community name is public
  Owner is RMON_SNMP

PARAMETERS

These parameters are displayed:

- **Index** – Index to this entry. (Range: 1-65535)

- **Type** – Specifies the type of event to initiate:
  - **None** – No event is generated.
  - **Log** – Generates an RMON log entry when the event is triggered. Log messages are processed based on the current configuration settings for event logging (see "System Log Configuration" on page 454).
  - **Trap** – Sends a trap message to all configured trap managers (see "Specifying Trap Managers" on page 500).
  - **Log and Trap** – Logs the event and sends a trap message.
- **Community** – A password-like community string sent with the trap operation to SNMP v1 and v2c hosts.

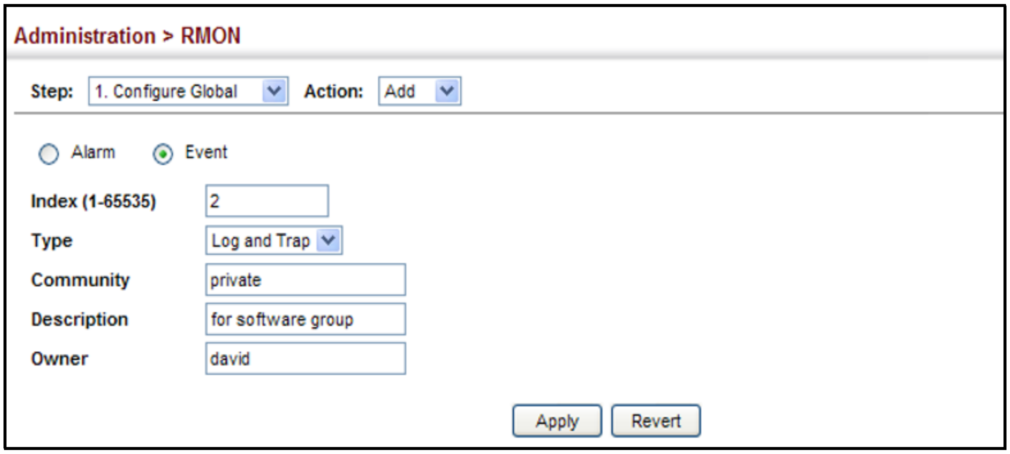
  Although the community string can be set on this configuration page, it is recommended that it be defined on the SNMP trap configuration page (see "Setting Community Access Strings" on page 494) prior to configuring it here. (Range: 1-127 characters)
- **Description** – A comment that describes this event. (Range: 1-127 characters)
- **Owner** – Name of the person who created this entry. (Range: 1-127 characters)

WEB INTERFACE

To configure an RMON event:

1. Click Administration, RMON.
2. Select Configure Global from the Step list.
3. Select Add from the Action list.
4. Click Event.
5. Enter an index number, the type of event to initiate, the community string to send with trap messages, the name of the person who created this event, and a brief description of the event.
6. Click Apply

Figure 277: Configuring an RMON Event



Administration > RMON

Step: 1. Configure Global Action: Add

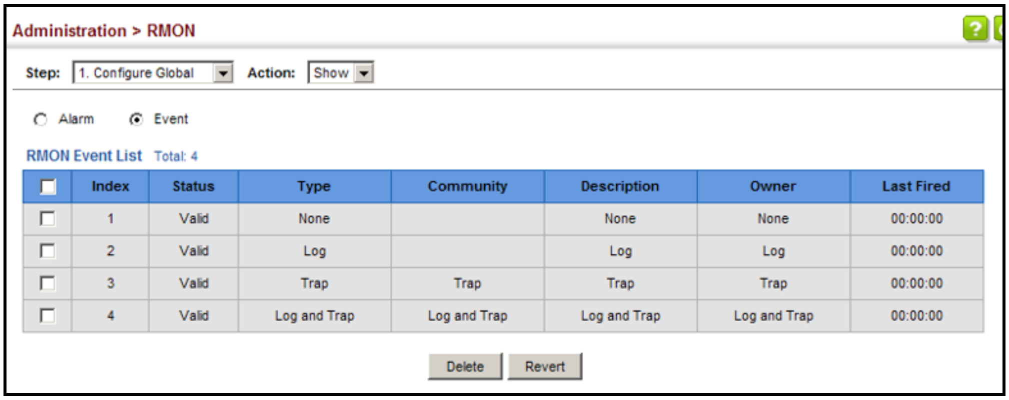
○ Alarm ● Event

Index (1-65535)	2
Type	Log and Trap
Community	private
Description	for software group
Owner	david

To show configured RMON events:

1. Click Administration, RMON.
2. Select Configure Global from the Step list.
3. Select Show from the Action list.
4. Click Event.

Figure 278: Showing Configured RMON Events



Administration > RMON

Step: 1. Configure Global Action: Show

○ Alarm ● Event

RMON Event List Total: 4

□	Index	Status	Type	Community	Description	Owner	Last Fired
□	1	Valid	None		None	None	00:00:00
□	2	Valid	Log		Log	Log	00:00:00
□	3	Valid	Trap	Trap	Trap	Trap	00:00:00
□	4	Valid	Log and Trap	Log and Trap	Log and Trap	Log and Trap	00:00:00

CONFIGURING RMON HISTORY SAMPLES

Use the Administration > RMON (Configure Interface - Add - History) page to collect statistics on a physical interface to monitor network utilization, packet types, and errors. A historical record of activity can be used to track down intermittent problems. The record can be used to establish normal baseline activity, which may reveal problems associated with high traffic levels, broadcast storms, or other unusual events. It can also be used to predict network growth and plan for expansion before your network becomes too overloaded.

CLI REFERENCES

- "Remote Monitoring Commands" on page 1017

COMMAND USAGE

- Each index number equates to a port on the switch.
- If history collection is already enabled on an interface, the entry must be deleted before any changes can be made.
- The information collected for each sample includes:

  input octets, packets, broadcast packets, multicast packets, undersize packets, oversize packets, fragments, jabbers, CRC alignment errors, collisions, drop events, and network utilization.

  For a description of the statistics displayed on the Show Details page, refer to "Showing Port or Trunk Statistics" on page 192.
- The switch reserves two index entries for each port. If a default index entry is re-assigned to another port using the Add page, this index will not appear in the Show nor Show Details page for the port to which is normally assigned. For example, if control entry 15 is assigned to port 5, this index entry will be removed from the Show and Show Details page for port 8.

PARAMETERS

These parameters are displayed:

- **Port** – The port number on the switch.
- **Index** – Index to this entry. (Range: 1-65535)
- **Interval** - The polling interval. (Range: 1-3600 seconds; Default: 1800 seconds)
- **Buckets** – The number of buckets requested for this entry. (Range: 1-65536; Default: 50)

  The number of buckets granted are displayed on the Show page.
- **Owner** - Name of the person who created this entry. (Range: 1-127 characters)

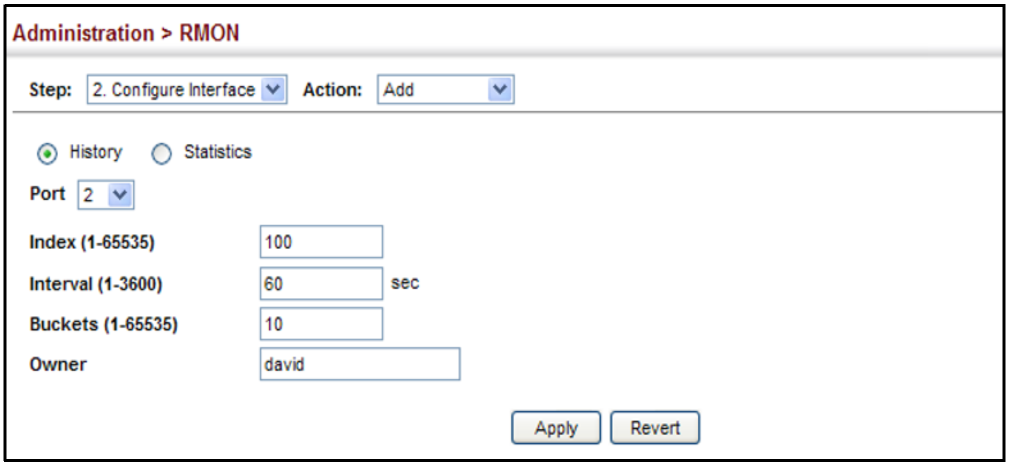
WEB INTERFACE

To periodically sample statistics on a port:

1. Click Administration, RMON.
2. Select Configure Interface from the Step list.
3. Select Add from the Action list.
4. Click History.
5. Select a port from the list as the data source.
6. Enter an index number, the sampling interval, the number of buckets to use, and the name of the owner for this entry.

7. Click Apply

Figure 279: Configuring an RMON History Sample



Administration > RMON

Step: 2. Configure Interface Action: Add

● History ○ Statistics

Port 2

Index (1-65535) 100

Interval (1-3600) 60 sec

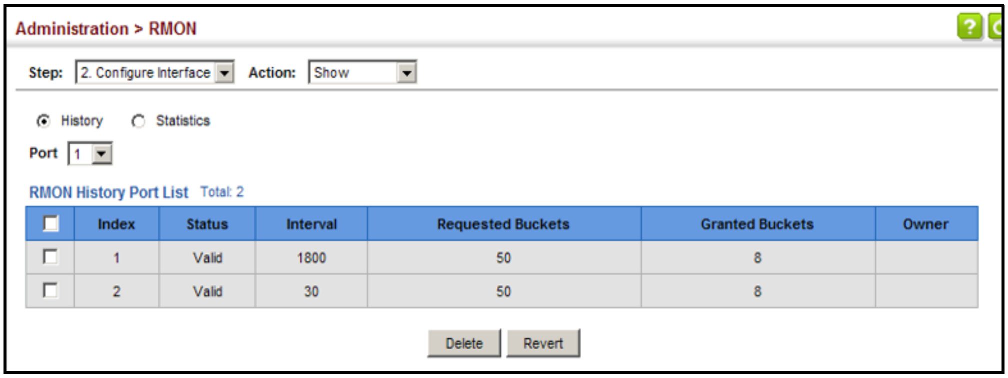
Buckets (1-65535) 10

Owner david

To show configured RMON history samples:

1. Click Administration, RMON.
2. Select Configure Interface from the Step list.
3. Select Show from the Action list.
4. Select a port from the list.
5. Click History.

Figure 280: Showing Configured RMON History Samples



Administration > RMON

Step: 2. Configure Interface Action: Show

● History ○ Statistics

Port 1

RMON History Port List Total: 2

□	Index	Status	Interval	Requested Buckets	Granted Buckets	Owner
□	1	Valid	1800	50	8	
□	2	Valid	30	50	8	

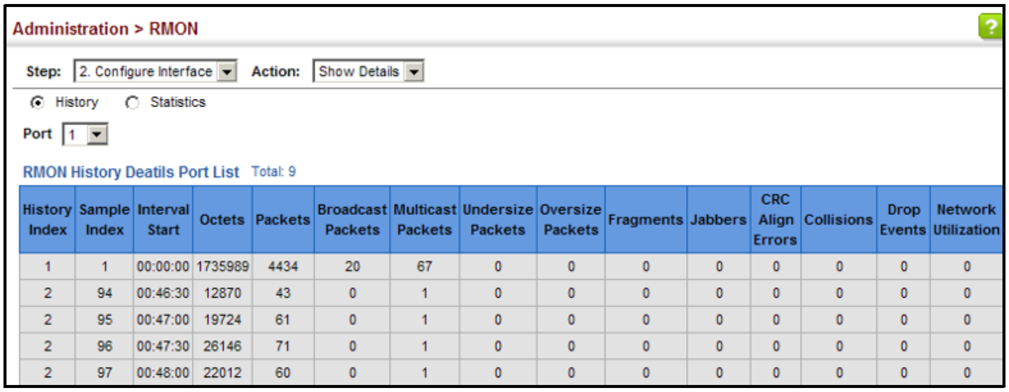
To show collected RMON history samples:

1. Click Administration, RMON.
2. Select Configure Interface from the Step list.
3. Select Show Details from the Action list.

4. Select a port from the list.

5. Click History.

Figure 281: Showing Collected RMON History Samples



Administration > RMON

Step: 2. Configure Interface Action: Show Details

● History ○ Statistics

Port 1

RMON History Deatils Port List Total: 9

History Index	Sample Index	Interval Start	Octets	Packets	Broadcast Packets	Multicast Packets	Undersize Packets	Oversize Packets	Fragments	Jabbers	CRC Align Errors	Collisions	Drop Events	Network Utilization
1	1	00:00:00	1735989	4434	20	67	0	0	0	0	0	0	0	0
2	94	00:46:30	12870	43	0	1	0	0	0	0	0	0	0	0
2	95	00:47:00	19724	61	0	1	0	0	0	0	0	0	0	0
2	96	00:47:30	26146	71	0	1	0	0	0	0	0	0	0	0
2	97	00:48:00	22012	60	0	1	0	0	0	0	0	0	0	0

CONFIGURING RMON STATISTICAL SAMPLES

Use the Administration > RMON (Configure Interface - Add - Statistics) page to collect statistics on a port, which can subsequently be used to monitor the network for common errors and overall traffic rates.

CLI REFERENCES

- "Remote Monitoring Commands" on page 1017

COMMAND USAGE

- If statistics collection is already enabled on an interface, the entry must be deleted before any changes can be made.

- The information collected for each entry includes:

  input octets, packets, broadcast packets, multicast packets, undersize packets, oversize packets, CRC alignment errors, jabbers, fragments, collisions, drop events, and frames of various sizes.

PARAMETERS

These parameters are displayed:

- **Port** – The port number on the switch.

- **Index** – Index to this entry. (Range: 1-65535)

- **Owner** – Name of the person who created this entry. (Range: 1-127 characters)

WEB INTERFACE

To enable regular sampling of statistics on a port:

1. Click Administration, RMON.

2. Select Configure Interface from the Step list.

3. Select Add from the Action list.

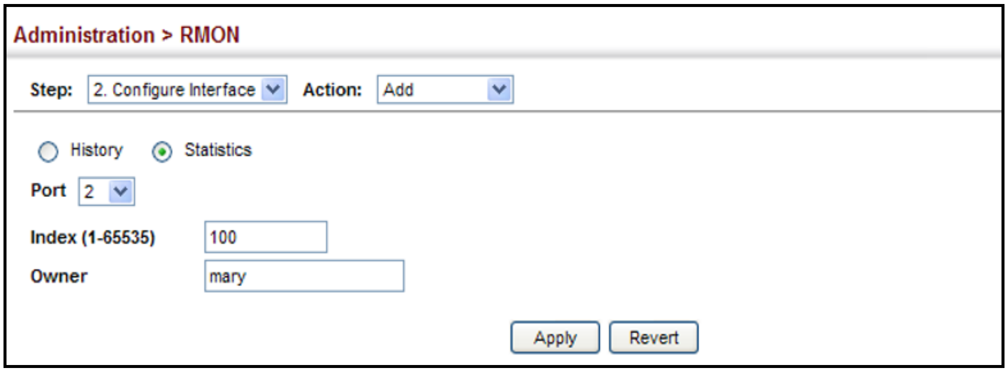
4. Click Statistics.

5. Select a port from the list as the data source.

6. Enter an index number, and the name of the owner for this entry

7. Click Apply

Figure 282: Configuring an RMON Statistical Sample



Administration > RMON

Step: 2. Configure Interface Action: Add

○ History ● Statistics

Port 2

Index (1-65535) 100

Owner mary

To show configured RMON statistical samples:

1. Click Administration, RMON.

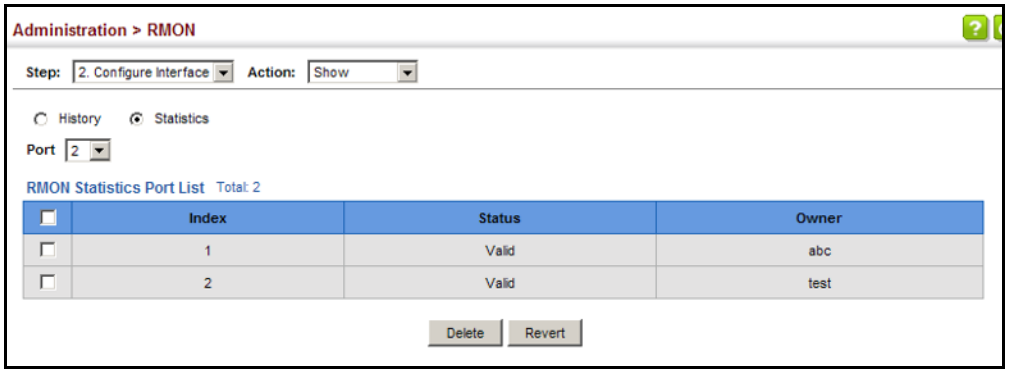
2. Select Configure Interface from the Step list.

3. Select Show from the Action list.

4. Select a port from the list.

5. Click Statistics.

Figure 283: Showing Configured RMON Statistical Samples



Administration > RMON

Step: 2. Configure Interface Action: Show

○ History ● Statistics

Port 2

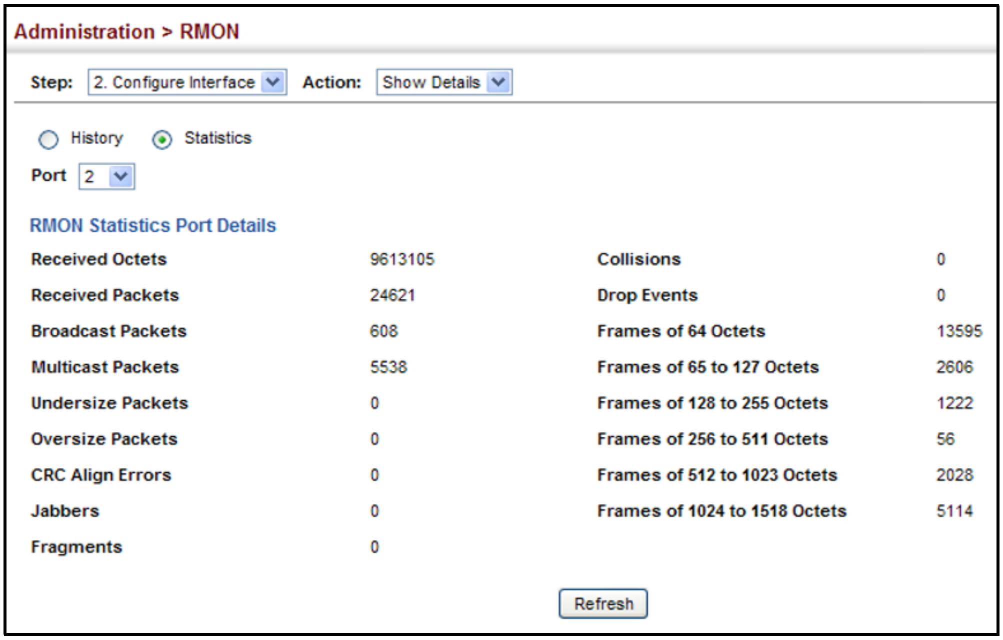
RMON Statistics Port List Total: 2

□	Index	Status	Owner
□	1	Valid	abc
□	2	Valid	test

To show collected RMON statistical samples:

1. Click Administration, RMON.
2. Select Configure Interface from the Step list.
3. Select Show Details from the Action list.
4. Select a port from the list.
5. Click Statistics.

Figure 284: Showing Collected RMON Statistical Samples



Step: 2. Configure Interface Action: Show Details

○ History ● Statistics

Port 2

RMON Statistics Port Details

Received Octets	9613105	Collisions	0
Received Packets	24621	Drop Events	0
Broadcast Packets	608	Frames of 64 Octets	13595
Multicast Packets	5538	Frames of 65 to 127 Octets	2606
Undersize Packets	0	Frames of 128 to 255 Octets	1222
Oversize Packets	0	Frames of 256 to 511 Octets	56
CRC Align Errors	0	Frames of 512 to 1023 Octets	2028
Jabbers	0	Frames of 1024 to 1518 Octets	5114
Fragments	0		

SWITCH CLUSTERING

Switch clustering is a method of grouping switches together to enable centralized management through a single unit. Switches that support clustering can be grouped together regardless of physical location or switch type, as long as they are connected to the same local network.

COMMAND USAGE

- A switch cluster has a primary unit called the "Commander" which is used to manage all other "Member" switches in the cluster. The management station can use either Telnet or the web interface to communicate directly with the Commander through its IP address, and then use the Commander to manage Member switches through the cluster's "internal" IP addresses.
- Clustered switches must be in the same Ethernet broadcast domain. In other words, clustering only functions for switches which can pass

information between the Commander and potential Candidates or active Members through VLAN 4094.

- Once a switch has been configured to be a cluster Commander, it automatically discovers other cluster-enabled switches in the network. These "Candidate" switches only become cluster Members when manually selected by the administrator through the management station.
- There can be up to 100 candidates and 36 member switches in one cluster.
- A switch can only be a member of one cluster.
- After the Commander and Members have been configured, any switch in the cluster can be managed from the web agent by choosing the desired Member ID from the Show Member page.

CONFIGURING GENERAL SETTINGS FOR CLUSTERS

Use the Administration > Cluster (Configure Global) page to create a switch cluster.

CLI REFERENCES

- "Switch Clustering" on page 989

COMMAND USAGE

First be sure that clustering is enabled on the switch (the default is disabled), then set the switch as a Cluster Commander. Set a Cluster IP Pool that does not conflict with the network IP subnet. Cluster IP addresses are assigned to switches when they become Members and are used for communication between Member switches and the Commander.

PARAMETERS

These parameters are displayed:

- **Cluster Status** – Enables or disables clustering on the switch. (Default: Disabled)
- **Commander Status** – Enables or disables the switch as a cluster Commander. (Default: Disabled)
- **IP Pool** – An "internal" IP address pool that is used to assign IP addresses to Member switches in the cluster. Internal cluster IP addresses are in the form 10.x.x.member-ID. Only the base IP address of the pool needs to be set since Member IDs can only be between 1 and 36. Note that you cannot change the cluster IP pool when the switch is currently in Commander mode. Commander mode must first be disabled. (Default: 10.254.254.1)
- **Role** – Indicates the current role of the switch in the cluster; either Commander, Member, or Candidate. (Default: Candidate)

- **Number of Members** – The current number of Member switches in the cluster.

- **Number of Candidates** – The current number of Candidate switches discovered in the network that are available to become Members.

WEB INTERFACE

To configure a switch cluster:

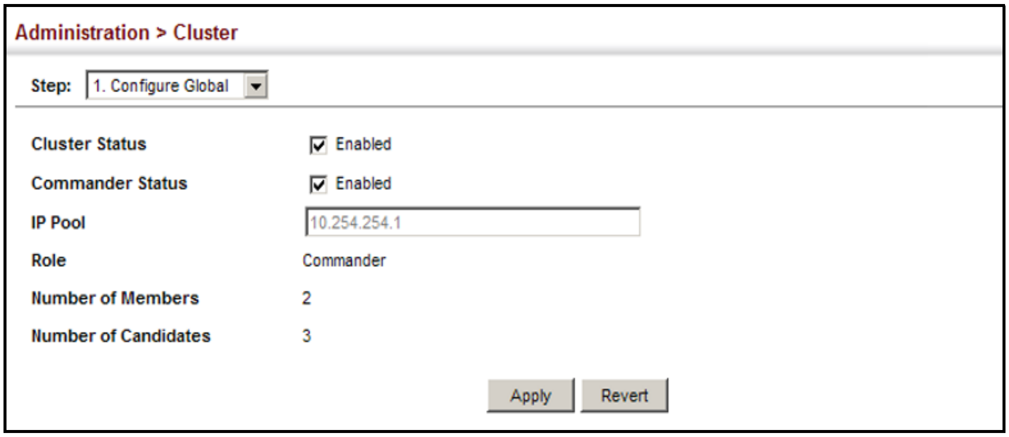
1. Click Administration, Cluster.

2. Select Configure Global from the Step list.

3. Set the required attributes for a Commander or a managed candidate.

4. Click Apply

Figure 285: Configuring a Switch Cluster



Administration > Cluster

Step: 1. Configure Global

Cluster Status ☑ Enabled
Commander Status ☑ Enabled
IP Pool 10.254.254.1
Role Commander
Number of Members 2
Number of Candidates 3

CLUSTER MEMBER CONFIGURATION

Use the Administration > Cluster (Configure Member - Add) page to add Candidate switches to the cluster as Members.

CLI REFERENCES

- "Switch Clustering" on page 989

PARAMETERS

These parameters are displayed:

- **Member ID** – Specify a Member ID number for the selected Candidate switch. (Range: 1-16)

- **MAC Address** – Select a discovered switch MAC address from the Candidate Table, or enter a specific MAC address of a known switch.

WEB INTERFACE

To configure cluster members:

1. Click Administration, Cluster.

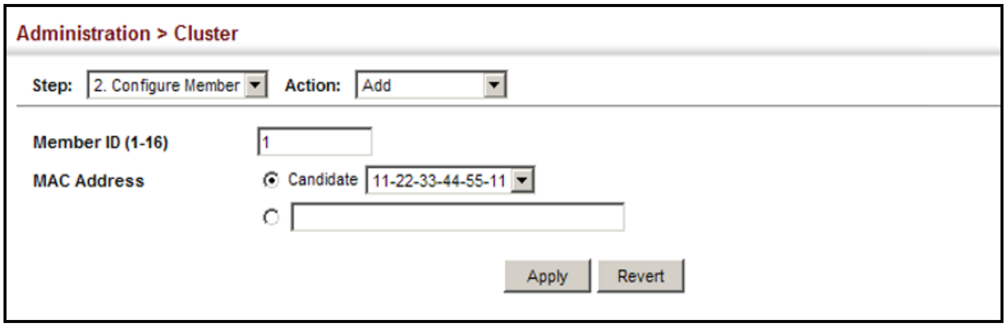
2. Select Configure Member from the Step list.

3. Select Add from the Action list.

4. Select one of the cluster candidates discovered by this switch, or enter the MAC address of a candidate.

5. Click Apply.

Figure 286: Configuring a Cluster Members



Administration > Cluster

Step: 2. Configure Member   Action: Add

Member ID (1-16)	1
MAC Address	● Candidate 11-22-33-44-55-11
	○

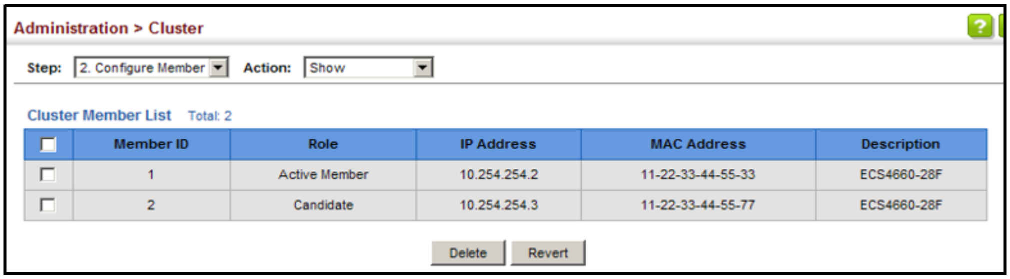
To show the cluster members:

1. Click Administration, Cluster.

2. Select Configure Member from the Step list.

3. Select Show from the Action list.

Figure 287: Showing Cluster Members



Administration > Cluster

Step: 2. Configure Member   Action: Show

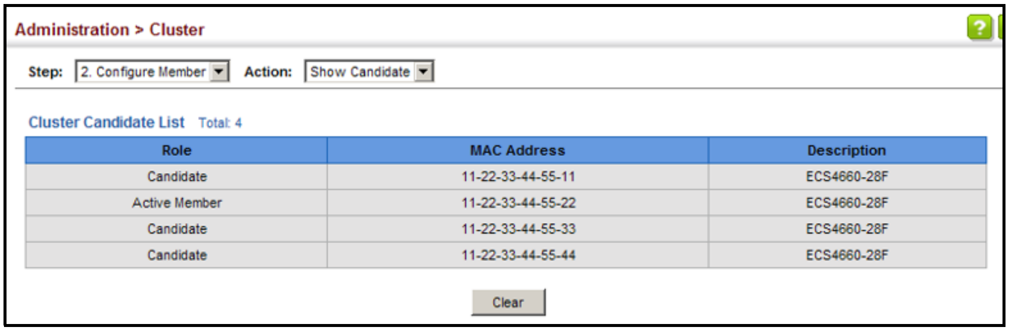
Cluster Member List   Total: 2

□	Member ID	Role	IP Address	MAC Address	Description
□	1	Active Member	10.254.254.2	11-22-33-44-55-33	ECS4660-28F
□	2	Candidate	10.254.254.3	11-22-33-44-55-77	ECS4660-28F

To show cluster candidates:

1. Click Administration, Cluster.
2. Select Configure Member from the Step list.
3. Select Show Candidate from the Action list.

Figure 288: Showing Cluster Candidates



Administration > Cluster

Step: 2. Configure Member Action: Show Candidate

Cluster Candidate List Total: 4

Role	MAC Address	Description
Candidate	11-22-33-44-55-11	ECS4660-28F
Active Member	11-22-33-44-55-22	ECS4660-28F
Candidate	11-22-33-44-55-33	ECS4660-28F
Candidate	11-22-33-44-55-44	ECS4660-28F

MANAGING CLUSTER MEMBERS

Use the Administration > Cluster (Show Member) page to manage another switch in the cluster.

CLI REFERENCES

- "Switch Clustering" on page 989

PARAMETERS

These parameters are displayed:

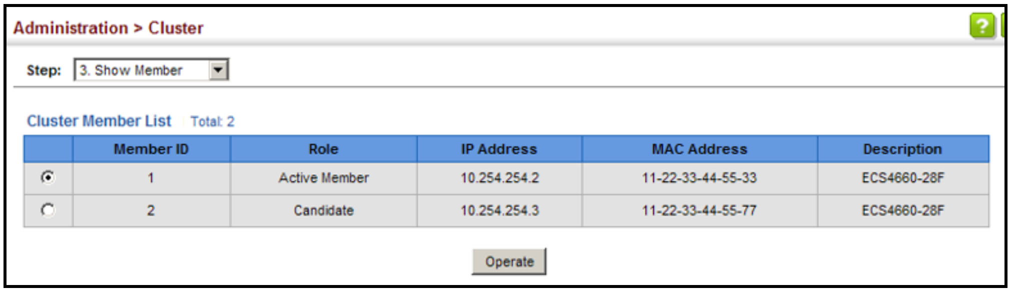
- **Member ID** – The ID number of the Member switch. (Range: 1-36)
- **Role** – Indicates the current status of the switch in the cluster.
- **IP Address** – The internal cluster IP address assigned to the Member switch.
- **MAC Address** – The MAC address of the Member switch.
- **Description** – The system description string of the Member switch.
- **Operate** – Remotely manage a cluster member.

WEB INTERFACE

To manage a cluster member:

1. Click Administration, Cluster.
2. Select Show Member from the Step list.
3. Select an entry from the Cluster Member List.
4. Click Operate.

Figure 289: Managing a Cluster Member



Step: 3. Show Member

Cluster Member List Total: 2

	Member ID	Role	IP Address	MAC Address	Description
●	1	Active Member	10.254.254.2	11-22-33-44-55-33	ECS4660-28F
○	2	Candidate	10.254.254.3	11-22-33-44-55-77	ECS4660-28F

ETHERNET RING PROTECTION SWITCHING

NOTE: Information in this section is based on ITU-T G.8032/Y.1344.

The ITU G.8032 recommendation specifies a protection switching mechanism and protocol for Ethernet layer network rings. Ethernet rings can provide wide-area multipoint connectivity more economically due to their reduced number of links. The mechanisms and protocol defined in G.8032 achieve highly reliable and stable protection; and never form loops, which would fatally affect network operation and service availability.

The G.8032 recommendation, also referred to as Ethernet Ring Protection Switching (ERPS), can be used to increase the availability and robustness of Ethernet rings. An Ethernet ring built using ERPS can provide resilience at a lower cost and than that provided by SONET or EAPS rings.

ERPS is more economical than EAPS in that only one physical link is required between each node in the ring. However, since it can tolerate only one break in the ring, it is not as robust as EAPS. ERPS supports up to 255 nodes in the ring structure. ERPS requires a higher convergence time when more that 16 nodes are used, but should always run under than 500 ms.

Operational Concept

Loop avoidance in the ring is achieved by guaranteeing that, at any time, traffic may flow on all but one of the ring links. This particular link is called the ring protection link (RPL), and under normal conditions this link is blocked to traffic. One designated node, the RPL owner, is responsible for blocking traffic over the RPL. When a ring failure occurs, the RPL owner is responsible for unblocking the RPL, allowing this link to be used for traffic.

Ring nodes may be in one of two states:

Idle – normal operation, no link/node faults detected in ring
Protection – Protection switching in effect after identifying a signal fault

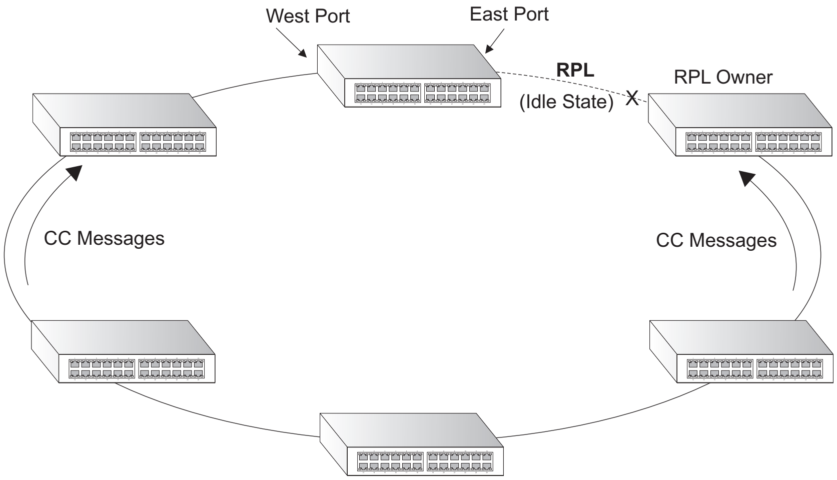
In Idle state, the physical topology has all nodes connected in a ring. The logical topology guarantees that all nodes are connected without a loop by blocking the RPL. Each link is monitored by its two adjacent nodes using Connectivity Fault Management (CFM) protocol messages.

Protection switching (opening the RPL to traffic) occurs when a signal failure message generated by the Connectivity Fault Management (CFM) protocol is declared on one of the ring links, and the detected failure has a higher priority than any other request; or a Ring – Automatic Protection Switching protocol request (R-APS, as defined in Y.1731) is received which has a higher priority than any other local request.

A link/node failure is detected by the nodes adjacent to the failure. These nodes block the failed link and report the failure to the ring using R-APS (SF) messages. This message triggers the RPL owner to unblock the RPL, and all nodes to flush their forwarding database. The ring is now in protection state, but it remains connected in a logical topology.

When the failed link recovers, the traffic is kept blocked on the nodes adjacent to the recovered link. The nodes adjacent to the recovered link transmit R-APS (NR - no request) message indicating they have no local request. When the RPL owner receives an R-APS (NR) message it starts the Wait-To-Recover (WTR) timer. Once WTR timer expires, the RPL owner blocks the RPL and transmits an R-APS (NR, RB - ring blocked) message. Nodes receiving this message flush the forwarding database and unblock their previously blocked ports. The ring is now returned to Idle state.

Figure 290: ERPS Ring Components



Multi-ring/Ladder Network – ERPSv2 also supports multipoint-to-multipoint connectivity within interconnected rings, called a "multi-ring/ladder network" topology. This arrangement consists of conjoined rings connected by one or more interconnection points, and is based on the following criteria:

- The R-APS channels are not shared across Ethernet Ring interconnections.
- On each ring port, each traffic channel and each R-APS channel are controlled (e.g., for blocking or flushing) by the Ethernet Ring Protection Control Process (ERP Control Process) of only one ring.
- Each Major Ring or Sub-Ring must have its own RPL.

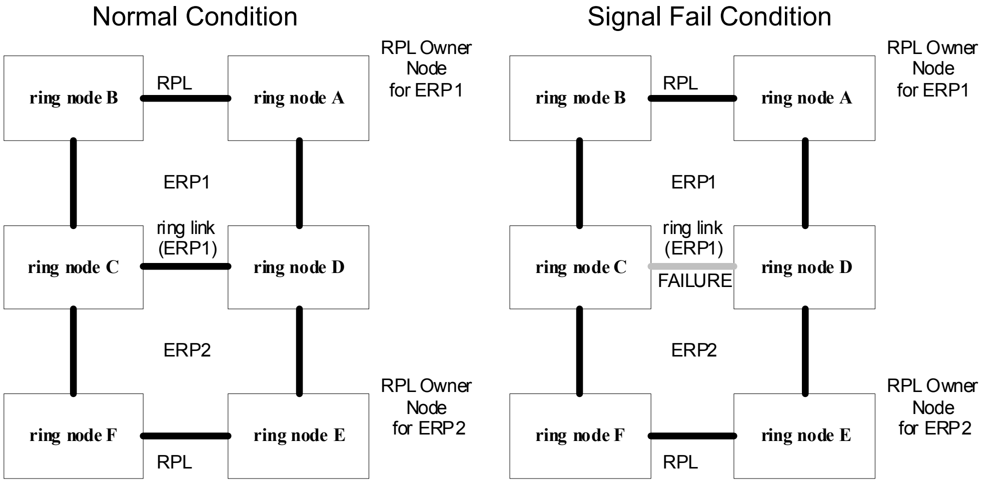
Figure 291 on page 526 (Normal Condition) depicts an example of a multi-ring/ladder network. If the network is in normal operating condition, the RPL owner node of each ring blocks the transmission and reception of traffic over the RPL for that ring. This figure presents the configuration when no failure exists on any ring link.

In the figure for the Normal Condition there are two interconnected rings. Ring ERP1 is composed of ring nodes A, B, C and D and the ring links between these nodes. Ring ERP2 is composed of ring nodes C, D, E and F and the ring links C-to-F, F-to-E, E-to-D. The ring link between D and C is used for traffic on rings ERP1 and ERP2. On their own ERP2 ring links do not form a closed loop. A closed loop may be formed by the ring links of ERP2 and the ring link between the interconnection nodes that is controlled by ERP1. ERP2 is a sub-ring. Ring node A is the RPL owner node for ERP1, and ring node E is the RPL owner node for ERP2. These ring nodes (A and E) are responsible for blocking the traffic channel on the RPL for ERP1 and ERP2 respectively. There is no restriction on which ring link on an ring may be set as the RPL. For example the RPL of ERP1 could be set as the link between ring node C and D.

Ring nodes C and D, that are common to both ERP1 and ERP2, are called interconnection nodes. The ring link between the interconnection nodes are controlled and protected by the ring it belongs to. In the example for the Normal Condition, the ring link between ring nodes C and D is part of ERP1, and, as such, are controlled and protected by ERP1. Ethernet characteristic information traffic corresponding to the traffic channel may be transferred over a common Ethernet connection for ERP1 and ERP2 through the interconnection nodes C and D. Interconnection nodes C and D have separate ERP Control Processes for each Ethernet Ring.

Figure 291 on page 526 (Signal Fail Condition) illustrates a situation where protection switching has occurred due to an SF condition on the ring link between interconnection nodes C and D. The failure of this ring link triggers protection only on the ring to which it belongs, in this case ERP1. The traffic and R-APS channels are blocked bi-directionally on the ports where the failure is detected and bi-directionally unblocked at the RPL connection point on ERP1. The traffic channels remain bi-directionally blocked at the RPL connection point on ERP2. This prevents the formation of a loop.

Figure 291: Ring Interconnection Architecture (Multi-ring/Ladder Network)



Configuration Guidelines for ERPS

1. Create an ERPS ring (Configure Domain – Add): The ring name is used as an index in the G.8032 database.

2. Configure the east and west interfaces (Configure Domain – Configure Details): Each node on the ring connects to it through two ring ports. Configure one port connected to the next node in the ring to the east (or clockwise direction) and another port facing west in the ring.

3. Configure the RPL owner (Configure Domain – Configure Details): Configure one node in the ring as the Ring Protection Link (RPL) owner. When this switch is configured as the RPL owner, the west ring port is set as being connected to the RPL. Under normal operations (Idle state), the RPL is blocked to ensure that a loop cannot form in the ring. If a signal failure brings down any other link in the ring, the RPL will be unblocked (Protection state) to ensure proper connectivity among all ring nodes until the failure is recovered.

4. Configure ERPS timers (Configure Domain – Configure Details): Set the Guard timer to prevent ring nodes from receiving outdated R-APS messages, the Hold-off timer to filter out intermittent link faults, and the WTR timer to verify that the ring has stabilized before blocking the RPL after recovery from a signal failure.

5. Configure the ERPS Control VLAN (Configure Domain – Configure Details): Specify the control VLAN (CVLAN) used to pass R-APS ring maintenance commands. The CVLAN must NOT be configured with an IP address. In addition, only ring ports may be added to the CVLAN (prior to configuring the VLAN as a CVLAN). No other ports can be members of this VLAN (once set as a CVLAN). Also, the ring ports of the CVLAN must be tagged. Failure to observe these restrictions can result in a loop in the network.

6. Enable ERPS (Configure Global): Before enabling a ring as described in the next step, first globally enable ERPS on the switch. If ERPS has not yet been enabled or has been disabled, no ERPS rings will work.

7. Enable an ERPS ring (Configure Domain – Configure Details): Before an ERPS ring can work, it must be enabled. When configuration is completed and the ring enabled, R-APS messages will start flowing in the control VLAN, and normal traffic will begin to flow in the data VLANs. A ring can be stopped by disabling the Admin Status on any node.

8. Display ERPS status information (Configure Domain – Show): Display ERPS status information for all configured rings.

Configuration Limitations for ERPS

The following configuration limitations apply to ERPS:

- One switch supports up to six ERPS rings – each ring must have one Control VLAN, and at most 255 Data VLANs.
- Ring ports can not be a member of a trunk, nor an LACP-enabled port.
- Dynamic VLANs are not supported as protected data ports.
- Exclusive use of STP or ERPS on any port.
- The switch takes about 350 ms to detect link-up on 1000Base-T copper ports, so the convergence time on this port type is more than 50 ms.
- One VLAN must be added to an ERPS domain as the CVLAN. This can be designated as any VLAN, other than the management VLAN. The CVLAN should only contain ring ports, and must not be configured with an IP address.

ERPS GLOBAL CONFIGURATION

Use the Administration > ERPS (Configure Global) page to globally enable or disable ERPS on the switch.

CLI REFERENCES

- "erps" on page 1307

PARAMETERS

These parameters are displayed:

- **ERPS Status** – Enables ERPS on the switch. (Default: Disabled)

  ERPS must be enabled globally on the switch before it can enabled on an ERPS ring (by setting the Admin Status on the Configure Domain – Configure Details page).

WEB INTERFACE

To globally enable ERPS on the switch:

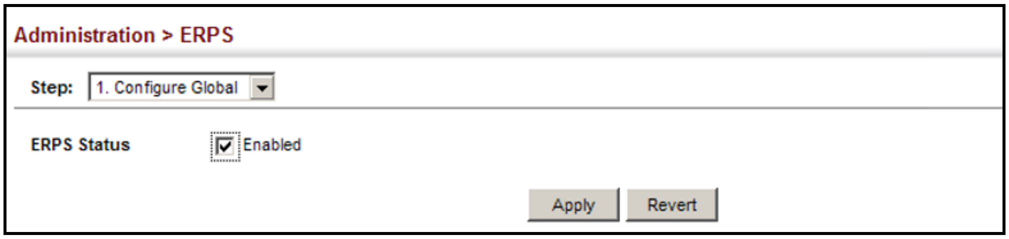
1. Click Administration, ERPS.

2. Select Configure Global from the Step list.

3. Mark the ERPS Status check box.

4. Click Apply.

Figure 292: Setting ERPS Global Status



Administration > ERPS

Step: 1. Configure Global

ERPS Status ☑ Enabled

ERPS RING CONFIGURATION

Use the Administration > ERPS (Configure Domain) pages to configure ERPS rings.

CLI REFERENCES

- "ERPS Commands" on page 1305

COMMAND USAGE

Ring Initialization

An ERPS ring containing one Control VLAN and one or more protected Data VLANs must be configured, and the global ERPS function enabled on the switch (see "ERPS Global Configuration" on page 527) before a ring can start running. Once enabled, the RPL owner node and non-owner node state machines will start, and the ring will enter the active state.

Limitations

When configuring a ring port, note that these ports cannot be part of a spanning tree, nor can they be members of a static or dynamic trunk.

PARAMETERS

These parameters are displayed:

Add

- **Domain Name** – Name of an ERPS ring. (Range: 1-12 characters)

- **Domain ID** – ERPS ring identifier used in R-APS messages. (Range: 1-255)

Show

- **Domain Name** – Name of a configured ERPS ring.
- **ID** – ERPS ring identifier used in R-APS messages.
- **Admin Status** – Shows whether ERPS is enabled on the switch.
- **Ver** – Shows the ERPS version.
- **MEG Level** – The maintenance entity group (MEG) level providing a communication channel for ring automatic protection switching (R-APS) information.
- **Control VLAN** – Shows the Control VLAN ID.
- **Node State** – Shows the following ERPS states:
  - Init – The ERPS ring has started but has not yet determined the status of the ring.
  - Idle – If all nodes in a ring are in this state, it means that all the links in the ring are up. This state will switch to protection state if a link failure occurs.
  - Protection – If a node in this state, it means that a link failure has occurred. This state will switch to idle state if all the failed links recover.
- **Type** – Shows node type as None, RPL Owner or RPL Neighbor.
- **Revertive** – Shows if revertive or non-revertive recovery is selected.
- **W/E** – Shows information on the west and east ring port for this node.
- **West Port** – Shows the west ring port for this node.
- **East Port** – Shows the east ring port for this node.
- **Interface** – The port or trunk which is configured as a ring port.
- **Port State** – The operational state:
  - Blocking – The transmission and reception of traffic is blocked and the forwarding of R-APS messages is blocked, but the transmission of locally generated R-APS messages is allowed and the reception of all R-APS messages is allowed.
  - Forwarding – The transmission and reception of traffic is allowed; transmission, reception and forwarding of R-APS messages is allowed.
  - Unknown – The interface is not in a known state (includes the domain being disabled).
- **Local SF** – A signal fault generated on a link to the local node.

- **Local FS** – Shows if a forced switch command was issued on this interface.
- **Local MS** – Shows if a manual switch command was issued on this interface.
- **MEP** – The CFM MEP used to monitor the status on this link.
- **RPL** – Shows if this node is connected to the RPL.

Configure Details

- **Domain Name** – Name of a configured ERPS ring. (Range: 1-12 characters)

  Service Instances within each ring are based on a unique maintenance association for the specific users, distinguished by the ring name, maintenance level, maintenance association’s name, and assigned VLAN. Up to 6 ERPS rings can be configured on the switch.

- **Domain ID** – ERPS ring identifier used in R-APS messages. (Range: 1-255; Default: None)

  R-APS information is carried in an R-APS PDUs. The last octet of the MAC address is designated as the Ring ID (01-19-A7-00-00-[Ring ID]). If use of the default MAC address is disabled for the R-APS Def MAC parameter, then the Domain ID will be used in R-APS PDUs.

- **Admin Status** – Activates the current ERPS ring. (Default: Disabled)

  Before enabling a ring, the global ERPS function should be enabled see ("ERPS Global Configuration" on page 527), the east and west ring ports configured on each node, the RPL owner specified, and the control VLAN configured.

  Once enabled, the RPL owner node and non-owner node state machines will start, and the ring will enter idle state if no signal failures are detected.

- **Version** – Specifies compatibility with the following ERPS versions:
  - 1 - ERPS version 1 based on ITU-T G.8032/Y.1344.
  - 2 - ERPS version 2 based on ITU-T G.8032/Y.1344 Version 2. (This is the default setting.)

  In addition to the basic features provided by version 1, version 2 also supports:

  - Multi-ring/ladder network support
  - Revertive/Non-revertive recovery
  - Forced Switch (FS) and Manual Switch (MS) commands for manually blocking a particular ring port
  - Flush FDB (forwarding database) logic which reduces amount of flush FDB operations in the ring
  - Support of multiple ERP instances on a single ring

Version 2 is backward compatible with Version 1. If version 2 is specified, the inputs and commands are forwarded transparently. If set to version 1, MS and FS operator commands are filtered, and the switch set to revertive mode.

The version number is automatically set to "1" when a ring node, supporting only the functionalities of G.8032v1, exists on the same ring with other nodes that support G.8032v2.

When ring nodes running G.8032v1 and G.8032v2 co-exist on a ring, the ring ID of each node is configured as "1".

In version 1, the MAC address 01-19-A7-00-00-01 is used for the node identifier. The R-APS Def MAC parameter has no effect.

- **MEG Level** – The maintenance entity group (MEG) level which provides a communication channel for ring automatic protection switching (R-APS) information. (Range: 0-7)

  This parameter is used to ensure that received R-APS PDUs are directed for this ring. A unique level should be configured for each local ring if there are many R-APS PDUs passing through this switch.

- **Control VLAN** – A dedicated VLAN used for sending and receiving E-APS protocol messages. (Range: 1-4094)

  Configure one control VLAN for each ERPS ring. First create the VLAN to be used as the control VLAN (see "Configuring VLAN Groups" on page 228), add the ring ports for the east and west interface as tagged members to this VLAN (see "Adding Static Members to VLANs" on page 231), and then use this parameter to add it to the ring.

  The following restrictions are recommended to avoid creating a loop in the network or other problems which may occur under some situations:

  - The Control VLAN must not be configured as a Layer 3 interface (with an IP address), a dynamic VLAN (with GVRP enabled), nor as a private VLAN.
  - In addition, only ring ports may be added to the Control VLAN. No other ports can be members of this VLAN.
  - Also, the ring ports of the Control VLAN must be tagged.

  Once the ring has been activated, the configuration of the control VLAN cannot be modified. Use the Admin Status parameter to stop the ERPS ring before making any configuration changes to the control VLAN.

- **Node State** – Refer to the parameters for the Show page.

- **Node Type** – Shows ERPS node type as one of the following:

  - **None** – Node is neither Ring Protection Link (RPL) owner nor neighbor. (This is the default setting.)

  - **RPL Owner** – Specifies a ring node to be the RPL owner.

    - Only one RPL owner can be configured on a ring. The owner blocks traffic on the RPL during Idle state, and unblocks it during Protection state (that is, when a signal fault is detected on the ring or the protection state is enabled with the Forced Switch or Manual Switch commands on the Configure Operation page).

    - The east and west connections to the ring must be specified for all ring nodes. When this switch is configured as the RPL owner, the west ring port is automatically set as being connected to the RPL.

  - **RPL Neighbor** – Specifies a ring node to be the RPL neighbor.

    - The RPL neighbor node, when configured, is a ring node adjacent to the RPL that is responsible for blocking its end of the RPL under normal conditions (i.e., the ring is established and no requests are present in the ring) in addition to the block at the other end by the RPL Owner Node. The RPL neighbor node may participate in blocking or unblocking its end of the RPL, but is not responsible for activating the reversion behavior.

    - Only one RPL owner can be configured on a ring. If the switch is set as the RPL owner for an ERPS domain, the west ring port is set as one end of the RPL. If the switch is set as the RPL neighbor for an ERPS domain, the east ring port is set as the other end of the RPL.

    - The east and west connections to the ring must be specified for all ring nodes. When this switch is configured as the RPL neighbor, the east ring port is set as being connected to the RPL.

    - Note that is not mandatory to declare a RPL neighbor.

- **Revertive** – Sets the method of recovery to Idle State through revertive or non-revertive mode. (Default: Enabled)

  - Revertive behavior allows the switch to automatically return the RPL from Protection state to Idle state through the exchange of protocol messages.

    Non-revertive behavior for Protection, Forced Switch (FS), and Manual Switch (MS) states are basically the same. Non-revertive behavior requires the RPL to be restored from Protection state to Idle state using the Clear command (Configure Operation page).

  - Recovery for Protection Switching – A ring node that has one or more ring ports in an SF (Signal Fail) condition, upon detecting the SF condition cleared, keeps at least one of its ring ports blocked for the traffic channel and for the R-APS channel, until the RPL is blocked as a result of ring protection reversion, or until there is another higher priority request (e.g., an SF condition) in the ring.

    A ring node that has one ring port in an SF condition and detects the SF condition cleared, continuously transmits the R-APS (NR – no request) message with its own Node ID as the priority information over both ring ports, informing that no request is present at this ring node and initiates a guard timer. When another recovered ring node (or nodes) holding the link block receives this message, it compares the Node ID information with its own Node ID. If the received R-APS (NR) message has the higher priority, this ring node unblocks its ring ports. Otherwise, the block remains unchanged. As a result, there is only one link with one end blocked.

The ring nodes stop transmitting R-APS (NR) messages when they accept an R-APS (NR, RB – RPL Blocked), or when another higher priority request is received.

- Recovery with Revertive Mode – When all ring links and ring nodes have recovered and no external requests are active, reversion is handled in the following way:

  a. The reception of an R-APS (NR) message causes the RPL Owner Node to start the WTR (Wait-to-Restore) timer.

  b. The WTR timer is cancelled if during the WTR period a higher priority request than NR is accepted by the RPL Owner Node or is declared locally at the RPL Owner Node.

  c. When the WTR timer expires, without the presence of any other higher priority request, the RPL Owner Node initiates reversion by blocking its traffic channel over the RPL, transmitting an R-APS (NR, RB) message over both ring ports, informing the ring that the RPL is blocked, and performing a flush FDB action.

  d. The acceptance of the R-APS (NR, RB) message causes all ring nodes to unblock any blocked non-RPL link that does not have an SF condition. If it is an R-APS (NR, RB) message without a DNF (do not flush) indication, all ring nodes flush the FDB.

- Recovery with Non-revertive Mode – In non-revertive operation, the ring does not automatically revert when all ring links and ring nodes have recovered and no external requests are active. Non-revertive operation is handled in the following way:

  a. The RPL Owner Node does not generate a response on reception of an R-APS (NR) messages.

  b. When other healthy ring nodes receive the NR (Node ID) message, no action is taken in response to the message.

  c. When the operator issues the Clear command (Configure Operation page) for non-revertive mode at the RPL Owner Node, the non-revertive operation is cleared, the RPL Owner Node blocks its RPL port, and transmits an R-APS (NR, RB) message in both directions, repeatedly.

  d. Upon receiving an R-APS (NR, RB) message, any blocking node should unblock its non-failed ring port. If it is an R-APS (NR, RB) message without a DNF indication, all ring nodes flush the FDB.

- Recovery for Forced Switching – A Forced Switch command is removed by issuing the Clear command (Configure Operation page) to the same ring node where Forced Switch mode is in effect. The clear command removes any existing local operator commands, and triggers reversion if the ring is in revertive behavior mode.

  The ring node where the Forced Switch was cleared continuously transmits the R-APS (NR) message on both ring ports, informing other nodes that no request is present at this ring node. The ring nodes stop transmitting R-APS (NR) messages when they accept an RAPS (NR, RB) message, or when another higher priority request is received.

  If the ring node where the Forced Switch was cleared receives an R-APS (NR) message with a Node ID higher than its own Node ID, it unblocks any ring port which does not have an SF condition and stops transmitting R-APS (NR) message over both ring ports.

  - Recovery with revertive mode is handled as follows:

    a. The reception of an R-APS (NR) message causes the RPL Owner Node to start the WTB timer.

    b. The WTB timer is cancelled if during the WTB period a higher priority request than NR is accepted by the RPL Owner Node or is declared locally at the RPL Owner Node.

    c. When the WTB timer expires, in the absence of any other higher priority request, the RPL Owner Node initiates reversion by blocking the traffic channel over the RPL, transmitting an R-APS (NR, RB) message over both ring ports, informing the ring that the RPL is blocked, and flushes the FDB.

    d. The acceptance of the R-APS (NR, RB) message causes all ring nodes to unblock any blocked non-RPL that does not have an SF condition. If it is an R-APS (NR, RB) message without a DNF indication, all ring nodes flush their FDB. This action unblocks the ring port which was blocked as a result of an operator command.

  - Recovery with non-revertive mode is handled as follows:

    a. The RPL Owner Node, upon reception of an R-APS(NR) message and in the absence of any other higher priority request does not perform any action.

    b. Then, after the operator issues the Clear command (Configure Operation page) at the RPL Owner Node, this ring node blocks the ring port attached to the RPL, transmits an R-APS (NR, RB) message on both ring ports, informing the ring that the RPL is blocked, and flushes its FDB.

   c. The acceptance of the R-APS (NR, RB) message triggers all ring nodes to unblock any blocked non-RPL which does not have an SF condition. If it is an R-APS (NR, RB) message without a DNF indication, all ring nodes flush their FDB. This action unblocks the ring port which was blocked as result of an operator command.

- Recovery for Manual Switching – A Manual Switch command is removed by issuing the Clear command (Configure Operation page) at the same ring node where the Manual Switch is in effect. The clear command removes any existing local operator commands, and triggers reversion if the ring is in revertive behavior mode.

  The ring node where the Manual Switch was cleared keeps the ring port blocked for the traffic channel and for the R-APS channel, due to the previous Manual Switch command. This ring port is kept blocked until the RPL is blocked as a result of ring protection reversion, or until there is another higher priority request (e.g., an SF condition) in the ring.

  The Ethernet Ring Node where the Manual Switch was cleared continuously transmits the R-APS (NR) message on both ring ports, informing that no request is present at this ring node. The ring nodes stop transmitting R-APS (NR) messages when they accept an RAPS (NR, RB) message, or when another higher priority request is received.

  If the ring node where the Manual Switch was cleared receives an R-APS (NR) message with a Node ID higher than its own Node ID, it unblocks any ring port which does not have an SF condition and stops transmitting R-APS (NR) message on both ring ports.

  - Recovery with revertive mode is handled as follows:

    a. The RPL Owner Node, upon reception of an R-APS (NR) message and in the absence of any other higher priority request, starts the WTB timer and waits for it to expire. While the WTB timer is running, any latent R-APS (MS) message is ignored due to the higher priority of the WTB running signal.

    b. When the WTB timer expires, it generates the WTB expire signal. The RPL Owner Node, upon reception of this signal, initiates reversion by blocking the traffic channel on the RPL, transmitting an R-APS (NR, RB) message over both ring ports, informing the ring that the RPL is blocked, and flushes its FDB.

    c. The acceptance of the R-APS (NR, RB) message causes all ring nodes to unblock any blocked non-RPL that does not have an SF condition. If it is an R-APS (NR, RB) message without a DNF indication, all Ethernet Ring Nodes flush their FDB. This action unblocks the ring port which was blocked as a result of an operator command.

- Recovery with non-revertive mode is handled as follows:

  a. The RPL Owner Node, upon reception of an R-APS (NR) message and in the absence of any other higher priority request does not perform any action.

  b. Then, after the operator issues the Clear command (Configure Operation page) at the RPL Owner Node, this ring node blocks the ring port attached to the RPL, transmits an R-APS (NR, RB) message over both ring ports, informing the ring that the RPL is blocked, and flushes its FDB.

  c. The acceptance of the R-APS (NR, RB) message triggers all ring nodes to unblock any blocked non-RPL which does not have an SF condition. If it is an R-APS (NR, RB) message without a DNF indication, all ring nodes flush their FDB. This action unblocks the ring port which was blocked as result of an operator command.

- **Major Domain** – The ERPS ring used for sending control packets.

  This switch can support up to six rings. However, ERPS control packets can only be sent on one ring. This parameter is used to indicate that the current ring is a secondary ring, and to specify the major ring which will be used to send ERPS control packets.

  The Ring Protection Link (RPL) is always the west port. So the physical port on a secondary ring must be the west port. In other words, if a domain has two physical ring ports, this ring can only be a major ring, not a secondary ring (or sub-domain) which can have only one physical ring port. The major domain therefore cannot be set if the east port is already configured.

- **Node ID** – A MAC address unique to the ring node. The MAC address must be specified in the format xx-xx-xx-xx-xx-xx or xxxxxxxxxxxx. (Default: CPU MAC address)

  The ring node identifier is used to identify a node in R-APS messages for both automatic and manual switching recovery operations.

  For example, a node that has one ring port in SF condition and detects that the condition has been cleared, will continuously transmit R-APS (NR) messages with its own Node ID as priority information over both ring ports, informing its neighbors that no request is present at this node. When another recovered node holding the link blocked receives this message, it compares the Node ID information with its own. If the received R-APS (NR) message has a higher priority, this unblocks its ring ports. Otherwise, the block remains unchanged.

  The node identifier may also be used for debugging, such as to distinguish messages when a node is connected to more than one ring.

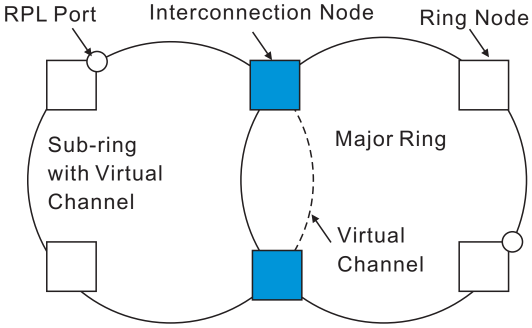
- **R-APS with VC** – Configures an R-APS virtual channel to connect two interconnection points on a sub-ring, allowing ERPS protocol traffic to be tunneled across an arbitrary Ethernet network. (Default: Enabled)

- A sub-ring may be attached to a primary ring with or without a virtual channel. A virtual channel is used to connect two interconnection points on the sub-ring, tunneling R-APS control messages across an arbitrary Ethernet network topology. If a virtual channel is not used to cross the intermediate Ethernet network, data in the traffic channel will still flow across the network, but the all R-APS messages will be terminated at the interconnection points.

- Sub-ring with R-APS Virtual Channel – When using a virtual channel to tunnel R-APS messages between interconnection points on a sub-ring, the R-APS virtual channel may or may not follow the same path as the traffic channel over the network. R-APS messages that are forwarded over the sub-ring's virtual channel are broadcast or multicast over the interconnected network. For this reason the broadcast/multicast domain of the virtual channel should be limited to the necessary links and nodes. For example, the virtual channel could span only the interconnecting rings or sub-rings that are necessary for forwarding R-APS messages of this sub-ring. Care must also be taken to ensure that the local RAPS messages of the sub-ring being transported over the virtual channel into the interconnected network can be uniquely distinguished from those of other interconnected ring R-APS messages. This can be achieved by, for example, by using separate VIDs for the virtual channels of different sub-rings.

  Note that the R-APS virtual channel requires a certain amount of bandwidth to forward R-APS messages on the interconnected Ethernet network where a sub-ring is attached. Also note that the protection switching time of the sub-ring may be affected if R-APS messages traverse a long distance over an R-APS virtual channel.

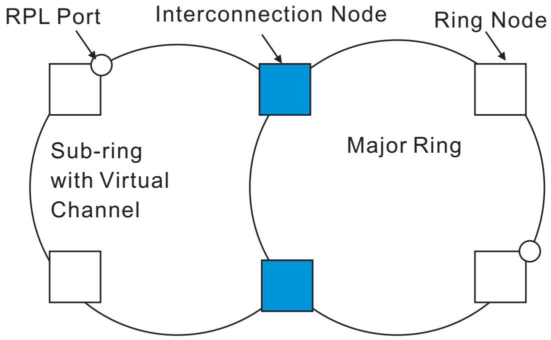
  Figure 293: Sub-ring with Virtual Channel

- Sub-ring without R-APS Virtual Channel – Under certain circumstances it may not be desirable to use a virtual channel to interconnect the sub-ring over an arbitrary Ethernet network. In this situation, the R-APS messages are terminated on the interconnection points. Since the sub-ring does not provide an R-APS channel nor R-APS virtual channel beyond the interconnection points, R-APS channel blocking is not employed on the normal ring links to avoid channel segmentation. As a result, a failure at any ring link in the sub-ring will cause the R-APS channel of the sub-ring to be segmented, thus preventing R-APS message exchange between some of the sub-ring's ring nodes.

No R-APS messages are inserted or extracted by other rings or sub-rings at the interconnection nodes where a sub-ring is attached. Hence there is no need for either additional bandwidth or for different VIDs/Ring IDs for the ring interconnection. Furthermore, protection switching time for a sub-ring is independent from the configuration or topology of the interconnected rings. In addition, this option always ensures that an interconnected network forms a tree topology regardless of its interconnection configuration. This means that it is not necessary to take precautions against forming a loop which is potentially composed of a whole interconnected network.

Figure 294: Sub-ring without Virtual Channel



- **R-APS Def MAC** – Sets the switch's MAC address to be used as the node identifier in R-APS messages. (Default: Enabled)

  When ring nodes running ERPSv1 and ERPSv2 co-exist on the same ring, the Ring ID of each ring node must be configured as "1".

  If this command is disabled, the following strings are used as the node identifier:

  - ERPSv1: 01-19-A7-00-00-01
  - ERPSv2: 01-19-A7-00-00-[Ring ID]

- **Propagate TC** – Enables propagation of topology change messages from a secondary ring to the primary ring. (Default: Disabled)

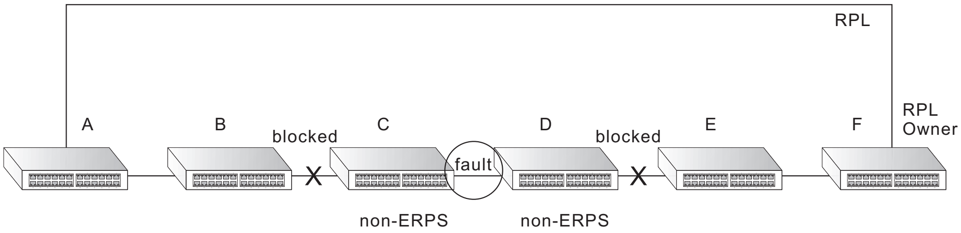
  When a secondary ring detects a topology change, it can pass a message about this event to the major ring. When the major ring receives this kind of message from a secondary ring, it can clear the MAC addresses on its ring ports to help the second ay ring restore its connections more quickly through protection switching.

  When the MAC addresses are cleared, data traffic may flood onto the major ring. The data traffic will become stable after the MAC addresses are learned again. The major ring will not be broken, but the bandwidth of data traffic on the major ring may suffer for a short period of time due to this flooding behavior.

- **Non-ERPS Device Protection** – Sends non-standard health-check packets when an owner node enters protection state without any link down event having been detected through Signal Fault messages. (Default: Disabled)

- The RPL owner node detects a failed link when it receives R-APS (SF - signal fault) messages from nodes adjacent to the failed link. The owner then enters protection state by unblocking the RPL. However, using this standard recovery procedure may cause a non-EPRS device to become isolated when the ERPS device adjacent to it detects a continuity check message (CCM) loss event and blocks the link between the non-ERPS device and ERPS device.

  CCMs are propagated by the Connectivity Fault Management (CFM) protocol as described under "Connectivity Fault Management" on page 548. If the standard recovery procedure were used as shown in the following figure, and node E detected CCM loss, it would send an R-APS (SF) message to the RPL owner and block the link to node D, isolating that non-ERPS device.



  When non-ERPS device protection is enabled on the ring, the ring ports on the RPL owner node and non-owner nodes will not be blocked when signal loss is detected by CCM loss events.

- When non-ERPS device protection is enabled on an RPL owner node, it will send non-standard health-check packets to poll the ring health when it enters the protection state. It does not use the normal procedure of waiting to receive an R-APS (NR - no request) message from nodes adjacent to the recovered link. Instead, it waits to see if the non-standard health-check packets loop back. If they do, indicating that the fault has been resolved, the RPL will be blocked.

  After blocking the RPL, the owner node will still transmit an R-APS (NR, RB - ring blocked) message. ERPS-compliant nodes receiving this message flush their forwarding database and unblock previously blocked ports. The ring is now returned to Idle state.

- **Holdoff Timer** – The hold-off timer is used to filter out intermittent link faults. Faults will only be reported to the ring protection mechanism if this timer expires. (Range: 0-10000 milliseconds, in steps of 100 milliseconds)

  In order to coordinate timing of protection switches at multiple layers, a hold-off timer may be required. Its purpose is to allow, for example, a server layer protection switch to have a chance to fix the problem before switching at a client layer.

  When a new defect or more severe defect occurs (new Signal Failure), this event will not be reported immediately to the protection switching mechanism if the provisioned hold-off timer value is non-zero. Instead, the hold-off timer will be started. When the timer expires, whether a defect still exists or not, the timer will be checked. If one does exist, that defect will be reported to the protection switching mechanism. The reported defect need not be the same one that started the timer.

- **Guard Timer** – The guard timer is used to prevent ring nodes from receiving outdated R-APS messages. During the duration of the guard timer, all received R-APS messages are ignored by the ring protection control process, giving time for old messages still circulating on the ring to expire. (Range: 10-2000 milliseconds, in steps of 10 milliseconds)

  The guard timer duration should be greater than the maximum expected forwarding delay for an R-APS message to pass around the ring. A side-effect of the guard timer is that during its duration, a node will be unaware of new or existing ring requests transmitted from other nodes.

- **WTB Timer** – The Wait to Block (WTB) timer is used when clearing Forced Switch (FS) and Manual Switch (MS) commands. As multiple FS commands are allowed to co-exist in a ring, the WTB timer ensures that clearing of a single FS command does not trigger re-blocking of the RPL. When clearing an MS command, the WTB timer prevents the formation of a closed loop due to possible a timing anomaly where the RPL owner node receives an outdated remote MS request during the recovery process.

  When recovering from an FS or MS command, the delay timer must be long enough to receive any latent remote FS or MS commands. This delay timer called the WTB timer is defined to be 5 seconds longer than the guard timer. This is enough time to allow a reporting ring node to transmit two R-APS messages and allow the ring to identify the latent condition.

  This delay timer is activated on the RPL owner node. When the relevant delay timer expires, the RPL owner node initiates the reversion process by transmitting an R-APS (NR, RB) message. The delay timer, (i.e., WTR or WTB) is deactivated when any higher priority request pre-empts this delay timer.

  The delay timers (i.e. WTR and WTB) may be started and stopped by the system. A request to start running the delay timer does not restart the delay timer. A request to stop the delay timer stops the delay timer and resets its value. The Clear command (Configure Operation page) can be used to stop the delay timer.

- **WTR Timer** – The wait-to-restore timer is used to verify that the ring has stabilized before blocking the RPL after recovery from a signal failure. (Range: 5-12 minutes)

  If the switch goes into ring protection state due to a signal failure, after the failure condition is cleared, the RPL owner will start the wait-to-restore timer and wait until it expires to verify that the ring has stabilized before blocking the RPL and returning to the Idle (normal operating) state.

- **WTB Expire** – The time before the wait-to-block timer expires.

- **WTR Expire** – The time before the wait-to-restore timer expires.

- **West/East** – Connects to next ring node to the west/east.

  Each node must be connected to two neighbors on the ring. For convenience, the ports connected are referred to as east and west ports. Alternatively, the closest neighbor to the east should be the next node in the ring in a clockwise direction, and the closest neighbor to the west should be the next node in the ring in a counter-clockwise direction.

- **Interface** – The port or trunk attached to the west or east ring port.

  Note that a ring port cannot be configured as a member of a spanning tree, a dynamic trunk, or a static trunk.

- **Port State** – Once configured, this field shows the operational state of the ring ports for this node:

  - Blocking – The transmission and reception of traffic is blocked and the forwarding of R-APS messages is blocked, but the transmission of locally generated R-APS messages is allowed and the reception of all R-APS messages is allowed.
  - Forwarding – The transmission and reception of traffic is allowed; transmission, reception and forwarding of R-APS messages is allowed.
  - Unknown – The interface is not in a known state.

- **Local SF** – Shows if a signal fault exists on a link to the local node.

- **Local FS** – Shows if a forced switch command was issued on this interface.

- **Local MS** – Shows if a manual switch command was issued on this interface.

- **MEP** – Specifies the CCM MEPs used to monitor the link on a ring node.

  If a MEP is used to monitor the link status of an ERPS node with CFM continuity check messages, then the MEG Level parameter on this configuration page must match the authorized maintenance level of the CFM domain to which the specified MEP belongs. (See "Configuring CFM Maintenance Domains" on page 555.)

  To ensure complete monitoring of a ring node, specify the CFM MEPs used to monitor both the east and west ports of the ring node.

  If CFM determines that a MEP node which has been configured to monitor a ring port with this command has gone down, this information is passed to ERPS, which in turn processes it as a ring node failure. For more information on how ERPS recovers from a node failure, refer to the description of the Revertive parameter on this configuration page.

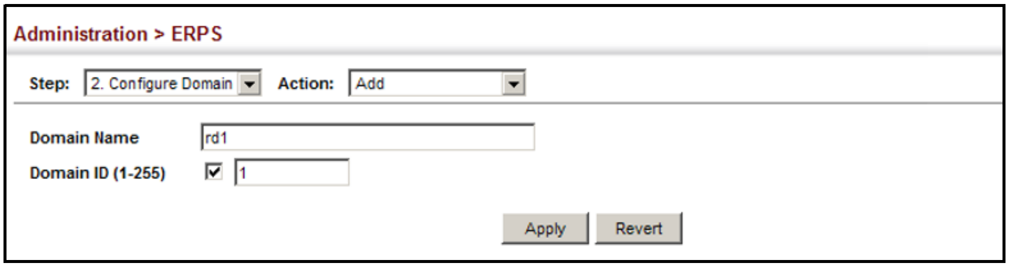
- **RPL** – If node is connected to the RPL, this shows by which interface.

WEB INTERFACE

To create an ERPS ring:

1. Click Administration, ERPS.
2. Select Configure Domain from the Step list.
3. Select Add from the Action list.
4. Enter a name and optional identifier for the ring.
5. Click Apply.

Figure 295: Creating an ERPS Ring



Administration > ERPS

Step: 2. Configure Domain Action: Add

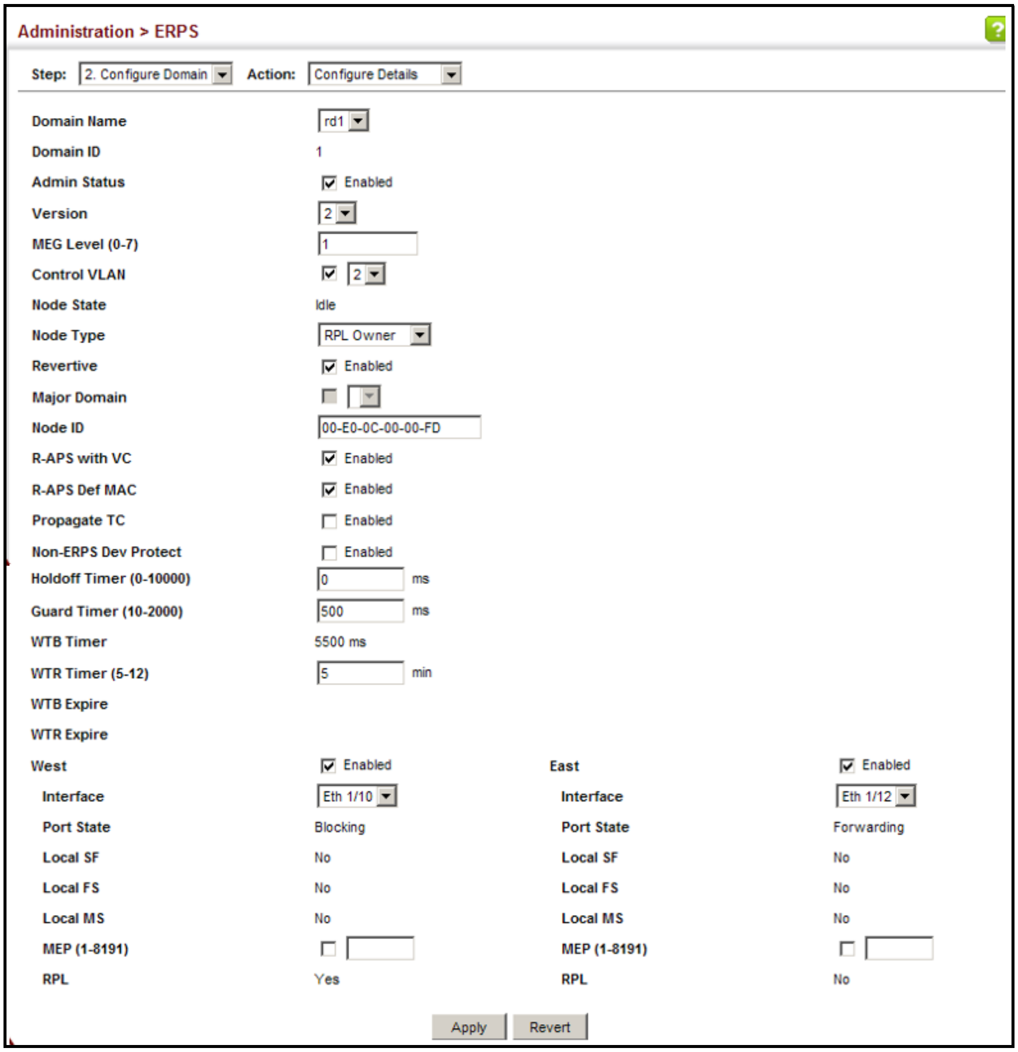
Domain Name: rd1

Domain ID (1-255): ☑ 1

To configure the ERPS parameters for a ring:

1. Click Administration, ERPS.
2. Select Configure Domain from the Step list.
3. Select Configure Details from the Action list.
4. Configure the ERPS parameters for this node. Note that spanning tree protocol cannot be configured on the ring ports, nor can these ports be members of a static or dynamic trunk. And the control VLAN must be unique for each ring. Adjust the protocol timers as required. The RPL owner must be set on one of the rings. And the administrative status enabled once all of the other settings have been entered.
5. Click Apply.

Figure 296: Creating an ERPS Ring



Administration > ERPS

Step: 2. Configure Domain Action: Configure Details

Domain Name	rd1		
Domain ID	1		
Admin Status	☑ Enabled		
Version	2		
MEG Level (0-7)	1		
Control VLAN	☑ 2		
Node State	Idle		
Node Type	RPL Owner		
Revertive	☑ Enabled		
Major Domain	□		
Node ID	00-E0-0C-00-00-FD		
R-APS with VC	☑ Enabled		
R-APS Def MAC	☑ Enabled		
Propagate TC	□ Enabled		
Non-ERPS Dev Protect	□ Enabled		
Holdoff Timer (0-10000)	0 ms		
Guard Timer (10-2000)	500 ms		
WTB Timer	5500 ms		
WTR Timer (5-12)	5 min		
WTB Expire			
WTR Expire			
West	☑ Enabled	East	☑ Enabled
Interface	Eth 1/10	Interface	Eth 1/12
Port State	Blocking	Port State	Forwarding
Local SF	No	Local SF	No
Local FS	No	Local FS	No
Local MS	No	Local MS	No
MEP (1-8191)	□	MEP (1-8191)	□
RPL	Yes	RPL	No

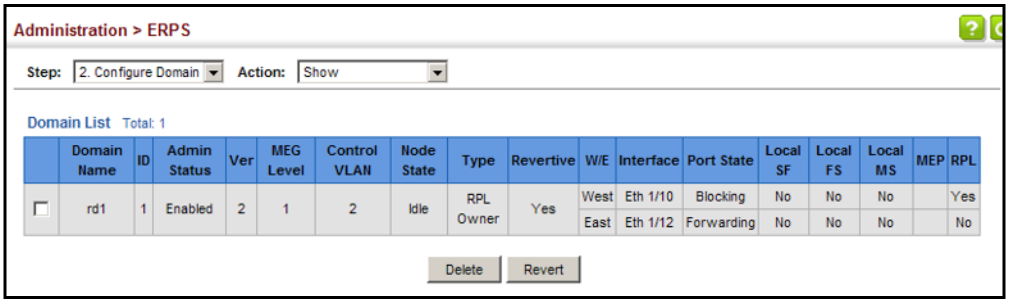
To show the configure ERPS rings:

1. Click Administration, ERPS.

2. Select Configure Domain from the Step list.

3. Select Show from the Action list.

Figure 297: Showing Configured ERPS Rings



Administration > ERPS

Step: 2. Configure Domain Action: Show

Domain List Total: 1

	Domain Name	ID	Admin Status	Ver	MEG Level	Control VLAN	Node State	Type	Revertive	W/E	Interface	Port State	Local SF	Local FS	Local MS	MEP	RPL
□	rd1	1	Enabled	2	1	2	Idle	RPL Owner	Yes	West	Eth 1/10	Blocking	No	No	No		Yes
										East	Eth 1/12	Forwarding	No	No	No		No

ERPS Forced and Manual Mode Operations

Use the Administration > ERPS (Configure Operation) page to block a ring port using Forced Switch or Manual Switch commands.

CLI References

- "erps forced-switch" on page 1327
- "erps manual-switch" on page 1329
- "erps clear" on page 1327

Parameters

These parameters are displayed:

- **Domain Name** – Name of a configured ERPS ring.
- **Operation** – Specifies a Forced Switch (FS) or Manual Switch (MS) operation on the east or west ring port.
  - **Forced Switch** – Blocks specified ring port.
    - A ring with no pending request has a logical topology with the traffic channel blocked at the RPL and unblocked on all other ring links. In this situation, the FS command triggers protection switching as follows:
      a. The ring node where an FS command was issued blocks the traffic channel and R-APS channel on the ring port to which the command was issued, and unblocks the other ring port.
      b. The ring node where the FS command was issued transmits R-APS messages indicating FS over both ring ports. R-APS (FS) messages are continuously transmitted by this ring node while the local FS command is the ring node's highest priority command (see Table 35 on page 545). The R-APS (FS) message informs other ring nodes of the FS command and that the traffic channel is blocked on one ring port.
      c. A ring node accepting an R-APS (FS) message, without any local higher priority requests unblocks any blocked ring port. This action subsequently unblocks the traffic channel over the RPL.
      d. The ring node accepting an R-APS (FS) message, without any local higher priority requests stops transmission of R-APS messages.
      e. The ring node receiving an R-APS (FS) message flushes its FDB.
    - Protection switching on a forced switch request is completed when the above actions are performed by each ring node. At this point, traffic flows around the ring are resumed. From this point on the following rules apply regarding processing of further forced switch commands:
      - While an existing forced switch request is present in a ring, any new forced switch request is accepted, except on a ring node having a prior local forced switch request. The ring

nodes where further forced switch commands are issued block the traffic channel and R-APS channel on the ring port at which the forced switch was issued. The ring node where the forced switch command was issued transmits an R-APS message over both ring ports indicating FS. R-APS (FS) messages are continuously transmitted by this ring node while the local FS command is the ring node's highest priority command. As such, two or more forced switches are allowed in the ring, which may inadvertently cause the segmentation of an ring. It is the responsibility of the operator to prevent this effect if it is undesirable.

Ring protection requests, commands and R-APS signals have the priorities as specified in the following table.

Table 35: ERPS Request/State Priority

Request / State and Status	Type	Priority
Clear	local	highest
FS	local	|
R-APS (FS)	remote	|
local SF*	local	|
local clear SF	local	|
R-APS (SF)	remote	|
R-APS (MS)	remote	|
MS	local	|
WTR Expires	local	|
WTR Running	local	|
WTB Expires	local	|
WTB Running	local	|
R-APS (NR, RB)	remote	|
R-APS (NR)	remote	lowest

* If an Ethernet Ring Node is in the Forced Switch state, local SF is ignored.

- Recovery for forced switching under revertive and non-revertive mode is described under the Revertive parameter.

- When a ring is under an FS condition, and the node at which an FS command was issued is removed or fails, the ring remains in FS state because the FS command can only be cleared at node where the FS command was issued. This results in an unrecoverable FS condition.

  When performing a maintenance procedure (e.g., replacing, upgrading) on a ring node (or a ring link), it is recommended that FS commands be issued at the two adjacent ring nodes instead of directly issuing a FS command at the ring node under maintenance in order to avoid falling into the above mentioned unrecoverable situation.

- **Manual Switch** – Blocks specified ring port, in the absence of a failure or an FS command.
  - A ring with no request has a logical topology with the traffic channel blocked at the RPL and unblocked on all other ring links. In this situation, the Manual Switch command triggers protection switching as follows:
    a. If no other higher priority commands exist, the ring node, where a manual switch command was issued, blocks the traffic channel and R-APS channel on the ring port to which the command was issued, and unblocks the other ring port.
    b. If no other higher priority commands exist, the ring node where the manual switch command was issued transmits R-APS messages over both ring ports indicating MS. R-APS (MS) message are continuously transmitted by this ring node while the local MS command is the ring node's highest priority command (see Table 35 on page 545). The R-APS (MS) message informs other ring nodes of the MS command and that the traffic channel is blocked on one ring port.
    c. If no other higher priority commands exist and assuming the ring node was in Idle state before the manual switch command was issued, the ring node flushes its local FDB.
    d. A ring node accepting an R-APS (MS) message, without any local higher priority requests unblocks any blocked ring port which does not have an SF condition. This action subsequently unblocks the traffic channel over the RPL.
    e. A ring node accepting an R-APS (MS) message, without any local higher priority requests stops transmitting R-APS messages.
    f. A ring node receiving an R-APS (MS) message flushes its FDB.
  - Protection switching on a manual switch request is completed when the above actions are performed by each ring node. At this point, traffic flows around the ring are resumed. From this point on, the following rules apply regarding processing of further manual switch commands:
    a. While an existing manual switch request is present in the ring, any new manual switch request is rejected. The request is rejected at the ring node where the new request is issued and a notification is generated to inform the operator that the new MS request was not accepted.
    b. A ring node with a local manual switch command which receives an R-APS (MS) message with a different Node ID clears its manual switch request and starts transmitting R-APS (NR) messages. The ring node keeps the ring port blocked due to the previous manual switch command.

  c. An ring node with a local manual switch command that receives an R-APS message or a local request of higher priority than R-APS (MS) clear its manual switch request. The ring node then processes the new higher priority request.

  - Recovery for manual switching under revertive and non-revertive mode is described under the Revertive parameter.

- **Clear** – Manually clears the protection state which has been invoked by a forced switch or manual switch command, and the node is operating under non-revertive mode; or before the WTR or WTB timer expires when the node is operating in revertive mode.

  - Two steps are required to make a ring operating in non-revertive mode return to Idle state from forced switch or manual switch state:

    1. Issue a Clear command to remove the forced switch command on the node where a local forced switch command is active.

    2. Issue a Clear command on the RPL owner node to trigger the reversion.

  - The Clear command will also stop the WTR and WTB delay timers and reset their values.

  - More detailed information about using this command for non-revertive mode is included under the Revertive parameter. (See the Command Usage section under "ERPS Ring Configuration" on page 528.)

WEB INTERFACE

To block a ring port:

1. Click Administration, ERPS.

2. Select Configure Domain from the Step list.

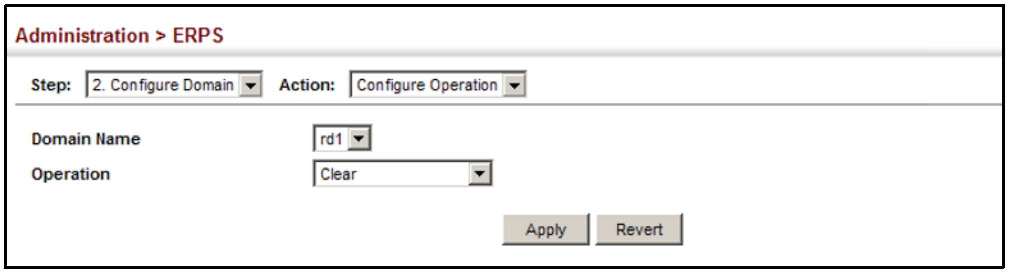
3. Select Configure Operation from the Action list.

4. Select the domain name from the drop-down list.

5. Specify a Forced Switch, Manual Switch, or Clear operation.

6. Click Apply.

Figure 298: Blocking an ERPS Ring Port



Administration > ERPS

Step: 2. Configure Domain Action: Configure Operation

Domain Name: rd1

Operation: Clear

CONNECTIVITY FAULT MANAGEMENT

Connectivity Fault Management (CFM) is an OAM protocol that includes proactive connectivity monitoring using continuity check messages, fault verification through loop back messages, and fault isolation by examining end-to-end connections between provider edge devices or between customer edge devices.

CFM is implemented as a service level protocol based on service instances which encompass only that portion of the metropolitan area network supporting a specific customer. CFM can also provide controlled management access to a hierarchy of maintenance domains (such as the customer, service provider, and equipment operator).

This switch supports functions for defining the CFM structure, including domains, maintenance associations, and maintenance access points. It also supports fault detection through continuity check messages for all known maintenance points, and cross-check messages which are used to verify a static list of remote maintenance points located on other devices (in the same maintenance association) against those found through continuity check messages. Fault verification is supported using loop back messages, and fault isolation with link trace messages. Fault notification is also provided by SNMP alarms which are automatically generated by maintenance points when connectivity faults or configuration errors are detected in the local maintenance domain.

Key Components of CFM

CFM provides restricted management access to each Service Instance using a structured conceptual network based on these components:

- A Maintenance Domain defines a part of the network controlled by a single operator, and supports management access to the domain through Domain Service Access Points (DSAPs) configured on the domain boundary, as well as connectivity testing between these DSAPs.

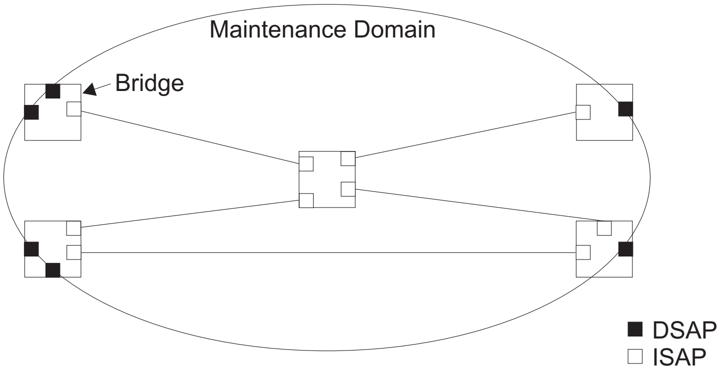
- A Maintenance Association (MA) contains the DSAPs for an individual Service Instance. DSAPs are the primary maintenance points used to monitor connectivity across a maintenance domain, and are the entry points to the paths which interconnect the access points allocated to a service instance.

- A Maintenance Level allows maintenance domains to be nested in a hierarchical fashion, providing access to the specific network portions required by each operator. Domains at lower levels may be either hidden or exposed to operators managing domains at a higher level, allowing either course or fine fault resolution.

- Maintenance End Points (MEPs) which provide full CFM access to a Service Instance (i.e., a specific MA), and Maintenance Intermediate Points (MIPs) which are passive entities that merely validate received CFM messages, or respond to link trace and loop back requests. MIPs are the interconnection points that make up all possible paths between the DSAPs within an MA, and may also include interconnection points in lower-level domains if exposed by CFM settings.

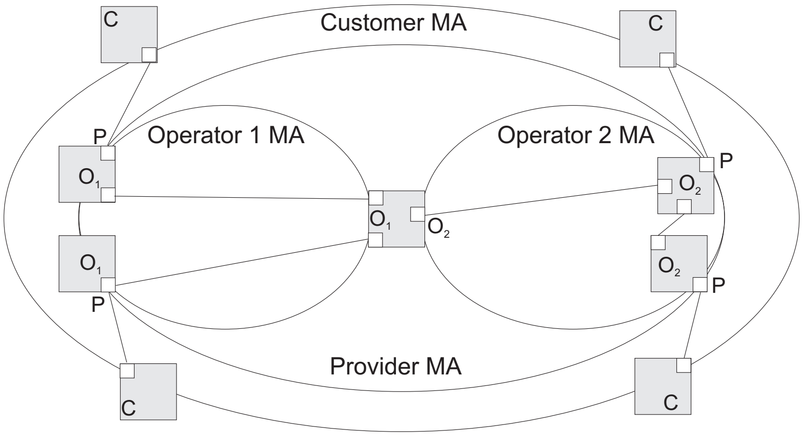
The following figure shows a single Maintenance Domain, with DSAPs located on the domain boundary, and Internal Service Access Points (ISAPs) inside the domain through which frames may pass between the DSAPs.

Figure 299: Single CFM Maintenance Domain



The figure below shows four maintenance associations contained within a hierarchical structure of maintenance domains. At the innermost level, there are two operator domains which include access points marked “O_1” and “O_2” respectively. The users of these domains can see their respective MEPs as well as all the MIPs within their domains. There is a service provider domain at the second level in the hierarchy. From the service provider’s view, the access points marked “P” are visible, and all access points within the operator domains have also been made visible as MIPs according to common practice. And finally, there is a customer domain at the top of the hierarchy. Users at this level can only see the access points marked “C” on the outer domain boundary. Again, normal practice is to hide the internal structure of the network from outsiders to reduce security risks.

Figure 300: Multiple CFM Maintenance Domains



Note that the Service Instances within each domain shown above are based on a unique maintenance association for the specific users, distinguished by the domain name, maintenance level, maintenance association’s name, and assigned VLAN.

Basic CFM Operations

CFM uses standard Ethernet frames for sending protocol messages. Both the source and destination address for these messages are based on unicast or multicast MAC addresses, and therefore confined to a single Layer 2 CFM service VLAN. For this reason, the transmission, forwarding, and processing of CFM frames is performed by bridges, not routers. Bridges that do not recognize CFM messages forward them as normal data. There are three basic types of CFM messages, including continuity check, link trace, and loop back.

Continuity check messages (CCMs) are multicast within a single Service Instance (i.e., a specific MA), allowing MEPs to discover other MEPs within the same MA, and MIPs to discover MEPs. Connectivity faults are indicated when a known MEP stops sending CCMs, or a remote MEP configured in a static list does not come up. Configuration errors, such as a cross-connect between different MAs, are indicated when a CCM is received with an incorrect MA identifier or maintenance level.

Loop back messages are used for fault verification. These messages can be sent using the MAC address of any destination MEP within the same MA. If the target MEP’s identifier has been discovered through CCM messages, then a loop back message can also be sent using the MEPs identifier. A reply indicates that the destination is reachable.

Link trace messages are used for fault verification. These messages are multicast frames sent out to track the hop-by-hop path to a target MEP within the same MA. Responses provide information on the ingress, egress, and relay action taken at each hop along the path, providing vital information about connectivity problems. Responses allow the sender to discover all of the maintenance points that would be traversed by a data frame sent to the target MAC address.

SNMP traps can also be configured to provide an automated method of fault notification. If the fault notification generator detects one or more defects within the configured time period, and fault alarms are enabled, a corresponding trap will be sent. No further fault alarms are sent until the fault notification generator has been reset by the passage of a configured time period without detecting any further faults. Upon receiving a fault alarm, you should inspect the related SNMP objects for the reporting MEP, diagnose the fault, correct it, and re-examine the MEP's SNMP objects to see whether the fault notification generator has been reset.

Configuration Guidelines

1. Configure the maintenance domains with the MD List (see "Configuring CFM Maintenance Domains").

2. Configure the maintenance associations with MA List (see "Configuring CFM Maintenance Associations").

3. Configure the local maintenance end points (MEPs) which will serve as the domain service access points for the specified maintenance association using the MEP List (see "Configuring CFM Maintenance Associations").

4. Enter a static list of MEPs assigned to other devices within the same maintenance association using the Remote MEP List (see "Configuring Remote Maintenance End Points"). This allows CFM to automatically verify the functionality of these remote end points by cross-checking the static list configured on this device against information learned through continuity check messages.

5. Enable CFM globally on the switch using the Configure Global screen (see "Configuring Global Settings for CFM").

6. Enable CFM on the local MEPs using the Configure Interface screen (see "Configuring Interfaces for CFM").

7. Enable continuity check and cross-check operations, and configure AIS parameters using the Configure MA – Configure Details screen (see "Configuring CFM Maintenance Associations").

Other configuration changes may be required for your particular environment, such as adjusting the interval at which continuity check messages are sent (see "Configuring CFM Maintenance Associations"), or setting the start-up delay for the cross-check operation (see "Configuring Global Settings for CFM"). You can also enable SNMP traps for events discovered by continuity check messages or cross-check messages (see "Configuring Global Settings for CFM").

CONFIGURING GLOBAL SETTINGS FOR CFM

Use the Administration > CFM (Configure Global) page to configure global settings for CFM, such as enabling the CFM process on the switch, setting the start-up delay for cross-check operations, configuring parameters for the link trace cache, and enabling traps for events discovered by continuity check messages or cross-check messages.

CLI REFERENCES

- "CFM Commands" on page 1561

PARAMETERS

These parameters are displayed:

Global Configuration

- **CFM Status** – Enables CFM processing globally on the switch. (Default: Enabled)

  To avoid generating an excessive number of traps, the complete CFM maintenance structure and process parameters should be configured prior to enabling CFM processing globally on the switch. Specifically, the maintenance domains, maintenance associations, and maintenance end-points (MEPs) should be configured on each participating bridge using the Configure MD page (see "Configuring CFM Maintenance Domains"), Configure MA page (see "Configuring CFM Maintenance Associations"), and the Configure MEP page (see "Configuring Maintenance End Points").

  When CFM is enabled, hardware resources are allocated for CFM processing.

- **MEP Cross Check Start Delay** – Sets the maximum delay that a device waits for remote MEPs to come up before starting the cross-check operation. (Range: 1-65535 seconds; Default: 10 seconds)

  This parameter sets the time to wait for a remote MEP to come up, and the switch starts cross-checking the list of statically configured remote MEPs in the local maintenance domain (Configure Remote MEP page, see "Configuring Remote Maintenance End Points") against the MEPs learned through continuity check messages (CCMs).

  The cross-check start delay should be configured to a value greater than or equal to the continuity check message interval to avoid generating unnecessary traps (see "Configuring CFM Maintenance Associations").

LInk Trace Cache Settings

- **Link Trace Cache** – Enables caching of CFM data learned through link trace messages. (Default: Enabled)

  A linktrace message is a multicast CFM frame initiated by a MEP, and forwarded from MIP to MIP, with each MIP generating a linktrace reply, up to the point at which the linktrace message reaches its destination or can no longer be forwarded.

  Use this command attribute to enable the link trace cache to store the results of link trace operations initiated on this device. Use the CFM Transmit Link Trace page (see "Transmitting Link Trace Messages") to transmit a linktrace message.

  Linktrace responses are returned from each MIP along the path and from the target MEP. Information stored in the cache includes the maintenance domain name, MA name, MEPID, sequence number, and TTL value (see "Displaying Fault Notification Settings").

- **Link Trace Cache Hold Time** – The hold time for CFM link trace cache entries. (Range: 1-65535 minutes; Default: 100 minutes)

  Before setting the aging time for cache entries, the cache must first be enabled in the Linktrace Cache attribute field.

- **Link Trace Cache Size** – The maximum size for the link trace cache. (Range: 1-4095 entries; Default: 100 entries)

  If the cache reaches the maximum number of specified entries, or the size is set to a value less than the current number of stored entries, no new entries are added. To add additional entries, the cache size must first be increased, or purged (see "Displaying Fault Notification Settings").

Continuity Check Errors

- **Connectivity Check Config** – Sends a trap if this device receives a continuity check message (CCM) with the same maintenance end point identifier (MPID) as its own but with a different source MAC address, indicating that a CFM configuration error exists.

- **Connectivity Check Loop** – Sends a trap if this device receives a CCM with the same source MAC address and MPID as its own, indicating that a forwarding loop exists.

- **Connectivity Check MEP Down** – Sends a trap if this device loses connectivity with a remote maintenance end point (MEP), or connectivity has been restored to a remote MEP which has recovered from an error condition.

- **Connectivity Check MEP Up** – Sends a trap if a remote MEP is discovered and added to the local database, the port state of a previously discovered remote MEP changes, or a CCM is received from a remote MEP which as an expired entry in the archived database.

  MEP Up traps are suppressed when cross-checking of MEPs is enabled[9] because cross-check traps include more detailed status information.

Cross-check Errors

- **Cross Check MA Up** – Sends a trap when all remote MEPs in an MA come up.

  An MA Up trap is sent if cross-checking is enabled[9], and a CCM is received from all remote MEPs configured in the static list for this maintenance association[10].

- **Cross Check MEP Missing** – Sends a trap if the cross-check timer expires and no CCMs have been received from a remote MEP configured in the static list.

  A MEP Missing trap is sent if cross-checking is enabled[9], and no CCM is received for a remote MEP configured in the static list[10].

[9] Cross-checking must be enabled for this type of trap to be reported (see "Configuring CFM Maintenance Associations").
[10] See "Configuring Maintenance End Points".

- **Cross Check MEP Unknown** – Sends a trap if an unconfigured MEP comes up.

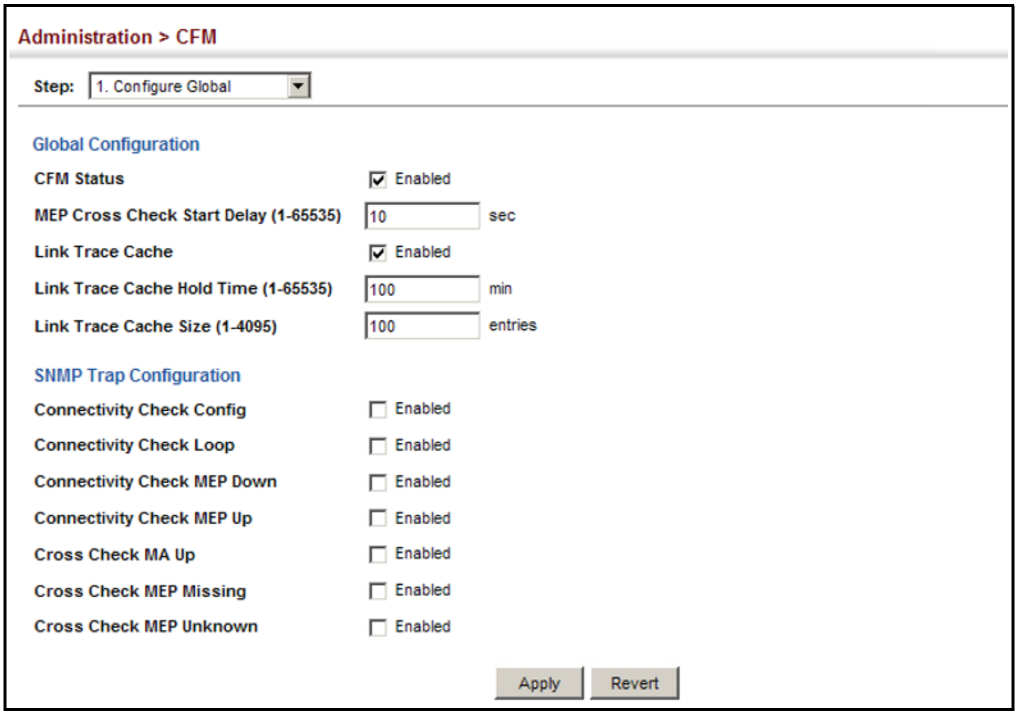
  A MEP Unknown trap is sent if cross-checking is enabled[9], and a CCM is received from a remote MEP that is not configured in the static list[10].

WEB INTERFACE

To configure global settings for CFM:

1. Click Administration, CFM.
2. Select Configure Global from the Step list.
3. Before enabling CFM processing on the switch, first configure the required CFM domains, maintenance associations, and static MEPs. Then set the delay time to wait for a remote MEP comes up before the switch starts cross-checking the end points learned through CCMs against those stored in the static list.
4. Adjust the parameters for the link trace cache as required.
5. Enable the required traps for continuity check and cross-check errors. Remember that the "Connectivity Check" and "Cross Check" fields on the MA Configuration page must be enabled before related errors can be generated.
6. Click Apply.

Figure 301: Configuring Global Settings for CFM



Administration > CFM

Step: 1. Configure Global

Global Configuration

CFM Status	☑ Enabled
MEP Cross Check Start Delay (1-65535)	10 sec
Link Trace Cache	☑ Enabled
Link Trace Cache Hold Time (1-65535)	100 min
Link Trace Cache Size (1-4095)	100 entries

SNMP Trap Configuration

Connectivity Check Config	□ Enabled
Connectivity Check Loop	□ Enabled
Connectivity Check MEP Down	□ Enabled
Connectivity Check MEP Up	□ Enabled
Cross Check MA Up	□ Enabled
Cross Check MEP Missing	□ Enabled
Cross Check MEP Unknown	□ Enabled

CONFIGURING INTERFACES FOR CFM

CFM processes are enabled by default for all physical interfaces, both ports and trunks. You can use the Administration > CFM (Configure Interface) page to change these settings.

CLI REFERENCES

- "ethernet cfm port-enable" on page 1572

COMMAND USAGE

- An interface must be enabled before a MEP can be created (see "Configuring Maintenance End Points").

- If a MEP has been configured on an interface, it must first be deleted before CFM can be disabled on that interface.

- When CFM is disabled, hardware resources previously used for CFM processing on that interface are released, and all CFM frames entering that interface are forwarded as normal data traffic.

WEB INTERFACE

To enable CFM on an interface:

1. Click Administration, CFM.

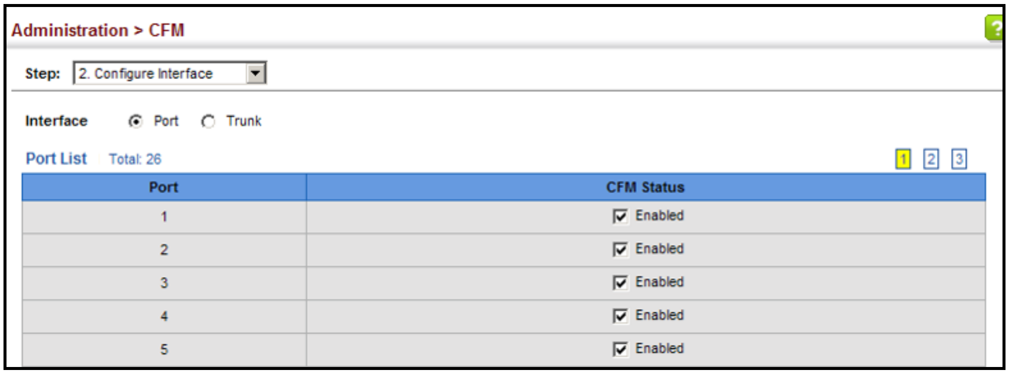
2. Select Configure Interface from the Step list.

3. Select Port or Trunk.

4. Enable CFM on the required interface.

5. Click Apply.

Figure 302: Configuring Interfaces for CFM



Step: 2. Configure Interface

Interface ● Port ○ Trunk

Port List Total: 26

Port	CFM Status
1	☑ Enabled
2	☑ Enabled
3	☑ Enabled
4	☑ Enabled
5	☑ Enabled

CONFIGURING CFM MAINTENANCE DOMAINS

Use the Administration > CFM (Configure MD) pages to create and configure a Maintenance Domain (MD) which defines a portion of the network for which connectivity faults can be managed. Domain access points are set up on the boundary of a domain to provide end-to-end connectivity fault detection, analysis, and recovery. Domains can be configured in a hierarchy to provide management access to the same basic network resources for different user levels.

CLI REFERENCES

- "CFM Commands" on page 1561

COMMAND USAGE

Configuring General Settings

- Where domains are nested, an upper-level hierarchical domain must have a higher maintenance level than the ones it encompasses. The higher to lower level domain types commonly include entities such as customer, service provider, and operator.

- More than one domain can be configured at the same maintenance level, but a single domain can only be configured with one maintenance level.

- If MEPs (see "Configuring Maintenance End Points") or MAs (see "Configuring CFM Maintenance Associations") are configured for a domain, they must first be removed before you can remove the domain.

  Maintenance domains are designed to provide a transparent method of verifying and resolving connectivity problems for end-to-end connections. By default, these connections run between the domain service access points (DSAPs) within each MA defined for a domain, and are manually configured (see "Configuring Maintenance End Points").

  In contrast, MIPs are interconnection points that make up all possible paths between the DSAPs within an MA. MIPs are automatically generated by the CFM protocol when the MIP Creation Type is set to “Default” or “Explicit,” and the MIP creation state machine is invoked (as defined in IEEE 802.1ag). The default option allows MIPs to be created for all interconnection points within an MA, regardless of the domain’s level in the maintenance hierarchy (e.g., customer, provider, or operator). While the explicit option only generates MIPs within an MA if its associated domain is not at the bottom of the maintenance hierarchy. This option is used to hide the structure of network at the lowest domain level.

  The diagnostic functions provided by CFM can be used to detect connectivity failures between any pair of MEPs in an MA. Using MIPs allows these failures to be isolated to smaller segments of the network.

  Allowing the CFM to generate MIPs exposes more of the network structure to users at higher domain levels, but can speed up the process of fault detection and recovery. This trade-off should be carefully considered when designing a CFM maintenance structure.

  Also note that while MEPs are active agents which can initiate consistency check messages (CCMs), transmit loop back or link trace messages, and maintain the local CCM database, MIPs, on the other hand, are passive agents which can only validate received CFM messages, and respond to loop back and link trace messages.

The MIP creation method defined for an MA (see "Configuring CFM Maintenance Associations") takes precedence over the method defined on the CFM Domain List.

Configuring Fault Notification

- A fault alarm can generate an SNMP notification. It is issued when the MEP fault notification generator state machine detects that the configured time period (MEP Fault Notify Alarm Time) has passed with one or more defects indicated, and fault alarms are enabled at or above the specified priority level (MEP Fault Notify Lowest Priority). The state machine transmits no further fault alarms until it is reset by the passage of a configured time period (MEP Fault Notify Reset Time) without a defect indication. The normal procedure upon receiving a fault alarm is to inspect the reporting MEP's managed objects using an appropriate SNMP software tool, diagnose the fault, correct it, re-examine the MEP's managed objects to see whether the MEP fault notification generator state machine has been reset, and repeat those steps until the fault is resolved.
- Only the highest priority defect currently detected is reported in the fault alarm.

Priority levels include the following options:

Table 36: Remote MEP Priority Levels

Priority Level	Level Name	Description
1	allDef	All defects.
2	macRemErrXcon	DefMACstatus, DefRemoteCCM, DefErrorCCM, or DefXconCCM.
3	remErrXcon	DefErrorCCM, DefXconCCM or DefRemoteCCM.
4	errXcon	DefErrorCCM or DefXconCCM.
5	xcon	DefXconCCM
6	noXcon	No defects DefXconCCM or lower are to be reported.

Table 37: MEP Defect Descriptions

Defect	Description
DefMACstatus	Either some remote MEP is reporting its Interface Status TLV as not isUp, or all remote MEPs are reporting a Port Status TLV that contains some value other than psUp.
DefRemoteCCM	The MEP is not receiving valid CCMs from at least one of the remote MEPs.
DefErrorCCM	The MEP has received at least one invalid CCM whose CCM Interval has not yet timed out.
DefXconCCM	The MEP has received at least one CCM from either another MAID or a lower MD Level whose CCM Interval has not yet timed out.

PARAMETERS

These parameters are displayed:

Creating a Maintenance Domain

- **MD Index** – Domain index. (Range: 1-65535)
- **MD Name** – Maintenance domain name. (Range: 1-43 alphanumeric characters)
- **MD Level** – Authorized maintenance level for this domain. (Range: 0-7)
- **MIP Creation Type** – Specifies the CFM protocol's creation method for maintenance intermediate points (MIPs) in this domain:
  - **Default** – MIPs can be created for any maintenance association (MA) configured in this domain on any bridge port through which the MA's VID can pass.
  - **Explicit** – MIPs can be created for any MA configured in this domain only on bridge ports through which the MA's VID can pass, and only if a maintenance end point (MEP) is created at some lower MA Level.
  - **None** – No MIP can be created for any MA configured in this domain.

Configuring Detailed Settings for a Maintenance Domain

- **MD Index** – Domain index. (Range: 1-65535)
- **MEP Archive Hold Time** – The time that data from a missing MEP is retained in the continuity check message (CCM) database before being purged. (Range: 1-65535 minutes; Default: 100 minutes)

  A change to the hold time only applies to entries stored in the database after this attribute is changed.
- **MEP Fault Notify Lowest Priority** – The lowest priority defect that is allowed to generate a fault alarm. (Range: 1-6, Default: 2)
- **MEP Fault Notify Alarm Time** – The time that one or more defects must be present before a fault alarm is issued. (Range: 3-10 seconds; Default: 3 seconds)
- **MEP Fault Notify Reset Time** – The time after a fault alarm has been issued, and no defect exists, before another fault alarm can be issued. (Range: 3-10 seconds; Default: 10 seconds)

WEB INTERFACE

To create a maintenance domain:

1. Click Administration, CFM.
2. Select Configure MD from the Step list.

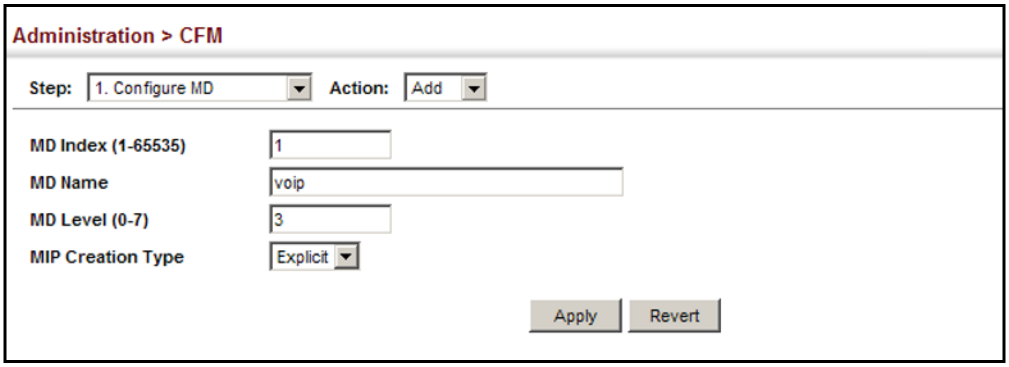
3. Select Add from the Action list.

4. Specify the maintenance domains and authorized maintenance levels (thereby setting the hierarchical relationship with other domains).

5. Specify the manner in which MIPs can be created within each domain.

6. Click Apply.

Figure 303: Configuring Maintenance Domains



Administration > CFM

Step: 1. Configure MD Action: Add

MD Index (1-65535)	1
MD Name	voip
MD Level (0-7)	3
MIP Creation Type	Explicit

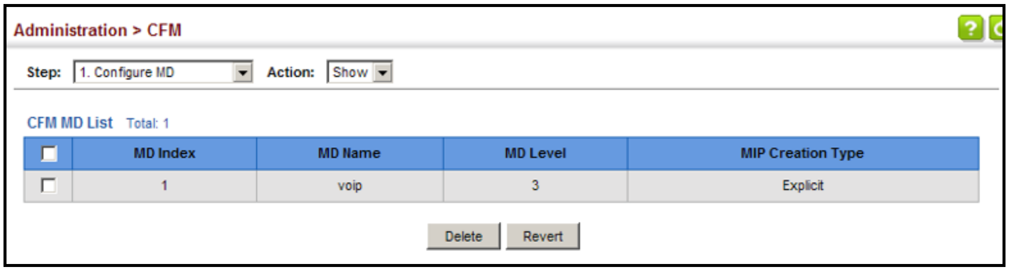
To show the configured maintenance domains:

1. Click Administration, CFM.

2. Select Configure MD from the Step list.

3. Select Show from the Action list.

Figure 304: Showing Maintenance Domains



Administration > CFM

Step: 1. Configure MD Action: Show

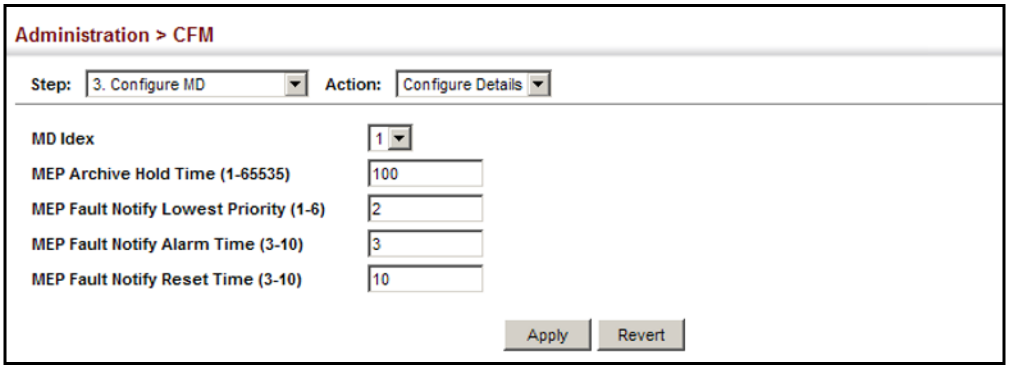
CFM MD List Total: 1

□	MD Index	MD Name	MD Level	MIP Creation Type
□	1	voip	3	Explicit

To configure detailed settings for maintenance domains:

1. Click Administration, CFM.
2. Select Configure MD from the Step list.
3. Select Configure Details from the Action list.
4. Select an entry from the MD Index.
5. Specify the MEP archive hold and MEP fault notification parameters.
6. Click Apply

Figure 305: Configuring Detailed Settings for Maintenance Domains



Administration > CFM

Step: 3. Configure MD Action: Configure Details

MD Idex: 1

MEP Archive Hold Time (1-65535): 100

MEP Fault Notify Lowest Priority (1-6): 2

MEP Fault Notify Alarm Time (3-10): 3

MEP Fault Notify Reset Time (3-10): 10

CONFIGURING CFM MAINTENANCE ASSOCIATIONS

Use the Administration > CFM (Configure MA) pages to create and configure the Maintenance Associations (MA) which define a unique CFM service instance. Each MA can be identified by its parent MD, the MD's maintenance level, the VLAN assigned to the MA, and the set of maintenance end points (MEPs) assigned to it.

CLI REFERENCES

- "CFM Commands" on page 1561

COMMAND USAGE

Creating a Maintenance Association

- Use the Configure MA – Add screen to create an MA within the selected MD, map it to a customer service instance (S-VLAN), and set the manner in which MIPs are created for this service instance. Then use the MEP List to assign domain service access points (DSAPs) to this service instance (see "Configuring Maintenance End Points" on page 565).

- An MA must be defined before any associated DSAPs or remote MEPs can be assigned (see "Configuring Remote Maintenance End Points" on page 567).

- Multiple domains at the same maintenance level cannot have an MA on the same VLAN (see "Configuring CFM Maintenance Domains" on page 555).
- Before removing an MA, first remove the MEPs assigned to it (see "Configuring Maintenance End Points" on page 565).
- For a detailed description of the MIP types, refer to the Command Usage section under "Configuring CFM Maintenance Domains" on page 555.

Configuring Detailed Settings for a Maintenance Association

- CCMs are multicast periodically by a MEP in order to discover other MEPs in the same MA, and to assure connectivity to all other MEPs/MIPs in the MA.
- Each CCM received is checked to verify that the MEP identifier field sent in the message does not match its own MEP ID, which would indicate a duplicate MEP or network loop. If these error types are not found, the CCM is stored in the MEP's local database until aged out.
- If a maintenance point fails to receive three consecutive CCMs from any other MEP in the same MA, a connectivity failure is registered.
- If a maintenance point receives a CCM with an invalid MEPID or MA level or an MA level lower than its own, a failure is registered which indicates a configuration error or cross-connect error (i.e., overlapping MAs).
- The interval at which CCMs are issued should be configured to detect connectivity problems in a timely manner, as dictated by the nature and size of the MA.
- The maintenance of a MIP CCM database by a MIP presents some difficulty for bridges carrying a large number of Service Instances, and for whose MEPs are issuing CCMs at a high frequency. For this reason, slower CCM transmission rates may have to be used.

PARAMETERS

These parameters are displayed:

Creating a Maintenance Association

- **MD Index** – Domain index. (Range: 1-65535)
- **MA Index** – MA identifier. (Range: 1-2147483647)
- **MA Name** – MA name. (Range: 1-43 alphanumeric characters)

  Each MA name must be unique within the CFM domain.
- **Primary VLAN** – Service VLAN ID. (Range: 1-4094)

  This is the VLAN through which all CFM functions are executed for this MA.

- **MIP Creation Type** – Specifies the CFM protocol's creation method for maintenance intermediate points (MIPs) in this MA:
  - **Default** – MIPs can be created for this MA on any bridge port through which the MA's VID can pass.
  - **Explicit** – MIPs can be created for this MA only on bridge ports through which the MA's VID can pass, and only if a maintenance end point (MEP) is created at some lower MA Level.
  - **None** – No MIP can be created for this MA.

Configuring Detailed Settings for a Maintenance Association

- **MD Index** – Domain index. (Range: 1-65535)
- **MA Index** – MA identifier. (Range: 1-2147483647)
- **MA Name Format** – Specifies the name format for the maintenance association as IEEE 802.1ag character based, or ITU-T SG13/SG15 Y.1731 defined ICC-based format.
  - **Character String** – IEEE 802.1ag defined character string format. This is an IETF RFC 2579 DisplayString.
  - **ICC Based** – ITU-T SG13/SG15 Y.1731 defined ICC based format.
- **Interval Level** – The delay between sending CCMs. The setting for this parameter is expressed as levels 4 through 7, which in turn map to specific intervals of time. (Options: 4 - 1 second, 5 - 10 seconds, 6 - 1 minute, 7 - 10 minutes)
- **Connectivity Check** – Enables transmission of CCMs. (Default: Disabled)
- **Cross Check** – Enables cross-checking between a static list of MEPs assigned to other devices within the same maintenance association and the MEPs learned through CCMs.

  Before starting the cross-check process, first configure the remote MEPs that exist on other devices inside the maintenance association using the Remote MEP List (see "Configuring Remote Maintenance End Points"). These remote MEPs are used in the cross-check operation to verify that all endpoints in the specified MA are operational.

  The cross-check start delay, which sets the maximum delay this device waits for a remote MEP to come up before starting the cross-check operation, is a domain-level parameter. To set this parameter, use the CFM MD Configuration screen (see "Configuring CFM Maintenance Domains").
- **AIS Status** – Enables/disables suppression of the Alarm Indication Signal (AIS). (Default: Disabled)
- **AIS Period** – Configures the period at which AIS is sent in an MA. (Range: 1 or 60 seconds; Default: 1 second)

- **AIS Transmit Level** – Configure the AIS maintenance level in an MA. (Range: 0-7; Default is 0)

  AIS Level must follow this rule: AIS Level >= Domain Level

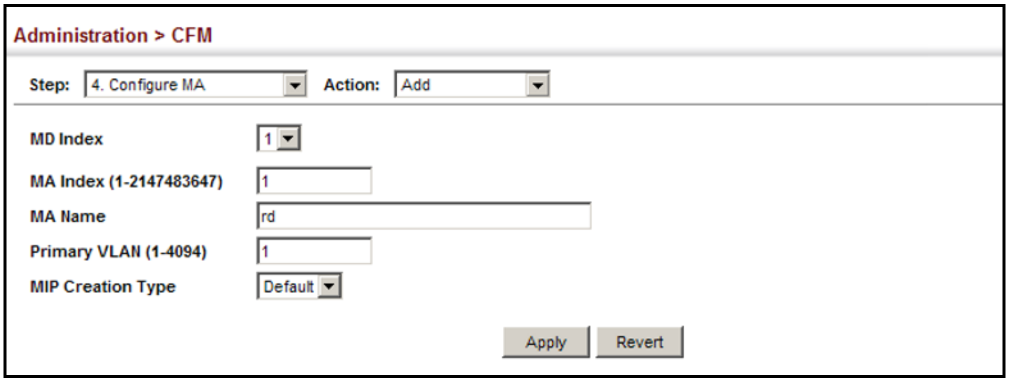
- **AIS Suppress Alarm** – Enables/disables suppression of the AIS. (Default: Disabled)

WEB INTERFACE

To create a maintenance association:

1. Click Administration, CFM.
2. Select Configure MA from the Step list.
3. Select Add from the Action list.
4. Select an entry from the MD Index list.
5. Specify the MAs assigned to each domain, the VLAN through which CFM messages are passed, and the manner in which MIPs can be created within each MA.
6. Click Apply.

Figure 306: Creating Maintenance Associations



Administration > CFM

Step: 4. Configure MA Action: Add

MD Index	1
MA Index (1-2147483647)	1
MA Name	rd
Primary VLAN (1-4094)	1
MIP Creation Type	Default

To show the configured maintenance associations:

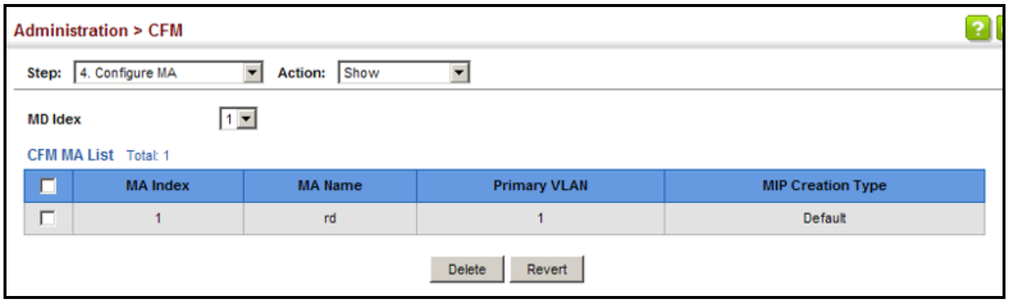
1. Click Administration, CFM.

2. Select Configure MA from the Step list.

3. Select Show from the Action list.

4. Select an entry from the MD Index list.

Figure 307: Showing Maintenance Associations



Administration > CFM

Step: 4. Configure MA   Action: Show

MD Idex: 1

CFM MA List Total: 1

□	MA Index	MA Name	Primary VLAN	MIP Creation Type
□	1	rd	1	Default

To configure detailed settings for maintenance associations:

1. Click Administration, CFM.

2. Select Configure MA from the Step list.

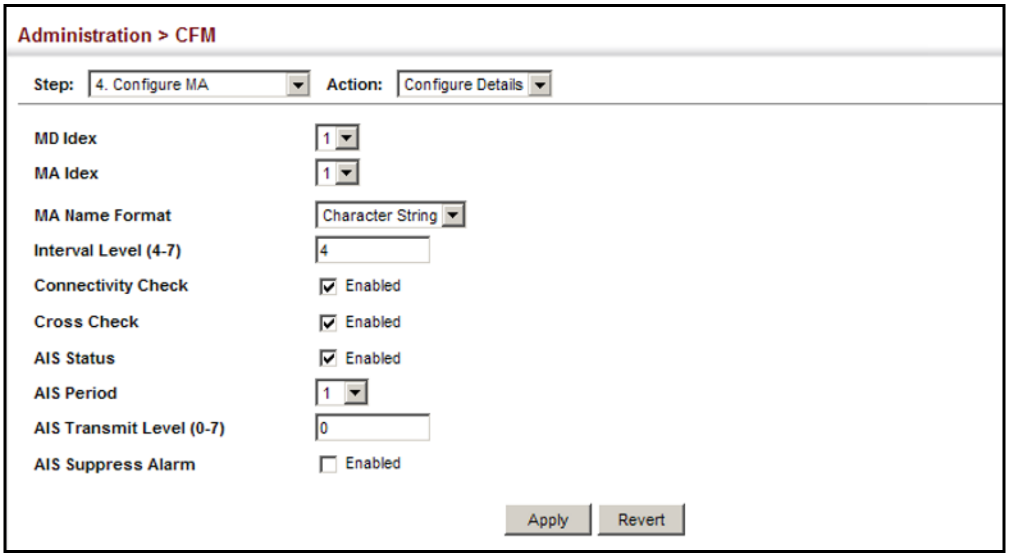
3. Select Configure Details from the Action list.

4. Select an entry from MD Index and MA Index.

5. Specify the CCM interval, enable the transmission of connectivity check and cross check messages, and configure the required AIS parameters.

6. Click Apply

Figure 308: Configuring Detailed Settings for Maintenance Associations



Administration > CFM

Step: 4. Configure MA
Action: Configure Details

MD Idex: 1
MA Idex: 1
MA Name Format: Character String
Interval Level (4-7): 4
Connectivity Check: ☑ Enabled
Cross Check: ☑ Enabled
AIS Status: ☑ Enabled
AIS Period: 1
AIS Transmit Level (0-7): 0
AIS Suppress Alarm: ☐ Enabled

CONFIGURING MAINTENANCE END POINTS

Use the Administration > CFM (Configure MEP – Add) page to configure Maintenance End Points (MEPs). MEPs, also called Domain Service Access Points (DSAPs), must be configured at the domain boundary to provide management access for each maintenance association.

CLI REFERENCES

- "CFM Commands" on page 1561

COMMAND USAGE

- CFM elements must be configured in the following order: (1) maintenance domain at the same level as the MEP to be configured (see "Configuring CFM Maintenance Domains"), (2) maintenance association within the domain (see "Configuring CFM Maintenance Associations"), and (3) finally the MEPs using the MEP List.

- An interface may belong to more than one domain, or to different MAs in different domains.

- To change the MEP's MA or the direction it faces, first delete the MEP, and then create a new one.

PARAMETERS

These parameters are displayed:

- **MD Index** – Domain index. (Range: 1-65535)

- **MA Index** – MA identifier. (Range: 1-2147483647)

- **MEP ID** – Maintenance end point identifier. (Range: 1-8191)

- **MEP Direction** – Up indicates that the MEP faces inward toward the switch cross-connect matrix, and transmits CFM messages towards, and receives them from, the direction of the internal bridge relay mechanism. If the **Up** option is not selected, then the MEP is facing away from the switch, and transmits CFM messages towards, and receives them from, the direction of the physical medium.

- **Interface** – Indicates a port or trunk.

WEB INTERFACE

To configure a maintenance end point:

1. Click Administration, CFM.

2. Select Configure MEP from the Step list.

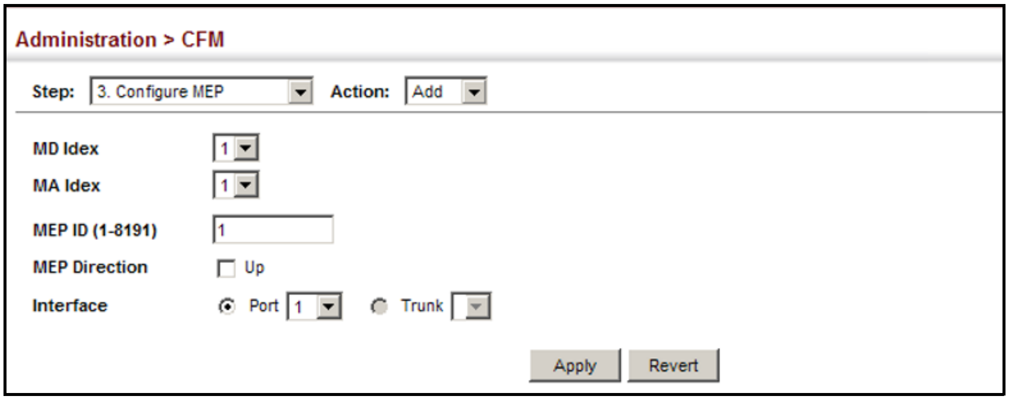
3. Select Add from the Action list.

4. Select an entry from MD Index and MA Index.

5. Specify the MEPs assigned to each MA, set the MEP identifier, the direction in which the MEP faces, and the physical interface serving as the DSAP.

6. Click Apply.

Figure 309: Configuring Maintenance End Points



Administration > CFM

Step: 3. Configure MEP Action: Add

MD Idex: 1

MA Idex: 1

MEP ID (1-8191): 1

MEP Direction: □ Up

Interface: ● Port 1 ○ Trunk

To show the configured maintenance end points:

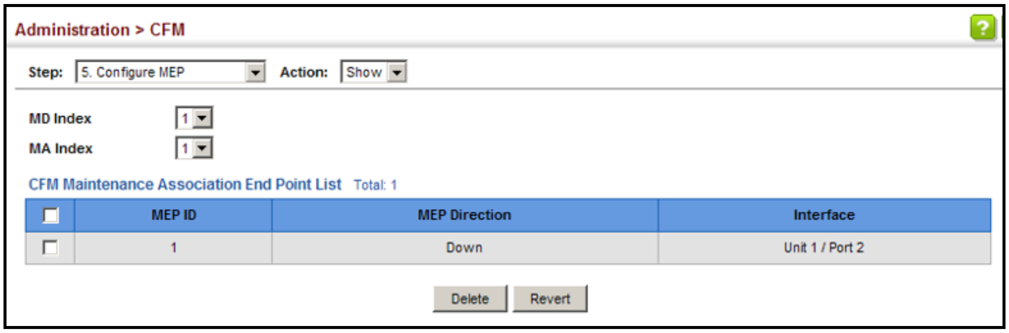
1. Click Administration, CFM.

2. Select Configure MEP from the Step list.

3. Select Show from the Action list.

4. Select an entry from MD Index and MA Index.

Figure 310: Showing Maintenance End Points



Administration > CFM

Step: 5. Configure MEP   Action: Show

MD Index: 1

MA Index: 1

CFM Maintenance Association End Point List Total: 1

☐	MEP ID	MEP Direction	Interface
☐	1	Down	Unit 1 / Port 2

Configuring Remote Maintenance End Points

Use the Administration > CFM (Configure Remote MEP – Add) page to specify remote maintenance end points (MEPs) set on other CFM-enabled devices within a common MA. Remote MEPs can be added to a static list in this manner to verify that each entry has been properly configured and is operational. When cross-checking is enabled, the list of statically configured remote MEPs is compared against the MEPs learned through continuity check messages (CCMs), and any discrepancies reported via SNMP traps.

CLI References

- "CFM Commands" on page 1561

Command Usage

- All MEPs that exist on other devices inside a maintenance association should be statically configured to ensure full connectivity through the cross-check process.

- Remote MEPs can only be configured if local domain service access points (DSAPs) have already been created (see "Configuring Maintenance End Points") at the same maintenance level and in the same MA. DSAPs are MEPs that exist on the edge of the domain, and act as primary service access points for end-to-end cross-check, loop-back, and link-trace functions.

- The MEP cross-check start delay which sets the maximum delay that a device waits for remote MEPs to come up before starting the cross-check operation can be configured on the Configure Global page (see "Configuring Global Settings for CFM").

- SNMP traps for continuity check events discovered by cross-check operations can also be configured on the Configure Global page (see "Configuring Global Settings for CFM").

Parameters

These parameters are displayed:

- **MD Index** – Domain index. (Range: 1-65535)

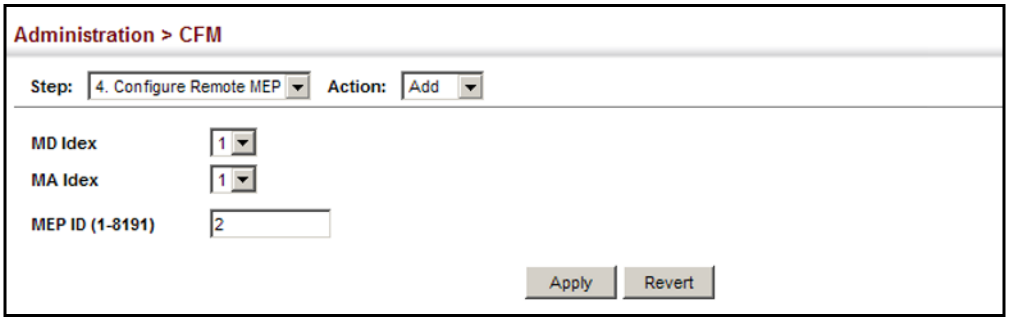
- **MA Index** – MA identifier. (Range: 1-2147483647)
- **MEP ID** – Identifier for a maintenance end point which exists on another CFM-enabled device within the same MA. (Range: 1-8191)

WEB INTERFACE

To configure a remote maintenance end point:

1. Click Administration, CFM.
2. Select Configure Remote MEP from the Step list.
3. Select Add from the Action list.
4. Select an entry from MD Index and MA Index.
5. Specify the remote MEPs which exist on other devices within the same MA.
6. Click Apply.

Figure 311: Configuring Remote Maintenance End Points


Administration > CFM

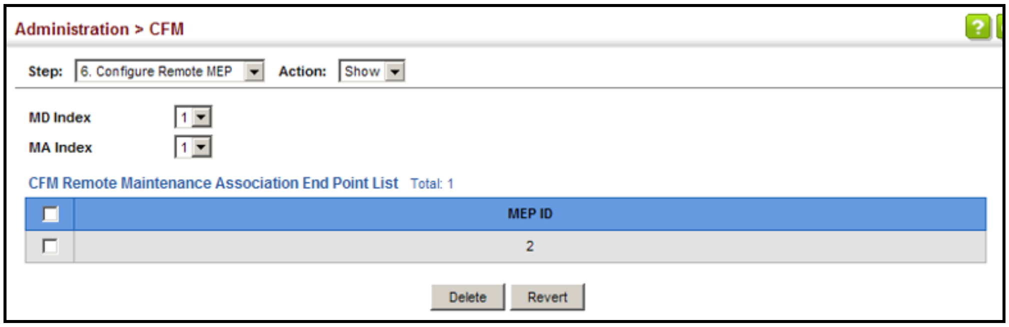
Step: 4. Configure Remote MEP Action: Add

MD Idex 1
MA Idex 1
MEP ID (1-8191) 2

To show the configured remote maintenance end points:

1. Click Administration, CFM.
2. Select Configure MEP from the Step list.
3. Select Show from the Action list.
4. Select an entry from MD Index and MA Index.

Figure 312: Showing Remote Maintenance End Points



Administration > CFM

Step: 6. Configure Remote MEP Action: Show

MD Index 1

MA Index 1

CFM Remote Maintenance Association End Point List Total: 1

□	MEP ID
□	2

Transmitting Link Trace Messages

Use the Administration > CFM (Transmit Link Trace) page to transmit link trace messages (LTMs). These messages can isolate connectivity faults by tracing the path through a network to the designated target node (i.e., a remote maintenance end point).

CLI References

- "CFM Commands" on page 1561

Command Usage

- LTMs can be targeted to MEPs, not MIPs. Before sending a link trace message, be sure you have configured the target MEP for the specified MA (see "Configuring Remote Maintenance End Points").

- If MAC address of target MEP has not been learned by any local MEP, then the linktrace may fail. Use the Show Remote MEP page (see "Displaying Remote MEPs") to verify that a MAC address has been learned for the target MEP.

- LTMs are sent as multicast CFM frames, and forwarded from MIP to MIP, with each MIP generating a link trace reply, up to the point at which the LTM reaches its destination or can no longer be forwarded.

- LTMs are used to isolate faults. However, this task can be difficult in an Ethernet environment, since each node is connected through multipoint links. Fault isolation is even more challenging since the MAC address of the target node can age out in several minutes. This can cause the traced path to vary over time, or connectivity lost if faults cause the target MEP to be isolated from other MEPs in an MA.

- When using the command line or web interface, the source MEP used by to send a link trace message is chosen by the CFM protocol. However, when using SNMP, the source MEP can be specified by the user.

- Parameters controlling the link trace cache, including operational state, entry hold time, and maximum size can be configured on the Configure Global page (see "Configuring Global Settings for CFM").

PARAMETERS

These parameters are displayed:

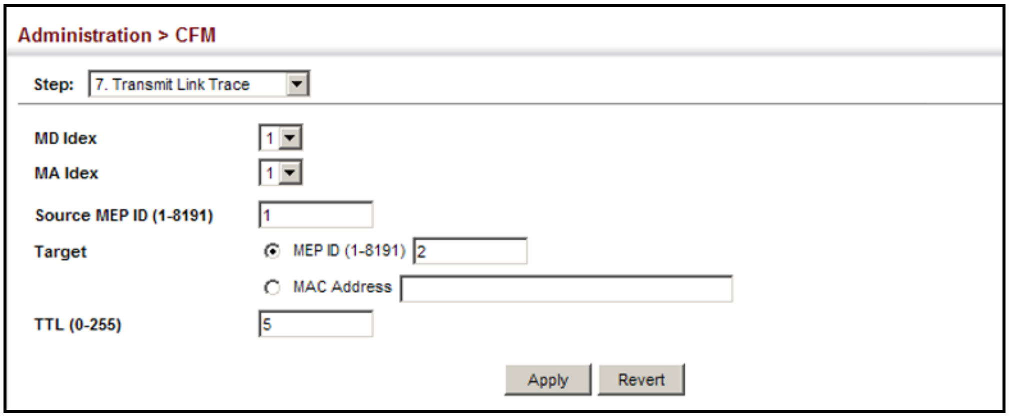
- **MD Index** – Domain index. (Range: 1-65535)
- **MA Index** – MA identifier. (Range: 1-2147483647)
- **Source MEP ID** – The identifier of a source MEP that will send the link trace message. (Range: 1-8191)
- **Target**
  - **MEP ID** – The identifier of a remote MEP that is the target of a link trace message. (Range: 1-8191)
  - **MAC Address** – MAC address of a remote MEP that is the target of a link trace message. This address can be entered in either of the following formats: xx-xx-xx-xx-xx-xx or xxxxxxxxxxxx
- **TTL** – The time to live of the link trace message. (Range: 0-255 hops)

WEB INTERFACE

To transmit link trace messages:

1. Click Administration, CFM.
2. Select Transmit Link Trace from the Step list.
3. Select an entry from MD Index and MA Index.
4. Specify the source MEP, the target MEP using either its MEP identifier or MAC address, and set the maximum number of hops allowed in the TTL field.
5. Click Apply.
6. Check the results in the Link Trace cache (see "Displaying the Link Trace Cache").

Figure 313: Transmitting Link Trace Messages



Administration > CFM

Step: 7. Transmit Link Trace

MD Idex	1
MA Idex	1
Source MEP ID (1-8191)	1
Target	● MEP ID (1-8191) 2 ○ MAC Address
TTL (0-255)	5

TRANSMITTING LOOP BACK MESSAGES

Use the Administration > CFM (Transmit Loopback) page to transmit Loopback Messages (LBMs). These messages can be used to isolate or verify connectivity faults by submitting a request to a target node (i.e., a remote MEP or MIP) to echo the message back to the source.

CLI REFERENCES

- "CFM Commands" on page 1561

COMMAND USAGE

- Loopback messages can be used for fault verification and isolation after automatic detection of a fault or receipt of some other error report. Loopback messages can also used to confirm the successful restoration or initiation of connectivity. The receiving maintenance point should respond to the loop back message with a loopback reply.

- The point from which the loopback message is transmitted (i.e., a local DSAP) and the target maintenance point must be within the same MA.

- If the continuity check database does not have an entry for the specified maintenance point, an error message will be displayed.

- When using the command line or web interface, the source MEP used by to send a loopback message is chosen by the CFM protocol. However, when using SNMP, the source MEP can be specified by the user.

PARAMETERS

These parameters are displayed:

- **MD Index** – Domain index. (Range: 1-65535)

- **MA Index** – MA identifier. (Range: 1-2147483647)

- **Source MEP ID** – The identifier of a source MEP that will send the loopback message. (Range: 1-8191)

- **Target**
  - **MEP ID** – The identifier of a remote MEP that is the target of a loopback message. (Range: 1-8191)
  - **MAC Address** – MAC address of a remote MEP that is the target of a loopback message. This address can be entered in either of the following formats: xx-xx-xx-xx-xx-xx or xxxxxxxxxxxx

- **Count** – The number of times the loopback message is sent. (Range: 1-1024)

- **Packet Size** – The size of the loopback message. (Range: 64-1518 bytes; Default: 64 bytes)

WEB INTERFACE

To transmit loopback messages:

1. Click Administration, CFM.

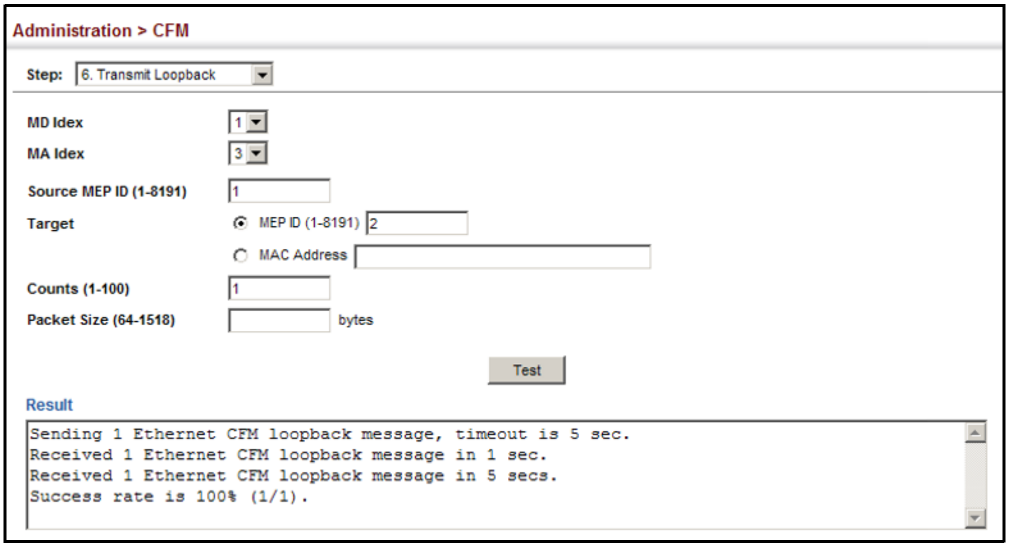
2. Select Transmit Loopback from the Step list.

3. Select an entry from MD Index and MA Index.

4. Specify the source MEP, the target MEP using either its MEP identifier or MAC address, set the number of times the loopback message is to be sent.

5. Click Apply.

Figure 314: Transmitting Loopback Messages



Step: 6. Transmit Loopback

MD Idex: 1

MA Idex: 3

Source MEP ID (1-8191): 1

Target: ● MEP ID (1-8191) 2
○ MAC Address

Counts (1-100): 1

Packet Size (64-1518): bytes

```
Sending 1 Ethernet CFM loopback message, timeout is 5 sec.
Received 1 Ethernet CFM loopback message in 1 sec.
Received 1 Ethernet CFM loopback message in 5 secs.
Success rate is 100% (1/1).
```

TRANSMITTING DELAY-MEASURE REQUESTS

Use the Administration > CFM (Transmit Delay Measure) page to send periodic delay-measure requests to a specified MEP within a maintenance association.

CLI REFERENCES

- "ethernet cfm delay-measure two-way" on page 1600

COMMAND USAGE

- Delay measurement can be used to measure frame delay and frame delay variation between MEPs.

- A local MEP must be configured for the same MA before you can use this function.

- If a MEP is enabled to generate frames with delay measurement (DM) information, it periodically sends DM frames to its peer MEP in the same MA., and expects to receive DM frames back from it.

- Frame delay measurement can be made only for two-way measurements, where the MEP transmits a frame with DM request information with the TxTimeStampf (Timestamp at the time of sending a frame with DM request information), and the receiving MEP responds with a frame with DM reply information with TxTimeStampf copied from the DM request information, RxTimeStampf (Timestamp at the time of receiving a frame with DM request information), and TxTimeStampb (Timestamp at the time of transmitting a frame with DM reply information):

  Frame Delay = (RxTimeStampb-TxTimeStampf)-(TxTimeStampb-RxTimeStampf)

- The MEP can also make two-way frame delay variation measurements based on its ability to calculate the difference between two subsequent two-way frame delay measurements.

PARAMETERS

These parameters are displayed:

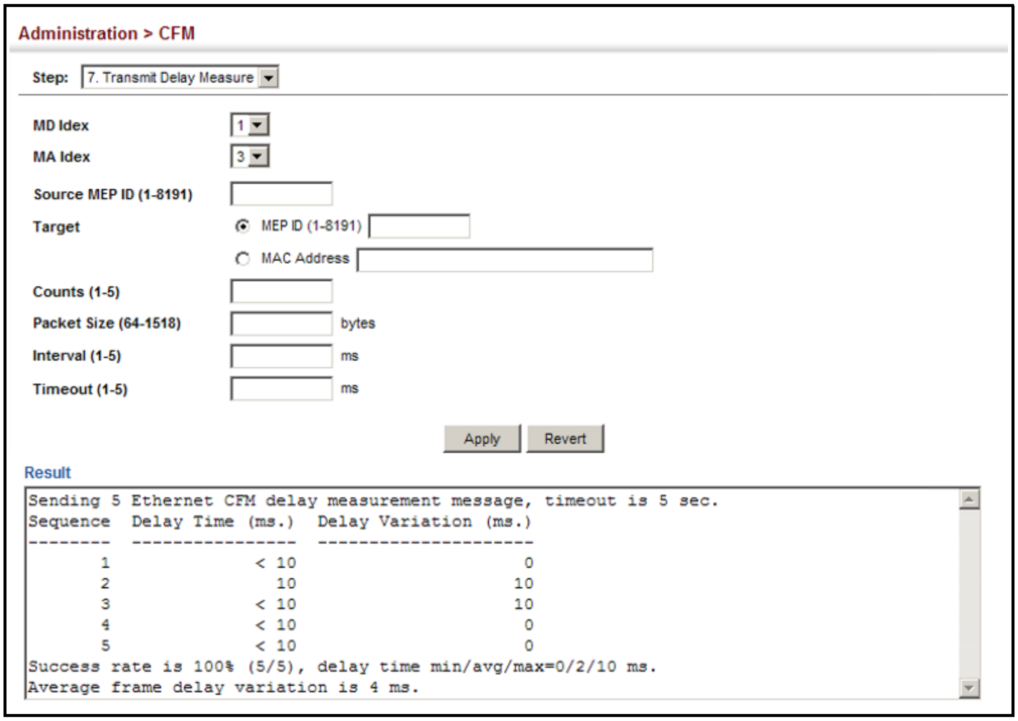
- **MD Index** – Domain index. (Range: 1-65535)
- **MA Index** – MA identifier. (Range: 1-2147483647)
- **Source MEP ID** – The identifier of a source MEP that will send the delay-measure message. (Range: 1-8191)
- **Target**
  - **MEP ID** – The identifier of a remote MEP that is the target of a delay-measure message. (Range: 1-8191)
  - **MAC Address** – MAC address of a remote MEP that is the target of a delay-measure message. This address can be entered in either of the following formats: xx-xx-xx-xx-xx-xx or xxxxxxxxxxxx
- **Count** – The number of times to retry sending the message if no response is received before the specified timeout. (Range: 1-5; Default: 5)
- **Packet Size** – The size of the delay-measure message. (Range: 64-1518 bytes; Default: 64 bytes)
- **Interval** – The transmission delay between delay-measure messages. (Range: 1-5 seconds; Default: 1 second)
- **Timeout** – The timeout to wait for a response. (Range: 1-5 seconds; Default: 5 seconds)

WEB INTERFACE

To transmit delay-measure messages:

1. Click Administration, CFM.
2. Select Transmit Delay Measure from the Step list.
3. Select an entry from MD Index and MA Index.
4. Specify the source MEP, the target MEP using either its MEP identifier or MAC address, set the number of times the delay-measure message is to be sent, the interval, and the timeout.
5. Click Apply.

Figure 315: Transmitting Delay-Measure Messages



Step: 7. Transmit Delay Measure

MD Idex 1

MA Idex 3

Target ● MEP ID (1-8191) ○ MAC Address

```
Sending 5 Ethernet CFM delay measurement message, timeout is 5 sec.
Sequence  Delay Time (ms.)  Delay Variation (ms.)
--------  ----------------  ---------------------
       1              < 10                      0
       2                10                     10
       3              < 10                     10
       4              < 10                      0
       5              < 10                      0
Success rate is 100% (5/5), delay time min/avg/max=0/2/10 ms.
Average frame delay variation is 4 ms.
```

DISPLAYING LOCAL MEPS

Use the Administration > CFM > Show Information (Show Local MEP) page to show information for the MEPs configured on this device.

CLI REFERENCES

- "show ethernet cfm maintenance-points local" on page 1576

PARAMETERS

These parameters are displayed:

- **MEP ID** – Maintenance end point identifier.
- **MD Name** – Maintenance domain name.

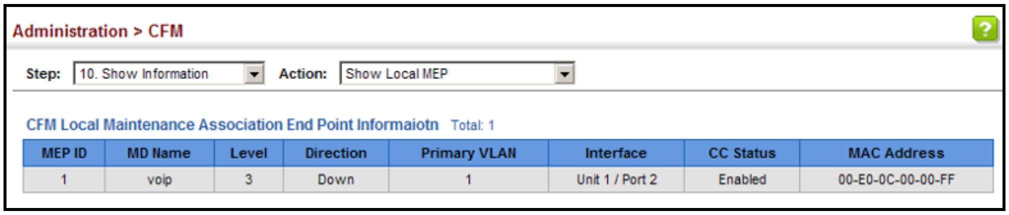
- **Level** – Authorized maintenance level for this domain.
- **Direction** – Direction in which the MEP communicates CFM messages:
  - Down indicates that the MEP is facing away from the switch, and transmits CFM messages towards, and receives them from, the direction of the physical medium.
  - Up indicates that the MEP faces inward toward the switch cross-connect matrix, and transmits CFM messages towards, and receives them from, the direction of the internal bridge relay mechanism.
- **Primary VLAN** – Service VLAN ID.
- **Interface** – Physical interface of this entry (either a port or trunk).
- **CC Status** – Shows administrative status of CCMs.
- **MAC Address** – MAC address of this MEP entry.

WEB INTERFACE

To show information for the MEPs configured on this device:

1. Click Administration, CFM.
2. Select Show Information from the Step list.
3. Select Show Local MEP from the Action list.

Figure 316: Showing Information on Local MEPs



Administration > CFM

Step: 10. Show Information Action: Show Local MEP

CFM Local Maintenance Association End Point Informaiotn Total: 1

MEP ID	MD Name	Level	Direction	Primary VLAN	Interface	CC Status	MAC Address
1	voip	3	Down	1	Unit 1 / Port 2	Enabled	00-E0-0C-00-00-FF

DISPLAYING DETAILS FOR LOCAL MEPS

Use the Administration > CFM > Show Information (Show Local MEP Details) page to show detailed CFM information about a local MEP in the continuity check database.

CLI REFERENCES

- "show ethernet cfm maintenance-points local detail mep" on page 1577

PARAMETERS

These parameters are displayed:

- **MD Index** – Domain index. (Range: 1-65535)
- **MA Index** – MA identifier. (Range: 1-2147483647)
- **MEP ID** – Maintenance end point identifier. (Range: 1-8191)

- **MD Name** – The maintenance domain for this entry.

- **MA Name** – Maintenance association to which this remote MEP belongs.

- **MA Name Format** – The format of the Maintenance Association name, including primary VID, character string, unsigned Integer 16, or RFC 2865 VPN ID.

- **Level** – Maintenance level of the local maintenance point.

- **Direction** – The direction in which the MEP faces on the Bridge port (up or down).

- **Interface** – The port to which this MEP is attached.

- **CC Status** – Shows if the MEP will generate CCM messages.

- **MAC Address** – MAC address of the local maintenance point. (If a CCM for the specified remote MEP has never been received or the local MEP record times out, the address will be set to the initial value of all Fs.)

- **Defect Condition** – Shows the defect detected on the MEP.

- **Received RDI** – Receive status of remote defect indication (RDI) messages on the MEP.

- **AIS Status** – Shows if MEPs within the specified MA are enabled to send frames with AIS information following detection of defect conditions.

- **AIS Period** – The interval at which AIS information is sent.

- **AIS Transmit Level** – The maintenance level at which AIS information will be sent for the specified MEP.

- **Suppress Alarm** – Shows if the specified MEP is configured to suppress sending frames containing AIS information following the detection of defect conditions.

- **Suppressing Alarms** – Shows if the specified MEP is currently suppressing sending frames containing AIS information following the detection of defect conditions.

WEB INTERFACE

To show detailed information for the MEPs configured on this device:

1. Click Administration, CFM.

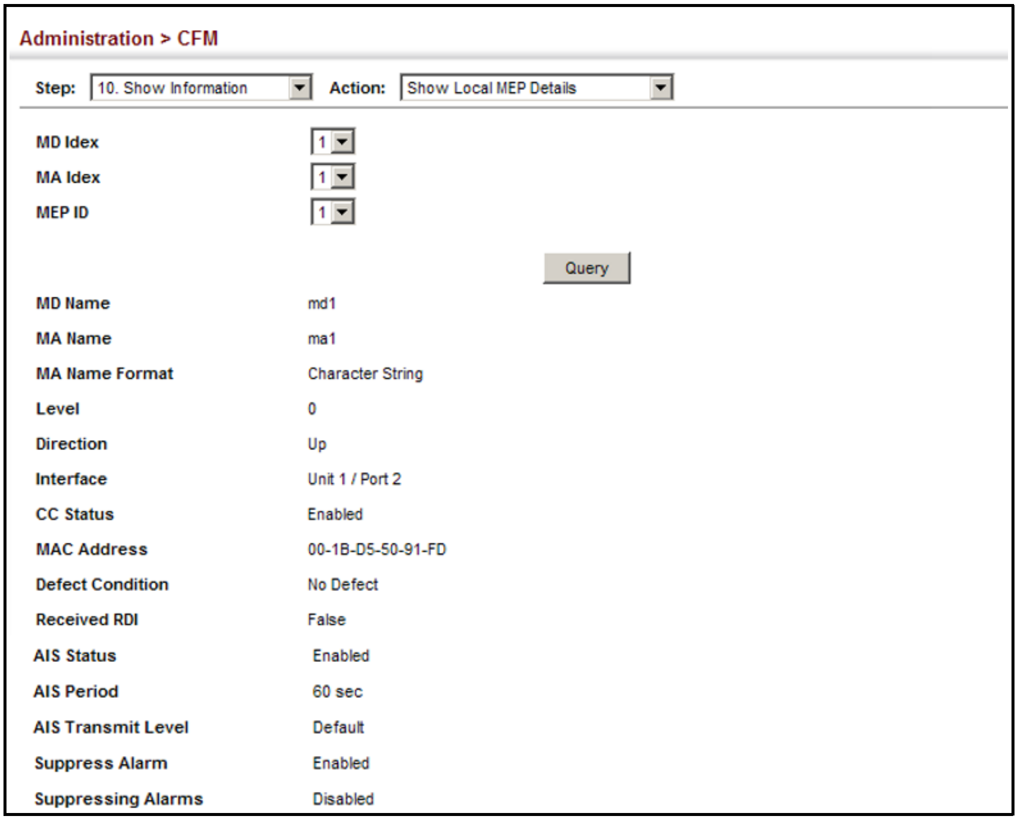
2. Select Show Information from the Step list.

3. Select Show Local MEP Details from the Action list.

4. Select an entry from MD Index and MA Index.

5. Select a MEP ID.

Figure 317: Showing Detailed Information on Local MEPs



Administration > CFM

Step: 10. Show Information Action: Show Local MEP Details

MD Idex 1
MA Idex 1
MEP ID 1

MD Name	md1
MA Name	ma1
MA Name Format	Character String
Level	0
Direction	Up
Interface	Unit 1 / Port 2
CC Status	Enabled
MAC Address	00-1B-D5-50-91-FD
Defect Condition	No Defect
Received RDI	False
AIS Status	Enabled
AIS Period	60 sec
AIS Transmit Level	Default
Suppress Alarm	Enabled
Suppressing Alarms	Disabled

DISPLAYING LOCAL MIPS

Use the Administration > CFM > Show Information (Show Local MIP) page to show the MIPs on this device discovered by the CFM protocol. (For a description of MIPs, refer to the Command Usage section under "Configuring CFM Maintenance Domains".)

CLI REFERENCES

- "show ethernet cfm maintenance-points local" on page 1576

PARAMETERS

These parameters are displayed:

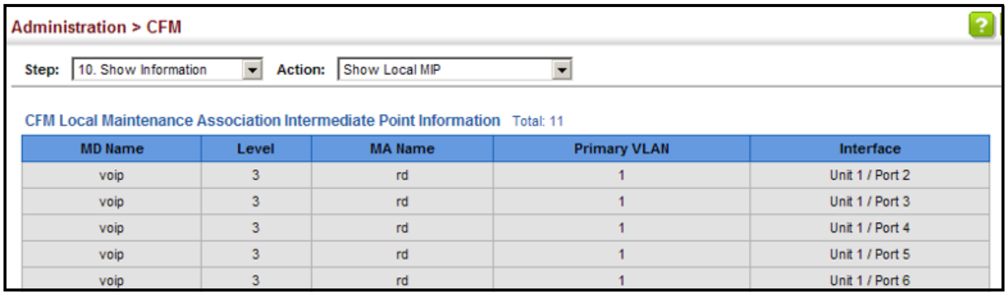
- **MD Name** – Maintenance domain name.
- **Level** – Authorized maintenance level for this domain.
- **MA Name** – Maintenance association name.
- **Primary VLAN** – Service VLAN ID.
- **Interface** – Physical interface of this entry (either a port or trunk).

WEB INTERFACE

To show information for the MIPs discovered by the CFM protocol:

1. Click Administration, CFM.
2. Select Show Information from the Step list.
3. Select Show Local MIP from the Action list.

Figure 318: Showing Information on Local MIPs



Administration > CFM

Step: 10. Show Information Action: Show Local MIP

CFM Local Maintenance Association Intermediate Point Information Total: 11

MD Name	Level	MA Name	Primary VLAN	Interface
voip	3	rd	1	Unit 1 / Port 2
voip	3	rd	1	Unit 1 / Port 3
voip	3	rd	1	Unit 1 / Port 4
voip	3	rd	1	Unit 1 / Port 5
voip	3	rd	1	Unit 1 / Port 6

DISPLAYING REMOTE MEPS

Use the Administration > CFM > Show Information (Show Remote MEP) page to show MEPs located on other devices which have been discovered through continuity check messages, or statically configured in the MEP database and verified through cross-check messages.

CLI REFERENCES

- "show ethernet cfm maintenance-points remote detail" on page 1579
- "clear ethernet cfm maintenance-points remote" on page 1584

PARAMETERS

These parameters are displayed:

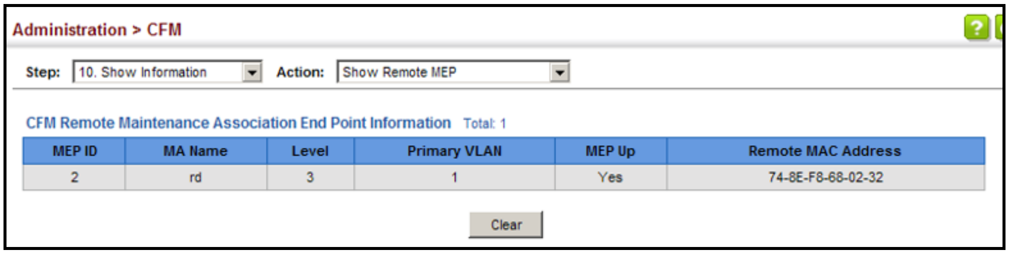
- **MEP ID** – Maintenance end point identifier.
- **MA Name** – Maintenance association name.
- **Level** – Authorized maintenance level for this domain.
- **Primary VLAN** – Service VLAN ID.
- **MEP Up** – Indicates whether or not this MEP is functioning normally.
- **Remote MAC Address** – MAC address of the remote maintenance point. (If a CCM for the specified remote MEP has never been received or the remote MEP record times out, the address will be set to the initial value of all Fs.)

WEB INTERFACE

To show information for remote MEPs:

1. Click Administration, CFM.
2. Select Show Information from the Step list.
3. Select Show Remote MEP from the Action list.

Figure 319: Showing Information on Remote MEPs



Administration > CFM

Step: 10. Show Information Action: Show Remote MEP

CFM Remote Maintenance Association End Point Information Total: 1

MEP ID	MA Name	Level	Primary VLAN	MEP Up	Remote MAC Address
2	rd	3	1	Yes	74-8E-F8-68-02-32

DISPLAYING DETAILS FOR REMOTE MEPS

Use the Administration > CFM > Show Information (Show Remote MEP Details) page to show detailed information for MEPs located on other devices which have been discovered through continuity check messages, or statically configured in the MEP database and verified through cross-check messages.

CLI REFERENCES

- "show ethernet cfm maintenance-points remote detail" on page 1579

PARAMETERS

These parameters are displayed:

- **MD Index** – Domain index. (Range: 1-65535)
- **MA Index** – MA identifier. (Range: 1-2147483647)
- **MEP ID** – Maintenance end point identifier. (Range: 1-8191)
- **MD Name** – Maintenance domain name.
- **MA Name** – Maintenance association name.
- **Level** – Authorized maintenance level for this domain.
- **MAC Address** – MAC address of this MEP entry.
- **Primary VLAN** – Service VLAN ID.
- **Incoming Port** – Port to which this remote MEP is attached.
- **CC Lifetime** – Length of time to hold messages about this MEP in the CCM database.

- **Age of Last CC Message** – Length of time the last CCM message about this MEP has been in the CCM database.

- **Frame Loss** – Percentage of transmitted frames lost.

- **CC Packet Statistics** – The number of CCM packets received successfully and those with errors.

- **Port State** – Port states include:
  - Up – The port is functioning normally.
  - Blocked – The port has been blocked by the Spanning Tree Protocol.
  - No port state – Either no CCM has been received, or nor port status TLV was received in the last CCM.

- **Interface State** – Interface states include:
  - No Status – Either no CCM has been received, or no interface status TLV was received in the last CCM.
  - Up – The interface is ready to pass packets.
  - Down – The interface cannot pass packets.
  - Testing – The interface is in some test mode.
  - Unknown – The interface status cannot be determined for some reason.
  - Dormant – The interface is not in a state to pass packets but is in a pending state, waiting for some external event.
  - Not Present – Some component of the interface is missing.
  - isLowerLayerDown – The interface is down due to state of the lower layer interfaces.

- **Crosscheck Status** – Shows if crosscheck function has been enabled.

WEB INTERFACE

To show detailed information for remote MEPs:

1. Click Administration, CFM.

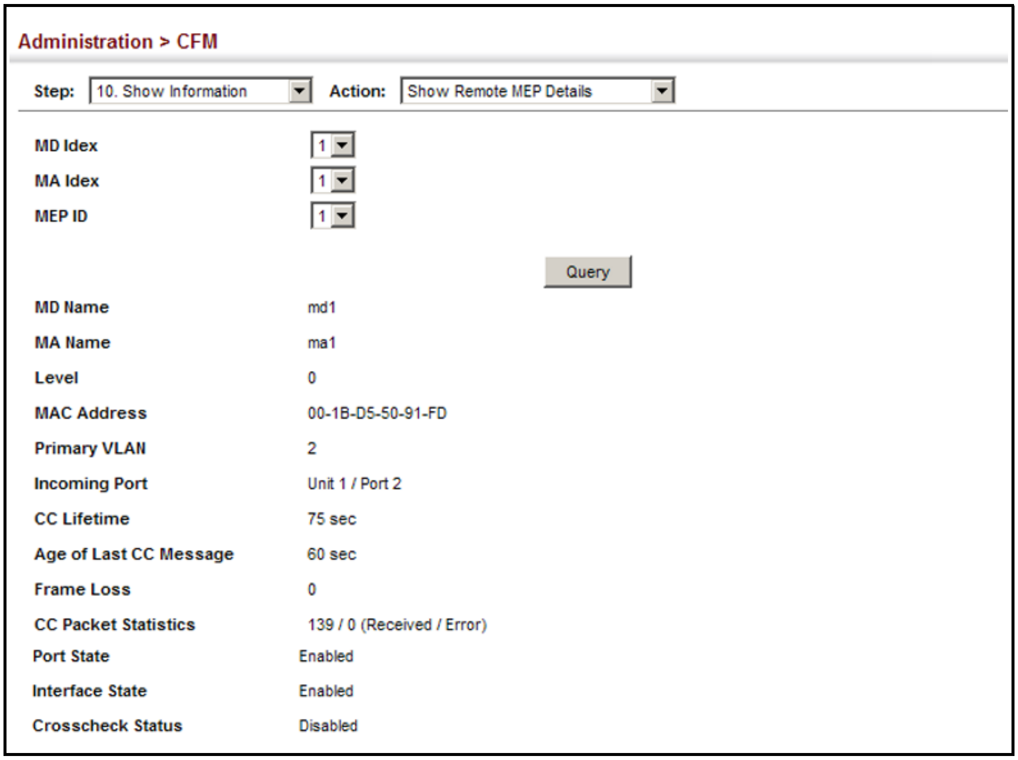
2. Select Show Information from the Step list.

3. Select Show Remote MEP Details from the Action list.

4. Select an entry from MD Index and MA Index.

5. Select a MEP ID.

Figure 320: Showing Detailed Information on Remote MEPs



Step: 10. Show Information
Action: Show Remote MEP Details

MD Idex: 1
MA Idex: 1
MEP ID: 1

MD Name	md1
MA Name	ma1
Level	0
MAC Address	00-1B-D5-50-91-FD
Primary VLAN	2
Incoming Port	Unit 1 / Port 2
CC Lifetime	75 sec
Age of Last CC Message	60 sec
Frame Loss	0
CC Packet Statistics	139 / 0 (Received / Error)
Port State	Enabled
Interface State	Enabled
Crosscheck Status	Disabled

DISPLAYING THE LINK TRACE CACHE

Use the Administration > CFM > Show Information (Show Link Trace Cache) page to show information about link trace operations launched from this device.

CLI REFERENCES

- "show ethernet cfm linktrace-cache" on page 1594
- "clear ethernet cfm linktrace-cache" on page 1593

PARAMETERS

These parameters are displayed:

- **Hops** – The number hops taken to reach the target MEP.
- **MA** – Maintenance association name.
- **IP/Alias** – IP address or DNS alias of the target device’s CPU.
- **Forwarded** – Shows whether or not this link trace message was forwarded. A message is not forwarded if received by the target MEP.
- **Ingress MAC Address** – MAC address of the ingress port on the target device.
- **Egress MAC Address** – MAC address of the egress port on the target device.

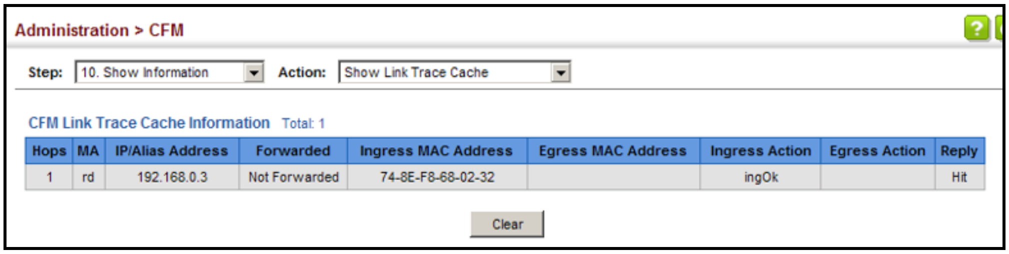
- **Ingress Action** – Action taken on the ingress port:
  - IngOk – The target data frame passed through to the MAC Relay Entity.
  - IngDown – The bridge port's MAC_Operational parameter is false. This value could be returned, for example, by an operationally Down MEP that has another Down MEP at a higher MD level on the same bridge port that is causing the bridge port's MAC_Operational parameter to be false.
  - IngBlocked – The ingress port can be identified, but the target data frame was not forwarded when received on this port due to active topology management, i.e., the bridge port is not in the forwarding state.
  - IngVid – The ingress port is not in the member set of the LTM's VIDs, and ingress filtering is enabled, so the target data frame was filtered by ingress filtering.
- **Egress Action** – Action taken on the egress port:
  - EgrOk – The targeted data frame was forwarded.
  - EgrDown – The Egress Port can be identified, but that bridge port's MAC_Operational parameter is false.
  - EgrBlocked – The egress port can be identified, but the data frame was not passed through the egress port due to active topology management, i.e., the bridge port is not in the forwarding state.
  - EgrVid – The Egress Port can be identified, but the bridge port is not in the LTM's VID member set, and was therefore filtered by egress filtering.
- **Reply** – Reply action:
  - FDB – Target address found in forwarding database.
  - MPDB – Target address found in the maintenance point database.
  - HIT – Target located on this device.

WEB INTERFACE

To show information about link trace operations launched from this device:

1. Click Administration, CFM.
2. Select Show Information from the Step list.
3. Select Show Link Trace Cache from the Action list.

Figure 321: Showing the Link Trace Cache



Administration > CFM

Step: 10. Show Information Action: Show Link Trace Cache

CFM Link Trace Cache Information Total: 1

Hops	MA	IP/Alias Address	Forwarded	Ingress MAC Address	Egress MAC Address	Ingress Action	Egress Action	Reply
1	rd	192.168.0.3	Not Forwarded	74-8E-F8-68-02-32		ingOk		Hit

Displaying Fault Notification Settings

Use the Administration > CFM > Show Information (Show Fault Notification Generator) page to display configuration settings for the fault notification generator.

CLI References

- "show ethernet cfm fault-notify-generator" on page 1599

Parameters

These parameters are displayed:

- **MEP ID** – Maintenance end point identifier.
- **MD Name** – Maintenance domain name.
- **MA Name** – Maintenance association name.
- **Highest Defect** – The highest defect that will generate a fault alarm. (This is disabled by default.)
- **Lowest Alarm** – The lowest defect that will generate a fault alarm[11].
- **Alarm Time** – The time a defect must exist before a fault alarm is issued[11].
- **Reset Time** – The time after a fault alarm has been issued, and no defect exists, before another fault alarm can be issued[11].

[11] See "Configuring CFM Maintenance Domains" on page 555.

WEB INTERFACE

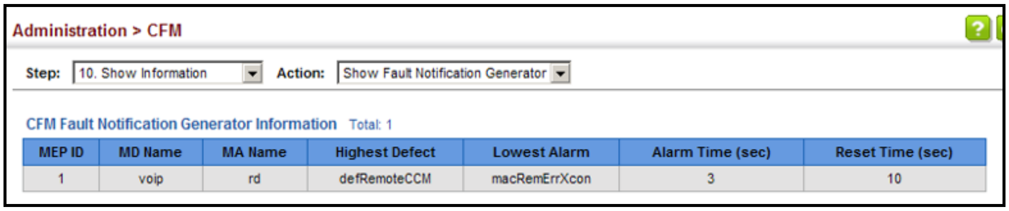
To show configuration settings for the fault notification generator:

1. Click Administration, CFM.

2. Select Show Information from the Step list.

3. Select Show Fault Notification Generator from the Action list.

Figure 322: Showing Settings for the Fault Notification Generator



Administration > CFM

Step: 10. Show Information Action: Show Fault Notification Generator

CFM Fault Notification Generator Information Total: 1

MEP ID	MD Name	MA Name	Highest Defect	Lowest Alarm	Alarm Time (sec)	Reset Time (sec)
1	voip	rd	defRemoteCCM	macRemErrXcon	3	10

DISPLAYING CONTINUITY CHECK ERRORS

Use the Administration > CFM > Show Information (Show Continuity Check Error) page to display the CFM continuity check errors logged on this device.

CLI REFERENCES

- "show ethernet cfm errors" on page 1585
- "clear ethernet cfm errors" on page 1585

PARAMETERS

These parameters are displayed:

- **Level** – Maintenance level associated with this entry.
- **Primary VLAN** – VLAN in which this error occurred.
- **MEP ID** – Identifier of remote MEP.
- **Interface** – Port at which the error was recorded.
- **Remote MAC** – MAC address of remote MEP.
- **Reason** – Error types include:
  - LEAK – MA *x* is associated with a specific VID list[12], one or more of the VIDs in this MA can pass through the bridge port, no MEP is configured facing outward (down) on any bridge port for this MA, and some other MA *y*, at a higher maintenance level, and associated with at least one of the VID(s) also in MA *x*, does have a MEP configured on the bridge port.

[12] This definition is based on the IEEE 802.1ag standard. Current software for this switch only supports a single VLAN per MA. However, since it may interact with other devices which support multiple VLAN assignments per MA, this error message may be reported.

- VIDS – MA *x* is associated with a specific VID list[12], an MEP is configured facing inward (up) on this MA on the bridge port, and some other MA *y*, associated with at least one of the VID(s) also in MA *x*, also has an Up MEP configured facing inward (up) on some bridge port.
- EXCESS_LEV – The number of different MD levels at which MIPs are to be created on this port exceeds the bridge's capabilities.
- OVERLAP_LEV – A MEP is created for one VID at one maintenance level, but a MEP is configured on another VID at an equivalent or higher level, exceeding the bridge's capabilities.

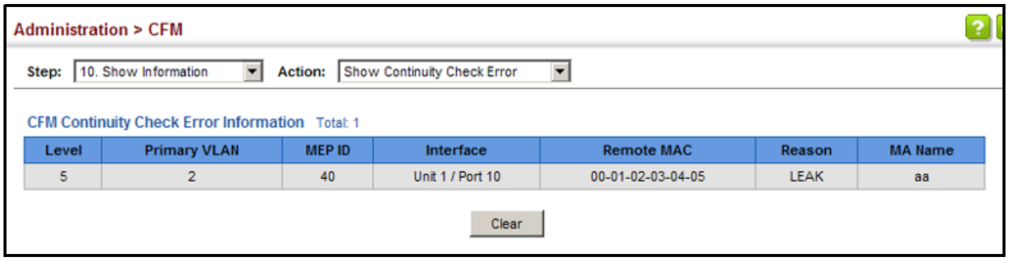
◆ **MA Name** – The maintenance association for this entry.

WEB INTERFACE

To show CFM continuity check errors:

1. Click Administration, CFM.
2. Select Show Information from the Step list.
3. Select Show Continuity Check Error from the Action list.

Figure 323: Showing Continuity Check Errors



Step: 10. Show Information Action: Show Continuity Check Error

CFM Continuity Check Error Information Total: 1

Level	Primary VLAN	MEP ID	Interface	Remote MAC	Reason	MA Name
5	2	40	Unit 1 / Port 10	00-01-02-03-04-05	LEAK	aa

OAM CONFIGURATION

The switch provides OAM (Operation, Administration, and Maintenance) remote management tools required to monitor and maintain the links to subscriber CPEs (Customer Premise Equipment). This section describes functions including enabling OAM for selected ports, loopback testing, and displaying remote device information.

ENABLING OAM ON LOCAL PORTS

Use the Administration > OAM > Interface page to enable OAM functionality on the selected port. Not all CPEs support operation and maintenance functions, so OAM is therefore disabled by default. If a CPE supports OAM, this functionality must first be enabled on the connected port to gain access to the configuration functions provided under the OAM menu.

CLI REFERENCES

- "OAM Commands" on page 1603

PARAMETERS

These parameters are displayed:

- **Port** – Port identifier. (Range: 1-28)
- **Admin Status** – Enables or disables OAM functions. (Default: Disabled)
- **Operation State** – Shows the operational state between the local and remote OAM devices. This value is always “disabled” if OAM is disabled on the local interface.

Table 38: OAM Operation State

State	Description
Disabled	OAM is disabled on this interface via the OAM Admin Status.
Link Fault	The link has detected a fault or the interface is not operational.
Passive Wait	This value is returned only by OAM entities in passive mode and indicates the OAM entity is waiting to see if the peer device is OAM capable.
Active Send Local	This value is used by active mode devices and indicates the OAM entity is actively trying to discover whether the peer has OAM capability but has not yet made that determination.
Send Local And Remote	The local OAM entity has discovered the peer but has not yet accepted or rejected the configuration of the peer.
Send Local And Remote OK	OAM peering is allowed by the local device.
OAM Peering Locally Rejected	The local OAM entity rejects the peering.
OAM Peering Remotely Rejected	The remote OAM entity rejects the peering.
Operational	When the local OAM entity learns that both it and the remote OAM entity have accepted the peering, the state moves to this state.
Non Oper Half Duplex	This state is returned whenever Ethernet OAM is enabled but the interface is in half-duplex operation.

- **Mode** – Sets the OAM operation mode. (Default: Active)
  - **Active** – All OAM functions are enabled.
  - **Passive** – All OAM functions are enabled, except for OAM discovery, sending variable request OAMPDUs, and sending loopback control OAMPDUs.

- **Critical Link Event** – Controls reporting of critical link events to its OAM peer.
  - **Dying Gasp** – If an unrecoverable condition occurs, the local OAM entity (i.e., this switch) indicates this by immediately sending a trap message. (Default: Enabled)

    Dying gasp events are caused by an unrecoverable failure, such as a power failure or device reset.

NOTE: When system power fails, the switch will always send a dying gasp trap message prior to power down.

  - **Critical Event** – If a critical event occurs, the local OAM entity indicates this to its peer by setting the appropriate flag in the next OAMPDU to be sent and stores this information in its OAM event log. (Default: Enabled)

    Critical events include various failures, such as abnormal voltage fluctuations, out-of-range temperature detected, fan failure, CRC error in flash memory, insufficient memory, or other hardware faults.

- **Errored Frame** – Controls reporting of errored frame link events.

  An errored frame is a frame in which one or more bits are errored.

  An errored frame link event occurs if the threshold is reached or exceeded within the specified period.

  If reporting is enabled and an errored frame link event occurs, the local OAM entity (this switch) sends an Event Notification OAMPDU to the remote OAM entity. The Errored Frame Event TLV includes the number of errored frames detected during the specified period.

  - **Status** – Enables reporting of errored frame link events. (Default: Enabled)
  - **Window Size** – The period of time in which to check the reporting threshold for errored frame link events. (Range: 10-65535 in units of 10 milliseconds; Default: 10 units of 10 milliseconds, or the equivalent of 1 second)
  - **Threshold Count** – The threshold for errored frame link events. (Range: 1-65535; Default: 1)

WEB INTERFACE

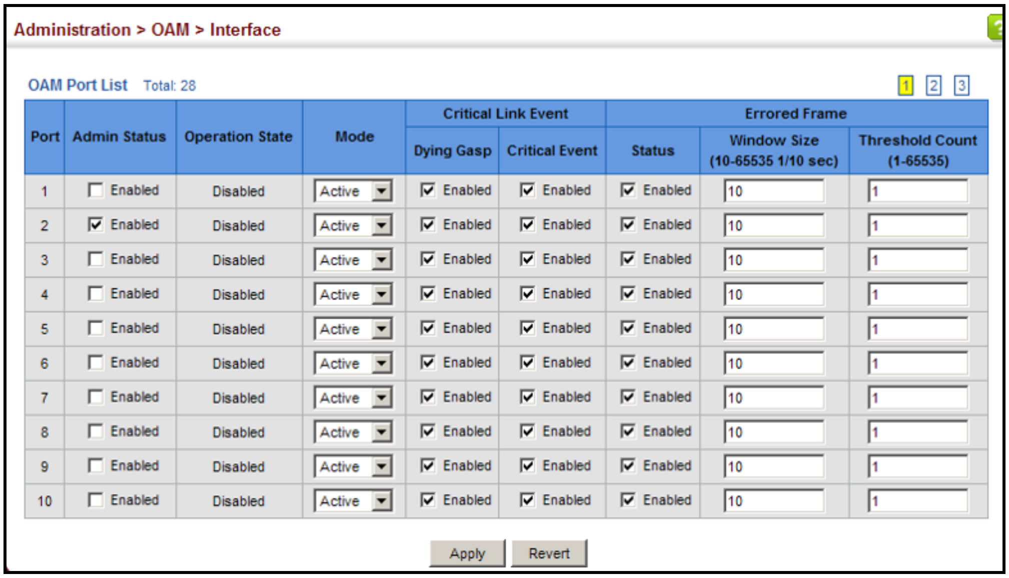
To enable OAM functionality on the selected port:

1. Click Administration, OAM, Interface.
2. Set the OAM administrative status and operational mode for the required ports. Specify whether or not critical link events will be

reported by the switch. Specify whether errored frame link events will be reported, as well as the required window size and threshold.

3. Click Apply.

Figure 324: Enabling OAM for Local Ports



OAM Port List Total: 28

Port	Admin Status	Operation State	Mode	Critical Link Event		Errored Frame		
				Dying Gasp	Critical Event	Status	Window Size (10-65535 1/10 sec)	Threshold Count (1-65535)
1	☐ Enabled	Disabled	Active ▾	☑ Enabled	☑ Enabled	☑ Enabled	10	1
2	☑ Enabled	Disabled	Active ▾	☑ Enabled	☑ Enabled	☑ Enabled	10	1
3	☐ Enabled	Disabled	Active ▾	☑ Enabled	☑ Enabled	☑ Enabled	10	1
4	☐ Enabled	Disabled	Active ▾	☑ Enabled	☑ Enabled	☑ Enabled	10	1
5	☐ Enabled	Disabled	Active ▾	☑ Enabled	☑ Enabled	☑ Enabled	10	1
6	☐ Enabled	Disabled	Active ▾	☑ Enabled	☑ Enabled	☑ Enabled	10	1
7	☐ Enabled	Disabled	Active ▾	☑ Enabled	☑ Enabled	☑ Enabled	10	1
8	☐ Enabled	Disabled	Active ▾	☑ Enabled	☑ Enabled	☑ Enabled	10	1
9	☐ Enabled	Disabled	Active ▾	☑ Enabled	☑ Enabled	☑ Enabled	10	1
10	☐ Enabled	Disabled	Active ▾	☑ Enabled	☑ Enabled	☑ Enabled	10	1

DISPLAYING STATISTICS FOR OAM MESSAGES

Use the Administration > OAM > Counters page to display statistics for the various types of OAM messages passed across each port.

CLI REFERENCES

- "show efm oam counters interface" on page 1610

PARAMETERS

These parameters are displayed:

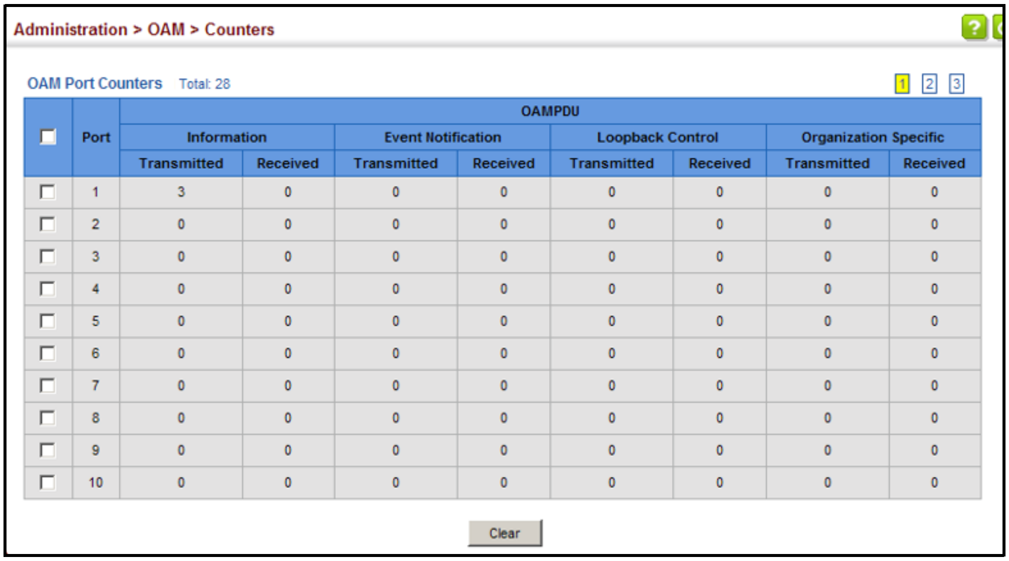
- **Port** – Port identifier. (Range: 1-28)
- **Clear** – Clears statistical counters for the selected ports.
- **OAMPDU** – Message types transmitted and received by the OAM protocol, including Information OAMPDUs, unique Event OAMPDUs, Loopback Control OAMPDUs, and Organization Specific OAMPDUs.

WEB INTERFACE

To display statistics for OAM messages:

1. Click Administration, OAM, Counters.

Figure 325: Displaying Statistics for OAM Messages



□	Port	OAMPDU							
		Information		Event Notification		Loopback Control		Organization Specific	
		Transmitted	Received	Transmitted	Received	Transmitted	Received	Transmitted	Received
□	1	3	0	0	0	0	0	0	0
□	2	0	0	0	0	0	0	0	0
□	3	0	0	0	0	0	0	0	0
□	4	0	0	0	0	0	0	0	0
□	5	0	0	0	0	0	0	0	0
□	6	0	0	0	0	0	0	0	0
□	7	0	0	0	0	0	0	0	0
□	8	0	0	0	0	0	0	0	0
□	9	0	0	0	0	0	0	0	0
□	10	0	0	0	0	0	0	0	0

DISPLAYING THE OAM EVENT LOG

Use the Administration > OAM > Event Log page to display link events for the selected port.

CLI REFERENCES

- "show efm oam event-log interface" on page 1611

COMMAND USAGE

- When a link event occurs, no matter whether the location is local or remote, this information is entered in OAM event log.
- When the log system becomes full, older events are automatically deleted to make room for new entries.
- The time of locally generated events can be accurately retrieved from the sysUpTime variable. For remotely generated events, the time of an event is indicated by the reception of an Event Notification OAMPDU from the peer.

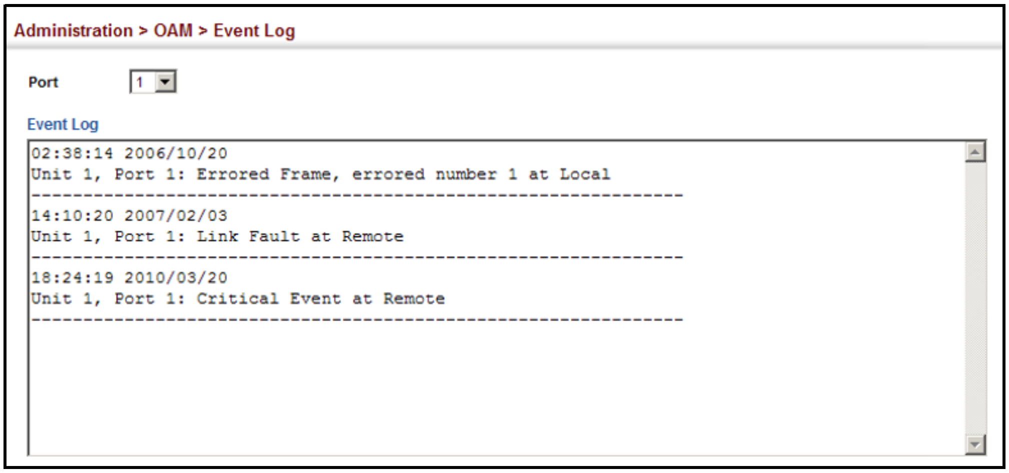
WEB INTERFACE

To display link events for the selected port:

1. Click Administration, OAM, Event Log.

2. Select a port from the drop-down list.

Figure 326: Displaying the OAM Event Log



```
02:38:14 2006/10/20
Unit 1, Port 1: Errored Frame, errored number 1 at Local
----------------------------------------------------------------
14:10:20 2007/02/03
Unit 1, Port 1: Link Fault at Remote
----------------------------------------------------------------
18:24:19 2010/03/20
Unit 1, Port 1: Critical Event at Remote
----------------------------------------------------------------
```

DISPLAYING THE STATUS OF REMOTE INTERFACES

Use the Administration > OAM > Remote Interface page to display information about attached OAM-enabled devices.

CLI REFERENCES

- "show efm oam status remote interface" on page 1613

PARAMETERS

These parameters are displayed:

- **Port** – Port identifier. (Range: 1-28)
- **MAC Address** – MAC address of the OAM peer.
- **OUI** – Organizational Unit Identifier of the OAM peer.
- **Remote Loopback** – Shows if remote loopback is supported by the OAM peer.
- **Unidirectional Function** – Shows if this function is supported by the OAM peer.

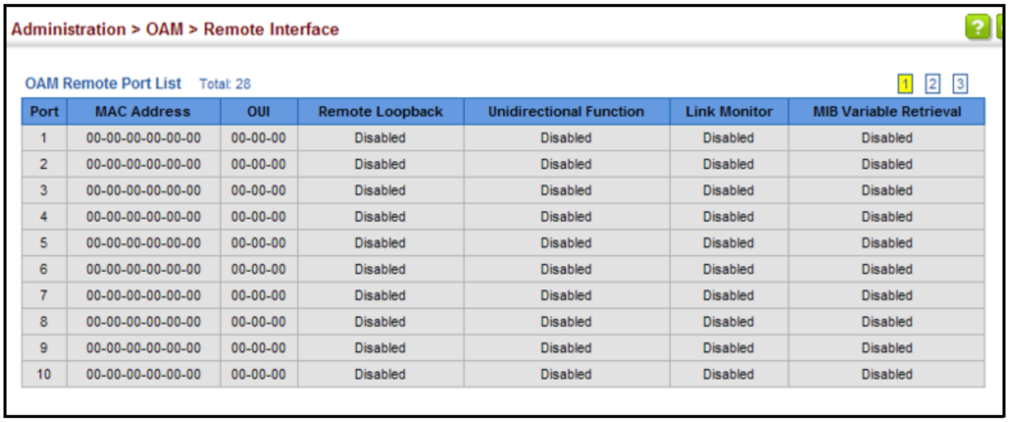
  If supported, this indicates that the OAM entity supports the transmission of OAMPDUs on links that are operating in unidirectional mode (where traffic flows in one direction only). Some newer physical layer devices support the optional ability to encode and transmit data while one direction of the link is non-operational. This function allows OAM remote fault indication during fault conditions. This switch does not support the unidirectional function, but can parse error messages sent from a peer with unidirectional capability.
- **Link Monitor** – Shows if the OAM entity can send and receive Event Notification OAMPDUs.
- **MIB Variable Retrieval** – Shows if the OAM entity can send and receive Variable Request and Response OAMPDUs.

Web Interface

To display information about attached OAM-enabled devices:

1. Click Administration, OAM, Remote Interface.

Figure 327: Displaying Status of Remote Interfaces



Administration > OAM > Remote Interface

OAM Remote Port List Total: 28

Port	MAC Address	OUI	Remote Loopback	Unidirectional Function	Link Monitor	MIB Variable Retrieval
1	00-00-00-00-00-00	00-00-00	Disabled	Disabled	Disabled	Disabled
2	00-00-00-00-00-00	00-00-00	Disabled	Disabled	Disabled	Disabled
3	00-00-00-00-00-00	00-00-00	Disabled	Disabled	Disabled	Disabled
4	00-00-00-00-00-00	00-00-00	Disabled	Disabled	Disabled	Disabled
5	00-00-00-00-00-00	00-00-00	Disabled	Disabled	Disabled	Disabled
6	00-00-00-00-00-00	00-00-00	Disabled	Disabled	Disabled	Disabled
7	00-00-00-00-00-00	00-00-00	Disabled	Disabled	Disabled	Disabled
8	00-00-00-00-00-00	00-00-00	Disabled	Disabled	Disabled	Disabled
9	00-00-00-00-00-00	00-00-00	Disabled	Disabled	Disabled	Disabled
10	00-00-00-00-00-00	00-00-00	Disabled	Disabled	Disabled	Disabled

Configuring a Remote Loop Back Test

Use the Administration > OAM > Remote Loopback (Remote Loopback Test) page to initiate a loop back test to the peer device attached to the selected port.

CLI References

- "efm oam remote-loopback" on page 1608
- "efm oam remote-loopback test" on page 1609

Command Usage

- You can use this command to perform an OAM remote loop back test on the specified port. The port that you specify to run this test must be connected to a peer OAM device capable of entering into OAM remote loop back mode.
- During a remote loop back test, the remote OAM entity loops back every frame except for OAMPDUs and pause frames.
- OAM remote loopback can be used for fault localization and link performance testing. Statistics from both the local and remote DTE can be queried and compared at any time during loop back testing.
- To perform a loopback test, first enable Remote Loop Back Mode, click Test, and then click End. The number of packets transmitted and received will be displayed.

PARAMETERS

These parameters are displayed:

Loopback Mode of Remote Device

- **Port** – Port identifier. (Range: 1-28)
- **Loopback Mode** – Shows if loop back mode is enabled on the peer. This attribute must be enabled before starting the loopback test.
- **Loopback Status** – Shows if loopback testing is currently running.

Loopback Test Parameters

- **Packets Number** – Number of packets to send. (Range: 1-99999999; Default: 10000)
- **Packet Size** – Size of packets to send. (Range: 64-1518 bytes; Default: 64 bytes)
- **Test** – Starts the loop back test.
- **End** – Stops the loop back test.

Loop Back Status of Remote Device

- **Result** – Shows the loop back status on the peer. The loop back states shown in this field are described below.

Table 39: OAM Operation State

State	Description
No Loopback	Operating in normal mode with no loopback in progress.
Initiating Loopback	The local OAM entity is starting the loopback process with its peer. It has yet to receive any acknowledgement that the remote OAM entity has received its loopback command request.
Remote Loopback	The local OAM client knows that the remote OAM entity is in loopback mode.
Terminating Loopback	The local OAM client is in the process of terminating the remote loopback.
Local Loopback	The remote OAM client has put the local OAM entity in loopback mode.
Unknown	This status may be returned if the OAM loopback is in a transition state but should not persist.

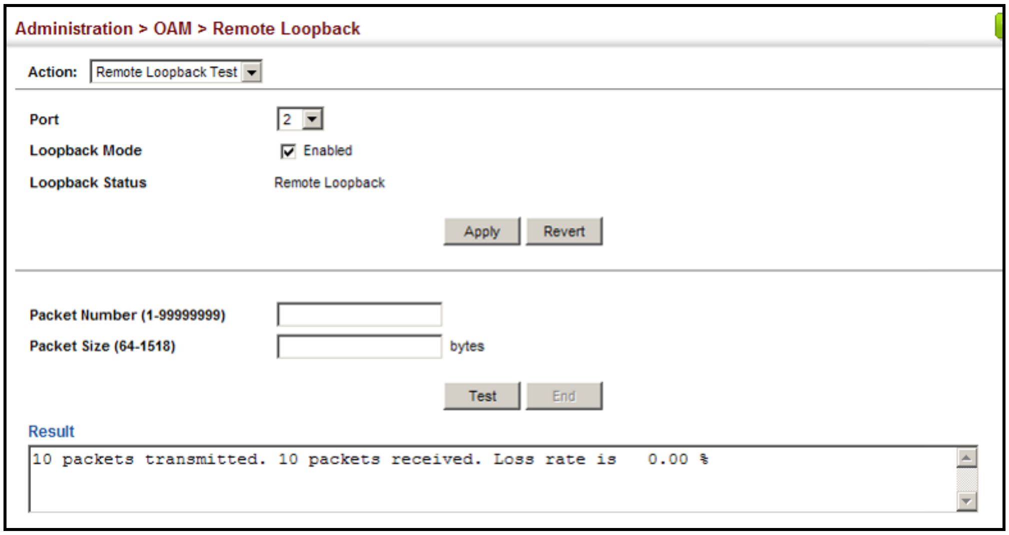
- **Packets Transmitted** – The number of loop back frames transmitted during the last loopback test on this interface.
- **Packets Received** – The number of loop back frames received during the last loopback test on this interface.
- **Loss Rate** – The percentage of packets for which there was no response.

WEB INTERFACE

To initiate a loop back test to the peer device attached to the selected port:

1. Click Administration, OAM, Remote Loop Back.
2. Select Remote Loopback Test from the Action list.
3. Select the port on which to initiate remote loop back testing, enable the Loop Back Mode attribute, and click Apply.
4. Set the number of packets to send and the packet size, and then click Test.

Figure 328: Running a Remote Loop Back Test



Action: Remote Loopback Test

Port: 2

Loopback Mode: ☑ Enabled

Loopback Status: Remote Loopback

Packet Number (1-99999999):

Packet Size (64-1518): bytes

Result

```
10 packets transmitted. 10 packets received. Loss rate is   0.00 %
```

DISPLAYING RESULTS OF REMOTE LOOP BACK TESTING

Use the Administration > OAM > Remote Loop Back (Show Test Result) page to display the results of remote loop back testing for each port for which this information is available.

CLI REFERENCES

- "show efm oam remote-loopback interface" on page 1612

PARAMETERS

These parameters are displayed:

- **Port** – Port identifier. (Range: 1-28)
- **Packets Transmitted** – The number of loop back frames transmitted during the last loop back test on this interface.
- **Packets Received** – The number of loop back frames received during the last loop back test on this interface.
- **Loss Rate** – The percentage of packets transmitted for which there was no response.

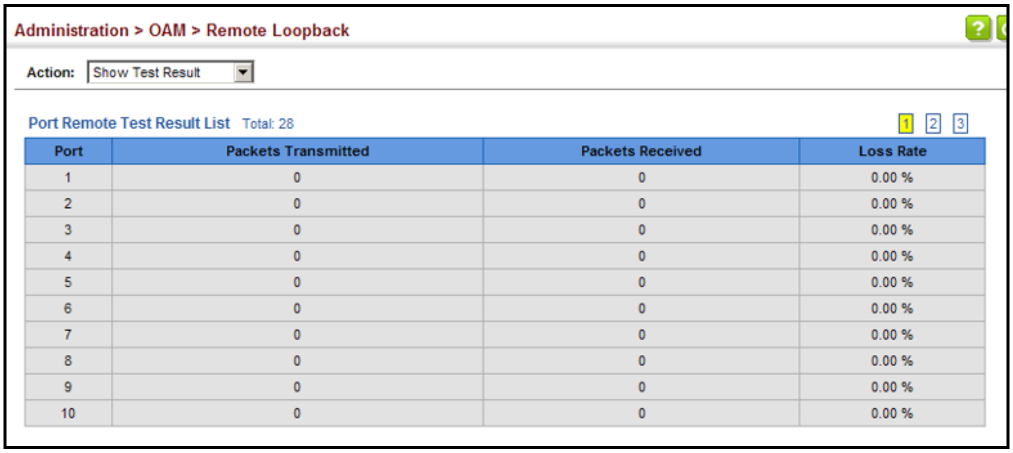
WEB INTERFACE

To display the results of remote loop back testing for each port for which this information is available:

1. Click Administration, OAM, Remote Loop Back.

2. Select Show Test Result from the Action list.

Figure 329: Displaying the Results of Remote Loop Back Testing



Administration > OAM > Remote Loopback

Action: Show Test Result

Port Remote Test Result List Total: 28

Port	Packets Transmitted	Packets Received	Loss Rate
1	0	0	0.00 %
2	0	0	0.00 %
3	0	0	0.00 %
4	0	0	0.00 %
5	0	0	0.00 %
6	0	0	0.00 %
7	0	0	0.00 %
8	0	0	0.00 %
9	0	0	0.00 %
10	0	0	0.00 %

PTP CONFIGURATION

Precision Time Protocol (PTP) provides high-precision time synchronization at an accuracy within the sub-microsecond range. PTP Version 2 (based on IEEE 1588-2008) is used to provide clock synchronization for measurement and control systems in a local area network.

PTP uses a hierarchical master-slave architecture for clock distribution, where the distribution system consists of one or more network segments, and one or more clocks. An ordinary clock has a single network connection and is either the source of (i.e., master) or destination for (i.e, slave) a synchronization reference. A boundary clock has multiple network connections and can accurately bridge time synchronization from one network segment to another. A synchronization master is elected for each network segment in the system. The root timing reference is called the grandmaster. The grandmaster transmits synchronization information to the clocks residing on its network segment. The boundary clocks on that segment then relay accurate time to the other segments to which they are also connected.

CONFIGURING GLOBAL SETTINGS FOR PTP

Use the Sync > PTP (Configure Global) page to set the operating mode, adjustment to received Sync messages, the preference level used to select the master clock, and clock synchronization domain to which the switch is assigned.

CLI REFERENCES

- "ptp mode" on page 963
- "ptp adjust" on page 961
- "ptp priority1" on page 965
- "ptp priority2" on page 966
- "ptp domain-number" on page 962
- "ptp e-latency" on page 962
- "ptp in-latency" on page 963

COMMAND USAGE

- When PTP mode is set to boundary clock, the delay mechanism is determined by the interface setting for this parameter (see "Configuring Interface Settings for PTP" on page 598). When set to transparent clock, the delay mechanism is determined by message exchanges with other clocks in the PTP domain.

PARAMETERS

These parameters are displayed:

- **PTP Mode** – Sets the operating mode to one of the following options:
  - **Disable** – Disables PTP on the switch. (This is the default setting.)
  - **Boundary** – A boundary clock can have multiple network connections and can accurately bridge synchronization from one network segment to another.

    Setting the switch to boundary mode allows it to participate in the selection of the best master clock. If no better clock is detected, it will become the grandmaster clock within its PTP domain, and the parent clock to all connected devices. However, if the best master clock is found to be a another clock connected to the switch, the switch will synchronize to that clock as its child, and then acts as the parent clock to devices connected to other ports. After initial synchronization, the switch and connected devices exchange timing messages to correct for time skew caused by clock offsets and network delays.
  - **Transparent** – A transparent clock modifies PTP messages as they pass through the switch, updating the time stamps to correct for time spent traversing the network.
    - **End-to-End** – This method measures the residence time required for PTP event messages to cross from the input port to the output port, and adjusts the time stamp to compensate for this delay. The value of the correction update and checksums are specific to each output port and message since the residence

time are not necessarily the same for all paths through the switch or for successive messages crossing the same path.

Setting the switch to end-to-end transparent mode makes it synchronize all ports with the grand master clock connected to the switch. The switch corrects PTP message time stamps for the delay incurred passing through it. This option causes less jitter and error accumulation than that incurred when using boundary mode.

- **Peer-to-Peer** – This method measures the delay required for PTP event messages to cross the link from the peer port on the upstream device to the input port on the switch, as well as the residence time required for PTP event messages to cross from the input port to the output port, and adjusts the time stamp to compensate for both of these delay times.

  Setting the switch to peer-to-peer transparent mode differs with end-to-end transparent mode only in the way it corrects and handles PTP timing messages. Unlike the end-to-end clock, which corrects and forwards all PTP timing messages, the peer-to-peer clock only corrects and forwards Sync and Follow_Up messages. These messages are updated for both the residence time of the Sync message and link delay on the port receiving the Sync message.

- **Adjust** – When this parameter is enabled, the switch will adjust the time of the local clock to match that of the master clock, based on information in received Sync messages. (Default: Disabled)

  When synchronization is enabled is thus enabled, the switch will exchange PTP timing messages on the communication path to the master clock. By exchanging Sync, Follow_Up, Delay_Req, and Delay_Resp messages, the switch calculates the offset of the slave's clock with respect to the master clock. It then adjusts the time reported in the received Sync message, ensuring that the offset from the master clock listed in the Current Data Set is now zero (see Show PTP Information – Current Data).

- **Priority1** – Sets a preference level used by slave devices in selecting the master clock. Slave devices use the priority1 value when selecting a master clock. (Range: 0-255; Default: 128)

  - Specify the Priority1 preference level to override the default criteria for best master clock selection. Lower values take precedence.

  - The best master clock algorithm (BMC), performs a distributed selection of the best candidate clock based on the following clock properties.

    - Priority – An administratively assigned precedence hint used by the BMC to help select a grandmaster for the PTP domain.
    - Class – An attribute defining the clock's International Atomic Time (TAI) traceability.
    - Accuracy – An attribute defining the accuracy of the clock.

    - Variance – A clock's estimate of its stability based on observation of its performance against the PTP reference.
    - Quality – Clock quality based on expected timing deviation, technology used to implement the clock, or location in a stratum schema.
    - Identifier – A universally unique numeric identifier for the clock. This is typically constructed based on a device's MAC address.
  - PTP uses a hierarchical selection algorithm based on the following properties in the order indicated.
    - Priority 1
    - Class
    - Accuracy
    - Variance
    - Priority 2
    - Unique identifier (tie breaker)

- **Priority2** – Sets a secondary preference level used by slave devices in selecting the master clock. (Range: 0-255; Default: 128)

  The Priority2 preference is only considered when it not possible to use Priority1 and other clock attributes to select a best master clock.

- **Domain Number** – Specifies the PTP clock synchronization domain to which the switch belongs. (Range: 0-255; Default: 0)

  A domain is a set of clocks that synchronize to one another using PTP.

  Multiple independent PTP clocking domains can be configured on a single network, but a device can only belong to one domain.

- **Ingress Latency** – The ingress latency is added to the actual timestamp of ingress PTP messages. Failure to make this correction will result in a time offset between the slave and master clocks. (Range: 0-1000000 nanoseconds; Default: 0 nanoseconds)

- **Egress Latency** – The egress latency is added to the actual timestamp of egress PTP messages. Failure to make this correction will result in a time offset between the slave and master clocks. (Range: 0-1000000 nanoseconds; Default: 0 nanoseconds)

WEB INTERFACE

To configure global settings for PTP:

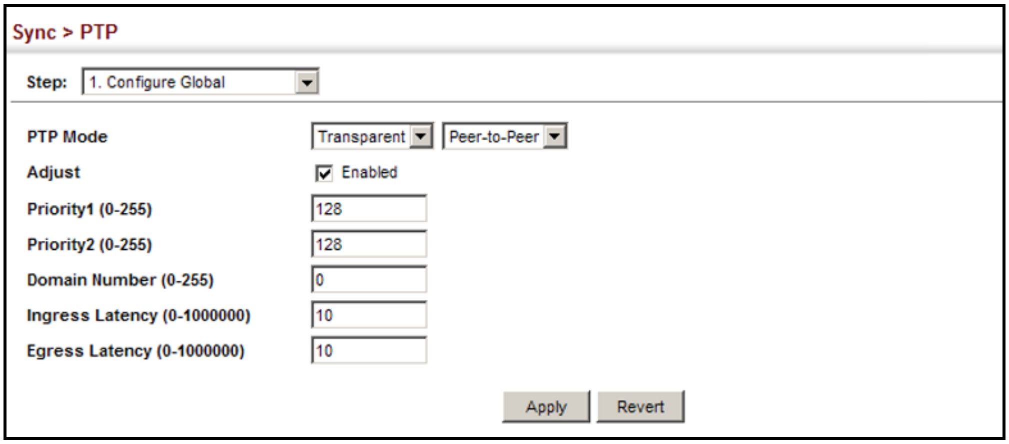
1. Click Sync, PTP.

2. Select Configure Global from the Step list.

3. Select the mode to the required clock type, enable local adjustment of received timing information, configure the priorities used in selecting the best master clock, and then specify the PTP domain to which this switch is assigned.

4. Click Apply.

Figure 330: Configuring Global Settings for PTP



Sync > PTP

Step: 1. Configure Global

PTP Mode: Transparent, Peer-to-Peer
Adjust: ☑ Enabled
Priority1 (0-255): 128
Priority2 (0-255): 128
Domain Number (0-255): 0
Ingress Latency (0-1000000): 10
Egress Latency (0-1000000): 10

CONFIGURING INTERFACE SETTINGS FOR PTP

Use the Sync > PTP (Configure Interface) page to set the interface-level administrative state, delay mechanism, transport mode, and timing attributes.

CLI REFERENCES

- "ptp port-enable" on page 971
- "ptp delay-mechanism" on page 967
- "ptp transport" on page 971
- "ptp log-sync-interval" on page 970
- "ptp log-announce-interval" on page 968
- "ptp announce-receipt-timeout" on page 966
- "ptp log-min-pdelay-request-interval" on page 969
- "ptp log-min-delay-request-interval" on page 969
- "ptp port-release" on page 973

COMMAND USAGE

- When the PTP mode is set to boundary clock under Global Configuration, the Delay Mechanism is determined by the setting for this parameter on the Interface Configuration page. When PTP mode is set to transparent clock, the delay mechanism is determined by message exchanges with other clocks in the PTP domain.

- For more information, refer to the Command Usage section under the "Configuring Global Settings for PTP" on page 595.

PARAMETERS

These parameters are displayed:

- **Interface** – Port or Trunk Identifier.

- **Port State** – Enables PTP capability on a port. (Default: Disabled)

- **Delay Mechanism** – Sets the delay measurement method for a boundary clock to one of the following options:
  - **End-to-End** – This method measures the residence time required for PTP event messages to cross from the input port to the output port, and adjusts the time stamp to compensate for this delay. The value of the correction update and checksums are specific to each output port and message since the residence time are not necessarily the same for all paths through the switch or for successive messages crossing the same path.
  - **Peer-to-Peer** – This method measures the delay required for PTP event messages to cross the link from the peer port on the upstream device to the input port on the switch, as well as the residence time required for PTP event messages to cross from the input port to the output port, and adjusts the time stamp to compensate for both of these delay times.
- **Transport** – Sets the message transport method to one of the following options:
  - **Ethernet** – PTP messages are transmitted using Ethernet format.

    When using Ethernet as the transport mechanism, PTP messages use Ethernet formatted packets with the 88F7 Ethertype. PTP messages use MAC addresses as specified below.

Table 40: Ethernet Multicast MAC Addresses

Message Types	Address (hex)
All except peer delay mechanism messages	01-1B-19-00-00-00
Peer delay mechanism messages	01-80-C2-00-00-0E

  - **IPv4 UDP** – PTP messages are transmitted using UDP over IPv4.

    When using UDP over IPv4 as a transport mechanism, the following UDP destination ports are reserved values assigned to PTP.

Table 41: UDP/IPv4 Destination Port Numbers

Message Types	UDP Port Number
Event message	319
Multicast general message	320
Unicast general message addressed to a clock	320

When using UDP over IPv4 as a transport mechanism, PTP messages use the multicast addresses as specified below.

Table 42: UDP/IPv4 Multicast Addresses

Message Types	Address
All except peer delay mechanism messages	224.0.1.129
Peer delay mechanism messages	224.0.0.107

- **IPv6 UDP** – PTP messages are transmitted using UDP over IPv6.

  When using UDP over IPv6 as a transport mechanism, the following UDP destination ports are reserved values assigned to PTP.

  Table 43: UDP/IPv6 Destination Port Numbers

Message Types	UDP Port Number
Event message	319
Multicast general message	320
Unicast general message addressed to a clock	320

  When using UDP over IPv6 as a transport mechanism, PTP messages use the multicast addresses as specified below.

  Table 44: UDP/IPv6 Multicast Addresses

Message Types	Address
All except peer delay mechanism messages	FF0X:0:0:0:0:0:0:183
Peer delay mechanism messages	FF02:0:0:0:0:0:0:6B

- **Log Sync Interval** – Sets the minimum interval between the transmission of (multicast) synchronization messages. (Range: -1 - 1 in log base 2; Default: 0)

  The log base 2 settings equate to the following values:

  - - 1 – 1 packet every 1/2 second
  - 0 – 1 packet every second
  - 1 – 1 packet every 2 seconds

  Synchronization messages are used to synchronize clocks within the same PTP domain. A boundary or transparent clock in slave state will synchronize to its master in the synchronization hierarchy established by the best master clock algorithm.

- **Log Announce Interval** – Sets the PTP announcement message transmit interval. (Range: 0-4 in log base 2)

  The log base 2 settings equate to the following values:

  - 0 – 1 packet every second
  - 1 – 1 packet every 2 seconds
  - 2 – 1 packet every 4 seconds
  - 3 – 1 packet every 8 seconds
  - 4 – 1 packet every 16 seconds

  It may be necessary for the announcement interval to be different in networks which employ different communication technologies, such as wired or wireless. Systems where the announcement interval varies from region to region will still function correctly. However, regions with short intervals may experience more reconfiguration events while waiting for slower regions to select master clocks.

- **Announce Receipt Timeout** – Sets the transmit timeout for PTP announcement messages. This parameter indicates the number of PTP announce message intervals which have to expire without the receipt of a announce message before the session times out. (Range: 2-10; Default: 3)

- **Log Min Pdelay Req Interval** – Sets the peer delay request message transmit interval. This parameter indicates the minimum interval between peer delay request messages used to measure the link delay between two clock ports implementing the peer-to-peer delay mechanism. (Range: 0-5 in log base 2; Default: 0)

  The log base 2 settings equate to the following values:

  - 0 – 1 packet every second
  - 1 – 1 packet every 2 seconds
  - 2 – 1 packet every 4 seconds
  - 3 – 1 packet every 8 seconds
  - 4 – 1 packet every 16 seconds
  - 5 – 1 packet every 32 seconds

  This parameter is only applicable for interfaces which are set to use the peer-to-peer delay mechanism.

- **Log Min Delay Req Interval** – Sets the delay request message transmit interval. This parameter indicates the minimum interval between delay request messages sent by a slave clock to a specific port on the master clock. (Range: 0-5 in log base 2)

  The log base 2 settings equate to the following values:

  - 0 – 1 packet every second
  - 1 – 1 packet every 2 seconds
  - 2 – 1 packet every 4 seconds
  - 3 – 1 packet every 8 seconds
  - 4 – 1 packet every 16 seconds
  - 5 – 1 packet every 32 seconds

  This value is determined and advertised by a master clock based on its ability to process delay request message traffic.

- **Port Release** – Returns a port to PTP enabled state after having been disabled by a PTP management message.

  Check the "Port State" field displayed by the Show PTP Information – Port Data page to see if a port has been disabled by a PTP management message.

WEB INTERFACE

To configure interface settings for PTP:

1. Click Sync, PTP.

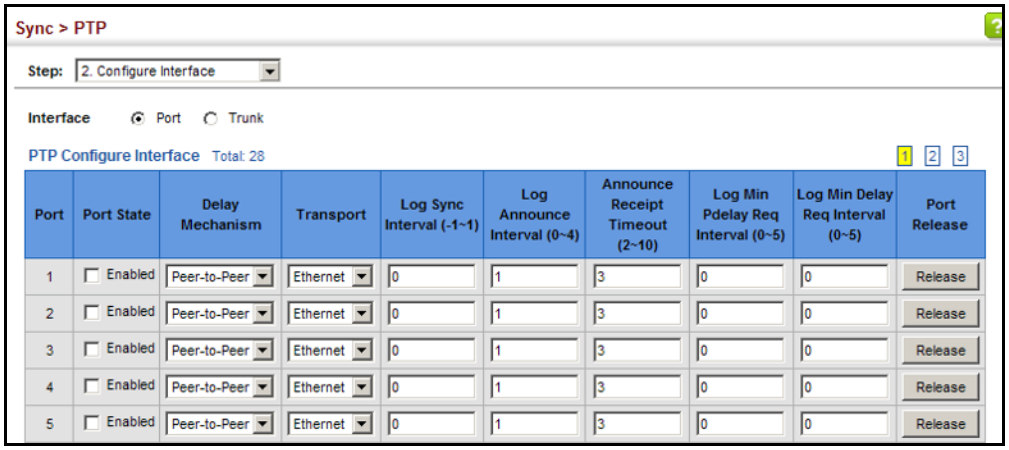
2. Select Configure Interface from the Step list.

3. Select Port or Trunk from the Interface options.

4. Set the operational state for each port, the message transport mechanism, and the timing attributes.

5. Click Apply.

Figure 331: Configuring Interface Settings for PTP



Sync > PTP

Step: 2. Configure Interface

Interface ● Port ○ Trunk

PTP Configure Interface Total: 28

Port	Port State	Delay Mechanism	Transport	Log Sync Interval (-1~1)	Log Announce Interval (0~4)	Announce Receipt Timeout (2~10)	Log Min Pdelay Req Interval (0~5)	Log Min Delay Req Interval (0~5)	Port Release
1	□ Enabled	Peer-to-Peer	Ethernet	0	1	3	0	0	Release
2	□ Enabled	Peer-to-Peer	Ethernet	0	1	3	0	0	Release
3	□ Enabled	Peer-to-Peer	Ethernet	0	1	3	0	0	Release
4	□ Enabled	Peer-to-Peer	Ethernet	0	1	3	0	0	Release
5	□ Enabled	Peer-to-Peer	Ethernet	0	1	3	0	0	Release

SHOWING PTP INFORMATION

Use the Sync > PTP (Show PTP Information) page to show the default data settings, current data set, parent data set, time properties, and port-related data.

CLI REFERENCES

- "show ptp information" on page 975

PARAMETERS

These parameters are displayed:

Default Data

- Two Step Flag – Shows if this device is a two-step clock. A two-step clock sends a time stamp in a Follow_Up message, while a one-step clock sends a time stamp in a Sync message.

- Clock Identity – A unique 8-octet array based on the IEEE EUI-64 assigned numbers.

- Number Ports – Number of PTP ports on this device.

- Clock Quality – A set of attributes defining the clock’s relative quality.

  - Clock Class – An attribute defining the clock’s International Atomic Time (TAI) traceability.

  - Clock Accuracy – An attribute defining the accuracy of the clock.

  - Offset Scaled Log Variance – An attribute defining the stability of the clock.

- Priority1 – A preference level used in selecting the master clock.

- Priority2 – A secondary preference level used in selecting the master clock.

- Domain Number – PTP clock synchronization domain.

- Slave Only – Shows if this device is operating in slave-only mode. (This operation mode is not supported by this device.)

Current Data

- Steps Removed – Number of steps (clock hops) from the grand master.

- Offset From Master – Time offset from the grand master.

- Mean Path Delay – Mean path delay from the grand master.

Parent Data

- Parent Identity – Parent identity information.

  - Clock Identity – A unique 8-octet array based on the IEEE EUI-64 assigned numbers.

  - Port Number – Port connected to the parent clock. (This attribute indicates a number from the sequence of ports supporting PTP, not a physical port number.)

- Observed Offset Scaled Log Variance – The variance of the parent's clock phase as measured by the local clock.

- Observed Clock Phase Change Rate – The variance of the parent's clock phase change rate as measured by the slave clock.

- Grandmaster Identity – A unique 8-octet array based on the IEEE EUI-64 assigned numbers

- Grandmaster Clock Quality

  - Clock Class – An attribute defining the clock's International Atomic Time (TAI) traceability.

  - Clock Accuracy – An attribute defining the accuracy of the clock.

  - Offset Scaled Log Variance – An attribute defining the stability of the clock

- Grandmaster Priority1 – A preference level used in selecting the grand master clock.

- Grandmaster Priority2 – A secondary preference level used in selecting the grand master clock.

Time Properties

- Current UTC Offset – Current offset between TAI (International Atomic Time) and UTC (Coordinated Universal Time).
- Current UTC Offset Valid – Indicates if the current UTC offset is known to be correct.
- Leap59 – Indicates if the last minute of the UTC day contains 59 seconds.
- Leap61 – Indicates if the last minute of the UTC day contains 61 seconds.
- Time Traceable – Indicates if the time scale of value of the current UTC offset are traceable to a primary reference.
- Frequency Traceable – Indicates if the frequency determining the time scale is traceable to a primary reference.
- PTP Timescale – Indicates if the clock time scale of the grand master clock is PTP.
- Time Source – The source of time used by the grand master clock.

Port Data

- Port Enabled – Shows if PTP is enabled on this port.
- Port Identity – Port identity information.
  - Clock Identity – A unique 8-octet array based on the IEEE EUI-64 assigned numbers.
  - Port Number – Port on the local switch.
- Boundary Clock – A clock at the domain boundary used to bridge synchronization from one network segment to another.
  - Port State – Shows if device is in master or slave state.
  - Log Min Delay Req. Interval – Delay request message transmit interval (log value).
  - Peer Mean Path Delay – Mean path delay between upstream peer and this device.
  - Announce Receipt Timeout – Transmit timeout for PTP announcement messages.

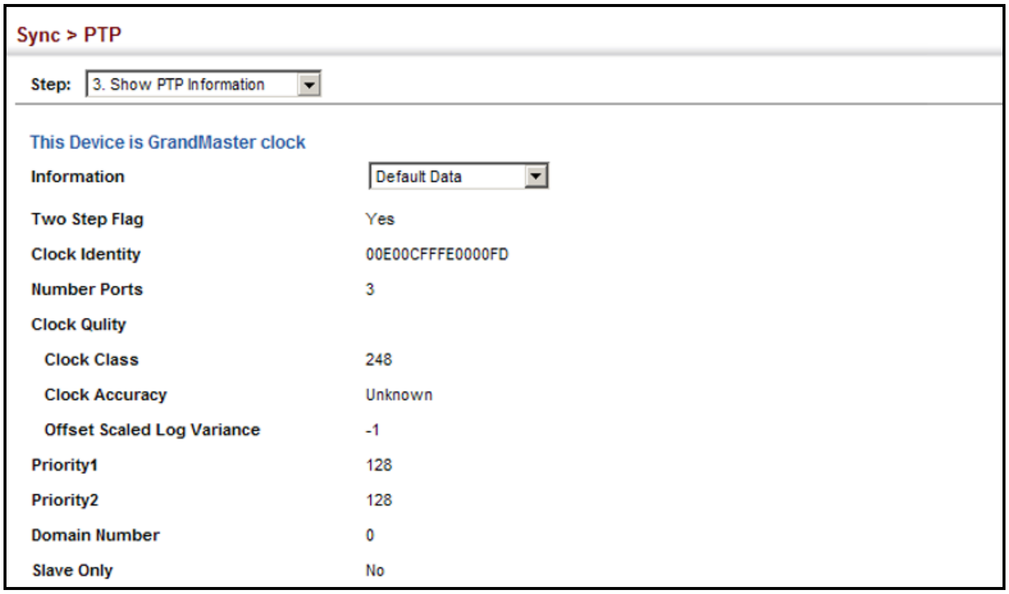
- Log Announce Interval – Announcement message transmit interval (log value).
- Log Sync Interval – Synchronization message transmit interval (log value).
- Delay Mechanism – Time delay measurement method (end-to-end or peer-to-peer).
- Log Min Pdelay Req. Interval – Peer delay request message transmit interval.
- Version Number – PTP version number (1 or 2).

WEB INTERFACE

To display default data and negotiated settings for PTP:

1. Click Sync, PTP.
2. Select Show PTP Information from the Step list.
3. Select any of the options from the Information box.

Figure 332: Displaying PTP Information (Default Data)



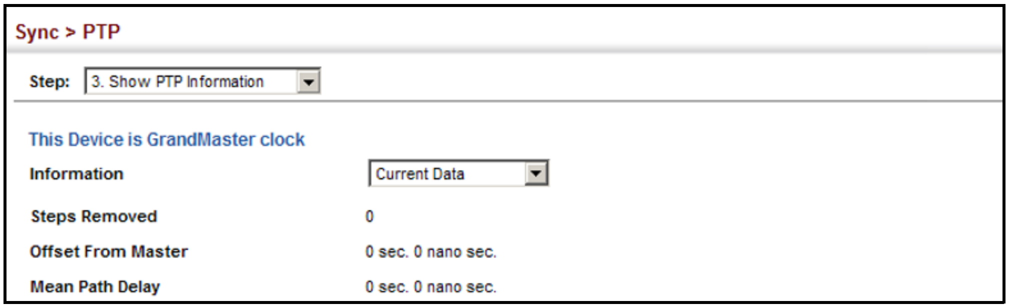
Sync > PTP

Step: 3. Show PTP Information

This Device is GrandMaster clock

Information	Default Data
Two Step Flag	Yes
Clock Identity	00E00CFFFE0000FD
Number Ports	3
Clock Qulity	
Clock Class	248
Clock Accuracy	Unknown
Offset Scaled Log Variance	-1
Priority1	128
Priority2	128
Domain Number	0
Slave Only	No

Figure 333: Displaying PTP Information (Current Data)



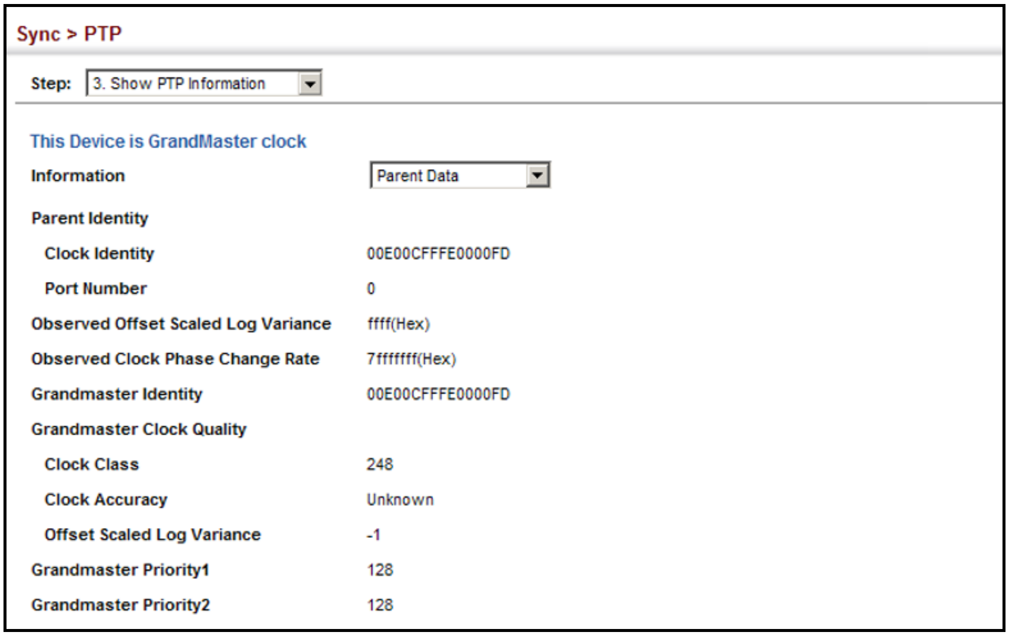
Sync > PTP

Step: 3. Show PTP Information

This Device is GrandMaster clock

Information	Current Data
Steps Removed	0
Offset From Master	0 sec. 0 nano sec.
Mean Path Delay	0 sec. 0 nano sec.

Figure 334: Displaying PTP Information (Parent Data)



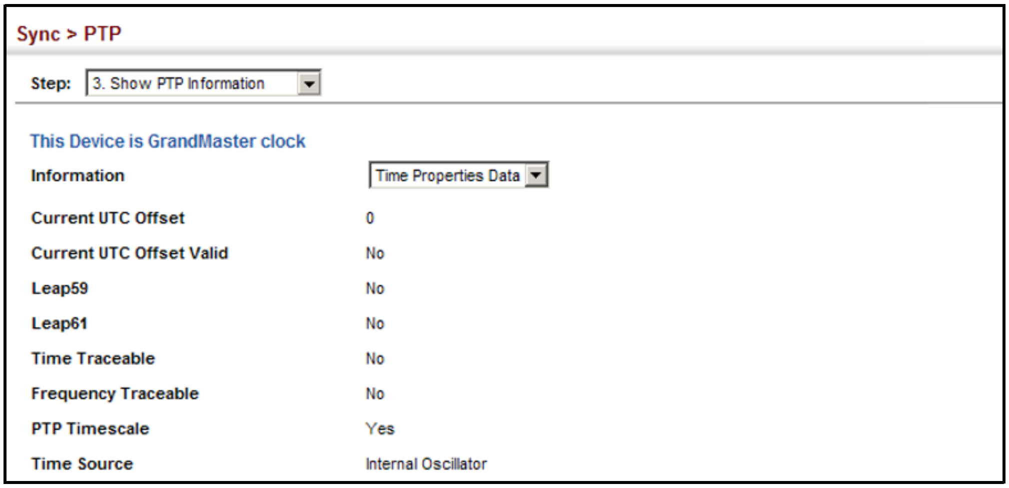
Sync > PTP

Step: 3. Show PTP Information

This Device is GrandMaster clock

Information	Parent Data
Parent Identity	
Clock Identity	00E00CFFFE0000FD
Port Number	0
Observed Offset Scaled Log Variance	ffff(Hex)
Observed Clock Phase Change Rate	7fffffff(Hex)
Grandmaster Identity	00E00CFFFE0000FD
Grandmaster Clock Quality	
Clock Class	248
Clock Accuracy	Unknown
Offset Scaled Log Variance	-1
Grandmaster Priority1	128
Grandmaster Priority2	128

Figure 335: Displaying PTP Information (Time Properties)



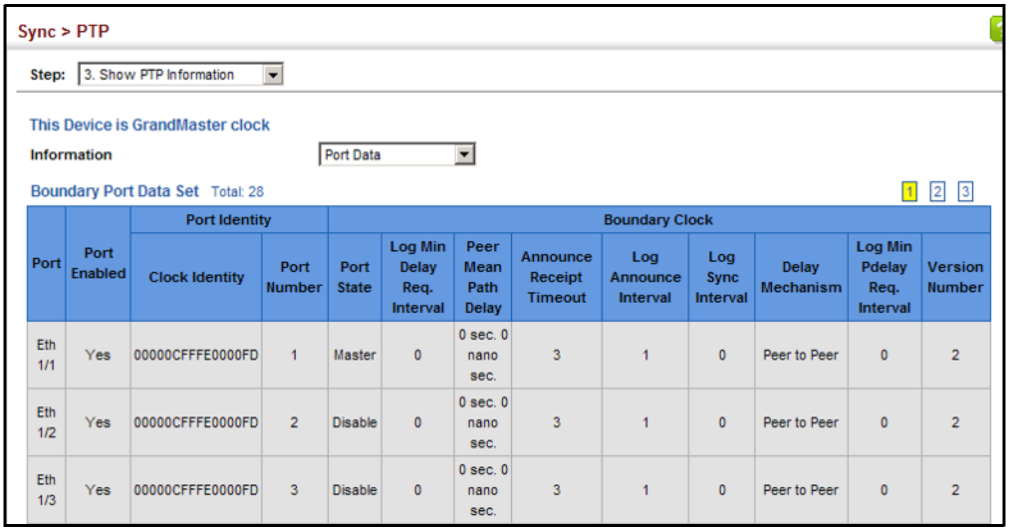
Sync > PTP

Step: 3. Show PTP Information

This Device is GrandMaster clock

Information	Time Properties Data
Current UTC Offset	0
Current UTC Offset Valid	No
Leap59	No
Leap61	No
Time Traceable	No
Frequency Traceable	No
PTP Timescale	Yes
Time Source	Internal Oscillator

Figure 336: Displaying PTP Information (Port Data)



Step: 3. Show PTP Information

This Device is GrandMaster clock

Information: Port Data

Boundary Port Data Set Total: 28

		Port Identity		Boundary Clock								
Port	Port Enabled	Clock Identity	Port Number	Port State	Log Min Delay Req. Interval	Peer Mean Path Delay	Announce Receipt Timeout	Log Announce Interval	Log Sync Interval	Delay Mechanism	Log Min Pdelay Req. Interval	Version Number
Eth 1/1	Yes	00000CFFFE0000FD	1	Master	0	0 sec. 0 nano sec.	3	1	0	Peer to Peer	0	2
Eth 1/2	Yes	00000CFFFE0000FD	2	Disable	0	0 sec. 0 nano sec.	3	1	0	Peer to Peer	0	2
Eth 1/3	Yes	00000CFFFE0000FD	3	Disable	0	0 sec. 0 nano sec.	3	1	0	Peer to Peer	0	2

SHOWING PTP FOREIGN MASTER

Use the Sync > PTP (Show PTP Foreign Master) page to show PTP announcements from neighbors.

CLI REFERENCES

- "show ptp foreign-master" on page 974

PARAMETERS

These parameters are displayed:

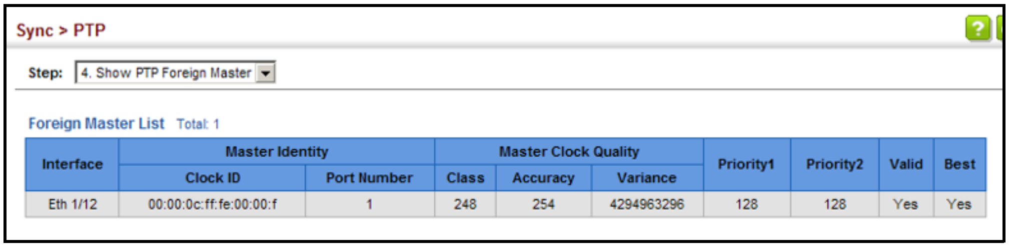
- **Interface** – Interface through which this message was received.
- **Master Identity** – A unique 8-octet array based on the IEEE EUI-64 assigned clock identifier numbers, and the port number.
- **Master Clock Quality** – The reported clock quality components include:
  - **Class** – Clock class defines the clock’s International Atomic Time (TAI) traceability.
  - **Accuracy** – Clock accuracy defines the accuracy of the clock.
  - **Variance** – Clock variance defines the stability of the clock.
- **Priority1** – A preference level used in selecting the master clock.
- **Priority2** – A secondary preference level used in selecting the master clock.
- **Valid** – This record is used to calculate Best master clock.
- **Best** – This record is the best record of all foreign masters.

WEB INTERFACE

To show PTP announcements from neighbors:

1. Click Sync, PTP.
2. Select Show PTP Foreign Master from the Step list.

Figure 337: Displaying PTP Neighbor Information



Sync > PTP

Step: 4. Show PTP Foreign Master

Foreign Master List Total: 1

Interface	Master Identity		Master Clock Quality			Priority1	Priority2	Valid	Best
	Clock ID	Port Number	Class	Accuracy	Variance				
Eth 1/12	00:00:0c:ff:fe:00:00:f	1	248	254	4294963296	128	128	Yes	Yes

15 Multicast Filtering

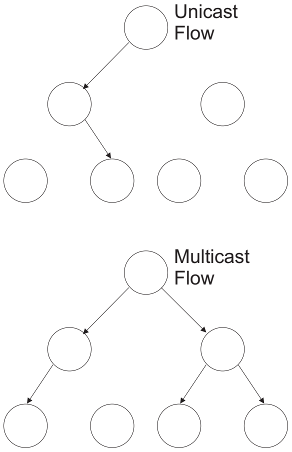
This chapter describes how to configure the following multicast services:

- IGMP Snooping – Configures snooping and query parameters for IPv4.
- Filtering and Throttling – Filters specified multicast service, or throttling the maximum of multicast groups allowed on an interface for IPv4.
- MLD Snooping – Configures snooping and query parameters for IPv6.
- Layer 3 IGMP – Configures IGMP query used with multicast routing.
- Multicast VLAN Registration for IPv4 – Configures a single network-wide multicast VLAN shared by hosts residing in other standard or private VLAN groups, preserving security and data isolation.
- Multicast VLAN Registration for IPv6 – Configures a single network-wide multicast VLAN shared by hosts residing in other standard or private VLAN groups, preserving security and data isolation.

Overview

Multicasting is used to support real-time applications such as video conferencing or streaming audio. A multicast server does not have to establish a separate connection with each client. It merely broadcasts its service to the network, and any hosts that want to receive the multicast register with their local multicast switch/router. Although this approach reduces the network overhead required by a multicast server, the broadcast traffic must be carefully pruned at every multicast switch/router it passes through to ensure that traffic is only passed on to the hosts which subscribed to this service.

Figure 338: Multicast Filtering Concept



This switch can use Internet Group Management Protocol (IGMP) to filter multicast traffic. IGMP Snooping can be used to passively monitor or “snoop” on exchanges between attached hosts and an IGMP-enabled device, most commonly a multicast router. In this way, the switch can discover the ports that want to join a multicast group, and set its filters accordingly.

If there is no multicast router attached to the local subnet, multicast traffic and query messages may not be received by the switch. In this case IGMP Query can be used to actively ask the attached hosts if they want to receive a specific multicast service. IGMP Query thereby identifies the ports containing hosts requesting to join the service and sends data out to those ports only. It then propagates the service request up to any neighboring multicast switch/router to ensure that it will continue to receive the multicast service.

The purpose of IP multicast filtering is to optimize a switched network’s performance, so multicast packets will only be forwarded to those ports containing multicast group hosts or multicast routers/switches, instead of flooding traffic to all ports in the subnet (VLAN).

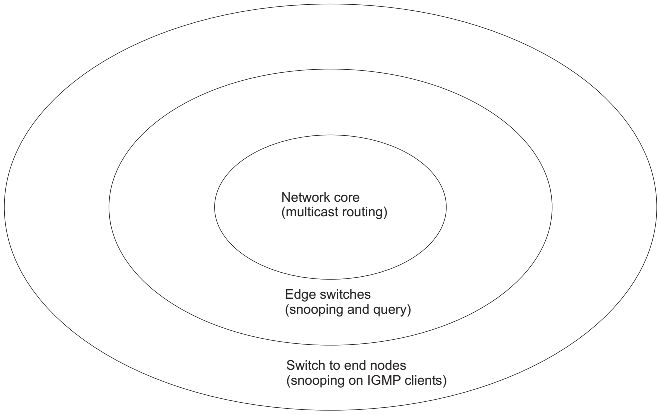
This switch not only supports IP multicast filtering by passively monitoring IGMP query, report messages and multicast routing probe messages to register end-stations as multicast group members, but also supports the Protocol Independent Multicasting (PIM) routing protocol required to forward multicast traffic to other subnets (page 1927).

You can also configure a single network-wide multicast VLAN shared by hosts residing in other standard or private VLAN groups, preserving security and data isolation "Multicast VLAN Registration for IPv4" on page 657.

IGMP PROTOCOL

The Internet Group Management Protocol (IGMP) runs between hosts and their immediately adjacent multicast router/switch. IGMP is a multicast host registration protocol that allows any host to inform its local router that it wants to receive transmissions addressed to a specific multicast group. A router, or multicast-enabled switch, can periodically ask their hosts if they want to receive multicast traffic. If there is more than one router/switch on the LAN performing IP multicasting, one of these devices is elected "querier" (at Layer 3) and assumes the role of querying the LAN for group members. It then propagates the service requests on to any adjacent multicast switch/router to ensure that it will continue to receive the multicast service. Based on the group membership information learned from IGMP, a router/switch can determine which (if any) multicast traffic needs to be forwarded to each of its ports. At Layer 3, multicast routers use this information, along with a multicast routing protocol such as Protocol Independent Multicasting (PIM), to support IP multicasting across the Internet. Note that IGMP neither alters nor routes IP multicast packets. A multicast routing protocol must be used to deliver IP multicast packets across different subnetworks. Therefore, when PIM routing is enabled for a subnet on the switch, IGMP is automatically enabled.

Figure 339: IGMP Protocol



LAYER 2 IGMP (SNOOPING AND QUERY FOR IPV4)

IGMP Snooping and Query – If multicast routing is not supported on other switches in your network, you can use IGMP Snooping and IGMP Query (page 613) to monitor IGMP service requests passing between multicast clients and servers, and dynamically configure the switch ports which need to forward multicast traffic. IGMP Snooping conserves bandwidth on network segments where no node has expressed interest in receiving a specific multicast service. For switches that do not support multicast routing, or where multicast routing is already enabled on other switches in the local network segment, IGMP Snooping is the only service required to support multicast filtering.

When using IGMPv3 snooping, service requests from IGMP Version 1, 2 or 3 hosts are all forwarded to the upstream router as IGMPv3 reports. The primary enhancement provided by IGMPv3 snooping is in keeping track of information about the specific multicast sources which downstream IGMPv3 hosts have requested or refused. The switch maintains information about both multicast groups and channels, where a group indicates a multicast flow for which the hosts have *not* requested a specific source (the only option for IGMPv1 and v2 hosts unless statically configured on the switch), and a channel indicates a flow for which the hosts have requested service from a specific source. For IGMPv1/v2 hosts, the source address of a channel is always null (indicating that any source is acceptable), but for IGMPv3 hosts, it may include a specific address when requested.

Only IGMPv3 hosts can request service from a specific multicast source. When downstream hosts request service from a specific source for a multicast service, these sources are all placed in the Include list, and traffic is forwarded to the hosts from each of these sources. IGMPv3 hosts may also request that service be forwarded from any source except for those specified. In this case, traffic is filtered from sources in the Exclude list, and forwarded from all other available sources.

NOTE: When the switch is configured to use IGMPv3 snooping, the snooping version may be downgraded to version 2 or version 1, depending on the version of the IGMP query packets detected on each VLAN.

NOTE: IGMP snooping will not function unless a multicast router port is enabled on the switch. This can accomplished in one of two ways. A static router port can be manually configured (see "Specifying Static Interfaces for an IPv4 Multicast Router" on page 617). Using this method, the router port is never timed out, and will continue to function until explicitly removed. The other method relies on the switch to dynamically create multicast routing ports whenever multicast routing protocol packets or IGMP query packets are detected on a port.

NOTE: A maximum of up to 1024 multicast entries can be maintained for IGMP snooping and 255 entries for Multicast Routing when both of these features are enabled. Once the table is full, no new entries are learned. Any subsequent multicast traffic not found in the table is dropped if unregistered-flooding is disabled (default behavior) and no router port is configured in the attached VLAN, or flooded throughout the VLAN if unregistered-flooding is enabled (see "Configuring IGMP Snooping and Query Parameters" on page 613).

Static IGMP Router Interface – If IGMP snooping cannot locate the IGMP querier, you can manually designate a known IGMP querier (i.e., a multicast router/switch) connected over the network to an interface on your switch (page 617). This interface will then join all the current multicast groups supported by the attached router/switch to ensure that multicast traffic is passed to all appropriate interfaces within the switch.

Static IGMP Host Interface – For multicast applications that you need to control more carefully, you can manually assign a multicast service to specific interfaces on the switch (page 619).

IGMP Snooping with Proxy Reporting – The switch supports last leave, and query suppression (as defined in DSL Forum TR-101, April 2006):

- When proxy reporting is disabled, all IGMP reports received by the switch are forwarded natively to the upstream multicast routers.
- Last Leave: Intercepts, absorbs and summarizes IGMP leaves coming from IGMP hosts. IGMP leaves are relayed upstream only when necessary, that is, when the last user leaves a multicast group.
- Query Suppression: Intercepts and processes IGMP queries in such a way that IGMP specific queries are never sent to client ports.

The only deviation from TR-101 is that report suppression, and the marking of IGMP traffic initiated by the switch with priority bits as defined in R-250 is not supported.

CONFIGURING IGMP SNOOPING AND QUERY PARAMETERS

Use the Multicast > IGMP Snooping > General page to configure the switch to forward multicast traffic intelligently. Based on the IGMP query and report messages, the switch forwards multicast traffic only to the ports that request it. This prevents the switch from broadcasting the traffic to all ports and possibly disrupting network performance.

CLI REFERENCES

- "IGMP Snooping" on page 1426

COMMAND USAGE

- **IGMP Snooping** – This switch can passively snoop on IGMP Query and Report packets transferred between IP multicast routers/switches and IP multicast host groups to identify the IP multicast group members. It simply monitors the IGMP packets passing through it, picks out the group registration information, and configures the multicast filters accordingly.

NOTE: If unknown multicast traffic enters a VLAN which has been configured with a router port, the traffic is forwarded to that port. However, if no router port exists on the VLAN, the traffic is dropped if unregistered data flooding is disabled (default behavior), or flooded throughout the VLAN if unregistered data flooding is enabled (see “Unregistered Data Flood” in the Command Attributes section).

- **IGMP Querier** – A router, or multicast-enabled switch, can periodically ask their hosts if they want to receive multicast traffic. If there is more than one router/switch on the LAN performing IP multicasting, one of these devices is elected “querier” and assumes the role of querying the LAN for group members. It then propagates the service requests on to any upstream multicast switch/router to ensure that it will continue to receive the multicast service.

NOTE: Multicast routers use this information from IGMP snooping and query reports, along with a multicast routing protocol such as PIM, to support IP multicasting across the Internet.

PARAMETERS

These parameters are displayed:

- **IGMP Snooping Status** – When enabled, the switch will monitor network traffic to determine which hosts want to receive multicast traffic. This is referred to as IGMP Snooping. (Default: Enabled)

  When IGMP snooping is enabled globally, the per VLAN interface settings for IGMP snooping take precedence (see "Setting IGMP Snooping Status per Interface" on page 621).

  When IGMP snooping is disabled globally, snooping can still be configured per VLAN interface, but the interface settings will not take effect until snooping is re-enabled globally.

- **Proxy Reporting Status** – Enables IGMP Snooping with Proxy Reporting. (Default: Disabled)

  When proxy reporting is enabled with this command, the switch performs “IGMP Snooping with Proxy Reporting” (as defined in DSL Forum TR-101, April 2006), including last leave, and query suppression.

  Last leave sends out a proxy query when the last member leaves a multicast group, and query suppression means that specific queries are not forwarded from an upstream multicast router to hosts downstream from this device.

  When proxy reporting is disabled, all IGMP reports received by the switch are forwarded natively to the upstream multicast routers.

- **TCN Flood** – Enables flooding of multicast traffic if a spanning tree topology change notification (TCN) occurs. (Default: Disabled)

  When a spanning tree topology change occurs, the multicast membership information learned by switch may be out of date. For example, a host linked to one port before the topology change (TC) may be moved to another port after the change. To ensure that multicast data is delivered to all receivers, by default, a switch in a VLAN (with IGMP snooping enabled) that receives a Bridge Protocol Data Unit (BPDU) with TC bit set (by the root bridge) will enter into “multicast flooding mode” for a period of time until the topology has stabilized and the new locations of all multicast receivers are learned.

  If a topology change notification (TCN) is received, and all the uplink ports are subsequently deleted, a time out mechanism is used to delete all of the currently learned multicast channels.

  When a new uplink port starts up, the switch sends unsolicited reports for all currently learned channels out the new uplink port.

  By default, the switch immediately enters into “multicast flooding mode” when a spanning tree topology change occurs. In this mode, multicast traffic will be flooded to all VLAN ports. If many ports have subscribed to different multicast groups, flooding may cause excessive packet loss on the link between the switch and the end host. Flooding may be disabled to avoid this, causing multicast traffic to be delivered only to those ports on which multicast group members have been learned. Otherwise, the time spent in flooding mode can be manually configured to reduce excessive loading.

When the spanning tree topology changes, the root bridge sends a proxy query to quickly re-learn the host membership/port relations for multicast channels. The root bridge also sends an unsolicited Multicast Router Discover (MRD) request to quickly locate the multicast routers in this VLAN.

The proxy query and unsolicited MRD request are flooded to all VLAN ports except for the receiving port when the switch receives such packets.

- **TCN Query Solicit** – Sends out an IGMP general query solicitation when a spanning tree topology change notification (TCN) occurs. (Default: Disabled)

  When the root bridge in a spanning tree receives a TCN for a VLAN where IGMP snooping is enabled, it issues a global IGMP leave message (or query solicitation). When a switch receives this solicitation, it floods it to all ports in the VLAN where the spanning tree change occurred. When an upstream multicast router receives this solicitation, it immediately issues an IGMP general query.

  A query solicitation can be sent whenever the switch notices a topology change, even if it is not the root bridge in spanning tree.

- **Router Alert Option** – Discards any IGMPv2/v3 packets that do not include the Router Alert option. (Default: Disabled)

  As described in Section 9.1 of RFC 3376 for IGMP Version 3, the Router Alert Option can be used to protect against DOS attacks. One common method of attack is launched by an intruder who takes over the role of querier, and starts overloading multicast hosts by sending a large number of group-and-source-specific queries, each with a large source list and the Maximum Response Time set to a large value.

  To protect against this kind of attack, (1) routers should not forward queries. This is easier to accomplish if the query carries the Router Alert option. (2) Also, when the switch is acting in the role of a multicast host (such as when using proxy routing), it should ignore version 2 or 3 queries that do not contain the Router Alert option.

- **Unregistered Data Flooding** – Floods unregistered multicast traffic into the attached VLAN. (Default: Disabled)

  Once the table used to store multicast entries for IGMP snooping and multicast routing is filled, no new entries are learned. If no router port is configured in the attached VLAN, and unregistered-flooding is disabled, any subsequent multicast traffic not found in the table is dropped, otherwise it is flooded throughout the VLAN.

- **Forwarding Priority** – Assigns a CoS priority to all multicast traffic. (Range: 0-7, where 7 is the highest priority)

  This parameter can be used to set a high priority for low-latency multicast traffic such as a video-conference, or to set a low priority for normal multicast traffic not sensitive to latency.

- **Version Exclusive** – Discards any received IGMP messages which use a version different to that currently configured by the IGMP Version attribute. (Default: Disabled)

- **IGMP Unsolicited Report Interval** – Specifies how often the upstream interface should transmit unsolicited IGMP reports when proxy reporting is enabled. (Range: 1-65535 seconds, Default: 400 seconds)

  When a new upstream interface (that is, uplink port) starts up, the switch sends unsolicited reports for all currently learned multicast channels via the new upstream interface.

  This command only applies when proxy reporting is enabled.

- **Router Port Expire Time** – The time the switch waits after the previous querier stops before it considers it to have expired. (Range: 1-65535, Recommended Range: 300-500 seconds, Default: 300)

- **IGMP Snooping Version** – Sets the protocol version for compatibility with other devices on the network. This is the IGMP Version the switch uses to send snooping reports. (Range: 1-3; Default: 2)

  This attribute configures the IGMP report/query version used by IGMP snooping. Versions 1 - 3 are all supported, and versions 2 and 3 are backward compatible, so the switch can operate with other devices, regardless of the snooping version employed.

- **Querier Status** – When enabled, the switch can serve as the Querier, which is responsible for asking hosts if they want to receive multicast traffic. This feature is not supported for IGMPv3 snooping. (Default: Disabled)

WEB INTERFACE

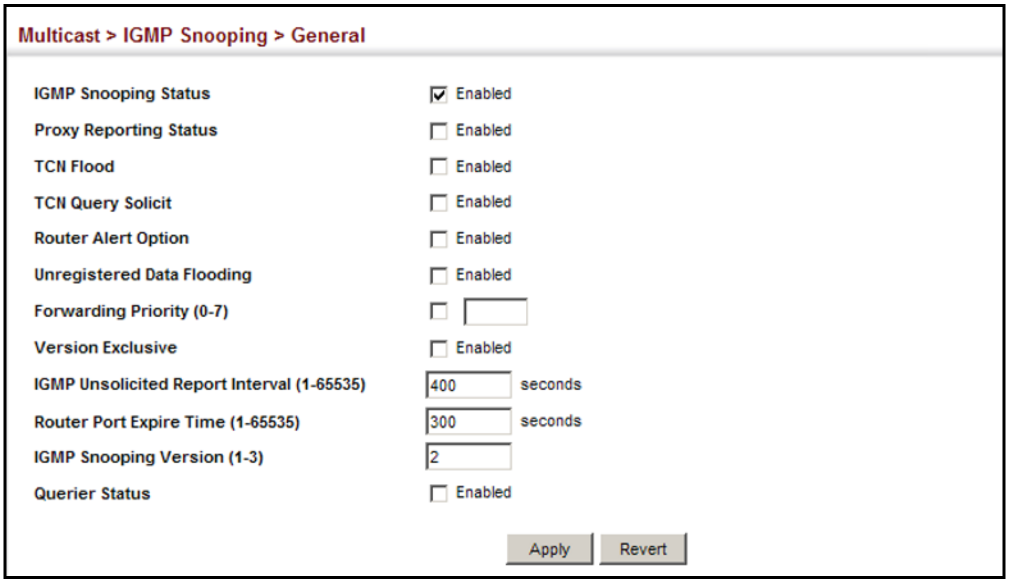
To configure general settings for IGMP Snooping and Query:

1. Click Multicast, IGMP Snooping, General.

2. Adjust the IGMP settings as required.

3. Click Apply.

Figure 340: Configuring General Settings for IGMP Snooping



Multicast > IGMP Snooping > General

IGMP Snooping Status	☑ Enabled
Proxy Reporting Status	□ Enabled
TCN Flood	□ Enabled
TCN Query Solicit	□ Enabled
Router Alert Option	□ Enabled
Unregistered Data Flooding	□ Enabled
Forwarding Priority (0-7)	□
Version Exclusive	□ Enabled
IGMP Unsolicited Report Interval (1-65535)	400 seconds
Router Port Expire Time (1-65535)	300 seconds
IGMP Snooping Version (1-3)	2
Querier Status	□ Enabled

Specifying Static Interfaces for an IPv4 Multicast Router

Use the Multicast > IGMP Snooping > Multicast Router (Add Static Multicast Router) page to statically attach an IPv4 interface to a multicast router/switch.

Depending on network connections, IGMP snooping may not always be able to locate the IGMP querier. Therefore, if the IGMP querier is a known multicast router/switch connected over the network to an interface (port or trunk) on the switch, the interface (and a specified VLAN) can be manually configured to join all the current multicast groups supported by the attached router. This can ensure that multicast traffic is passed to all the appropriate interfaces within the switch.

CLI References

- "Static Multicast Routing" on page 1446

Command Usage

IGMP Snooping must be enabled globally on the switch (see "Configuring IGMP Snooping and Query Parameters" on page 613) before a multicast router port can take effect.

Parameters

These parameters are displayed:

- **VLAN** – Selects the VLAN which is to propagate all multicast traffic coming from the attached multicast router. (Range: 1-4094)
- **Interface** – Activates the Port or Trunk scroll down list.
- **Port** or **Trunk** – Specifies the interface attached to a multicast router.

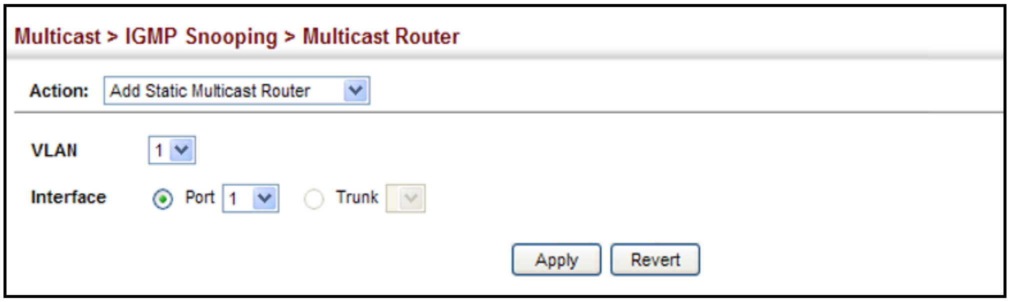
- **Type** (Show Current Multicast Router) – Shows if this entry is static or dynamic.
- **Expire** (Show Current Multicast Router) – Time until this dynamic entry expires.

WEB INTERFACE

To specify a static interface attached to a multicast router:

1. Click Multicast, IGMP Snooping, Multicast Router.
2. Select Add Static Multicast Router from the Action list.
3. Select the VLAN which will forward all the corresponding multicast traffic, and select the port or trunk attached to the multicast router.
4. Click Apply.

Figure 341: Configuring a Static Interface for an IPv4 Multicast Router



Multicast > IGMP Snooping > Multicast Router

Action: Add Static Multicast Router

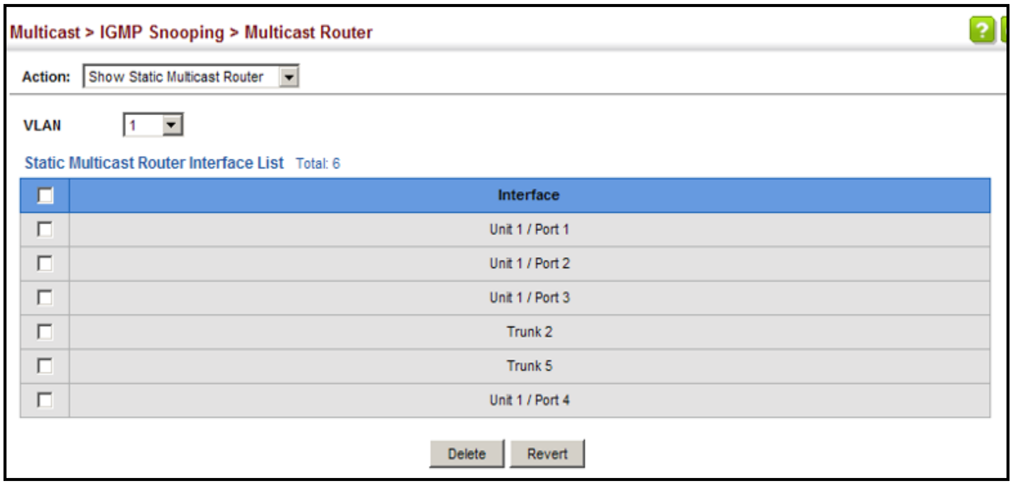
VLAN: 1

Interface: ● Port 1 ○ Trunk

To show the static interfaces attached to a multicast router:

1. Click Multicast, IGMP Snooping, Multicast Router.
2. Select Show Static Multicast Router from the Action list.
3. Select the VLAN for which to display this information.

Figure 342: Showing Static Interfaces Attached an IPv4 Multicast Router



Multicast > IGMP Snooping > Multicast Router

Action: Show Static Multicast Router

VLAN 1

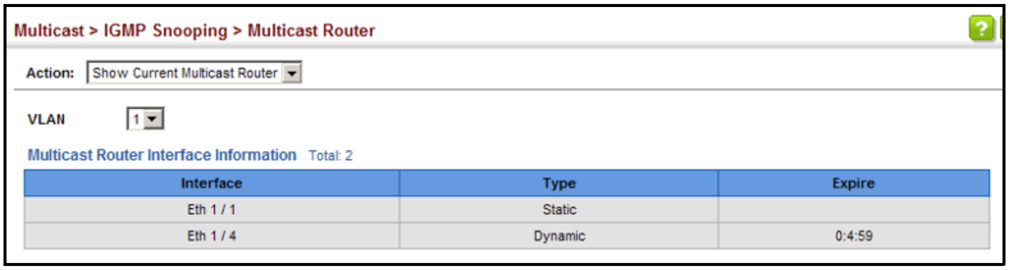
Static Multicast Router Interface List Total: 6

□	Interface
□	Unit 1 / Port 1
□	Unit 1 / Port 2
□	Unit 1 / Port 3
□	Trunk 2
□	Trunk 5
□	Unit 1 / Port 4

Multicast routers that are attached to ports on the switch use information obtained from IGMP, along with a multicast routing protocol (such as PIM) to support IP multicasting across the Internet. These routers may be dynamically discovered by the switch or statically assigned to an interface on the switch. To show all the interfaces attached to a multicast router:

1. Click Multicast, IGMP Snooping, Multicast Router.
2. Select Show Current Multicast Router from the Action list.
3. Select the VLAN for which to display this information. Ports in the selected VLAN which are attached to a neighboring multicast router/ switch are displayed.

Figure 343: Showing Current Interfaces Attached an IPv4 Multicast Router



Multicast > IGMP Snooping > Multicast Router

Action: Show Current Multicast Router

VLAN 1

Multicast Router Interface Information Total: 2

Interface	Type	Expire
Eth 1 / 1	Static	
Eth 1 / 4	Dynamic	0:4:59

Assigning Interfaces to IPv4 Multicast Services

Use the Multicast > IGMP Snooping > IGMP Member (Add Static Member) page to statically assign an IPv46 multicast service to an interface.

Multicast filtering can be dynamically configured using IGMP Snooping and IGMP Query messages (see "Configuring IGMP Snooping and Query Parameters" on page 613). However, for certain applications that require tighter control, it may be necessary to statically configure a multicast service on the switch. First add all the ports attached to participating hosts to a common VLAN, and then assign the multicast service to that VLAN group.

CLI References

- "ip igmp snooping vlan static" on page 1442

Command Usage

- Static multicast addresses are never aged out.
- When a multicast address is assigned to an interface in a specific VLAN, the corresponding traffic can only be forwarded to ports within that VLAN.

Parameters

These parameters are displayed:

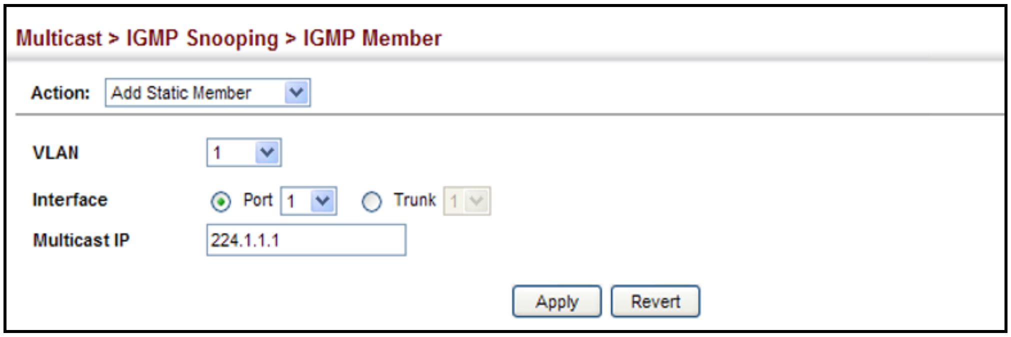
- **VLAN** – Specifies the VLAN which is to propagate the multicast service. (Range: 1-4094)
- **Interface** – Activates the Port or Trunk scroll down list.
- **Port** or **Trunk** – Specifies the interface assigned to a multicast group.
- **Multicast IP** – The IP address for a specific multicast service.

Web Interface

To statically assign an interface to an IPv4 multicast service:

1. Click Multicast, IGMP Snooping, IGMP Member.
2. Select Add Static Member from the Action list.
3. Select the VLAN that will propagate the multicast service, specify the interface attached to a multicast service (through an IGMP-enabled switch or multicast router), and enter the multicast IP address.
4. Click Apply.

Figure 344: Assigning an Interface to an IPv4 Multicast Service



Multicast > IGMP Snooping > IGMP Member

Action: Add Static Member

VLAN: 1

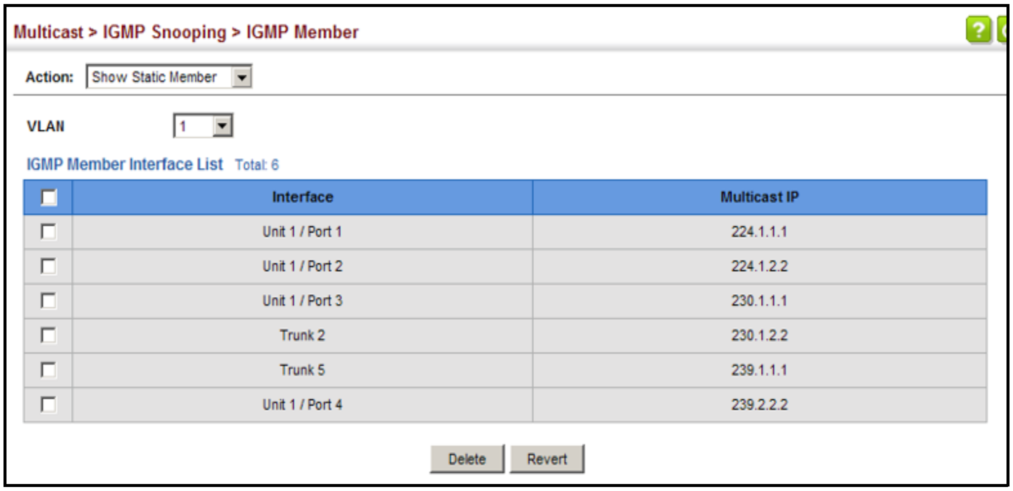
Interface: ● Port 1 ○ Trunk 1

Multicast IP: 224.1.1.1

To show the static interfaces assigned to an IPv4 multicast service:

1. Click Multicast, IGMP Snooping, IGMP Member.
2. Select Show Static Member from the Action list.
3. Select the VLAN for which to display this information.

Figure 345: Showing Static Interfaces Assigned to an IPv4 Multicast Service



Multicast > IGMP Snooping > IGMP Member

Action: Show Static Member

VLAN 1

IGMP Member Interface List Total: 6

□	Interface	Multicast IP
□	Unit 1 / Port 1	224.1.1.1
□	Unit 1 / Port 2	224.1.2.2
□	Unit 1 / Port 3	230.1.1.1
□	Trunk 2	230.1.2.2
□	Trunk 5	239.1.1.1
□	Unit 1 / Port 4	239.2.2.2

SETTING IGMP SNOOPING STATUS PER INTERFACE

Use the Multicast > IGMP Snooping > Interface (Configure VLAN) page to configure IGMP snooping attributes for a VLAN. To configure snooping globally, refer to "Configuring IGMP Snooping and Query Parameters" on page 613.

CLI REFERENCES

- "IGMP Snooping" on page 1426

COMMAND USAGE

Multicast Router Discovery

There have been many mechanisms used in the past to identify multicast routers. This has lead to interoperability issues between multicast routers and snooping switches from different vendors. In response to this problem, the Multicast Router Discovery (MRD) protocol has been developed for use by IGMP snooping and multicast routing devices. MRD is used to discover which interfaces are attached to multicast routers, allowing IGMP-enabled devices to determine where to send multicast source and group membership messages. (MRD is specified in draft-ietf-magma-mrdisc-07.)

Multicast source data and group membership reports must be received by all multicast routers on a segment. Using the group membership protocol query messages to discover multicast routers is insufficient due to query suppression. MRD therefore provides a standardized way to identify multicast routers without relying on any particular multicast routing protocol.

NOTE: The default values recommended in the MRD draft are implemented in the switch.

Multicast Router Discovery uses the following three message types to discover multicast routers:

- Multicast Router Advertisement – Advertisements are sent by routers to advertise that IP multicast forwarding is enabled. These messages are sent unsolicited periodically on all router interfaces on which multicast forwarding is enabled. They are sent upon the occurrence of these events:
  - Upon the expiration of a periodic (randomized) timer.
  - As a part of a router's start up procedure.
  - During the restart of a multicast forwarding interface.
  - On receipt of a Solicitation message.
- Multicast Router Solicitation – Devices send Solicitation messages in order to solicit Advertisement messages from multicast routers. These messages are used to discover multicast routers on a directly attached link. Solicitation messages are also sent whenever a multicast forwarding interface is initialized or re-initialized. Upon receiving a solicitation on an interface with IP multicast forwarding and MRD enabled, a router will respond with an Advertisement.
- Multicast Router Termination – These messages are sent when a router stops IP multicast routing functions on an interface. Termination messages are sent by multicast routers when:
  - Multicast forwarding is disabled on an interface.
  - An interface is administratively disabled.
  - The router is gracefully shut down.

Advertisement and Termination messages are sent to the All-Snoopers multicast address. Solicitation messages are sent to the All-Routers multicast address.

NOTE: MRD messages are flooded to all ports in a VLAN where IGMP snooping or routing has been enabled. To ensure that older switches which do not support MRD can also learn the multicast router port, the switch floods IGMP general query packets, which do not have a null source address (0.0.0.0), to all ports in the attached VLAN. IGMP packets with a null source address are only flooded to all ports in the VLAN if the system is operating in multicast flooding mode, such as when a new VLAN or new router port is being established, or an spanning tree topology change has occurred. Otherwise, this kind of packet is only forwarded to known multicast routing ports.

PARAMETERS

These parameters are displayed:

- **VLAN** – ID of configured VLANs. (Range: 1-4094)
- **IGMP Snooping Status** – When enabled, the switch will monitor network traffic on the indicated VLAN interface to determine which hosts want to receive multicast traffic. This is referred to as IGMP Snooping. (Default: Enabled)

  When IGMP snooping is enabled globally (see page 613), the per VLAN interface settings for IGMP snooping take precedence.

  When IGMP snooping is disabled globally, snooping can still be configured per VLAN interface, but the interface settings will not take effect until snooping is re-enabled globally.
- **Version Exclusive** – Discards any received IGMP messages (except for multicast protocol packets) which use a version different to that currently configured by the IGMP Version attribute. (Default: Disabled)

  If version exclusive is disabled on a VLAN, then this setting is based on the global setting configured on the Multicast > IGMP Snooping > General page. If it is enabled on a VLAN, then this setting takes precedence over the global setting.
- **Immediate Leave Status** – Immediately deletes a member port of a multicast service if a leave packet is received at that port and immediate leave is enabled for the parent VLAN. (Default: Disabled)

  If immediate leave is not used, a multicast router (or querier) will send a group-specific query message when an IGMPv2 group leave message is received. The router/querier stops forwarding traffic for that group only if no host replies to the query within the specified time out period. Note that this time out is set to Last Member Query Interval * Robustness Variable (fixed at 2 as defined in RFC 2236).

  If immediate leave is enabled, the switch assumes that only one host is connected to the interface. Therefore, immediate leave should only be enabled on an interface if it is connected to only one IGMP-enabled device, either a service host or a neighbor running IGMP snooping.

  This attribute is only effective if IGMP snooping is enabled, and IGMPv2 snooping is used.
- **Multicast Router Discovery** – MRD is used to discover which interfaces are attached to multicast routers. (Default: Disabled)
- **General Query Suppression** – Suppresses general queries except for ports attached to downstream multicast hosts. (Default: Disabled)

  By default, general query messages are flooded to all ports, except for the multicast router through which they are received.

  If general query suppression is enabled, then these messages are forwarded only to downstream ports which have joined a multicast service.

- **Proxy Reporting** – Enables IGMP Snooping with Proxy Reporting. (Default: Based on global setting)

  When proxy reporting is enabled with this command, the switch performs "IGMP Snooping with Proxy Reporting" (as defined in DSL Forum TR-101, April 2006), including last leave, and query suppression.

  Last leave sends out a proxy query when the last member leaves a multicast group, and query suppression means that specific queries are not forwarded from an upstream multicast router to hosts downstream from this device.

- **Interface Version** – Sets the protocol version for compatibility with other devices on the network. This is the IGMP Version the switch uses to send snooping reports. (Range: 1-3; Default: 2)

  This attribute configures the IGMP report/query version used by IGMP snooping. Versions 1 - 3 are all supported, and versions 2 and 3 are backward compatible, so the switch can operate with other devices, regardless of the snooping version employed.

- **Query Interval** – The interval between sending IGMP proxy general queries. (Range: 2-31744 seconds; Default: 125 seconds)

  An IGMP general query message is sent by the switch at the interval specified by this attribute. When this message is received by downstream hosts, all receivers build an IGMP report for the multicast groups they have joined.

  This attribute applies when the switch is serving as the querier (page 613), or as a proxy host when IGMP snooping proxy reporting is enabled (page 613).

- **Query Response Interval** – The maximum time the system waits for a response to proxy general queries. (Range: 10-31740 tenths of a second; Default: 10 seconds)

  This attribute applies when the switch is serving as the querier (page 613), or as a proxy host when IGMP snooping proxy reporting is enabled (page 613).

- **Last Member Query Interval** – The interval to wait for a response to a group-specific or group-and-source-specific query message. (Range: 1-31744 tenths of a second in multiples of 10; Default: 1 second)

  When a multicast host leaves a group, it sends an IGMP leave message. When the leave message is received by the switch, it checks to see if this host is the last to leave the group by sending out an IGMP group-specific or group-and-source-specific query message, and starts a timer. If no reports are received before the timer expires, the group record is deleted, and a report is sent to the upstream multicast router.

  A reduced value will result in reduced time to detect the loss of the last member of a group or source, but may generate more burst traffic.

  This attribute will take effect only if IGMP snooping proxy reporting is enabled (see page 613).

- **Last Member Query Count** – The number of IGMP proxy group-specific or group-and-source-specific query messages that are sent out before the system assumes there are no more local members. (Range: 1-255; Default: 2)

  This attribute will take effect only if IGMP snooping proxy reporting or IGMP querier is enabled.

- **Proxy Query Address** – A static source address for locally generated query and report messages used by IGMP Proxy Reporting. (Range: Any valid IP unicast address; Default: 0.0.0.0)

  IGMP Snooping uses a null IP address of 0.0.0.0 for the source of IGMP query messages which are proxied to downstream hosts to indicate that it is not the elected querier, but is only proxying these messages as defined in RFC 4541. The switch also uses a null address in IGMP reports sent to upstream ports.

  Many hosts do not implement RFC 4541, and therefore do not understand query messages with the source address of 0.0.0.0. These hosts will therefore not reply to the queries, causing the multicast router to stop sending traffic to them.

  To resolve this problem, the source address in proxied IGMP query messages can be replaced with any valid unicast address (other than the router's own address).

  Rules Used for Proxy Reporting

  When IGMP Proxy Reporting is disabled, the switch will use a null IP address for the source of IGMP query and report messages unless a proxy query address has been set.

  When IGMP Proxy Reporting is enabled, the source address is based on the following criteria:

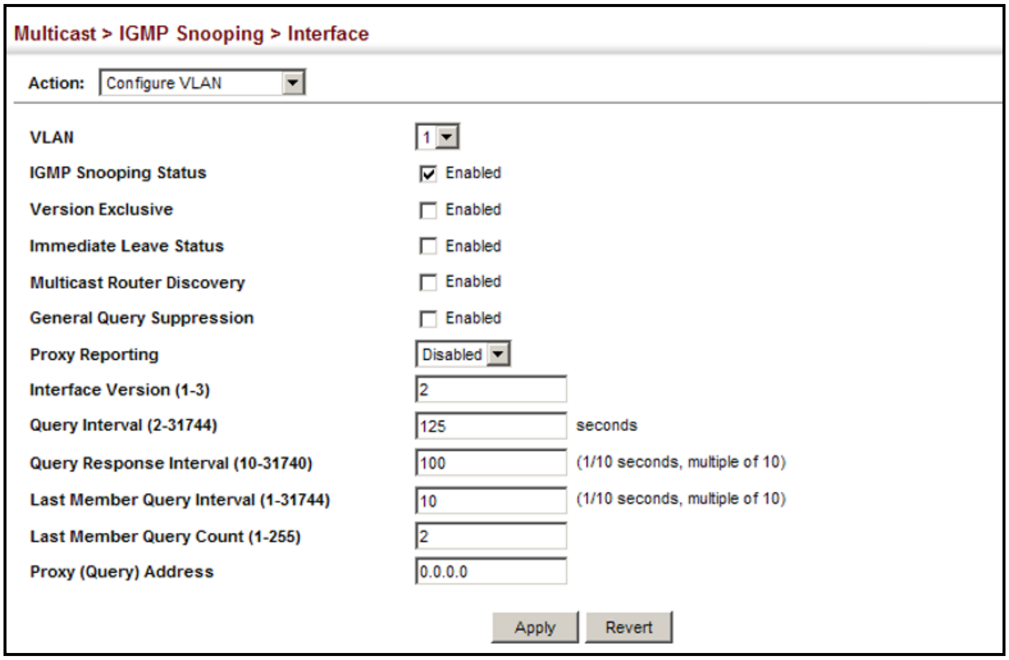
  - If a proxy query address is configured, the switch will use that address as the source IP address in general and group-specific query messages sent to downstream hosts, and in report and leave messages sent upstream from the multicast router port.
  - If a proxy query address is not configured, the switch will use the VLAN's IP address as the IP source address in general and group-specific query messages sent downstream, and use the source address of the last IGMP message received from a downstream host in report and leave messages sent upstream from the multicast router port.

WEB INTERFACE

To configure IGMP snooping on a VLAN:

1. Click Multicast, IGMP Snooping, Interface.
2. Select Configure VLAN from the Action list.
3. Select the VLAN to configure and update the required parameters.
4. Click Apply.

Figure 346: Configuring IGMP Snooping on a VLAN



Multicast > IGMP Snooping > Interface

Action: Configure VLAN

VLAN: 1

IGMP Snooping Status: ☑ Enabled

Version Exclusive: □ Enabled

Immediate Leave Status: □ Enabled

Multicast Router Discovery: □ Enabled

General Query Suppression: □ Enabled

Proxy Reporting: Disabled

Interface Version (1-3): 2

Query Interval (2-31744): 125 seconds

Query Response Interval (10-31740): 100 (1/10 seconds, multiple of 10)

Last Member Query Interval (1-31744): 10 (1/10 seconds, multiple of 10)

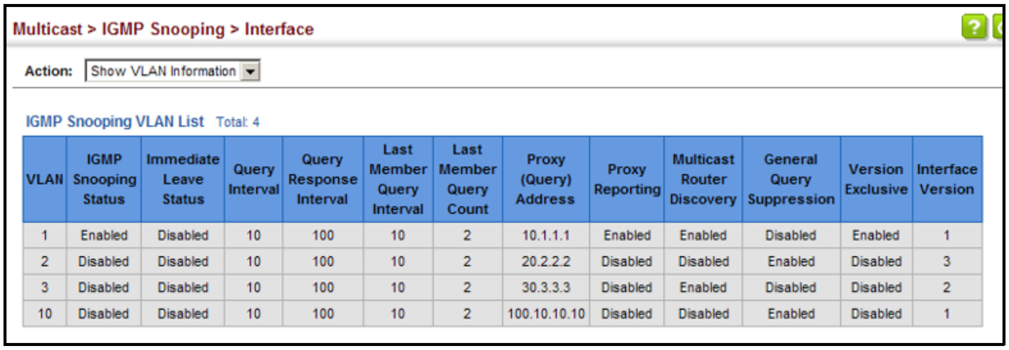
Last Member Query Count (1-255): 2

Proxy (Query) Address: 0.0.0.0

To show the interface settings for IGMP snooping:

1. Click Multicast, IGMP Snooping, Interface.
2. Select Show VLAN Information from the Action list.

Figure 347: Showing Interface Settings for IGMP Snooping



Multicast > IGMP Snooping > Interface

Action: Show VLAN Information

IGMP Snooping VLAN List Total: 4

VLAN	IGMP Snooping Status	Immediate Leave Status	Query Interval	Query Response Interval	Last Member Query Interval	Last Member Query Count	Proxy (Query) Address	Proxy Reporting	Multicast Router Discovery	General Query Suppression	Version Exclusive	Interface Version
1	Enabled	Disabled	10	100	10	2	10.1.1.1	Enabled	Enabled	Disabled	Enabled	1
2	Disabled	Disabled	10	100	10	2	20.2.2.2	Disabled	Disabled	Enabled	Disabled	3
3	Disabled	Disabled	10	100	10	2	30.3.3.3	Disabled	Enabled	Disabled	Disabled	2
10	Disabled	Disabled	10	100	10	2	100.10.10.10	Disabled	Disabled	Enabled	Disabled	1

FILTERING IGMP QUERY PACKETS AND MULTICAST DATA

Use the Multicast > IGMP Snooping > Interface page to configure an interface to drop IGMP query packets or multicast data packets.

CLI REFERENCES

- "ip igmp query-drop" on page 1455
- "ip multicast-data-drop" on page 1455

PARAMETERS

These parameters are displayed:

- **IGMP Query Drop** – Configures an interface to drop any IGMP query packets received on the specified interface. If this switch is acting as a Querier, this prevents it from being affected by messages received from another Querier.

- **Multicast Data Drop** – Configures an interface to stop multicast services from being forwarded to users attached to the downstream port (i.e., the interfaces specified by this command).

WEB INTERFACE

To drop IGMP query packets or multicast data packets:

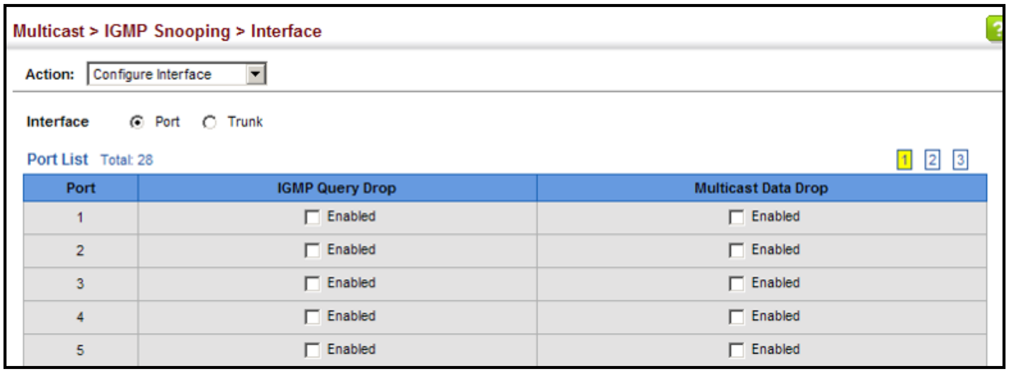
1. Click Multicast, IGMP Snooping, Interface.

2. Select Configure Interface from the Action List.

3. Enable the required drop functions for any interface.

4. Click Apply.

Figure 348: Dropping IGMP Query or Multicast Data Packets



Multicast > IGMP Snooping > Interface

Action: Configure Interface

Interface ● Port ○ Trunk

Port List Total: 28

Port	IGMP Query Drop	Multicast Data Drop
1	□ Enabled	□ Enabled
2	□ Enabled	□ Enabled
3	□ Enabled	□ Enabled
4	□ Enabled	□ Enabled
5	□ Enabled	□ Enabled

DISPLAYING MULTICAST GROUPS DISCOVERED BY IGMP SNOOPING

Use the Multicast > IGMP Snooping > Forwarding Entry page to display the forwarding entries learned through IGMP Snooping.

CLI REFERENCES

- "show ip igmp snooping group" on page 1443

COMMAND USAGE

To display information about multicast groups, IGMP Snooping must first be enabled on the switch (see page 613).

PARAMETERS

These parameters are displayed:

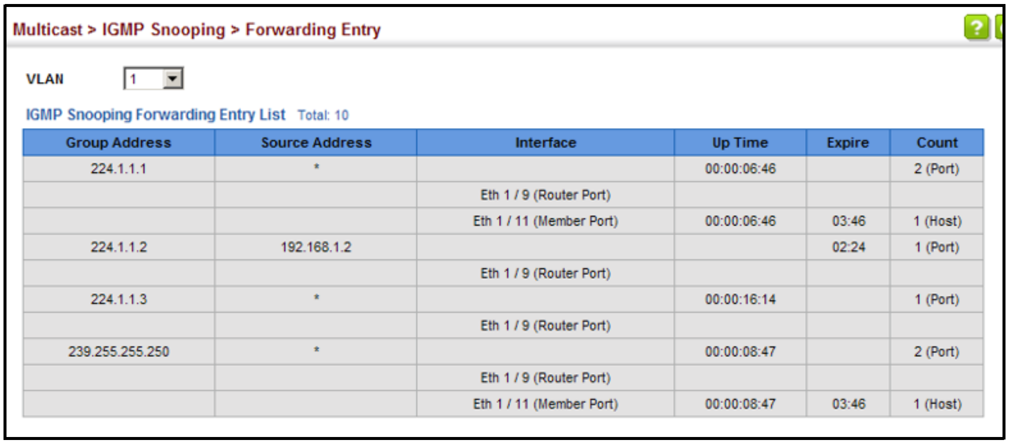
- **VLAN** – An interface on the switch that is forwarding traffic to downstream ports for the specified multicast group address.
- **Group Address** – IP multicast group address with subscribers directly attached or downstream from the switch, or a static multicast group assigned to this interface.
- **Source Address** – The address of one of the multicast servers transmitting traffic to the specified group.
- **Interface** – A downstream port or trunk that is receiving traffic for the specified multicast group. This field may include both dynamically and statically configured multicast router ports.
- **Up Time** – Time that this multicast group has been known.
- **Expire** – The time until this entry expires.
- **Count** – The number of times this address has been learned by IGMP snooping.

WEB INTERFACE

To show multicast groups learned through IGMP snooping:

1. Click Multicast, IGMP Snooping, Forwarding Entry.
2. Select the VLAN for which to display this information.

Figure 349: Showing Multicast Groups Learned by IGMP Snooping



Multicast > IGMP Snooping > Forwarding Entry

VLAN: 1

IGMP Snooping Forwarding Entry List Total: 10

Group Address	Source Address	Interface	Up Time	Expire	Count
224.1.1.1	*		00:00:06:46		2 (Port)
		Eth 1 / 9 (Router Port)			
		Eth 1 / 11 (Member Port)	00:00:06:46	03:46	1 (Host)
224.1.1.2	192.168.1.2			02:24	1 (Port)
		Eth 1 / 9 (Router Port)			
224.1.1.3	*		00:00:16:14		1 (Port)
		Eth 1 / 9 (Router Port)			
239.255.255.250	*		00:00:08:47		2 (Port)
		Eth 1 / 9 (Router Port)			
		Eth 1 / 11 (Member Port)	00:00:08:47	03:46	1 (Host)

DISPLAYING IGMP SNOOPING STATISTICS

Use the Multicast > IGMP Snooping > Statistics pages to display IGMP snooping protocol-related statistics for the specified interface.

CLI REFERENCES

- "show ip igmp snooping statistics" on page 1444

PARAMETERS

These parameters are displayed:

- **VLAN** – VLAN identifier. (Range: 1-4094)
- **Port** – Port identifier. (Range: 1-28)
- **Trunk** – Trunk identifier. (Range: 1-8)

Query Statistics

- **Querier IP Address** – The IP address of the querier on this interface.
- **Querier Expire Time** – The time after which this querier is assumed to have expired.
- **General Query Received** – The number of general queries received on this interface.
- **General Query Sent** – The number of general queries sent from this interface.

- **Specific Query Received** – The number of specific queries received on this interface.

- **Specific Query Sent** – The number of specific queries sent from this interface.

- **Number of Reports Sent** – The number of reports sent from this interface.

- **Number of Leaves Sent** – The number of leaves sent from this interface.

VLAN, Port, and Trunk Statistics

Input Statistics

- **Report** – The number of IGMP membership reports received on this interface.

- **Leave** – The number of leave messages received on this interface.

- **G Query** – The number of general query messages received on this interface.

- **G(-S)-S Query** – The number of group specific or group-and-source specific query messages received on this interface.

- **Drop** – The number of times a report, leave or query was dropped. Packets may be dropped due to invalid format, rate limiting, packet content not allowed, or IGMP group report received.

- **Join Success** – The number of times a multicast group was successfully joined.

- **Group** – The number of IGMP groups active on this interface.

Output Statistics

- **Report** – The number of IGMP membership reports sent from this interface.

- **Leave** – The number of leave messages sent from this interface.

- **G Query** – The number of general query messages sent from this interface.

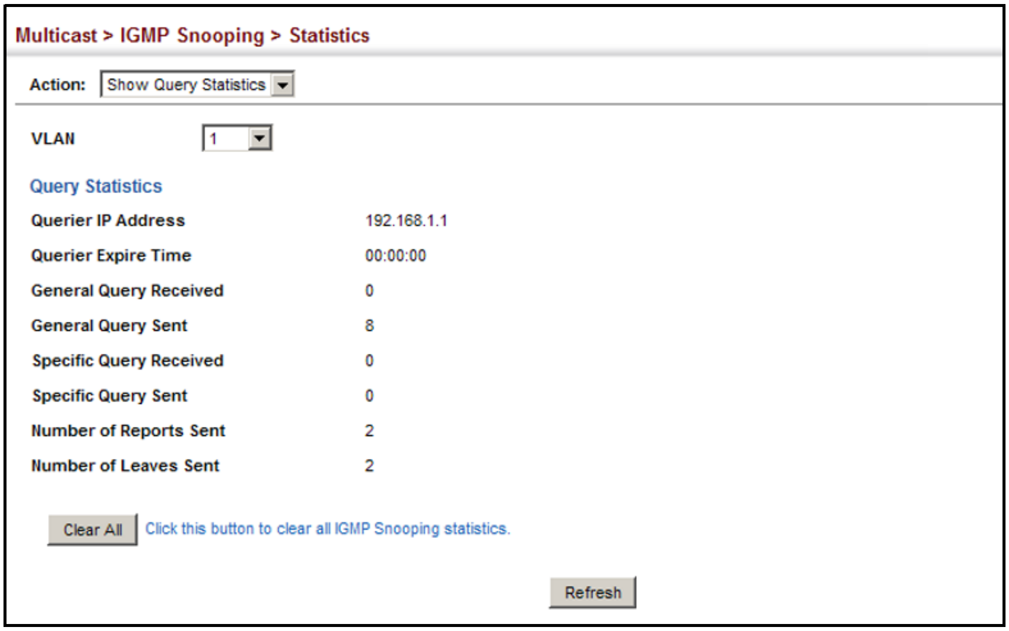
- **G(-S)-S Query** – The number of group specific or group-and-source specific query messages sent from this interface.

WEB INTERFACE

To display statistics for IGMP snooping query-related messages:

1. Click Multicast, IGMP Snooping, Statistics.
2. Select Show Query Statistics from the Action list.
3. Select a VLAN.

Figure 350: Displaying IGMP Snooping Statistics – Query



Multicast > IGMP Snooping > Statistics

Action: Show Query Statistics

VLAN: 1

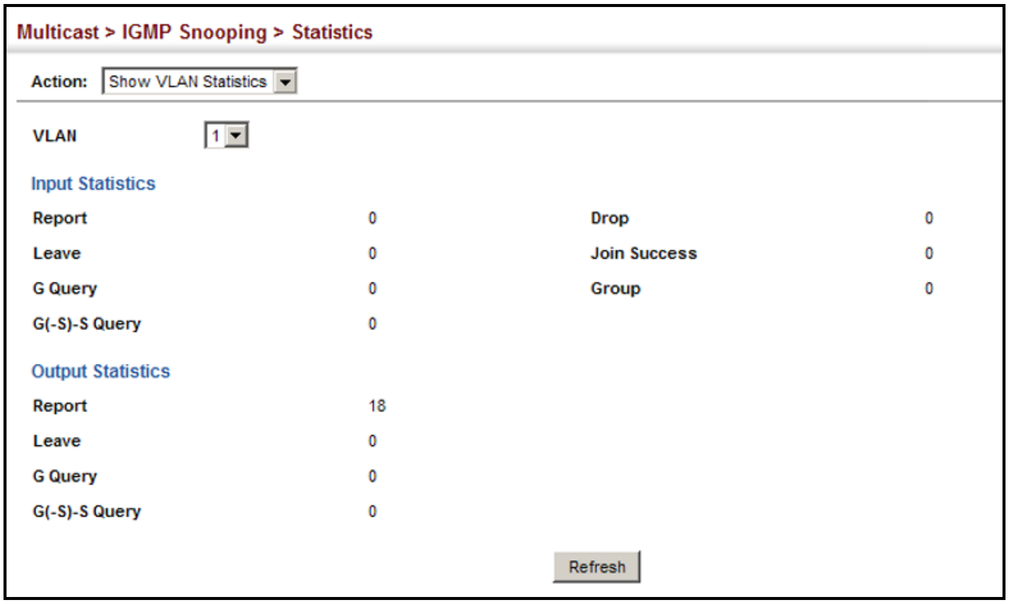
Query Statistics

Querier IP Address	192.168.1.1
Querier Expire Time	00:00:00
General Query Received	0
General Query Sent	8
Specific Query Received	0
Specific Query Sent	0
Number of Reports Sent	2
Number of Leaves Sent	2

To display IGMP snooping protocol-related statistics for a VLAN:

1. Click Multicast, IGMP Snooping, Statistics.
2. Select Show VLAN Statistics from the Action list.
3. Select a VLAN.

Figure 351: Displaying IGMP Snooping Statistics – VLAN



Multicast > IGMP Snooping > Statistics

Action: Show VLAN Statistics

VLAN 1

Input Statistics

Report	0	Drop	0
Leave	0	Join Success	0
G Query	0	Group	0
G(-S)-S Query	0		

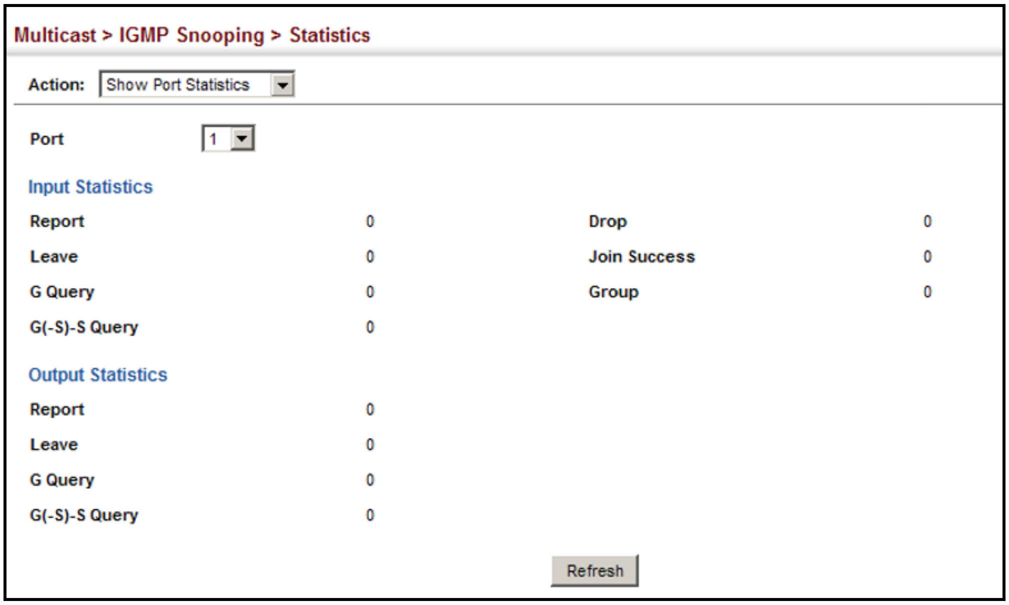
Output Statistics

Report	18
Leave	0
G Query	0
G(-S)-S Query	0

To display IGMP snooping protocol-related statistics for a port:

1. Click Multicast, IGMP Snooping, Statistics.
2. Select Show Port Statistics from the Action list.
3. Select a Port.

Figure 352: Displaying IGMP Snooping Statistics – Port



Multicast > IGMP Snooping > Statistics

Action: Show Port Statistics

Port 1

Input Statistics

Report	0	Drop	0
Leave	0	Join Success	0
G Query	0	Group	0
G(-S)-S Query	0		

Output Statistics

Report	0
Leave	0
G Query	0
G(-S)-S Query	0

FILTERING AND THROTTLING IGMP GROUPS

In certain switch applications, the administrator may want to control the multicast services that are available to end users. For example, an IP/TV service based on a specific subscription plan. The IGMP filtering feature fulfills this requirement by restricting access to specified multicast services on a switch port, and IGMP throttling limits the number of simultaneous multicast groups a port can join.

IGMP filtering enables you to assign a profile to a switch port that specifies multicast groups that are permitted or denied on the port. An IGMP filter profile can contain one or more addresses, or a range of multicast addresses; but only one profile can be assigned to a port. When enabled, IGMP join reports received on the port are checked against the filter profile. If a requested multicast group is permitted, the IGMP join report is forwarded as normal. If a requested multicast group is denied, the IGMP join report is dropped.

IGMP throttling sets a maximum number of multicast groups that a port can join at the same time. When the maximum number of groups is reached on a port, the switch can take one of two actions; either “deny” or “replace.” If the action is set to deny, any new IGMP join reports will be dropped. If the action is set to replace, the switch randomly removes an existing group and replaces it with the new multicast group.

ENABLING IGMP FILTERING AND THROTTLING

Use the Multicast > IGMP Snooping > Filter (Configure General) page to enable IGMP filtering and throttling globally on the switch.

CLI REFERENCES

- "ip igmp filter (Global Configuration)" on page 1449

PARAMETERS

These parameters are displayed:

- **IGMP Filter Status** – Enables IGMP filtering and throttling globally for the switch. (Default: Disabled)

WEB INTERFACE

To enable IGMP filtering and throttling on the switch:

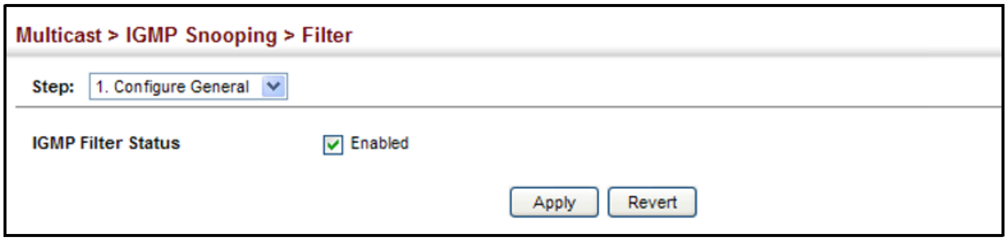
1. Click Multicast, IGMP Snooping, Filter.

2. Select Configure General from the Step list.

3. Enable IGMP Filter Status.

4. Click Apply.

Figure 353: Enabling IGMP Filtering and Throttling



Multicast > IGMP Snooping > Filter

Step: 1. Configure General

IGMP Filter Status ☑ Enabled

CONFIGURING IGMP FILTER PROFILES

Use the Multicast > IGMP Snooping > Filter (Configure Profile – Add) page to create an IGMP profile and set its access mode. Then use the (Add Multicast Group Range) page to configure the multicast groups to filter.

CLI REFERENCES

- "IGMP Filtering and Throttling" on page 1448

COMMAND USAGE

Specify a range of multicast groups by entering a start and end IP address; or specify a single multicast group by entering the same IP address for the start and end of the range.

PARAMETERS

These parameters are displayed:

Add

- **Profile ID** – Creates an IGMP profile. (Range: 1-4294967295)

- **Access Mode** – Sets the access mode of the profile; either permit or deny. (Default: Deny)

  When the access mode is set to permit, IGMP join reports are processed when a multicast group falls within the controlled range. When the access mode is set to deny, IGMP join reports are only processed when the multicast group is not in the controlled range.

Add Multicast Group Range

- **Profile ID** – Selects an IGMP profile to configure.

- **Start Multicast IP Address** – Specifies the starting address of a range of multicast groups.

- **End Multicast IP Address** – Specifies the ending address of a range of multicast groups.

WEB INTERFACE

To create an IGMP filter profile and set its access mode:

1. Click Multicast, IGMP Snooping, Filter.

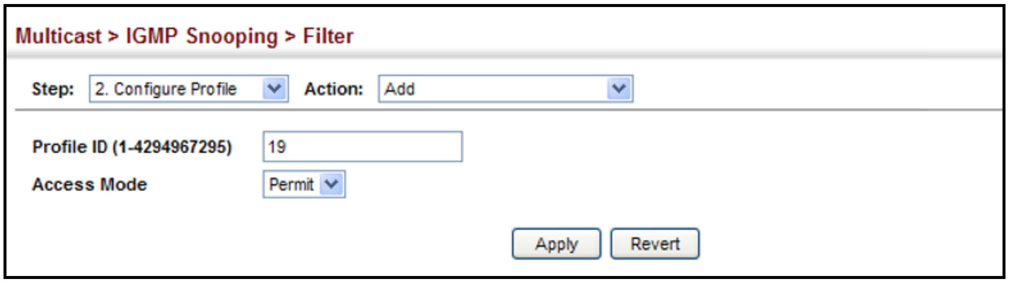
2. Select Configure Profile from the Step list.

3. Select Add from the Action list.

4. Enter the number for a profile, and set its access mode.

5. Click Apply.

Figure 354: Creating an IGMP Filtering Profile



Multicast > IGMP Snooping > Filter

Step: 2. Configure Profile   Action: Add

Profile ID (1-4294967295): 19

Access Mode: Permit

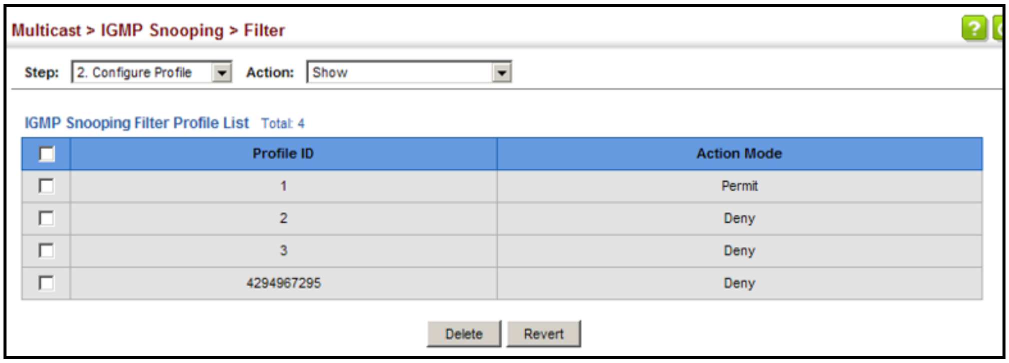
To show the IGMP filter profiles:

1. Click Multicast, IGMP Snooping, Filter.

2. Select Configure Profile from the Step list.

3. Select Show from the Action list.

Figure 355: Showing the IGMP Filtering Profiles Created



Multicast > IGMP Snooping > Filter

Step: 2. Configure Profile   Action: Show

IGMP Snooping Filter Profile List Total: 4

□	Profile ID	Action Mode
□	1	Permit
□	2	Deny
□	3	Deny
□	4294967295	Deny

To add a range of multicast groups to an IGMP filter profile:

1. Click Multicast, IGMP Snooping, Filter.

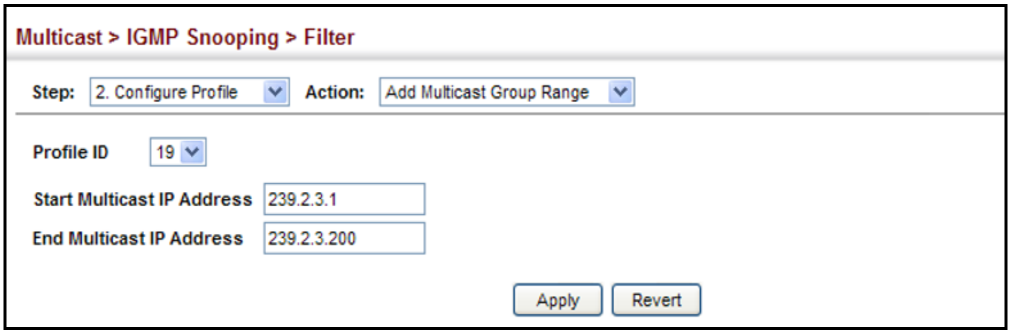
2. Select Configure Profile from the Step list.

3. Select Add Multicast Group Range from the Action list.

4. Select the profile to configure, and add a multicast group address or range of addresses.

5. Click Apply.

Figure 356: Adding Multicast Groups to an IGMP Filtering Profile


Multicast > IGMP Snooping > Filter

Step: 2. Configure Profile Action: Add Multicast Group Range

Profile ID: 19

Start Multicast IP Address: 239.2.3.1

End Multicast IP Address: 239.2.3.200

To show the multicast groups configured for an IGMP filter profile:

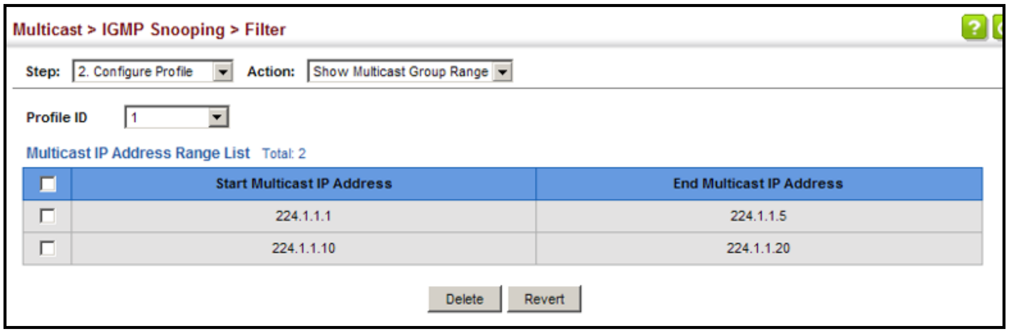
1. Click Multicast, IGMP Snooping, Filter.

2. Select Configure Profile from the Step list.

3. Select Show Multicast Group Range from the Action list.

4. Select the profile for which to display this information.

Figure 357: Showing the Groups Assigned to an IGMP Filtering Profile


Multicast > IGMP Snooping > Filter

Step: 2. Configure Profile Action: Show Multicast Group Range

Profile ID: 1

Multicast IP Address Range List Total: 2

□	Start Multicast IP Address	End Multicast IP Address
□	224.1.1.1	224.1.1.5
□	224.1.1.10	224.1.1.20

CONFIGURING IGMP FILTERING AND THROTTLING FOR INTERFACES

Use the Multicast > IGMP Snooping > Filter (Configure Interface) page to assign and IGMP filter profile to interfaces on the switch, or to throttle multicast traffic by limiting the maximum number of multicast groups an interface can join at the same time.

CLI REFERENCES

- "IGMP Filtering and Throttling" on page 1448

COMMAND USAGE

- IGMP throttling sets a maximum number of multicast groups that a port can join at the same time. When the maximum number of groups is reached on a port, the switch can take one of two actions; either "deny" or "replace." If the action is set to deny, any new IGMP join reports will be dropped. If the action is set to replace, the switch randomly removes an existing group and replaces it with the new multicast group.

PARAMETERS

These parameters are displayed:

- **Interface** – Port or trunk identifier.

  An IGMP profile or throttling setting can be applied to a port or trunk. When ports are configured as trunk members, the trunk uses the settings applied to the first port member in the trunk.

- **Profile ID** – Selects an existing profile to assign to an interface.

- **Max Multicast Groups** – Sets the maximum number of multicast groups an interface can join at the same time. (Range: 1-1024; Default: 1024)

- **Current Multicast Groups** – Displays the current multicast groups the interface has joined.

- **Throttling Action Mode** – Sets the action to take when the maximum number of multicast groups for the interface has been exceeded. (Default: Deny)

  - **Deny** - The new multicast group join report is dropped.
  - **Replace** - The new multicast group replaces an existing group.

- **Throttling Status** – Indicates if the throttling action has been implemented on the interface. (Options: True or False)

WEB INTERFACE

To configure IGMP filtering or throttling for a port or trunk:

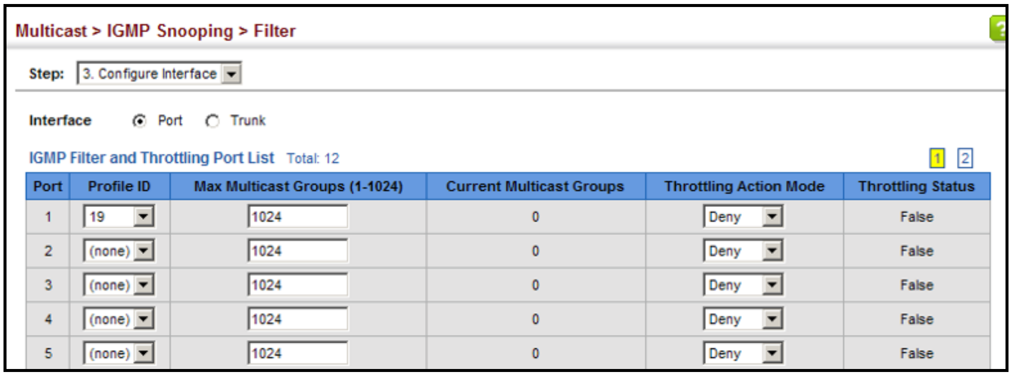
1. Click Multicast, IGMP Snooping, Filter.

2. Select Configure Interface from the Step list.

3. Select a profile to assign to an interface, then set the maximum number of allowed multicast groups and the throttling response.

4. Click Apply.

Figure 358: Configuring IGMP Filtering and Throttling Interface Settings



Multicast > IGMP Snooping > Filter

Step: 3. Configure Interface

Interface ● Port ○ Trunk

IGMP Filter and Throttling Port List Total: 12

Port	Profile ID	Max Multicast Groups (1-1024)	Current Multicast Groups	Throttling Action Mode	Throttling Status
1	19	1024	0	Deny	False
2	(none)	1024	0	Deny	False
3	(none)	1024	0	Deny	False
4	(none)	1024	0	Deny	False
5	(none)	1024	0	Deny	False

MLD SNOOPING (SNOOPING AND QUERY FOR IPV6)

Multicast Listener Discovery (MLD) snooping operates on IPv6 traffic and performs a similar function to IGMP snooping for IPv4. That is, MLD snooping dynamically configures switch ports to limit IPv6 multicast traffic so that it is forwarded only to ports with users that want to receive it. This reduces the flooding of IPv6 multicast packets in the specified VLANs.

There are two versions of the MLD protocol, version 1 and version 2. MLDv1 control packets include Listener Query, Listener Report, and Listener Done messages (equivalent to IGMPv2 query, report, and leave messages). MLDv2 control packets include MLDv2 query and report messages, as well as MLDv1 report and done messages.

Remember that IGMP Snooping and MLD Snooping are independent functions, and can therefore both function at the same time.

CONFIGURING MLD SNOOPING AND QUERY PARAMETERS

Use the Multicast > MLD Snooping > General page to configure the switch to forward multicast traffic intelligently. Based on the MLD query and report messages, the switch forwards multicast traffic only to the ports that request it. This prevents the switch from broadcasting the traffic to all ports and possibly disrupting network performance.

CLI REFERENCES

- "MLD Snooping Commands" on page 1469

PARAMETERS

These parameters are displayed:

- **MLD Snooping Status** – When enabled, the switch will monitor network traffic to determine which hosts want to receive multicast traffic. (Default: Disabled)

- **Querier Status** – When enabled, the switch can serve as the querier for MLDv2 snooping if elected. The querier is responsible for asking hosts if they want to receive multicast traffic. (Default: Disabled)

An IPv6 address must be configured on the VLAN interface from which the querier will act if elected. When serving as the querier, the switch uses this IPv6 address as the query source address.

The querier will not start or will disable itself after having started if it detects an IPv6 multicast router on the network.

- **Robustness** – MLD Snooping robustness variable. A port will be removed from the receiver list for a multicast service when no MLD reports are detected in response to a number of MLD queries. The robustness variable sets the number of queries on ports for which there is no report. (Range: 2-10 Default: 2)
- **Query Interval** – The interval between sending MLD general queries. (Range: 60-125 seconds; Default: 125 seconds)

  This attribute applies when the switch is serving as the querier.

  An MLD general query message is sent by the switch at the interval specified by this attribute. When this message is received by downstream hosts, all receivers build an MLD report for the multicast groups they have joined.
- **Query Max Response Time** – The maximum response time advertised in MLD general queries. (Range: 5-25 seconds; Default: 10 seconds)

  This attribute controls how long the host has to respond to an MLD Query message before the switch deletes the group if it is the last member.
- **Router Port Expiry Time** – The time the switch waits after the previous querier stops before it considers the router port (i.e., the interface that had been receiving query packets) to have expired. (Range: 300-500 seconds; Default: 300 seconds)
- **MLD Snooping Version** – The protocol version used for compatibility with other devices on the network. This is the MLD version the switch uses to send snooping reports. (Range: 1-2; Default: 2)
- **Unknown Multicast Mode** – The action for dealing with unknown multicast packets. Options include:
  - **Flood** – Floods any received IPv6 multicast packets that have not been requested by a host to all ports in the VLAN.
  - **To Router Port** – Forwards any received IPv6 multicast packets that have not been requested by a host to ports that are connected to a detected multicast router. (This is the default action.)

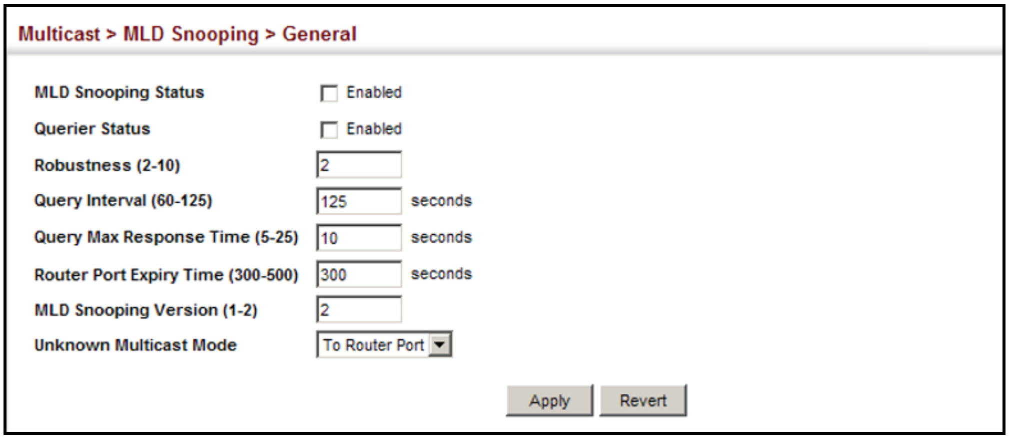
WEB INTERFACE

To configure general settings for MLD Snooping:

1. Click Multicast, MLD Snooping, General.
2. Adjust the settings as required.

3. Click Apply.

Figure 359: Configuring General Settings for MLD Snooping



Multicast > MLD Snooping > General

MLD Snooping Status □ Enabled
Querier Status □ Enabled
Robustness (2-10) 2
Query Interval (60-125) 125 seconds
Query Max Response Time (5-25) 10 seconds
Router Port Expiry Time (300-500) 300 seconds
MLD Snooping Version (1-2) 2
Unknown Multicast Mode To Router Port

Setting Immediate Leave Status for MLD Snooping per Interface

Use the Multicast > MLD Snooping > Interface page to configure Immediate Leave status for a VLAN.

CLI References

- "ipv6 mld snooping vlan immediate-leave" on page 1476

Parameters

These parameters are displayed:

- **VLAN** – A VLAN identification number. (Range: 1-4094)
- **Immediate Leave Status** – Immediately deletes a member port of an IPv6 multicast service when a leave packet is received at that port and immediate leave is enabled for the parent VLAN. (Default: Disabled)

  If MLD immediate-leave is *not* used, a multicast router (or querier) will send a group-specific query message when an MLD group leave message is received. The router/querier stops forwarding traffic for that group only if no host replies to the query within the specified timeout period.

  If MLD immediate-leave is enabled, the switch assumes that only one host is connected to the interface. Therefore, immediate leave should only be enabled on an interface if it is connected to only one MLD-enabled device, either a service host or a neighbor running MLD snooping.

Web Interface

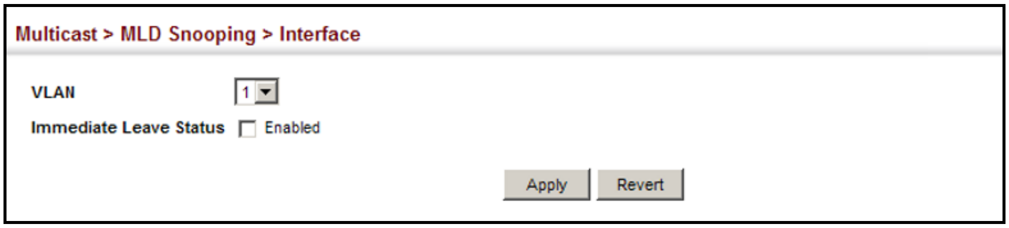
To configure immediate leave for MLD Snooping:

1. Click Multicast, MLD Snooping, Interface.

2. Select a VLAN, and set the status for immediate leave.

3. Click Apply.

Figure 360: Configuring Immediate Leave for MLD Snooping



Multicast > MLD Snooping > Interface

VLAN 1

Immediate Leave Status □ Enabled

SPECIFYING STATIC INTERFACES FOR AN IPV6 MULTICAST ROUTER

Use the Multicast > MLD Snooping > Multicast Router (Add Static Multicast Router) page to statically attach an interface to an IPv6 multicast router/switch.

Depending on your network connections, MLD snooping may not always be able to locate the MLD querier. Therefore, if the MLD querier is a known multicast router/switch connected over the network to an interface (port or trunk) on the switch, you can manually configure that interface to join all the current multicast groups.

CLI REFERENCES

- "ipv6 mld snooping vlan mrouter" on page 1474

COMMAND USAGE

MLD Snooping must be enabled globally on the switch (see "Configuring MLD Snooping and Query Parameters" on page 638) before a multicast router port can take effect.

PARAMETERS

These parameters are displayed:

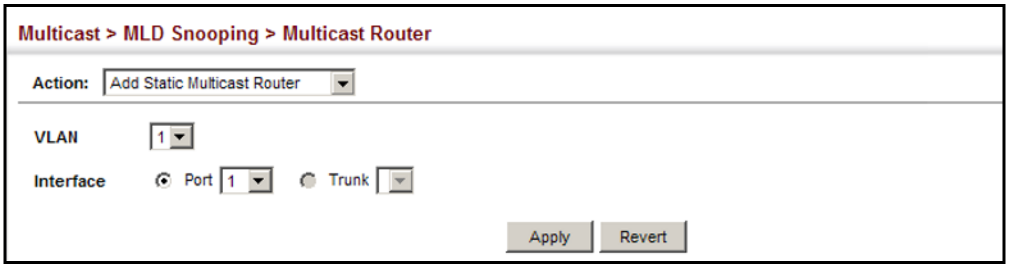
- **VLAN** – Selects the VLAN which is to propagate all IPv6 multicast traffic coming from the attached multicast router. (Range: 1-4094)
- **Interface** – Activates the Port or Trunk scroll down list.
- **Port** or **Trunk** – Specifies the interface attached to a multicast router.

WEB INTERFACE

To specify a static interface attached to a multicast router:

1. Click Multicast, MLD Snooping, Multicast Router.
2. Select Add Static Multicast Router from the Action list.
3. Select the VLAN which will forward all the corresponding IPv6 multicast traffic, and select the port or trunk attached to the multicast router.
4. Click Apply.

Figure 361: Configuring a Static Interface for an IPv6 Multicast Router



Action: Add Static Multicast Router

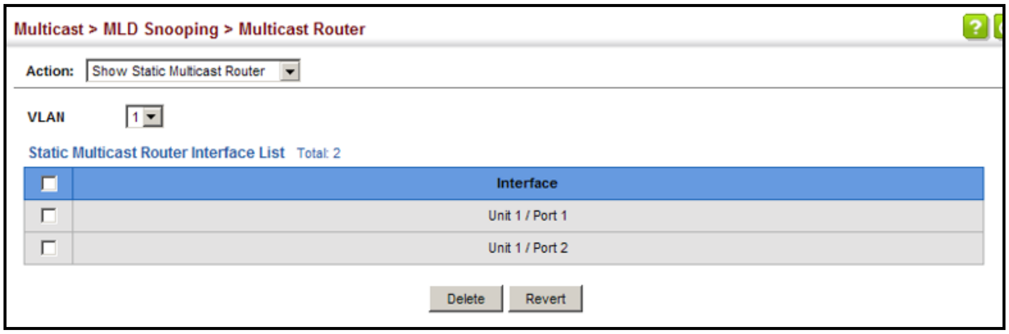
VLAN 1

Interface ● Port 1 ○ Trunk

To show the static interfaces attached to a multicast router:

1. Click Multicast, MLD Snooping, Multicast Router.
2. Select Show Static Multicast Router from the Action list.
3. Select the VLAN for which to display this information.

Figure 362: Showing Static Interfaces Attached an IPv6 Multicast Router



Action: Show Static Multicast Router

VLAN 1

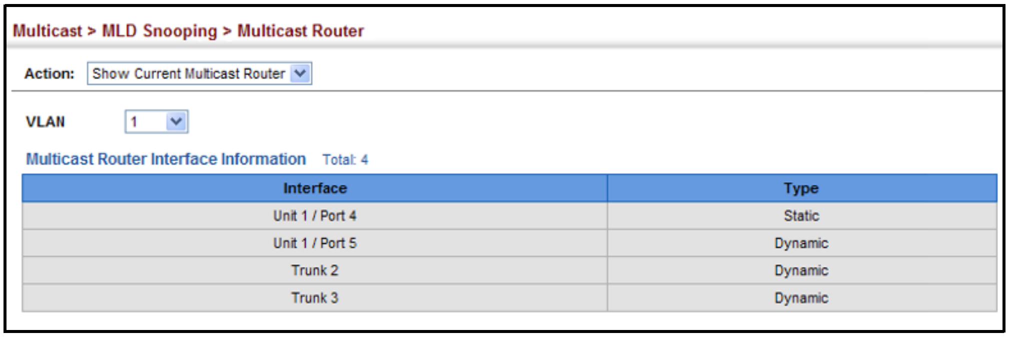
Static Multicast Router Interface List Total: 2

□	Interface
□	Unit 1 / Port 1
□	Unit 1 / Port 2

To show all the interfaces attached to a multicast router:

1. Click Multicast, MLD Snooping, Multicast Router.
2. Select Current Multicast Router from the Action list.
3. Select the VLAN for which to display this information. Ports in the selected VLAN which are attached to a neighboring multicast router/ switch are displayed.

Figure 363: Showing Current Interfaces Attached an IPv6 Multicast Router



Action: Show Current Multicast Router

VLAN 1

Multicast Router Interface Information Total: 4

Interface	Type
Unit 1 / Port 4	Static
Unit 1 / Port 5	Dynamic
Trunk 2	Dynamic
Trunk 3	Dynamic

ASSIGNING INTERFACES TO IPV6 MULTICAST SERVICES

Use the Multicast > MLD Snooping > MLD Member (Add Static Member) page to statically assign an IPv6 multicast service to an interface.

Multicast filtering can be dynamically configured using MLD snooping and query messages (see "Configuring MLD Snooping and Query Parameters" on page 638). However, for certain applications that require tighter control, it may be necessary to statically configure a multicast service on the switch. First add all the ports attached to participating hosts to a common VLAN, and then assign the multicast service to that VLAN group.

CLI REFERENCES

- "ipv6 mld snooping vlan static" on page 1475

COMMAND USAGE

- Static multicast addresses are never aged out.
- When a multicast address is assigned to an interface in a specific VLAN, the corresponding traffic can only be forwarded to ports within that VLAN.

PARAMETERS

These parameters are displayed:

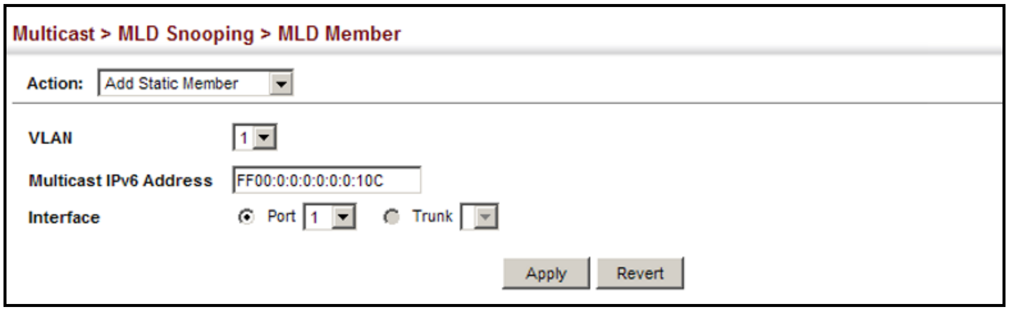
- **VLAN** – Specifies the VLAN which is to propagate the multicast service. (Range: 1-4094)
- **Multicast IPv6 Address** – The IP address for a specific multicast service.
- **Interface** – Activates the Port or Trunk scroll down list.
- **Port** or **Trunk** – Specifies the interface assigned to a multicast group.
- **Type** (Show Current Member) – Shows if this multicast stream was statically configured by the user, discovered by MLD Snooping, or is a data stream to which no other ports are subscribing (i.e., the stream is flooded onto VLAN instead of being trapped to the CPU for processing, or is being processed by MVR6).

WEB INTERFACE

To statically assign an interface to an IPv6 multicast service:

1. Click Multicast, MLD Snooping, MLD Member.
2. Select Add Static Member from the Action list.
3. Select the VLAN that will propagate the multicast service, specify the interface attached to a multicast service (through an MLD-enabled switch or multicast router), and enter the multicast IP address.
4. Click Apply.

Figure 364: Assigning an Interface to an IPv6 Multicast Service



Multicast > MLD Snooping > MLD Member

Action: Add Static Member

VLAN: 1

Multicast IPv6 Address: FF00:0:0:0:0:0:0:10C

Interface: ● Port 1 ○ Trunk

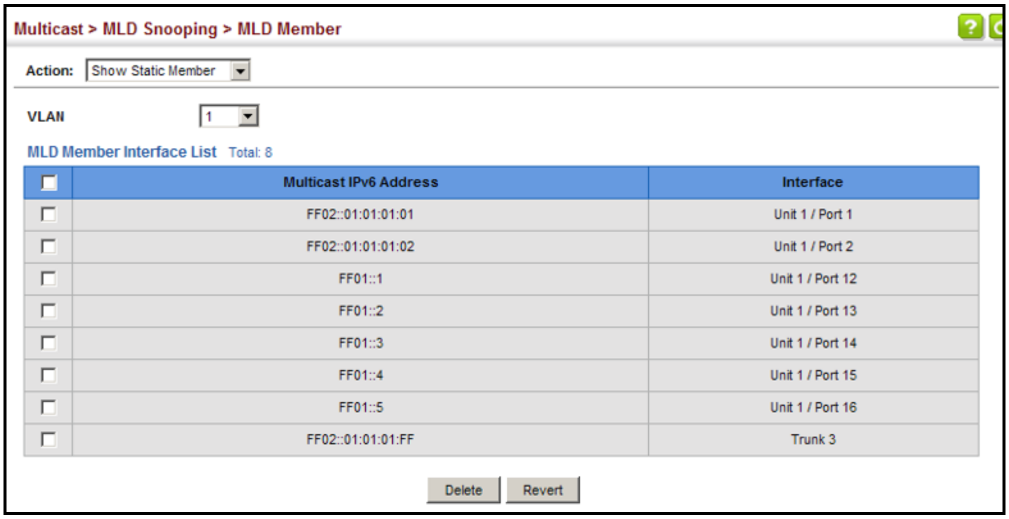
To show the static interfaces assigned to an IPv6 multicast service:

1. Click Multicast, MLD Snooping, MLD Member.

2. Select Show Static Member from the Action list.

3. Select the VLAN for which to display this information.

Figure 365: Showing Static Interfaces Assigned to an IPv6 Multicast Service



Multicast > MLD Snooping > MLD Member

Action: Show Static Member

VLAN: 1

MLD Member Interface List Total: 8

□	Multicast IPv6 Address	Interface
□	FF02::01:01:01:01	Unit 1 / Port 1
□	FF02::01:01:01:02	Unit 1 / Port 2
□	FF01::1	Unit 1 / Port 12
□	FF01::2	Unit 1 / Port 13
□	FF01::3	Unit 1 / Port 14
□	FF01::4	Unit 1 / Port 15
□	FF01::5	Unit 1 / Port 16
□	FF02::01:01:01:FF	Trunk 3

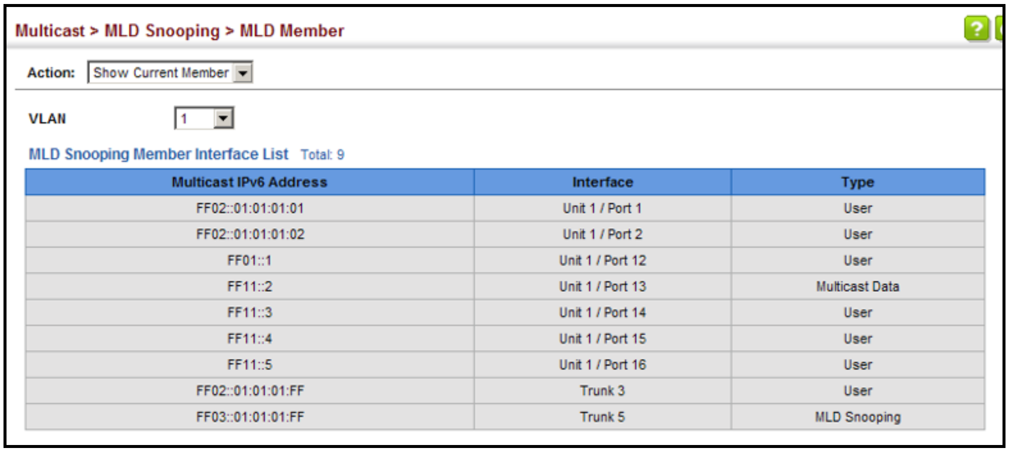
To display information about all IPv6 multicast groups, MLD Snooping or multicast routing must first be enabled on the switch. To show all of the interfaces statically or dynamically assigned to an IPv6 multicast service:

1. Click Multicast, MLD Snooping, MLD Member.

2. Select Show Current Member from the Action list.

3. Select the VLAN for which to display this information.

Figure 366: Showing Current Interfaces Assigned to an IPv6 Multicast Service



Multicast > MLD Snooping > MLD Member

Action: Show Current Member

VLAN 1

MLD Snooping Member Interface List Total: 9

Multicast IPv6 Address	Interface	Type
FF02::01:01:01:01	Unit 1 / Port 1	User
FF02::01:01:01:02	Unit 1 / Port 2	User
FF01::1	Unit 1 / Port 12	User
FF11::2	Unit 1 / Port 13	Multicast Data
FF11::3	Unit 1 / Port 14	User
FF11::4	Unit 1 / Port 15	User
FF11::5	Unit 1 / Port 16	User
FF02::01:01:01:FF	Trunk 3	User
FF03::01:01:01:FF	Trunk 5	MLD Snooping

SHOWING MLD SNOOPING GROUPS AND SOURCE LIST

Use the Multicast > MLD Snooping > Group Information page to display known multicast groups, member ports, the means by which each group was learned, and the corresponding source list.

CLI REFERENCES

- "show ipv6 mld snooping group source-list" on page 1477

PARAMETERS

These parameters are displayed:

- **VLAN** – VLAN identifier. (Range: 1-4094)

- **Interface** – Port or trunk identifier.

- **Group Address** – The IP address for a specific multicast service.

- **Type** – The means by which each group was learned – MLD Snooping or Multicast Data.

- **Filter Mode** – The filter mode is used to summarize the total listening state of a multicast address to a minimum set such that all nodes' listening states are respected. In Include mode, the router only uses the request list, indicating that the reception of packets sent to the specified multicast address is requested only from those IP source addresses listed in the hosts' source-list. In Exclude mode, the router only both the request list and exclude list, indicating that the reception of packets sent to the given multicast address is requested from all IP source addresses, except for those listed in the exclude source-list and for any other sources where the source timer status has expired.

- **Filter Timer Elapse** – The Filter timer is only used when a specific multicast address is in Exclude mode. It represents the time for the multicast address filter mode to expire and change to Include mode.

- **Request List** – Sources included on the router's request list.

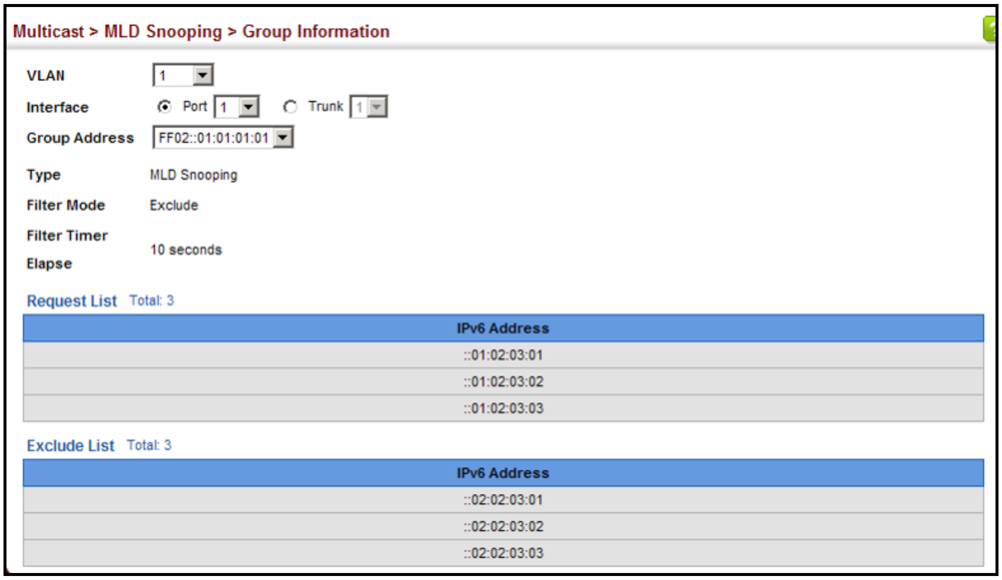
- **Exclude List** – Sources included on the router's exclude list.

WEB INTERFACE

To display known MLD multicast groups:

1. Click Multicast, MLD Snooping, Group Information.
2. Select the port or trunk, and then select a multicast service assigned to that interface.

Figure 367: Showing IPv6 Multicast Services and Corresponding Sources



Multicast > MLD Snooping > Group Information

VLAN: 1

Interface: ● Port 1 ○ Trunk 1

Group Address: FF02::01:01:01:01

Type: MLD Snooping

Filter Mode: Exclude

Filter Timer Elapse: 10 seconds

Request List Total: 3

IPv6 Address
::01:02:03:01
::01:02:03:02
::01:02:03:03

Exclude List Total: 3

IPv6 Address
::02:02:03:01
::02:02:03:02
::02:02:03:03

LAYER 3 IGMP (QUERY USED WITH MULTICAST ROUTING)

IGMP Snooping – IGMP Snooping (page 613) is a key part of the overall set of functions required to support multicast filtering. It is used to passively monitor IGMP service requests from multicast clients, and dynamically configure the switch ports which need to forward multicast traffic.

IGMP Query – Multicast query is used to poll each known multicast group for active members, and dynamically configure the switch ports which need to forward multicast traffic. Layer 3 IGMP Query, as described below, is used in conjunction with both Layer 2 IGMP Snooping and multicast routing.

IGMP – This protocol includes a form of multicast query specifically designed to work with multicast routing. A router periodically asks its hosts if they want to receive multicast traffic. It then propagates service requests on to any upstream multicast router to ensure that it will continue to receive the multicast service. IGMP can be enabled for individual VLAN interfaces (page 650).

NOTE: Multicast Routing Discovery (MRD) is used to discover which interfaces are attached to multicast routers. (For a description of this protocol, see “Multicast Router Discovery” on page 621.)

IGMP Proxy – A device can learn about the multicast service requirements of hosts attached to its downstream interfaces, proxy this group membership information to the upstream router, and forward multicast packets based on that information.

CONFIGURING IGMP PROXY ROUTING

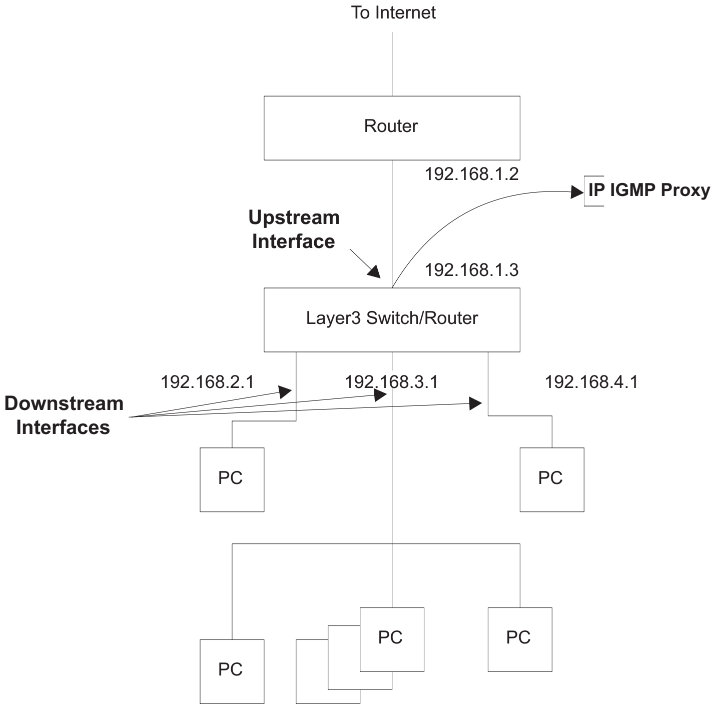
Use the Multicast > IGMP > Proxy page to configure IGMP Proxy Routing.

In simple network topologies, it is sufficient for a device to learn multicast requirements from its downstream interfaces and proxy this group membership information to the upstream router. Multicast packets can then be forwarded downstream based solely upon that information. This mechanism, known as IGMP proxy routing, enables the system to issue IGMP host messages on behalf of hosts that the system has discovered through standard IGMP interfaces.

CLI REFERENCES

- "IGMP Proxy Routing" on page 1523

Figure 368: IGMP Proxy Routing



Using IGMP proxy routing to forward multicast traffic on edge switches greatly reduces the processing load on those devices by not having to run more complicated multicast routing protocols such as PIM. It also makes the proxy devices independent of the multicast routing protocols used by core routers.

IGMP proxy routing uses a tree topology, where the root of the tree is connected to a complete multicast infrastructure (with the upstream interface connected to the Internet as shown in the figure above). In such a simple topology, it is sufficient to send the group membership information learned upstream, and then to forward multicast packets based upon that information to the downstream hosts. For the switch, IGMP proxy routing has only one upstream connection to the core network side and multiple downstream connections to the customer side.

The IGMP proxy routing tree must be manually configured by designating one upstream interface and multiple downstream interfaces on each proxy device. No other multicast routers except for the proxy devices can exist within the tree, and the root of the tree must be connected to a wider multicast infrastructure. Note that this protocol is limited to a single administrative domain.

In more complicated scenarios where the topology is not a tree (such as when there are diverse paths to multiple sources), a more robust failover mechanism should be used. If more than one administrative domain is involved, a multicast routing protocol should be used instead of IGMP proxy.

To enable IGMP proxy service, follow these steps:

1. Enable IP multicasting globally on the router (see "Configuring Global Settings for Multicast Routing" on page 828).

2. Enable IGMP on the downstream interfaces which require proxy multicast service (see "Configuring IGMP Interface Parameters" on page 650).

3. Enable IGMP proxy on the interface that is attached to an upstream multicast router using the proxy settings described in this section.

4. Optional – Indicate how often the system will send unsolicited reports to the upstream router using the Multicast > IGMP > Proxy page as described later in this section.

COMMAND USAGE

- When IGMP proxy is enabled on an interface, that interface is known as the upstream or host interface. This interface performs only the host portion of IGMP by sending IGMP membership reports, and automatically disables IGMP router functions.

- Interfaces with IGMP enabled, but not located in the direction of the multicast tree root are known as downstream or router interfaces. These interfaces perform the standard IGMP router functions by maintaining a database of all IGMP subscriptions on the downstream interface. IGMP must therefore be enabled on all interfaces which require proxy multicast service.

- The system periodically checks the multicast route table for (*,G) any-source multicast forwarding entries. When changes occur in the downstream IGMP groups, an IGMP state change report is created and sent to the upstream router.

- If there is an IGMPv1 or IGMPv2 querier on the upstream network, then the proxy device will act as an IGMPv1 or IGMPv2 host on the upstream interface accordingly, and set the v1/v2 query present timer to indicate that there is an active v1/v2 querier in this VLAN. Otherwise, it will act as an IGMPv3 host.

- Multicast routing protocols are not supported when IGMP proxy service is enabled.

- Only one upstream interface is supported on the system.

- A maximum of 1024 multicast entries are supported.

PARAMETERS

These parameters are displayed:

- **VLAN** – VLAN interface on which to configure IGMP proxy service. (Range: 1-4094)

- **IGMP Proxy Status** – Enables IGMP proxy service for multicast routing, forwarding IGMP membership information monitored on downstream interfaces onto the upstream interface in a summarized report. (Default: Disabled)

- **Unsolicited Report Interval** – Specifies how often the upstream interface should transmit unsolicited IGMP reports. (Range: 1-65535 seconds; Default: 400 seconds)

WEB INTERFACE

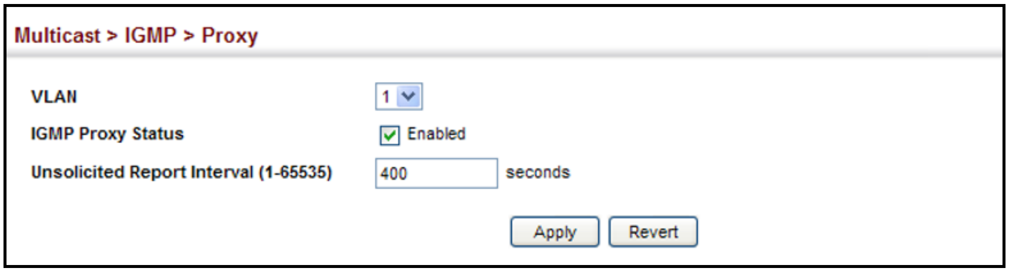
To configure IGMP Proxy Routing:

1. Click Multicast, IGMP, Proxy.

2. Select the upstream interface, enable the IGMP Proxy Status, and modify the interval for unsolicited IGMP reports if required.

3. Click Apply.

Figure 369: Configuring IGMP Proxy Routing



Multicast > IGMP > Proxy

VLAN: 1

IGMP Proxy Status: ☑ Enabled

Unsolicited Report Interval (1-65535): 400 seconds

CONFIGURING IGMP INTERFACE PARAMETERS

Use the Multicast > IGMP > Interface page to configure interface settings for IGMP.

The switch uses IGMP (Internet Group Management Protocol) to query for any attached hosts that want to receive a specific multicast service. The hosts may respond with several types of IP multicast messages. Hosts respond to queries with report messages that indicate which groups they want to join or the groups to which they already belong. If a router does not receive a report message within a specified period of time, it will prune that interface from the multicast tree. A host can also submit a join message at any time without waiting for a query from the router. Hosts can also signal when they no longer want to receive traffic for a specific group by sending a leave-group message.

If more than one router on the LAN is performing IP multicasting, one of these is elected as the “querier” and assumes the role of querying for group members. It then propagates the service request up to any neighboring multicast router to ensure that it will continue to receive the multicast service. The parameters described in this section are used to control Layer 3 IGMP and query functions.

NOTE: IGMP Protocol Status should be enabled on all the interfaces that need to support downstream multicast hosts (as described in this section).

NOTE: IGMP is disabled when multicast routing is disabled (see "Enabling Multicast Routing Globally" on page 828).

CLI REFERENCES

- "IGMP (Layer 3)" on page 1513

PARAMETERS

These parameters are displayed:

- **VLAN** – VLAN interface bound to a primary IP address. (Range: 1-4094)

- **IGMP Protocol Status** – Enables IGMP (including IGMP query functions) on a VLAN interface. (Default: Disabled)

  When a multicast routing protocol, such as PIM, is enabled, IGMP is also enabled.

- **IGMP Version** – Configures the IGMP version used on an interface. (Options: Version 1-3; Default: Version 2)

- **Robustness Variable** – Specifies the robustness (or expected packet loss) for this interface. The robustness value is used in calculating the appropriate range for other IGMP variables, such as the Group Membership Interval, as well as the Other Querier Present Interval, and the Startup Query Count (RFC 2236). (Range: 1-255; Default: 2)

  Routers adopt the robustness value from the most recently received query. If the querier's robustness variable (QRV) is zero, indicating that the QRV field does not contain a declared robustness value, the switch will set the robustness variable to the value statically configured by this command. If the QRV exceeds 7, the maximum value of the QRV field, the robustness value is set to zero, meaning that this device will not advertise a QRV in any query messages it subsequently sends.

- **Query Interval** – Configures the frequency at which host query messages are sent. (Range: 1-255; Default: 125 seconds)

  Multicast routers send host query messages to determine the interfaces that are connected to downstream hosts requesting a specific multicast service. Only the designated multicast router for a subnet sends host query messages, which are addressed to the multicast address 224.0.0.1, and use a time-to-live (TTL) value of 1.

  For IGMP Version 1, the designated router is elected according to the multicast routing protocol that runs on the LAN. But for IGMP Version 2 and 3, the designated querier is the lowest IP-addressed multicast router on the subnet.

- **Query Max Response Time** – Configures the maximum response time advertised in IGMP queries. (Range: 0-255 tenths of a second; Default: 10 seconds)

  IGMPv1 does not support a configurable maximum response time for query messages. It is fixed at 10 seconds for IGMPv1.

  By varying the Query Maximum Response Time, the burstiness of IGMP messages passed on the subnet can be tuned; where larger values make the traffic less bursty, as host responses are spread out over a larger interval.

  The number of seconds represented by the maximum response interval must be less than the Query Interval.

- **Last Member Query Interval** – The frequency at which to send IGMP group-specific or IGMPv3 group-source-specific query messages in response to receiving a group-specific or group-source-specific leave message. (Range: 1-255 tenths of a second; Default: 1 second)

  When the switch receives an IGMPv2 or IGMPv3 leave message from a host that wants to leave a multicast group, source or channel, it sends a number of group-specific or group-source-specific query messages as defined by the Last Member Query Count at intervals defined by the Last Member Query Interval. If no response is received after this period, the -switch stops forwarding for the group, source or channel.

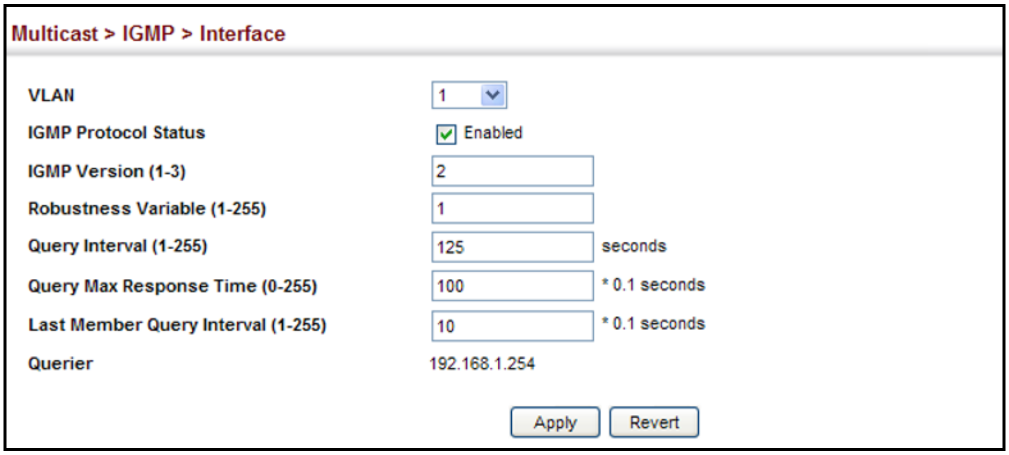
- **Querier** – Device currently serving as the IGMP querier for this multicast service. A querier can only be displayed if IGMP multicasting is enabled, the VLAN for this entry is up, and is configured with a valid IP address.

WEB INTERFACE

To configure IGMP interface settings:

1. Click Multicast, IGMP, Interface.
2. Select each interface that will support IGMP (Layer 3), and set the required IGMP parameters.
3. Click Apply.

Figure 370: Configuring IGMP Interface Settings



Multicast > IGMP > Interface

VLAN	1	
IGMP Protocol Status	☑ Enabled	
IGMP Version (1-3)	2	
Robustness Variable (1-255)	1	
Query Interval (1-255)	125	seconds
Query Max Response Time (0-255)	100	* 0.1 seconds
Last Member Query Interval (1-255)	10	* 0.1 seconds
Querier	192.168.1.254	

CONFIGURING STATIC IGMP GROUP MEMBERSHIP

Use the Multicast > IGMP > Static Group page to manually propagate traffic from specific multicast groups onto the specified VLAN interface.

CLI REFERENCES

- "ip igmp static-group" on page 1518

COMMAND USAGE

- Group addresses within the entire multicast group address range can be specified. However, if any address within the source-specific multicast (SSM) address range (default 232/8) is specified, but no source address is included, the request to join the multicast group will fail unless the next node up the reverse path tree has statically mapped this group to a specific source address. Also, if an address outside of the SSM address range is specified, and a specific source address is included in the command, the request to join the multicast group will also fail if the next node up the reverse path tree has enabled the PIM-SSM protocol.

- If a static group is configured for an any-source multicast (*,G), a source address cannot subsequently be defined for this group without first deleting the entry.

- If a static group is configured for one or more source-specific multicasts (S,G), an any-source multicast (*,G) cannot subsequently be defined for this group without first deleting all of the associated (S,G) entries.

- The switch supports a maximum of 64 static group entries.

PARAMETERS

These parameters are displayed:

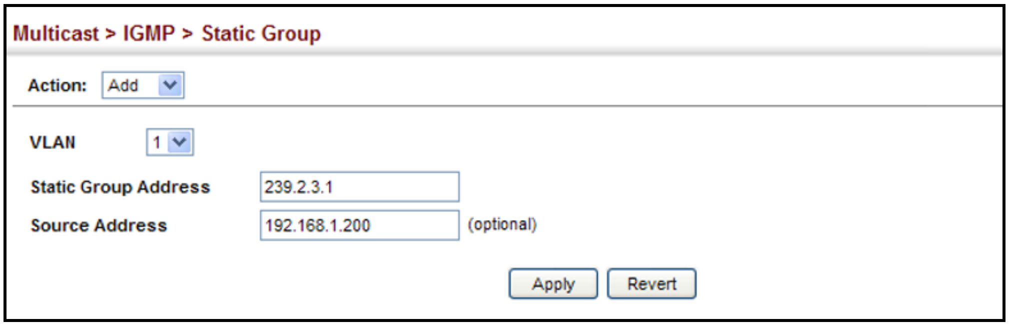
- **VLAN** – VLAN interface to assign as a static member of the specified multicast group. (Range: 1-4094)
- **Static Group Address** – An IP multicast group address. (The group addresses specified cannot be in the range of 224.0.0.1 - 239.255.255.255.)
- **Source Address** – The source address of a multicast server transmitting traffic to the specified multicast group address.

WEB INTERFACE

To configure static IGMP groups:

1. Click Multicast, IGMP, Static Group.
2. Select Add from the Action list.
3. Select a VLAN interface to be assigned as a static multicast group member, and then specify the multicast group. If source-specific multicasting is supported by the next hop router in the reverse path tree for the specified multicast group, then the source address should also be specified.
4. Click Apply.

Figure 371: Configuring Static IGMP Groups



Multicast > IGMP > Static Group

Action: Add

VLAN 1

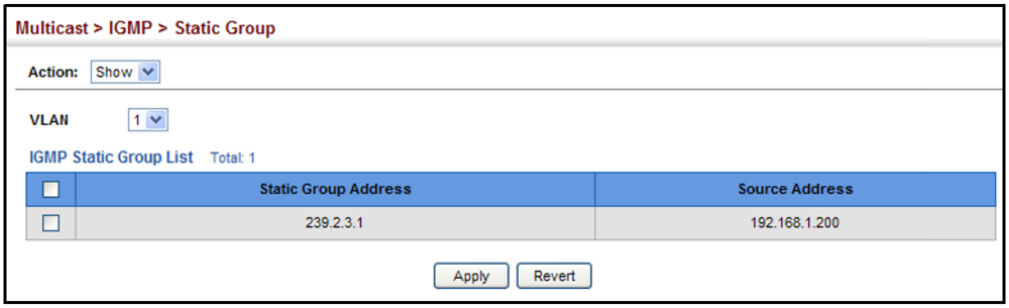
Static Group Address 239.2.3.1

Source Address 192.168.1.200 (optional)

To display configured static IGMP groups:

1. Click Multicast, IGMP, Static Group.
2. Select Show from the Action list.
3. Click Apply.

Figure 372: Showing Static IGMP Groups



Multicast > IGMP > Static Group

Action: Show

VLAN 1

IGMP Static Group List Total: 1

□	Static Group Address	Source Address
□	239.2.3.1	192.168.1.200

DISPLAYING MULTICAST GROUP INFORMATION

When IGMP (Layer 3) is enabled on the switch, use the Multicast > IGMP > Group Information pages to display the current multicast groups learned through IGMP. When IGMP (Layer 3) is disabled and IGMP (Layer 2) is enabled, the active multicast groups can be viewed on the Multicast > IGMP Snooping > Forwarding Entry page (see page 628).

COMMAND USAGE

To display information about multicast groups, IGMP must first be enabled on the interface to which a group has been assigned (see "Configuring IGMP Interface Parameters" on page 650), and multicast routing must be enabled globally on the system (see "Configuring Global Settings for Multicast Routing" on page 828).

CLI REFERENCES

- "show ip igmp groups" on page 1520

PARAMETERS

These parameters are displayed:

Show Information

- **VLAN** – VLAN identifier. The selected entry must be a configured IP interface. (Range: 1-4094)
- **Group Address** – IP multicast group address with subscribers directly attached or downstream from the switch.
- **Last Reporter** – The IP address of the source of the last membership report received for this multicast group address on this interface.
- **Up Time** – The time elapsed since this entry was created. (Depending on the elapsed time, information may displayed for w:weeks, d:days, h:hours, m:minutes, or s:seconds.)
- **Expire** – The time remaining before this entry will be aged out. (Default: 260 seconds)

  This parameter displays “stopped” if the Group Mode is INCLUDE.

- **V1 Timer** – The time remaining until the switch assumes that there are no longer any IGMP Version 1 members on the IP subnet attached to this interface.
  - If the switch receives an IGMP Version 1 Membership Report, it sets a timer to note that there are Version 1 hosts present which are members of the group for which it heard the report.
  - If there are Version 1 hosts present for a particular group, the switch will ignore any Leave Group messages that it receives for that group.

Show Details

The following additional information is displayed on this page:

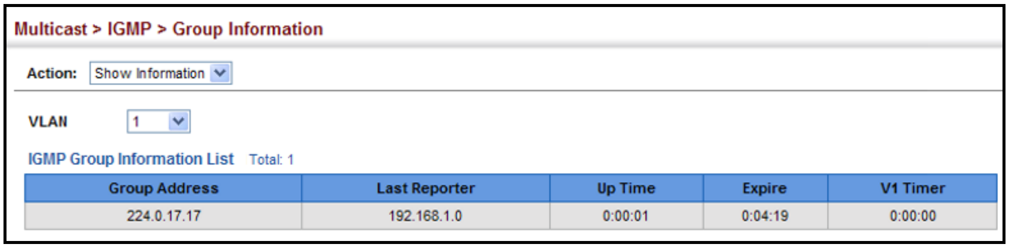
- **VLAN** – VLAN identifier. The selected entry must be a configured IP interface. (Range: 1-4094)
- **Group Address** – IP multicast group address with subscribers directly attached or downstream from the switch, or a static multicast group assigned to this interface.
- **Interface** – The interface on the switch that has received traffic directed to the multicast group address.
- **Up Time** – The time elapsed since this entry was created. (Depending on the elapsed time, information may displayed for w:weeks, d:days, h:hours, m:minutes, or s:seconds.)
- **Group Mode** – In INCLUDE mode, reception of packets sent to the specified multicast address is requested only from those IP source addresses listed in the source-list parameter. In EXCLUDE mode, reception of packets sent to the given multicast address is requested from all IP source addresses, except for those listed in the source-list parameter and for any other sources where the source timer status has expired.
- **Group Source List** – A list of zero or more IP unicast addresses from which multicast reception is desired or not desired, depending on the filter mode.
  - **Source Address** – The address of one of the multicast servers transmitting traffic to the specified group.
  - **Up Time** – The time elapsed since this entry was created. (Depending on the elapsed time, information may displayed for w:weeks, d:days, h:hours, m:minutes, or s:seconds.)
  - **V3 Expire** – The time remaining before this entry will be aged out. The V3 label indicates that the expire time is only provided for sources learned through IGMP Version 3. (The default is 260 seconds.)
  - **Forward** – Indicates whether or not traffic will be forwarded from the multicast source.

WEB INTERFACE

To display the current multicast groups learned through IGMP:

1. Click Multicast, IGMP, Group Information.
2. Select Show Information from the Action list.
3. Select a VLAN. The selected entry must be a configured IP interface.

Figure 373: Displaying Multicast Groups Learned from IGMP (Information)



Multicast > IGMP > Group Information

Action: Show Information

VLAN 1

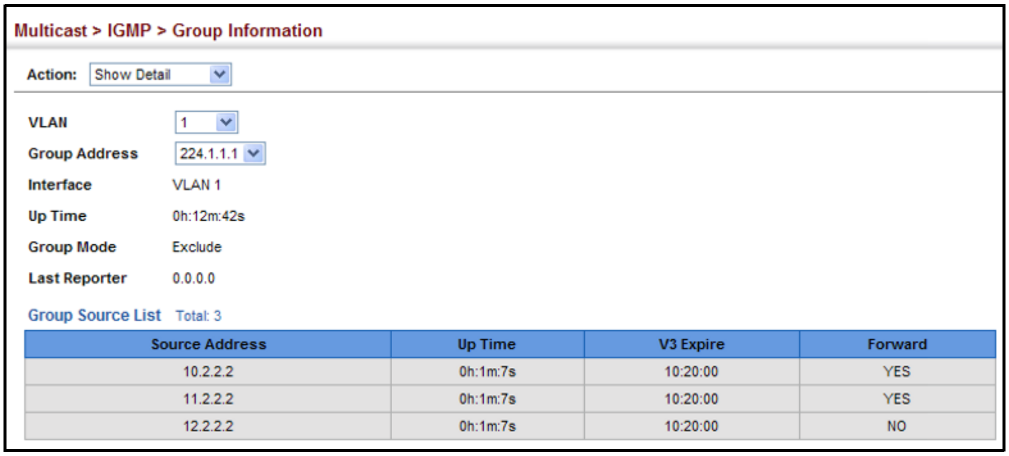
IGMP Group Information List Total: 1

Group Address	Last Reporter	Up Time	Expire	V1 Timer
224.0.17.17	192.168.1.0	0:00:01	0:04:19	0:00:00

To display detailed information about the current multicast groups learned through IGMP:

1. Click Multicast, IGMP, Group Information.
2. Select Show Details from the Action list.
3. Select a VLAN. The selected entry must be a configured IP interface.

Figure 374: Displaying Multicast Groups Learned from IGMP (Detail)



Multicast > IGMP > Group Information

Action: Show Detail

VLAN 1
Group Address 224.1.1.1
Interface VLAN 1
Up Time 0h:12m:42s
Group Mode Exclude
Last Reporter 0.0.0.0

Group Source List Total: 3

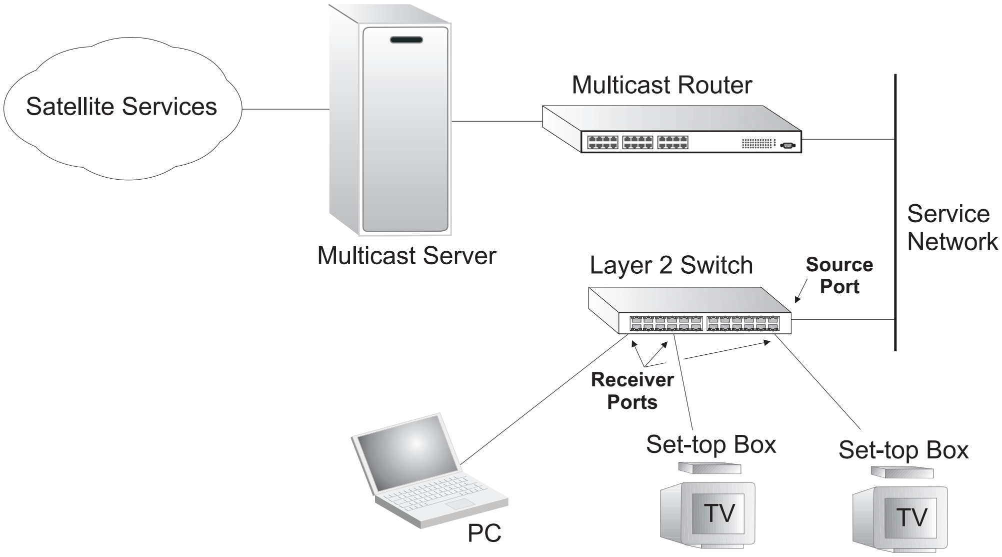
Source Address	Up Time	V3 Expire	Forward
10.2.2.2	0h:1m:7s	10:20:00	YES
11.2.2.2	0h:1m:7s	10:20:00	YES
12.2.2.2	0h:1m:7s	10:20:00	NO

MULTICAST VLAN REGISTRATION FOR IPV4

Multicast VLAN Registration (MVR) is a protocol that controls access to a single network-wide VLAN most commonly used for transmitting multicast traffic (such as television channels or video-on-demand) across a service provider's network. Any multicast traffic entering an MVR VLAN is sent to all attached subscribers. This protocol can significantly reduce to processing overhead required to dynamically monitor and establish the distribution tree for a normal multicast VLAN. This makes it possible to support common multicast services over a wide part of the network without having to use any multicast routing protocol.

MVR maintains the user isolation and data security provided by VLAN segregation by passing only multicast traffic into other VLANs to which the subscribers belong. Even though common multicast streams are passed onto different VLAN groups from the MVR VLAN, users in different IEEE 802.1Q or private VLANs cannot exchange any information (except through upper-level routing services).

Figure 375: MVR Concept



COMMAND USAGE

- General Configuration Guidelines for MVR:

  1. Enable MVR for a domain on the switch, and select the MVR VLAN (see "Configuring MVR Domain Settings" on page 660).
  2. Create an MVR profile by specifying the multicast groups that will stream traffic to attached hosts, and assign the profile to an MVR domain (see "Configuring MVR Group Address Profiles" on page 662).
  3. Set the interfaces that will join the MVR as source ports or receiver ports (see "Configuring MVR Interface Status" on page 665).
  4. For multicast streams that will run for a long term and be associated with a stable set of hosts, you can statically bind the multicast

group to the participating interfaces (see "Assigning Static MVR Multicast Groups to Interfaces" on page 667).

- Although MVR operates on the underlying mechanism of IGMP snooping, the two features operate independently of each other. One can be enabled or disabled without affecting the behavior of the other. However, if IGMP snooping and MVR are both enabled, MVR reacts only to join and leave messages from multicast groups configured under MVR. Join and leave messages from all other multicast groups are managed by IGMP snooping. Also, note that only IGMP version 2 or 3 hosts can issue multicast join or leave messages.

CONFIGURING MVR GLOBAL SETTINGS

Use the Multicast > MVR (Configure Global) page to configure proxy switching and the robustness variable.

CLI REFERENCES

- "MVR for IPv4" on page 1478

PARAMETERS

These parameters are displayed:

- **Proxy Switching** – Configures MVR proxy switching, where the source port acts as a host, and the receiver port acts as an MVR router with querier service enabled. (Default: Enabled)
  - When MVR proxy-switching is enabled, an MVR source port serves as the upstream or host interface, and the MVR receiver port serves as the querier. The source port performs only the host portion of MVR by sending summarized membership reports, and automatically disables MVR router functions.
  - Receiver ports are known as downstream or router interfaces. These interfaces perform the standard MVR router functions by maintaining a database of all MVR subscriptions on the downstream interface. Receiver ports must therefore be configured on all downstream interfaces which require MVR proxy service.
  - When the source port receives report and leave messages, it only forwards them to other source ports.
  - When receiver ports receive any query messages, they are dropped.
  - When changes occurring in the downstream MVR groups are learned by the receiver ports through report and leave messages, an MVR state change report is created and sent to the upstream source port, which in turn forwards this information upstream.
  - When MVR proxy switching is disabled:
    - Any membership reports received from receiver/source ports are forwarded to all source ports.

    - When a source port receives a query message, it will be forwarded to all downstream receiver ports.
    - When a receiver port receives a query message, it will be dropped.

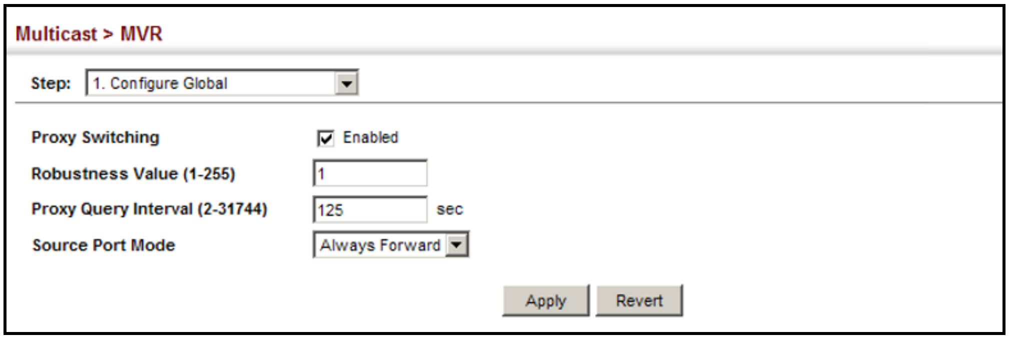
- **Robustness Value** – Configures the expected packet loss, and thereby the number of times to generate report and group-specific queries. (Range: 1-255; Default: 1)
  - This parameter is used to set the number of times report messages are sent upstream when changes are learned about downstream groups, and the number of times group-specific queries are sent to downstream receiver ports.
  - This parameter only takes effect when MVR proxy switching is enabled.
- **Proxy Query Interval** – Configures the interval at which the receiver port sends out general queries. (Range: 2-31744 seconds; Default: 125 seconds)
  - This parameter sets the general query interval at which active receiver ports send out general queries.
  - This interval is only effective when proxy switching is enabled.
- **Source Port Mode** – Configures the switch to forward any multicast streams within the parameters set by a profile, or to only forward multicast streams which the source port has dynamically joined.
  - **Always Forward** – By default, the switch forwards any multicast streams within the address range set by a profile, and bound to a domain. The multicast streams are sent to all source ports on the switch and to all receiver ports that have elected to receive data on that multicast address. (This is the default setting.)
  - **Dynamic** – When dynamic mode is enabled, the switch only forwards multicast streams which the source port has dynamically joined. In other words, both the receiver port and source port must subscribe to a multicast group before a multicast stream is forwarded to any attached client. Note that the requested streams are still restricted to the address range which has been specified in a profile and bound to a domain.

WEB INTERFACE

To configure global settings for MVR:

1. Click Multicast, MVR.
2. Select Configure Global from the Step list.
3. Set the status for MVR proxy switching, the robustness value used for report and query messages, the proxy query interval, and source port mode.
4. Click Apply.

Figure 376: Configuring Global Settings for MVR


Multicast > MVR

Step: 1. Configure Global

Proxy Switching ☑ Enabled
Robustness Value (1-255) 1
Proxy Query Interval (2-31744) 125 sec
Source Port Mode Always Forward

CONFIGURING MVR DOMAIN SETTINGS

Use the Multicast > MVR (Configure Domain) page to enable MVR globally on the switch, and select the VLAN that will serve as the sole channel for common multicast streams supported by the service provider.

CLI REFERENCES

- "MVR for IPv4" on page 1478

PARAMETERS

These parameters are displayed:

- **Domain ID** – An independent multicast domain. (Range: 1-5)
- **MVR Status** – When MVR is enabled on the switch, any multicast data associated with an MVR group is sent from all designated source ports, to all receiver ports that have registered to receive data from that multicast group. (Default: Disabled)
- **MVR VLAN** – Identifier of the VLAN that serves as the channel for streaming multicast services using MVR. MVR source ports should be configured as members of the MVR VLAN (see "Adding Static Members to VLANs" on page 231), but MVR receiver ports should not be manually configured as members of this VLAN. (Default: 1)
- **MVR Running Status** – Indicates whether or not all necessary conditions in the MVR environment are satisfied. Running status is Active as long as MVR is enabled, the specified MVR VLAN exists, and a

source port with a valid link has been configured (see "Configuring MVR Interface Status" on page 665).

- **MVR Current Learned Groups** – The number of MVR groups currently assigned to this domain.

- **Forwarding Priority** – The CoS priority assigned to all multicast traffic forwarded into this domain. (Range: 0-7, where 7 is the highest priority)

  This parameter can be used to set a high priority for low-latency multicast traffic such as a video-conference, or to set a low priority for normal multicast traffic not sensitive to latency.

- **Upstream Source IP** – The source IP address assigned to all MVR control packets sent upstream on the specified domain. By default, all MVR reports sent upstream use a null source IP address.

WEB INTERFACE

To configure settings for an MVR domain:

1. Click Multicast, MVR.

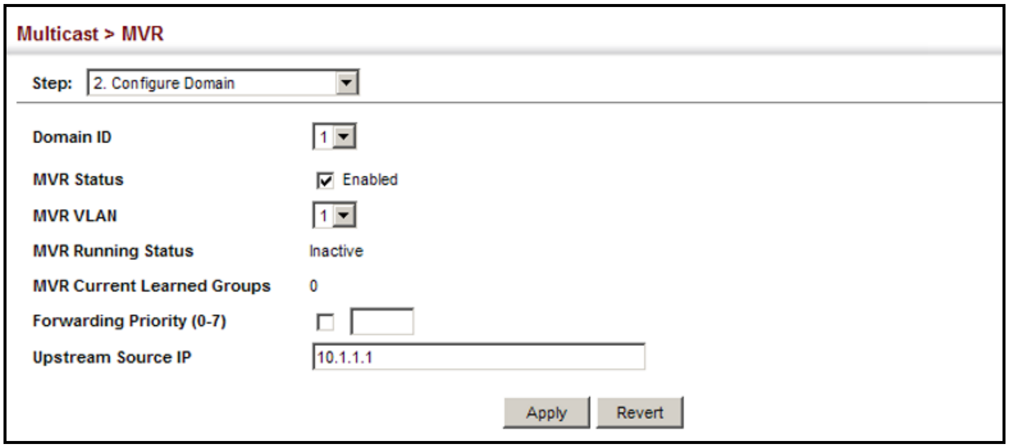
2. Select Configure Domain from the Step list.

3. Select a domain from the scroll-down list.

4. Enable MVR for the selected domain, select the MVR VLAN, set the forwarding priority to be assigned to all ingress multicast traffic, and set the source IP address for all control packets sent upstream as required.

5. Click Apply.

Figure 377: Configuring Domain Settings for MVR



Multicast > MVR

Step: 2. Configure Domain

Domain ID	1
MVR Status	☑ Enabled
MVR VLAN	1
MVR Running Status	Inactive
MVR Current Learned Groups	0
Forwarding Priority (0-7)	□
Upstream Source IP	10.1.1.1

CONFIGURING MVR GROUP ADDRESS PROFILES

Use the Multicast > MVR (Configure Profile and Associate Profile) pages to assign the multicast group address for required services to one or more MVR domains.

CLI REFERENCES

- "MVR for IPv4" on page 1478

COMMAND USAGE

- Use the Configure Profile page to statically configure all multicast group addresses that will join the MVR VLAN. Any multicast data associated with an MVR group is sent from all source ports to all receiver ports that have registered to receive data from that multicast group.
- The IP address range from 224.0.0.0 to 239.255.255.255 is used for multicast streams. MVR group addresses cannot fall within the reserved IP multicast address range of 224.0.0.x.
- IGMP snooping and MVR share a maximum number of 1024 groups. Any multicast streams received in excess of this limitation will be flooded to all ports in the associated domain.

PARAMETERS

These parameters are displayed:

Configure Profile

- **Profile Name** – The name of a profile containing one or more MVR group addresses. (Range: 1-21 characters)
- **Start IP Address** – Starting IP address for an MVR multicast group. (Range: 224.0.1.0 - 239.255.255.255)
- **End IP Address** – Ending IP address for an MVR multicast group. (Range: 224.0.1.0 - 239.255.255.255)

Associate Profile

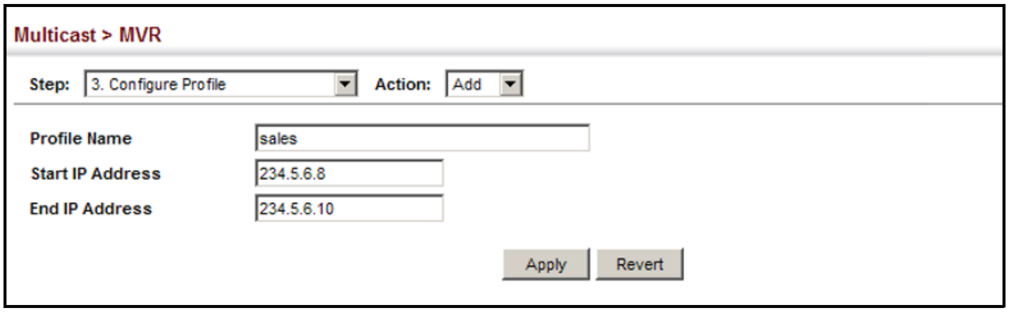
- **Domain ID** – An independent multicast domain. (Range: 1-5)
- **Profile Name** – The name of a profile to be assigned to this domain. (Range: 1-21 characters)

WEB INTERFACE

To configure an MVR group address profile:

1. Click Multicast, MVR.
2. Select Configure Profile from the Step list.
3. Select Add from the Action list.
4. Enter the name of a group profile to be assigned to one or more domains, and specify a multicast group that will stream traffic to participating hosts.
5. Click Apply.

Figure 378: Configuring an MVR Group Address Profile



Multicast > MVR

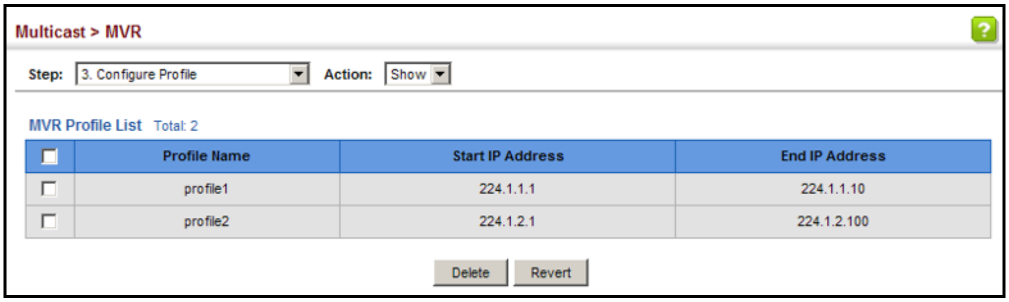
Step: 3. Configure Profile Action: Add

Profile Name: sales
Start IP Address: 234.5.6.8
End IP Address: 234.5.6.10

To show the configured MVR group address profiles:

1. Click Multicast, MVR.
2. Select Configure Profile from the Step list.
3. Select Show from the Action list.

Figure 379: Displaying MVR Group Address Profiles



Multicast > MVR

Step: 3. Configure Profile Action: Show

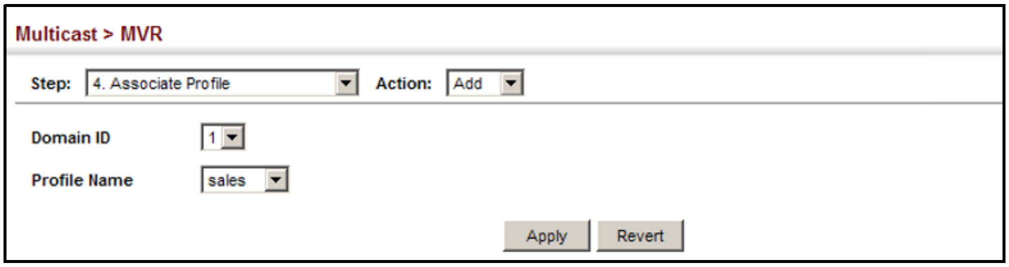
MVR Profile List Total: 2

□	Profile Name	Start IP Address	End IP Address
□	profile1	224.1.1.1	224.1.1.10
□	profile2	224.1.2.1	224.1.2.100

To assign an MVR group address profile to a domain:

1. Click Multicast, MVR.
2. Select Associate Profile from the Step list.
3. Select Add from the Action list.
4. Select a domain from the scroll-down list, and enter the name of a group profile.
5. Click Apply.

Figure 380: Assigning an MVR Group Address Profile to a Domain



Multicast > MVR

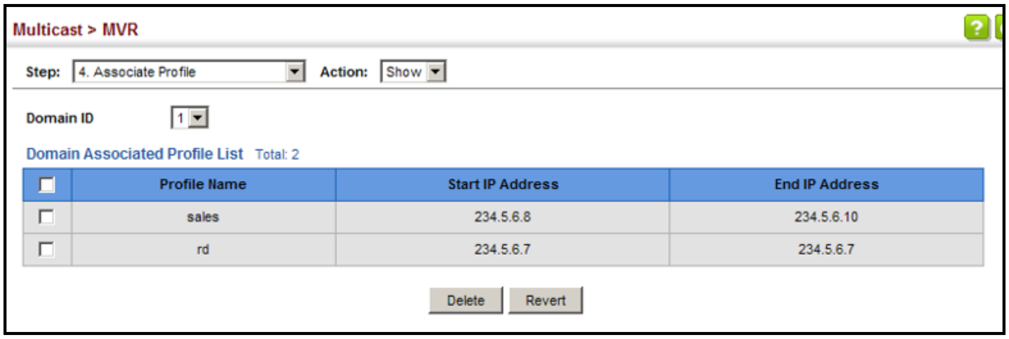
Step: 4. Associate Profile
Action: Add

Domain ID: 1
Profile Name: sales

To show the MVR group address profiles assigned to a domain:

1. Click Multicast, MVR.
2. Select Associate Profile from the Step list.
3. Select Show from the Action list.

Figure 381: Showing the MVR Group Address Profiles Assigned to a Domain



Multicast > MVR

Step: 4. Associate Profile
Action: Show

Domain ID: 1

Domain Associated Profile List Total: 2

□	Profile Name	Start IP Address	End IP Address
□	sales	234.5.6.8	234.5.6.10
□	rd	234.5.6.7	234.5.6.7

CONFIGURING MVR INTERFACE STATUS

Use the Multicast > MVR (Configure Interface) page to configure each interface that participates in the MVR protocol as a source port or receiver port. If you are sure that only one subscriber attached to an interface is receiving multicast services, you can enable the immediate leave function.

CLI REFERENCES

- "MVR for IPv4" on page 1478

COMMAND USAGE

- A port configured as an MVR receiver or source port can join or leave multicast groups configured under MVR. However, note that these ports can also use IGMP snooping to join or leave any other multicast groups using the standard rules for multicast filtering.

- Receiver ports can belong to different VLANs, but should not be configured as a member of the MVR VLAN. MVR allows a receiver port to dynamically join or leave multicast groups within an MVR VLAN. Multicast groups can also be statically assigned to a receiver port (see "Assigning Static MVR Multicast Groups to Interfaces" on page 667).

  Receiver ports should not be statically configured as a member of the MVR VLAN. If so configured, its MVR status will be inactive.

- One or more interfaces may be configured as MVR source ports. A source port is able to both receive and send data for configured MVR groups or for groups which have been statically assigned (see "Assigning Static MVR Multicast Groups to Interfaces" on page 667).

  All source ports must belong to the MVR VLAN.

  Subscribers should not be directly connected to source ports.

- Immediate leave applies only to receiver ports. When enabled, the receiver port is immediately removed from the multicast group identified in the leave message. When immediate leave is disabled, the switch follows the standard rules by sending a query message to the receiver port and waiting for a response to determine if there are any remaining subscribers for that multicast group before removing the port from the group list.

  - Using immediate leave can speed up leave latency, but should only be enabled on a port attached to one multicast subscriber to avoid disrupting services to other group members attached to the same interface.

  - Immediate leave does not apply to multicast groups which have been statically assigned to a port.

PARAMETERS

These parameters are displayed:

- **Domain ID** – An independent multicast domain. (Range: 1-5)

- **Port/Trunk** – Interface identifier.

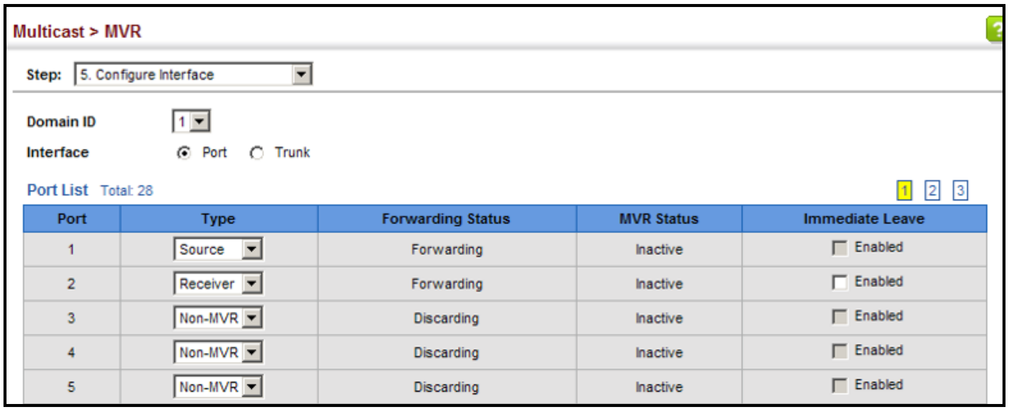
- **Type** – The following interface types are supported:
  - **Source** – An uplink port that can send and receive multicast data for the groups assigned to the MVR VLAN. Note that the source port must be manually configured as a member of the MVR VLAN (see "Adding Static Members to VLANs" on page 231).
  - **Receiver** – A subscriber port that can receive multicast data sent through the MVR VLAN. Any port configured as an receiver port will be dynamically added to the MVR VLAN when it forwards an IGMP report or join message from an attached host requesting any of the designated multicast services supported by the MVR VLAN. Just remember that only IGMP version 2 or 3 hosts can issue multicast join or leave messages. If MVR must be configured for an IGMP version 1 host, the multicast groups must be statically assigned (see "Assigning Static MVR Multicast Groups to Interfaces" on page 667).
  - **Non-MVR** – An interface that does not participate in the MVR VLAN. (This is the default type.)
- **Forwarding Status** – Shows if MVR traffic is being forwarded or discarded.
- **MVR Status** – Shows the MVR status. MVR status for source ports is “Active” if MVR is globally enabled on the switch. MVR status for receiver ports is “Active” only if there are subscribers receiving multicast traffic from one of the MVR groups, or a multicast group has been statically assigned to an interface.
- **Immediate Leave** – Configures the switch to immediately remove an interface from a multicast stream as soon as it receives a leave message for that group. (This option only applies to an interface configured as an MVR receiver.)

WEB INTERFACE

To configure interface settings for MVR:

1. Click Multicast, MVR.
2. Select Configure Interface from the Step list.
3. Select Configure Port or Configure Trunk from the Action list.
4. Select an MVR domain.
5. Set each port that will participate in the MVR protocol as a source port or receiver port, and optionally enable Immediate Leave on any receiver port to which only one subscriber is attached.
6. Click Apply.

Figure 382: Configuring Interface Settings for MVR



Multicast > MVR

Step: 5. Configure Interface

Domain ID: 1

Interface: ● Port ○ Trunk

Port List Total: 28

Port	Type	Forwarding Status	MVR Status	Immediate Leave
1	Source	Forwarding	Inactive	□ Enabled
2	Receiver	Forwarding	Inactive	□ Enabled
3	Non-MVR	Discarding	Inactive	□ Enabled
4	Non-MVR	Discarding	Inactive	□ Enabled
5	Non-MVR	Discarding	Inactive	□ Enabled

ASSIGNING STATIC MVR MULTICAST GROUPS TO INTERFACES

Use the Multicast > MVR (Configure Static Group Member) page to statically bind multicast groups to a port which will receive long-term multicast streams associated with a stable set of hosts.

CLI REFERENCES

- "mvr vlan group" on page 1488

COMMAND USAGE

- Multicast groups can be statically assigned to a receiver port using this configuration page.
- The IP address range from 224.0.0.0 to 239.255.255.255 is used for multicast streams. MVR group addresses cannot fall within the reserved IP multicast address range of 224.0.0.x.
- Only IGMP version 2 or 3 hosts can issue multicast join or leave messages. If MVR must be configured for an IGMP version 1 host, the multicast groups must be statically assigned.
- The MVR VLAN cannot be specified as the receiver VLAN for static bindings.

PARAMETERS

These parameters are displayed:

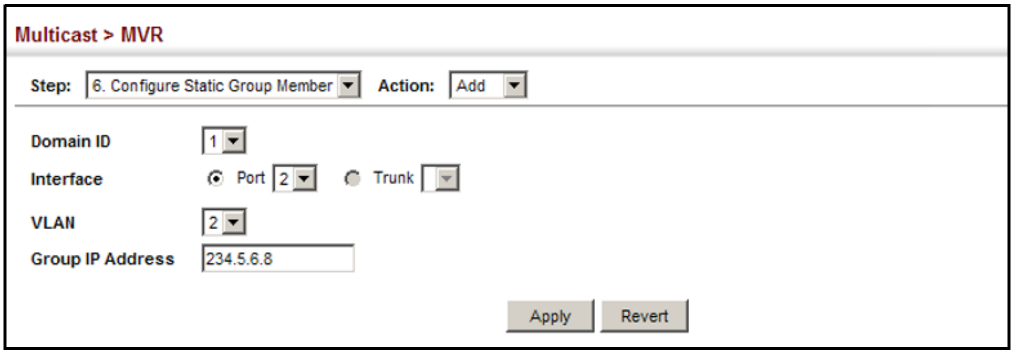
- **Domain ID** – An independent multicast domain. (Range: 1-5)
- **Interface** – Port or trunk identifier.
- **VLAN** – VLAN identifier. (Range: 1-4094)
- **Group IP Address** – Defines a multicast service sent to the selected port. Multicast groups must be assigned from the MVR group range configured on the Configure General page.

WEB INTERFACE

To assign a static MVR group to an interface:

1. Click Multicast, MVR.
2. Select Configure Static Group Member from the Step list.
3. Select Add from the Action list.
4. Select an MVR domain.
5. Select a VLAN and interface to receive the multicast stream, and then enter the multicast group address.
6. Click Apply.

Figure 383: Assigning Static MVR Groups to a Port



Multicast > MVR

Step: 6. Configure Static Group Member Action: Add

Domain ID: 1

Interface: ● Port 2 ○ Trunk

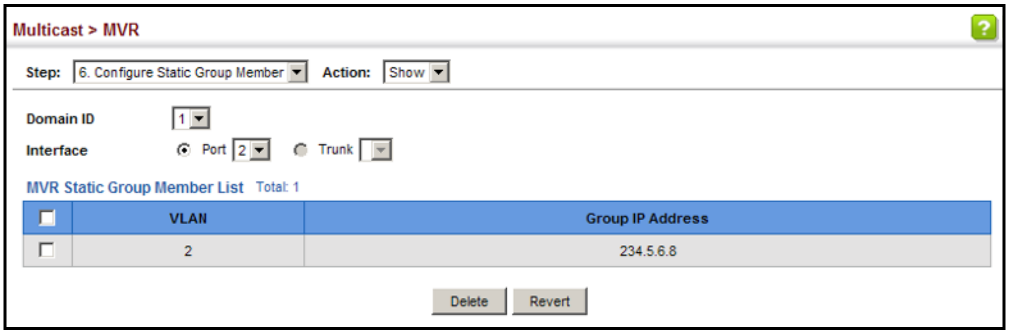
VLAN: 2

Group IP Address: 234.5.6.8

To show the static MVR groups assigned to an interface:

1. Click Multicast, MVR.
2. Select Configure Static Group Member from the Step list.
3. Select Show from the Action list.
4. Select an MVR domain.
5. Select the port or trunk for which to display this information.

Figure 384: Showing the Static MVR Groups Assigned to a Port



Multicast > MVR

Step: 6. Configure Static Group Member Action: Show

Domain ID: 1

Interface: ● Port 2 ○ Trunk

MVR Static Group Member List Total: 1

□	VLAN	Group IP Address
□	2	234.5.6.8

Displaying MVR Receiver Groups

Use the Multicast > MVR (Show Member) page to show the multicast groups either statically or dynamically assigned to the MVR receiver groups on each interface.

CLI References

- "show mvr members" on page 1492

Parameters

These parameters are displayed:

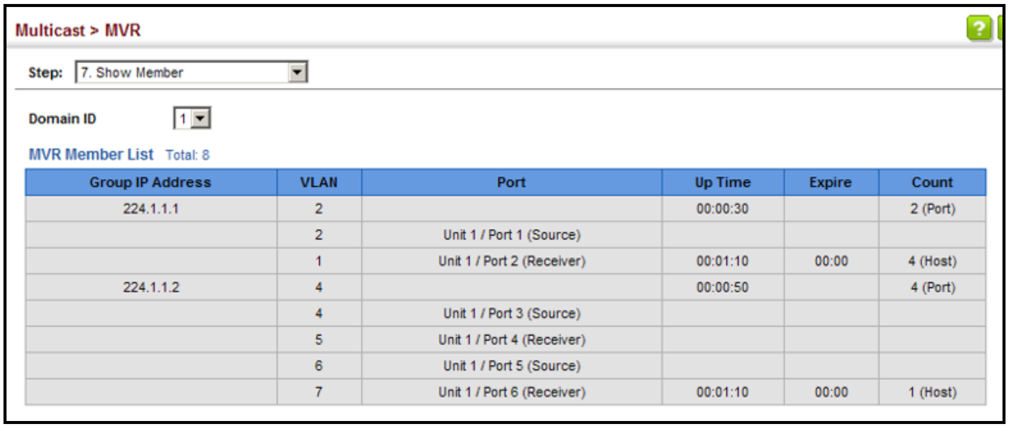
- **Domain ID** – An independent multicast domain. (Range: 1-5)
- **Group IP Address** – Multicast groups assigned to the MVR VLAN.
- **VLAN** – The VLAN through which the service is received. Note that this may be different from the MVR VLAN if the group address has been statically assigned.
- **Port** – Shows the interfaces with subscribers for multicast services provided through the MVR VLAN.
- **Up Time** – Time this service has been forwarded to attached clients.
- **Expire** – Time before this entry expires if no membership report is received from currently active or new clients.
- **Count** – The number of multicast services currently being forwarded from the MVR VLAN.

Web Interface

To display the interfaces assigned to the MVR receiver groups:

1. Click Multicast, MVR.
2. Select Show Member from the Step list.
3. Select an MVR domain.

Figure 385: Displaying MVR Receiver Groups



Multicast > MVR

Step: 7. Show Member

Domain ID 1

MVR Member List Total: 8

Group IP Address	VLAN	Port	Up Time	Expire	Count
224.1.1.1	2		00:00:30		2 (Port)
	2	Unit 1 / Port 1 (Source)			
	1	Unit 1 / Port 2 (Receiver)	00:01:10	00:00	4 (Host)
224.1.1.2	4		00:00:50		4 (Port)
	4	Unit 1 / Port 3 (Source)			
	5	Unit 1 / Port 4 (Receiver)			
	6	Unit 1 / Port 5 (Source)			
	7	Unit 1 / Port 6 (Receiver)	00:01:10	00:00	1 (Host)

DISPLAYING MVR STATISTICS

Use the Multicast > MVR > Show Statistics pages to display MVR protocol-related statistics for the specified interface.

CLI REFERENCES

- "show mvr statistics" on page 1494

PARAMETERS

These parameters are displayed:

- **Domain ID** – An independent multicast domain. (Range: 1-5)
- **VLAN** – VLAN identifier. (Range: 1-4094)
- **Port** – Port identifier. (Range: 1-28)
- **Trunk** – Trunk identifier. (Range: 1-8)

Query Statistics

- **Querier IP Address** – The IP address of the querier on this interface.
- **Querier Expire Time** – The time after which this querier is assumed to have expired.
- **General Query Received** – The number of general queries received on this interface.
- **General Query Sent** – The number of general queries sent from this interface.
- **Specific Query Received** – The number of specific queries received on this interface.
- **Specific Query Sent** – The number of specific queries sent from this interface.
- **Number of Reports Sent** – The number of reports sent from this interface.
- **Number of Leaves Sent** – The number of leaves sent from this interface.

VLAN, Port, and Trunk Statistics

Input Statistics

- **Report** – The number of IGMP membership reports received on this interface.
- **Leave** – The number of leave messages received on this interface.
- **G Query** – The number of general query messages received on this interface.

- **G(-S)-S Query** – The number of group specific or group-and-source specific query messages received on this interface.
- **Drop** – The number of times a report, leave or query was dropped. Packets may be dropped due to invalid format, rate limiting, packet content not allowed, or MVR group report received.
- **Join Success** – The number of times a multicast group was successfully joined.
- **Group** – The number of MVR groups active on this interface.

Output Statistics

- **Report** – The number of IGMP membership reports sent from this interface.
- **Leave** – The number of leave messages sent from this interface.
- **G Query** – The number of general query messages sent from this interface.
- **G(-S)-S Query** – The number of group specific or group-and-source specific query messages sent from this interface.

WEB INTERFACE

To display statistics for MVR query-related messages:

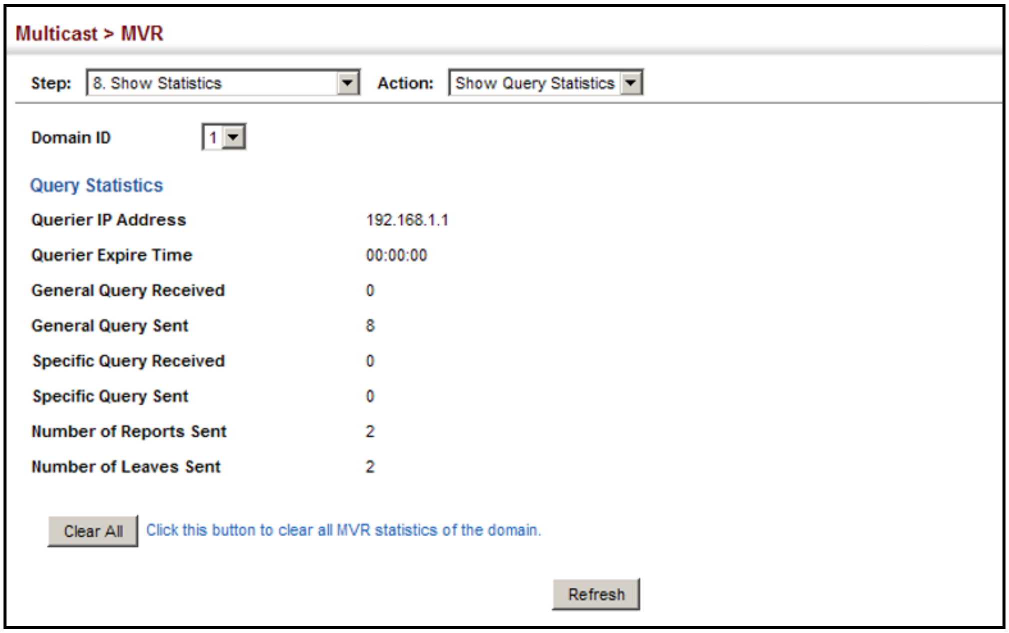
1. Click Multicast, MVR.

2. Select Show Statistics from the Step list.

3. Select Show Query Statistics from the Action list.

4. Select an MVR domain.

Figure 386: Displaying MVR Statistics – Query



Multicast > MVR

Step: 8. Show Statistics Action: Show Query Statistics

Domain ID 1

Query Statistics

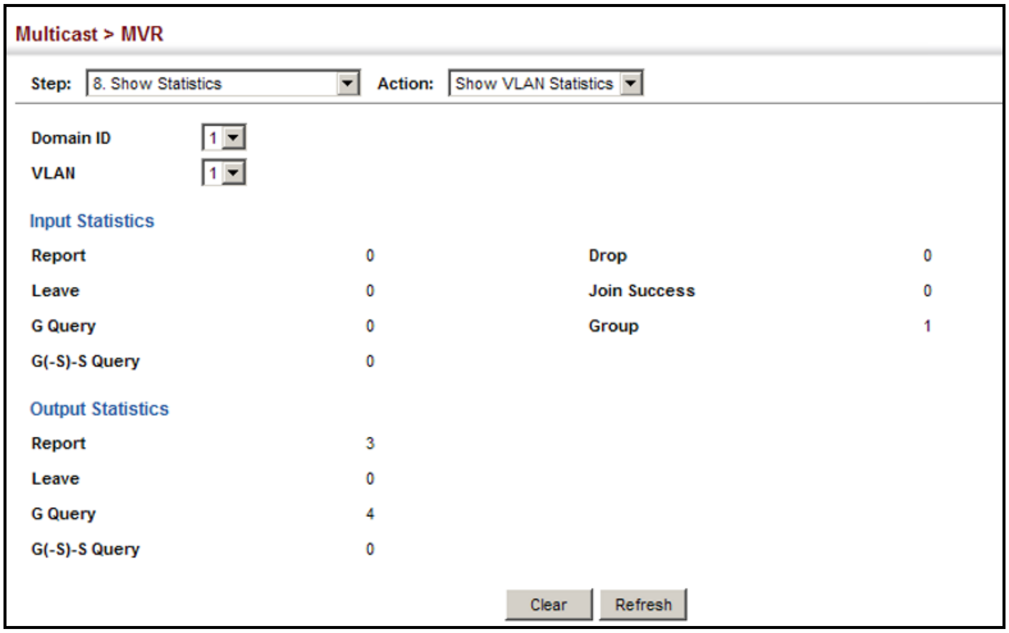
Querier IP Address	192.168.1.1
Querier Expire Time	00:00:00
General Query Received	0
General Query Sent	8
Specific Query Received	0
Specific Query Sent	0
Number of Reports Sent	2
Number of Leaves Sent	2

Click this button to clear all MVR statistics of the domain.

To display MVR protocol-related statistics for a VLAN:

1. Click Multicast, MVR.
2. Select Show Statistics from the Step list.
3. Select Show VLAN Statistics from the Action list.
4. Select an MVR domain.
5. Select a VLAN.

Figure 387: Displaying MVR Statistics – VLAN



Multicast > MVR

Step: 8. Show Statistics Action: Show VLAN Statistics

Domain ID 1

VLAN 1

Input Statistics

Report	0	Drop	0
Leave	0	Join Success	0
G Query	0	Group	1
G(-S)-S Query	0		

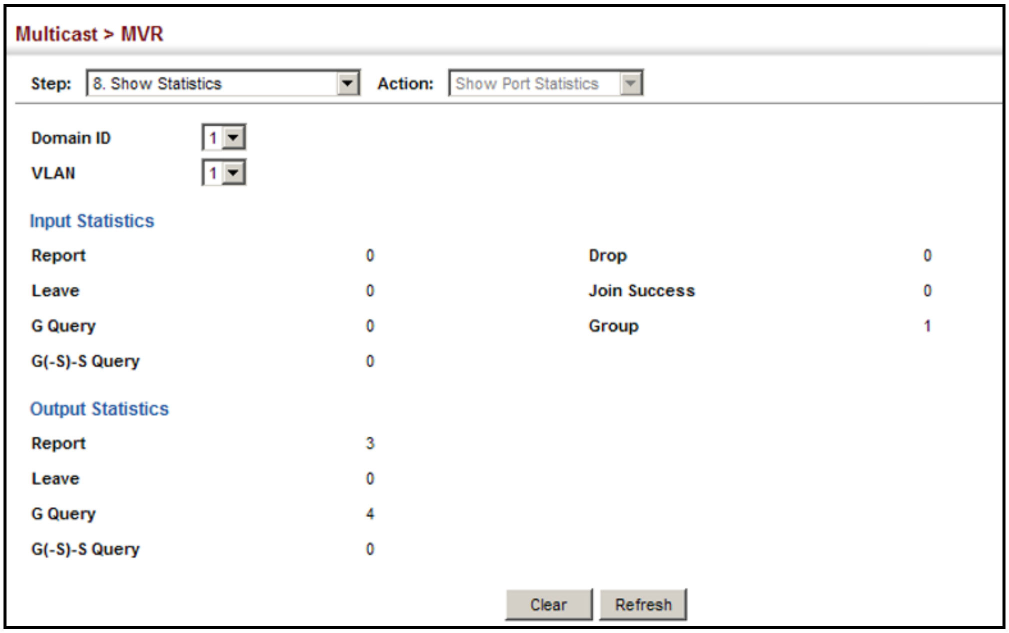
Output Statistics

Report	3
Leave	0
G Query	4
G(-S)-S Query	0

To display MVR protocol-related statistics for a port:

1. Click Multicast, MVR.
2. Select Show Statistics from the Step list.
3. Select Show Port Statistics from the Action list.
4. Select an MVR domain.
5. Select a Port.

Figure 388: Displaying MVR Statistics – Port



Multicast > MVR

Step: 8. Show Statistics   Action: Show Port Statistics

Domain ID: 1
VLAN: 1

Input Statistics

Report	0	Drop	0
Leave	0	Join Success	0
G Query	0	Group	1
G(-S)-S Query	0		

Output Statistics

Report	3
Leave	0
G Query	4
G(-S)-S Query	0

MULTICAST VLAN REGISTRATION FOR IPV6

MVR6 functions in a manner similar to that described for MRV (see "Multicast VLAN Registration for IPv4" on page 657).

COMMAND USAGE

- General Configuration Guidelines for MVR6:

  1. Enable MVR6 for a domain on the switch, and select the MVR VLAN (see "Configuring MVR6 Domain Settings" on page 677).
  2. Create an MVR6 profile by specifying the multicast groups that will stream traffic to attached hosts, and assign the profile to an MVR6 domain (see "Configuring MVR6 Group Address Profiles" on page 678).
  3. Set the interfaces that will join the MVR as source ports or receiver ports (see "Configuring MVR6 Interface Status" on page 681).

4. For multicast streams that will run for a long term and be associated with a stable set of hosts, you can statically bind the multicast group to the participating interfaces (see "Assigning Static MVR6 Multicast Groups to Interfaces" on page 684).

CONFIGURING MVR6 GLOBAL SETTINGS

Use the Multicast > MVR6 (Configure Global) page to configure proxy switching and the robustness variable.

CLI REFERENCES

- "MVR for IPv6" on page 1496

PARAMETERS

These parameters are displayed:

- **Proxy Switching** – Configures MVR proxy switching, where the source port acts as a host, and the receiver port acts as an MVR router with querier service enabled. (Default: Enabled)
  - When MVR proxy-switching is enabled, an MVR source port serves as the upstream or host interface, and the MVR receiver port serves as the querier. The source port performs only the host portion of MVR by sending summarized membership reports, and automatically disables MVR router functions.
  - Receiver ports are known as downstream or router interfaces. These interfaces perform the standard MVR router functions by maintaining a database of all MVR subscriptions on the downstream interface. Receiver ports must therefore be configured on all downstream interfaces which require MVR proxy service.
  - When the source port receives report and leave messages, it only forwards them to other source ports.
  - When receiver ports receive any query messages, they are dropped.
  - When changes occurring in the downstream MVR groups are learned by the receiver ports through report and leave messages, an MVR state change report is created and sent to the upstream source port, which in turn forwards this information upstream.
  - When MVR proxy switching is disabled:
    - Any membership reports received from receiver/source ports are forwarded to all source ports.
    - When a source port receives a query message, it will be forwarded to all downstream receiver ports.
    - When a receiver port receives a query message, it will be dropped.
- **Robustness Value** – Configures the expected packet loss, and thereby the number of times to generate report and group-specific queries. (Range: 1-10; Default: 1)
  - This parameter is used to set the number of times report messages are sent upstream when changes are learned about downstream

  groups, and the number of times group-specific queries are sent to downstream receiver ports.

  - This parameter only takes effect when MVR6 proxy switching is enabled.

- **Proxy Query Interval** – Configures the interval at which the receiver port sends out general queries. (Range: 2-31744 seconds; Default: 125 seconds)

  - This parameter sets the general query interval at which active receiver ports send out general queries.

  - This interval is only effective when proxy switching is enabled.

- **Source Port Mode** – Configures the switch to forward any multicast streams within the parameters set by a profile, or to only forward multicast streams which the source port has dynamically joined.

  - **Always Forward** – By default, the switch forwards any multicast streams within the address range set by a profile, and bound to a domain. The multicast streams are sent to all source ports on the switch and to all receiver ports that have elected to receive data on that multicast address.

  - **Dynamic** – When dynamic mode is enabled, the switch only forwards multicast streams which the source port has dynamically joined. In other words, both the receiver port and source port must subscribe to a multicast group before a multicast stream is forwarded to any attached client. Note that the requested streams are still restricted to the address range which has been specified in a profile and bound to a domain.

WEB INTERFACE

To configure global settings for MVR6:

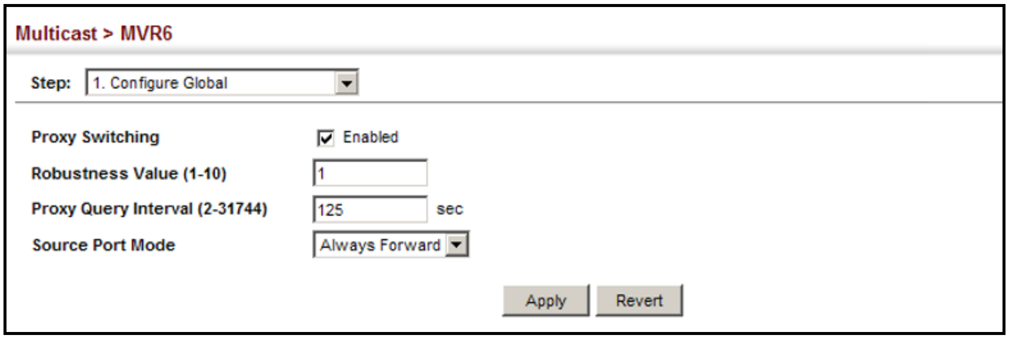
1. Click Multicast, MVR6.

2. Select Configure Global from the Step list.

3. Set the status for MVR6 proxy switching, the robustness value used for report and query messages, the proxy query interval, and source port mode.

4. Click Apply.

Figure 389: Configuring Global Settings for MVR6



Multicast > MVR6

Step: 1. Configure Global

Proxy Switching ☑ Enabled

Robustness Value (1-10) 1

Proxy Query Interval (2-31744) 125 sec

Source Port Mode Always Forward

CONFIGURING MVR6 DOMAIN SETTINGS

Use the Multicast > MVR6 (Configure Domain) page to enable MVR6 globally on the switch, and select the VLAN that will serve as the sole channel for common multicast streams supported by the service provider.

CLI REFERENCES

- "MVR for IPv6" on page 1496

PARAMETERS

These parameters are displayed:

- **Domain ID** – An independent multicast domain. (Range: 1-5)
- **MVR6 Status** – When MVR6 is enabled on the switch, any multicast data associated with an MVR6 group is sent from all designated source ports, to all receiver ports that have registered to receive data from that multicast group. (Default: Disabled)
- **MVR6 VLAN** – Identifier of the VLAN that serves as the channel for streaming multicast services using MVR6. MVR6 source ports should be configured as members of the MVR6 VLAN (see "Adding Static Members to VLANs" on page 231), but MVR6 receiver ports should not be manually configured as members of this VLAN. (Default: 1)
- **MVR6 Running Status** – Indicates whether or not all necessary conditions in the MVR6 environment are satisfied. Running status is Active as long as MVR6 is enabled, the specified MVR6 VLAN exists, and a source port with a valid link has been configured (see "Configuring MVR6 Interface Status" on page 681).
- **MVR6 Current Learned Groups** – The number of MVR6 groups currently assigned to this domain.
- **Forwarding Priority** – The CoS priority assigned to all multicast traffic forwarded into this domain. (Range: 0-7, where 7 is the highest priority)

  This parameter can be used to set a high priority for low-latency multicast traffic such as a video-conference, or to set a low priority for normal multicast traffic not sensitive to latency.

- **Upstream Source IPv6** – The source IPv6 address assigned to all MVR6 control packets sent upstream on the specified domain. This parameter must be a full IPv6 address including the network prefix and host address bits. By default, all MVR6 reports sent upstream use a null source IP address.

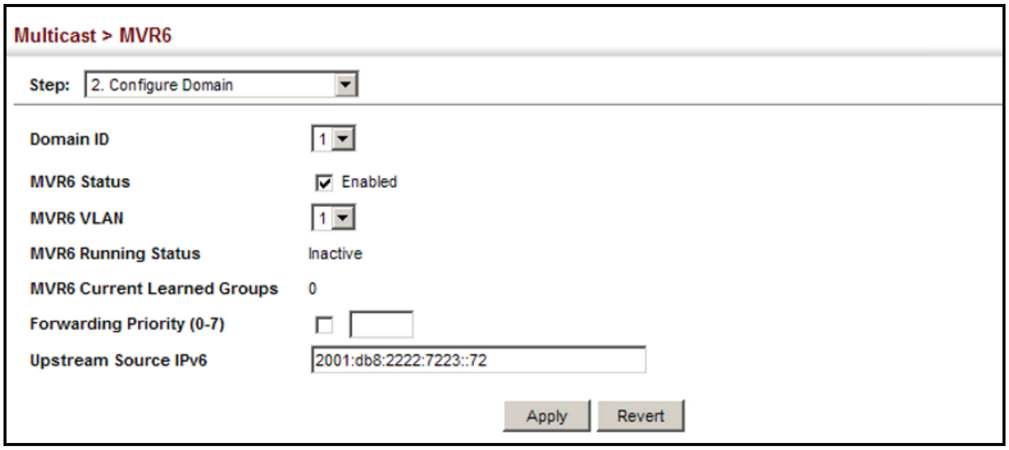
  All IPv6 addresses must be according to RFC 2373 “IPv6 Addressing Architecture,” using 8 colon-separated 16-bit hexadecimal values. One double colon may be used in the address to indicate the appropriate number of zeros required to fill the undefined fields. (Note that the IP address ff02::X is reserved.)

WEB INTERFACE

To configure settings for an MVR6 domain:

1. Click Multicast, MVR6.
2. Select Configure Domain from the Step list.
3. Select a domain from the scroll-down list.
4. Enable MVR6 for the selected domain, select the MVR6 VLAN, set the forwarding priority to be assigned to all ingress multicast traffic, and set the source IP address for all control packets sent upstream as required.
5. Click Apply.

Figure 390: Configuring Domain Settings for MVR6



Multicast > MVR6

Step: 2. Configure Domain

Domain ID	1
MVR6 Status	☑ Enabled
MVR6 VLAN	1
MVR6 Running Status	Inactive
MVR6 Current Learned Groups	0
Forwarding Priority (0-7)	☐
Upstream Source IPv6	2001:db8:2222:7223::72

CONFIGURING MVR6 GROUP ADDRESS PROFILES

Use the Multicast > MVR6 (Configure Profile and Associate Profile) pages to assign the multicast group address for required services to one or more MVR6 domains.

CLI REFERENCES

- "MVR for IPv6" on page 1496

COMMAND USAGE

- Use the Configure Profile page to statically configure all multicast group addresses that will join the MVR6 VLAN. Any multicast data associated with an MVR6 group is sent from all source ports to all receiver ports that have registered to receive data from that multicast group.

- MLD snooping and MVR6 share a maximum number of 1024 groups. Any multicast streams received in excess of this limitation will be flooded to all ports in the associated domain.

- All IPv6 addresses must be according to RFC 2373 “IPv6 Addressing Architecture,” using 8 colon-separated 16-bit hexadecimal values. One double colon may be used in the address to indicate the appropriate number of zeros required to fill the undefined fields. (Note that the IP address ff02::X is reserved.)

- The MVR6 group address range assigned to a profile cannot overlap with the group address range of any other profile.

- MRV6 domains can be associated with more than one MVR6 profile. But since MVR6 domains cannot share the group range, an MRV6 profile can only be associated with one MVR6 domain.

PARAMETERS

These parameters are displayed:

Configure Profile

- **Profile Name** – The name of a profile containing one or more MVR6 group addresses. (Range: 1-21 characters)

- **Start IPv6 Address** – Starting IP address for an MVR6 multicast group. This parameter must be a full IPv6 address including the network prefix and host address bits.

- **End IPv6 Address** – Ending IP address for an MVR6 multicast group. This parameter must be a full IPv6 address including the network prefix and host address bits.

Associate Profile

- **Domain ID** – An independent multicast domain. (Range: 1-5)

- **Profile Name** – The name of a profile to be assigned to this domain. (Range: 1-20 characters)

WEB INTERFACE

To configure an MVR6 group address profile:

1. Click Multicast, MVR6.

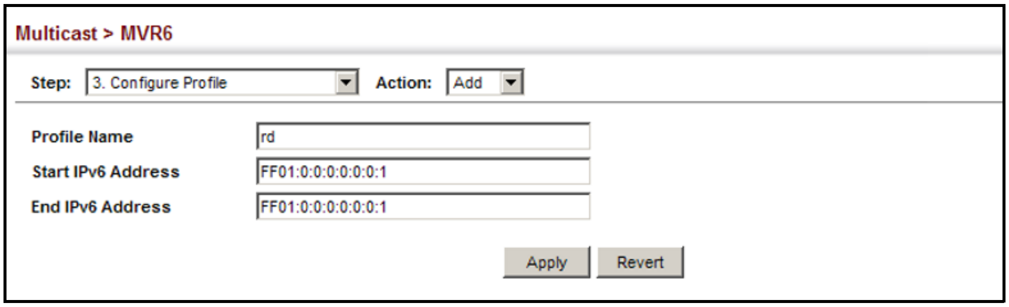
2. Select Configure Profile from the Step list.

3. Select Add from the Action list.

4. Enter the name of a group profile to be assigned to one or more domains, and specify a multicast group that will stream traffic to participating hosts.

5. Click Apply.

Figure 391: Configuring an MVR6 Group Address Profile



Multicast > MVR6

Step: 3. Configure Profile
Action: Add

Profile Name: rd
Start IPv6 Address: FF01:0:0:0:0:0:0:1
End IPv6 Address: FF01:0:0:0:0:0:0:1

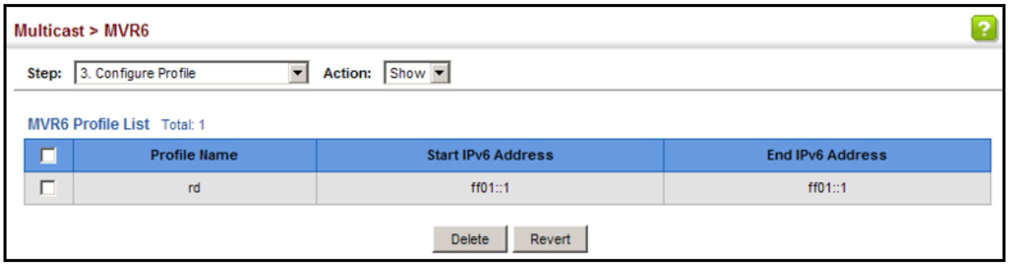
To show the configured MVR6 group address profiles:

1. Click Multicast, MVR6.

2. Select Configure Profile from the Step list.

3. Select Show from the Action list.

Figure 392: Displaying MVR6 Group Address Profiles



Multicast > MVR6

Step: 3. Configure Profile
Action: Show

MVR6 Profile List Total: 1

□	Profile Name	Start IPv6 Address	End IPv6 Address
□	rd	ff01::1	ff01::1

To assign an MVR6 group address profile to a domain:

1. Click Multicast, MVR6.

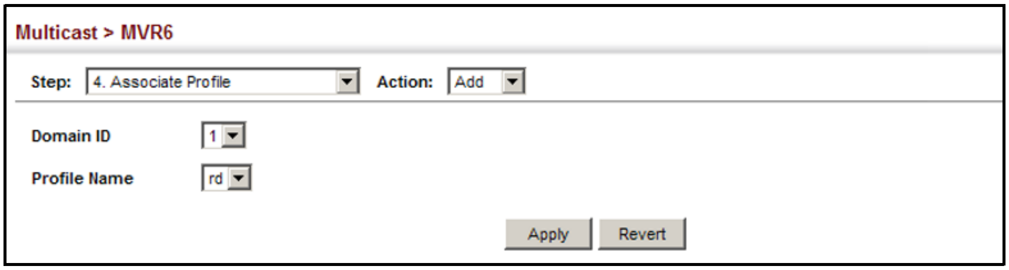
2. Select Associate Profile from the Step list.

3. Select Add from the Action list.

4. Select a domain from the scroll-down list, and enter the name of a group profile.

5. Click Apply.

Figure 393: Assigning an MVR6 Group Address Profile to a Domain


Multicast > MVR6

Step: 4. Associate Profile Action: Add

Domain ID: 1

Profile Name: rd

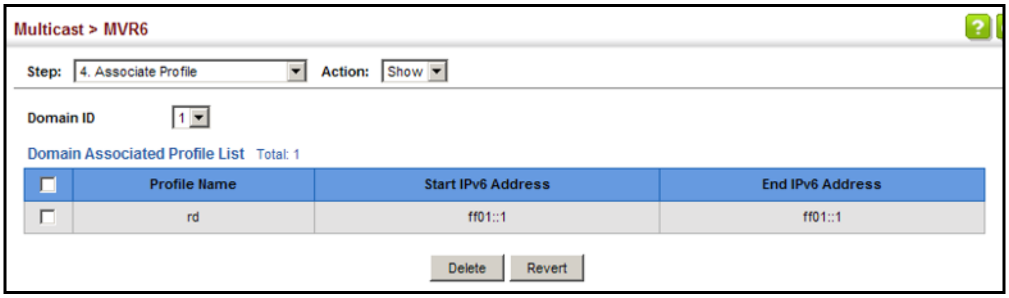
To show the MVR6 group address profiles assigned to a domain:

1. Click Multicast, MVR6.

2. Select Associate Profile from the Step list.

3. Select Show from the Action list.

Figure 394: Showing MVR6 Group Address Profiles Assigned to a Domain


Multicast > MVR6

Step: 4. Associate Profile Action: Show

Domain ID: 1

Domain Associated Profile List Total: 1

□	Profile Name	Start IPv6 Address	End IPv6 Address
□	rd	ff01::1	ff01::1

CONFIGURING MVR6 INTERFACE STATUS

Use the Multicast > MVR6 (Configure Interface) page to configure each interface that participates in the MVR6 protocol as a source port or receiver port. If you are sure that only one subscriber attached to an interface is receiving multicast services, you can enable the immediate leave function.

CLI REFERENCES

- "MVR for IPv6" on page 1496

COMMAND USAGE

- A port configured as an MVR6 receiver or source port can join or leave multicast groups configured under MVR6. A port which is not configured as an MVR receiver or source port can use MLD snooping to join or leave multicast groups using the standard rules for multicast filtering (see "MLD Snooping Commands" on page 1469).

- Receiver ports can belong to different VLANs, but should not be configured as a member of the MVR6 VLAN. MVR6 allows a receiver port to dynamically join or leave multicast groups within an MVR6 VLAN. Multicast groups can also be statically assigned to a receiver port (see "Assigning Static MVR Multicast Groups to Interfaces" on page 667).

Receiver ports should not be statically configured as a member of the MVR6 VLAN. If so configured, its MVR6 status will be inactive. Also, note that VLAN membership for MVR6 receiver ports cannot be set to access mode (see"Adding Static Members to VLANs" on page 231).

- One or more interfaces may be configured as MVR6 source ports. A source port is able to both receive and send data for configured MVR6 groups or for groups which have been statically assigned (see "Assigning Static MVR Multicast Groups to Interfaces" on page 667).

  All source ports must belong to the MVR6 VLAN.

  Subscribers should not be directly connected to source ports.

- Immediate leave applies only to receiver ports. When enabled, the receiver port is immediately removed from the multicast group identified in the leave message. When immediate leave is disabled, the switch follows the standard rules by sending a group-specific query to the receiver port and waiting for a response to determine if there are any remaining subscribers for that multicast group before removing the port from the group list.
  - Using immediate leave can speed up leave latency, but should only be enabled on a port attached to one multicast subscriber to avoid disrupting services to other group members attached to the same interface.
  - Immediate leave does not apply to multicast groups which have been statically assigned to a port.

PARAMETERS

These parameters are displayed:

- **Domain ID** – An independent multicast domain. (Range: 1-5)
- **Port/Trunk** – Interface identifier.
- **Type** – The following interface types are supported:
  - **Non-MVR6** – An interface that does not participate in the MVR6 VLAN. (This is the default type.)
  - **Source** – An uplink port that can send and receive multicast data for the groups assigned to the MVR6 VLAN. Note that the source port must be manually configured as a member of the MVR6 VLAN (see "Adding Static Members to VLANs" on page 231).
  - **Receiver** – A subscriber port that can receive multicast data sent through the MVR6 VLAN. Also, note that VLAN membership for MVR receiver ports cannot be set to access mode (see "Adding Static Members to VLANs" on page 231).
- **Forwarding Status** – Shows if multicast traffic is being forwarded or blocked.

- **MVR6 Status** – Shows the MVR6 status. MVR6 status for source ports is "Active" if MVR6 is globally enabled on the switch. MVR6 status for receiver ports is "Active" only if there are subscribers receiving multicast traffic from one of the MVR6 groups, or a multicast group has been statically assigned to an interface.

- **Immediate Leave** – Configures the switch to immediately remove an interface from a multicast stream as soon as it receives a leave message for that group. (This option only applies to an interface configured as an MVR6 receiver.)

WEB INTERFACE

To configure interface settings for MVR6:

1. Click Multicast, MVR6.

2. Select Configure Interface from the Step list.

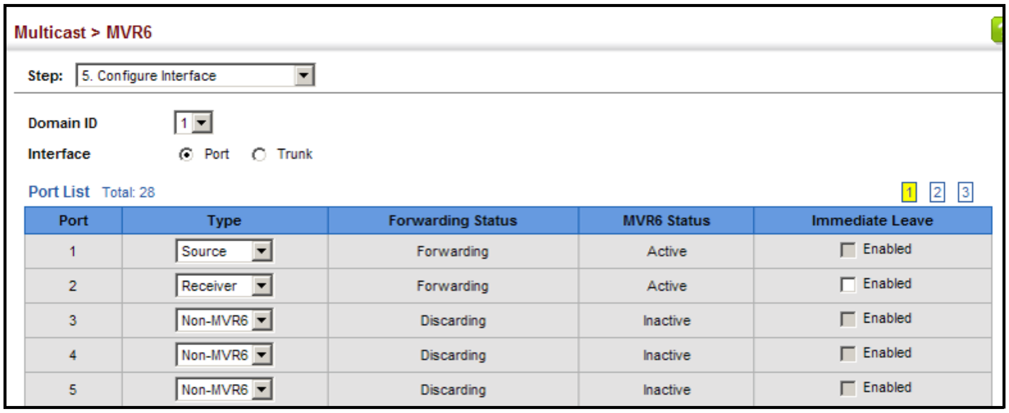
3. Select an MVR6 domain.

4. Click Port or Trunk.

5. Set each port that will participate in the MVR6 protocol as a source port or receiver port, and optionally enable Immediate Leave on any receiver port to which only one subscriber is attached.

6. Click Apply.

Figure 395: Configuring Interface Settings for MVR6



Multicast > MVR6

Step: 5. Configure Interface

Domain ID 1

Interface ● Port ○ Trunk

Port List Total: 28

Port	Type	Forwarding Status	MVR6 Status	Immediate Leave
1	Source	Forwarding	Active	□ Enabled
2	Receiver	Forwarding	Active	□ Enabled
3	Non-MVR6	Discarding	Inactive	□ Enabled
4	Non-MVR6	Discarding	Inactive	□ Enabled
5	Non-MVR6	Discarding	Inactive	□ Enabled

ASSIGNING STATIC MVR6 MULTICAST GROUPS TO INTERFACES

Use the Multicast > MVR6 (Configure Static Group Member) page to statically bind multicast groups to a port which will receive long-term multicast streams associated with a stable set of hosts.

CLI REFERENCES

- "mvr6 vlan group" on page 1505

COMMAND USAGE

- Multicast groups can be statically assigned to a receiver port using this configuration page.
- All IPv6 addresses must be according to RFC 2373 “IPv6 Addressing Architecture,” using 8 colon-separated 16-bit hexadecimal values. One double colon may be used in the address to indicate the appropriate number of zeros required to fill the undefined fields. (Note that the IP address ff02::X is reserved.)
- The MVR6 VLAN cannot be specified as the receiver VLAN for static bindings.

PARAMETERS

These parameters are displayed:

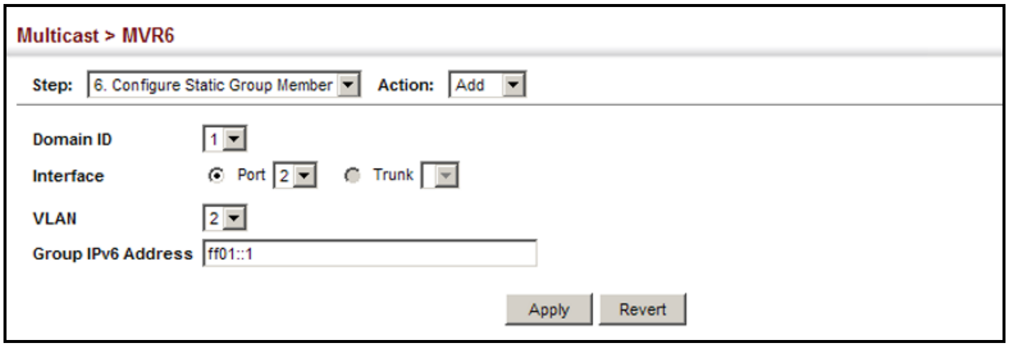
- **Domain ID** – An independent multicast domain. (Range: 1-5)
- **Interface** – Port or trunk identifier.
- **VLAN** – VLAN identifier. (Range: 1-4094)
- **Group IPv6 Address** – Defines a multicast service sent to the selected port. Multicast groups must be assigned from the MVR6 group range configured on the Configure General page.

WEB INTERFACE

To assign a static MVR6 group to an interface:

1. Click Multicast, MVR6.
2. Select Configure Static Group Member from the Step list.
3. Select Add from the Action list.
4. Select an MVR6 domain.
5. Select a VLAN and interface to receive the multicast stream, and then enter the multicast group address.
6. Click Apply.

Figure 396: Assigning Static MVR6 Groups to a Port



Multicast > MVR6

Step: 6. Configure Static Group Member Action: Add

Domain ID: 1

Interface: ● Port 2 ○ Trunk

VLAN: 2

Group IPv6 Address: ff01::1

To show the static MVR6 groups assigned to an interface:

1. Click Multicast, MVR6.

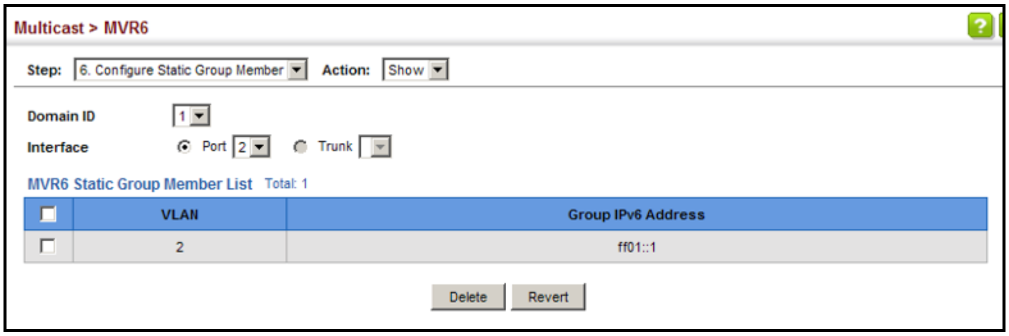
2. Select Configure Static Group Member from the Step list.

3. Select Show from the Action list.

4. Select an MVR6 domain.

5. Select the port or trunk for which to display this information.

Figure 397: Showing the Static MVR6 Groups Assigned to a Port



Multicast > MVR6

Step: 6. Configure Static Group Member Action: Show

Domain ID: 1

Interface: ● Port 2 ○ Trunk

MVR6 Static Group Member List Total: 1

□	VLAN	Group IPv6 Address
□	2	ff01::1

DISPLAYING MVR6 RECEIVER GROUPS

Use the Multicast > MVR6 (Show Member) page to show the multicast groups either statically or dynamically assigned to the MVR6 receiver groups on each interface.

CLI REFERENCES

- "show mvr6 members" on page 1510

PARAMETERS

These parameters are displayed:

- **Domain ID** – An independent multicast domain. (Range: 1-5)

- **Group IPv6 Address** – Multicast groups assigned to the MVR6 VLAN.

- **VLAN** – The VLAN through which the service is received. Note that this may be different from the MVR6 VLAN if the group address has been statically assigned.

- **Port** – Indicates the source address of the multicast service, or displays an asterisk if the group address has been statically assigned (these entries are marked as “Source”). Also shows the interfaces with subscribers for multicast services provided through the MVR6 VLAN (these entries are marked as “Receiver”).

- **Up Time** – Time this service has been forwarded to attached clients.

- **Expire** – Time before this entry expires if no membership report is received from currently active or new clients.

- **Count** – The number of multicast services currently being forwarded from the MVR6 VLAN.

WEB INTERFACE

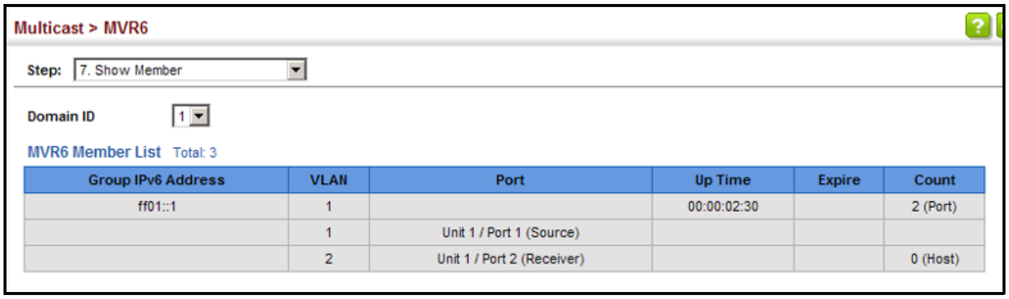
To display the interfaces assigned to the MVR6 receiver groups:

1. Click Multicast, MVR6.

2. Select Show Member from the Step list.

3. Select an MVR6 domain.

Figure 398: Displaying MVR6 Receiver Groups



Multicast > MVR6

Step: 7. Show Member

Domain ID 1

MVR6 Member List Total: 3

Group IPv6 Address	VLAN	Port	Up Time	Expire	Count
ff01::1	1		00:00:02:30		2 (Port)
	1	Unit 1 / Port 1 (Source)			
	2	Unit 1 / Port 2 (Receiver)			0 (Host)

DISPLAYING MVR6 STATISTICS

Use the Multicast > MVR6 > Show Statistics pages to display MVR6 protocol-related statistics for the specified interface.

CLI REFERENCES

- "show mvr6 statistics" on page 1511

PARAMETERS

These parameters are displayed:

- **Domain ID** – An independent multicast domain. (Range: 1-5)

- **VLAN** – VLAN identifier. (Range: 1-4094)

- **Port** – Port identifier. (Range: 1-28)

- **Trunk** – Trunk identifier. (Range: 1-8)

Query Statistics

- **Querier IPv6 Address** – The IP address of the querier on this interface.

- **Querier Expire Time** – The time after which this querier is assumed to have expired.

- **General Query Received** – The number of general queries received on this interface.

- **General Query Sent** – The number of general queries sent from this interface.

- **Specific Query Received** – The number of specific queries received on this interface.

- **Specific Query Sent** – The number of specific queries sent from this interface.

- **Number of Reports Sent** – The number of reports sent from this interface.

- **Number of Leaves Sent** – The number of leaves sent from this interface.

VLAN, Port, and Trunk Statistics

Input Statistics

- **Report** – The number of MLD membership reports received on this interface.

- **Leave** – The number of leave messages received on this interface.

- **G Query** – The number of general query messages received on this interface.

- **G(-S)-S Query** – The number of group specific or group-and-source specific query messages received on this interface.

- **Drop** – The number of times a report, leave or query was dropped. Packets may be dropped due to invalid format, rate limiting, packet content not allowed, or MVR6 group report received.

- **Join Success** – The number of times a multicast group was successfully joined.

- **Group** – The number of MVR6 groups active on this interface.

Output Statistics

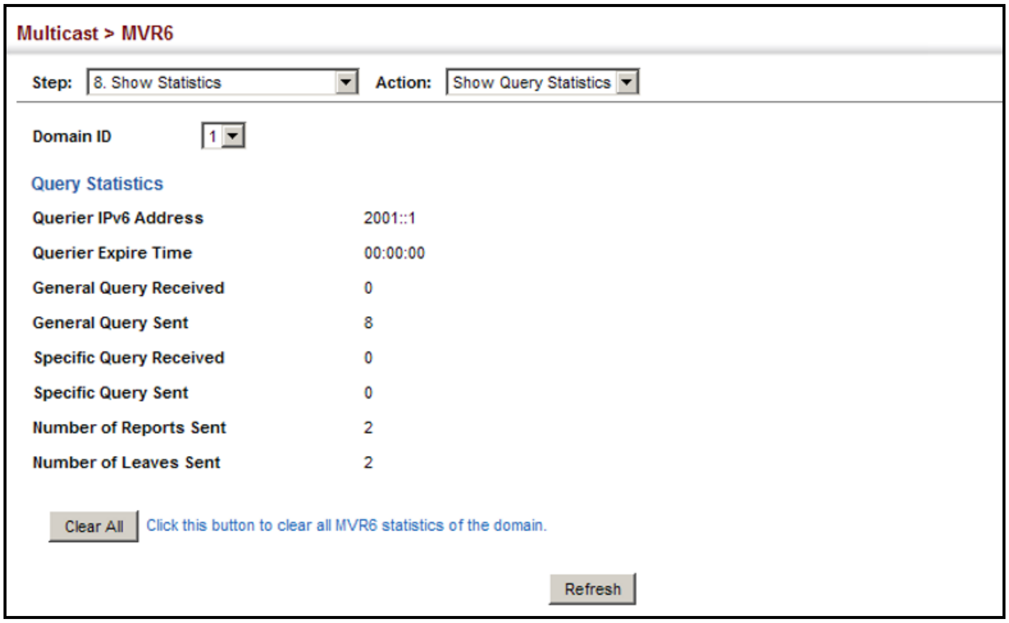
- **Report** – The number of MLD membership reports sent from this interface.
- **Leave** – The number of leave messages sent from this interface.
- **G Query** – The number of general query messages sent from this interface.
- **G(-S)-S Query** – The number of group specific or group-and-source specific query messages sent from this interface.

WEB INTERFACE

To display statistics for MVR6 query-related messages:

1. Click Multicast, MVR6.
2. Select Show Statistics from the Step list.
3. Select Show Query Statistics from the Action list.
4. Select an MVR6 domain.

Figure 399: Displaying MVR6 Statistics – Query



Multicast > MVR6

Step: 8. Show Statistics Action: Show Query Statistics

Domain ID: 1

Query Statistics

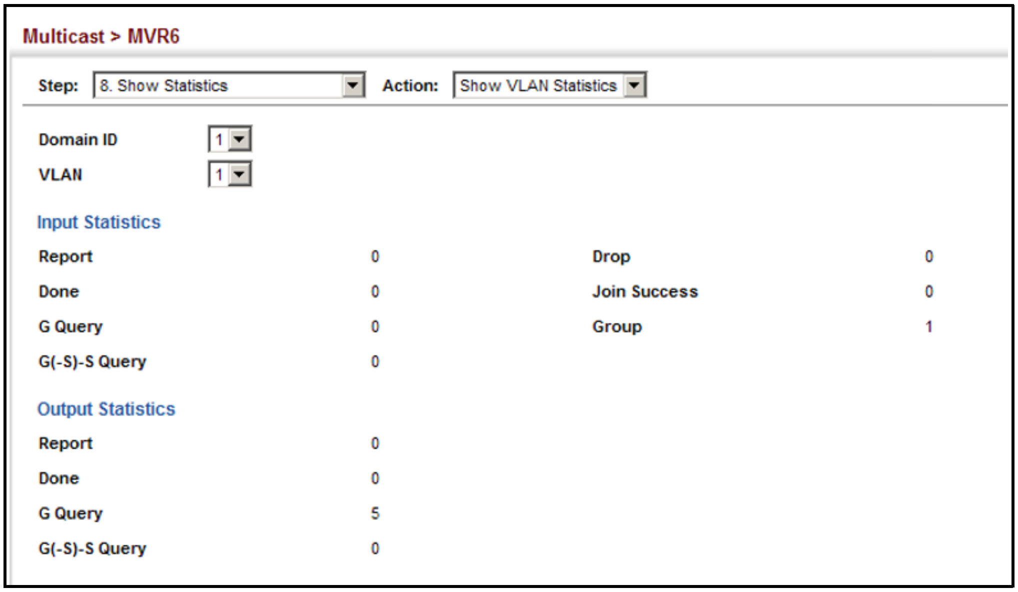
Querier IPv6 Address	2001::1
Querier Expire Time	00:00:00
General Query Received	0
General Query Sent	8
Specific Query Received	0
Specific Query Sent	0
Number of Reports Sent	2
Number of Leaves Sent	2

Click this button to clear all MVR6 statistics of the domain.

To display MVR6 protocol-related statistics for a VLAN:

1. Click Multicast, MVR6.
2. Select Show Statistics from the Step list.
3. Select Show VLAN Statistics from the Action list.
4. Select an MVR6 domain.
5. Select a VLAN.

Figure 400: Displaying MVR6 Statistics – VLAN



Multicast > MVR6

Step: 8. Show Statistics Action: Show VLAN Statistics

Domain ID: 1
VLAN: 1

Input Statistics

Report	0	Drop	0
Done	0	Join Success	0
G Query	0	Group	1
G(-S)-S Query	0		

Output Statistics

Report	0
Done	0
G Query	5
G(-S)-S Query	0

To display MVR6 protocol-related statistics for a port:

1. Click Multicast, MVR6.

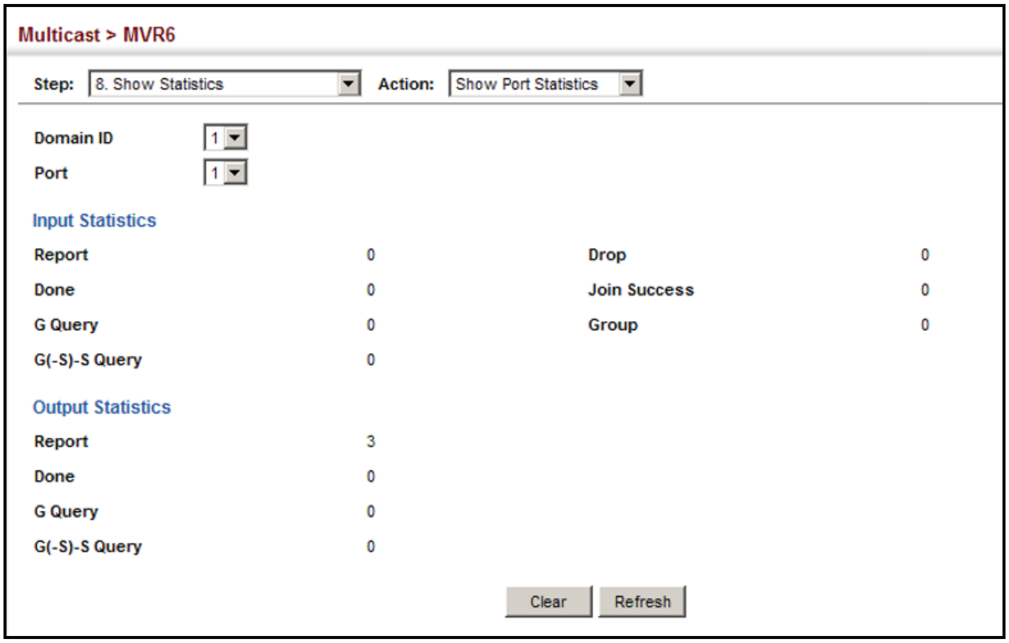
2. Select Show Statistics from the Step list.

3. Select Show Port Statistics from the Action list.

4. Select an MVR6 domain.

5. Select a Port.

Figure 401: Displaying MVR6 Statistics – Port



Multicast > MVR6

Step: 8. Show Statistics Action: Show Port Statistics

Domain ID 1
Port 1

Input Statistics

Report	0	Drop	0
Done	0	Join Success	0
G Query	0	Group	0
G(-S)-S Query	0		

Output Statistics

Report	3
Done	0
G Query	0
G(-S)-S Query	0

16 IP Configuration

This chapter describes how to configure an initial IP interface for management access to the switch over the network. This switch supports both IP Version 4 and Version 6, and can be managed simultaneously through either of these address types. You can manually configure a specific IPv4 or IPv6 address, or direct the switch to obtain an IPv4 address from a BOOTP or DHCP server. An IPv6 global unicast or link-local address can be manually configured, or a link-local address can be dynamically generated.

This chapter provides information on network functions including:

- IPv4 Configuration – Sets an IPv4 address for management access.
- IPv6 Configuration – Sets an IPv6 address for management access.

Setting the Switch's IP Address (IP Version 4)

This section describes how to configure an initial IPv4 interface for management access over the network, or for creating an interface to multiple subnets. This switch supports both IPv4 and IPv6, and can be managed through either of these address types. For information on configuring the switch with an IPv6 address, see "Setting the Switch's IP Address (IP Version 6)" on page 695.

Use the IP > General > Routing Interface (Add Address) page to configure an IPv4 address for the switch. An IPv4 address is obtained via DHCP by default for VLAN 1. To configure a static address, you need to change the switch's default settings to values that are compatible with your network. You may also need to a establish a default gateway between the switch and management stations that exist on another network segment (if no routing protocols are enabled).

You can direct the device to obtain an address from a BOOTP or DHCP server, or manually configure a static IP address. Valid IP addresses consist of four decimal numbers, 0 to 255, separated by periods. Anything other than this format will not be accepted.

CLI References

- "DHCP Client" on page 1625
- "Basic IPv4 Configuration" on page 1648

COMMAND USAGE

- This section describes how to configure a single local interface for initial access to the switch. To configure multiple IP interfaces, set up an IP interface for each VLAN.
- Once an IP address has been assigned to an interface, routing between different interfaces on the switch is enabled.
- To enable routing between interfaces defined on this switch and external network interfaces, you must configure static routes (page 753) or use dynamic routing; i.e., RIP, OSPFv2 or OSPFv3 (page 770, 788 or 1790 respectively).
- The precedence for configuring IP interfaces is the IP > General > Routing Interface (Add) menu, static routes (page 753), and then dynamic routing.

PARAMETERS

These parameters are displayed:

- **VLAN** – ID of the configured VLAN (1-4094). By default, all ports on the switch are members of VLAN 1. However, the management station can be attached to a port belonging to any VLAN, as long as that VLAN has been assigned an IP address.
- **IP Address Mode** – Specifies whether IP functionality is enabled via manual configuration (User Specified), Dynamic Host Configuration Protocol (DHCP), or Boot Protocol (BOOTP). If DHCP/BOOTP is enabled, IP will not function until a reply has been received from the server. Requests will be broadcast periodically by the switch for an IP address. DHCP/BOOTP responses can include the IP address, subnet mask, and default gateway. (Default: DHCP)
- **IP Address Type** – Specifies a primary or secondary IP address. An interface can have only one primary IP address, but can have many secondary IP addresses. In other words, secondary addresses need to be specified if more than one IP subnet can be accessed through this interface. For initial configuration, set this parameter to Primary. (Options: Primary, Secondary; Default: Primary)

  Note that a secondary address cannot be configured prior to setting the primary IP address, and the primary address cannot be removed if a secondary address is still present. Also, if any router or switch in a network segment uses a secondary address, all other routers/switches in that segment must also use a secondary address from the same network or subnet address space.
- **IP Address – IP Address** – IP Address of the VLAN. Valid IP addresses consist of four numbers, 0 to 255, separated by periods. (Default: None)

NOTE: You can manage the switch through any configured IP interface.

- **Subnet Mask** – This mask identifies the host address bits used for routing to specific subnets. (Default: None)

- **Restart DHCP** – Requests a new IP address from the DHCP server.

WEB INTERFACE

To set a static IPv4 address for the switch:

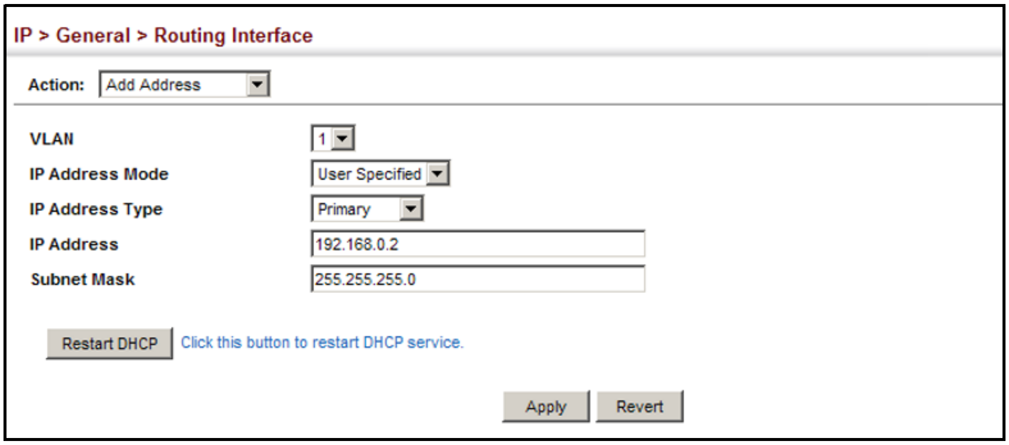
1. Click IP, General, Routing Interface.

2. Select Add Address from the Action list.

3. Select any configured VLAN, set IP Address Mode to "User Specified," set IP Address Type to "Primary" if no address has yet been configured for this interface, and then enter the IP address and subnet mask.

4. Click Apply.

Figure 402: Configuring a Static IPv4 Address



IP > General > Routing Interface

Action: Add Address

VLAN	1
IP Address Mode	User Specified
IP Address Type	Primary
IP Address	192.168.0.2
Subnet Mask	255.255.255.0

To obtain an dynamic IPv4 address through DHCP/BOOTP for the switch:

1. Click IP, General, Routing Interface.

2. Select Add Address from the Action list.

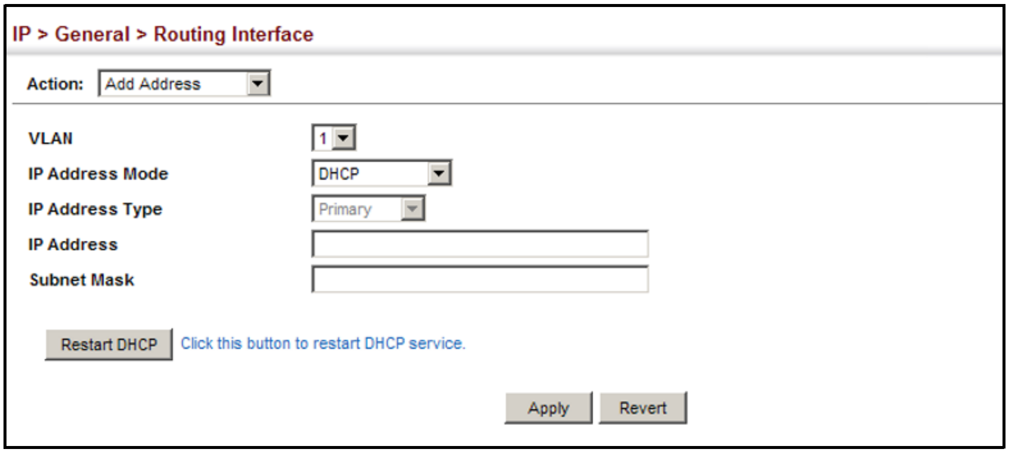
3. Select any configured VLAN, and set IP Address Mode to "BOOTP" or "DHCP."

4. Click Apply to save your changes.

5. Then click Restart DHCP to immediately request a new address.

IP will be enabled but will not function until a BOOTP or DHCP reply is received. Requests are broadcast every few minutes using exponential backoff until IP configuration information is obtained from a BOOTP or DHCP server.

Figure 403: Configuring a Dynamic IPv4 Address



IP > General > Routing Interface

Action: Add Address

VLAN: 1
IP Address Mode: DHCP
IP Address Type: Primary
IP Address:
Subnet Mask:

NOTE: The switch will also broadcast a request for IP configuration settings on each power reset.

NOTE: If you lose the management connection, make a console connection to the switch and enter "show ip interface" to determine the new switch address.

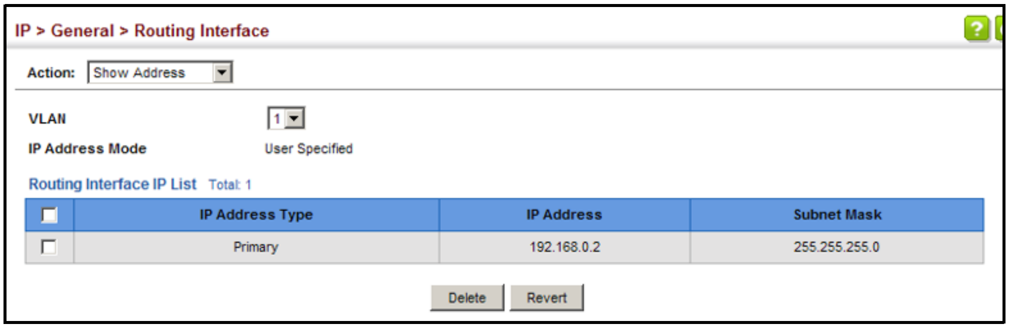
Renewing DCHP – DHCP may lease addresses to clients indefinitely or for a specific period of time. If the address expires or the switch is moved to another network segment, you will lose management access to the switch. In this case, you can reboot the switch or submit a client request to restart DHCP service via the CLI.

If the address assigned by DHCP is no longer functioning, you will not be able to renew the IP settings via the web interface. You can only restart DHCP service via the web interface if the current address is still available.

To show the IPv4 address configured for an interface:

1. Click IP, General, Routing Interface.
2. Select Show Address from the Action list.
3. Select an entry from the VLAN list.

Figure 404: Showing the IPv4 Address for an Interface



IP > General > Routing Interface

Action: Show Address

VLAN: 1

IP Address Mode: User Specified

Routing Interface IP List Total: 1

□	IP Address Type	IP Address	Subnet Mask
□	Primary	192.168.0.2	255.255.255.0

SETTING THE SWITCH'S IP ADDRESS (IP VERSION 6)

This section describes how to configure an initial IPv6 interface for management access over the network, or for creating an interface to multiple subnets. This switch supports both IPv4 and IPv6, and can be managed through either of these address types. For information on configuring the switch with an IPv4 address, see "Setting the Switch's IP Address (IP Version 4)" on page 691.

COMMAND USAGE

- IPv6 includes two distinct address types – link-local unicast and global unicast. A link-local address makes the switch accessible over IPv6 for all devices attached to the same local subnet. Management traffic using this kind of address cannot be passed by any router outside of the subnet. A link-local address is easy to set up, and may be useful for simple networks or basic troubleshooting tasks. However, to connect to a larger network with multiple segments, the switch must be configured with a global unicast address. A link-local address can be dynamically assigned (using the Configure Interface page) or manually configured (using the Add IPv6 Address page). A global unicast address can only be manually configured (using the Add IPv6 Address page).

- An IPv6 global unicast or link-local address can be manually configured (using the Add IPv6 Address page), or a link-local address can be dynamically generated (using the Configure Interface page).

CONFIGURING THE IPV6 DEFAULT GATEWAY

Use the IP > IPv6 Configuration (Configure Global) page to configure an IPv6 default gateway for the switch.

CLI REFERENCES

- "ipv6 default-gateway" on page 1664

PARAMETERS

These parameters are displayed:

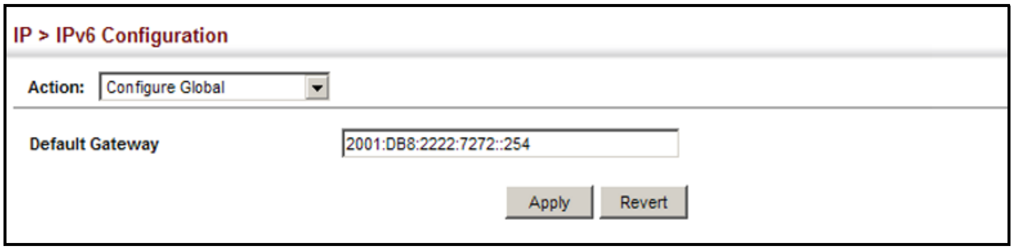
- **Default Gateway** – Sets the IPv6 address of the default next hop router to use when no routing information is known about an IPv6 address.
  - If no routing protocol is enabled or static route defined, you must define a gateway if the target device is located in a different subnet.
  - If a routing protocol is enabled (page 769), you can still define a static route (page 753) to ensure that traffic to the designated address or subnet passes through a preferred gateway.
  - An IPv6 default gateway can only be successfully set when a network interface that directly connects to the gateway has been configured on the switch.
  - An IPv6 address must be configured according to RFC 2373 "IPv6 Addressing Architecture," using 8 colon-separated 16-bit hexadecimal values. One double colon may be used in the address to indicate the appropriate number of zeros required to fill the undefined fields.

WEB INTERFACE

To configure an IPv6 default gateway for the switch:

1. Click IP, IPv6 Configuration.
2. Select Configure Global from the Action list.
3. Enter the IPv6 default gateway.
4. Click Apply.

Figure 405: Configuring the IPv6 Default Gateway



IP > IPv6 Configuration

Action: Configure Global

Default Gateway: 2001:DB8:2222:7272::254

CONFIGURING IPv6 INTERFACE SETTINGS

Use the IP > IPv6 Configuration (Configure Interface) page to configure general IPv6 settings for the selected VLAN, including explicit configuration of a link local interface address, the MTU size, and neighbor discovery protocol settings for duplicate address detection and the neighbor solicitation interval.

CLI REFERENCES

- "IPv6 Interface" on page 1663
- "DHCP Client" on page 1625

COMMAND USAGE

- The switch must be configured with a link-local address. The option to explicitly enable IPv6 creates a link-local address, but will not generate a global IPv6 address. The global unicast address must be manually configured (see "Configuring an IPv6 Address" on page 700).

- IPv6 Neighbor Discovery Protocol supersedes IPv4 Address Resolution Protocol in IPv6 networks. IPv6 nodes on the same network segment use Neighbor Discovery to discover each other's presence, to determine each other's link-layer addresses, to find routers and to maintain reachability information about the paths to active neighbors. The key parameters used to facilitate this process are the number of attempts made to verify whether or not a duplicate address exists on the same network segment, and the interval between neighbor solicitations used to verify reachability information.

PARAMETERS

These parameters are displayed:

VLAN Mode

- **VLAN** – ID of a configured VLAN which is to be used for management access, or as a standard interface for a subnet. By default, all ports on the switch are members of VLAN 1. However, the management station can be attached to a port belonging to any VLAN, as long as that VLAN has been assigned an IP address. (Range: 1-4094)

- **Enable IPv6 Explicitly** – Enables IPv6 on an interface and assigns it a link-local address. Note that when an explicit address is assigned to an interface, IPv6 is automatically enabled, and cannot be disabled until all assigned addresses have been removed. (Default: Disabled)

  Disabling this parameter does not disable IPv6 for an interface that has been explicitly configured with an IPv6 address.

- **MTU** – Sets the size of the maximum transmission unit (MTU) for IPv6 packets sent on an interface. (Range: 1280-65535 bytes;
  Default: 1500 bytes)

  - The maximum value set in this field cannot exceed the MTU of the physical interface, which is currently fixed at 1500 bytes.

  - If a non-default value is configured, an MTU option is included in the router advertisements sent from this device. This option is provided to ensure that all nodes on a link use the same MTU value in cases where the link MTU is not otherwise well known.

  - IPv6 routers do not fragment IPv6 packets forwarded from other routers. However, traffic originating from an end-station connected to an IPv6 router may be fragmented.
  - All devices on the same physical medium must use the same MTU in order to operate correctly.
  - IPv6 must be enabled on an interface before the MTU can be set. If an IPv6 address has not been assigned to the switch, "N/A" is displayed in the MTU field.

- **ND DAD Attempts** – The number of consecutive neighbor solicitation messages sent on an interface during duplicate address detection. (Range: 0-600, Default: 1)
  - Configuring a value of 0 disables duplicate address detection.
  - Duplicate address detection determines if a new unicast IPv6 address already exists on the network before it is assigned to an interface.
  - Duplicate address detection is stopped on any interface that has been suspended (see "Configuring VLAN Groups" on page 228). While an interface is suspended, all unicast IPv6 addresses assigned to that interface are placed in a "pending" state. Duplicate address detection is automatically restarted when the interface is administratively re-activated.
  - An interface that is re-activated restarts duplicate address detection for all unicast IPv6 addresses on the interface. While duplicate address detection is performed on the interface's link-local address, the other IPv6 addresses remain in a "tentative" state. If no duplicate link-local address is found, duplicate address detection is started for the remaining IPv6 addresses.
  - If a duplicate address is detected, it is set to "duplicate" state, and a warning message is sent to the console. If a duplicate link-local address is detected, IPv6 processes are disabled on the interface. If a duplicate global unicast address is detected, it is not used. All configuration commands associated with a duplicate address remain configured while the address is in "duplicate" state.
  - If the link-local address for an interface is changed, duplicate address detection is performed on the new link-local address, but not for any of the IPv6 global unicast addresses already associated with the interface.

- **ND NS Interval** – The interval between transmitting IPv6 neighbor solicitation messages on an interface. (Range: 1000-3600000 milliseconds;

  Default: 1000 milliseconds is used for neighbor discovery operations,
  0 milliseconds is advertised in router advertisements.

  This attribute specifies the interval between transmitting neighbor solicitation messages when resolving an address, or when probing the reachability of a neighbor. Therefore, avoid using very short intervals for normal IPv6 operations.

When a non-default value is configured, the specified interval is used both for router advertisements and by the router itself.

- **ND Reachable-Time** – The amount of time that a remote IPv6 node is considered reachable after some reachability confirmation event has occurred. (Range: 0-3600000 milliseconds)

  Default: 30000 milliseconds is used for neighbor discovery operations,
  0 milliseconds is advertised in router advertisements.

  - The time limit configured by this parameter allows the router to detect unavailable neighbors.
  - This time limit is included in all router advertisements sent out through an interface, ensuring that nodes on the same link use the same time value.
  - Setting the time limit to 0 means that the configured time is unspecified by this router.

RA Mode

- **Interface** – Shows port or trunk configuration page.

- **RA Guard** – Blocks incoming Router Advertisement and Router Redirect packets. (Default: Disabled)

  IPv6 Router Advertisements (RA) convey information that enables nodes to auto-configure on the network. This information may include the default router address taken from the observed source address of the RA message, as well as on-link prefix information. However, note that unintended misconfigurations, or possibly malicious attacks on the network, may lead to bogus RAs being sent, which in turn can cause operational problems for hosts on the network.

  RA Guard can be used to block RAs and Router Redirect (RR) messages on the specified interface. Determine which interfaces are connected to known routers, and enable RA Guard on all other untrusted interfaces.

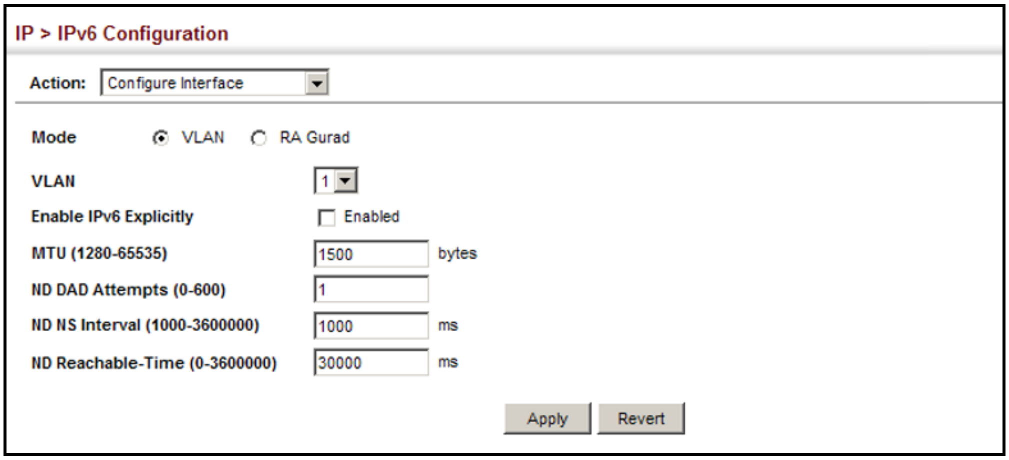
WEB INTERFACE

To configure general IPv6 settings for the switch:

1. Click IP, IPv6 Configuration.
2. Select Configure Interface from the Action list.
3. Select VLAN mode.
4. Specify the VLAN to configure.
5. Specify the VLAN to configure, enable IPv6 Explicitly to automatically configure a link-local address and enable IPv6 on the selected interface. (To manually configure the link-local address, use the Add IPv6 Address page.) Set the MTU size, the maximum number of duplicate address detection messages, the neighbor solicitation message interval, and the amount of time that a remote IPv6 node is considered reachable.

6. Click Apply.

Figure 406: Configuring General Settings for an IPv6 Interface



IP > IPv6 Configuration

Action: Configure Interface

Mode ● VLAN ○ RA Gurad

VLAN 1

Enable IPv6 Explicitly □ Enabled

MTU (1280-65535) 1500 bytes

ND DAD Attempts (0-600) 1

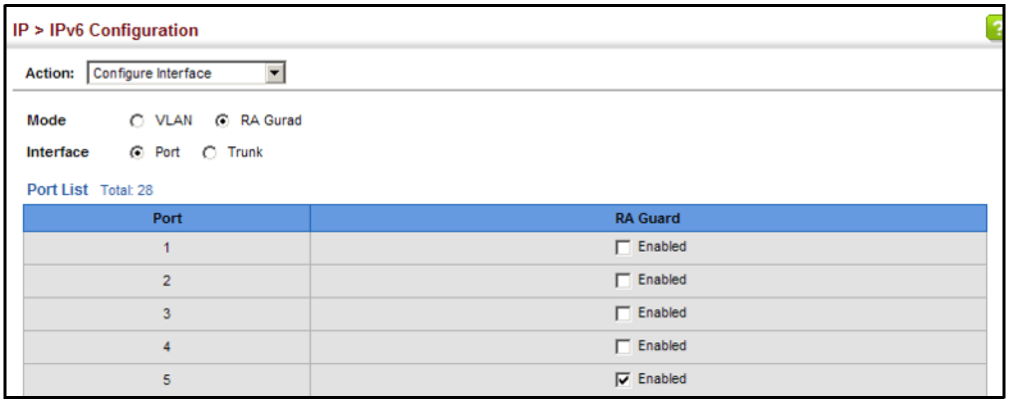
ND NS Interval (1000-3600000) 1000 ms

ND Reachable-Time (0-3600000) 30000 ms

To configure RA Guard for the switch:

1. Click IP, IPv6 Configuration.
2. Select Configure Interface from the Action list.
3. Select RA Guard mode.
4. Enable RA Guard for untrusted interfaces.
5. Click Apply.

Figure 407: Configuring RA Guard for an IPv6 Interface



IP > IPv6 Configuration

Action: Configure Interface

Mode ○ VLAN ● RA Gurad

Interface ● Port ○ Trunk

Port List Total: 28

Port	RA Guard
1	□ Enabled
2	□ Enabled
3	□ Enabled
4	□ Enabled
5	☑ Enabled

CONFIGURING AN IPV6 ADDRESS

Use the IP > IPv6 Configuration (Add IPv6 Address) page to configure an initial IPv6 interface for management access over the network, or for creating an interface to multiple subnets.

CLI REFERENCES

- "IPv6 Interface" on page 1663

COMMAND USAGE

- All IPv6 addresses must be formatted according to RFC 2373 “IPv6 Addressing Architecture,” using 8 colon-separated 16-bit hexadecimal values. One double colon may be used in the address to indicate the appropriate number of zeros required to fill the undefined fields.
- The switch must always be configured with a link-local address. Therefore, explicitly enabling IPv6 (see "Configuring IPv6 Interface Settings" on page 697) or manually assigning a global unicast address will also automatically generate a link-local unicast address. The prefix length for a link-local address is fixed at 64 bits, and the host portion of the default address is based on the modified EUI-64 (Extended Universal Identifier) form of the interface identifier (i.e., the physical MAC address). Alternatively, you can manually configure the link-local address by entering the full address with a network prefix in the range of FE80~FEBF.
- To connect to a larger network with multiple subnets, you must configure a global unicast address. There are several alternatives to configuring this address type:
  - It can be manually configured by specifying the entire network prefix and prefix length, and using the EUI-64 form of the interface identifier to automatically create the low-order 64 bits in the host portion of the address.
  - You can also manually configure the global unicast address by entering the full address and prefix length.
- You can configure multiple IPv6 global unicast addresses per interface, but only one link-local address per interface.
- If a duplicate link-local address is detected on the local segment, this interface is disabled and a warning message displayed on the console. If a duplicate global unicast address is detected on the network, the address is disabled on this interface and a warning message displayed on the console.
- When an explicit address is assigned to an interface, IPv6 is automatically enabled, and cannot be disabled until all assigned addresses have been removed.

PARAMETERS

These parameters are displayed:

- **VLAN** – ID of a configured VLAN which is to be used for management access, or for creating an interface to multiple subnets. By default, all ports on the switch are members of VLAN 1. However, the management station can be attached to a port belonging to any VLAN, as long as that VLAN has been assigned an IP address. (Range: 1-4094)
- **Address Type** – Defines the address type configured for this interface.
  - **Global** – Configures an IPv6 global unicast address with a full IPv6 address including the network prefix and host address bits, followed

by a forward slash, and a decimal value indicating how many contiguous bits (from the left) of the address comprise the prefix (i.e., the network portion of the address).

- **EUI-64** (Extended Universal Identifier) – Configures an IPv6 address for an interface using an EUI-64 interface ID in the low order 64 bits.

  - When using EUI-64 format for the low-order 64 bits in the host portion of the address, the value entered in the IPv6 Address field includes the network portion of the address, and the prefix length indicates how many contiguous bits (starting at the left) of the address comprise the prefix (i.e., the network portion of the address). Note that the value specified in the IPv6 Address field may include some of the high-order host bits if the specified prefix length is less than 64 bits. If the specified prefix length exceeds 64 bits, then the bits used in the network portion of the address will take precedence over the interface identifier.

  - IPv6 addresses are 16 bytes long, of which the bottom 8 bytes typically form a unique host identifier based on the device's MAC address. The EUI-64 specification is designed for devices that use an extended 8-byte MAC address. For devices that still use a 6-byte MAC address (also known as EUI-48 format), it must be converted into EUI-64 format by inverting the universal/local bit in the address and inserting the hexadecimal number FFFE between the upper and lower three bytes of the MAC address.

    For example, if a device had an EUI-48 address of 28-9F-18-1C-82-35, the global/local bit must first be inverted to meet EUI-64 requirements (i.e., 1 for globally defined addresses and 0 for locally defined addresses), changing 28 to 2A. Then the two bytes FFFE are inserted between the OUI (i.e., organizationally unique identifier, or company identifier) and the rest of the address, resulting in a modified EUI-64 interface identifier of 2A-9F-18-FF-FE-1C-82-35.

  - This host addressing method allows the same interface identifier to be used on multiple IP interfaces of a single device, as long as those interfaces are attached to different subnets.

- **Link Local** – Configures an IPv6 link-local address.

  - The address prefix must be in the range of FE80~FEBF.

  - You can configure only one link-local address per interface.

  - The specified address replaces a link-local address that was automatically generated for the interface.

◆ **IPv6 Address** – IPv6 address assigned to this interface.

WEB INTERFACE

To configure an IPv6 address:

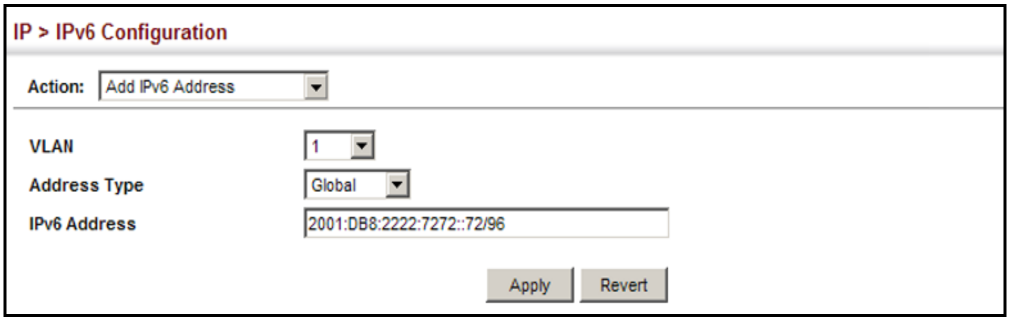
1. Click IP, IPv6 Configuration.

2. Select Add IPv6 Address from the Action list.

3. Specify the VLAN to configure, select the address type, and then enter an IPv6 address and prefix length.

4. Click Apply.

Figure 408: Configuring an IPv6 Address



IP > IPv6 Configuration

Action: Add IPv6 Address

VLAN: 1

Address Type: Global

IPv6 Address: 2001:DB8:2222:7272::72/96

SHOWING IPV6 ADDRESSES

Use the IP > IPv6 Configuration (Show IPv6 Address) page to display the IPv6 addresses assigned to an interface.

CLI REFERENCES

- "show ipv6 interface" on page 1672

PARAMETERS

These parameters are displayed:

- **VLAN** – ID of a configured VLAN. By default, all ports on the switch are members of VLAN 1. However, the management station can be attached to a port belonging to any VLAN, as long as that VLAN has been assigned an IP address. (Range: 1-4094)

- **IPv6 Address Type** – The address type (Global, EUI-64, Link Local).

- **IPv6 Address** – An IPv6 address assigned to this interface.

  In addition to the unicast addresses assigned to an interface, a node is also required to listen to the all-nodes multicast addresses FF01::1 (interface-local scope) and FF02::1 (link-local scope).

  FF01::1/16 is the transient interface-local multicast address for all attached IPv6 nodes, and FF02::1/16 is the link-local multicast address for all attached IPv6 nodes. The interface-local multicast address is only used for loopback transmission of multicast traffic. Link-local multicast addresses cover the same types as used by link-local unicast addresses, including all nodes (FF02::1), all routers (FF02::2), and solicited nodes (FF02::1:FFXX:XXXX) as described below.

A node is also required to compute and join the associated solicited-node multicast addresses for every unicast and anycast address it is assigned. IPv6 addresses that differ only in the high-order bits, e.g. due to multiple high-order prefixes associated with different aggregations, will map to the same solicited-node address, thereby reducing the number of multicast addresses a node must join. In this example, FF02::1:FF90:0/104 is the solicited-node multicast address which is formed by taking the low-order 24 bits of the address and appending those bits to the prefix.

Note that the solicited-node multicast address (link-local scope FF02) is used to resolve the MAC addresses for neighbor nodes since IPv6 does not support the broadcast method used by the Address Resolution Protocol in IPv4.

These additional addresses are displayed by the CLI (see "show ip interface" on page 1651).

◆ **Configuration Mode** – Indicates if this address was automatically generated or manually configured.

WEB INTERFACE

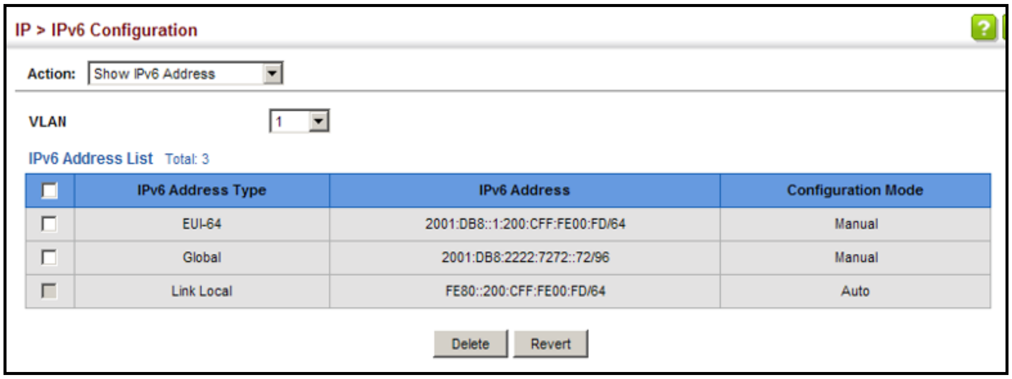
To show the configured IPv6 addresses:

1. Click IP, IPv6 Configuration.

2. Select Show IPv6 Address from the Action list.

3. Select a VLAN from the list.

Figure 409: Showing Configured IPv6 Addresses



IP > IPv6 Configuration

Action: Show IPv6 Address

VLAN 1

IPv6 Address List Total: 3

□	IPv6 Address Type	IPv6 Address	Configuration Mode
□	EUI-64	2001:DB8::1:200:CFF:FE00:FD/64	Manual
□	Global	2001:DB8:2222:7272::72/96	Manual
□	Link Local	FE80::200:CFF:FE00:FD/64	Auto

SHOWING THE IPV6 NEIGHBOR CACHE

Use the IP > IPv6 Configuration (Show IPv6 Neighbor Cache) page to display the IPv6 addresses detected for neighbor devices.

CLI REFERENCES

- "show ipv6 neighbors" on page 1694

PARAMETERS

These parameters are displayed:

Table 45: Show IPv6 Neighbors - display description

Field	Description
IPv6 Address	IPv6 address of neighbor
Age	The time since the address was verified as reachable (in seconds). A static entry is indicated by the value "Permanent."
Link-layer Address	Physical layer MAC address.
State	The following states are used for dynamic entries: ◆ Incomplete - Address resolution is being carried out on the entry. A neighbor solicitation message has been sent to the multicast address of the target, but it has not yet returned a neighbor advertisement message. ◆ Invalid - An invalidated mapping. Setting the state to invalid dis-associates the interface identified with this entry from the indicated mapping (RFC 4293). ◆ Reachable - Positive confirmation was received within the last ReachableTime interval that the forward path to the neighbor was functioning. While in Reachable state, the device takes no special action when sending packets. ◆ Stale - More than the ReachableTime interval has elapsed since the last positive confirmation was received that the forward path was functioning. While in Stale state, the device takes no action until a packet is sent. ◆ Delay - More than the ReachableTime interval has elapsed since the last positive confirmation was received that the forward path was functioning. A packet was sent within the last DELAY_FIRST_PROBE_TIME interval. If no reachability confirmation is received within this interval after entering the DELAY state, the switch will 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 interval until confirmation of reachability is received. ◆ Unknown - Unknown state. The following states are used for static entries: ◆ Incomplete -The interface for this entry is down. ◆ Permanent - Indicates a static entry. ◆ Reachable - The interface for this entry is up. Reachability detection is not applied to static entries in the IPv6 neighbor discovery cache.
VLAN	VLAN interface from which the address was reached.

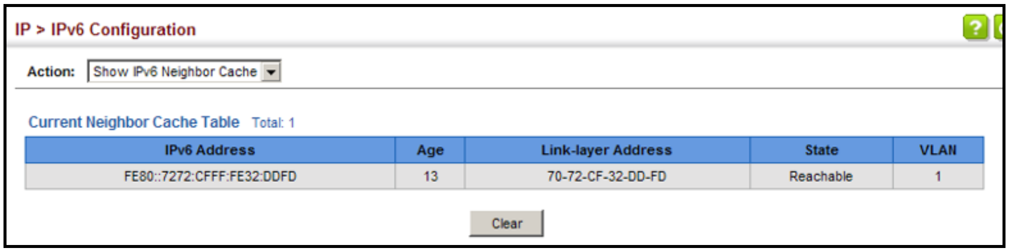
WEB INTERFACE

To show neighboring IPv6 devices:

1. Click IP, IPv6 Configuration.

2. Select Show IPv6 Neighbors from the Action list.

Figure 410: Showing IPv6 Neighbors



Current Neighbor Cache Table Total: 1

IPv6 Address	Age	Link-layer Address	State	VLAN
FE80::7272:CFFF:FE32:DDFD	13	70-72-CF-32-DD-FD	Reachable	1

SHOWING IPV6 STATISTICS

Use the IP > IPv6 Configuration (Show Statistics) page to display statistics about IPv6 traffic passing through this switch.

CLI REFERENCES

- "show ipv6 traffic" on page 1675

COMMAND USAGE

This switch provides statistics for the following traffic types:

- **IPv6** – The Internet Protocol for Version 6 addresses provides a mechanism for transmitting blocks of data (often called packets or frames) from a source to a destination, where these network devices (that is, hosts) are identified by fixed length addresses. The Internet Protocol also provides for fragmentation and reassembly of long packets, if necessary, for transmission through "small packet" networks.

- **ICMPv6** – Internet Control Message Protocol for Version 6 addresses is a network layer protocol that transmits message packets to report errors in processing IPv6 packets. ICMP is therefore an integral part of the Internet Protocol. ICMP messages may be used to report various situations, such as when a datagram cannot reach its destination, when the gateway does not have the buffering capacity to forward a datagram, and when the gateway can direct the host to send traffic on a shorter route. ICMP is also used by routers to feed back information about more suitable routes (that is, the next hop router) to use for a specific destination.

- **UDP** – User Datagram Protocol provides a datagram mode of packet switched communications. It uses IP as the underlying transport mechanism, providing access to IP-like services. UDP packets are delivered just like IP packets – connection-less datagrams that may be discarded before reaching their targets. UDP is useful when TCP would be too complex, too slow, or just unnecessary.

PARAMETERS

These parameters are displayed:

Table 46: Show IPv6 Statistics - display description

Field	Description
IPv6 Statistics	
IPv6 Received	
Total	The total number of input datagrams received by the interface, including those received in error.
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, IPv6 options, etc.
Too Big Errors	The number of input datagrams that could not be forwarded because their size exceeded the link MTU of outgoing interface.
No Routes	The number of input datagrams discarded because no route could be found to transmit them to their destination.
Address Errors	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.
Unknown Protocols	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.
Truncated Packets	The number of input datagrams discarded because datagram frame didn't carry enough data.
Discards	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.
Delivers	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.
Reassembly Request Datagrams	The number of IPv6 fragments received which needed to be reassembled at this interface. Note that this counter is increment ed at the interface to which these fragments were addressed which might not be necessarily the input interface for some of the fragments.
Reassembly Succeeded	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.
Reassembly Failed	The number of failures detected by the IPv6 re-assembly 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.

Table 46: Show IPv6 Statistics - display description (Continued)

Field	Description
IPv6 Transmitted	
Forwards Datagrams	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."
Requests	The 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.
Discards	The 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.
No Routes	The number of input datagrams discarded because no route could be found to transmit them to their destination.
Generated Fragments	The number of output datagram fragments that have been generated as a result of fragmentation at this output interface.
Fragment Succeeded	The number of IPv6 datagrams that have been successfully fragmented at this output interface.
Fragment Failed	The number of IPv6 datagrams that have been discarded because they needed to be fragmented at this output interface but could not be.
ICMPv6 Statistics	
ICMPv6 received	
Input	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.
Errors	The number of ICMP messages which the interface received but determined as having ICMP-specific errors (bad ICMP check sums, bad length, etc.).
Destination Unreachable Messages	The number of ICMP Destination Unreachable messages received by the interface.
Packet Too Big Messages	The number of ICMP Packet Too Big messages received by the interface.
Time Exceeded Messages	The number of ICMP Time Exceeded messages received by the interface.
Parameter Problem Messages	The number of ICMP Parameter Problem messages received by the interface.
Echo Request Messages	The number of ICMP Echo (request) messages received by the interface.
Echo Reply Messages	The number of ICMP Echo Reply messages received by the interface.
Router Solicit Messages	The number of ICMP Router Solicit messages received by the interface.
Router Advertisement Messages	The number of ICMP Router Advertisement messages received by the interface.
Neighbor Solicit Messages	The number of ICMP Neighbor Solicit messages received by the interface.

Table 46: Show IPv6 Statistics - display description (Continued)

Field	Description
Neighbor Advertisement Messages	The number of ICMP Neighbor Advertisement messages received by the interface.
Redirect Messages	The number of Redirect messages received by the interface.
Group Membership Query Messages	The number of ICMPv6 Group Membership Query messages received by the interface.
Group Membership Response Messages	The number of ICMPv6 Group Membership Response messages received by the interface.
Group Membership Reduction Messages	The number of ICMPv6 Group Membership Reduction messages received by the interface.
Multicast Listener Discovery Version 2 Reports	The number of MLDv2 reports received by the interface.
ICMPv6 Transmitted	
Output	The total number of ICMP messages which this interface attempted to send. Note that this counter includes all those counted by icmpOutErrors.
Destination Unreachable Messages	The number of ICMP Destination Unreachable messages sent by the interface.
Packet Too Big Messages	The number of ICMP Packet Too Big messages sent by the interface.
Time Exceeded Messages	The number of ICMP Time Exceeded messages sent by the interface.
Parameter Problem Message	The number of ICMP Parameter Problem messages sent by the interface.
Echo Request Messages	The number of ICMP Echo (request) messages sent by the interface.
Echo Reply Messages	The number of ICMP Echo Reply messages sent by the interface.
Router Solicit Messages	The number of ICMP Router Solicitation messages sent by the interface.
Router Advertisement Messages	The number of ICMP Router Advertisement messages sent by the interface.
Neighbor Solicit Messages	The number of ICMP Neighbor Solicit messages sent by the interface.
Neighbor Advertisement Messages	The number of ICMP Router Advertisement messages sent by the interface.
Redirect Messages	The number of Redirect messages sent. For a host, this object will always be zero, since hosts do not send redirects.
Group Membership Query Messages	The number of ICMPv6 Group Membership Query messages sent by the interface.
Group Membership Response Messages	The number of ICMPv6 Group Membership Response messages sent.
Group Membership Reduction Messages	The number of ICMPv6 Group Membership Reduction messages sent.
Multicast Listener Discovery Version 2 Reports	The number of MLDv2 reports sent by the interface.
UDP Statistics	
Input	The total number of UDP datagrams delivered to UDP users.

Table 46: Show IPv6 Statistics - display description (Continued)

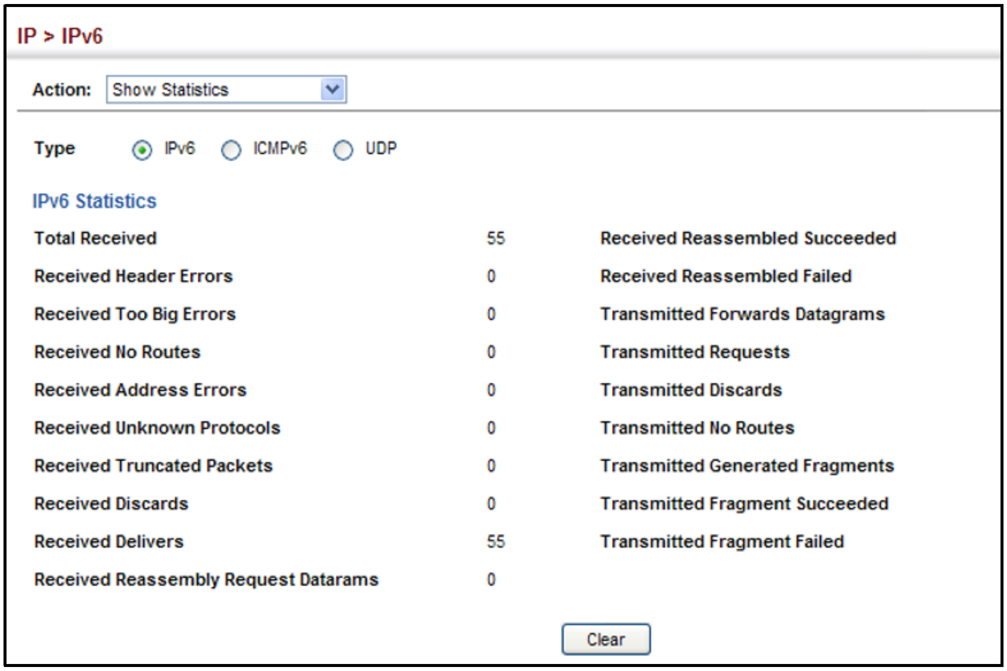
Field	Description
No Port Errors	The total number of received UDP datagrams for which there was no application at the destination port.
Other Errors	The number of received UDP datagrams that could not be delivered for reasons other than the lack of an application at the destination port.
Output	The total number of UDP datagrams sent from this entity.

WEB INTERFACE

To show the IPv6 statistics:

1. Click IP, IPv6 Configuration.
2. Select Show Statistics from the Action list.
3. Click IPv6, ICMPv6 or UDP.

Figure 411: Showing IPv6 Statistics (IPv6)



IP > IPv6

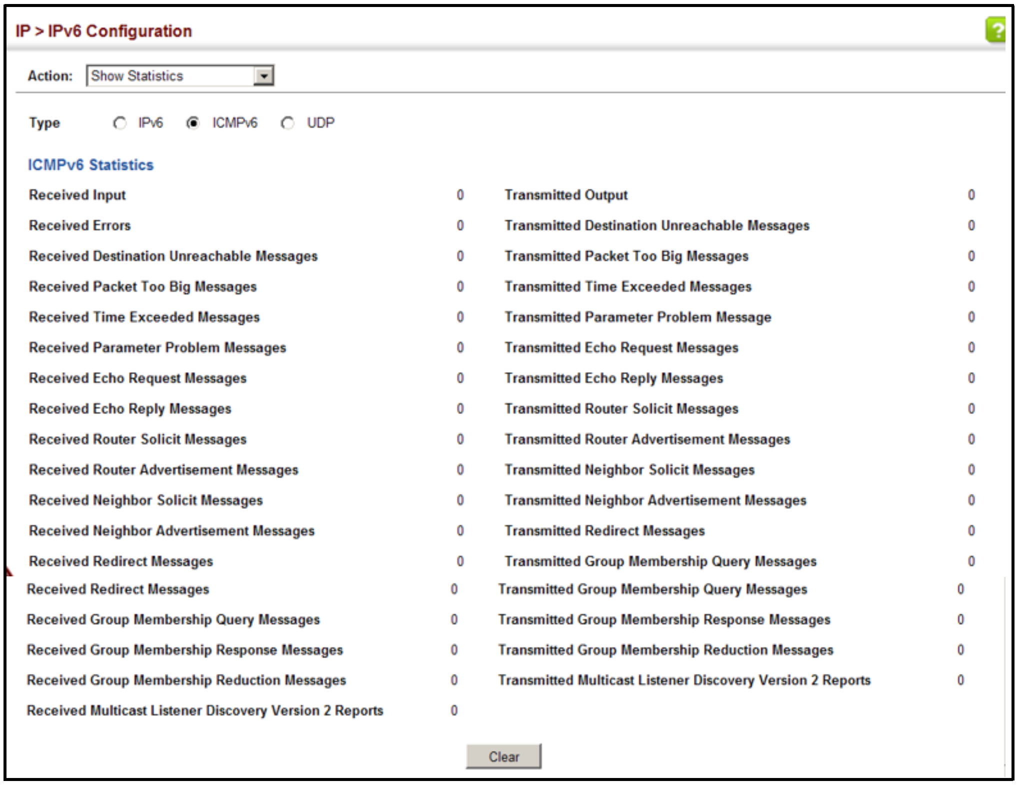
Action: Show Statistics

Type ● IPv6 ○ ICMPv6 ○ UDP

IPv6 Statistics

Total Received	55	Received Reassembled Succeeded
Received Header Errors	0	Received Reassembled Failed
Received Too Big Errors	0	Transmitted Forwards Datagrams
Received No Routes	0	Transmitted Requests
Received Address Errors	0	Transmitted Discards
Received Unknown Protocols	0	Transmitted No Routes
Received Truncated Packets	0	Transmitted Generated Fragments
Received Discards	0	Transmitted Fragment Succeeded
Received Delivers	55	Transmitted Fragment Failed
Received Reassembly Request Datarams	0	

Figure 412: Showing IPv6 Statistics (ICMPv6)



IP > IPv6 Configuration

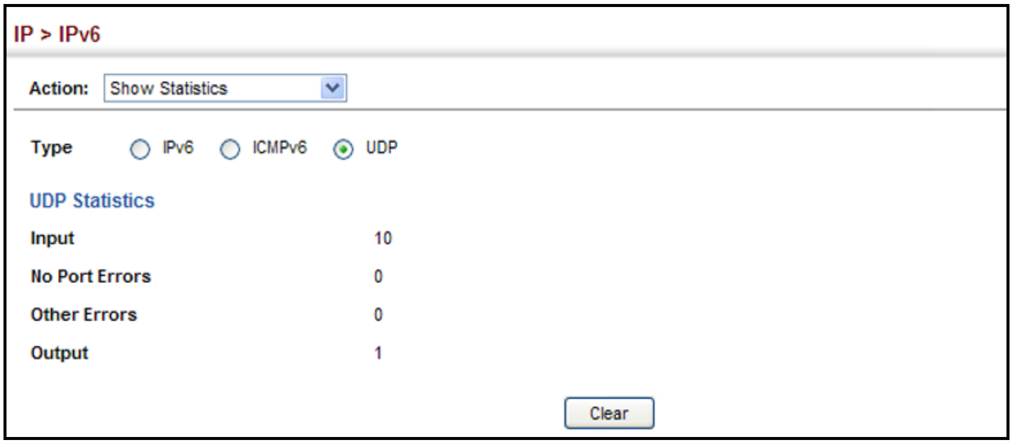
Action: Show Statistics

Type ○ IPv6 ● ICMPv6 ○ UDP

ICMPv6 Statistics

Received Input	0	Transmitted Output	0
Received Errors	0	Transmitted Destination Unreachable Messages	0
Received Destination Unreachable Messages	0	Transmitted Packet Too Big Messages	0
Received Packet Too Big Messages	0	Transmitted Time Exceeded Messages	0
Received Time Exceeded Messages	0	Transmitted Parameter Problem Message	0
Received Parameter Problem Messages	0	Transmitted Echo Request Messages	0
Received Echo Request Messages	0	Transmitted Echo Reply Messages	0
Received Echo Reply Messages	0	Transmitted Router Solicit Messages	0
Received Router Solicit Messages	0	Transmitted Router Advertisement Messages	0
Received Router Advertisement Messages	0	Transmitted Neighbor Solicit Messages	0
Received Neighbor Solicit Messages	0	Transmitted Neighbor Advertisement Messages	0
Received Neighbor Advertisement Messages	0	Transmitted Redirect Messages	0
Received Redirect Messages	0	Transmitted Group Membership Query Messages	0
Received Redirect Messages	0	Transmitted Group Membership Query Messages	0
Received Group Membership Query Messages	0	Transmitted Group Membership Response Messages	0
Received Group Membership Response Messages	0	Transmitted Group Membership Reduction Messages	0
Received Group Membership Reduction Messages	0	Transmitted Multicast Listener Discovery Version 2 Reports	0
Received Multicast Listener Discovery Version 2 Reports	0		

Figure 413: Showing IPv6 Statistics (UDP)



IP > IPv6

Action: Show Statistics

Type ○ IPv6 ○ ICMPv6 ● UDP

UDP Statistics

Input	10
No Port Errors	0
Other Errors	0
Output	1

SHOWING THE MTU FOR RESPONDING DESTINATIONS

Use the IP > IPv6 Configuration (Show MTU) page to display the maximum transmission unit (MTU) cache for destinations that have returned an ICMP packet-too-big message along with an acceptable MTU to this switch.

CLI REFERENCES

- "show ipv6 mtu" on page 1674

PARAMETERS

These parameters are displayed:

Table 47: Show MTU - display description

Field	Description
MTU	Adjusted MTU contained in the ICMP packet-too-big message returned from this destination, and now used for all traffic sent along this path.
Since	Time since an ICMP packet-too-big message was received from this destination.
Destination Address	Address which sent an ICMP packet-too-big message.

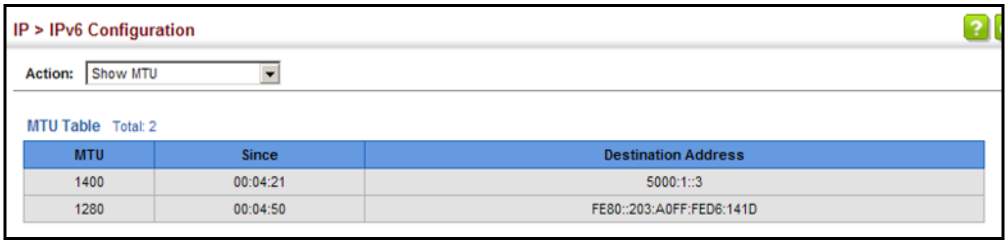
WEB INTERFACE

To show the MTU reported from other devices:

1. Click IP, IPv6 Configuration.

2. Select Show MTU from the Action list.

Figure 414: Showing Reported MTU Values



IP > IPv6 Configuration

Action: Show MTU

MTU Table Total: 2

MTU	Since	Destination Address
1400	00:04:21	5000:1::3
1280	00:04:50	FE80::203:A0FF:FED6:141D

17 IP Services

This chapter describes the following IP services:

- DNS – Configures default domain names, identifies servers to use for dynamic lookup, and shows how to configure static entries.
- DHCP Client – Specifies the DHCP client identifier for an interface.
- DHCP Relay – Enables DHCP relay service, and defines the servers to which client requests are forwarded.
- DHCP Server – Configures address to be allocated to networks or specific hosts.
- UDP Helper – Configures the switch to forward UDP broadcast packets originating from host applications to another part of the network.
- PPPoE Intermediate Agent – Configures PPPoE Intermediate Agent (PPPoE IA) relay parameters required for passing authentication messages between a client and broadband remote access servers.

Domain Name Service

DNS service on this switch allows host names to be mapped to IP addresses using static table entries or by redirection to other name servers on the network. When a client device designates this switch as a DNS server, the client will attempt to resolve host names into IP addresses by forwarding DNS queries to the switch, and waiting for a response.

You can manually configure entries in the DNS table used for mapping domain names to IP addresses, configure default domain names, or specify one or more name servers to use for domain name to address translation.

Configuring General DNS Service Parameters

Use the IP Service > DNS - General (Configure Global) page to enable domain lookup and set the default domain name.

CLI References

- "ip domain-lookup" on page 1616
- "ip domain-name" on page 1617

COMMAND USAGE

- To enable DNS service on this switch, enable domain lookup status, and configure one or more name servers (see "Configuring a List of Name Servers" on page 716).

PARAMETERS

These parameters are displayed:

- **Domain Lookup** – Enables DNS host name-to-address translation. (Default: Disabled)

- **Default Domain Name** – Defines the default domain name appended to incomplete host names. Do not include the initial dot that separates the host name from the domain name.
  (Range: 1-127 alphanumeric characters)

WEB INTERFACE

To configure general settings for DNS:

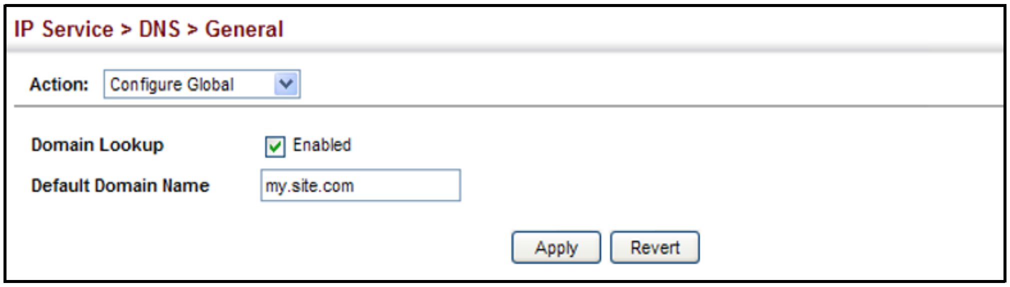
1. Click IP Service, DNS.

2. Select Configure Global from the Action list.

3. Enable domain lookup, and set the default domain name.

4. Click Apply.

Figure 415: Configuring General Settings for DNS



IP Service > DNS > General

Action: Configure Global

Domain Lookup ☑ Enabled

Default Domain Name my.site.com

CONFIGURING A LIST OF DOMAIN NAMES

Use the IP Service > DNS - General (Add Domain Name) page to configure a list of domain names to be tried in sequential order.

CLI REFERENCES

- "ip domain-list" on page 1615
- "show dns" on page 1621

COMMAND USAGE

- Use this page to define a list of 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).

- If there is no domain list, the default domain name is used (see "Configuring General DNS Service Parameters" on page 713). If there is a domain list, the system will search it for a corresponding entry. If none is found, it will use the default domain name.

- When an incomplete host name is received by the DNS service on this switch and a domain name list has been specified, the switch will work through the domain list, appending each domain name in the list to the host name, and checking with the specified name servers for a match (see "Configuring a List of Name Servers" on page 716).

PARAMETERS

These parameters are displayed:

Domain Name – Name of the host. Do not include the initial dot that separates the host name from the domain name.
(Range: 1-68 characters)

WEB INTERFACE

To create a list domain names:

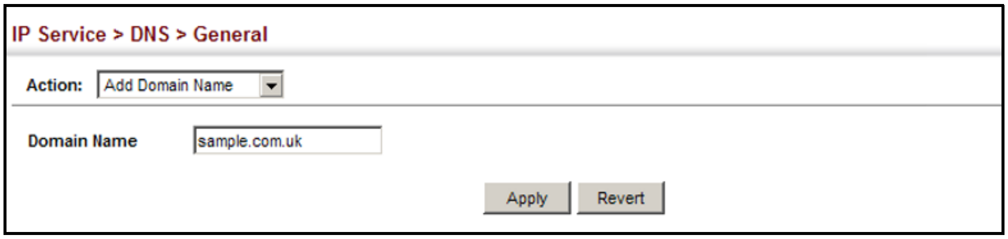
1. Click IP Service, DNS.

2. Select Add Domain Name from the Action list.

3. Enter one domain name at a time.

4. Click Apply.

Figure 416: Configuring a List of Domain Names for DNS



IP Service > DNS > General

Action: Add Domain Name

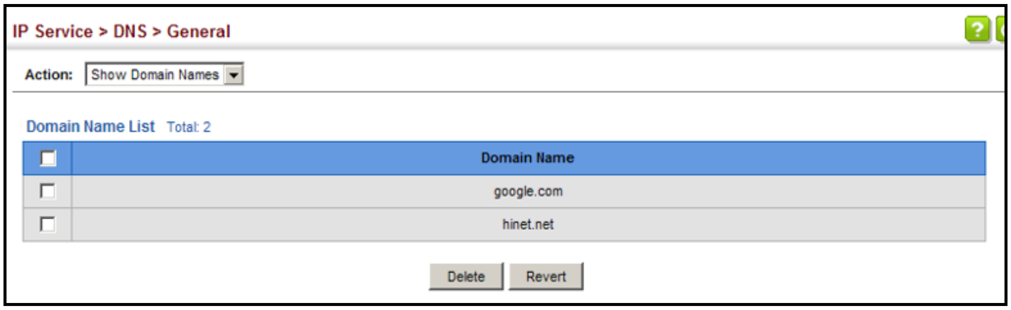
Domain Name: sample.com.uk

To show the list domain names:

1. Click IP Service, DNS.

2. Select Show Domain Names from the Action list.

Figure 417: Showing the List of Domain Names for DNS



IP Service > DNS > General

Action: Show Domain Names

Domain Name List Total: 2

□	Domain Name
□	google.com
□	hinet.net

Configuring a List of Name Servers

Use the IP Service > DNS - General (Add Name Server) page to configure a list of name servers to be tried in sequential order.

CLI References

- "ip name-server" on page 1619
- "show dns" on page 1621

Command Usage

- To enable DNS service on this switch, configure one or more name servers, and enable domain lookup status (see "Configuring General DNS Service Parameters" on page 713).

- When more than one name server is specified, the servers are queried in the specified sequence until a response is received, or the end of the list is reached with no response.

- If all name servers are deleted, DNS will automatically be disabled. This is done by disabling the domain lookup status.

Parameters

These parameters are displayed:

Name Server IP Address – Specifies the IPv4 or IPv6 address of a domain name server to use for name-to-address resolution. Up to six IP addresses can be added to the name server list.

Web Interface

To create a list name servers:

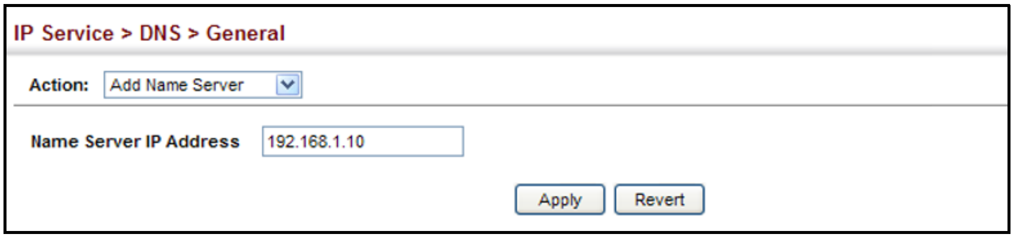
1. Click IP Service, DNS.

2. Select Add Name Server from the Action list.

3. Enter one name server at a time.

4. Click Apply.

Figure 418: Configuring a List of Name Servers for DNS



IP Service > DNS > General

Action: Add Name Server

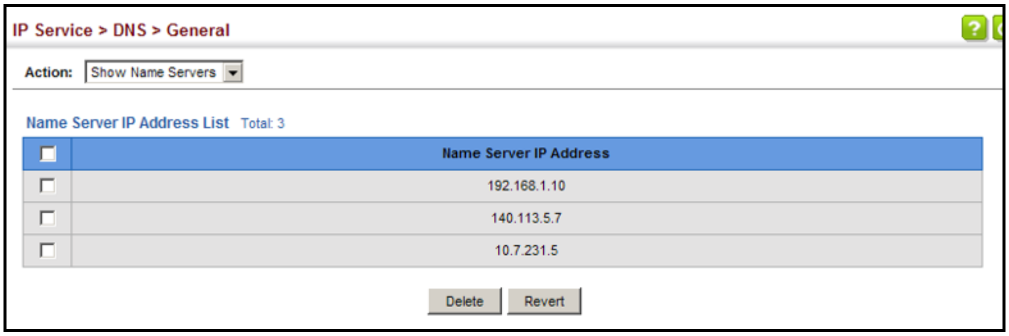
Name Server IP Address: 192.168.1.10

To show the list name servers:

1. Click IP Service, DNS.

2. Select Show Name Servers from the Action list.

Figure 419: Showing the List of Name Servers for DNS



IP Service > DNS > General

Action: Show Name Servers

Name Server IP Address List Total: 3

□	Name Server IP Address
□	192.168.1.10
□	140.113.5.7
□	10.7.231.5

CONFIGURING STATIC DNS HOST TO ADDRESS ENTRIES

Use the IP Service > DNS - Static Host Table (Add) page to manually configure static entries in the DNS table that are used to map domain names to IP addresses.

CLI REFERENCES

- "ip host" on page 1618
- "show hosts" on page 1622

COMMAND USAGE

- Static entries may be used for local devices connected directly to the attached network, or for commonly used resources located elsewhere on the network.

PARAMETERS

These parameters are displayed:

- **Host Name** – Name of a host device that is mapped to one or more IP addresses. (Range: 1-127 characters)

- **IP Address** – Internet address(es) associated with a host name.

WEB INTERFACE

To configure static entries in the DNS table:

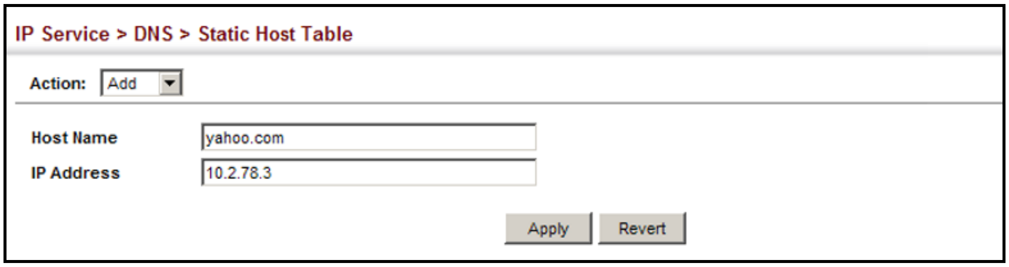
1. Click IP Service, DNS, Static Host Table.

2. Select Add from the Action list.

3. Enter a host name and the corresponding address.

4. Click Apply.

Figure 420: Configuring Static Entries in the DNS Table



IP Service > DNS > Static Host Table

Action: Add

Host Name: yahoo.com

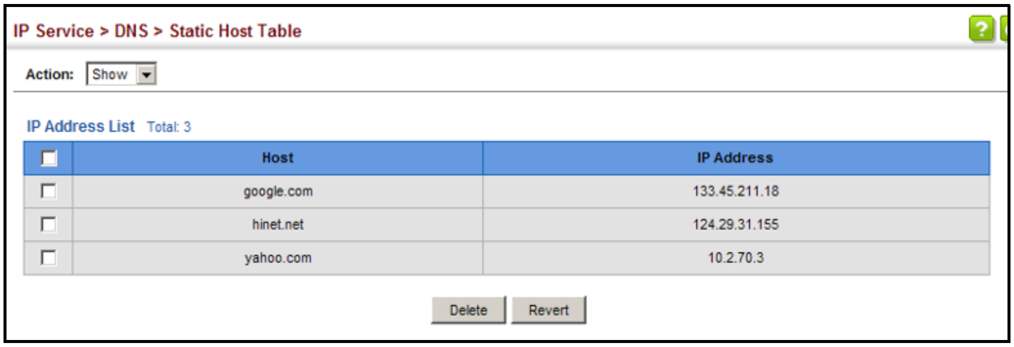
IP Address: 10.2.78.3

To show static entries in the DNS table:

1. Click IP Service, DNS, Static Host Table.

2. Select Show from the Action list.

Figure 421: Showing Static Entries in the DNS Table



IP Service > DNS > Static Host Table

Action: Show

IP Address List Total: 3

□	Host	IP Address
□	google.com	133.45.211.18
□	hinet.net	124.29.31.155
□	yahoo.com	10.2.70.3

DISPLAYING THE DNS CACHE

Use the IP Service > DNS - Cache page to display entries in the DNS cache that have been learned via the designated name servers.

CLI REFERENCES

- "show dns cache" on page 1622

COMMAND USAGE

- Servers or other network devices may support one or more connections via multiple IP addresses. If more than one IP address is associated with a host name via information returned from a name server, a DNS client can try each address in succession, until it establishes a connection with the target device.

Parameters

These parameters are displayed:

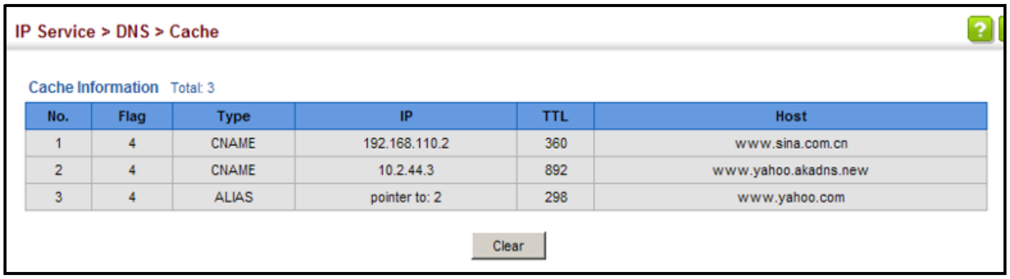
- **No.** – The entry number for each resource record.
- **Flag** – The flag is always "4" indicating a cache entry and therefore unreliable.
- **Type** – This field includes CNAME which specifies the host address for the owner, and ALIAS which specifies an alias.
- **IP** – The IP address associated with this record.
- **TTL** – The time to live reported by the name server.
- **Host** – The host name associated with this record.

Web Interface

To display entries in the DNS cache:

1. Click IP Service, DNS, Cache.

Figure 422: Showing Entries in the DNS Cache



IP Service > DNS > Cache

Cache Information Total: 3

No.	Flag	Type	IP	TTL	Host
1	4	CNAME	192.168.110.2	360	www.sina.com.cn
2	4	CNAME	10.2.44.3	892	www.yahoo.akadns.new
3	4	ALIAS	pointer to: 2	298	www.yahoo.com

Dynamic Host Configuration Protocol

Dynamic Host Configuration Protocol (DHCP) can dynamically allocate an IP address and other configuration information to network clients when they boot up. If a subnet does not already include a BOOTP or DHCP server, you can relay DHCP client requests to a DHCP server on another subnet, or configure the DHCP server on this switch to support that subnet.

When configuring the DHCP server on this switch, you can configure an address pool for each unique IP interface, or manually assign a static IP address to clients based on their hardware address or client identifier. The DHCP server can provide the host's IP address, domain name, gateway router and DNS server, information about the host's boot image including the TFTP server to access for download and the name of the boot file, or boot information for NetBIOS Windows Internet Naming Service (WINS).

SPECIFYING A DHCP CLIENT IDENTIFIER

Use the IP Service > DHCP > Client page to specify the DHCP client identifier for a VLAN interface.

CLI REFERENCES

- "ip dhcp client class-id" on page 1625

COMMAND USAGE

- The class identifier is used identify the vendor class and configuration of the switch to the DHCP server, which then uses this information to decide on how to service the client or the type of information to return.

- The general framework for this DHCP option is set out in RFC 2132 (Option 60). This information is used to convey configuration settings or other identification information about a client, but the specific string to use should be supplied by your service provider or network administrator. Options 60, 66 and 67 statements can be added to the server daemon's configuration file.

Table 48: Options 60, 66 and 67 Statements

Option	Statement	
	Keyword	Parameter
60	vendor-class-identifier	a string indicating the vendor class identifier
66	tftp-server-name	a string indicating the tftp server name
67	bootfile-name	a string indicating the bootfile name

- By default, DHCP option 66/67 parameters are not carried in a DHCP server reply. To ask for a DHCP reply with option 66/67 information, the DHCP client request sent by this switch includes a "parameter request list" asking for this information. Besides, the client request also includes a "vendor class identifier" that allows the DHCP server to identify the device, and select the appropriate configuration file for download. This information is included in Option 55 and 124.

Table 49: Options 55 and 124 Statements

Option	Statement	
	Keyword	Parameter
55	dhcp-parameter-request-list	a list of parameters, separated by ','
124	vendor-class-identifier	a string indicating the vendor class identifier

- The server should reply with the TFTP server name and boot file name.

- Note that the vendor class identifier can be formatted in either text or hexadecimal, but the format used by both the client and server must be the same.

PARAMETERS

These parameters are displayed:

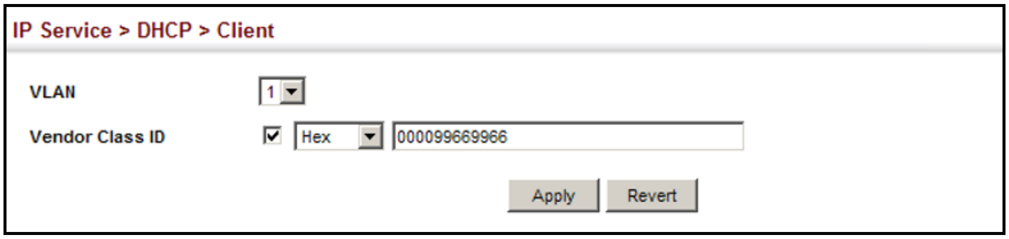
- **VLAN** – ID of configured VLAN.
- **Vendor Class ID** – The following options are supported when the check box is marked to enable this feature:
  - **Default** – The default string is ECS4660-28F.
  - **Text** – A text string. (Range: 1-32 characters)
  - **Hex** – A hexadecimal value. (Range: 1-64 characters)

WEB INTERFACE

To configure a DHCP client identifier:

1. Click IP Service, DHCP, Client.
2. Mark the check box to enable this feature. Select the default setting, or the format for a vendor class identifier. If a non-default value is used, enter a text string or hexadecimal value.
3. Click Apply.

Figure 423: Specifying A DHCP Client Identifier



IP Service > DHCP > Client

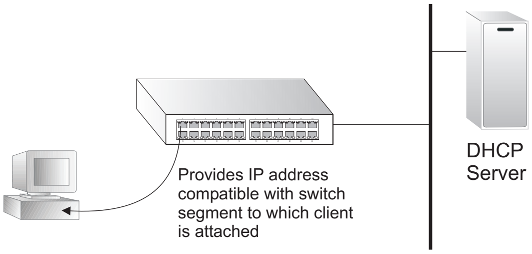
VLAN: 1

Vendor Class ID: ☑ Hex 000099669966

CONFIGURING DHCP RELAY SERVICE

Use the IP Service > DHCP > Relay page to configure DHCP relay service for attached host devices. If DHCP relay is enabled, and this switch sees a DHCP request broadcast, it inserts its own IP address into the request so that the DHCP server will know the subnet where the client is located. Then, the switch forwards the packet to the DHCP server. When the server receives the DHCP request, it allocates a free IP address for the DHCP client from its defined scope for the DHCP client’s subnet, and sends a DHCP response back to the DHCP relay agent (i.e., this switch). This switch then broadcasts the DHCP response received from the server to the client.

Figure 424: Layer 3 DHCP Relay Service


Provides IP address compatible with switch segment to which client is attached
DHCP Server

CLI REFERENCES

- "ip dhcp relay server" on page 1629
- "ip dhcp restart relay" on page 1630

COMMAND USAGE

- You must specify the IP address for at least one DHCP server. Otherwise, the switch’s DHCP relay agent will not forward client requests to a DHCP server.
- DHCP relay configuration will be disabled if an active DHCP server is detected on the same network segment.

PARAMETERS

These parameters are displayed:

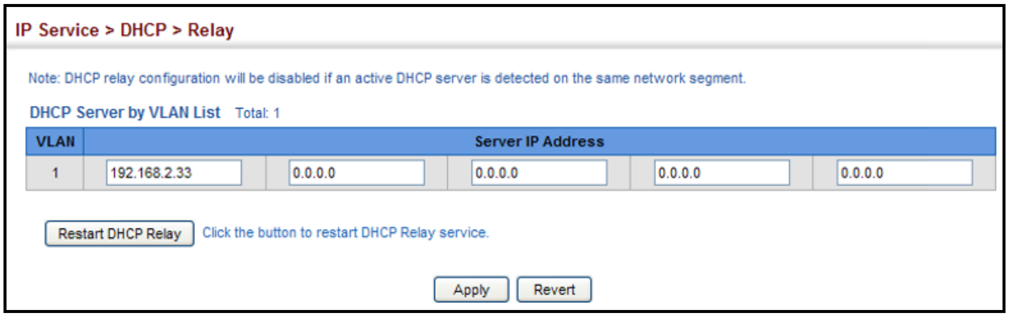
- **VLAN ID** – ID of configured VLAN.
- **Server IP Address** – Addresses of DHCP servers to be used by the switch’s DHCP relay agent in order of preference.
- **Restart DHCP Relay** – Use this button to re-initialize DHCP relay service.

WEB INTERFACE

To configure DHCP relay service:

1. Click IP Service, DHCP, Relay.
2. Enter up to five IP addresses for any VLAN.
3. Click Apply.

Figure 425: Configuring DHCP Relay Service



IP Service > DHCP > Relay

Note: DHCP relay configuration will be disabled if an active DHCP server is detected on the same network segment.

DHCP Server by VLAN List Total: 1

VLAN	Server IP Address				
1	192.168.2.33	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0

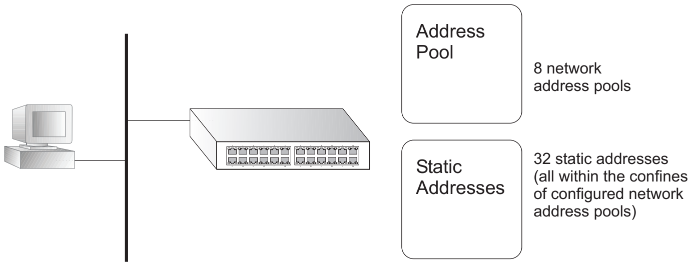
Click the button to restart DHCP Relay service.

CONFIGURING THE DHCP SERVER

This switch includes a Dynamic Host Configuration Protocol (DHCP) server that can assign temporary IP addresses to any attached host requesting service. It can also provide other network settings such as the domain name, default gateway, Domain Name Servers (DNS), Windows Internet Naming Service (WINS) name servers, or information on the bootup file for the host device to download.

Addresses can be assigned to clients from a common address pool configured for a specific IP interface on this switch, or fixed addresses can be assigned to hosts based on the client identifier code or MAC address.

Figure 426: DHCP Server



Address Pool
8 network address pools
Static Addresses
32 static addresses (all within the confines of configured network address pools)

COMMAND USAGE

- First configure any excluded addresses, including the address for this switch.
- Then configure address pools for the network interfaces. You can configure up to 8 network address pools. You can also manually bind an address to a specific client if required. However, any fixed addresses must fall within the range of an existing network address pool. You can configure up to 32 fixed host addresses (i.e., entering one address per pool).
- If the DHCP server is running, you must disable it and then re-enable it to implement any configuration changes. This can be done on the IP Service > DHCP > Server (Configure Global) page.

ENABLING THE SERVER

Use the IP Service > DHCP > Server (Configure Global) page to enable the DHCP Server.

CLI REFERENCES

- "service dhcp" on page 1634

PARAMETERS

These parameters are displayed:

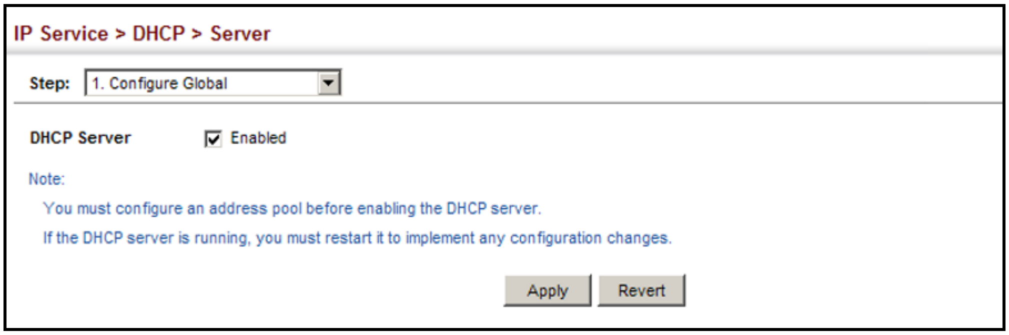
- **DHCP Server** – Enables or disables the DHCP server on this switch. (Default: Disabled)

WEB INTERFACE

To enable the DHCP server:

1. Click IP Service, DHCP, Server.
2. Select Configure Global from the Step list.
3. Mark the Enabled box.
4. Click Apply.

Figure 427: Enabling the DHCP Server



IP Service > DHCP > Server

Step: 1. Configure Global

DHCP Server ☑ Enabled

Note:
You must configure an address pool before enabling the DHCP server.
If the DHCP server is running, you must restart it to implement any configuration changes.

SETTING EXCLUDED ADDRESSES

Use the IP Service > DHCP > Server (Configure Excluded Addresses – Add) page to specify the IP addresses that should not be assigned to clients.

CLI REFERENCES

- "ip dhcp excluded-address" on page 1633

PARAMETERS

These parameters are displayed:

- **Start IP Address** – Specifies a single IP address or the first address in a range that the DHCP server should not assign to DHCP clients.
- **End IP Address** – The last address in a range that the DHCP server should not assign to DHCP clients.

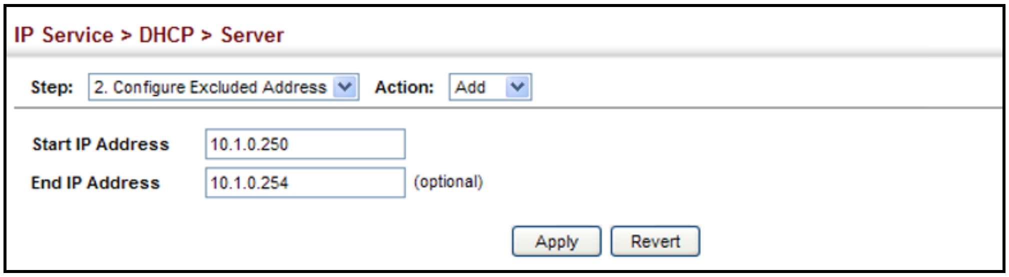
NOTE: Be sure you exclude the address for this switch and other key network devices.

WEB INTERFACE

To configure IP addresses excluded for DHCP clients:

1. Click IP Service, DHCP, Server.
2. Select Configure Excluded Addresses from the Step list.
3. Select Add from the Action list.
4. Enter a single address or an address range.
5. Click Apply.

Figure 428: Configuring Excluded Addresses on the DHCP Server



IP Service > DHCP > Server

Step: 2. Configure Excluded Address Action: Add

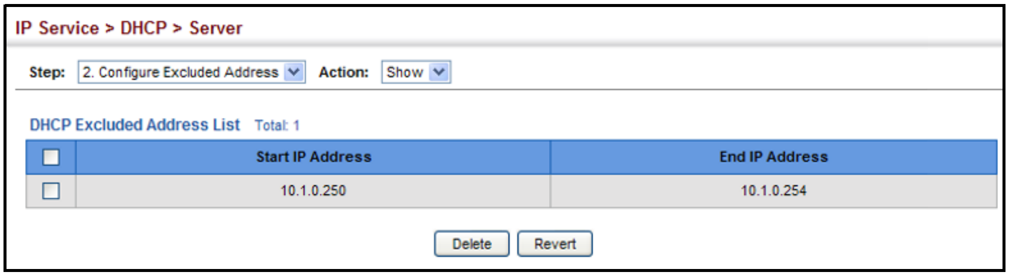
Start IP Address 10.1.0.250

End IP Address 10.1.0.254 (optional)

To show the IP addresses excluded for DHCP clients:

1. Click IP Service, DHCP, Server.
2. Select Configure Excluded Addresses from the Step list.
3. Select Show from the Action list.

Figure 429: Showing Excluded Addresses on the DHCP Server



IP Service > DHCP > Server

Step: 2. Configure Excluded Address Action: Show

DHCP Excluded Address List Total: 1

□	Start IP Address	End IP Address
□	10.1.0.250	10.1.0.254

CONFIGURING ADDRESS POOLS

Use the IP Service > DHCP > Server (Configure Pool – Add) page configure IP address pools for each IP interface that will provide addresses to attached clients via the DHCP server.

CLI REFERENCES

- "DHCP Server" on page 1632

COMMAND USAGE

- First configure address pools for the network interfaces. Then you can manually bind an address to a specific client if required. However, note that any static host address must fall within the range of an existing network address pool. You can configure up to 8 network address pools, and up to 32 manually bound host address pools (i.e., one address per host pool). Just note that any address specified in a host address pool must fall within the range of a configured network address pool.

- When a client request is received, the switch first checks for a network address pool matching the gateway where the request originated (i.e., if the request was forwarded by a relay server). If there is no gateway in the client request (i.e., the request was not forwarded by a relay server), the switch searches for a network pool matching the interface through which the client request was received. It then searches for a manually configured host address that falls within the matching network pool. If no manually configured host address is found, it assigns an address from the matching network address pool. However, if no matching address pool is found the request is ignored.

- When searching for a manual binding, the switch compares the client identifier and then the hardware address for DHCP clients. Since BOOTP clients cannot transmit a client identifier, you must configure a hardware address for this host type. If no manual binding has been specified for a host entry with a hardware address or client identifier, the switch will assign an address from the first matching network pool.

- If the subnet mask is not specified for network or host address pools, the class A, B, or C natural mask is used (see "Specifying Network Interfaces" on page 775). The DHCP server assumes that all host addresses are available. You can exclude subsets of the address space by using the IP Service > DHCP > Server (Configure Excluded Addresses – Add) page.

PARAMETERS

These parameters are displayed:

Creating a New Address Pool

- **Pool Name** – A string or integer. (Range: 1-8 characters)

- **Type** – Sets the address pool type to Network or Host.

Setting Parameters for a Network Pool

- **IP** – The IP address of the DHCP address pool.

- **Subnet Mask** – The bit combination that identifies the network (or subnet) and the host portion of the DHCP address pool.

Setting Parameters for a Static Host

- **IP** – The IP address to assign to the host.
- **Subnet Mask** – Specifies the network mask of the client.
- **Client-Identifier** – A unique designation for the client device, either a text string (1-15 characters) or hexadecimal value. The information included in the identifier is based on RFC 2132 Option 60, and must be unique for all clients in the same administrative domain.
- **Hardware Address** – Specifies the MAC address and protocol used on the client. (Options: Ethernet, IEEE802, FDDI, None; Default: Ethernet)

Setting Optional Parameters

- **Default Router** – The IP address of the primary and alternate gateway router. The IP address of the router should be on the same subnet as the client.
- **DNS Server** – The IP address of the primary and alternate DNS server. DNS servers must be configured for a DHCP client to map host names to IP addresses.
- **Netbios Server** – IP address of the primary and alternate NetBIOS Windows Internet Naming Service (WINS) name server used for Microsoft DHCP clients.
- **Netbios Type** – NetBIOS node type for Microsoft DHCP clients. (Options: Broadcast, Hybrid, Mixed, Peer to Peer; Default: Hybrid)
- **Domain Name** – The domain name of the client. (Range: 1-128 characters)
- **Bootfile** – The default boot image for a DHCP client. This file should placed on the Trivial File Transfer Protocol (TFTP) server specified as the Next Server.
- **Next Server** – The IP address of the next server in the boot process, which is typically a Trivial File Transfer Protocol (TFTP) server.
- **Lease Time** – The duration that an IP address is assigned to a DHCP client. (Options: Finite, Infinite; Default: Infinite)

WEB INTERFACE

To configure DHCP address pools:

1. Click IP Service, DHCP, Server.
2. Select Configure Pool from the Step list.

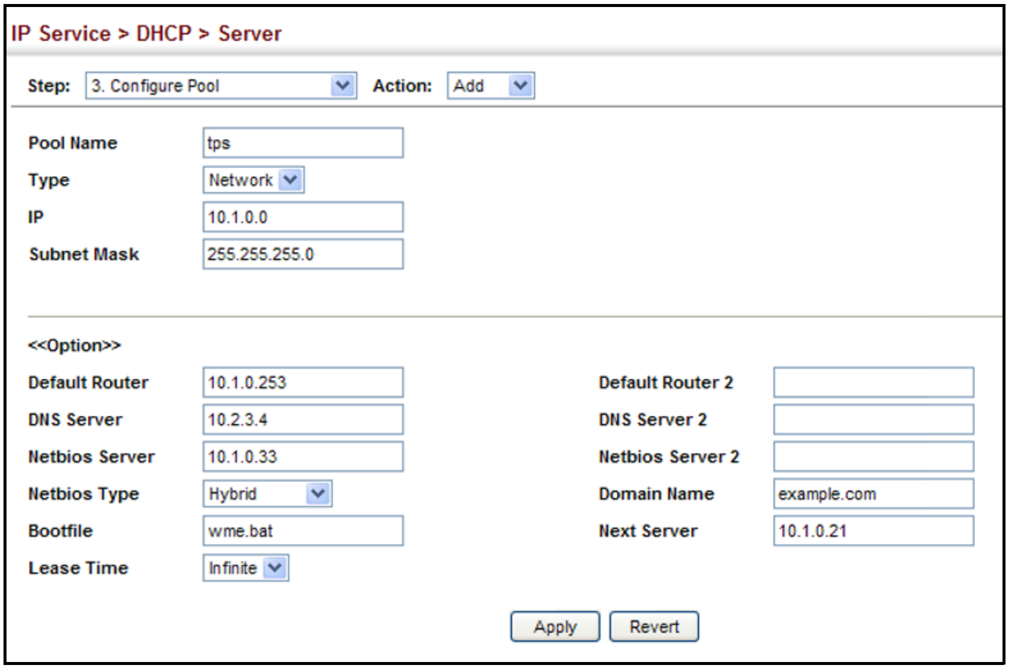
3. Select Add from the Action list.

4. Set the pool Type to Network or Host.

5. Enter the IP address and subnet mask for a network pool or host. If configuring a static binding for a host, enter the client identifier or hardware address for the host device. Configure the optional parameters such as a gateway server and DNS server.

6. Click Apply.

Figure 430: Configuring DHCP Server Address Pools (Network)



IP Service > DHCP > Server

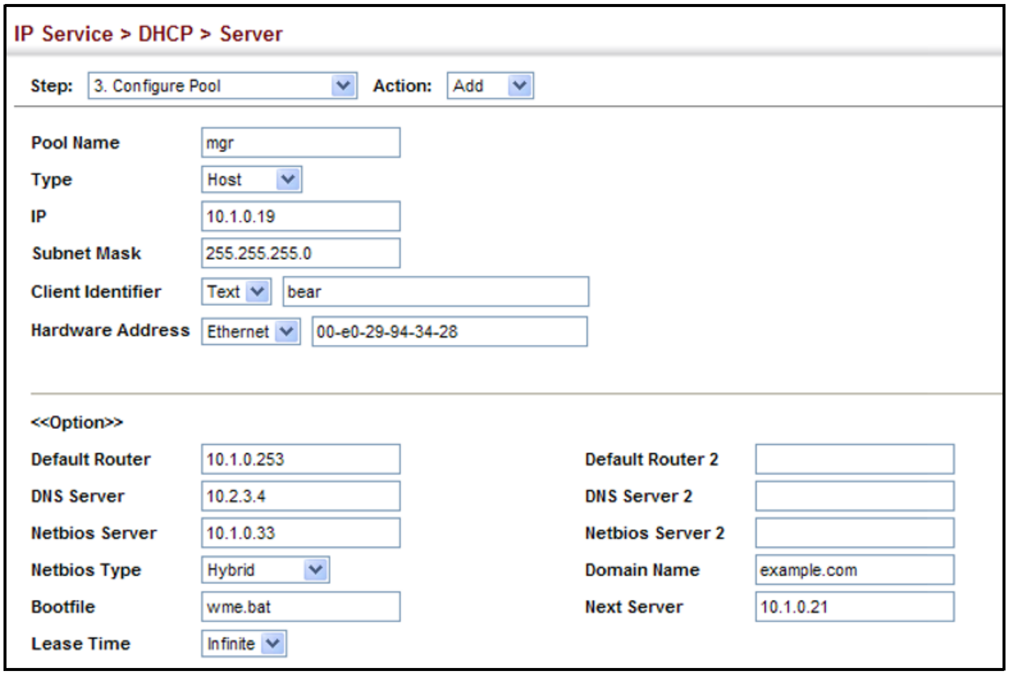
Step: 3. Configure Pool Action: Add

Pool Name	tps
Type	Network
IP	10.1.0.0
Subnet Mask	255.255.255.0

<<Option>>

Default Router	10.1.0.253	Default Router 2	
DNS Server	10.2.3.4	DNS Server 2	
Netbios Server	10.1.0.33	Netbios Server 2	
Netbios Type	Hybrid	Domain Name	example.com
Bootfile	wme.bat	Next Server	10.1.0.21
Lease Time	Infinite		

Figure 431: Configuring DHCP Server Address Pools (Host)



IP Service > DHCP > Server

Step: 3. Configure Pool Action: Add

Pool Name: mgr
Type: Host
IP: 10.1.0.19
Subnet Mask: 255.255.255.0
Client Identifier: Text bear
Hardware Address: Ethernet 00-e0-29-94-34-28

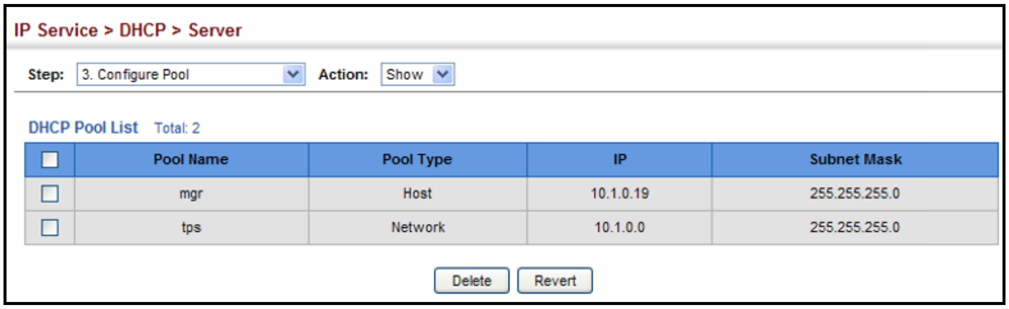
<<Option>>

Default Router: 10.1.0.253
DNS Server: 10.2.3.4
Netbios Server: 10.1.0.33
Netbios Type: Hybrid
Bootfile: wme.bat
Lease Time: Infinite
Default Router 2:
DNS Server 2:
Netbios Server 2:
Domain Name: example.com
Next Server: 10.1.0.21

To show the configured DHCP address pools:

1. Click IP Service, DHCP, Server.
2. Select Configure Pool from the Step list.
3. Select Show from the Action list.

Figure 432: Showing Configured DHCP Server Address Pools



IP Service > DHCP > Server

Step: 3. Configure Pool Action: Show

DHCP Pool List Total: 2

□	Pool Name	Pool Type	IP	Subnet Mask
□	mgr	Host	10.1.0.19	255.255.255.0
□	tps	Network	10.1.0.0	255.255.255.0

DISPLAYING ADDRESS BINDINGS

Use the IP Service > DHCP > Server (Show IP Binding) page display the host devices which have acquired an IP address from this switch's DHCP server.

CLI REFERENCES

- "show ip dhcp binding" on page 1644

PARAMETERS

These parameters are displayed:

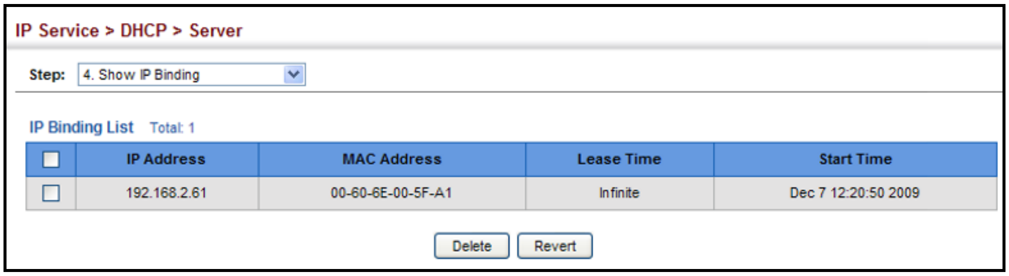
- **IP Address** – IP address assigned to host.
- **MAC Address** – MAC address of host.
- **Lease Time** – Duration that this IP address can be used by the host.
- **Start Time** – Time this address was assigned by the switch.

WEB INTERFACE

To show the addresses assigned to DHCP clients:

1. Click IP Service, DHCP, Server.
2. Select Show IP Binding from the Step list.

Figure 433: Shows Addresses Assigned by the DHCP Server



IP Service > DHCP > Server

Step: 4. Show IP Binding

IP Binding List Total: 1

□	IP Address	MAC Address	Lease Time	Start Time
□	192.168.2.61	00-60-6E-00-5F-A1	Infinite	Dec 7 12:20:50 2009

FORWARDING UDP SERVICE REQUESTS

This section describes how this switch can forward UDP broadcast packets originating from host applications to another part of the network when an local application server is not available.

COMMAND USAGE

- Network hosts occasionally use UDP broadcasts to determine information such as address configuration, and domain name mapping. These broadcasts are confined to the local subnet, either as an all hosts broadcast (all ones broadcast - 255.255.255.255), or a directed subnet broadcast (such as 10.10.10.255). To reduce the number of application servers deployed in a multi-segment network, UDP helper can be used to forward broadcast packets for specified UDP application ports to remote servers located in another network segment.

- To configure UDP helper, enable it globally (see "Configuring General DNS Service Parameters" on page 713), specify the UDP destination ports for which broadcast traffic will be forwarded (see "Specifying UDP Destination Ports" on page 731), and specify the remote application servers or the subnet where the servers are located (see "Specifying The Target Server or Subnet" on page 733).

ENABLING THE UDP HELPER

Use the IP Service > UDP Helper > General page to enable the UDP helper globally on the switch.

CLI REFERENCES

- "ip helper" on page 1660

PARAMETERS

These parameters are displayed:

- **UDP Helper Status** – Enables or disables the UDP helper. (Default: Disabled)

WEB INTERFACE

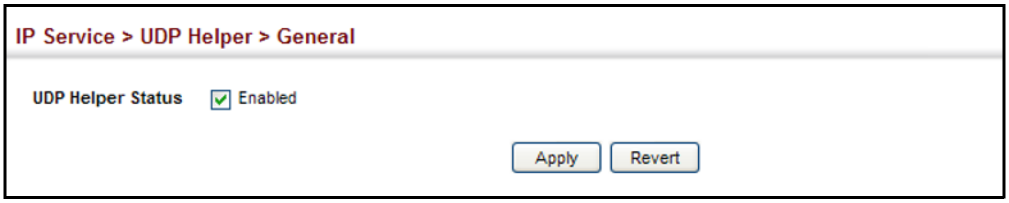
To enable the UDP help:

1. Click IP Service, UDP Helper, General.

2. Mark the Enabled check box.

3. Click Apply.

Figure 434: Enabling the UDP Helper



IP Service > UDP Helper > General

UDP Helper Status ☑ Enabled

SPECIFYING UDP DESTINATION PORTS

Use the IP Service > UDP Helper > Forwarding page to specify the UDP destination ports for which broadcast traffic will be forwarded when the UDP helper is enabled.

CLI REFERENCES

- "ip forward-protocol udp" on page 1659

COMMAND USAGE

- Up to 100 UDP ports can be specified with this command for forwarding to one or more remote servers.

PARAMETERS

These parameters are displayed:

- **Destination UDP Port** – UDP application port for which UDP service requests are forwarded. (Range: 1-65535)

  The following UDP ports are included in the forwarding list when the UDP helper is enabled, and a remote server address is configured:

BOOTP client	port 67
BOOTP server	port 68
Domain Name Service	port 53
IEN-116 Name Service	port 42
NetBIOS Datagram Server	port 138
NetBIOS Name Server	port 137
NTP	port 37
TACACS service	port 49
TFTP	port 69

WEB INTERFACE

To specify UDP destination ports for forwarding:

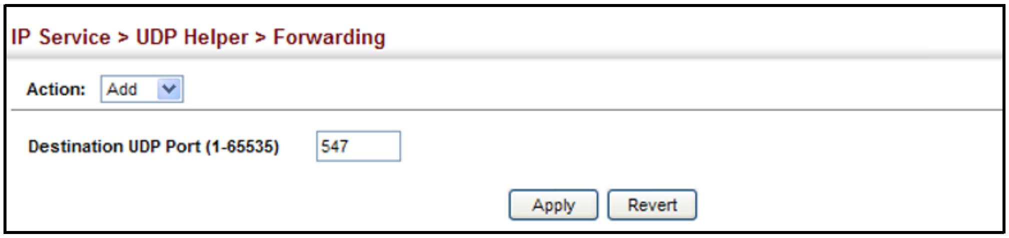
1. Click IP Service, UDP Helper, Forwarding.

2. Select Add from the Action list.

3. Enter a destination UDP port number for which service requests are to be forwarded to a remote application server.

4. Click Apply.

Figure 435: Specifying UDP Destination Ports



IP Service > UDP Helper > Forwarding

Action: Add

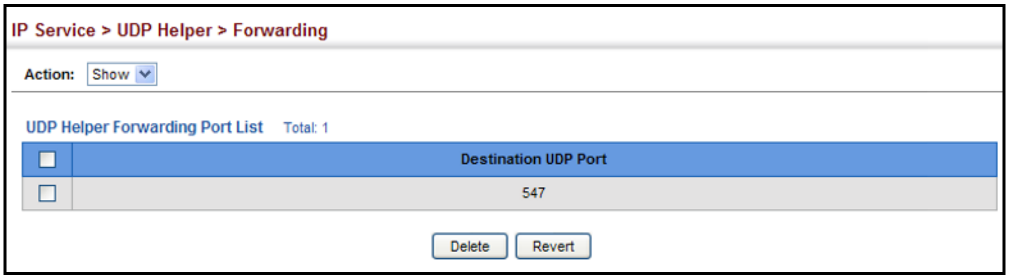
Destination UDP Port (1-65535) 547

To show the configured UDP destination ports:

1. Click IP Service, UDP Helper, Forwarding.

2. Select Show from the Action list.

Figure 436: Showing the UDP Destination Ports



IP Service > UDP Helper > Forwarding

Action: Show

UDP Helper Forwarding Port List Total: 1

□	Destination UDP Port
□	547

SPECIFYING THE TARGET SERVER OR SUBNET

Use the IP Service > UDP Helper > Address page to specify the application server or subnet (indicated by a directed broadcast address) to which designated UDP broadcast packets are forwarded.

CLI REFERENCES

- "ip helper-address" on page 1661

COMMAND USAGE

- Up to 20 helper addresses can be specified.
- To forward UDP packets with the UDP helper, the clients must be connected to the selected interface, and the interface configured with an IP address.
- The UDP packets to be forwarded must be specified in the IP Service > UDP Helper > Forwarding page, and the packets meet the following criteria:
  - The MAC address of the received frame must be the all-ones broadcast address (ffff.ffff.ffff).
  - The IP destination address must be one of the following:
    - all-ones broadcast (255.255.255.255)
    - subnet broadcast for the receiving interface
  - The IP time-to-live (TTL) value must be at least 2.
  - The IP protocol must be UDP (17).
  - The UDP destination port must be TFTP, Domain Name System (DNS), Time, NetBIOS, BOOTP or DHCP packet, or a UDP port specified on the IP Service > UDP Helper > Forwarding page.
- If a helper address is specified on this configuration page, but no UDP ports have been specified on the IP Service > UDP Helper > Forwarding page, broadcast traffic for several UDP protocol types will be forwarded by default as described on page 731.

PARAMETERS

These parameters are displayed:

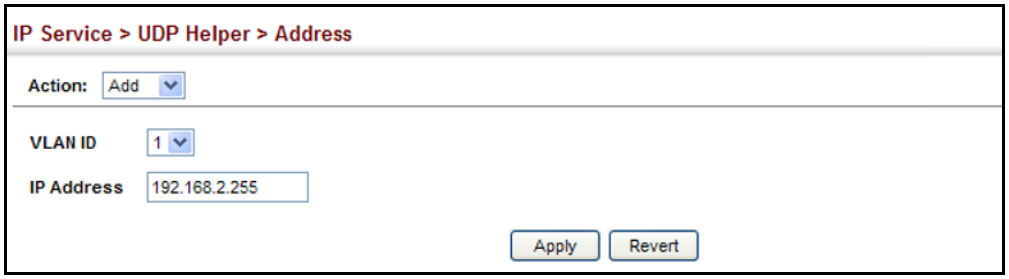
- **VLAN ID** – VLAN identifier (Range: 1-4094)
- **IP Address** – Host address or directed broadcast address to which UDP broadcast packets are forwarded. (Range: 1-65535)

WEB INTERFACE

To specify the target server or subnet for forwarding UDP request packets:

1. Click IP Service, UDP Helper, Address.
2. Select Add from the Action list.
3. Enter the address of the remote server or subnet where UDP request packets are to be forwarded.
4. Click Apply.

Figure 437: Specifying the Target Server or Subnet for UDP Requests



IP Service > UDP Helper > Address

Action: Add

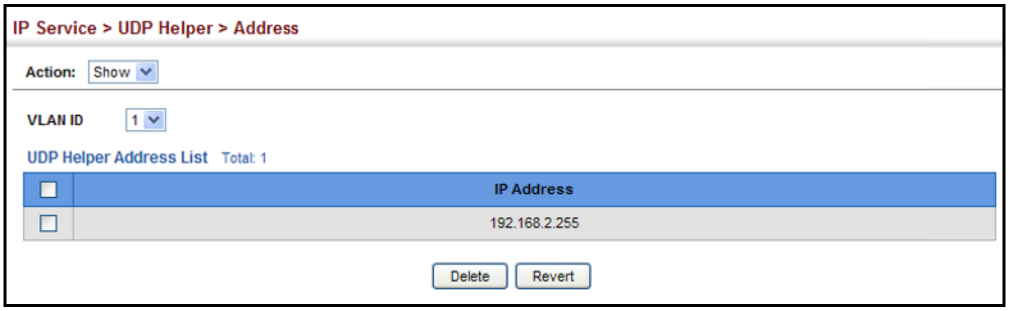
VLAN ID: 1

IP Address: 192.168.2.255

To show the target server or subnet for UDP requests:

1. Click IP Service, UDP Helper, Address.
2. Select Show from the Action list.

Figure 438: Showing the Target Server or Subnet for UDP Requests



IP Service > UDP Helper > Address

Action: Show

VLAN ID: 1

UDP Helper Address List Total: 1

□	IP Address
□	192.168.2.255

CONFIGURING THE PPPOE INTERMEDIATE AGENT

This section describes how to configure the PPPoE Intermediate Agent (PPPoE IA) relay parameters required for passing authentication messages between a client and broadband remote access servers.

CONFIGURING PPPOE IA GLOBAL SETTINGS

Use the IP Service > PPPoE Intermediate Agent (Configure Global) page to enable the PPPoE IA on the switch, set the access node identifier, and set the generic error message.

CLI REFERENCES

- "pppoe intermediate-agent" on page 1081
- "pppoe intermediate-agent port-format-type" on page 1083
- "show pppoe intermediate-agent info" on page 1086

COMMAND USAGE

When PPPoE IA is enabled, the switch inserts a tag identifying itself as a PPPoE IA residing between the attached client requesting network access and the ports connected to broadband remote access servers (BRAS). The switch extracts access-loop information from the client's PPPoE Active Discovery Request, and forwards this information to all trusted ports (designated on the Configure Interface page). The BRAS detects the presence of the subscriber's circuit-ID tag inserted by the switch during the PPPoE discovery phase, and sends this tag as a NAS-port-ID attribute in PPP authentication and AAA accounting requests to a RADIUS server.

PARAMETERS

These parameters are displayed:

- **PPPoE IA Global Status** – Enables the PPPoE Intermediate Agent globally on the switch. (Default: Disabled)

  Note that PPPoE IA must be enabled globally before it can be enabled on an interface.

- **Access Node Identifier** – String identifying this switch as an PPPoE IA to the PPPoE server. (Range: 1-48 ASCII characters: Default: IP address of first IPv4 interface on the switch.)

  The switch uses the access-node-identifier to generate the circuit-id for PPPoE discovery stage packets sent to the BRAS, but does not modify the source or destination MAC address of these PPPoE discovery packets. These messages are forwarded to all trusted ports designated on the Configure Interface page.

- **Operational Access Node Identifier** – The configured access node identifier.

- **Generic Error Message** – An error message notifying the sender that the PPPoE Discovery packet was too large. (Range: 0-127; Default: PPPoE Discover packet too large to process. Try reducing the number of tags added.)

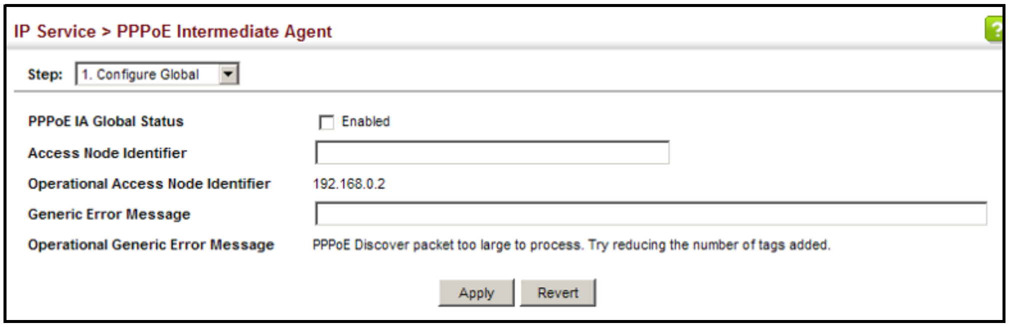
- **Operational Generic Error Message** – The configured generic error message.

WEB INTERFACE

To configure global settings for PPPoE IA:

1. Click IP Service, PPPoE Intermediate Agent.
2. Select Configure Global from the Step list.
3. Enable the PPPoE IA on the switch, set the access node identifier, and set the generic error message.
4. Click Apply.

Figure 439: Configuring Global Settings for PPPoE Intermediate Agent



Step: 1. Configure Global

PPPoE IA Global Status □ Enabled

Access Node Identifier

Operational Access Node Identifier 192.168.0.2

Generic Error Message

Operational Generic Error Message PPPoE Discover packet too large to process. Try reducing the number of tags added.

CONFIGURING PPPOE IA INTERFACE SETTINGS

Use the IP Service > PPPoE Intermediate Agent (Configure Interface) page to enable PPPoE IA on an interface, set trust status, enable vendor tag stripping, and set the circuit ID and remote ID.

CLI REFERENCES

- "PPPoE Intermediate Agent" on page 1081

PARAMETERS

These parameters are displayed:

- **Interface** – Port or trunk selection.
- **PPPoE IA Status** – Enables the PPPoE IA on an interface. (Default: Disabled)

  Note that PPPoE IA must also be enabled globally on the switch for this command to take effect.
- **Trust Status** – Sets an interface to trusted mode to indicate that it is connected to a PPPoE server. (Default: Disabled)
  - Set any interfaces connecting the switch to a PPPoE Server as trusted. Interfaces that connect the switch to users (PPPoE clients) should be set as untrusted.

- At least one trusted interface must be configured on the switch for the PPPoE IA to function.

- **Vendor Tag Strip** – Enables the stripping of vendor tags from PPPoE Discovery packets sent from a PPPoE server. (Default: Disabled)

  This parameter only applies to trusted interfaces. It is used to strip off vendor-specific tags (which carry subscriber and line identification information) in PPPoE Discovery packets received from an upstream PPPoE server before forwarding them to a user.

- **Circuit ID** – String identifying the circuit identifier (or interface) on this switch to which the user is connected. (Range: 1-10 ASCII characters; Default: Unit/Port:VLAN-ID, or 0/Trunk-ID:VLAN-ID)

  - The PPPoE server extracts the Line-ID tag from PPPoE discovery stage messages, and uses the Circuit-ID field of that tag as a NAS-Port-ID attribute in AAA access and accounting requests.
  - The switch intercepts PPPoE discovery frames from the client and inserts a unique line identifier using the PPPoE Vendor-Specific tag (0x0105) to PPPoE Active Discovery Initiation (PADI) and Request (PADR) packets. The switch then forwards these packets to the PPPoE server. The tag contains the Line-ID of the customer line over which the discovery packet was received, entering the switch (or access node) where the intermediate agent resides.
  - Outgoing PAD Offer (PADO) and Session-confirmation (PADS) packets sent from the PPPoE Server include the Circuit-ID tag inserted by the switch, and should be stripped out of PADO and PADS packets which are to be passed directly to end-node clients.

- **Operational Circuit ID** – The configured circuit identifier.

- **Remote ID** – String identifying the remote identifier (or interface) on this switch to which the user is connected. (Range: 1-63 ASCII characters; Default: Port MAC address)

- **Operational Remote ID** – The configured circuit identifier.

WEB INTERFACE

To configure interface settings for PPPoE IA:

1. Click IP Service, PPPoE Intermediate Agent.

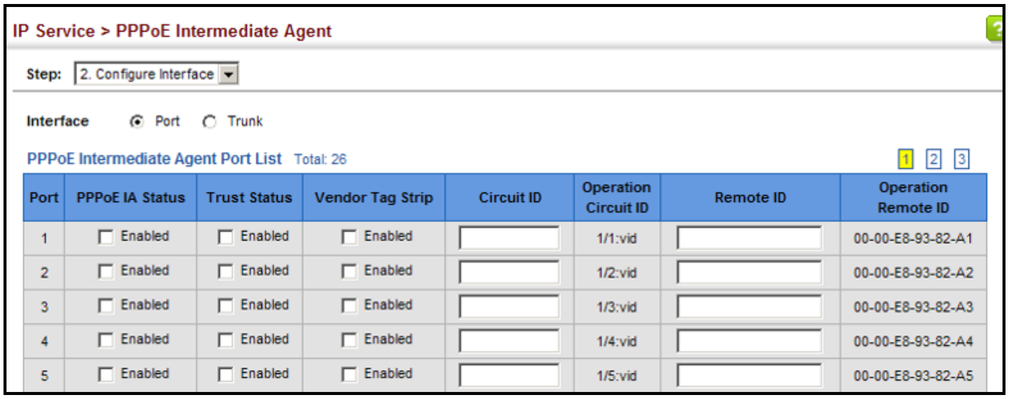
2. Select Configure Interface from the Step list.

3. Select Port or Trunk interface type.

4. Enable PPPoE IA on an interface, set trust status, enable vendor tag stripping if required, and set the circuit ID and remote ID.

5. Click Apply.

Figure 440: Configuring Interface Settings for PPPoE Intermediate Agent



IP Service > PPPoE Intermediate Agent

Step: 2. Configure Interface

Interface ● Port ○ Trunk

PPPoE Intermediate Agent Port List Total: 26

Port	PPPoE IA Status	Trust Status	Vendor Tag Strip	Circuit ID	Operation Circuit ID	Remote ID	Operation Remote ID
1	□ Enabled	□ Enabled	□ Enabled		1/1:vid		00-00-E8-93-82-A1
2	□ Enabled	□ Enabled	□ Enabled		1/2:vid		00-00-E8-93-82-A2
3	□ Enabled	□ Enabled	□ Enabled		1/3:vid		00-00-E8-93-82-A3
4	□ Enabled	□ Enabled	□ Enabled		1/4:vid		00-00-E8-93-82-A4
5	□ Enabled	□ Enabled	□ Enabled		1/5:vid		00-00-E8-93-82-A5

SHOWING PPPOE IA STATISTICS

Use the IP Service > PPPoE Intermediate Agent (Show Statistics) page to show statistics on PPPoE IA protocol messages.

CLI REFERENCES

- "show pppoe intermediate-agent statistics" on page 1087

PARAMETERS

These parameters are displayed:

- **Interface** – Port or trunk selection.
- **Received** – Received PPPoE active discovery messages.
  - **All** – All PPPoE active discovery message types.
  - **PADI** – PPPoE Active Discovery Initiation messages.
  - **PADO** – PPPoE Active Discovery Offer messages.
  - **PADR** – PPPoE Active Discovery Request messages.
  - **PADS** – PPPoE Active Discovery Session-Confirmation messages.
  - **PADT** – PPPoE Active Discovery Terminate messages.
- **Dropped** – Dropped PPPoE active discovery messages.
  - **Response from untrusted** – Response from an interface which not been configured as trusted.
  - **Request towards untrusted** – Request sent to an interface which not been configured as trusted.
  - **Malformed** – Corrupted PPPoE message.

WEB INTERFACE

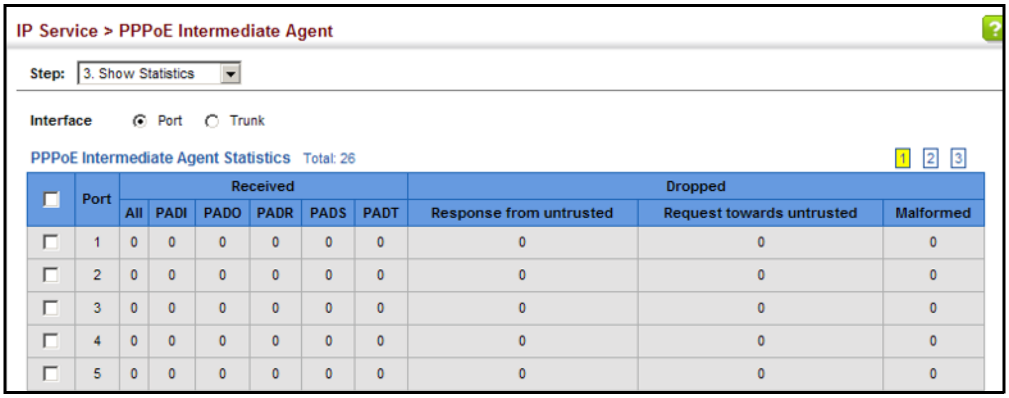
To show statistics for PPPoE IA protocol messages:

1. Click IP Service, PPPoE Intermediate Agent.

2. Select Show Statistics from the Step list.

3. Select Port or Trunk interface type.

Figure 441: Showing PPPoE Intermediate Agent Statistics



IP Service > PPPoE Intermediate Agent

Step: 3. Show Statistics

Interface ● Port ○ Trunk

PPPoE Intermediate Agent Statistics Total: 26

□	Port	Received						Dropped		
		All	PADI	PADO	PADR	PADS	PADT	Response from untrusted	Request towards untrusted	Malformed
□	1	0	0	0	0	0	0	0	0	0
□	2	0	0	0	0	0	0	0	0	0
□	3	0	0	0	0	0	0	0	0	0
□	4	0	0	0	0	0	0	0	0	0
□	5	0	0	0	0	0	0	0	0	0

18 General IP Routing

This chapter provides information on network functions including:

- Ping – Sends ping message to another node on the network.
- Trace – Sends ICMP echo request packets to another node on the network.
- Address Resolution Protocol – Describes how to configure ARP aging time, proxy ARP, or static addresses. Also shows how to display dynamic entries in the ARP cache.
- Static Routes – Configures static routes to other network segments.
- Routing Table – Displays routing entries learned through dynamic routing and statically configured entries.
- Equal-cost Multipath Routing – Configures the maximum number of equal-cost paths that can transmit traffic to the same destination

Overview

This switch supports IP routing and routing path management via static routing definitions (page 753) and dynamic routing protocols such as RIP, OSPFv2, OSPv3[13], or BGPv4[13]. When IP routing is functioning, this switch acts as a wire-speed router, passing traffic between VLANs with different IP interfaces, and routing traffic to external IP networks. However, when the switch is first booted, default routing can only forward traffic between local IP interfaces. As with all traditional routers, static and dynamic routing functions must first be configured to work.

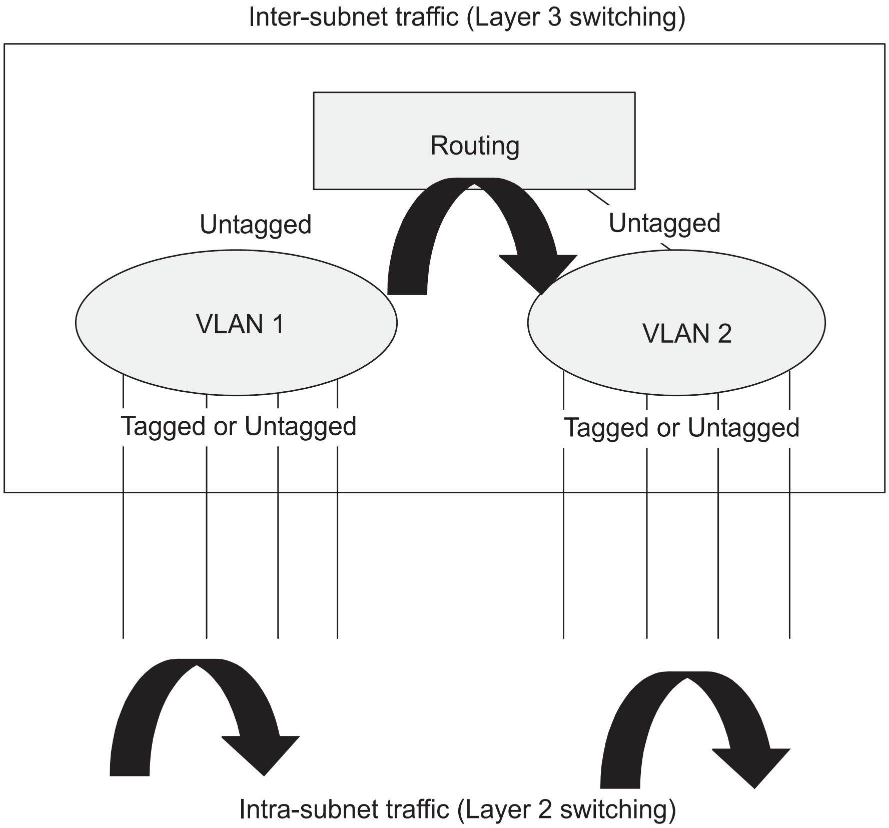
Initial Configuration

By default, all ports belong to the same VLAN and the switch provides only Layer 2 functionality. To segment the attached network, first create VLANs for each unique user group or application traffic (page 228), assign all ports that belong to the same group to these VLANs (page 231), and then assign an IP interface to each VLAN (page 691 or page 695). By separating the network into different VLANs, it can be partitioned into subnetworks that are disconnected at Layer 2. Network traffic within the same subnet is still switched using Layer 2 switching. And the VLANs can now be interconnected (as required) with Layer 3 switching.

[13] Refer to the *Command Reference Guide* for information on configuring these protocols.

Each VLAN represents a virtual interface to Layer 3. You just need to provide the network address for each virtual interface, and the traffic between different subnetworks will be routed by Layer 3 switching.

Figure 442: Virtual Interfaces and Layer 3 Routing


Inter-subnet traffic (Layer 3 switching)
Routing
Untagged
Untagged
VLAN 1
VLAN 2
Tagged or Untagged
Tagged or Untagged
Intra-subnet traffic (Layer 2 switching)

IP ROUTING AND SWITCHING

IP Switching (or packet forwarding) encompasses tasks required to forward packets for both Layer 2 and Layer 3, as well as traditional routing. These functions include:

- Layer 2 forwarding (switching) based on the Layer 2 destination MAC address
- Layer 3 forwarding (routing):
  - Based on the Layer 3 destination address
  - Replacing destination/source MAC addresses for each hop
  - Incrementing the hop count
  - Decrementing the time-to-live
  - Verifying and recalculating the Layer 3 checksum

If the destination node is on the same subnetwork as the source network, then the packet can be transmitted directly without the help of a router. However, if the MAC address is not yet known to the switch, an Address Resolution Protocol (ARP) packet with the destination IP address is broadcast to get the destination MAC address from the destination node. The IP packet can then be sent directly with the destination MAC address.

If the destination belongs to a different subnet on this switch, the packet can be routed directly to the destination node. However, if the packet belongs to a subnet not included on this switch, then the packet should be sent to the next hop router (with the MAC address of the router itself used as the destination MAC address, and the destination IP address of the destination node). The router will then forward the packet to the destination node through the correct path. The router can also use the ARP protocol to find out the MAC address of the destination node of the next router as necessary.

NOTE: In order to perform IP switching, the switch should be recognized by other network nodes as an IP router, either by setting it as the default gateway or by redirection from another router via the ICMP process.

When the switch receives an IP packet addressed to its own MAC address, the packet follows the Layer 3 routing process. The destination IP address is checked against the Layer 3 address table. If the address is not already there, the switch broadcasts an ARP packet to all the ports on the destination VLAN to find out the destination MAC address. After the MAC address is discovered, the packet is reformatted and sent out to the destination. The reformat process includes decreasing the Time-To-Live (TTL) field of the IP header, recalculating the IP header checksum, and replacing the destination MAC address with either the MAC address of the destination node or that of the next hop router.

When another packet destined to the same node arrives, the destination MAC can be retrieved directly from the Layer 3 address table; the packet is then reformatted and sent out the destination port. IP switching can be done at wire-speed when the destination address entry is already in the Layer 3 address table.

If the switch determines that a frame must be routed, the route is calculated only during setup. Once the route has been determined, all packets in the current flow are simply switched or forwarded across the chosen path. This takes advantage of the high throughput and low latency of switching by enabling the traffic to bypass the routing engine once the path calculation has been performed.

ROUTING PATH MANAGEMENT

Routing Path Management involves the determination and updating of all the routing information required for packet forwarding, including:

- Handling routing protocols
- Updating the routing table
- Updating the Layer 3 switching database

ROUTING PROTOCOLS

The switch supports both static and dynamic routing.

- Static routing requires routing information to be stored in the switch either manually or when a connection is set up by an application outside the switch.
- Dynamic routing uses a routing protocol to exchange routing information, calculate routing tables, and respond to changes in the status or loading of the network.

CONFIGURING IP ROUTING INTERFACES

CONFIGURING LOCAL AND REMOTE INTERFACES

Use the IP > General > Routing Interface (Add Address) page to configure routing interfaces for directly connected IPv4 subnets (see "Setting the Switch’s IP Address (IP Version 4)" on page 691. Or use the IP > IPv6 Configuration pages to configure routing interfaces for directly connected IPv6 subnets (see "Setting the Switch’s IP Address (IP Version 6)" on page 695).

If this router is directly connected to end node devices (or connected to end nodes through shared media) that will be assigned to a specific subnet, then you must create a router interface for each VLAN that will support routing. The router interface consists of an IP address and subnet mask. This interface address defines both the network prefix number to which the router interface is attached and the router’s host number on that network. In other words, a router interface address defines the network segment that is connected to that interface, and allows you to send IP packets to or from the router.

You can specify the IP subnets connected directly to this router by manually assigning an IP address to each VLAN, or using BOOTP or DHCP to dynamically assign an address. To specify IP subnets not directly connected to this router, you can either configure static routes (see page 753), or use RIP, OSPFv2, OSPFv3[13], or BGPv4[13] or dynamic routing protocols to identify routes that lead to other interfaces by exchanging protocol messages with other routers on the network.

Once IP interfaces have been configured, the switch functions as a multilayer routing switch, operating at either Layer 2 or 3 as required. All IP packets are routed directly between local interfaces, or indirectly to remote interfaces using either static or dynamic routing. All other packets for non-IP protocols (for example, NetBuei, NetWare or AppleTalk) are switched based on MAC addresses).

To route traffic between remote IP interfaces, the switch should be recognized by other network nodes as an IP router, either by setting it to advertise itself as the default gateway or by redirection from another router via the ICMP process used by various routing protocols.

If the switch is configured to advertise itself as the default gateway, a routing protocol must still be used to determine the next hop router for any unknown destinations, i.e., packets that do not match any routing table entry. If another router is designated as the default gateway, then the switch will pass packets to this router for any unknown hosts or subnets.

To configure a default gateway for IPv4, use the static routing table as described on page 753, enter 0.0.0.0 for the IP address and subnet mask, and then specify this switch itself or another router as the gateway. To configure a gateway for IPv6, see "Configuring the IPv6 Default Gateway" on page 696.

USING THE PING FUNCTION

Use the IP > General > Ping page to send ICMP echo request packets to another node on the network.

CLI REFERENCES

- "ping" on page 1654

PARAMETERS

These parameters are displayed:

- **Host Name/IP Address** – IPv4/IPv6 address or alias of the host.
- **Probe Count** – Number of packets to send. (Range: 1-16)
- **Packet Size** – Number of bytes in a packet. (Range: 32-1472 bytes for IPv4, 0-512 bytes for IPv6)

  The actual packet size will be eight bytes larger than the size specified because the switch adds header information.

COMMAND USAGE

- Use the ping command to see if another site on the network can be reached.
- The following are some results of the **ping** command:
  - *Normal response* - The normal response occurs in one to ten seconds, depending on network traffic.
  - *Destination does not respond* - If the host does not respond, a “timeout” appears in ten seconds.
  - *Destination unreachable* - The gateway for this destination indicates that the destination is unreachable.
  - *Network or host unreachable* - The gateway found no corresponding entry in the route table.
- The same link-local address may be used by different interfaces/nodes in different zones (RFC 4007). Therefore, when specifying a link-local address, include zone-id information indicating the VLAN identifier after

the % delimiter. For example, FE80::7272%1 identifies VLAN 1 as the interface.

WEB INTERFACE

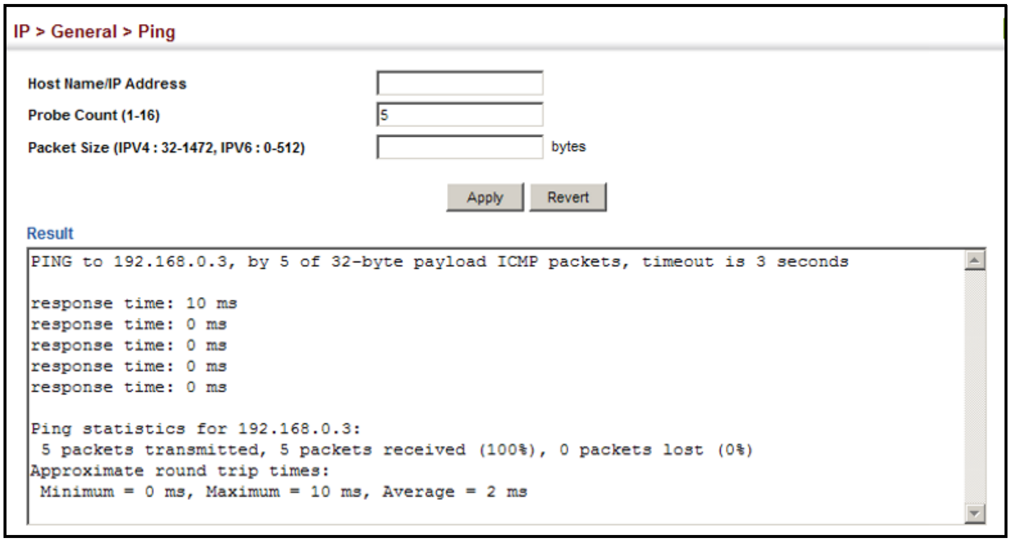
To ping another device on the network:

1. Click IP, General, Ping.

2. Specify the target device and ping parameters.

3. Click Apply.

Figure 443: Pinging a Network Device



IP > General > Ping

Host Name/IP Address

Probe Count (1-16): 5

Packet Size (IPV4 : 32-1472, IPV6 : 0-512) bytes

Result

```
PING to 192.168.0.3, by 5 of 32-byte payload ICMP packets, timeout is 3 seconds

response time: 10 ms
response time: 0 ms
response time: 0 ms
response time: 0 ms
response time: 0 ms

Ping statistics for 192.168.0.3:
 5 packets transmitted, 5 packets received (100%), 0 packets lost (0%)
Approximate round trip times:
 Minimum = 0 ms, Maximum = 10 ms, Average = 2 ms
```

USING THE TRACE ROUTE FUNCTION

Use the IP > General > Trace Route page to show the route packets take to the specified destination.

CLI REFERENCES

- "traceroute" on page 1653

PARAMETERS

These parameters are displayed:

- **Destination IP Address** – IPv4/IPv6 address of the host.

- **IPv4 Max Failures** – The maximum number of failures before which the trace route is terminated. (Fixed: 5)

- **IPv6 Max Failures** – The maximum number of failures before which the trace route is terminated. (Range: 1-255; Default: 5)

COMMAND USAGE

- Use the trace route function to determine the path taken to reach a specified destination.

- A trace terminates when the destination responds, when the maximum timeout (TTL) is exceeded, or the maximum number of hops is exceeded.

- The trace route function first sends probe datagrams with the TTL value set at one. This causes the first router to discard the datagram and return an error message. The trace function then sends several probe messages at each subsequent TTL level and displays the round-trip time for each message. Not all devices respond correctly to probes by returning an "ICMP port unreachable" message. If the timer goes off before a response is returned, the trace function prints a series of asterisks and the "Request Timed Out" message. A long sequence of these messages, terminating only when the maximum timeout has been reached, may indicate this problem with the target device.

- The same link-local address may be used by different interfaces/nodes in different zones (RFC 4007). Therefore, when specifying a link-local address, include zone-id information indicating the VLAN identifier after the % delimiter. For example, FE80::7272%1 identifies VLAN 1 as the interface.

WEB INTERFACE

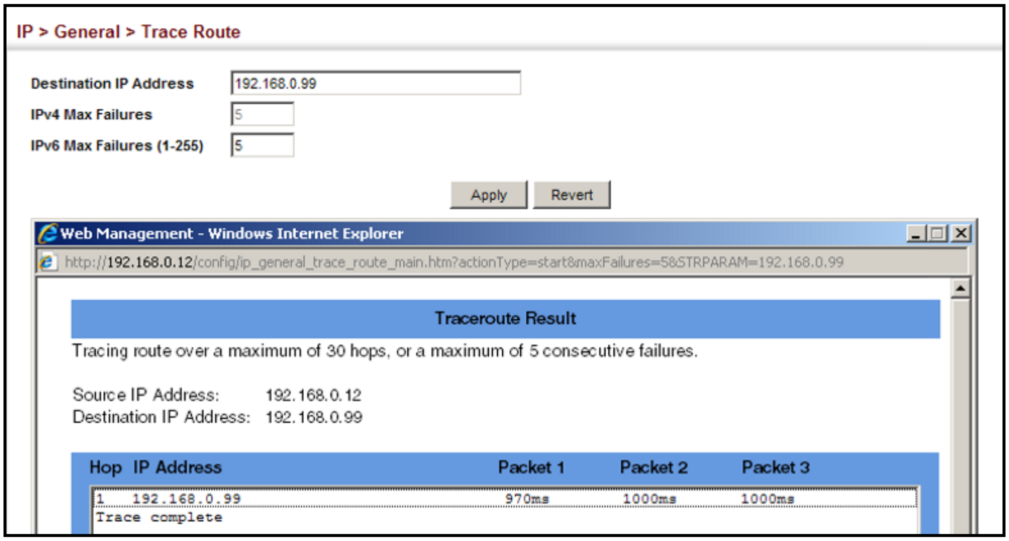
To trace the route to another device on the network:

1. Click IP, General, Trace Route.

2. Specify the target device.

3. Click Apply.

Figure 444: Tracing the Route to a Network Device



IP > General > Trace Route

Destination IP Address: 192.168.0.99
IPv4 Max Failures: 5
IPv6 Max Failures (1-255): 5

http://192.168.0.12/config/ip_general_trace_route_main.htm?actionType=start&maxFailures=5&STRPARAM=192.168.0.99

Traceroute Result

Tracing route over a maximum of 30 hops, or a maximum of 5 consecutive failures.

Source IP Address: 192.168.0.12
Destination IP Address: 192.168.0.99

Hop	IP Address	Packet 1	Packet 2	Packet 3
1	192.168.0.99	970ms	1000ms	1000ms

```
Trace complete
```

ADDRESS RESOLUTION PROTOCOL

If IP routing is enabled (page 769), the router uses its routing tables to make routing decisions, and uses Address Resolution Protocol (ARP) to forward traffic from one hop to the next. ARP is used to map an IP address to a physical layer (i.e., MAC) address. When an IP frame is received by this router (or any standards-based router), it first looks up the MAC address corresponding to the destination IP address in the ARP cache. If the address is found, the router writes the MAC address into the appropriate field in the frame header, and forwards the frame on to the next hop. IP traffic passes along the path to its final destination in this way, with each routing device mapping the destination IP address to the MAC address of the next hop toward the recipient, until the packet is delivered to the final destination.

If there is no entry for an IP address in the ARP cache, the router will broadcast an ARP request packet to all devices on the network. The ARP request contains the following fields similar to that shown in this example:

Table 50: Address Resolution Protocol

destination IP address	10.1.0.19
destination MAC address	?
source IP address	10.1.0.253
source MAC address	00-00-ab-cd-00-00

When devices receive this request, they discard it if their address does not match the destination IP address in the message. However, if it does match, they write their own hardware address into the destination MAC address field and send the message back to the source hardware address. When the source device receives a reply, it writes the destination IP address and corresponding MAC address into its cache, and forwards the IP traffic on to the next hop. As long as this entry has not timed out, the router will be able forward traffic directly to the next hop for this destination without having to broadcast another ARP request.

Also, if the switch receives a request for its own IP address, it will send back a response, and also cache the MAC of the source device's IP address.

BASIC ARP CONFIGURATION

Use the IP > ARP (Configure General) page to specify the timeout for ARP cache entries, or to enable Proxy ARP for specific VLAN interfaces.

CLI REFERENCES

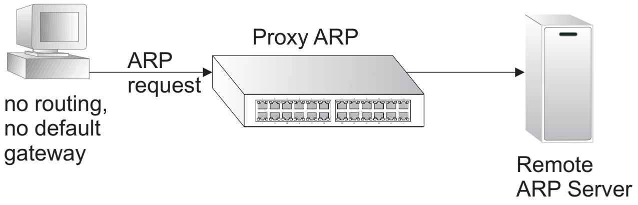
- "arp timeout" on page 1656
- "ip proxy-arp" on page 1657

COMMAND USAGE

Proxy ARP

When a node in the attached subnetwork does not have routing or a default gateway configured, Proxy ARP can be used to forward ARP requests to a remote subnetwork. When the router receives an ARP request for a remote network and Proxy ARP is enabled, it determines if it has the best route to the remote network, and then answers the ARP request by sending its own MAC address to the requesting node. That node then sends traffic to the router, which in turn uses its own routing table to forward the traffic to the remote destination.

Figure 445: Proxy ARP



PARAMETERS

These parameters are displayed:

- **Timeout** – Sets the aging time for dynamic entries in the ARP cache. (Range: 300 - 86400 seconds; Default: 1200 seconds or 20 minutes)

  The ARP aging timeout can be set for any configured VLAN.

  The aging time determines how long dynamic entries remain in the cache. If the timeout is too short, the router may tie up resources by repeating ARP requests for addresses recently flushed from the table.

  When a ARP entry expires, it is deleted from the cache and an ARP request packet is sent to re-establish the MAC address.

- **Proxy ARP** – Enables or disables Proxy ARP for specified VLAN interfaces, allowing a non-routing device to determine the MAC address of a host on another subnet or network. (Default: Disabled)

  End stations that require Proxy ARP must view the entire network as a single network. These nodes must therefore use a smaller subnet mask than that used by the router or other relevant network devices.

  Extensive use of Proxy ARP can degrade router performance because it may lead to increased ARP traffic and increased search time for larger ARP address tables.

WEB INTERFACE

To configure the timeout for the ARP cache or to enable Proxy ARP for a VLAN (i.e., IP subnetwork):

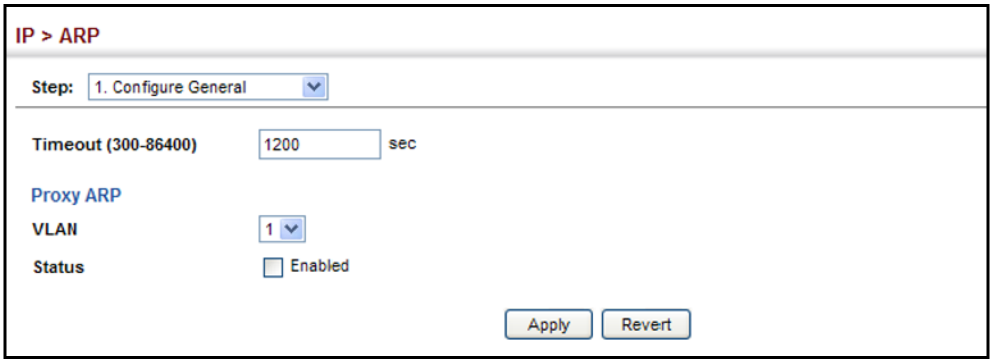
1. Click IP, ARP.

2. Select Configure General from the Step List.

3. Set the timeout to a suitable value for the ARP cache, or enable Proxy ARP for subnetworks that do not have routing or a default gateway.

4. Click Apply.

Figure 446: Configuring General Settings for ARP



IP > ARP

Step: 1. Configure General

Timeout (300-86400) 1200 sec

Proxy ARP

VLAN 1

Status □ Enabled

CONFIGURING STATIC ARP ADDRESSES

For devices that do not respond to ARP requests or do not respond in a timely manner, traffic will be dropped because the IP address cannot be mapped to a physical address. If this occurs, use the IP > ARP (Configure Static Address – Add) page to manually map an IP address to the corresponding physical address in the ARP cache.

CLI REFERENCES

- "arp" on page 1655

COMMAND USAGE

- The ARP cache is used to map 32-bit IP addresses into 48-bit hardware (that is, Media Access Control) addresses. This cache includes entries for hosts and other routers on local network interfaces defined on this router.

- You can define up to 128 static entries in the ARP cache.

- A static entry may need to be used if there is no response to an ARP broadcast message. For example, some applications may not respond to ARP requests or the response arrives too late, causing network operations to time out.

- Static entries will not be aged out or deleted when power is reset. You can only remove a static entry via the configuration interface.

- Static entries are only displayed on the Show page for VLANs that are up. In other words, static entries are only displayed when configured for the IP subnet of an existing VLAN, and that VLAN is linked up.

PARAMETERS

These parameters are displayed:

- **IP Address** – IP address statically mapped to a physical MAC address. (Valid IP addresses consist of four numbers, 0 to 255, separated by periods.)

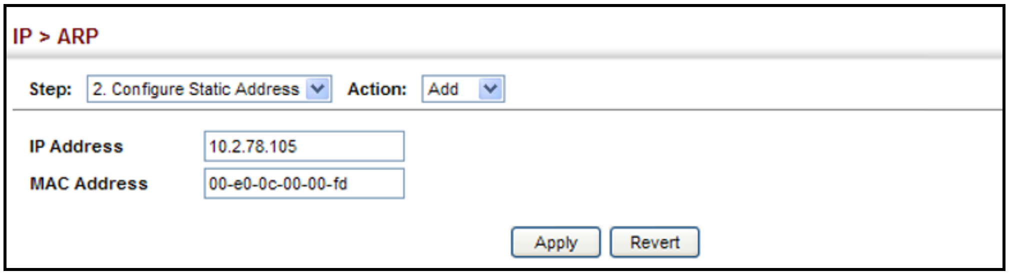
- **MAC Address** – MAC address statically mapped to the corresponding IP address. (Valid MAC addresses are hexadecimal numbers in the format: xx-xx-xx-xx-xx-xx)

WEB INTERFACE

To map an IP address to the corresponding physical address in the ARP cache using the web interface:

1. Click IP, ARP.
2. Select Configure Static Address from the Step List.
3. Select Add from the Action List.
4. Enter the IP address and the corresponding MAC address.
5. Click Apply.

Figure 447: Configuring Static ARP Entries



IP > ARP

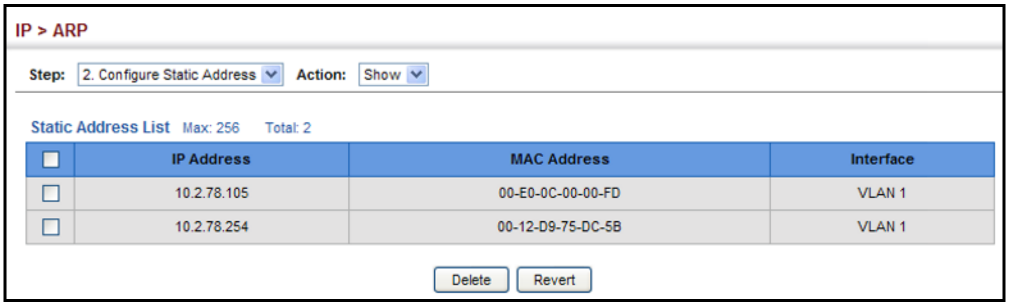
Step: 2. Configure Static Address Action: Add

IP Address: 10.2.78.105
MAC Address: 00-e0-0c-00-00-fd

To display static entries in the ARP cache:

1. Click IP, ARP.
2. Select Configure Static Address from the Step List.
3. Select Show from the Action List.

Figure 448: Displaying Static ARP Entries



IP > ARP

Step: 2. Configure Static Address Action: Show

Static Address List Max: 256 Total: 2

□	IP Address	MAC Address	Interface
□	10.2.78.105	00-E0-0C-00-00-FD	VLAN 1
□	10.2.78.254	00-12-D9-75-DC-5B	VLAN 1

DISPLAYING DYNAMIC OR LOCAL ARP ENTRIES

Use the IP > ARP (Show Information) page to display dynamic or local entries in the ARP cache. The ARP cache contains static entries, and entries for local interfaces, including subnet, host, and broadcast addresses. However, most entries will be dynamically learned through replies to broadcast messages.

CLI REFERENCES

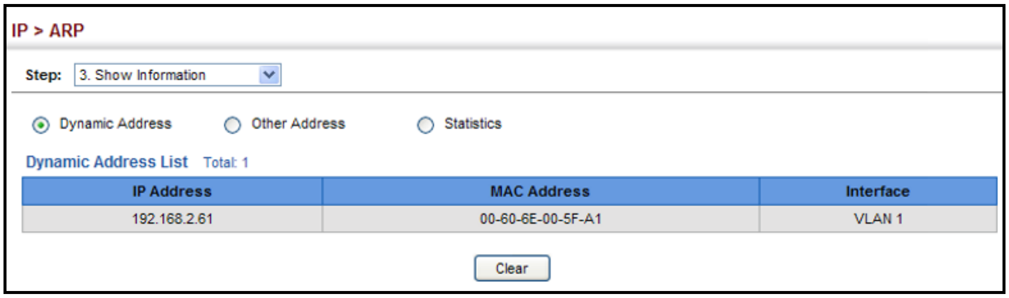
- "show arp" on page 1658

WEB INTERFACE

To display all dynamic entries in the ARP cache:

1. Click IP, ARP.
2. Select Show Information from the Step List.
3. Click Dynamic Address.

Figure 449: Displaying Dynamic ARP Entries


IP > ARP
Step: 3. Show Information
● Dynamic Address ○ Other Address ○ Statistics
Clear

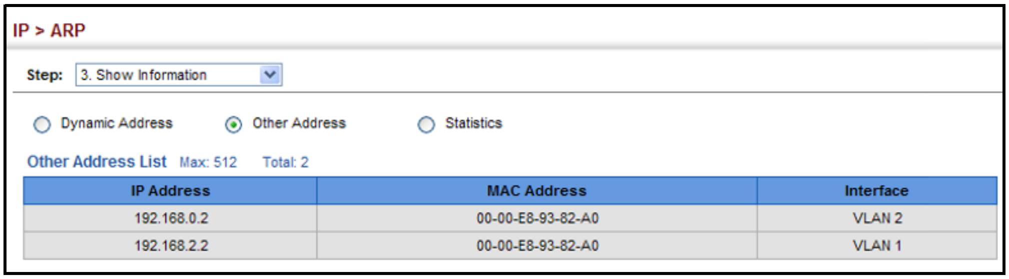
Dynamic Address List Total: 1

IP Address	MAC Address	Interface
192.168.2.61	00-60-6E-00-5F-A1	VLAN 1

To display all local entries in the ARP cache:

1. Click IP, ARP.
2. Select Show Information from the Step List.
3. Click Other Address.

Figure 450: Displaying Local ARP Entries


IP > ARP
Step: 3. Show Information
○ Dynamic Address ● Other Address ○ Statistics

Other Address List Max: 512 Total: 2

IP Address	MAC Address	Interface
192.168.0.2	00-00-E8-93-82-A0	VLAN 2
192.168.2.2	00-00-E8-93-82-A0	VLAN 1

DISPLAYING ARP STATISTICS

Use the IP > ARP (Show Information) page to display statistics for ARP messages crossing all interfaces on this router.

CLI REFERENCES

- "show ip traffic" on page 1728

PARAMETERS

These parameters are displayed:

Table 51: ARP Statistics

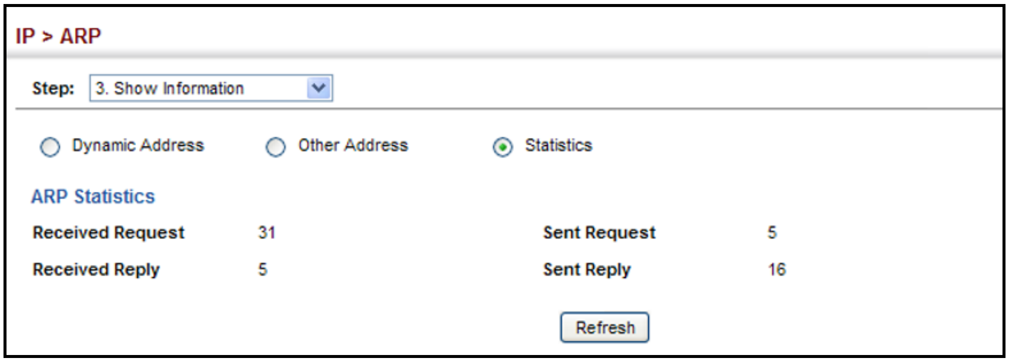
Parameter	Description
Received Request	Number of ARP Request packets received by the router.
Received Reply	Number of ARP Reply packets received by the router.
Sent Request	Number of ARP Request packets sent by the router.
Sent Reply	Number of ARP Reply packets sent by the router.

WEB INTERFACE

To display ARP statistics:

1. Click IP, ARP.
2. Select Show Information from the Step List.
3. Click Statistics.

Figure 451: Displaying ARP Statistics



IP > ARP

Step: 3. Show Information

○ Dynamic Address ○ Other Address ● Statistics

ARP Statistics

Received Request	31	Sent Request	5
Received Reply	5	Sent Reply	16

CONFIGURING STATIC ROUTES

This router can dynamically configure routes to other network segments using dynamic routing protocols (i.e., RIP, OSPF, BGP). However, you can also manually enter static routes in the routing table using the IP > Routing > Static Routes (Add) page. Static routes may be required to access network segments where dynamic routing is not supported, or can be set to force the use of a specific route to a subnet, rather than using dynamic routing. Static routes do not automatically change in response to changes in network topology, so you should only configure a small number of stable routes to ensure network accessibility.

CLI REFERENCES

- "ip route" on page 1724

COMMAND USAGE

- Up to 256 static routes can be configured.
- Up to eight equal-cost multipaths (ECMP) can be configured for static routing (see "Equal-cost Multipath Routing" on page 757).
- If an administrative distance is defined for a static route, and the same destination can be reached through a dynamic route at a lower administration distance, then the dynamic route will be used.
- If both static and dynamic paths have the same lowest cost, the first route stored in the routing table, either statically configured or dynamically learned via a routing protocol, will be used.
- Static routes are included in RIP and OSPF updates periodically sent by the router if this feature is enabled (see page 779 or 807, respectively).

PARAMETERS

These parameters are displayed:

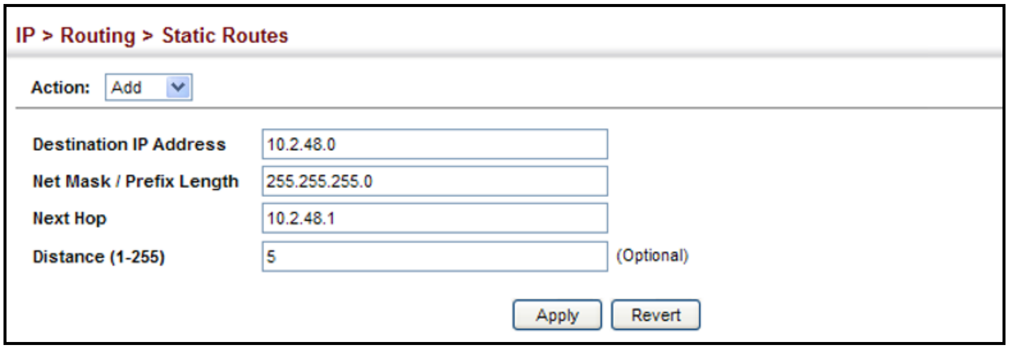
- **Destination IP Address** – IP address of the destination network, subnetwork, or host.
- **Netmask / Prefix Length** – Network mask for the associated IP subnet. This mask identifies the host address bits used for routing to specific subnets.
- **Next Hop** – IP address of the next router hop used for this route.
- **Distance** – An administrative distance indicating that this route can be overridden by dynamic routing information if the distance of the dynamic route is less than that configured for the static route. Note that the default administrative distances used by the dynamic unicast routing protocols is 110 for OSPF and 120 for RIP.
(Range: 1-255, Default: 1)

WEB INTERFACE

To configure static routes:

1. Click IP, Routing, Static Routes.
2. Select Add from the Action List.
3. Enter the destination address, subnet mask, and next hop router.
4. Click Apply.

Figure 452: Configuring Static Routes



IP > Routing > Static Routes

Action: Add

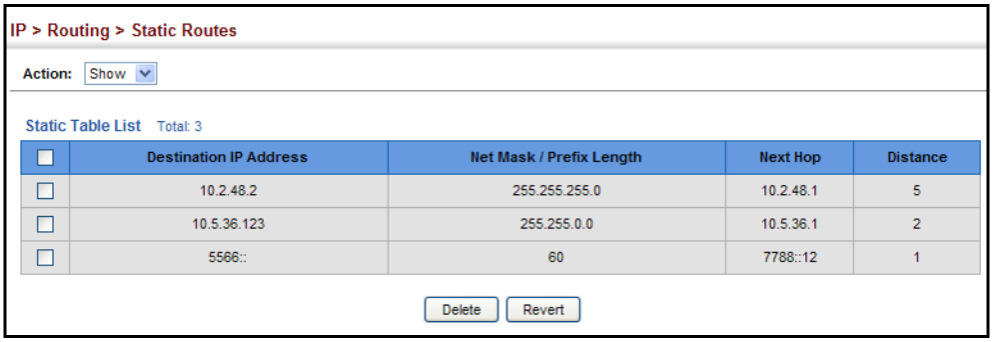
Destination IP Address: 10.2.48.0
Net Mask / Prefix Length: 255.255.255.0
Next Hop: 10.2.48.1
Distance (1-255): 5 (Optional)

To display static routes:

1. Click IP, Routing, Static Routes.

2. Select Show from the Action List.

Figure 453: Displaying Static Routes



IP > Routing > Static Routes

Action: Show

Static Table List Total: 3

□	Destination IP Address	Net Mask / Prefix Length	Next Hop	Distance
□	10.2.48.2	255.255.255.0	10.2.48.1	5
□	10.5.36.123	255.255.0.0	10.5.36.1	2
□	5566::	60	7788::12	1

DISPLAYING THE ROUTING TABLE

Use the IP > Routing > Routing Table (Show Information) page to display all routes that can be accessed via local network interfaces, through static routes, or through a dynamically learned route. If route information is available through more than one of these methods, the priority for route selection is local, static, and then dynamic (except when the distance parameter of a dynamic route is set to a value that makes its priority exceed that of a static route). Also note that the route for a local interface is not enabled (i.e., listed in the routing table) unless there is at least one active link connected to that interface.

CLI REFERENCES

- "show ip route" on page 1726

COMMAND USAGE

- The Forwarding Information Base (FIB) contains information required to forward IP traffic. It contains the interface identifier and next hop information for each reachable destination network prefix based on the IP routing table. When routing or topology changes occur in the network, the routing table is updated, and those changes are immediately reflected in the FIB.

The FIB is distinct from the routing table (or, Routing Information Base – RIB), which holds all routing information received from routing peers. The FIB contains unique paths only. It does not contain any secondary paths. A FIB entry consists of the minimum amount of information necessary to make a forwarding decision on a particular packet. The typical components within a FIB entry are a network prefix, a router (i.e., VLAN) interface, and next hop information.

- The Routing Table (and show ip route command) only displays routes which are currently accessible for forwarding. The router must be able to directly reach the next hop, so the VLAN interface associated with any dynamic or static route entry must be up. Note that routes currently not accessible for forwarding, may still be displayed by using the show ip route database command.

PARAMETERS

These parameters are displayed:

- **VLAN** – VLAN identifier (i.e., configure as a valid IP subnet).

- **Destination IP Address** – IP address of the destination network, subnetwork, or host. Note that the address 0.0.0.0 indicates the default gateway for this router.

- **Net Mask / Prefix Length** – Network mask for the associated IP subnet. This mask identifies the host address bits used for routing to specific subnets.

- **Next Hop** – The IP address of the next hop (or gateway) in this route.

- **Metric** – Cost for this interface.

- **Protocol** – The protocol which generated this route information. (Options: Local, Static, RIP, OSPF, Others)

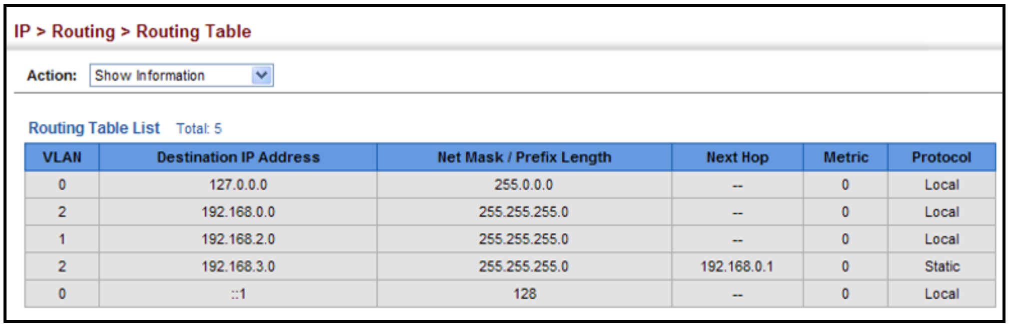
WEB INTERFACE

To display the routing table:

1. Click IP, Routing, Routing Table.

2. Select Show Information from the Action List.

Figure 454: Displaying the Routing Table



IP > Routing > Routing Table

Action: Show Information

Routing Table List Total: 5

VLAN	Destination IP Address	Net Mask / Prefix Length	Next Hop	Metric	Protocol
0	127.0.0.0	255.0.0.0	--	0	Local
2	192.168.0.0	255.255.255.0	--	0	Local
1	192.168.2.0	255.255.255.0	--	0	Local
2	192.168.3.0	255.255.255.0	192.168.0.1	0	Static
0	::1	128	--	0	Local

EQUAL-COST MULTIPATH ROUTING

Use the IP > Routing > Routing Table (Configure ECMP Number) page to configure the maximum number of equal-cost paths that can transmit traffic to the same destination. The Equal-cost Multipath routing algorithm is a technique that supports load sharing over multiple equal-cost paths for data passing to the same destination. Whenever multiple paths with equal path cost to the same destination are found in the routing table, the ECMP algorithm first checks if the cost is lower than that of any other entries in the routing table. If the cost is the lowest in the table, the switch will use up to eight of the paths with equal lowest cost to balance the traffic forwarded to the destination. ECMP uses either equal-cost multipaths manually configured in the static routing table, or equal-cost multipaths dynamically generated by the Open Shortest Path Algorithm (OSPF). In other words, it uses either static or OSPF entries, not both. Normal unicast routing simply selects the path to the destination that has the lowest cost. Multipath routing still selects the path with the lowest cost, but can forward traffic over multiple paths if they all have the same lowest cost. ECMP is enabled by default on the switch. If there is only one lowest cost path toward the destination, this path will be used to forward all traffic. If there is more than one lowest-cost path configured in the static routing table (see "Configuring Static Routes" on page 753), or dynamically generated by OSPFv2 (see "Configuring the Open Shortest Path First Protocol (Version 2)" on page 788), then up to 8 paths with the same lowest cost can be used to forward traffic to the destination.

CLI REFERENCES

- "maximum-paths" on page 1725

COMMAND USAGE

- ECMP only selects paths of the same protocol type. It cannot be applied to both static paths and dynamic paths at the same time for the same destination. If both static and dynamic paths have the same lowest cost, the static paths have precedence over dynamic paths.

- Each path toward the same destination with equal-cost takes up one entry in the routing table to record routing information. In other words, a route with 8 paths will take up 8 entries.

- The routing table can only have up to 8 equal-cost multipaths for static routing and 8 for dynamic routing for a common destination. However, the system supports up to 256 total ECMP entries in ASIC for fast switching, with any additional entries handled by software routing.

- When there are multiple paths toward the same destination with equal-cost, the system chooses one of these paths to forward each packet toward the destination by applying a load-splitting algorithm.

  A hash value is calculated based upon the source and destination IP fields of each packet as an indirect index to one of the multiple paths. Because the hash algorithm is calculated based upon the packet header information which can identify specific traffic flows, this technique minimizes the number of times a path is changed for individual flows. In general, path changes for individual flows will only occur when a path is added or removed from the multipath group.

PARAMETERS

These parameters are displayed:

- **ECMP Number** – Sets the maximum number of equal-cost paths to the same destination that can be installed in the routing table.
  (Range: 1-8; Default: 8)

WEB INTERFACE

To configure the maximum ECMP number:

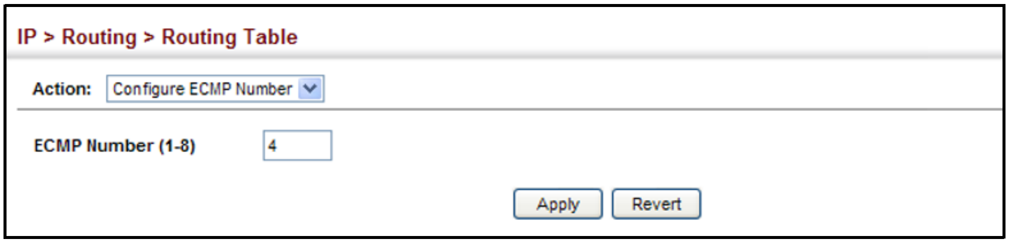
1. Click IP, Routing, Routing Table.

2. Select Configure ECMP Number from the Action List.

3. Enter the maximum number of equal-cost paths used to route traffic to the same destination that are permitted on the switch.

4. Click Apply

Figure 455: Setting the Maximum ECMP Number



IP > Routing > Routing Table

Action: Configure ECMP Number

ECMP Number (1-8) 4

19 Configuring Router Redundancy

Router redundancy protocols use a virtual IP address to support a primary router and multiple backup routers. The backup routers can be configured to take over the workload if the master router fails, or can also be configured to share the traffic load. The primary goal of router redundancy is to allow a host device which has been configured with a fixed gateway to maintain network connectivity in case the primary gateway goes down.

This switch supports the Virtual Router Redundancy Protocol (VRRP). VRRP allows you to specify the interface of one of the routers participating in the virtual group as the address for the master virtual router, or to configure an arbitrary address for the virtual master router. VRRP then selects the backup routers based on the specified virtual router priority.

Router redundancy can be set up in any of the following configurations. These examples use the address of one of the participating routers as the master router. When the virtual router IP address is not a real address, the master router is selected based on priority. When the priority is the same on several competing routers, then the router with the highest IP address is selected as the master.

Figure 456: Master Virtual Router with Backup Routers

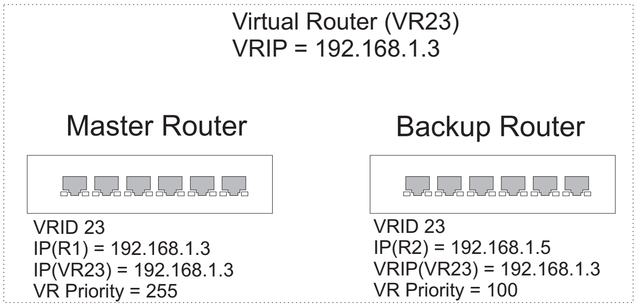


Figure 457: Several Virtual Master Routers Using Backup Routers

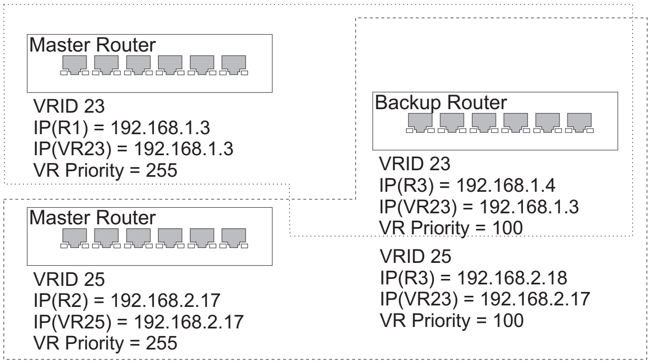
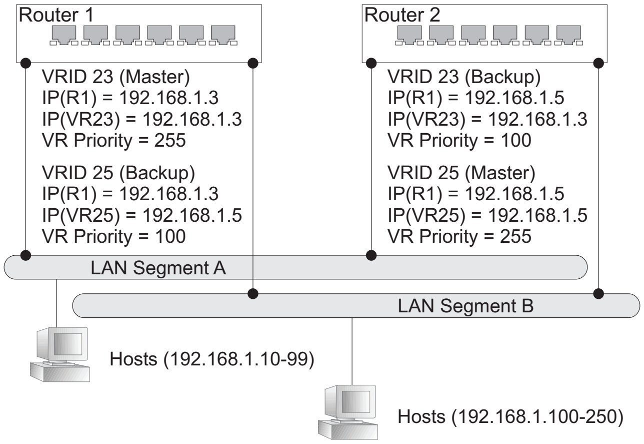


Figure 458: Several Virtual Master Routers Configured for Mutual Backup and Load Sharing



NOTE: Load sharing can be accomplished by assigning a subset of addresses to different host address pools using the DHCP server. (See "Configuring Address Pools" on page 726)

CONFIGURING VRRP GROUPS

Use the IP > VRRP pages to configure VRRP. To configure VRRP groups, select an interface on each router in the group that will participate in the protocol as the master router or a backup router. To select a specific device as the master router, set the address of this interface as the virtual router address for the group. Now set the same virtual address and a priority on the backup routers, and configure an authentication string. You can also enable the preempt feature which allows a router to take over as the master router when it comes on line if it has a higher priority than the currently active master router.

CLI REFERENCES

- "VRRP Commands" on page 1713

COMMAND USAGE

Address Assignment –

- To designate a specific router as the VRRP master, the IP address assigned to the virtual router must already be configured on the router that will become the Owner of the group address. In other words, the IP address for the virtual router exists on one, and only one, router in the virtual router group, and the network mask for the virtual router address is derived from the Owner. The Owner will also assume the role of the Master virtual router in the group.

- If a virtual address is assigned to the group which does not exist on any of the group members, then the master router is selected based on priority. In cases where the configured priority is the same on several group members, then the master router with the highest IP address is selected from this group.

- If you have multiple secondary addresses configured on the current VLAN interface, you can add any of these addresses to the virtual router group.

- The interfaces of all routers participating in a virtual router group must be within the same IP subnet.

- VRRP creates a virtual MAC address for the master router based on a standard prefix, with the last octet equal to the group ID. When a backup router takes over as the master, it continues to forward traffic addressed to this virtual MAC address. However, the backup router cannot reply to ICMP pings sent to addresses associated with the virtual group because the IP address owner is off line.

Virtual Router Priority –

- The Owner of the virtual IP address is automatically assigned the highest possible virtual router priority of 255. The backup router with the highest priority will become the master router if the current master fails. However, because the priority of the virtual IP address Owner is the highest, the original master router will always become the active master router when it recovers.

- If two or more routers are configured with the same VRRP priority, the router with the higher IP address is elected as the new master router if the current master fails.

Preempting the Acting Master –

- The virtual IP Owner has the highest priority, so no other router can preempt it, and it will always resume control as the master virtual router when it comes back on line. The preempt function only allows a backup router to take over from a master router if no router in the group is the virtual IP owner, or from another backup router that is temporarily acting as the group master. If preemption is enabled and this router has a higher priority than the current acting master when it comes on line, it will take over as the acting group master.

- You can add a delay to the preempt function to give additional time to receive an advertisement message from the current master before taking control. If the router attempting to become the master has just come on line, this delay also gives it time to gather information for its routing table before actually preempting the currently active master router.

PARAMETERS

These parameters are displayed:

Adding a VRRP Group

- **VRID** – VRRP group identifier. (Range: 1-255)

- **VLAN** – ID of a VLAN configured with an IP interface. (Range: 1-4094; Default: 1)

Adding a Virtual IP Address

- **VLAN ID** – ID of a VLAN configured with an IP interface. (Range: 1-4094)

- **VRID** – VRRP group identifier. (Range: 1-255)

- **IP Address** – Virtual IP address for this group.

  Use the IP address of a real interface on this router to make it the master virtual router for the group. Otherwise, use the virtual address for an existing group to make it a backup router, or to compete as the master based on configured priority if no other members are set as the owner of the group address.

Configuring Detailed Settings

- **VLAN ID** – VLAN configured with an IP interface. (Range: 1-4094)

- **VRID** – VRRP group identifier. (Range: 1-255)

- **Advertisement Interval** – Interval at which the master virtual router sends advertisements communicating its state as the master. (Range: 1-255 seconds; Default: 1 second)

  VRRP advertisements from the current master virtual router include information about its priority and current state as the master.

  VRRP advertisements are sent to the multicast address 224.0.0.8. Using a multicast address reduces the amount of traffic that has to be processed by network devices that are not part of the designated VRRP group.

  If the master router stops sending advertisements, backup routers will bid to become the master router based on priority. The dead interval before attempting to take over as the master is three times the hello interval plus half a second.

- **Priority** – The priority of this router in a VRRP group. (Range: 1-254; Default: 100)

  - The priority for the VRRP group address owner is automatically set to 255.

  - The priority for backup routers is used to determine which router will take over as the acting master router if the current master fails.

- **Preempt Mode** – Allows a backup router to take over as the master virtual router if it has a higher priority than the acting master virtual router (i.e., a master router that is not the group’s address owner, or another backup router that has taken over from the previous master). (Default: Enabled)

- **Preempt Delay Time** – Time to wait before issuing a claim to become the master. (Range: 0-120 seconds; 0 seconds)

- **Authentication Mode** – Authentication mode used to verify VRRP packets received from other routers. (Options: None, Simple Text; Default: None)

  If simple text authentication is selected, then you must also enter an authentication string.

  All routers in the same VRRP group must be set to the same authentication mode, and be configured with the same authentication string.

  Plain text authentication does not provide any real security. It is supported only to prevent a misconfigured router from participating in VRRP.

- **Authentication String** – Key used to authenticate VRRP packets received from other routers. (Range: 1-8 alphanumeric characters)

  When a VRRP packet is received from another router in the group, its authentication string is compared to the string configured on this router. If the strings match, the message is accepted. Otherwise, the packet is discarded.

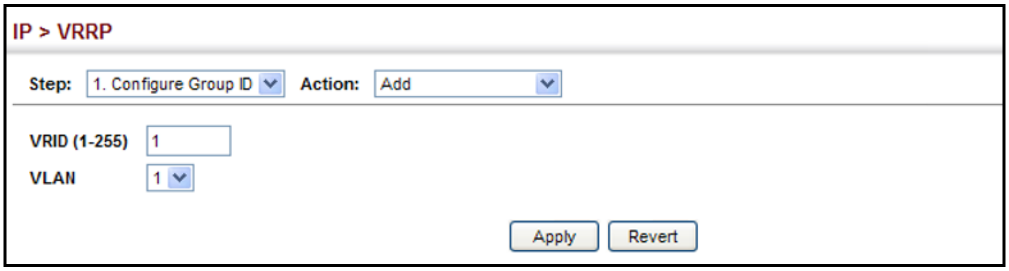
- **State** – VRRP router role. (Values: Master, Backup)
- **Virtual MAC Address** – Virtual MAC address for this group.
- **Master Router** – The primary router servicing this group.
- **Master Priority** – The priority of the master router.
- **Master Advertisement Interval** – The interval at which the master router sends messages advertising itself as the group master.
- **Master Down Interval** – If no advertisement message is received from the master router after this interval, backup routers will assume that the master is dead, and will start bidding to become the group master.

WEB INTERFACE

To configure VRRP:

1. Click IP, VRRP.
2. Select Configure Group ID from the Step List.
3. Select Add from the Action List.
4. Enter the VRID group number, and select the VLAN (i.e., IP subnet) which is to be serviced by this group.
5. Click Apply.

Figure 459: Configuring the VRRP Group ID



IP > VRRP

Step: 1. Configure Group ID   Action: Add

VRID (1-255) 1

VLAN 1

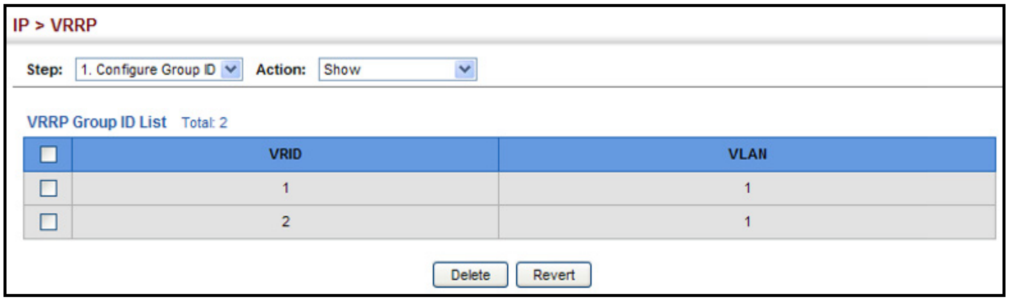
To show the configured VRRP groups:

1. Click IP, VRRP.

2. Select Configure Group ID from the Step List.

3. Select Show from the Action List.

Figure 460: Showing Configured VRRP Groups



IP > VRRP

Step: 1. Configure Group ID   Action: Show

VRRP Group ID List Total: 2

□	VRID	VLAN
□	1	1
□	2	1

To configure the virtual router address for a VRRP group:

1. Click IP, VRRP.

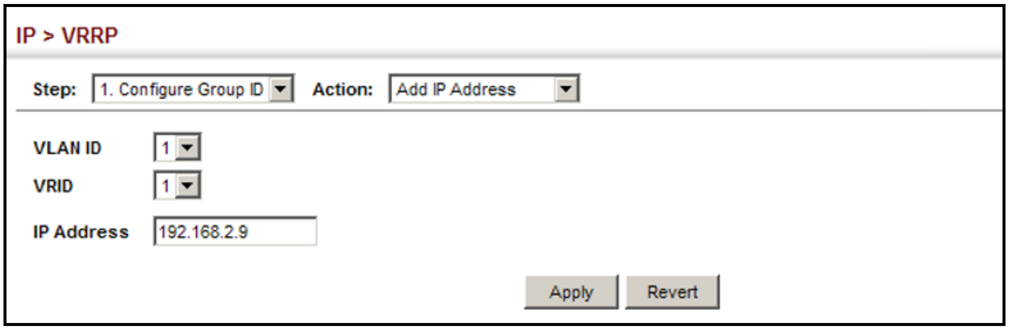
2. Select Configure Group ID from the Step List.

3. Select Add IP Address from the Action List.

4. Select a VLAN, a VRRP group identifier, and enter the IP address for the virtual router.

5. Click Apply.

Figure 461: Setting the Virtual Router Address for a VRRP Group



IP > VRRP

Step: 1. Configure Group ID Action: Add IP Address

VLAN ID 1

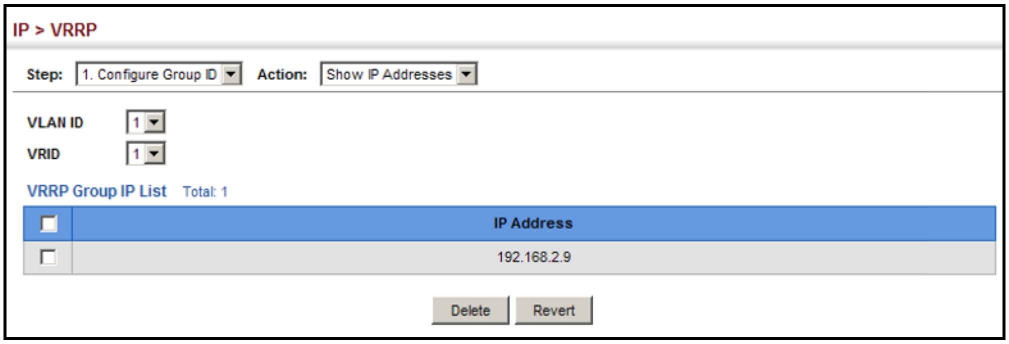
VRID 1

IP Address 192.168.2.9

To show the virtual IP address assigned to a VRRP group:

1. Click IP, VRRP.
2. Select Configure Group ID from the Step List.
3. Select Show IP Addresses from the Action List.
4. Select a VLAN, and a VRRP group identifier.

Figure 462: Showing the Virtual Addresses Assigned to VRRP Groups



IP > VRRP

Step: 1. Configure Group ID Action: Show IP Addresses

VLAN ID 1

VRID 1

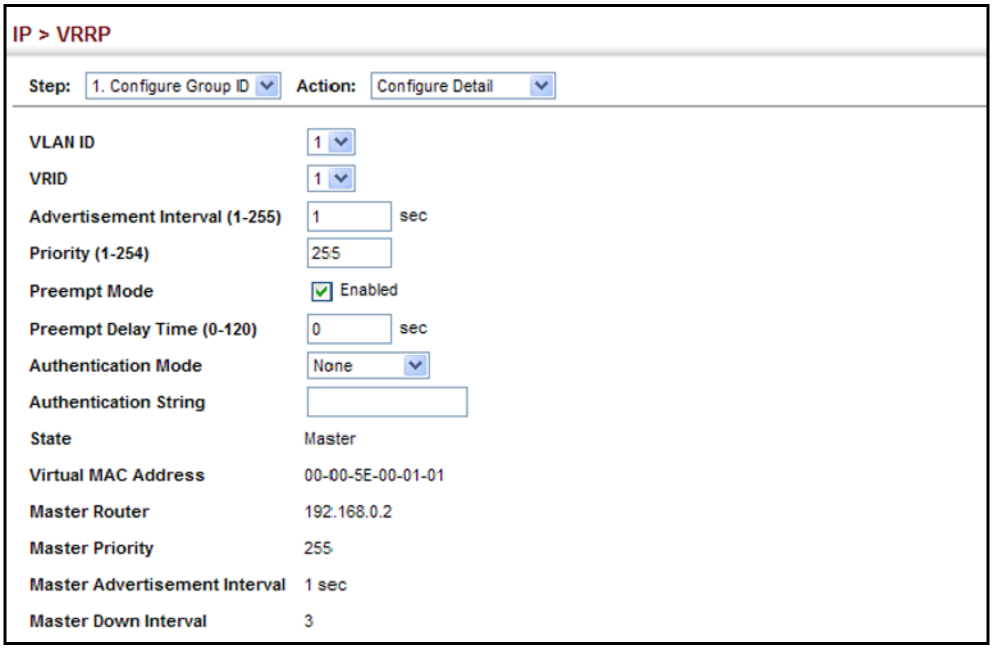
VRRP Group IP List Total: 1

□	IP Address
□	192.168.2.9

To configure detailed settings for a VRRP group:

1. Click IP, VRRP.
2. Select Configure Group ID from the Step List.
3. Select Configure Detail from the Action List.
4. Select a VRRP group identifier, and set any of the VRRP protocol parameters as required.
5. Click Apply.

Figure 463: Configuring Detailed Settings for a VRRP Group



IP > VRRP

Step: 1. Configure Group ID Action: Configure Detail

VLAN ID	1
VRID	1
Advertisement Interval (1-255)	1 sec
Priority (1-254)	255
Preempt Mode	☑ Enabled
Preempt Delay Time (0-120)	0 sec
Authentication Mode	None
Authentication String	
State	Master
Virtual MAC Address	00-00-5E-00-01-01
Master Router	192.168.0.2
Master Priority	255
Master Advertisement Interval	1 sec
Master Down Interval	3

DISPLAYING VRRP GLOBAL STATISTICS

Use the IP > VRRP (Show Statistics – Global Statistics) page to display counters for errors found in VRRP protocol packets.

CLI REFERENCES

- "show vrrp router counters" on page 1722

PARAMETERS

These parameters are displayed:

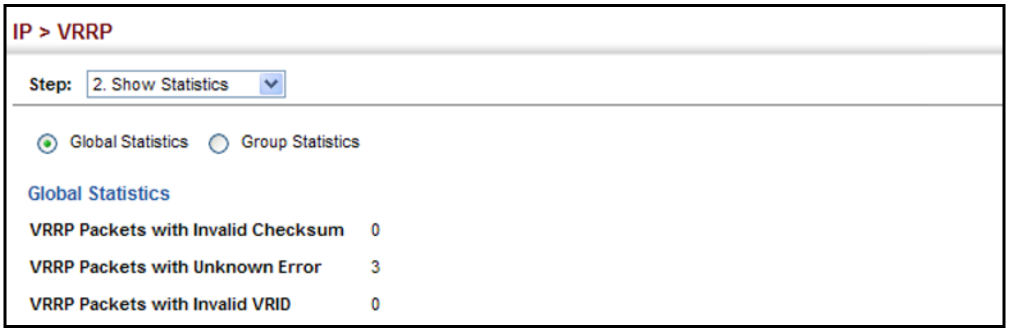
- **VRRP Packets with Invalid Checksum** – The total number of VRRP packets received with an invalid VRRP checksum value.
- **VRRP Packets with Unknown Error** – The total number of VRRP packets received with an unknown or unsupported version number.
- **VRRP Packets with Invalid VRID** – The total number of VRRP packets received with an invalid VRID for this virtual router.

WEB INTERFACE

To show counters for errors found in VRRP protocol packets:

1. Click IP, VRRP.
2. Select Show Statistics from the Step List.
3. Click Global Statistics.

Figure 464: Showing Counters for Errors Found in VRRP Packets



Global Statistics

VRRP Packets with Invalid Checksum 0

VRRP Packets with Unknown Error 3

VRRP Packets with Invalid VRID 0

DISPLAYING VRRP GROUP STATISTICS

Use the IP > VRRP (Show Statistics – Group Statistics) page to display counters for VRRP protocol events and errors that have occurred on a specific VRRP interface.

CLI REFERENCES

- "show vrrp interface counters" on page 1721

PARAMETERS

These parameters are displayed:

- **VLAN ID** – VLAN configured with an IP interface. (Range: 1-4094)
- **VRID** – VRRP group identifier. (Range: 1-255)

The following statistics are displayed:

Table 52: VRRP Group Statistics

Parameter	Description
Times Transitioned to Master	Number of times this router has transitioned to master.
Received Advertisement Packets	Number of VRRP advertisements received by this router.
Received Error Advertisement Interval Packets	Number of VRRP advertisements received for which the advertisement interval is different from the one configured for the local virtual router.
Received Authentication Failure Packets	Number of VRRP packets received that do not pass the authentication check.
Received Error IP TTL VRRP Packets	Number of VRRP packets received by the virtual router with IP TTL (Time-To-Live) not equal to 255.
Received Priority 0 VRRP Packets	Number of VRRP packets received by the virtual router with priority set to 0.
Sent Priority 0 VRRP Packets	Number of VRRP packets sent by the virtual router with priority set to 0. A priority value of zero indicates that the group master has stopped participating in VRRP, and is used to quickly transition a backup unit to master mode without having to wait for the master to time out.

Table 52: VRRP Group Statistics (Continued)

Parameter	Description
Received Invalid Type VRRP Packets	Number of VRRP packets received by the virtual router with an invalid value in the “type” field.
Received Error Address List VRRP Packets	Number of packets received for which the address list does not match the locally configured list for the virtual router.
Received Invalid Authentication Type VRRP Packets	Number of packets received with an unknown authentication type.
Received Mismatch Authentication Type VRRP Packets	Number of packets received with “Auth Type” not equal to the locally configured authentication method.
Received Error Packets Length VRRP Packets	Number of packets received with a packet length less than the length of the VRRP header.

WEB INTERFACE

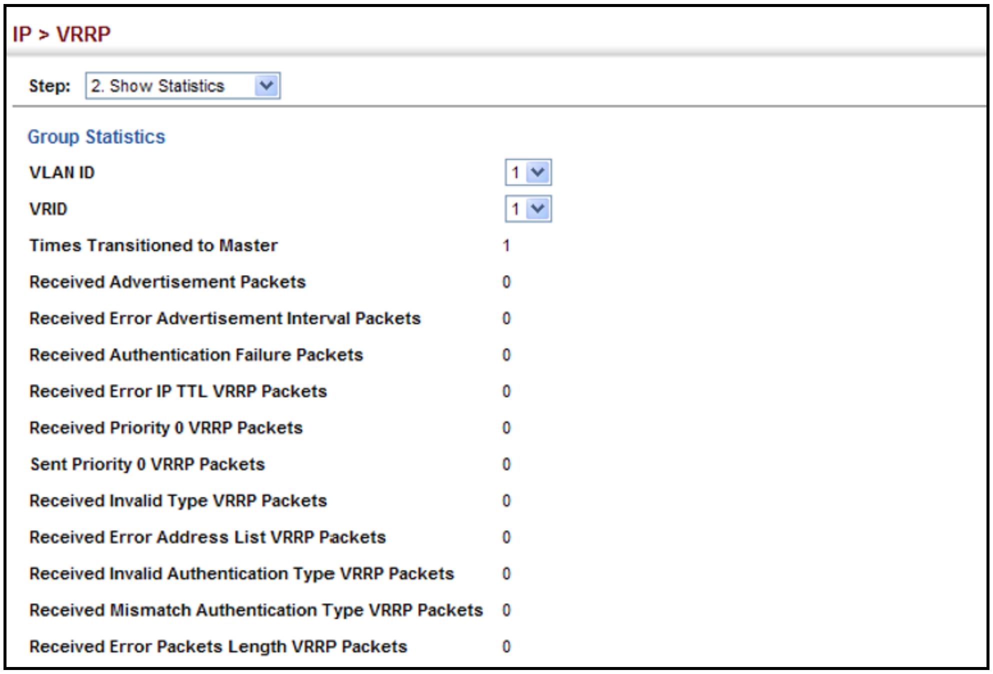
To show counters for VRRP protocol events and errors that occurred on a specific VRRP interface:

1. Click IP, VRRP.

2. Select Show Statistics from the Step List.

3. Click Group Statistics.

Figure 465: Showing Counters for Errors Found in a VRRP Group



IP > VRRP

Step: 2. Show Statistics

Group Statistics

VLAN ID	1
VRID	1
Times Transitioned to Master	1
Received Advertisement Packets	0
Received Error Advertisement Interval Packets	0
Received Authentication Failure Packets	0
Received Error IP TTL VRRP Packets	0
Received Priority 0 VRRP Packets	0
Sent Priority 0 VRRP Packets	0
Received Invalid Type VRRP Packets	0
Received Error Address List VRRP Packets	0
Received Invalid Authentication Type VRRP Packets	0
Received Mismatch Authentication Type VRRP Packets	0
Received Error Packets Length VRRP Packets	0

20 UNICAST ROUTING

This chapter describes how to configure the following unicast routing protocols:

RIP – Configures Routing Information Protocol.

OSPFv2 – Configures Open Shortest Path First (Version 2) for IPv4.

OVERVIEW

This switch can route unicast traffic to different subnetworks using the Routing Information Protocol (RIP) or Open Shortest Path First (OSPF) protocol. It supports RIP, RIP-2 and OSPFv2 dynamic routing in the web management interface. These protocols exchange routing information, calculate routing tables, and can respond to changes in the status or loading of the network. For information on configuring OSPFv3 and BGPv4, refer to the appropriate sections under Chapter 54: IP Routing Commands.

RIP and RIP-2 Dynamic Routing Protocols

The RIP protocol is the most widely used routing protocol. RIP uses a distance-vector-based approach to routing. Routes are determined on the basis of minimizing the distance vector, or hop count, which serves as a rough estimate of transmission cost. Each router broadcasts its advertisement every 30 seconds, together with any updates to its routing table. This allows all routers on the network to learn consistent tables of next hop links which lead to relevant subnets.

OSPFv2 Dynamic Routing Protocols

OSPF overcomes all the problems of RIP. It uses a link state routing protocol to generate a shortest-path tree, then builds up its routing table based on this tree. OSPF produces a more stable network because the participating routers act on network changes predictably and simultaneously, converging on the best route more quickly than RIP. Moreover, when several equal-cost routes to a destination exist, traffic can be distributed equally among them.

Non-IP Protocol Routing

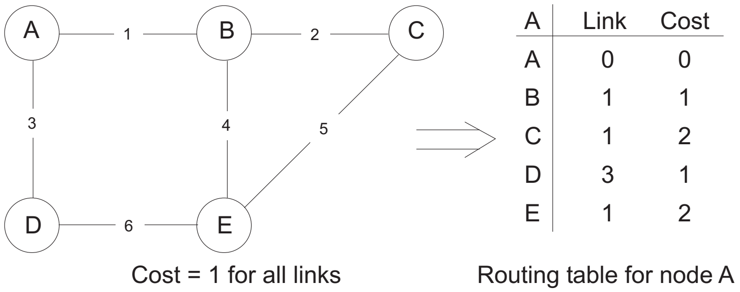
The switch supports IP routing only. Non-IP protocols such as IPX and Appletalk cannot be routed by this switch, and will be confined within their local VLAN group unless bridged by an external router.

To coexist with a network built on multilayer switches, the subnetworks for non-IP protocols must follow the same logical boundary as that of the IP subnetworks. A separate multi-protocol router can then be used to link the subnetworks by connecting to one port from each available VLAN on the network.

CONFIGURING THE ROUTING INFORMATION PROTOCOL

The RIP protocol is the most widely used routing protocol. The RIP protocol uses a distance-vector-based approach to routing. Routes are determined on the basis of minimizing the distance vector, or hop count, which serves as a rough estimate of transmission cost. Each router broadcasts its advertisement every 30 seconds, together with any updates to its routing table. This allows all routers on the network to learn consistent tables of next hop links which lead to relevant subnets.

Figure 466: Configuring RIP



A	Link	Cost
A	0	0
B	1	1
C	1	2
D	3	1
E	1	2

Cost = 1 for all links

Routing table for node A

COMMAND USAGE

- Just as Layer 2 switches use the Spanning Tree Algorithm to prevent loops, routers also use methods for preventing loops that would cause endless retransmission of data traffic. RIP utilizes the following three methods to prevent loops from occurring:

  - Split horizon – Never propagate routes back to an interface port from which they have been acquired.

  - Poison reverse – Propagate routes back to an interface port from which they have been acquired, but set the distance-vector metrics to infinity. (This provides faster convergence.)

  - Triggered updates – Whenever a route gets changed, broadcast an update message after waiting for a short random delay, but without waiting for the periodic cycle.

- RIP-2 is a compatible upgrade to RIP. RIP-2 adds useful capabilities for plain text authentication, multiple independent RIP domains, variable length subnet masks, and multicast transmissions for route advertising (RFC 1723).

- There are several serious problems with RIP that you should consider. First of all, RIP (version 1) has no knowledge of subnets, both RIP versions can take a long time to converge on a new route after the failure of a link or router during which time routing loops may occur, and its small hop count limitation of 15 restricts its use to smaller networks. Moreover, RIP (version 1) wastes valuable network bandwidth by propagating routing information via broadcasts; it also considers too few network variables to make the best routing decision.

CONFIGURING GENERAL PROTOCOL SETTINGS

Use the Routing Protocol > RIP > General (Configure) page to configure general settings and the basic timers.

RIP is used to specify how routers exchange routing information. When RIP is enabled on this router, it sends RIP messages to all devices in the network every 30 seconds (by default), and updates its own routing table when RIP messages are received from other routers. To communicate properly with other routers using RIP, you need to specify the RIP version used globally by the router, as well as the RIP send and receive versions used on specific interfaces (see "Configuring Network Interfaces for RIP" on page 782).

CLI REFERENCES

- "Routing Information Protocol (RIP)" on page 1733

COMMAND USAGE

- RIP is used to specify how routers exchange routing information. When RIP is enabled on this router, it sends RIP messages to all devices in the network every 30 seconds (by default), and updates its own routing table when RIP messages are received from other routers. To communicate properly with other routers using RIP, you need to specify the RIP version used globally by the router, as well as the RIP send and receive versions used on specific interfaces (page 782).

PARAMETERS

These parameters are displayed:

Global Settings

- **RIP Routing Process** – Enables RIP routing globally. RIP must also be enabled on each network interface which will participate in the routing process as described under "Specifying Network Interfaces" on page 775. (Default: Disabled)

- **Global RIP Version** – Specifies a RIP version used globally by the router. (Version 1, Version 2, By Interface; Default: By Interface)

  When a Global RIP Version is specified, any VLAN interface not previously set to a specific Receive or Send Version (page 782) is set to the following values:

  - RIP Version 1 configures previously unset interfaces to send RIPv1 compatible protocol messages and receive either RIPv1 or RIPv2 protocol messages.

  - RIP Version 2 configures previously unset interfaces to use RIPv2 for both sending and receiving protocol messages.

  RIP send/receive versions set on the RIP Interface settings screen (page 782) always take precedence over the settings for the Global RIP Version. However, when the Global RIP Version is set to "By Interface," any VLAN interface not previously set to a specific receive or send version is set to the following default values:

- Receive: Accepts RIPv1 or RIPv2 packets.
- Send: Route information is broadcast to other routers with RIPv2.

- **RIP Default Metric** – Sets the default metric assigned to external routes imported from other protocols. (Range: 1-15; Default: 1)

  The default metric must be used to resolve the problem of redistributing external routes with incompatible metrics.

  It is advisable to use a low metric when redistributing routes from another protocol into RIP. Using a high metric limits the usefulness of external routes redistributed into RIP. For example, if a metric of 10 is defined for redistributed routes, these routes can only be advertised to routers up to 5 hops away, at which point the metric exceeds the maximum hop count of 15. By defining a low metric of 1, traffic can follow a imported route the maximum number of hops allowed within a RIP domain. However, note that using a low metric can increase the possibility of routing loops. For example, this can occur if there are multiple redistribution points and the router learns about the same external network with a better metric from a redistribution point other than that derived from the original source.

  The default metric does not override the metric value set in the Redistribute screen (see "Configuring Route Redistribution" on page 779). When a metric value has not been configured in the Redistribute screen, the default metric sets the metric value to be used for all imported external routes.

- **RIP Max Prefix** – Sets the maximum number of RIP routes which can be installed in the routing table. (Range: 1-7168; Default: 7168)

- **Default Information Originate** – Generates a default external route into the local RIP autonomous system. (Default: Disabled)

  A default route is set for every Layer 3 interface where RIP is enabled. The response packet to external queries marks each active RIP interface as a default router with the IP address 0.0.0.0.

- **Default Distance** – Defines an administrative distance for external routes learned from other routing protocols. External routes are routes for which the best path is learned from a neighbor external to the local RIP autonomous system. Routes with a distance of 255 are not installed in the routing table. (Range: 1-255; Default: 120)

  Administrative distance is used by the routers to select the preferred path when there are two or more different routes to the same destination from two different routing protocols. A smaller administrative distance indicates a more reliable protocol.

  Use the Routing Protocol > RIP > Distance page (see page 781) to configure the distance to a specific network address, or to configure an access list that filters networks according to the IP address of the router supplying the routing information.

- **Number of Route Changes** – The number of route changes made to the IP route database by RIP.

- **Number of Queries** – The number of responses sent to RIP queries from other systems.

Basic Timer Settings

NOTE: The timers must be set to the same values for all routers in the network.

- **Update** – Sets the rate at which updates are sent. This is the fundamental timer used to control all basic RIP processes. (Range: 5-2147483647 seconds; Default: 30 seconds)

  Setting the update timer to a short interval can cause the router to spend an excessive amount of time processing updates. On the other hand, setting it to an excessively long time will make the routing protocol less sensitive to changes in the network configuration.

- **Timeout** – Sets the time after which there have been no update messages that a route is declared dead. The route is marked inaccessible (i.e., the metric set to infinite) and advertised as unreachable. However, packets are still forwarded on this route. (Range: 90-360 seconds; Default: 180 seconds)

- **Garbage Collection** – After the *timeout* interval expires, the router waits for an interval specified by the *garbage-collection* timer before removing this entry from the routing table. This timer allows neighbors to become aware of an invalid route prior to purging. (Range: 60-240 seconds; Default: 120 seconds)

WEB INTERFACE

To configure general settings for RIP:

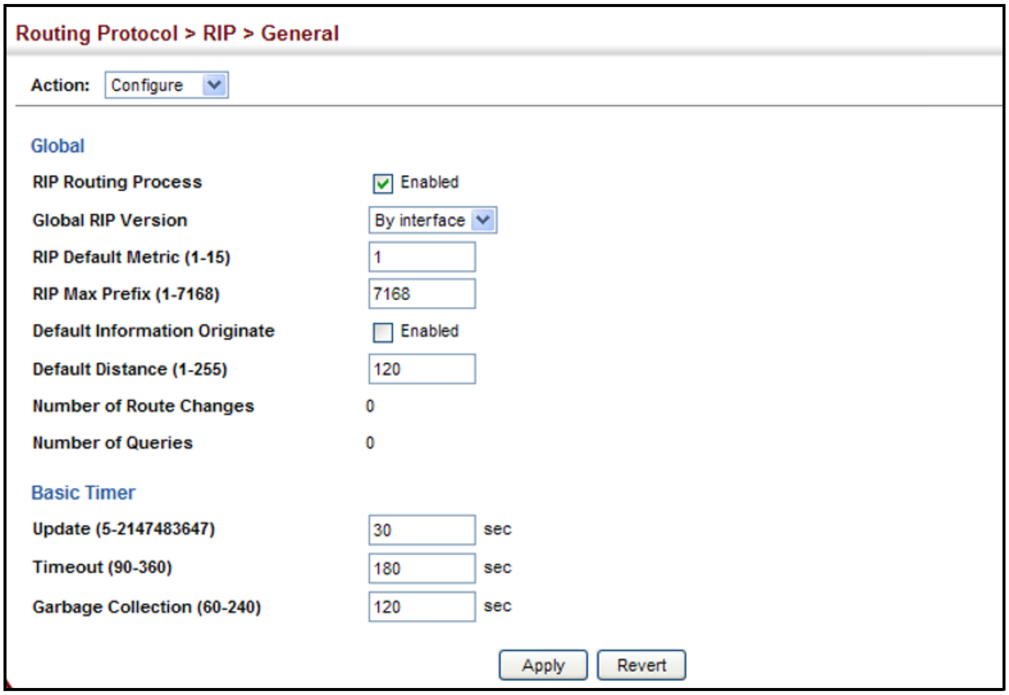
1. Click Routing Protocol, RIP, General.

2. Select Configure Global from the Action list.

3. Enable RIP, set the RIP version used on unset interfaces to RIPv1 or RIPv2, set the default metric assigned to external routes, set the maximum number of routes allowed by the system, and set the basic timers.

4. Click Apply.

Figure 467: Configuring General Settings for RIP



Routing Protocol > RIP > General

Action: Configure

Global

RIP Routing Process	☑ Enabled
Global RIP Version	By interface
RIP Default Metric (1-15)	1
RIP Max Prefix (1-7168)	7168
Default Information Originate	□ Enabled
Default Distance (1-255)	120
Number of Route Changes	0
Number of Queries	0

Basic Timer

Update (5-2147483647)	30 sec
Timeout (90-360)	180 sec
Garbage Collection (60-240)	120 sec

CLEARING ENTRIES FROM THE ROUTING TABLE

Use the Routing Protocol > RIP > General (Clear Route) page to clear entries from the routing table based on route type or a specific network address.

CLI REFERENCES

- "clear ip rip route" on page 1748

COMMAND USAGE

- Clearing "All" types deletes all routes in the RIP table. To avoid deleting the entire RIP network, redistribute connected routes using the Routing Protocol > RIP > Redistribute screen (page 779) to make the RIP network a connected route. To delete the RIP routes learned from neighbors, but keep the RIP network intact, clear "RIP" types from the routing table.

PARAMETERS

These parameters are displayed:

- **Clear Route By Type** – Clears entries from the RIP routing table based on the following types:
  - **All** – Deletes all entries from the routing table.
  - **Connected** – Deletes all currently connected entries.
  - **OSPF** – Deletes all entries learned through OSPF.
  - **RIP** – Deletes all entries learned through the RIP.
  - **Static** – Deletes all static entries.

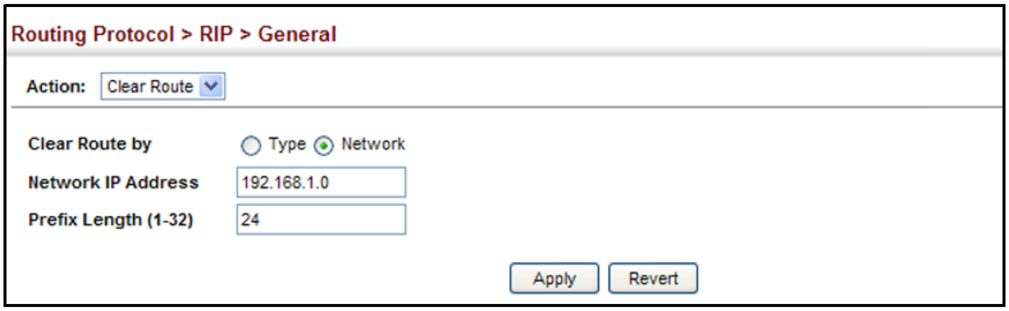
- **Clear Route By Network** – Clears a specific route based on its IP address and prefix length.
  - **Network IP Address** – Deletes all related entries for the specified network address.
  - **Prefix Length** – A decimal value indicating how many contiguous bits (from the left) of the address comprise the network portion of the address.

WEB INTERFACE

To clear entries from the routing table RIP:

1. Click Routing Protocol, RIP, General.
2. Select Clear Route from the Action list.
3. When clearing routes by type, select the required type from the drop-down list. When clearing routes by network, enter a valid network address and prefix length.
4. Click Apply.

Figure 468: Clearing Entries from the Routing Table



Routing Protocol > RIP > General

Action: Clear Route

Clear Route by ○ Type ● Network

Network IP Address 192.168.1.0

Prefix Length (1-32) 24

SPECIFYING NETWORK INTERFACES

Use the Routing Protocol > RIP > Network (Add) page to specify the network interfaces that will be included in the RIP routing process.

CLI REFERENCES

- "network" on page 1738

COMMAND USAGE

- RIP only sends and receives updates on specified interfaces. If a network is not specified, the interfaces in that network will not be advertised in any RIP updates.
- No networks are specified by default.

PARAMETERS

These parameters are displayed:

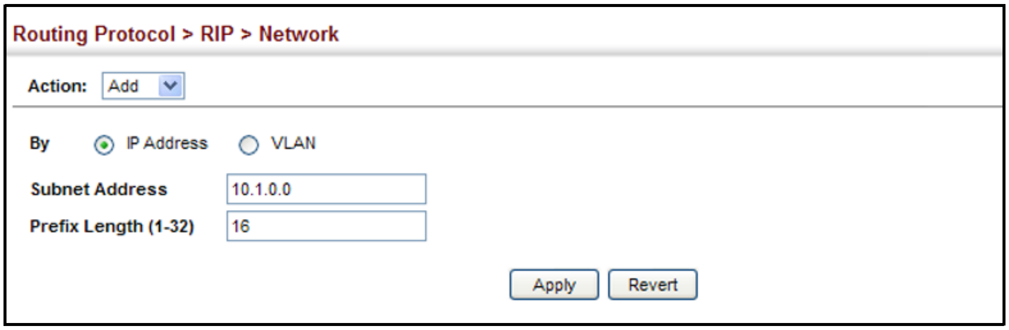
- **By Address** – Adds a network to the RIP routing process.
  - **Subnet Address** – IP address of a network directly connected to this router. (Default: No networks are specified)
  - **Prefix Length** – A decimal value indicating how many contiguous bits (from the left) of the address comprise the network portion of the address. This mask identifies the network address bits used for the associated routing entries.
- **By VLAN** – Adds a Layer 3 VLAN to the RIP routing process. The VLAN must be configured with an IP address. (Range: 1-4094)

WEB INTERFACE

To add a network interface to RIP:

1. Click Routing Protocol, RIP, Network.
2. Select Add from the Action list.
3. Add an interface that will participate in RIP.
4. Click Apply.

Figure 469: Adding Network Interfaces to RIP



Routing Protocol > RIP > Network

Action: Add

By ● IP Address ○ VLAN

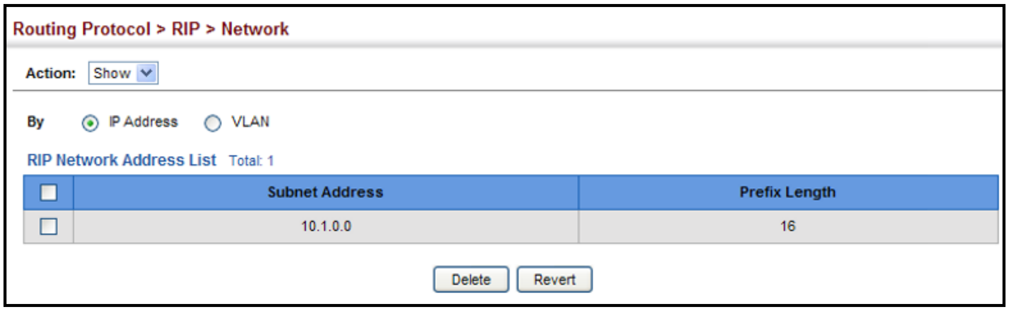
Subnet Address 10.1.0.0

Prefix Length (1-32) 16

To show the network interfaces using RIP:

1. Click Routing Protocol, RIP, Network.
2. Select Show from the Action list.
3. Click IP Address or VLAN.

Figure 470: Showing Network Interfaces Using RIP



Routing Protocol > RIP > Network

Action: Show

By ● IP Address ○ VLAN

RIP Network Address List Total: 1

□	Subnet Address	Prefix Length
□	10.1.0.0	16

SPECIFYING PASSIVE INTERFACES

Use the Routing Protocol > RIP > Passive Interface (Add) page to stop RIP from sending routing updates on the specified interface.

CLI REFERENCES

- "passive-interface" on page 1738

COMMAND USAGE

- Network interfaces can be configured to stop RIP broadcast and multicast messages from being sent. If the sending of routing updates is blocked on an interface, the attached subnet will still continue to be advertised to other interfaces, and updates from other routers on the specified interface will continue to be received and processed.

- This feature can be used in conjunction with the static neighbor feature (described in the next section) to control the routing updates sent to specific neighbors.

PARAMETERS

These parameters are displayed:

- **VLAN** – VLAN interface on which to stop sending RIP updates. (Range: 1-4094)

WEB INTERFACE

To specify a passive RIP interface:

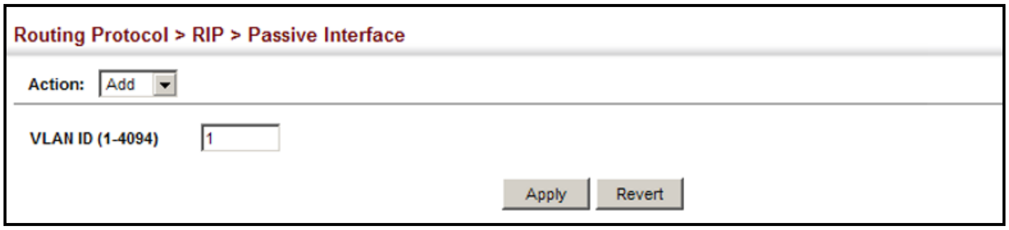
1. Click Routing Protocol, RIP, Passive Interface.

2. Select Add from the Action list.

3. Add the interface on which to stop sending RIP updates.

4. Click Apply.

Figure 471: Specifying a Passive RIP Interface



Routing Protocol > RIP > Passive Interface

Action: Add

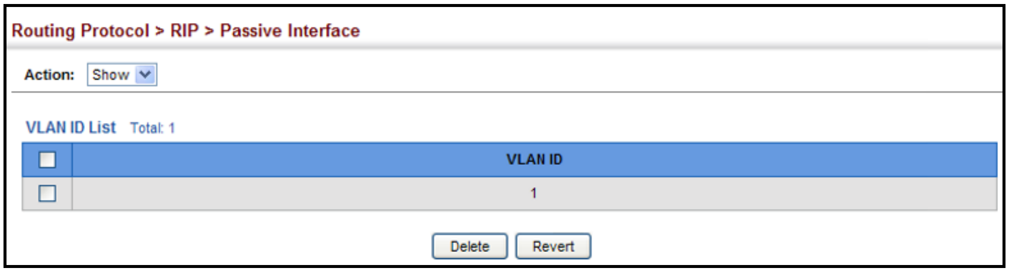
VLAN ID (1-4094) 1

To show the passive RIP interfaces:

1. Click Routing Protocol, RIP, Passive Interface.

2. Select Show from the Action list.

Figure 472: Showing Passive RIP Interfaces



Routing Protocol > RIP > Passive Interface

Action: Show

VLAN ID List Total: 1

□	VLAN ID
□	1

SPECIFYING STATIC NEIGHBORS

Use the Routing Protocol > RIP > Passive Interface (Add) page to configure this router to directly exchange routing information with a static neighbor (specifically for point-to-point links), rather than relying on broadcast or multicast messages generated by the RIP protocol. This feature can be used in conjunction with the passive interface feature (described in the preceding section) to control the routing updates sent to specific neighbors.

CLI REFERENCES

- "neighbor" on page 1737

PARAMETERS

These parameters are displayed:

- **IP Address** – IP address of a static neighboring router with which to exchange routing information.

WEB INTERFACE

To specify a static RIP neighbor:

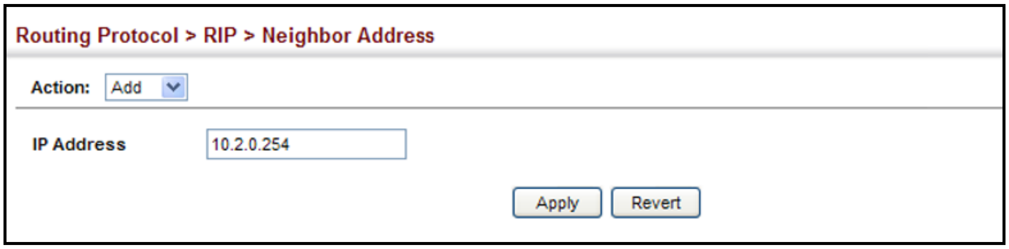
1. Click Routing Protocol, RIP, Neighbor Address.

2. Select Add from the Action list.

3. Add the address of any static neighbors which may not readily to discovered through RIP.

4. Click Apply.

Figure 473: Specifying a Static RIP Neighbor



Routing Protocol > RIP > Neighbor Address

Action: Add

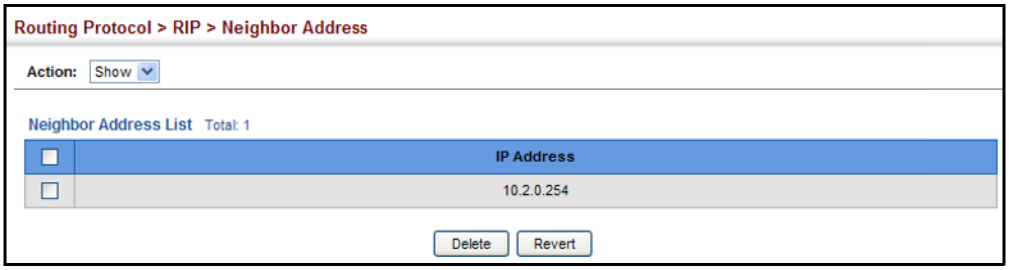
IP Address: 10.2.0.254

To show static RIP neighbors:

1. Click Routing Protocol, RIP, Neighbor Address.

2. Select Show from the Action list.

Figure 474: Showing Static RIP Neighbors



Routing Protocol > RIP > Neighbor Address

Action: Show

Neighbor Address List Total: 1

□	IP Address
□	10.2.0.254

CONFIGURING ROUTE REDISTRIBUTION

Use the Routing Protocol > RIP > Redistribute (Add) page to import external routing information from other routing domains (that is, directly connected routes, protocols, or static routes) into this autonomous system.

CLI REFERENCES

- "redistribute" on page 1739

PARAMETERS

These parameters are displayed:

- **Protocol** – The type of routes that can be imported include:
  - **Connected** – Imports routes that are established automatically just by enabling IP on an interface.
  - **Static** – Static routes will be imported into this routing domain.
  - **OSPF** – External routes will be imported from the Open Shortest Path First protocol into this routing domain.

- **Metric** – Metric assigned to all external routes for the specified protocol. (Range: 0-16; Default: the default metric as described under "Configuring General Protocol Settings" on page 771.)

  A route metric must be used to resolve the problem of redistributing external routes with incompatible metrics.

  When a metric value has not been configured on this page, the default-metric determines the metric value to be used for all imported external routes.

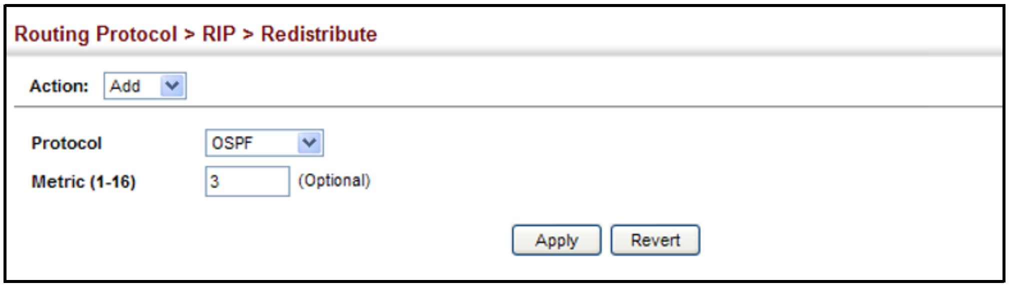
  It is advisable to use a low metric when redistributing routes from another protocol into RIP. Using a high metric limits the usefulness of external routes redistributed into RIP. For example, if a metric of 10 is defined for redistributed routes, these routes can only be advertised to routers up to 5 hops away, at which point the metric exceeds the maximum hop count of 15. By defining a low metric of 1, traffic can follow an imported route the maximum number of hops allowed within a RIP domain. However, using a low metric can increase the possibility of routing loops For example, this can occur if there are multiple redistribution points and the router learns about the same external network with a better metric from a redistribution point other than that derived from the original source.

WEB INTERFACE

To import external routing information from other routing domains:

1. Click Routing Protocol, RIP, Redistribute.
2. Select Add from the Action list.
3. Specify the protocol types (directly connected, OSPF or static) from which to import external routes, and the metric to assign to these routes.
4. Click Apply.

Figure 475: Redistributing External Routes into RIP



Routing Protocol > RIP > Redistribute

Action: Add

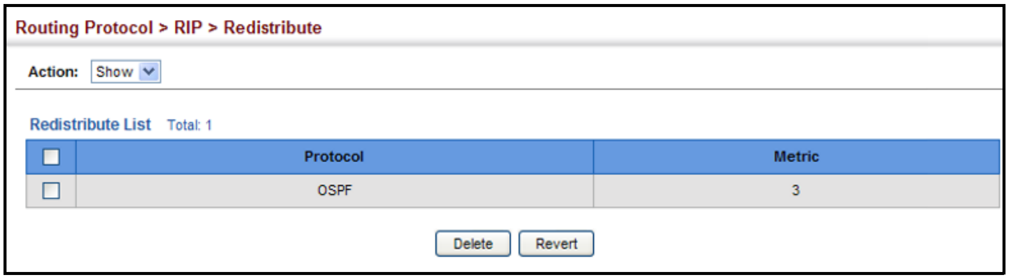
Protocol: OSPF

Metric (1-16): 3 (Optional)

To show external routes imported into RIP:

1. Click Routing Protocol, RIP, Redistribute.
2. Select Show from the Action list.

Figure 476: Showing External Routes Redistributed into RIP



Routing Protocol > RIP > Redistribute

Redistribute List Total: 1

□	Protocol	Metric
□	OSPF	3

SPECIFYING AN ADMINISTRATIVE DISTANCE

Use the Routing Protocol > RIP > Distance (Add) page to define an administrative distance for external routes learned from other routing protocols.

CLI REFERENCES

- "distance" on page 1736

COMMAND USAGE

- Administrative distance is used by the routers to select the preferred path when there are two or more different routes to the same destination from two different routing protocols. A smaller administrative distance indicates a more reliable protocol.

- The administrative distance is applied to all routes learned for the specified network.

PARAMETERS

These parameters are displayed:

- **Distance** – Administrative distance for external routes. External routes are routes for which the best path is learned from a neighbor external to the local RIP autonomous system. Routes with a distance of 255 are not installed in the routing table. (Range: 1-255)

- **IP Address** – IP address of a route entry.

- **Subnet Mask** – This mask identifies the host address bits used for associated routing entries.

WEB INTERFACE

To define an administrative distance for external routes learned from other routing protocols:

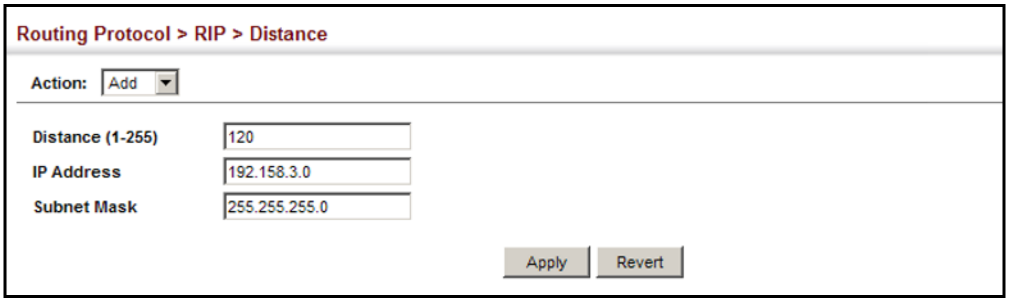
1. Click Routing Protocol, RIP, Distance.

2. Select Add from the Action list.

3. Enter the distance, the external route, and optionally enter the name of an ACL to filter networks according to the IP address of the router supplying the routing information.

4. Click Apply.

Figure 477: Setting the Distance Assigned to External Routes



Routing Protocol > RIP > Distance

Action: Add

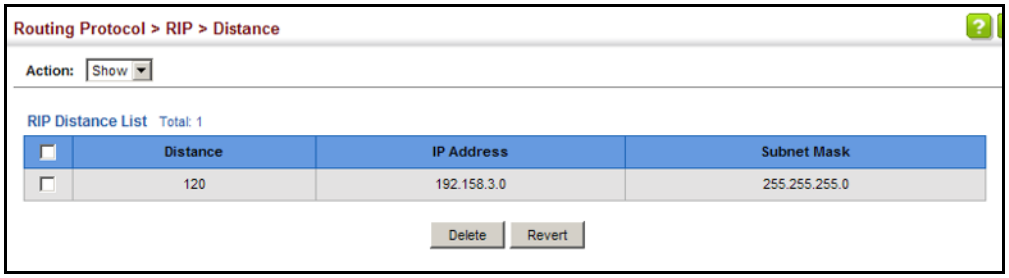
Distance (1-255): 120
IP Address: 192.158.3.0
Subnet Mask: 255.255.255.0

To show the distance assigned to external routes learned from other routing protocols:

1. Click Routing Protocol, RIP, Distance.

2. Select Show from the Action list.

Figure 478: Showing the Distance Assigned to External Routes



Routing Protocol > RIP > Distance

Action: Show

RIP Distance List Total: 1

□	Distance	IP Address	Subnet Mask
□	120	192.158.3.0	255.255.255.0

CONFIGURING NETWORK INTERFACES FOR RIP

Use the Routing Protocol > RIP > Distance (Add) page to configure the send/receive version, authentication settings, and the loopback prevention method for each interface that participates in the RIP routing process.

CLI REFERENCES

- "ip rip receive version" on page 1744
- "ip rip send version" on page 1745
- "ip rip authentication mode" on page 1742
- "ip rip authentication string" on page 1743
- "ip rip split-horizon" on page 1747

COMMAND USAGE

Specifying Receive and Send Protocol Types

- Specify the protocol message type accepted (that is, RIP version) and the message type sent (that is, RIP version or compatibility mode) for each RIP interface.

- Setting the RIP Receive Version or Send Version for an interface overrides the global setting specified in the RIP General Settings screen (see "Configuring General Protocol Settings" on page 771).

- The Send Version can be specified based on these options:
  - Use “RIPv1” or “RIPv2” if all routers in the local network are based on RIPv1 or RIPv2, respectively.
  - Use “RIPv1 Compatible” to propagate route information by broadcasting to other routers on the network using the RIPv2 advertisement list, instead of multicasting as normally required by RIPv2. (Using this mode allows older RIPv2 routers which only receive RIP broadcast messages to receive all of the information provided by RIPv2, including subnet mask, next hop and authentication information. (This is the default setting.)
  - Use “Do Not Send” to passively monitor route information advertised by other routers attached to the network.
- The Receive Version can be specified based on these options:
  - Use “RIPv1” or “RIPv2” if all routers in the local network are based on RIPv1 or RIPv2, respectively.
  - Use “RIPv1 and RIPv2” if some routers in the local network are using RIPv2, but there are still some older routers using RIPv1. (This is the default setting.)
  - Use “Do Not Receive” if dynamic entries are not required to be added to the routing table for an interface. (For example, when only static routes are to be allowed for a specific interface.)

Protocol Message Authentication

RIPv1 is not a secure protocol. Any device sending protocol messages from UDP port 520 will be considered a router by its neighbors. Malicious or unwanted protocol messages can be easily propagated throughout the network if no authentication is required.

RIPv2 supports authentication using a simple password or MD5 key encryption. When a router is configured to exchange authentication messages, it will insert the password into all transmitted protocol packets, and check all received packets to ensure that they contain the authorized password. If any incoming protocol messages do not contain the correct password, they are simply dropped.

For authentication to function properly, both the sending and receiving interface must be configured with the same password or authentication key.

Loopback Prevention

Just as Layer 2 switches use the Spanning Tree Algorithm to prevent loops, routers also use methods for preventing loops that would cause endless retransmission of data traffic. When protocol packets are caught in a loop, links will be congested, and protocol packets may be lost. However, the network will slowly converge to the new state. RIP supports several methods which can provide faster convergence when the network topology changes and prevent most loops from occurring.

PARAMETERS

These parameters are displayed:

- **VLAN ID** – Layer 3 VLAN interface. This interface must be configured with an IP address and have an active link. (Range: 1-4094)
- **Send Version** – The RIP version to send on an interface.
  - **RIPv1**: Sends only RIPv1 packets.
  - **RIPv2**: Sends only RIPv2 packets.
  - **RIPv1 Compatible**: Route information is broadcast to other routers with RIPv2.
  - **Do Not Send**: Does not transmit RIP updates. Passively monitors route information advertised by other routers attached to the network.

  The default depends on the setting for the Global RIP Version. (See "Configuring General Protocol Settings" on page 771.)
- **Receive Version** – The RIP version to receive on an interface.
  - **RIPv1**: Accepts only RIPv1 packets.
  - **RIPv2**: Accepts only RIPv2 packets.
  - **RIPv1 and RIPv2**: Accepts RIPv1 and RIPv2 packets.
  - **Do Not Receive**: Does not accept incoming RIP packets. This option does not add any dynamic entries to the routing table for an interface.

  The default depends on the setting for the Global RIP Version. (See "Configuring General Protocol Settings" on page 771.)
- **Authentication Type** – Specifies the type of authentication required for exchanging RIPv2 protocol messages. (Default: No Authentication)
  - **No Authentication**: No authentication is required.
  - **Simple Password**: Requires the interface to exchange routing information with other routers based on an authorized password. (Note that authentication only applies to RIPv2.)
  - **MD5**: Message Digest 5 (MD5) authentication.

    MD5 is a one-way hash algorithm is that takes the authentication key and produces a 128 bit message digest or “fingerprint.” This makes it computationally infeasible to produce two messages having the same message digest, or to produce any message having a given pre-specified target message digest.

- **Authentication Key** – Specifies the key to use for authenticating RIPv2 packets. For authentication to function properly, both the sending and receiving interface must use the same password. (Range: 1-16 characters, case sensitive)

- **Instability Prevention** – Specifies the method used to reduce the convergence time when the network topology changes, and to prevent RIP protocol messages from looping back to the source router.

  - **Split Horizon** – This method never propagate routes back to an interface from which they have been acquired.

  - **Poison Reverse** – This method propagates routes back to an interface from which they have been acquired, but sets the distance-vector metrics to infinity. This provides faster convergence. (This is the default setting.)

  - **None** – No loopback prevention method is employed. If a loop occurs without using any prevention method, the hop count for a route may be gradually incremented to infinity (that is, 16) before the route is deemed unreachable.

WEB INTERFACE

To network interface settings for RIP:

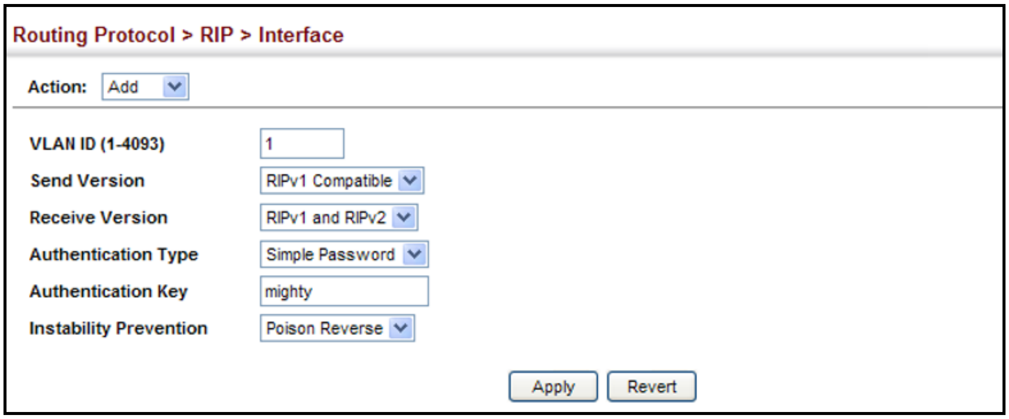
1. Click Routing Protocol, RIP, Interface.

2. Select Add from the Action list.

3. Select a Layer 3 VLAN interface to participate in RIP. Select the RIP protocol message types that will be received and sent. Select the RIP authentication method and password. And then set the loopback prevention method.

4. Click Apply.

Figure 479: Configuring a Network Interface for RIP



Routing Protocol > RIP > Interface

Action: Add

VLAN ID (1-4093): 1

Send Version: RIPv1 Compatible

Receive Version: RIPv1 and RIPv2

Authentication Type: Simple Password

Authentication Key: mighty

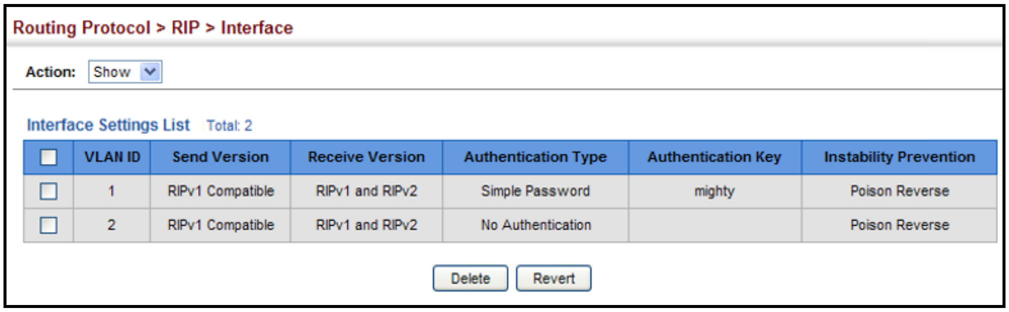
Instability Prevention: Poison Reverse

To show the network interface settings configured for RIP:

1. Click Routing Protocol, RIP, Interface.

2. Select Show from the Action list.

Figure 480: Showing RIP Network Interface Settings



Routing Protocol > RIP > Interface

Action: Show

Interface Settings List Total: 2

□	VLAN ID	Send Version	Receive Version	Authentication Type	Authentication Key	Instability Prevention
□	1	RIPv1 Compatible	RIPv1 and RIPv2	Simple Password	mighty	Poison Reverse
□	2	RIPv1 Compatible	RIPv1 and RIPv2	No Authentication		Poison Reverse

DISPLAYING RIP INTERFACE SETTINGS

Use the Routing Protocol > RIP > Statistics (Show Interface Information) page to display information about RIP interface configuration settings.

CLI REFERENCES

- "show ip rip" on page 1749

PARAMETERS

These parameters are displayed:

- **Interface** – Source IP address of RIP router interface.
- **Auth Type** – The type of authentication used for exchanging RIPv2 protocol messages.
- **Send Version** – The RIP version to sent on this interface.
- **Receive Version** – The RIP version accepted on this interface.
- **Rcv Bad Packets** – Number of bad RIP packets received.
- **Rcv Bad Routes** – Number of bad routes received.
- **Send Updates** – Number of route changes.

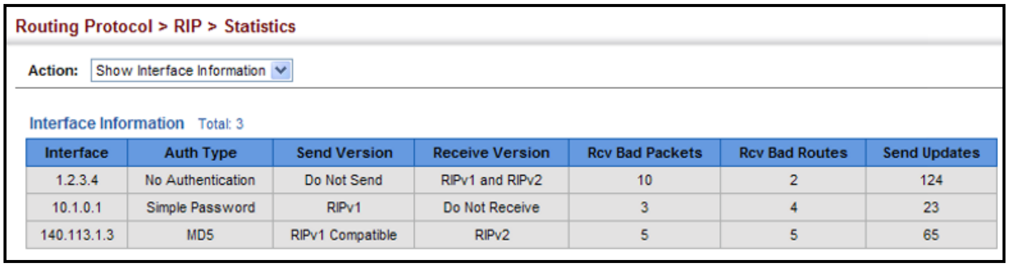
WEB INTERFACE

To display RIP interface configuration settings:

1. Click Routing Protocol, RIP, Statistics.

2. Select Show Interface Information from the Action list.

Figure 481: Showing RIP Interface Settings



Routing Protocol > RIP > Statistics

Action: Show Interface Information

Interface Information Total: 3

Interface	Auth Type	Send Version	Receive Version	Rcv Bad Packets	Rcv Bad Routes	Send Updates
1.2.3.4	No Authentication	Do Not Send	RIPv1 and RIPv2	10	2	124
10.1.0.1	Simple Password	RIPv1	Do Not Receive	3	4	23
140.113.1.3	MD5	RIPv1 Compatible	RIPv2	5	5	65

DISPLAYING PEER ROUTER INFORMATION

Use the Routing Protocol > RIP > Statistics (Show Peer Information) page to display information on neighboring RIP routers.

CLI REFERENCES

- "show ip protocols rip" on page 1748

PARAMETERS

These parameters are displayed:

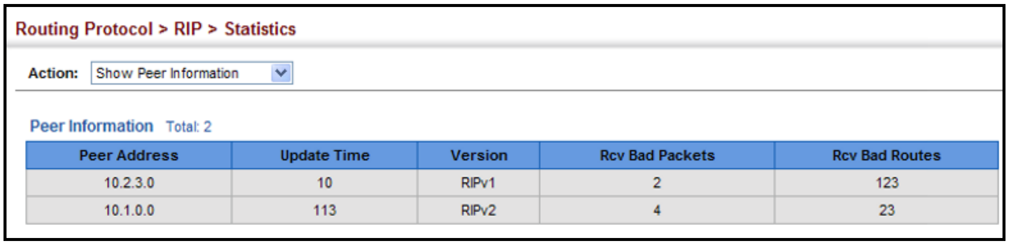
- **Peer Address** – IP address of a neighboring RIP router.
- **Update Time** – Last time a route update was received from this peer.
- **Version** – Shows whether RIPv1 or RIPv2 packets were received from this peer.
- **Rcv Bad Packets** – Number of bad RIP packets received from this peer.
- **Rcv Bad Routes** – Number of bad routes received from this peer.

WEB INTERFACE

To display information on neighboring RIP routers:

1. Click Routing Protocol, RIP, Statistics.
2. Select Show Peer Information from the Action list.

Figure 482: Showing RIP Peer Information



Routing Protocol > RIP > Statistics

Action: Show Peer Information

Peer Information Total: 2

Peer Address	Update Time	Version	Rcv Bad Packets	Rcv Bad Routes
10.2.3.0	10	RIPv1	2	123
10.1.0.0	113	RIPv2	4	23

RESETTING RIP STATISTICS

Use the Routing Protocol > RIP > Statistics (Reset Statistics) page to reset all statistics for RIP protocol messages.

CLI REFERENCES

- ◆ no comparable command

WEB INTERFACE

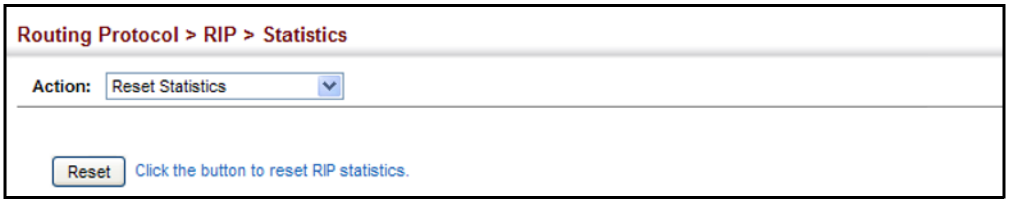
To reset RIP statistics:

1. Click Routing Protocol, RIP, Statistics.

2. Select Reset Statistics from the Action list.

3. Click Reset.

Figure 483: Resetting RIP Statistics



Routing Protocol > RIP > Statistics

Action: Reset Statistics

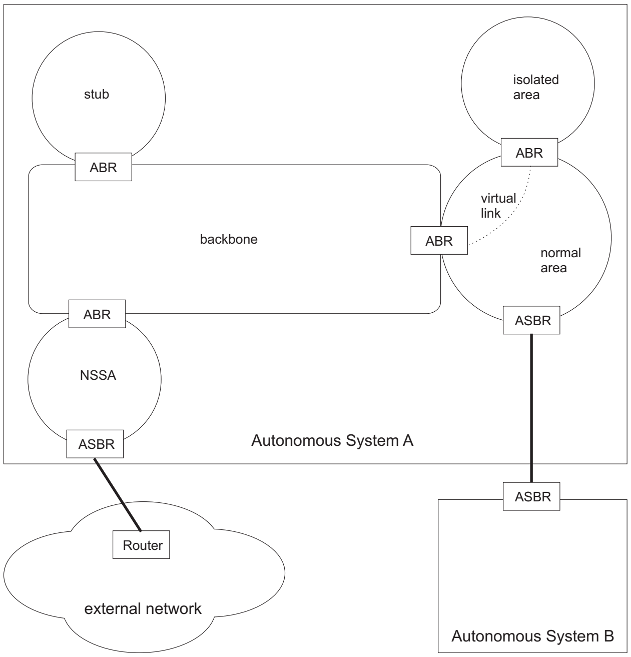
Reset Click the button to reset RIP statistics.

CONFIGURING THE OPEN SHORTEST PATH FIRST PROTOCOL (VERSION 2)

Open Shortest Path First (OSPF) is more suited for large area networks which experience frequent changes in the links. It also handles subnets much better than RIP. OSPF protocol actively tests the status of each link to its neighbors to generate a shortest path tree, and builds a routing table based on this information. OSPF then utilizes IP multicast to propagate routing information. A separate routing area scheme is also used to further reduce the amount of routing traffic.

NOTE: The OSPF protocol implemented in this device is based on RFC 2328 (Version 2). It also supports RFC 1583 (early Version 2) compatibility mode to ensure that the same method is used to calculate summary route costs throughout the network when older OSPF routers exist; as well as the not-so-stubby area option (RFC 3101).

Figure 484: Configuring OSPF



COMMAND USAGE

- OSPF looks at more than just the simple hop count. When adding the shortest path to any node into the tree, the optimal path is chosen on the basis of delay, throughput and connectivity. OSPF utilizes IP multicast to reduce the amount of routing traffic required when sending or receiving routing path updates. The separate routing area scheme used by OSPF further reduces the amount of routing traffic, and thus inherently provides another level of routing protection. In addition, all routing protocol exchanges can be authenticated. Finally, the OSPF algorithms have been tailored for efficient operation in TCP/IP Internets.

- OSPFv2 is a compatible upgrade to OSPF. It involves enhancements to protocol message authentication, and the addition of a point-to-multipoint interface which allows OSPF to run over non-broadcast networks, as well as support for overlapping area ranges.

- When using OSPF, you must organize your network (i.e., autonomous system) into normal, stub, or not-so-stubby areas; configure the ranges of subnet addresses that can be aggregated by link state advertisements; and configure virtual links for areas that do not have direct physical access to the OSFP backbone.

  - To implement OSPF for a large network, you must first organize the network into logical areas to limit the number of OSPF routers that actively exchange Link State Advertisements (LSAs). You can then define an OSPF interface by assigning an IP interface configured on this router to one of these areas. This OSPF interface will send and receive OSPF traffic to neighboring OSPF routers.

- You can further optimize the exchange of OSPF traffic by specifying an area range that covers a large number of subnetwork addresses. This is an important technique for limiting the amount of traffic exchanged between Area Border Routers (ABRs).
- And finally, you must specify a virtual link to any OSPF area that is not physically attached to the OSPF backbone. Virtual links can also be used to provide a redundant link between contiguous areas to prevent areas from being partitioned, or to merge backbone areas. (Note that virtual links are not supported for stubs or NSSAs.)

DEFINING NETWORK AREAS BASED ON ADDRESSES

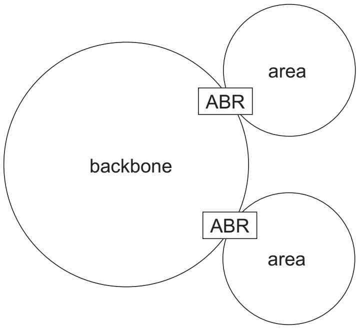
OSPF protocol broadcast messages (i.e., Link State Advertisements or LSAs) are restricted by area to limit their impact on network performance. A large network should be split up into separate OSPF areas to increase network stability, and to reduce protocol traffic by summarizing routing information into more compact messages. Each router in an area shares the same view of the network topology, including area links, route summaries for directly connected areas, and external links to other areas.

Use the Routing Protocol > OSPF > Network Area (Add) page to define an OSPF area and the interfaces that operate within this area. An autonomous system must be configured with a backbone area, designated by the area identifier 0.0.0.0. By default, all other areas are created as normal transit areas.

Routers in a normal area may import or export routing information about individual nodes. To reduce the amount of routing traffic flooded onto the network, an area can be configured to export a single summarized route that covers a broad range of network addresses within the area (page 805). To further reduce the amount of routes passed between areas, an area can be configured as a stub (page 798, page 802) or a not-so-stubby area (page 798, page 799).

Normal Area – A large OSPF domain should be broken up into several areas to increase network stability and reduce the amount of routing traffic required through the use of route summaries that aggregate a range of addresses into a single route. The backbone or any normal area can pass traffic between other areas, and are therefore known as transit areas. Each router in an area has identical routing tables. These tables may include area links, summarized links, or external links that depict the topology of the autonomous system.

Figure 485: OSPF Areas



CLI REFERENCES

- "router ospf" on page 1751
- "network area" on page 1768

COMMAND USAGE

- Specify an Area ID and the corresponding network address range for each OSPF broadcast area. Each area identifies a logical group of OSPF routers that actively exchange Link State Advertisements (LSAs) to ensure that they share an identical view of the network topology.

- Each area must be connected to a backbone area. This area passes routing information between other areas in the autonomous system. All routers must be connected to the backbone, either directly, or through a virtual link if a direct physical connection is not possible.

- All areas are created as normal transit areas using the Network Area (Add) page. A normal area (or transit area) can send and receive external LSAs. If necessary, an area can be configured as a not-so-stubby area (NSSA) that can import external route information into its area, or as a stubby area that cannot send or receive external LSAs.

- An area must be assigned a range of subnetwork addresses. This area and the corresponding address range forms a routing interface, and can be configured to aggregate LSAs from all of its subnetwork addresses and exchange this information with other routers in the network as described under "Configuring Area Ranges (Route Summarization for ABRs)" on page 805.

- If an address range overlaps other network areas, the router will use the network area with the address range that most closely matches the interface address. Also, note that if a more specific address range is removed from an area, the interface belonging to that range may still remain active if a less specific address range covering that area has been specified.

PARAMETERS

These parameters are displayed:

- **Process ID** – Protocol identifier used to distinguish between multiple routing instances. (Range: 1-65535)

- **IP Address** – Address of the interfaces to add to the area.

- **Netmask** – Network mask of the address range to add to the area.

- **Area ID** – Area to which the specified address or range is assigned. An OSPF area identifies a group of routers that share common routing information. The area ID can be in the form of an IPv4 address, or as a four octet unsigned integer ranging from 0-4294967295.

  Set the area ID to the same value for all routers on a network segment using the network mask to add one or more interfaces to an area.

WEB INTERFACE

To define an OSPF area and the interfaces that operate within this area:

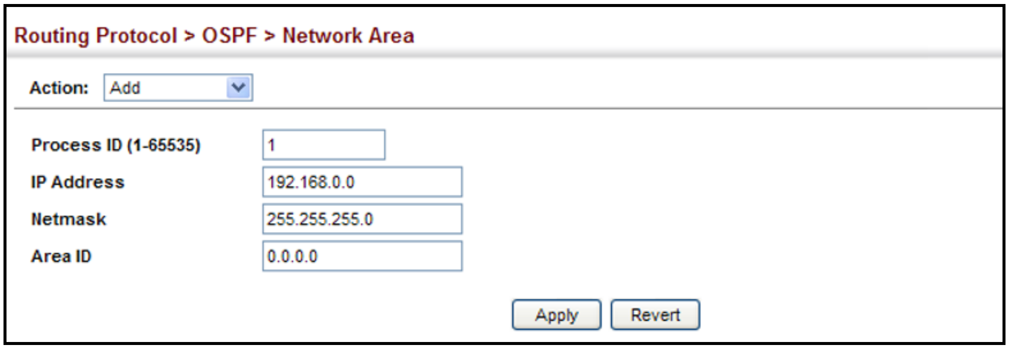
1. Click Routing Protocol, OSPF, Network Area.

2. Select Add from the Action list.

3. Configure a backbone area that is contiguous with all the other areas in the network, and configure an area for all of the other OSPF interfaces.

4. Click Apply

Figure 486: Defining OSPF Network Areas Based on Addresses



Routing Protocol > OSPF > Network Area

Action: Add

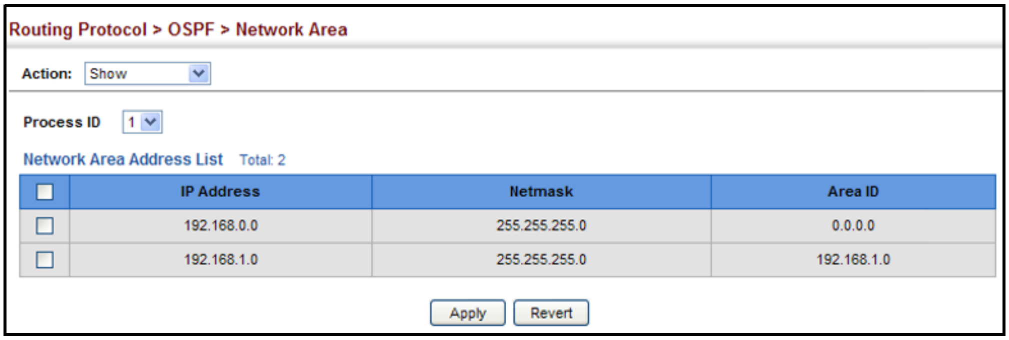
Process ID (1-65535): 1
IP Address: 192.168.0.0
Netmask: 255.255.255.0
Area ID: 0.0.0.0

To to show the OSPF areas and the assigned interfaces:

1. Click Routing Protocol, OSPF, Network Area.

2. Select Show from the Action list.

Figure 487: Showing OSPF Network Areas



Routing Protocol > OSPF > Network Area

Action: Show

Process ID: 1

Network Area Address List Total: 2

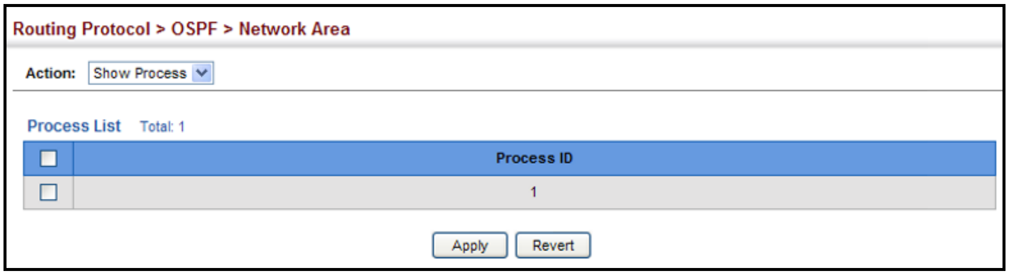
□	IP Address	Netmask	Area ID
□	192.168.0.0	255.255.255.0	0.0.0.0
□	192.168.1.0	255.255.255.0	192.168.1.0

To to show the OSPF process identifiers:

1. Click Routing Protocol, OSPF, Network Area.

2. Select Show Process from the Action list.

Figure 488: Showing OSPF Process Identifiers



Routing Protocol > OSPF > Network Area

Action: Show Process

Process List Total: 1

□	Process ID
□	1

CONFIGURING GENERAL PROTOCOL SETTINGS

To implement dynamic OSPF routing, first assign VLAN groups to each IP subnet to which this router will be attached (as described in the preceding section), then use the Routing Protocol > OSPF > System (Configure) page to assign an Router ID to this device, and set the other basic protocol parameters.

CLI REFERENCES

- "Open Shortest Path First (OSPFv2)" on page 1750

PARAMETERS

These parameters are displayed:

- **Process ID** – Protocol identifier as configured on the Routing Protocol > OSPF > Network Area (Add) page. (Range: 1-65535)

General Information

- **RFC1583 Compatible** – If one or more routers in a routing domain are using early Version 2 of OSPF, this router should use RFC 1583 (early OSPFv2) compatibility mode to ensure that all routers are using the same RFC for calculating summary route costs. Enable this field to force the router to calculate summary route costs using RFC 1583. (Default: Disabled)

  When RFC 1583 compatibility is enabled, only cost is used when choosing among multiple AS-external LSAs advertising the same destination. When disabled, preference is based on type of path, using cost only to break ties (see RFC 2328).

  If there any OSPF routers in an area exchanging summary information (specifically, ABRs) which have not been upgraded to OSPFv2 (RFC 2328), RFC 1583 should be used on the newly upgraded OSPFv2 routers to ensure compatibility with routers still running older OSPFv2 code.

- **OSPF Router ID** – Assigns a unique router ID for this device within the autonomous system for the current OSPF process.

  The router ID must be unique for every router in the autonomous system. Note that the router ID cannot be set to 0.0.0.0.

  If this router already has registered neighbors, the new router ID will be used when the router is rebooted, or manually restarted using the no router ospf command followed by the router ospf command.

- **Auto Cost** – Calculates the cost for an interface by dividing the reference bandwidth by the interface bandwidth. The reference bandwidth is defined in Mbits per second. (Range: 1-4294967)

  By default, the cost is 0.1 for Gigabit ports, and 0.01 for 10 Gigabit ports. A higher reference bandwidth can be used for aggregate links to indicate preferred use as a lower cost interface.

- **SPF Hold Time** – The hold time between making two consecutive shortest path first (SPF) calculations. (Range: 0-65535 seconds; Default: 10 seconds)

  Setting the SPF holdtime to 0 means that there is no delay between consecutive calculations.

- **SPF Delay Time** – The delay after receiving a topology change notification and starting the SPF calculation. (Range: 0-65535 seconds; Default: 5 seconds)

  Using a low value for the delay and hold time allows the router to switch to a new path faster, but uses more CPU processing time.

- **Default Metric** – The default metric for external routes imported from other protocols. (Range: 0-16777214; Default: 20)

  A default metric must be used to resolve the problem of redistributing external routes from other protocols that use incompatible metrics.

  This default metric does not override the metric value set on the Redistribute configuration screen (see page 807). When a metric value has not been configured on the Redistribute page, the default metric configured on the System configuration page sets the metric value to be used for all imported external routes.

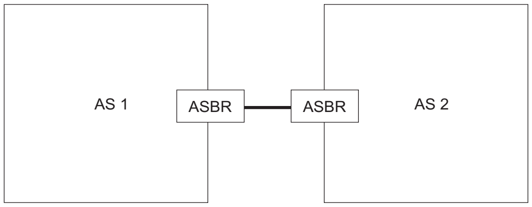
Default Information

- **Originate Default Route**[14] – Generates a default external route into an autonomous system. Note that the **Advertise Default Route** field must also be properly configured. (Default: Disabled)

  When this feature is used to redistribute routes into a routing domain (that is, an Autonomous System), this router automatically becomes an Autonomous System Boundary Router (ASBR). This allows the router to exchange routing information with boundary routers in other autonomous systems to which it may be attached. If a router is functioning as an ASBR, then every other router in the autonomous system can learn about external routes from this device.

[14] These are configured with the default-information originate command.

Figure 489: AS Boundary Router



- **Advertise Default Route**[14] – The router can advertise a default external route into the autonomous system (AS). (Options: Not Always, Always; Default: Not Always)

  - **Always** – The router will advertise itself as a default external route for the local AS, even if a default external route does not actually exist. (To define a default route, see "Configuring Static Routes" on page 753.)

  - **NotAlways** – It can only advertise a default external route into the AS if it has been configured to import external routes through RIP or static routes, and such a route is known. (See "Redistributing External Routes" on page 807.)

- **External Metric Type**[14] – The external link type used to advertise the default route. Type 1 route advertisements add the internal cost to the external route metric. Type 2 routes do not add the internal cost metric. When comparing Type 2 routes, the internal cost is only used as a tie-breaker if several Type 2 routes have the same cost. (Default: Type 2)

- **Default External Metric**[14] – Metric assigned to the default route. (Range: 0-16777215; Default: 20)

  The metric for the default external route is used to calculate the path cost for traffic passed from other routers within the AS out through the ASBR.

  Redistribution of routing information from other protocols is controlled by the Redistribute function (see page 807).

WEB INTERFACE

To configure general settings for OSPF:

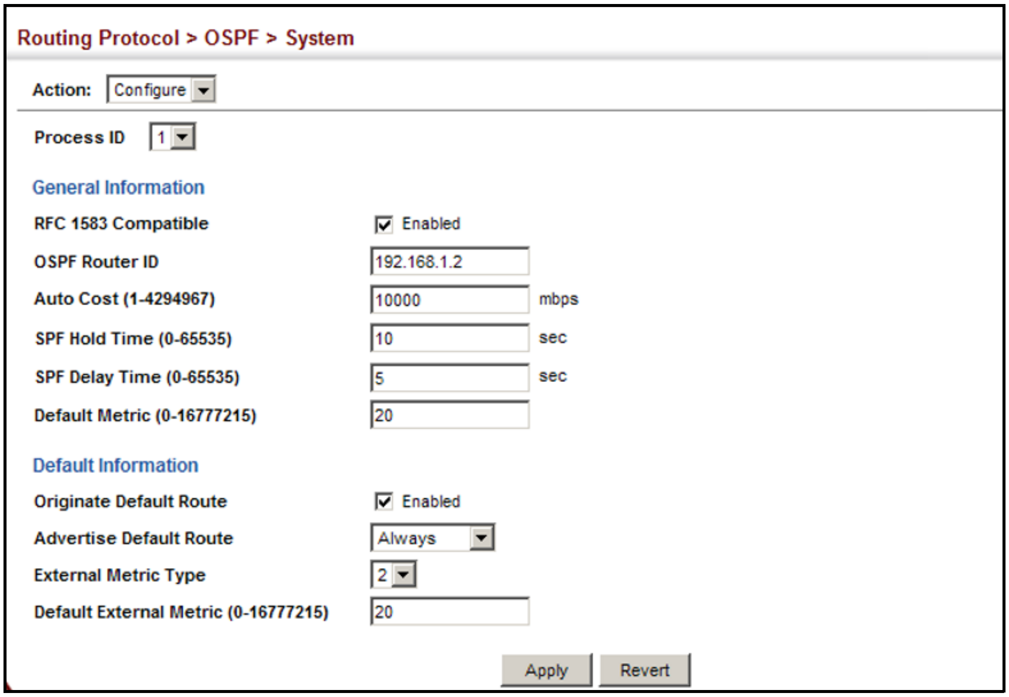
1. Click Routing Protocol, OSPF, System.

2. Select Configure from the Action list.

3. Select a Process ID, and then specify the Router ID and other global attributes as required. For example, by setting the Auto Cost to 10000, the cost of using an interface is set to 10 for Gigabit ports, and 1 for 10 Gigabit ports.

4. Click Apply

Figure 490: Configure General Settings for OSPF



Routing Protocol > OSPF > System

Action: Configure

Process ID 1

General Information

RFC 1583 Compatible	☑ Enabled
OSPF Router ID	192.168.1.2
Auto Cost (1-4294967)	10000 mbps
SPF Hold Time (0-65535)	10 sec
SPF Delay Time (0-65535)	5 sec
Default Metric (0-16777215)	20

Default Information

Originate Default Route	☑ Enabled
Advertise Default Route	Always
External Metric Type	2
Default External Metric (0-16777215)	20

Displaying Administrative Settings and Statistics

Use the Routing Protocol > OSPF > System (Show) page to display general administrative settings and statistics for OSPF.

CLI References

- "show ip ospf" on page 1777
- "show ip protocols ospf" on page 1790

Parameters

These parameters are displayed:

Table 53: OSPF System Information

Parameter	Description
Router ID Type	Indicates if the router ID was manually configured or automatically generated by the system.
Rx LSAs	The number of link-state advertisements that have been received.
Originate LSAs	The number of new link-state advertisements that have been originated.
AS LSA Count	The number of autonomous system LSAs in the link-state database.
External LSA Count	The number of external link-state advertisements in the link-state database.
External LSA Checksum	Checksum of the external link-state advertisement database.
Admin Status	Indicates if there are one or more configured OSPF areas with an active interface (that is, a Layer 3 interface that is enabled and up).

Table 53: OSPF System Information (Continued)

Parameter	Description
ABR Status (Area Border Router)	Indicates if this router connects directly to networks in two or more areas. An area border router runs a separate copy of the Shortest Path First algorithm, maintaining a separate routing database for each area.
ASBR Status (Autonomous System Boundary Router)	Indicates if this router exchanges routing information with boundary routers in other autonomous systems to which it may be attached. If a router is enabled as an ASBR, then every other router in the autonomous system can learn about external routes from this device.
Restart Status	Indicates if the OSPF process is in graceful-restart state.
Area Number	The number of configured areas attached to this router.
Version Number	The OSPF version number. The OSPF protocol implemented in this device is based on RFC 2328 (Version 2). It also supports RFC 1583 (early Version 2) compatibility mode.

WEB INTERFACE

To show administrative settings and statistics for OSPF:

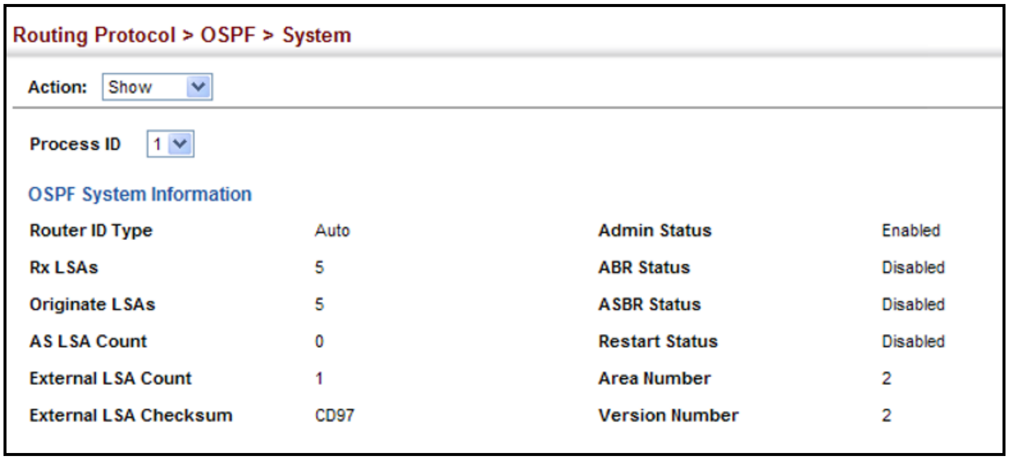
To display general settings for OSPF:

1. Click Routing Protocol, OSPF, System.

2. Select Show from the Action list.

3. Select a Process ID.

Figure 491: Showing General Settings for OSPF



Routing Protocol > OSPF > System

Action: Show

Process ID 1

OSPF System Information

Router ID Type	Auto	Admin Status	Enabled
Rx LSAs	5	ABR Status	Disabled
Originate LSAs	5	ASBR Status	Disabled
AS LSA Count	0	Restart Status	Disabled
External LSA Count	1	Area Number	2
External LSA Checksum	CD97	Version Number	2

ADDING AN NSSA OR STUB

Use the Routing Protocol > OSPF > Area (Configure Area – Add Area) page to add a not-so-stubby area (NSSA) or a stubby area (Stub).

CLI REFERENCES

- "router ospf" on page 1751
- "area stub" on page 1764
- "area nssa" on page 1762

COMMAND USAGE

- This router supports up to 5 stubs or NSSAs.

PARAMETERS

These parameters are displayed:

- **Process ID** – Protocol identifier as configured on the Routing Protocol > OSPF > Network Area (Add) page. (Range: 1-65535)
- **Area ID** – Identifier for a not-so-stubby area (NSSA) or stub. The area ID can be in the form of an IPv4 address, or as a four octet unsigned integer ranging from 0-4294967295.

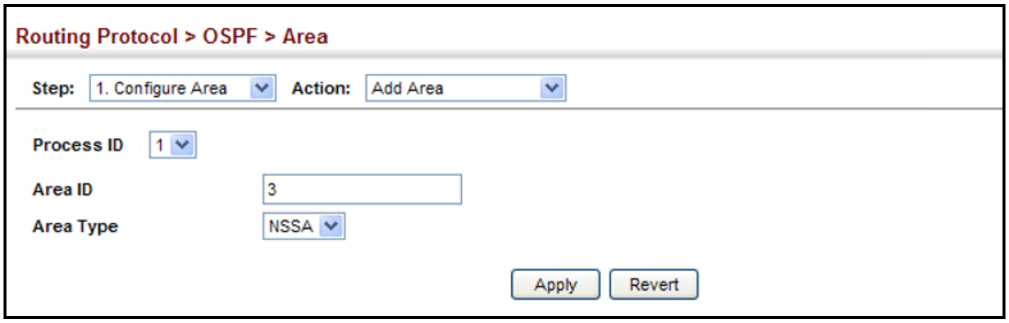
  Set the area ID to the same value for all routers on a network segment using the network mask to add one or more interfaces to an area.
- **Area Type** – Specifies an NSSA or stub.

WEB INTERFACE

To add an NSSA or stub to the OSPF administrative domain:

1. Click Routing Protocol, OSPF, Area.
2. Select Configure Area from the Step list.
3. Select Add Area from the Action list.
4. Select a Process ID, enter the area identifier, and set the area type to NSSA or Stub.
5. Click Apply

Figure 492: Adding an NSSA or Stub



Routing Protocol > OSPF > Area

Step: 1. Configure Area Action: Add Area

Process ID 1

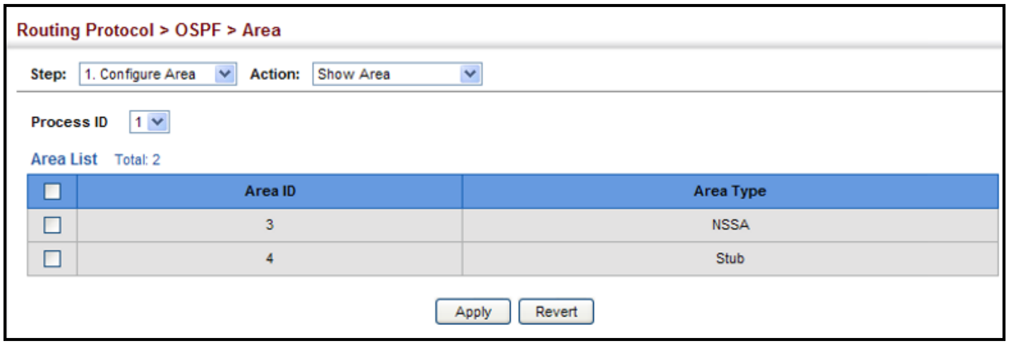
Area ID 3

Area Type NSSA

To show the NSSA or stubs added to the specified OSPF domain:

1. Click Routing Protocol, OSPF, Area.
2. Select Configure Area from the Step list.
3. Select Show Area from the Action list.
4. Select a Process ID.

Figure 493: Showing NSSAs or Stubs



Routing Protocol > OSPF > Area

Step: 1. Configure Area Action: Show Area

Process ID 1

Area List Total: 2

□	Area ID	Area Type
□	3	NSSA
□	4	Stub

CONFIGURING NSSA SETTINGS

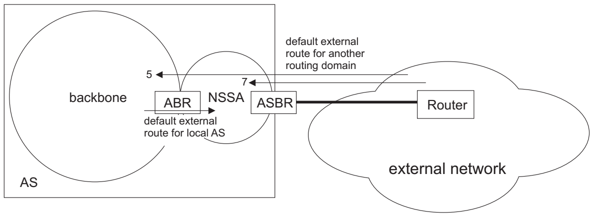
Use the Routing Protocol > OSPF > Area (Configure Area – Configure NSSA Area) page to configure protocol settings for a not-so-stubby area (NSSA).

An NSSA can be configured to control the use of default routes for Area Border Routers (ABRs) and Autonomous System Boundary Routers (ASBRs), or external routes learned from other routing domains and imported through an ABR.

An NSSA is similar to a stub. It blocks most external routing information, and can be configured to advertise a single default route for traffic passing between the NSSA and other areas within the autonomous system (AS) when the router is an ABR.

An NSSA can also import external routes from one or more small routing domains that are not part of the AS, such as a RIP domain or locally configured static routes. This external AS routing information is generated by the NSSA's ASBR and advertised only within the NSSA. By default, these routes are not flooded onto the backbone or into any other area by ABRs. However, the NSSA's ABRs will convert NSSA external LSAs (Type 7) into external LSAs (Type-5) which are propagated into other areas within the AS.

Figure 494: OSPF NSSA



CLI REFERENCES

- "router ospf" on page 1751
- "area default-cost" on page 1756
- "area nssa" on page 1762

COMMAND USAGE

- Before creating an NSSA, first specify the address range for the area (see "Defining Network Areas Based on Addresses" on page 790). Then create an NSSA as described under "Adding an NSSA or Stub" on page 798.
- NSSAs cannot be used as a transit area, and should therefore be placed at the edge of the routing domain.
- An NSSA can have multiple ABRs or exit points. However, all of the exit points and local routers must contain the same external routing data so that the exit point does not need to be determined for each external destination.
- There are no external routes in an OSPF stub area, so routes cannot be redistributed from another protocol into a stub area. On the other hand, an NSSA allows external routes from another protocol to be redistributed into its own area, and then leaked to adjacent areas.
- Routes that can be advertised with NSSA external LSAs include network destinations outside the AS learned through OSPF, the default route, static routes, routes derived from other routing protocols such as RIP, or directly connected networks that are not running OSPF.
- An NSSA can be used to simplify administration when connecting a central site using OSPF to a remote site that is using a different routing protocol. OSPF can be easily extended to cover the remote connection by defining the area between the central router and the remote router as an NSSA.

PARAMETERS

These parameters are displayed:

- **Process ID** – Process ID as configured in the Network Area configuration screen (see page 790).
- **Area ID** – Identifier for a not-so-stubby area (NSSA).
- **Translator Role** – Indicates NSSA-ABR translator role for converting Type 7 external LSAs into Type 5 external LSAs. These roles include:
  - **Never** – A router that never translates NSSA LSAs to Type-5 external LSAs.
  - **Always** – A router that always translates NSSA LSA to Type-5 external LSA.
  - **Candidate** – A router translates NSSA LSAs to Type-5 external LSAs if elected.

- **Redistribute** – Disable this option when the router is an NSSA Area Border Router (ABR) and routes only need to be imported into normal areas (see "Redistributing External Routes" on page 807), but not into the NSSA. In other words, redistribution should be disabled to prevent the NSSA ABR from advertising external routing information (learned through routers in other areas) into the NSSA. (Default: Enabled)

- **Originate Default Information** – When the router is an NSSA Area Border Router (ABR) or an NSSA Autonomous System Boundary Router (ASBR), this option causes it to generate a Type-7 default LSA into the NSSA. This default provides a route to other areas within the AS for an NSSA ABR, or to areas outside the AS for an NSSA ASBR.
  (Default: Disabled)

  An NSSA is similar to a stub, because when the router is an ABR, it can send a default route for other areas in the AS into the NSSA using the Originate Default Information option. However, an NSSA is different from a stub, because when the router is an ASBR, it can import a default external AS route (for routing protocol domains adjacent to the NSSA but not within the OSPF AS) into the NSSA using this option.

- **Metric Type** – Type 1 or Type 2 external routes. When using Type 2, routers do not add internal cost to the external route metric.
  (Default: Type 2)

- **Metric** – Metric assigned to Type-7 default LSAs. (Range: 0-16777214; Default: 1)

- **Default Cost** – Cost for the default summary route sent into an NSSA from an area border router (ABR). (Range: 0-16777215; Default: 0)

  Note that when the default cost is set to “0,” the router will not advertise a default route into the attached NSSA.

- **Summary** – Controls the use of summary routes. (Default: Summary)

  - **Summary** – Unlike stub areas, all Type-3 summary LSAs will be imported into NSSAs to ensure that internal routes are always chosen over Type-7 NSSA external routes.

  - **No Summary** – Allows an area to retain standard NSSA features, but does not inject inter-area routes (Type-3 and Type-4 summary routes) into this area. Instead, it advertises a default route as a Type-3 LSA.

WEB INTERFACE

To configure protocol settings for an NSSA:

1. Click Routing Protocol, OSPF, Area.

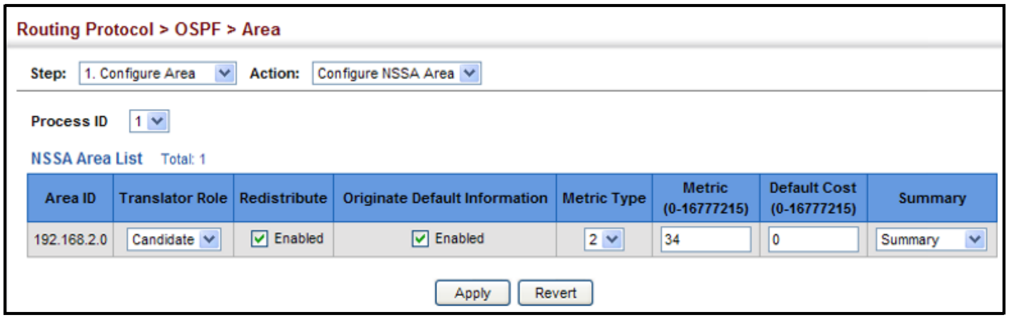
2. Select Configure Area from the Step list.

3. Select Configure NSSA Area from the Action list.

4. Select a Process ID, and modify the routing behavior for an NSSA.

5. Click Apply

Figure 495: Configuring Protocol Settings for an NSSA



Routing Protocol > OSPF > Area

Step: 1. Configure Area Action: Configure NSSA Area

Process ID 1

NSSA Area List Total: 1

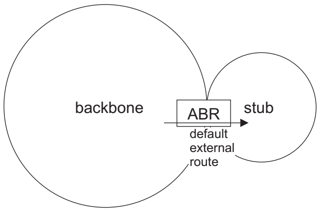
Area ID	Translator Role	Redistribute	Originate Default Information	Metric Type	Metric (0-16777215)	Default Cost (0-16777215)	Summary
192.168.2.0	Candidate	☑ Enabled	☑ Enabled	2	34	0	Summary

CONFIGURING STUB SETTINGS

Use the Routing Protocol > OSPF > Area (Configure Area – Configure Stub Area) page to configure protocol settings for a stub.

A stub does not accept external routing information. Instead, an area border router adjacent to a stub can be configured to send a default external route into the stub for all destinations outside the local area or the autonomous system. This route will also be advertised as a single entry point for traffic entering the stub. Using a stub can significantly reduce the amount of topology data that has to be exchanged over the network.

Figure 496: OSPF Stub Area



By default, a stub can only pass traffic to other areas in the autonomous system through the default external route. However, an area border router can also be configured to send Type 3 summary link advertisements into the stub about subnetworks located elsewhere in the autonomous system.

CLI REFERENCES

- "router ospf" on page 1751
- "area default-cost" on page 1756
- "area stub" on page 1764

COMMAND USAGE

- Before creating a stub, first specify the address range for the area (see "Defining Network Areas Based on Addresses" on page 790). Then create a stub as described under "Adding an NSSA or Stub" on page 798.

- Stubs cannot be used as a transit area, and should therefore be placed at the edge of the routing domain.

- A stub can have multiple ABRs or exit points. However, all of the exit points and local routers must contain the same external routing data so that the exit point does not need to be determined for each external destination.

PARAMETERS

These parameters are displayed:

- **Process ID** – Process ID as configured in the Network Area configuration screen (see page 790).
- **Area ID** – Identifier for a stub.
- **Default Cost** – Cost for the default summary route sent into a stub from an area border router (ABR). (Range: 0-16777215; Default: 0)

  Note that he the default cost is set to "0," the router will not advertise a default route into the attached stub.
- **Summary** – Controls the use of summary routes.
  - **Summary** – Allows an Area Border Router (ABR) to send a summary link advertisement into the stub area.
  - **No Summary** – Stops an ABR from sending a summary link advertisement into a stub area.

    Routing table space is saved in a stub by blocking Type-4 AS summary LSAs and Type 5 external LSAs. This option can be used to completely isolate the stub by also stopping an ABR from sending Type-3 summary LSAs that advertise the default route for destinations external to the local area or the autonomous system.

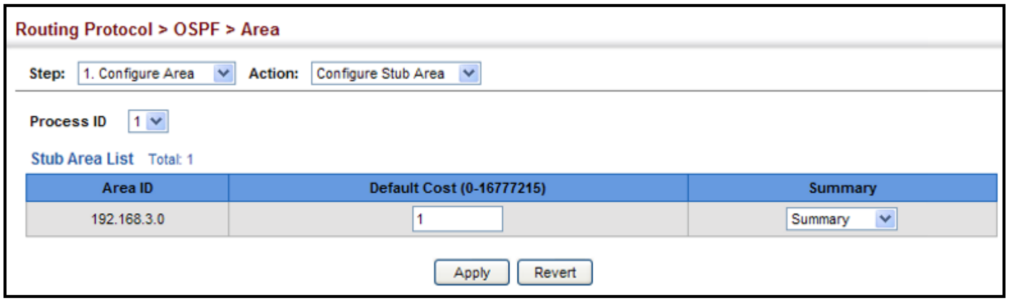
    Define an area as a totally stubby area only if routers in the area do not require summary LSAs from other areas.

WEB INTERFACE

To configure protocol settings for a stub:

1. Click Routing Protocol, OSPF, Area.
2. Select Configure Area from the Step list.
3. Select Configure Stub Area from the Action list.
4. Select a Process ID, and modify the routing behavior for a stub.
5. Click Apply

Figure 497: Configuring Protocol Settings for a Stub



Routing Protocol > OSPF > Area

Step: 1. Configure Area Action: Configure Stub Area

Process ID 1

Stub Area List Total: 1

Area ID	Default Cost (0-16777215)	Summary
192.168.3.0	1	Summary

Displaying Information on NSSA and Stub Areas

Use the Routing Protocol > OSPF > Area (Show Information) page to protocol information on NSSA and Stub areas.

CLI References

- "show ip ospf" on page 1777

Parameters

These parameters are displayed:

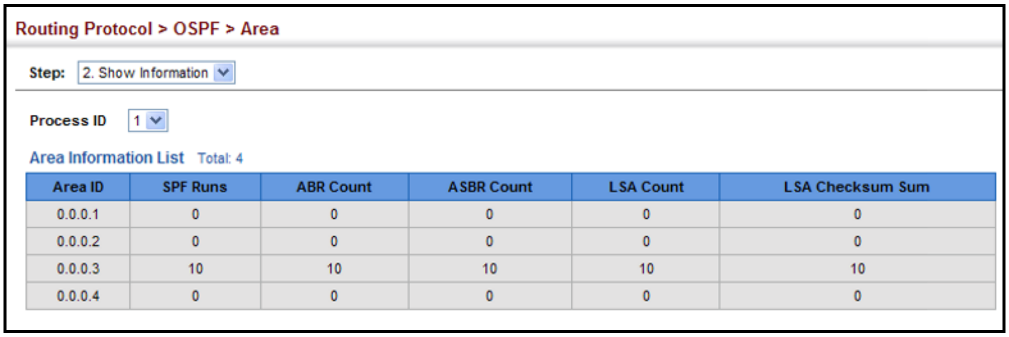
- **Process ID** – Process ID as configured in the Network Area configuration screen (see page 790).
- **Area ID** – Identifier for a not-so-stubby area (NSSA) or stub.
- **SPF Runs** – The number of times the Shortest Path First algorithm has been run for this area.
- **ABR Count** – The number of Area Border Routers attached to this area.
- **ASBR Count** – The number of Autonomous System Boundary Routers attached to this area.
- **LSA Count** – The number of new link-state advertisements that have been originated.
- **LSA Checksum Sum** – The sum of the link-state advertisements' LS checksums contained in this area's link-state database.

Web Interface

To display information on NSSA and stub areas:

1. Click Routing Protocol, OSPF, Area.
2. Select Show Information from the Action list.
3. Select a Process ID.

Figure 498: Displaying Information on NSSA and Stub Areas



Routing Protocol > OSPF > Area

Step: 2. Show Information

Process ID 1

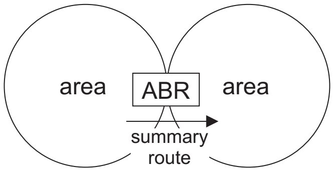
Area Information List Total: 4

Area ID	SPF Runs	ABR Count	ASBR Count	LSA Count	LSA Checksum Sum
0.0.0.1	0	0	0	0	0
0.0.0.2	0	0	0	0	0
0.0.0.3	10	10	10	10	10
0.0.0.4	0	0	0	0	0

CONFIGURING AREA RANGES (ROUTE SUMMARIZATION FOR ABRS)

An OSPF area can include a large number of nodes. If the Area Border Router (ABR) has to advertise route information for each of these nodes, this wastes a lot of bandwidth and processor time. Instead, you can use the Routing Protocol > OSPF > Area Range (Add) page to configure an ABR to advertise a single summary route that covers all the individual networks within its area. When using route summaries, local changes do not have to be propagated to other area routers. This allows OSPF to be easily scaled for larger networks, and provides a more stable network topology.

Figure 499: Route Summarization for ABRs



CLI REFERENCES

- "router ospf" on page 1751
- "area range" on page 1757

COMMAND USAGE

- Use the Area Range configuration page to summarize intra-area routes, and advertise this information to other areas through Area Border Routers (ABRs). The summary route for an area is defined by an IP address and network mask. You therefore need to structure each area with a contiguous set of addresses so that all routes in the area fall within an easily specified range. If it is not possible to use one contiguous set of addresses, then the routes can be summarized for several area ranges.This router also supports Variable Length Subnet Masks (VLSMs), so you can summarize an address range on any bit boundary in a network address.

- To summarize the external LSAs imported into your autonomous system (i.e., local routing domain), use the Summary Address configuration screen (page 805).

- This router supports up five summary routes for area ranges.

PARAMETERS

These parameters are displayed:

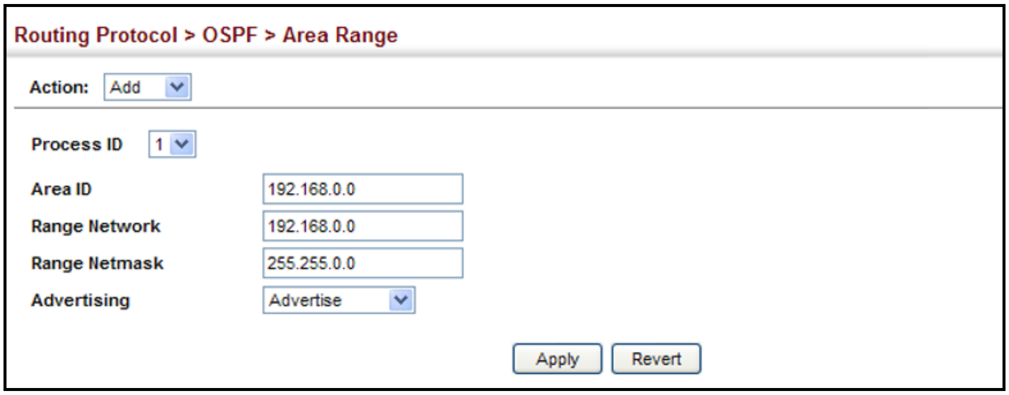
- **Process ID** – Process ID as configured in the Network Area configuration screen (see page 790).
- **Area ID** – Identifies an area for which the routes are summarized. The area ID can be in the form of an IPv4 address, or also as a four octet unsigned integer ranging from 0-4294967295.
- **Range Network** – Base address for the routes to summarize.
- **Range Netmask** – Network mask for the summary route.
- **Advertising** – Indicates whether or not to advertise the summary route. If the routes are set to be advertised, the router will issue a Type 3 summary LSA for each specified address range. If the summary is not advertised, the specified routes remain hidden from the rest of the network. (Default: Advertise)

WEB INTERFACE

To configure a route summary for an area range:

1. Click Routing Protocol, OSPF, Area Range.
2. Select Add from the Action list.
3. Specify the process ID, area identifier, the base address and network mask, and select whether or not to advertise the summary route to other areas.
4. Click Apply

Figure 500: Configuring Route Summaries for an Area Range



Routing Protocol > OSPF > Area Range

Action: Add

Process ID: 1

Area ID: 192.168.0.0

Range Network: 192.168.0.0

Range Netmask: 255.255.0.0

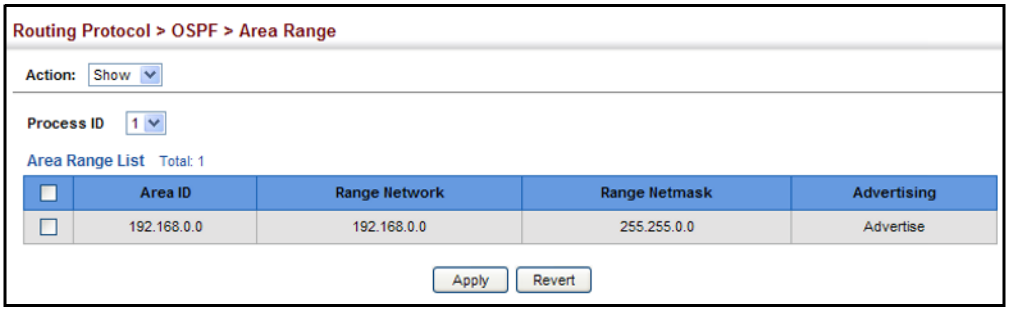
Advertising: Advertise

To show the configured route summaries:

1. Click Routing Protocol, OSPF, Area Range.
2. Select Show from the Action list.

3. Select the process ID.

Figure 501: Showing Configured Route Summaries



Routing Protocol > OSPF > Area Range

Action: Show

Process ID 1

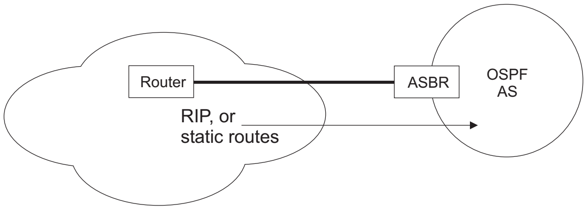
Area Range List Total: 1

□	Area ID	Range Network	Range Netmask	Advertising
□	192.168.0.0	192.168.0.0	255.255.0.0	Advertise

REDISTRIBUTING EXTERNAL ROUTES

Use the Routing Protocol > OSPF > Redistribute (Add) page to import external routing information from other routing protocols, static routes, or directly connected routes into the autonomous system, and to generate AS-external-LSAs.

Figure 502: Redistributing External Routes



CLI REFERENCES

- "router ospf" on page 1751
- "redistribute" on page 1799

COMMAND USAGE

- This router supports redistribution for all currently connected routes, entries learned through RIP, and static routes.
- When you redistribute external routes into an OSPF autonomous system (AS), the router automatically becomes an autonomous system boundary router (ASBR).
- However, if the router has been configured as an ASBR via the General Configuration screen, but redistribution is not enabled, the router will only generate a “default” external route into the AS if it has been configured to “always” advertise a default route even if an external route does not actually exist (page 793).

PARAMETERS

These parameters are displayed:

- **Process ID** – Process ID as configured in the Network Area configuration screen (see page 790).

- **Protocol Type** – Specifies the external routing protocol type for which routing information is to be redistributed into the local routing domain. (Options: RIP, Static; Default: RIP)

- **Metric Type** – Indicates the method used to calculate external route costs. (Options: Type 1, Type 2; Default: Type 1)

  Metric type specifies the way to advertise routes to destinations outside the autonomous system (AS) through External LSAs. Specify Type 1 to add the internal cost metric to the external route metric. In other words, the cost of the route from any router within the AS is equal to the cost associated with reaching the advertising ASBR, plus the cost of the external route. Specify Type 2 to only advertise the external route metric.

- **Metric** – Metric assigned to all external routes for the specified protocol. (Range: 1-65535: Default: 10)

  The metric value specified for redistributed routes supersedes the Default External Metric specified in the Routing Protocol > OSPF > System screen (page 793).

- **Tag** – A tag placed in the AS-external LSA to identify a specific external routing domain, or to pass additional information between routers. (Range: 0-4294967295)

  A tag can be used to distinguish between routes learned from different external autonomous systems (other routing protocols). For example, if there are two ASBRs in a routing domain: A and B. ASBR A can be configured to redistribute routes learned from RIP domain 1 (identified by tag 1) and ASBR B can redistribute routes learned from RIP domain 2 (identified by tag 2).

WEB INTERFACE

To configure the router to import external routing information:

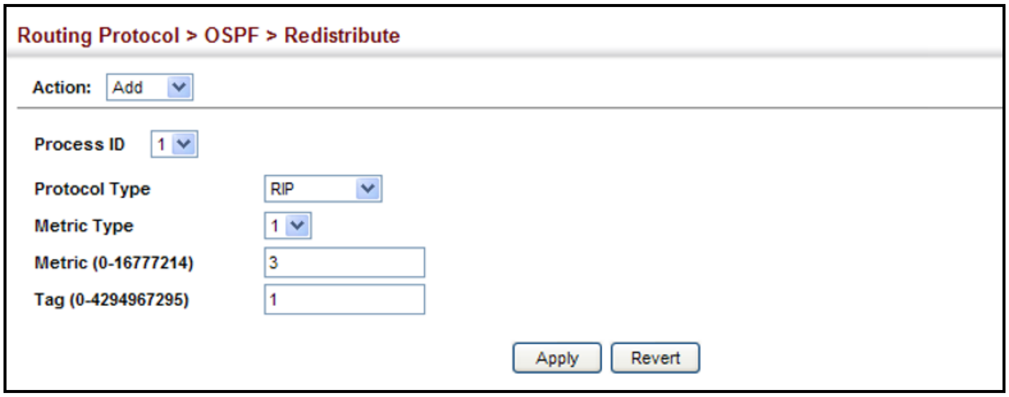
1. Click Routing Protocol, OSPF, Redistribute.

2. Select Add from the Action list.

3. Specify the process ID, the protocol type to import, the metric type, path cost, and optional tag.

4. Click Apply.

Figure 503: Importing External Routes



Routing Protocol > OSPF > Redistribute

Action: Add

Process ID: 1

Protocol Type: RIP

Metric Type: 1

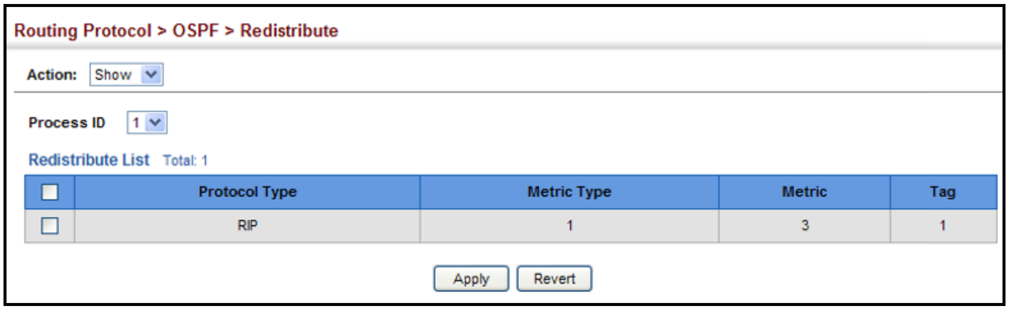
Metric (0-16777214): 3

Tag (0-4294967295): 1

To show the imported external route types:

1. Click Routing Protocol, OSPF, Redistribute.
2. Select Show from the Action list.
3. Select the process ID.

Figure 504: Showing Imported External Route Types



Routing Protocol > OSPF > Redistribute

Action: Show

Process ID: 1

Redistribute List Total: 1

□	Protocol Type	Metric Type	Metric	Tag
□	RIP	1	3	1

Configuring Summary Addresses (for External AS Routes)

Redistributing routes from other protocols into OSPF normally requires the router to advertise each route individually in an external LSA as described in the preceding section. The reduce the number of protocol messages required to redistribute these external routes, an Autonomous System Boundary Router (ASBR) can instead be configured to redistribute routes learned from other protocols into all attached autonomous systems.

To reduce the amount of external LSAs sent to other autonomous systems, you can use the Routing Protocol > OSPF > Summary Address (Add) page to configure the router to advertise an aggregate route that consolidates a broad range of external addresses. This helps both to decrease the number of external LSAs advertised and the size of the OSPF link state database.

CLI REFERENCES

- "router ospf" on page 1751
- "summary-address" on page 1761

COMMAND USAGE

- If you are not sure what address ranges to consolidate, first enable external route redistribution via the Redistribute configuration screen, view the routes imported into the routing table, and then configure one or more summary addresses to reduce the size of the routing table and consolidate these external routes for advertising into the local domain.
- To summarize routes sent between OSPF areas, use the Area Range Configuration screen (page 805).
- This router supports up 20 Type-5 summary routes.

PARAMETERS

These parameters are displayed:

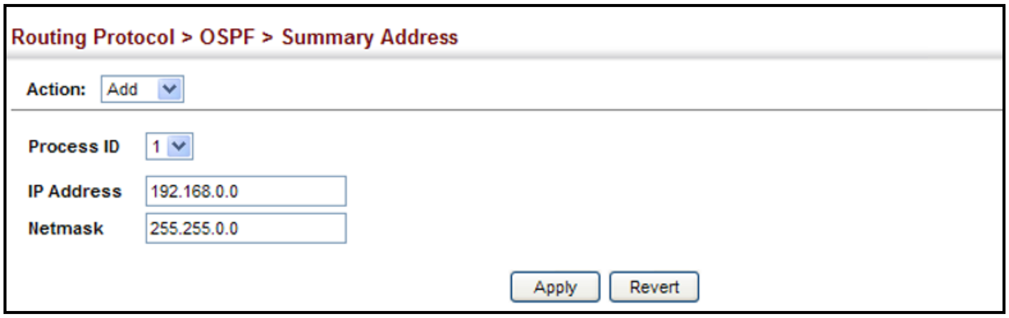
- **Process ID** – Process ID as configured in the Network Area configuration screen (see page 790).
- **IP Address** – Summary address covering a range of addresses.
- **Netmask** – Network mask for the summary route.

WEB INTERFACE

To configure the router to summarize external routing information:

1. Click Routing Protocol, OSPF, Summary Address.
2. Select Add from the Action list.
3. Specify the process ID, the base address and network mask.
4. Click Apply.

Figure 505: Summarizing External Routes



Routing Protocol > OSPF > Summary Address

Action: Add

Process ID: 1

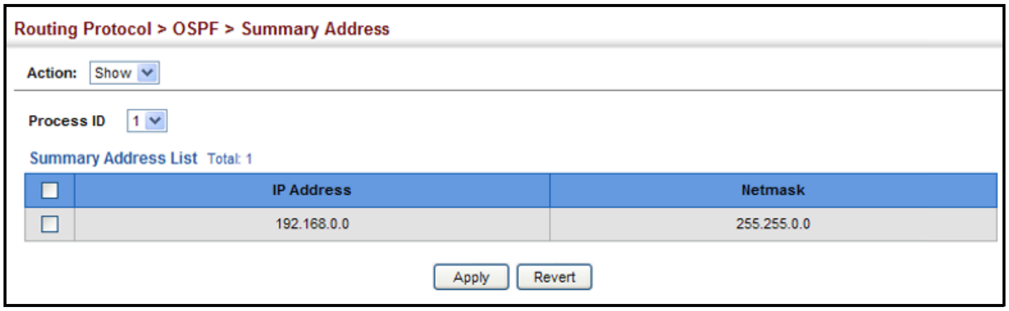
IP Address: 192.168.0.0

Netmask: 255.255.0.0

To show the summary addresses for external routes:

1. Click Routing Protocol, OSPF, Summary Address.
2. Select Show from the Action list.
3. Select the process ID.

Figure 506: Showing Summary Addresses for External Routes



Routing Protocol > OSPF > Summary Address

Action: Show

Process ID 1

Summary Address List Total: 1

☐	IP Address	Netmask
☐	192.168.0.0	255.255.0.0

Configuring OSPF Interfaces

You should specify a routing interface for any local subnet that needs to communicate with other network segments located on this router or elsewhere in the network. First configure a VLAN for each subnet that will be directly connected to this router, assign IP interfaces to each VLAN (i.e., one primary interface and one or more secondary interfaces), and then use the Network Area configuration page to assign an interface address range to an OSPF area.

After assigning a routing interface to an OSPF area, use the Routing Protocol > OSPF > Interface (Configure by VLAN) or (Configure by Address) page to configure the interface-specific parameters used by OSPF to set the cost used to select preferred paths, select the designated router, control the timing of link state advertisements, and specify the method used to authenticate routing messages.

CLI References

- "Open Shortest Path First (OSPFv2)" on page 1750

Command Usage

- The Configure by VLAN page is used to set the OSPF interface settings for the all areas assigned to a VLAN on the Network Area (Add) page (see page 790).

- The Configure by Address page is used to set the OSPF interface settings for a specific area assigned to a VLAN on the Network Area (Add) page (see page 790).

Parameters

These parameters are displayed:

- **VLAN ID** – A VLAN to which an IP interface has been assigned.

- **IP Address** – Address of the interfaces assigned to a VLAN on the Network Area (Add) page.

  This parameter only applies to the Configure by Address page.

- **Cost** – Sets the cost of sending a protocol packet on an interface, where higher values indicate slower ports. (Range: 1-65535; Default: 1)

  The interface cost indicates the overhead required to send packets across a certain interface. This is advertised as the link cost in router link state advertisements.

  Routes are assigned a metric equal to the sum of all metrics for each interface link in the route.

  This router uses a default cost of 1 for all ports. Therefore, if you install a 10 Gigabit module, you need to reset the cost for all of the 1 Gbps ports to a value greater than 1 to reflect the actual interface bandwidth.

- **Router Priority** – Sets the interface priority for this router. (Range: 0-255; Default: 1)

  This priority determines the designated router (DR) and backup designated router (BDR) for each OSPF area. The DR forms an active adjacency to all other routers in the area to exchange routing topology information. If for any reason the DR fails, the BDR takes over this role.

  Set the priority to zero to prevent a router from being elected as a DR or BDR. If set to any value other than zero, the router with the highest priority becomes the DR and the router with the next highest priority becomes the BDR. If two or more routers are set to the same highest priority, the router with the higher ID will be elected.

  If a DR already exists for an area when this interface comes up, the new router will accept the current DR regardless of its own priority. The DR will not change until the next time the election process is initiated.

  Configure router priority for multi-access networks only and not for point-to-point networks.

- **Hello Interval** – Sets the interval between sending hello packets on an interface. This interval must be set to the same value for all routers on the network. (Range: 1-65535 seconds; Default: 10)

  Hello packets are used to inform other routers that the sending router is still active. Setting the hello interval to a smaller value can reduce the delay in detecting topological changes, but will increase routing traffic.

- **Dead Interval** – Sets the interval at which hello packets are not seen before neighbors declare the router down. This interval must be set to the same value for all routers on the network. (Range: 1-65535 seconds; Default: 40, or 4 times the Hello Interval)

  The dead-interval is advertised in the router's hello packets. It must be a multiple of hello-interval and be the same for all routers on a specific network.

- **Transmit Delay** – Sets the estimated time to send a link-state update packet over an interface. (Range: 1-65535 seconds; Default: 1 second)

  LSAs have their age incremented by this delay before transmission. You should consider both the transmission and propagation delays for an interface when estimating this delay. Set the transmit delay according to link speed, using larger values for lower-speed links.

  If this delay is not added, the time required to transmit an LSA over the link is not taken into consideration by the routing process. On slow links, the router may send packets more quickly than devices can receive them. To avoid this problem, you can use the transmit delay to force the router to wait a specified interval between transmissions.

- **Retransmit Interval** – Sets the time between re-sending link-state advertisements. (Range: 1-65535 seconds; Default: 5 seconds)

  A router will resend an LSA to a neighbor if it receives no acknowledgment after the specified retransmit interval. The retransmit interval should be set to a conservative value that provides an adequate flow of routing information, but does not produce unnecessary protocol traffic. Note that this value should be larger for virtual links.

  Set this interval to a value that is greater than the round-trip delay between any two routers on the attached network to avoid unnecessary retransmissions.

- **Authentication Type** – Specifies the authentication type used for an interface. (Options: None, Simple, MD5; Default: None)

  Use authentication to prevent routers from inadvertently joining an unauthorized area. Configure routers in the same area with the same password (or key). All neighboring routers on the same network with the same password will exchange routing data.

  When using simple password authentication, a password is included in the packet. If it does not match the password configured on the receiving router, the packet is discarded. This method provides very little security as it is possible to learn the authentication key by snooping on routing protocol packets.

  When using Message-Digest 5 (MD5) authentication, the router uses the MD5 algorithm to verify data integrity by creating a 128-bit message digest from the authentication key. Without the proper key and key-id, it is nearly impossible to produce any message that matches the prespecified target message digest.

  The Message Digest Key ID and Authentication Key and must be used consistently throughout the autonomous system.

- **Authentication Key** – Assign a plain-text password used by neighboring routers to verify the authenticity of routing protocol messages. (Range: 1-8 characters for simple password or 1-16 characters for MD5 authentication; Default: no key)

  When plain-text or Message-Digest 5 (MD5) authentication is enabled as described in the preceding item, this password (key) is inserted into the OSPF header when routing protocol packets are originated by this device.

A different password can be assigned to each network interface, but the password must be used consistently on all neighboring routers throughout a network (that is, autonomous system). All neighboring routers in the same network with the same password will exchange routing data.

- **Message Digest Key ID** – Assigns a key identifier used in conjunction with the authentication key to verify the authenticity of routing protocol messages sent to neighboring routers. (Range: 1-255; Default: none)

  Normally, only one key is used per interface to generate authentication information for outbound packets and to authenticate incoming packets. Neighbor routers must use the same key identifier and key value.

  When changing to a new key, the router will send multiple copies of all protocol messages, one with the old key and another with the new key. Once all the neighboring routers start sending protocol messages back to this router with the new key, the router will stop using the old key. This rollover process gives the network administrator time to update all of the routers on the network without affecting the network connectivity. Once all the network routers have been updated with the new key, the old key should be removed for security reasons.

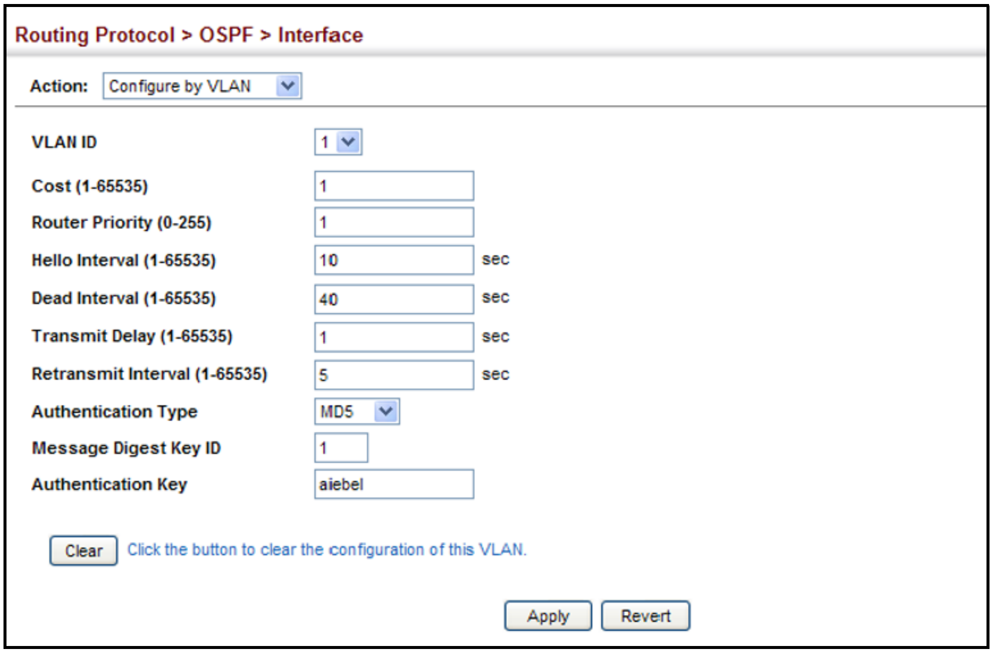
  Before setting a new key identifier, the current key must first be deleted on the Show MD5 Key page.

WEB INTERFACE

To configure OSPF interface for all areas assigned to a VLAN:

1. Click Routing Protocol, OSPF, Interface.
2. Select Configure by VLAN from the Action list.
3. Specify the VLAN ID, and configure the required interface settings.
4. Click Apply.

Figure 507: Configuring Settings for All Interfaces Assigned to a VLAN



Routing Protocol > OSPF > Interface

Action: Configure by VLAN

VLAN ID	1
Cost (1-65535)	1
Router Priority (0-255)	1
Hello Interval (1-65535)	10 sec
Dead Interval (1-65535)	40 sec
Transmit Delay (1-65535)	1 sec
Retransmit Interval (1-65535)	5 sec
Authentication Type	MD5
Message Digest Key ID	1
Authentication Key	aiebel

Clear — Click the button to clear the configuration of this VLAN.

To configure interface settings for a specific area assigned to a VLAN:

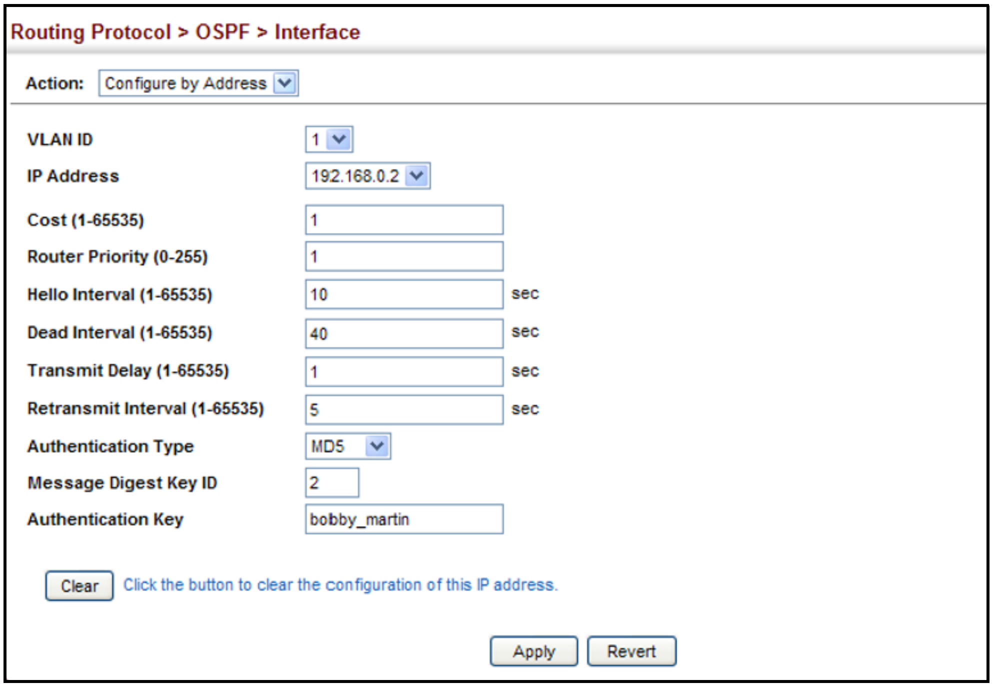
1. Click Routing Protocol, OSPF, Interface.

2. Select Configure by Address from the Action list.

3. Specify the VLAN ID, enter the address assigned to an area, and configure the required interface settings.

4. Click Apply.

Figure 508: Configuring Settings for a Specific Area Assigned to a VLAN



Routing Protocol > OSPF > Interface

Action: Configure by Address

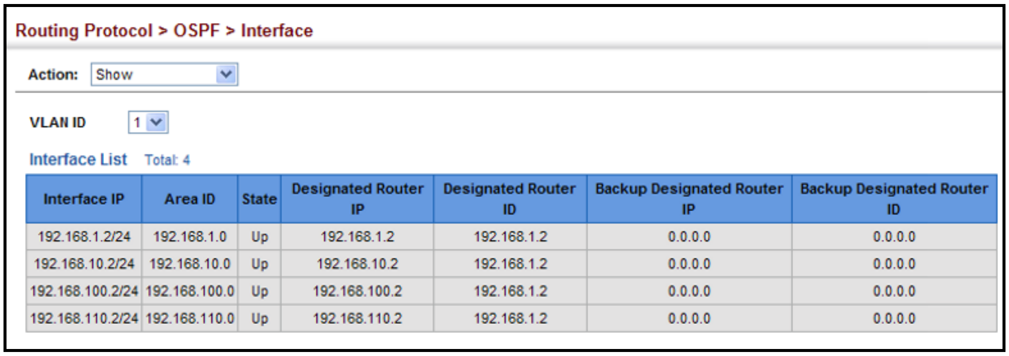
VLAN ID	1
IP Address	192.168.0.2
Cost (1-65535)	1
Router Priority (0-255)	1
Hello Interval (1-65535)	10 sec
Dead Interval (1-65535)	40 sec
Transmit Delay (1-65535)	1 sec
Retransmit Interval (1-65535)	5 sec
Authentication Type	MD5
Message Digest Key ID	2
Authentication Key	bobby_martin

Clear Click the button to clear the configuration of this IP address.

To show the configuration settings for OSPF interfaces:

1. Click Routing Protocol, OSPF, Interface.
2. Select Show from the Action list.
3. Select the VLAN ID.

Figure 509: Showing OSPF Interfaces



Routing Protocol > OSPF > Interface

Action: Show

VLAN ID 1

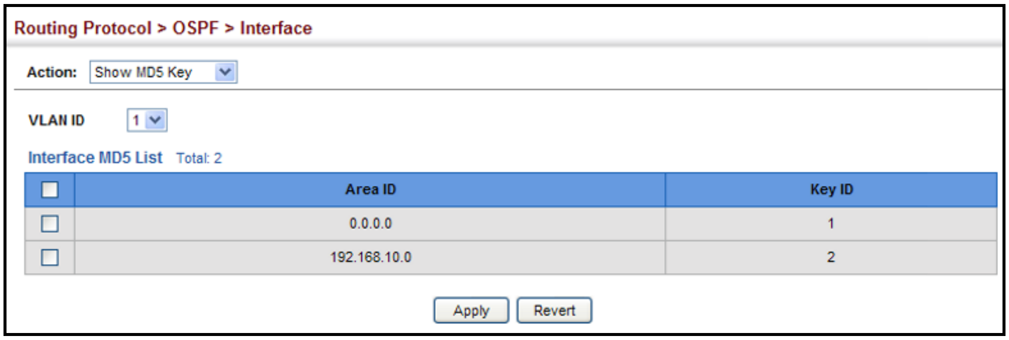
Interface List Total: 4

Interface IP	Area ID	State	Designated Router IP	Designated Router ID	Backup Designated Router IP	Backup Designated Router ID
192.168.1.2/24	192.168.1.0	Up	192.168.1.2	192.168.1.2	0.0.0.0	0.0.0.0
192.168.10.2/24	192.168.10.0	Up	192.168.10.2	192.168.1.2	0.0.0.0	0.0.0.0
192.168.100.2/24	192.168.100.0	Up	192.168.100.2	192.168.1.2	0.0.0.0	0.0.0.0
192.168.110.2/24	192.168.110.0	Up	192.168.110.2	192.168.1.2	0.0.0.0	0.0.0.0

To show the MD5 authentication keys configured for an interface:

1. Click Routing Protocol, OSPF, Interface.
2. Select Show MD5 Key from the Action list.
3. Select the VLAN ID.

Figure 510: Showing MD5 Authentication Keys



Routing Protocol > OSPF > Interface

Action: Show MD5 Key

VLAN ID 1

Interface MD5 List Total: 2

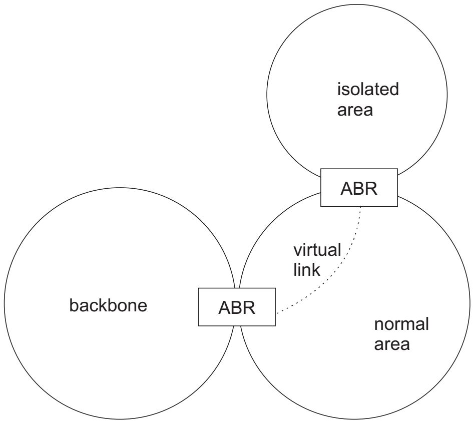
□	Area ID	Key ID
□	0.0.0.0	1
□	192.168.10.0	2

CONFIGURING VIRTUAL LINKS

Use the Routing Protocol > OSPF > Virtual Link (Add) and (Configure Detailed Settings) pages to configure a virtual link from an area that does not have a direct physical connection to the OSPF backbone.

All OSPF areas must connect to the backbone. If an area does not have a direct physical connection to the backbone, you can configure a virtual link that provides a logical path to the backbone. To connect an isolated area to the backbone, the logical path can cross a single non-backbone area (i.e., transit area) to reach the backbone. To define this path, you must configure an ABR that serves as an endpoint connecting the isolated area to the common transit area, and specify a neighboring ABR at the other endpoint connecting the common transit area to the backbone itself. (Note that you cannot configure a virtual link that runs through a stub or NSSA.)

Figure 511: OSPF Virtual Link



Virtual links can also be used to create a redundant link between any area and the backbone to help prevent partitioning, or to connect two existing backbone areas into a common backbone.

Any area disconnected from the backbone must include the transit area ID and the router ID for a virtual link neighbor that is adjacent to the backbone.

This router supports up five virtual links.

CLI REFERENCES

- "router ospf" on page 1751
- "area virtual-link" on page 1765

COMMAND USAGE

- Use the Add page to create a virtual link, and then use the Configure Detailed Settings page to set the protocol timers and authentication settings for the link. The parameters to be configured on the Configure Detailed Settings page are described under "Configuring OSPF Interfaces" on page 811.

PARAMETERS

These parameters are displayed:

- **Process ID** – Process ID as configured in the Network Area configuration screen (see page 790).

- **Transit Area ID** – Identifies the transit area for the virtual link. The area ID must be in the form of an IPv4 address, or also as a four octet unsigned integer ranging from 0-4294967295.

- **Neighbor ID** – Router ID of the virtual link neighbor. This specifies the Area Border Router (ABR) at the other end of the virtual link. To create a virtual link, it must be configured for an ABR at both ends of the link.

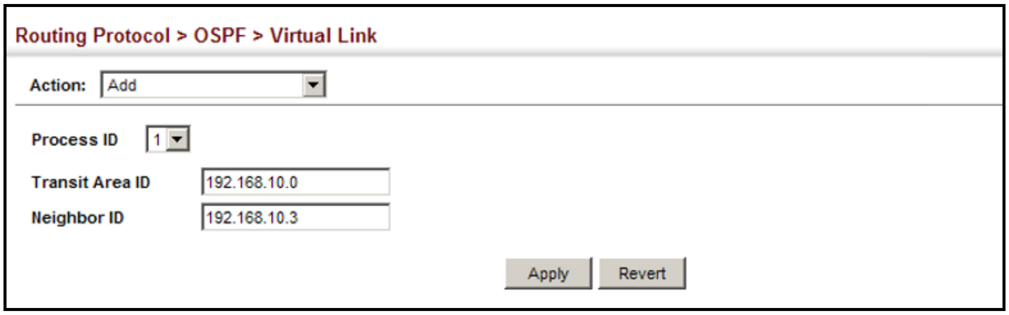
One of the ABRs must be next to the isolated area and the transit area at one end of the link, while the other ABR must be next to the transit area and backbone at the other end of the link.

WEB INTERFACE

To create a virtual link:

1. Click Routing Protocol, OSPF, Virtual Link.
2. Select Add from the Action list.
3. Specify the process ID, the Area ID, and Neighbor router ID.
4. Click Apply.

Figure 512: Adding a Virtual Link



Routing Protocol > OSPF > Virtual Link

Action: Add

Process ID 1

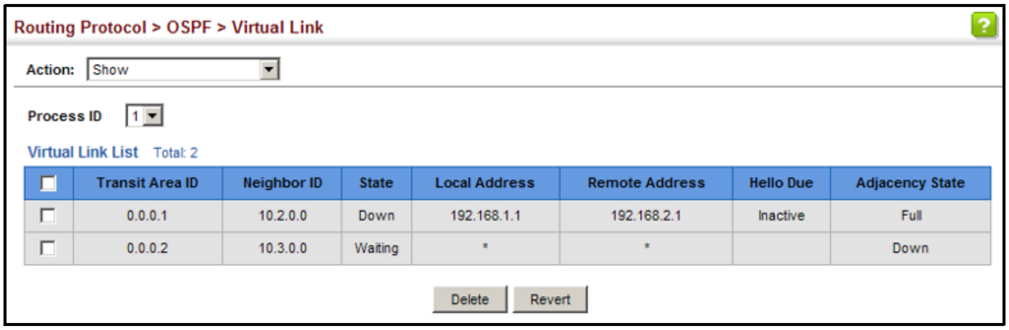
Transit Area ID 192.168.10.0

Neighbor ID 192.168.10.3

To show virtual links:

1. Click Routing Protocol, OSPF, Virtual Link.
2. Select Show from the Action list.
3. Select the process ID.

Figure 513: Showing Virtual Links



Routing Protocol > OSPF > Virtual Link

Action: Show

Process ID 1

Virtual Link List Total: 2

□	Transit Area ID	Neighbor ID	State	Local Address	Remote Address	Hello Due	Adjacency State
□	0.0.0.1	10.2.0.0	Down	192.168.1.1	192.168.2.1	Inactive	Full
□	0.0.0.2	10.3.0.0	Waiting	*	*		Down

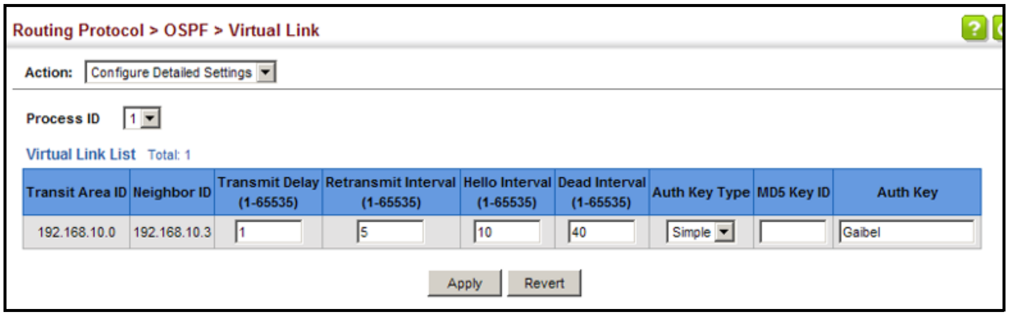
To configure detailed settings for a virtual link:

1. Click Routing Protocol, OSPF, Virtual Link.
2. Select Configure Detailed Settings from the Action list.

3. Specify the process ID, then modify the protocol timers and authentication settings as required.

4. Click Apply.

Figure 514: Configuring Detailed Settings for a Virtual Link



Routing Protocol > OSPF > Virtual Link

Action: Configure Detailed Settings

Process ID 1

Virtual Link List Total: 1

Transit Area ID	Neighbor ID	Transmit Delay (1-65535)	Retransmit Interval (1-65535)	Hello Interval (1-65535)	Dead Interval (1-65535)	Auth Key Type	MD5 Key ID	Auth Key
192.168.10.0	192.168.10.3	1	5	10	40	Simple		Gaibel

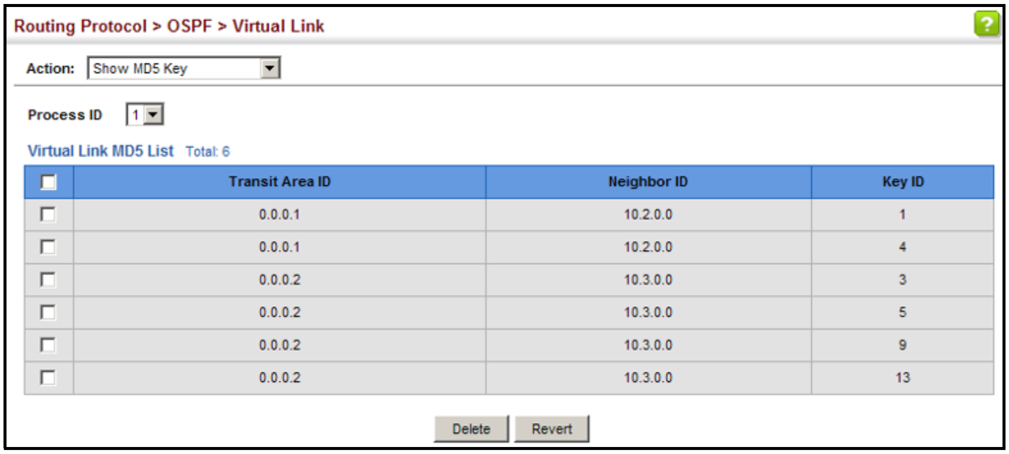
To show the MD5 authentication keys configured for a virtual link:

1. Click Routing Protocol, OSPF, Interface.

2. Select Show MD5 Key from the Action list.

3. Select the VLAN ID.

Figure 515: Showing MD5 Authentication Keys



Routing Protocol > OSPF > Virtual Link

Action: Show MD5 Key

Process ID 1

Virtual Link MD5 List Total: 6

□	Transit Area ID	Neighbor ID	Key ID
□	0.0.0.1	10.2.0.0	1
□	0.0.0.1	10.2.0.0	4
□	0.0.0.2	10.3.0.0	3
□	0.0.0.2	10.3.0.0	5
□	0.0.0.2	10.3.0.0	9
□	0.0.0.2	10.3.0.0	13

DISPLAYING LINK STATE DATABASE INFORMATION

Use the Routing Protocol > OSPF > Information (LSDB) page to show the Link State Advertisements (LSAs) sent by OSPF routers advertising routes. The full collection of LSAs collected by a router interface from the attached area is known as a link state database. Routers that are connected to multiple interfaces will have a separate database for each area. Each router in the same area should have an identical database describing the topology for that area, and the shortest path to external destinations.

The full database is exchanged between neighboring routers as soon as a new router is discovered. Afterwards, any changes that occur in the routing tables are synchronized with neighboring routers through a process called reliable flooding. You can show information about different LSAs stored in this router's database, which may include any of the following types:

- Router (Type 1) – All routers in an OSPF area originate Router LSAs that describe the state and cost of its active interfaces and neighbors.
- Network (Type 2) – The designated router for each area originates a Network LSA that describes all the routers that are attached to this network segment.
- Summary (Type 3) – Area border routers can generate Summary LSAs that give the cost to a subnetwork located outside the area.
- AS Summary (Type 4) – Area border routers can generate AS Summary LSAs that give the cost to an autonomous system boundary router (ASBR).
- AS External (Type 5) – An ASBR can generate an AS External LSA for each known network destination outside the AS.
- NSSA External (Type 7) – An ASBR within an NSSA generates an NSSA external link state advertisement for each known network destination outside the AS.

CLI References

- "show ip ospf database" on page 1780

Parameters

These parameters are displayed:

- **Process ID** – Process ID as configured in the Network Area configuration screen (see page 790).
- **Query by** – The LSA database can be searched using the following criteria:
  - Self-Originate – LSAs generated by this router.
  - Link ID – LSAs advertising a specific link.
  - Adv Router – LSAs advertised by a specific router.
- **Link State Type** – The information returned by a query can be displayed for all LSA types or for a specific type. (Default: All)

Information displayed for each LSA entry includes:

- **Area ID** – Area defined for which LSA information is to be displayed.
- **Link ID** – Network portion described by an LSA. The Link ID is either:
  - An IP network number for Type 3 Summary and Type 5 AS External LSAs. (When an Type 5 AS External LSA is describing a default route, its Link ID is set to the default destination 0.0.0.0.)
  - A Router ID for Router, Network, and Type 4 AS Summary LSAs.

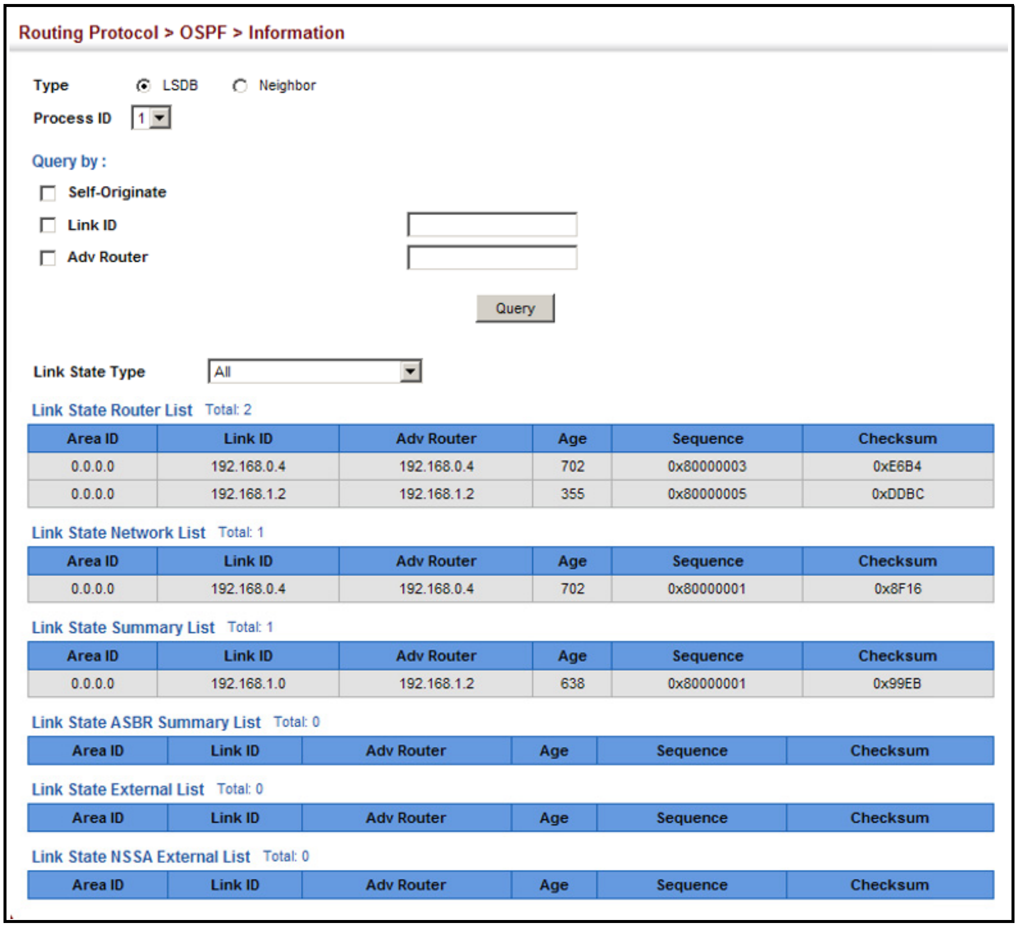
- **Adv Router** – IP address of the advertising router.
- **Age** – Age of LSA (in seconds).
- **Sequence** – Sequence number of LSA (used to detect older duplicate LSAs).
- **Checksum** – Checksum of the complete contents of the LSA.

WEB INTERFACE

To display information in the link state database:

1. Click Routing Protocol, OSPF, Information.
2. Click LSDB.
3. Select the process identifier.
4. Specify required search criteria, such as self-originated LSAs, LSAs with a specific link ID, or LSAs advertised by a specific router.
5. Then select the database entries to display based on LSA type.

Figure 516: Displaying Information in the Link State Database



Routing Protocol > OSPF > Information

Type ● LSDB ○ Neighbor

Process ID 1

Query by :

□ Self-Originate

□ Link ID

□ Adv Router

Link State Type All

Link State Router List Total: 2

Area ID	Link ID	Adv Router	Age	Sequence	Checksum
0.0.0.0	192.168.0.4	192.168.0.4	702	0x80000003	0xE6B4
0.0.0.0	192.168.1.2	192.168.1.2	355	0x80000005	0xDDBC

Link State Network List Total: 1

Area ID	Link ID	Adv Router	Age	Sequence	Checksum
0.0.0.0	192.168.0.4	192.168.0.4	702	0x80000001	0x8F16

Link State Summary List Total: 1

Area ID	Link ID	Adv Router	Age	Sequence	Checksum
0.0.0.0	192.168.1.0	192.168.1.2	638	0x80000001	0x99EB

Link State ASBR Summary List Total: 0

Area ID	Link ID	Adv Router	Age	Sequence	Checksum

Link State External List Total: 0

Area ID	Link ID	Adv Router	Age	Sequence	Checksum

Link State NSSA External List Total: 0

Area ID	Link ID	Adv Router	Age	Sequence	Checksum

DISPLAYING INFORMATION ON NEIGHBORING ROUTERS

Use the Routing Protocol > OSPF > Information (Neighbor) page to display information about neighboring routers on each interface.

CLI REFERENCES

- "show ip ospf neighbor" on page 1787

PARAMETERS

These parameters are displayed:

- **Process ID** – Process ID as configured in the Network Area configuration screen (see page 790).
- **ID** – Neighbor’s router ID.
- **Priority** – Neighbor’s router priority.
- **State** – OSPF state and identification flag.

  States include:

  - Down – Connection down
  - Attempt – Connection down, but attempting contact (non-broadcast networks)
  - Init – Have received Hello packet, but communications not yet established
  - Two-way – Bidirectional communications established
  - ExStart – Initializing adjacency between neighbors
  - Exchange – Database descriptions being exchanged
  - Loading – LSA databases being exchanged
  - Full – Neighboring routers now fully adjacent

  Identification flags include:

  - D – Dynamic neighbor
  - S – Static neighbor
  - DR – Designated router
  - BDR – Backup designated router

- **Address** – IP address of this interface.
- **Interface** – A Layer 3 interface on which OSPF has been enabled.

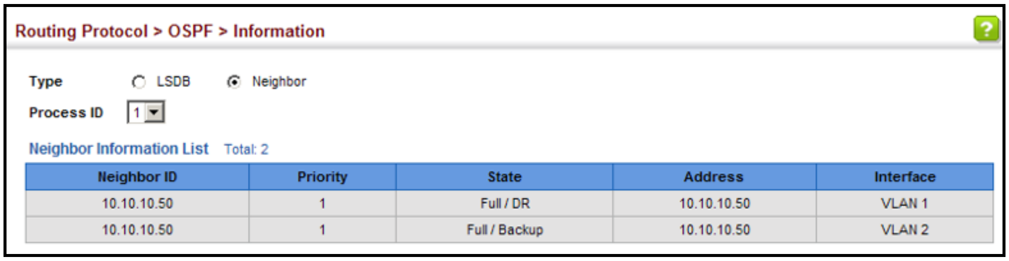
WEB INTERFACE

To display information about neighboring routers stored in the link state database:

1. Click Routing Protocol, OSPF, Information.
2. Click Neighbor.

3. Select the process identifier.

Figure 517: Displaying Neighbor Routers Stored in the Link State Database



Routing Protocol > OSPF > Information

Type ○ LSDB ● Neighbor

Process ID 1

Neighbor Information List Total: 2

Neighbor ID	Priority	State	Address	Interface
10.10.10.50	1	Full / DR	10.10.10.50	VLAN 1
10.10.10.50	1	Full / Backup	10.10.10.50	VLAN 2

21 MULTICAST ROUTING

This chapter describes the following multicast routing topics:

- Enabling Multicast Routing Globally – Describes how to globally enable multicast routing.
- Displaying the Multicast Routing Table – Describes how to display the multicast routing table.
- Configuring PIM for IPv4 – Describes how to configure PIM-DM and PIM-SM for IPv4.
- Configuring PIMv6 for IPv6 – Describes how to configure PIM-DM and PIM-SM (Version 6) for IPv6.

OVERVIEW

This router can route multicast traffic to different subnetworks using Protocol-Independent Multicasting - Dense Mode or Sparse Mode (PIM-DM or PIM-SM) for IPv4, as well as PIM-DM for IPv6. PIM for IPv4 (also called PIMv4 in this manual) relies on messages sent from IGMP-enabled Layer 2 switches and hosts to determine when hosts want to join or leave multicast groups. PIM for IPv6 (also called PIMv6 in this manual) uses the Multicast Listener Discovery (MLDv1) protocol which is the IPv6 equivalent to IGMPv2. PIM-DM is designed for networks where the probability of multicast group members is high, such as a local network. PIM-SM is designed for networks where the probability of multicast group members is low, such as the Internet.

Also, note that if PIM is not enabled on this router or another multicast routing protocol is used on the network, the switch ports attached to a multicast router can be manually configured to forward multicast traffic (see "Specifying Static Interfaces for an IPv4 Multicast Router" on page 617).

Configuring PIM-DM

PIM-DM floods multicast traffic downstream, and calculates the shortest-path, source-rooted delivery tree between each source and destination host group. Other multicast routing protocols, such as DVMRP, build their own source-rooted multicast delivery tree (i.e., a separate routing table) that allows it to prevent looping and determine the shortest path to the source of the multicast traffic. PIM-DM also builds a source-rooted multicast delivery tree for each multicast source, but uses information from the router’s unicast routing table, instead of maintaining its own multicast routing table, making it routing protocol independent.

PIM-DM is a simple multicast routing protocol that uses flood and prune to build a source-routed multicast delivery tree for each multicast source-group pair. As mentioned above, it does not maintain it's own routing table, but instead, uses the routing table provided by whatever unicast routing protocol is enabled on the router interface. When the router receives a multicast packet for a source-group pair, PIM-DM checks the unicast routing table on the inbound interface to determine if this is the same interface used for routing unicast packets to the multicast source network. If it is not, the router drops the packet and sends an Assert message back out the source interface. An Assert winner is then selected to continue forwarding traffic from this source. On the other hand, if it is the same interface used by the unicast protocol, then the router forwards a copy of the packet to all the other interfaces for which is has not already received a prune message for this specific source-group pair.

DVMRP holds the prune state for about two hours, while PIM-DM holds it for only about three minutes. Although this results in more flooding than encountered with DVMRP, this is the only major trade-off for the lower processing overhead and simplicity of configuration for PIM-DM.

Configuring PIM-SM

PIM-SM uses the router's local unicast routing table to route multicast traffic, not to flood it. It only forwards multicast traffic when requested by a local or downstream host. When service is requested by a host, it can use a Reverse Path Tree (RPT) that channels the multicast traffic from each source through a single Rendezvous Point (RP) within the local PIM-SM domain, and then forwards this traffic to the Designated Router (DR) in the local network segment to which the host is attached. However, when the multicast load from a particular source is heavy enough to justify it, PIM-SM can be configured to construct a Shortest Path Tree (SPT) directly from the DR up to the source, bypassing the RP and thereby reducing service delays for active hosts and setup time for new hosts.

PIM-SM reduces the amount of multicast traffic by forwarding it only to the ports that are attached to receivers for a group. The key components to filtering multicast traffic are listed below.

Common Domain – A common domain must be set up in which all of the multicast routers are configured with the same basic PIM-SM settings.

Bootstrap Router (BSR) – After the common domain is set, a bootstrap router is elected from this domain. Each time a PIM-SM router is booted up, or the multicast mode reconfigured to enable PIM-SM, the bootstrap router candidates start flooding bootstrap messages on all of their interfaces (using reverse path forwarding to limit the impact on the network). When neighboring routers receive bootstrap messages, they process the message and forward it out through all interfaces, except for the interface on which this message was received. If a router receives a bootstrap message with a BSR priority larger than its own, it stops advertising itself as a BSR candidate. Eventually, only the router with the highest BSR priority will continue sending bootstrap messages.

Rendezvous Point (RP) – A router may periodically sends PIMv2 messages to the BSR advertising itself as a candidate RP for specified group addresses. The BSR places information about all of the candidate RPs in subsequent bootstrap messages. The BSR and all the routers receiving these messages use the same hash algorithm to elect an RP for each multicast group. If each router is properly configured, the results of the election process will be the same for each router. Each elected RP then starts to serve as the root of a shared distribution tree for one or more multicast groups.

Designated Router (DR) – A DR advertising the highest priority in its hello messages is elected for each subnet. The DR is responsible for collecting information from the subnet about multicast clients that want to join or leave a group. Join messages from the DR (receiver) for each group are sent towards the RP, and data from multicast sources is sent to the RP. Receivers can now start receiving traffic destined for the client group from the RP, or they can identify the senders and optionally set up a direct connection to the source through a shortest path tree (SPT) if the loading warrants this change over.

Shared Tree – When many receivers join a group, their Join messages converge on the RP, and form a distribution tree for the group that is rooted at the RP. This is known as the Reverse Path Tree (RPT), or the shared tree since it is shared by all sources sending to that group. When a multicast source sends data destined for a group, the source's local DR takes those data packets, unicast-encapsulates them, and sends them to the RP. When the RP receives these encapsulated data packets, it decapsulates them, and forwards them onto the shared tree. These packets follow the group mapping maintained by routers along the RP Tree, are replicated wherever the RP Tree branches, and eventually reach all the receivers for that multicast group. Because all routers along the shared tree are using PIM-SM, the multicast flow is confined to the shared tree. Also, note that more than one flow can be carried over the same shared tree, but only one RP is responsible for each flow.

Shortest Path Tree (SPT) – When using the Shared Tree, multicast traffic is contained within the shared tree. However, there are several drawbacks to using the shared tree. Decapsulation of traffic at the RP into multicast packets is a resource intensive process. The protocol does not take into account the location of group members when selecting the RP, and the path from the RP to the receiver is not always optimal. Moreover, a high degree of latency may occur for hosts wanting to join a group because the RP must wait for a register message from the DR before setting up the shared tree and establishing a path back to the source. There is also a problem with bursty sources. When a source frequently times out, the shared tree has to be rebuilt each time, causing further latency in sending traffic to the receiver. To enhance overall network performance, the switch uses the RP only to forward the first packet from a source to the receivers. After the first packet, it calculates the shortest path between the receiver and source and uses the SPT to send all subsequent packets from the source directly to the receiver. When the first packet arrives natively through the shortest path, the RP sends a register-stop message back to the DR near the source. When this DR receives the register-stop message, it stops sending register messages to the RP. If there are no other sources using the shared tree, it is also torn down. Setting up the SPT requires more memory than when using the shared tree, but can significantly reduce group join and data transmission delays. The switch can also be configured to use SPT only for specific multicast groups, or to disable the change over to SPT for specific groups.

CONFIGURING GLOBAL SETTINGS FOR MULTICAST ROUTING

To use multicast routing on this router, first globally enable multicast routing as described in this section, then specify the interfaces that will employ multicast routing protocols (PIM-DM or PIM-SM). Note that only one multicast routing protocol (PIM-DM or PIM-SM) can be enabled on any given interface, but both PIMv4 and PIMv6 can be enabled on the same interface.

ENABLING MULTICAST ROUTING GLOBALLY

Use the Multicast > Multicast Routing > General page or the Multicast > IPv6 Multicast Routing > General page to enable IPv4 or IPv6 multicast routing globally on the switch.

CLI REFERENCES

- "ip multicast-routing" on page 1919
- "ipv6 multicast-routing" on page 1922

PARAMETERS

These parameters are displayed:

IPv4 Multicast Routing

- **Multicast Forwarding Status** – Enables IP multicast routing. (Default: Disabled)

IPv6 Multicast Routing

- **IPv6 Multicast Forwarding Status** – Enables IPv6 multicast routing. (Default: Disabled)

WEB INTERFACE (IPV4)

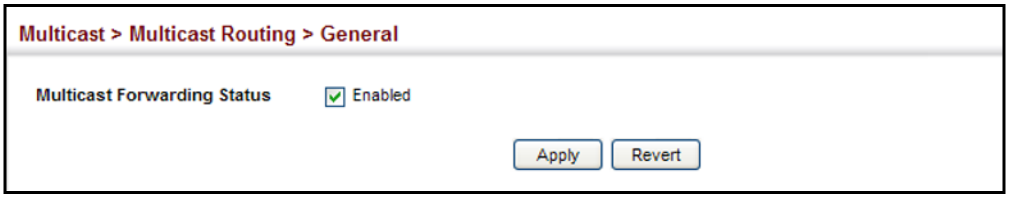
To enable IPv4 multicast routing:

1. Click Multicast, Multicast Routing, General.

2. Enable Multicast Forwarding Status.

3. Click Apply.

Figure 518: Enabling IPv4 Multicast Routing



Multicast > Multicast Routing > General

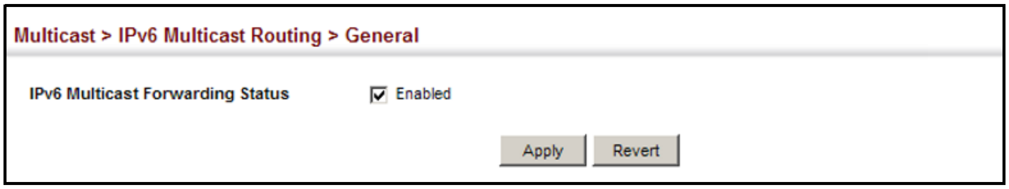
Multicast Forwarding Status ☑ Enabled

WEB INTERFACE (IPV6)

To enable IPv6 multicast routing:

1. Click Multicast, IPv6 Multicast Routing, General.
2. Enable Multicast Forwarding Status.
3. Click Apply.

Figure 519: Enabling IPv6 Multicast Routing



Multicast > IPv6 Multicast Routing > General

IPv6 Multicast Forwarding Status ☑ Enabled

DISPLAYING THE MULTICAST ROUTING TABLE

Use the Multicast > Multicast Routing > Information page or the IPv6 Multicast > Multicast Routing > Information page to display IPv4 or IPv6 information on each multicast route the switch has learned through PIM. The router learns multicast routes from neighboring routers, and also advertises these routes to its neighbors. The router stores entries for all paths learned by itself or from other routers, without considering actual group membership or prune messages. The routing table therefore does not indicate that the router has processed multicast traffic from any particular source listed in the table. It uses these routes to forward multicast traffic only if group members appear on directly-attached subnetworks or on subnetworks attached to downstream routers.

CLI REFERENCES

- "show ip mroute" on page 1920
- "show ipv6 mroute" on page 1923

PARAMETERS

These parameters are displayed for IPv4:

Show Summary

- **Group Address** – IP group address for a multicast service.
- **Source Address** – Subnetwork containing the IP multicast source.
- **Source Mask** – Network mask for the IP multicast source. Note that the switch cannot detect the source mask, and therefore displays 255.255.255.255 in this field. (This parameter applies to IPv4 only.)
- **Interface** – Upstream interface leading to the upstream neighbor.

  PIM creates a multicast routing tree based on the unicast routing table. If the related unicast routing table does not exist, PIM will still create a multicast routing entry, displaying the upstream interface to indicate that this entry is valid. This field may also display “Register” to indicate that a pseudo interface is being used to receive PIM-SM register packets. This can occur for the Rendezvous Point (RP), which is the root of the Reverse Path Tree (RPT). In this case, any VLAN receiving register packets will be converted into the register interface.

- **Owner** – The associated multicast protocol (PIM-DM, PIM-SM, IGMP Proxy for PIMv4, MLD Proxy for PIMv6).
- **Flags** – The flags associated with each routing entry indicate:
  - **Forward** – Traffic received from the upstream interface is being forwarded to this interface.
  - **Local** – This is the outgoing interface.
  - **Pruned** – This interface has been pruned by a downstream neighbor which no longer wants to receive the traffic.

Show Details

- **Group Address** – IP group address for a multicast service.
- **Source Address** – Subnetwork containing the IP multicast source.
- **Source Mask** – Network mask for the IP multicast source.
- **Upstream Neighbor** – The multicast router (RPF Neighbor) immediately upstream for this group.
- **Upstream Interface** – Interface leading to the upstream neighbor.
- **Up Time** – Time since this entry was created.
- **Owner** – The associated multicast protocol (PIM-DM, PIM-SM, IGMP Proxy for PIMv4, MLD Proxy for PIMv6).
- **Flags** – The flags associated with each routing entry indicate:
  - **Dense** – PIM Dense mode in use.
  - **Sparse** – PIM Sparse mode in use.
  - **Connected** – This route is directly connected to the source.
  - **Pruned** – This route has been terminated.
  - **Register flag** – This device is registering for a multicast source.
  - **RPT-bit set** – The (S,G) entry is pointing to the Rendezvous Point (RP), which normally indicates a pruned state along the shared tree for a particular source.
  - **SPT-bit set** – Multicast packets have been received from a source on shortest path tree.

- **Join SPT** – The rate of traffic arriving over the shared tree has exceeded the SPT-threshold for this group. If the SPT flag is set for (*,G) entries, the next (S,G) packet received will cause the router to join the shortest path tree. If the SPT flag is set for (S,G), the router immediately joins the shortest path tree.

Downstream Interface List –

- **Interface** – Interface(s) on which multicast subscribers have been recorded.

- **State** – The flags associated with each downstream interface indicate:
  - **Forward** – Traffic received from the upstream interface is being forwarded to this interface.
  - **Local** – Downstream interface has received IGMP report message from host in this subnet.
  - **Pruned** – This route has been terminated.
  - **Registering** - A downstream device is registering for a multicast source.

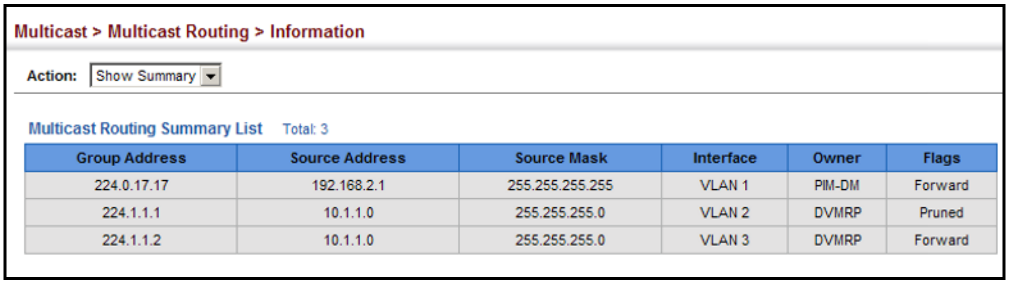
WEB INTERFACE (IPV4)

To display the multicast routing table:

1. Click Multicast, Multicast Routing, Information.

2. Select Show Summary from the Action List.

Figure 520: Displaying the IPv4 Multicast Routing Table



Multicast > Multicast Routing > Information

Action: Show Summary

Multicast Routing Summary List Total: 3

Group Address	Source Address	Source Mask	Interface	Owner	Flags
224.0.17.17	192.168.2.1	255.255.255.255	VLAN 1	PIM-DM	Forward
224.1.1.1	10.1.1.0	255.255.255.0	VLAN 2	DVMRP	Pruned
224.1.1.2	10.1.1.0	255.255.255.0	VLAN 3	DVMRP	Forward

To display detailed information on a specific flow in multicast routing table:

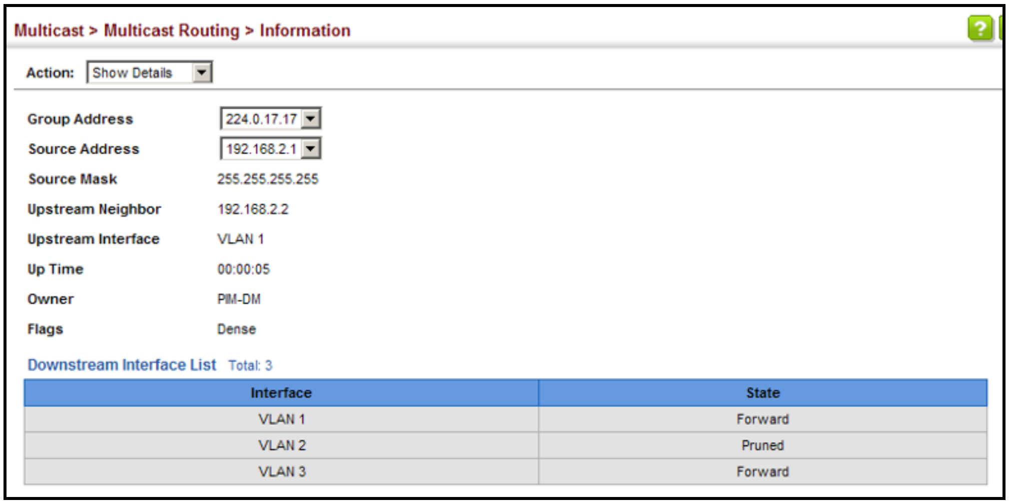
1. Click Multicast, Multicast Routing, Information.

2. Select Show Details from the Action List.

3. Select a Group Address.

4. Select a Source Address.

Figure 521: Displaying Detailed Entries from IPv4 Multicast Routing Table



Multicast > Multicast Routing > Information

Action: Show Details

Group Address	224.0.17.17
Source Address	192.168.2.1
Source Mask	255.255.255.255
Upstream Neighbor	192.168.2.2
Upstream Interface	VLAN 1
Up Time	00:00:05
Owner	PIM-DM
Flags	Dense

Downstream Interface List Total: 3

Interface	State
VLAN 1	Forward
VLAN 2	Pruned
VLAN 3	Forward

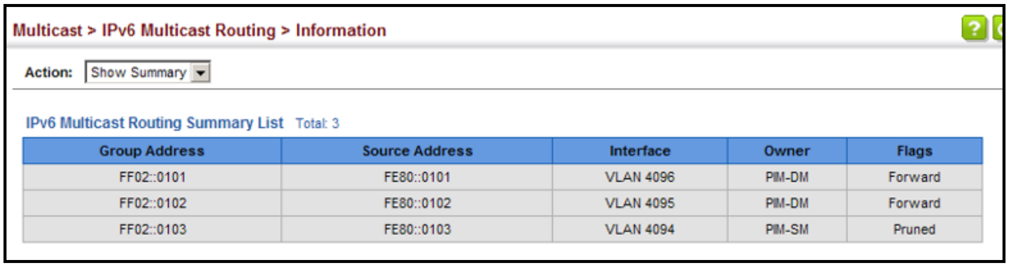
WEB INTERFACE (IPV6)

To display the multicast routing table:

1. Click Multicast, IPv6 Multicast Routing, Information.

2. Select Show Summary from the Action List.

Figure 522: Displaying the IPv6 Multicast Routing Table



Multicast > IPv6 Multicast Routing > Information

Action: Show Summary

IPv6 Multicast Routing Summary List Total: 3

Group Address	Source Address	Interface	Owner	Flags
FF02::0101	FE80::0101	VLAN 4096	PIM-DM	Forward
FF02::0102	FE80::0102	VLAN 4095	PIM-DM	Forward
FF02::0103	FE80::0103	VLAN 4094	PIM-SM	Pruned

To display detailed information on a specific flow in multicast routing table:

1. Click Multicast, IPv6 Multicast Routing, Information.

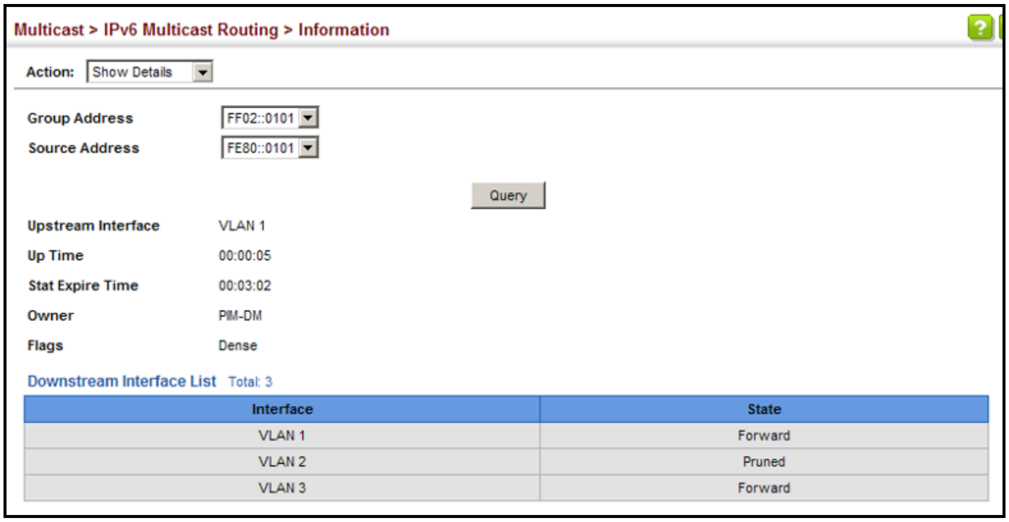
2. Select Show Details from the Action List.

3. Select a Group Address.

4. Select a Source Address.

5. Click Query.

Figure 523: Displaying Detailed Entries from IPv6 Multicast Routing Table



Action: Show Details

Group Address: FF02::0101
Source Address: FE80::0101

Upstream Interface: VLAN 1
Up Time: 00:00:05
Stat Expire Time: 00:03:02
Owner: PIM-DM
Flags: Dense

Downstream Interface List Total: 3

Interface	State
VLAN 1	Forward
VLAN 2	Pruned
VLAN 3	Forward

CONFIGURING PIM FOR IPV4

This section describes how to configure PIM-DM and PIM-SM for IPv4.

ENABLING PIM GLOBALLY

Use the Routing Protocol > PIM > General page to enable IPv4 PIM routing globally on the router.

CLI REFERENCES

- "router pim" on page 1928

COMMAND USAGE

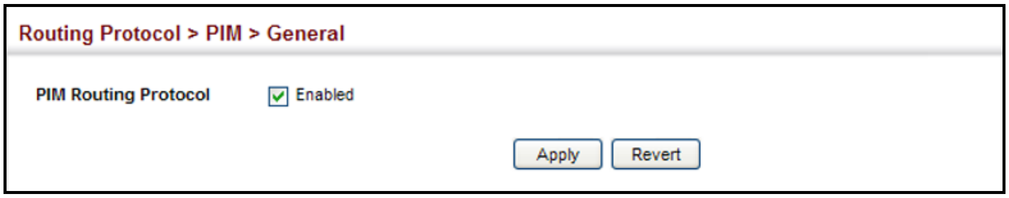
- This feature enables PIM-DM and PIM-SM globally for the router. You also need to enable PIM-DM or PIM-SM for each interface that will support multicast routing (see page 834), and make any changes necessary to the multicast protocol parameters.
- To use PIM, multicast routing must be enabled on the switch (see "Enabling Multicast Routing Globally" on page 828).

WEB INTERFACE

To enable PIM multicast routing:

1. Click Routing Protocol, PIM, General.
2. Enable PIM Routing Protocol.
3. Click Apply.

Figure 524: Enabling PIM Multicast Routing



Routing Protocol > PIM > General

PIM Routing Protocol ☑ Enabled

CONFIGURING PIM INTERFACE SETTINGS

Use the Routing Protocol > PIM > Interface page configure the routing protocol's functional attributes for each interface.

CLI REFERENCES

- "IPv4 PIM Commands" on page 1927

COMMAND USAGE

- Most of the attributes on this page are common to both PIM-DM and PIM-SM. Select Dense or Sparse Mode to display the common attributes, as well as those applicable to the selected mode.

- PIM and IGMP proxy cannot be used at the same time. When an interface is set to use PIM Dense mode or Sparse mode, IGMP proxy cannot be enabled on any interface of the device (see "Configuring IGMP Snooping and Query Parameters" on page 613). Also, when IGMP proxy is enabled on an interface, PIM cannot be enabled on any interface.

PIM-DM

- PIM-DM functions similar to DVMRP by periodically flooding the network with traffic from any active multicast server. It also uses IGMP to determine the presence of multicast group members. The main difference, is that it uses the router's unicast routing table to determine if the interface through which a packet is received provides the shortest path back to the source.

- Dense-mode interfaces are subject to multicast flooding by default, and are only removed from the multicast routing table when the router determines that there are no group members or downstream routers, or when a prune message is received from a downstream router.

PIM-SM

- A PIM-SM interface is used to forward multicast traffic only if a join message is received from a downstream router or if group members are directly connected to the interface. When routers want to receive a multicast flow, they periodically send join messages to the RP, and are subsequently added to the shared path for the specified flow back up to the RP. If routers want to join the source path up through the SPT, they periodically send join messages toward the source. They also send prune messages toward the RP to prune the shared path once they have connected to the source through the SPT, or if there are no longer any group members connected to the interface.

PARAMETERS

These parameters are displayed:

Common Attributes

- **VLAN** – Layer 3 VLAN interface. (Range: 1-4094)

- **Mode** – PIM routing mode. (Options: Dense, Sparse, None)

- **IP Address** – Primary IP address assigned to the selected VLAN.

- **Hello Holdtime** – Sets the interval to wait for hello messages from a neighboring PIM router before declaring it dead. Note that the hello holdtime should be greater than or equal to the value of Hello Interval, otherwise it will be automatically set to 3.5 x the Hello Interval. (Range: 1-65535 seconds; Default: 105 seconds, or 3.5 times the hello interval if set)

- **Hello Interval** – Sets the frequency at which PIM hello messages are transmitted out on all interfaces. (Range: 1-65535 seconds; Default: 30 seconds)

  Hello messages are sent to neighboring PIM routers from which this device has received probes, and are used to verify whether or not these neighbors are still active members of the multicast tree. PIM-SM routers use these messages not only to inform neighboring routers of their presence, but also to determine which router for each LAN segment will serve as the Designated Router (DR).

  When a router is booted or first configured to use PIM, it sends an initial hello message, and then sets its Hello timer to the configured value. If a router does not hear from a neighbor for the period specified by the Hello Holdtime, that neighbor is dropped. This hold time is included in each hello message received from a neighbor. Also note that hello messages also contain the DR priority of the router sending the message.

  If the hello holdtime is already configured, and the hello interval is set to a value longer than the hello holdtime, this command will fail.

- **Join/Prune Holdtime** – Sets the hold time for the prune state. (Range: 1-65535 seconds; Default: 210 seconds)

  - PIM-DM: The multicast interface that first receives a multicast stream from a particular source forwards this traffic to all other PIM-DM interfaces on the router. If there are no requesting groups on that interface, the leaf node sends a prune message upstream and enters a prune state for this multicast stream. The prune state is maintained until the join/prune holdtime timer expires or a graft message is received for the forwarding entry.

  - PIM-SM: The multicast interface that first receives a multicast stream from a particular source forwards this traffic only to those interfaces on the router that have requests to join this group. When there are no longer any requesting groups on that interface, the leaf node sends a prune message upstream and enters a prune state for this multicast stream. The protocol maintains both the current join state and the pending RPT prune state for this (source, group) pair until the join/prune interval timer expires.

- **LAN Prune Delay** – Causes this device to inform downstream routers of how long it will wait before pruning a flow after receiving a prune request. (Default: Disabled)

  When other downstream routers on the same VLAN are notified that this upstream router has received a prune request, they must send a Join to override the prune before the prune delay expires if they want to continue receiving the flow. The message generated by this command effectively prompts any downstream neighbors with hosts receiving the flow to reply with a Join message. If no join messages are received after the prune delay expires, this router will prune the flow.

  The sum of the Override Interval and Propagation Delay are used to calculate the LAN prune delay.

- **Override Interval** – The time required for a downstream router to respond to a LAN Prune Delay message by sending back a Join message if it wants to continue receiving the flow referenced in the message. (Range: 500-6000 milliseconds; Default: 2500 milliseconds)

  The override interval and the propagation delay are used to calculate the LAN prune delay. If a downstream router has group members which want to continue receiving the flow referenced in a LAN prune delay message, then the override interval represents the time required for the downstream router to process the message and then respond by sending a Join message back to the upstream router to ensure that the flow is not terminated.

- **Propagation Delay** – The time required for a LAN prune delay message to reach downstream routers. (Range: 100-5000 milliseconds; Default: 500 milliseconds)

  The override interval and pro po gat ion delay are used to calculate the LAN prune delay. If a downstream router has group members which want to continue receiving the flow referenced in a LAN prune delay message, then the propagation delay represents the time required for the LAN prune delay message to be propagated down from the upstream router to all downstream routers attached to the same VLAN interface.

- **Trigger Hello Delay** – The maximum time before transmitting a triggered PIM Hello message after the router is rebooted or PIM is enabled on an interface. (Range: 0-5 seconds; Default: 5 seconds)

  When a router first starts or PIM is enabled on an interface, the hello delay is set to random value between 0 and the trigger hello delay. This prevents synchronization of Hello messages on multi-access links if multiple routers are powered on simultaneously.

  Also, if a Hello message is received from a new neighbor, the receiving router will send its own Hello message after a random delay between 0 and the trigger hello delay.

Dense-Mode Attributes

- **Graft Retry Interval** – The time to wait for a Graft acknowledgement before resending a Graft message. (Range: 1-10 seconds; Default: 3 seconds)

  A graft message is sent by a router to cancel a prune state. When a router receives a graft message, it must respond with an graft acknowledgement message. If this acknowledgement message is lost, the router that sent the graft message will resend it a number of times (as defined by Max. Graft Retries).

- **Max. Graft Retries** – The maximum number of times to resend a Graft message if it has not been acknowledged. (Range: 1-10; Default: 3)

- **State Refresh Origination Interval** – The interval between sending PIM-DM state refresh control messages. (Range: 1-100 seconds; Default: 60 seconds)

  The pruned state times out approximately every three minutes and the entire PIM-DM network is reflooded with multicast packets and prune messages. The state refresh feature keeps the pruned state from timing out by periodically forwarding a control message down the distribution tree, refreshing the prune state on the outgoing interfaces of each router in the tree. This also enables PIM routers to recognize topology changes (sources joining or leaving a multicast group) before the default three-minute state timeout expires.

  This command is only effectively for interfaces of first hop, PIM-DM routers that are directly connected to the sources of multicast groups.

Sparse-Mode Attributes

- **DR Priority** – Sets the priority advertised by a router when bidding to become the Designated Router (DR). (Range: 0-4294967294; Default: 1)

  More than one PIM-SM router may be connected to an Ethernet or other shared-media LAN. If multicast hosts are directly connected to the LAN, then only one of these routers is elected as the DR, and acts on behalf of these hosts, sending periodic Join/Prune messages toward a group-specific RP for each group. A single DR is elected per interface (LAN or otherwise) using a simple election process.

  The router with the highest priority configured on an interface is elected as the DR. If more than one router attached to this interface uses the same priority, then the router with the highest IP address is elected to serve as the DR.

  If a router does not advertise a priority in its hello messages, it is assumed to have the highest priority and is elected as the DR. If more than one router is not advertising its priority, then the router with the highest IP address is elected to serve as the DR.

- **Join/Prune Interval** – Sets the interval at which join/prune messages are sent. (Range: 1-65535 seconds; Default: 60 seconds)

By default, the switch sends join/prune messages every 60 seconds to inform other PIM-SM routers about clients who want to join or leave a multicast group.

Use the same join/prune message interval on all PIM-SM routers in the same PIM-SM domain, otherwise the routing protocol's performance will be adversely affected.

The multicast interface that first receives a multicast stream from a particular source forwards this traffic only to those interfaces on the router that have requests to join this group. When there are no longer any requesting groups on that interface, the leaf node sends a prune message upstream and enters a prune state for this multicast stream. The protocol maintains both the current join state and the pending RPT prune state for this (source, group) pair until the join/prune interval timer expires.

WEB INTERFACE

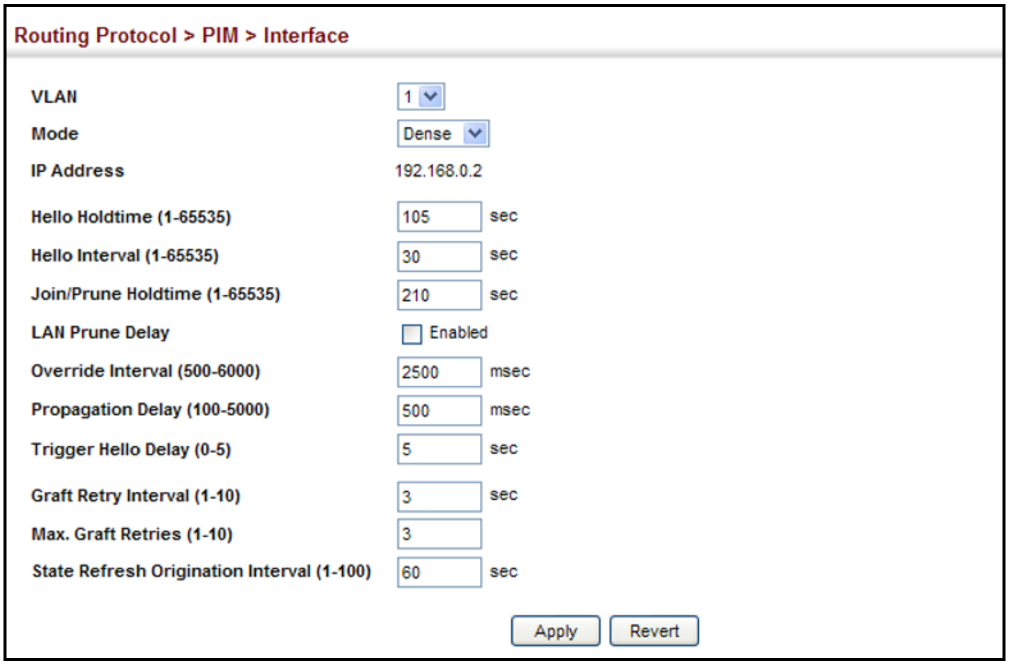
To configure PIM interface settings:

1. Click Routing Protocol, PIM, Interface.

2. Modify any of the protocol parameters as required.

3. Click Apply.

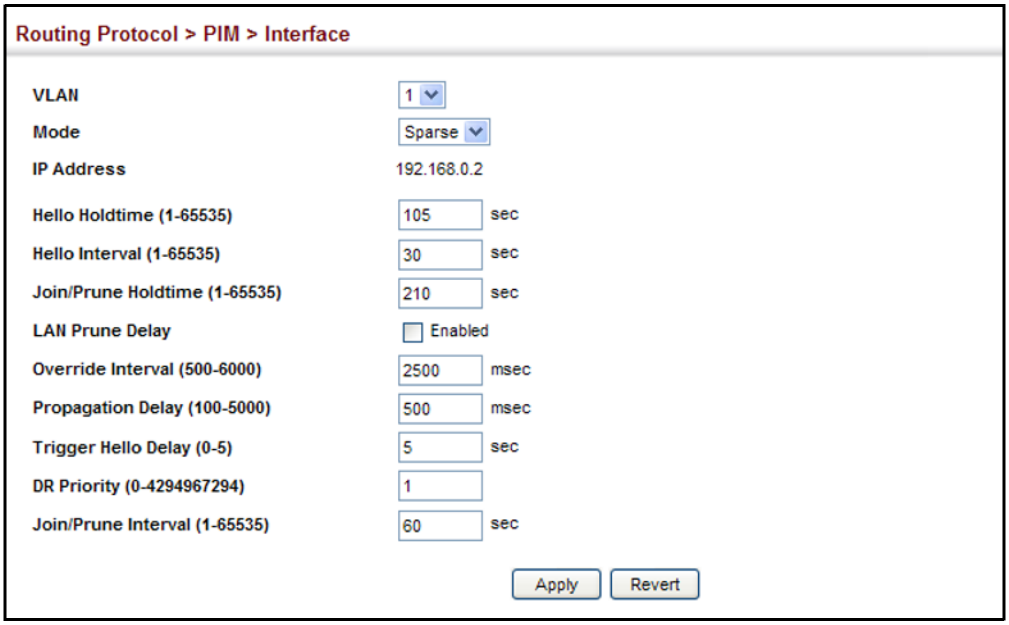
Figure 525: Configuring PIM Interface Settings (Dense Mode)



Routing Protocol > PIM > Interface

VLAN	1
Mode	Dense
IP Address	192.168.0.2
Hello Holdtime (1-65535)	105 sec
Hello Interval (1-65535)	30 sec
Join/Prune Holdtime (1-65535)	210 sec
LAN Prune Delay	□ Enabled
Override Interval (500-6000)	2500 msec
Propagation Delay (100-5000)	500 msec
Trigger Hello Delay (0-5)	5 sec
Graft Retry Interval (1-10)	3 sec
Max. Graft Retries (1-10)	3
State Refresh Origination Interval (1-100)	60 sec

Figure 526: Configuring PIM Interface Settings (Sparse Mode)



Routing Protocol > PIM > Interface

VLAN	1	
Mode	Sparse	
IP Address	192.168.0.2	
Hello Holdtime (1-65535)	105	sec
Hello Interval (1-65535)	30	sec
Join/Prune Holdtime (1-65535)	210	sec
LAN Prune Delay	□ Enabled	
Override Interval (500-6000)	2500	msec
Propagation Delay (100-5000)	500	msec
Trigger Hello Delay (0-5)	5	sec
DR Priority (0-4294967294)	1	
Join/Prune Interval (1-65535)	60	sec

DISPLAYING PIM NEIGHBOR INFORMATION

Use the Routing Protocol > PIM > Neighbor page to display all neighboring PIM routers.

CLI REFERENCES

- "show ip pim neighbor" on page 1936

PARAMETERS

These parameters are displayed:

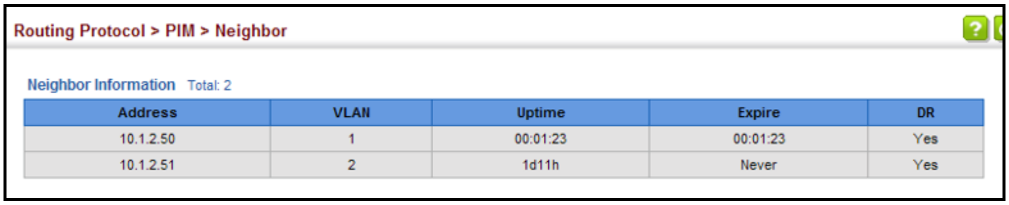
- **Address** – IP address of the next-hop router.
- **VLAN** – VLAN that is attached to this neighbor.
- **Uptime** – The duration this entry has been active.
- **Expire** – The time before this entry will be removed.
- **DR** – Indicates if a neighbor is the designated router.

WEB INTERFACE

To display neighboring PIM routers:

1. Click Routing Protocol, PIM, Neighbor.

Figure 527: Showing PIM Neighbors



Routing Protocol > PIM > Neighbor

Neighbor Information Total: 2

Address	VLAN	Uptime	Expire	DR
10.1.2.50	1	00:01:23	00:01:23	Yes
10.1.2.51	2	1d11h	Never	Yes

CONFIGURING GLOBAL PIM-SM SETTINGS

Use the Routing Protocol > PIM > SM (Configure Global) page to configure the rate at which register messages are sent, the source of register messages, and switchover to the Shortest Path Tree (SPT).

CLI REFERENCES

- "IPv4 PIM Commands" on page 1927

PARAMETERS

These parameters are displayed:

- **Register Rate Limit** – Configures the rate at which register messages are sent by the Designated Router (DR) for each (source, group) entry. (Range: 1-65535 packets per second: Default: disabled)

  This parameter can be used to relieve the load on the designated router (DR) and rendezvous point (RP). However, because register messages exceeding the limit are dropped, some receivers may experience data packet loss within the first few seconds in which register messages are sent from bursty sources.

- **Register Source** – Configures the IP source address of a register message to an address other than the outgoing interface address of the DR that leads back toward the RP. (Range: VLAN 1-4094; Default: The IP address of the DR's outgoing interface that leads back to the RP)

  When the source address of a register message is filtered by intermediate network devices, or is not a uniquely routed address to which the RP can send packets, the replies sent from the RP to the source address will fail to reach the DR, resulting in PIM-SM protocol failures. This type of problem can be overcome by manually configuring the source address of register messages to an interface that leads back to the RP.

- **SPT Threshold** – Prevents the last-hop PIM-SM router from switching to Shortest Path Source Tree (SPT) mode. (Options: Infinity, Reset; Default: Reset, to use the SPT)

  The default path for packets from a multicast source to a receiver is through the RP. However, the path through the RP is not always the shortest path. Therefore, the router uses the RP to forward only the first packet from a new multicast group to its receivers. Afterwards, it calculates the shortest path tree (SPT) directly between the receiver and source, and then uses the SPT to send all subsequent packets from the source to the receiver instead of using the shared tree. Note that when the SPT threshold is not set by this command, the PIM leaf router will join the shortest path tree immediately after receiving the first packet from a new source.

Enable the SPT threshold by selecting “Reset” to force the router to use the shared tree for all multicast groups, or just for the specified multicast groups. (This is the default setting.)

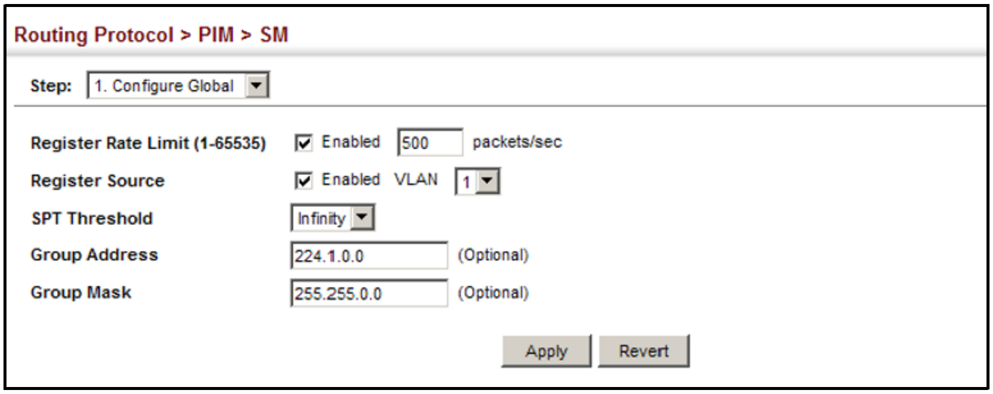
- **Group Address** – An IP multicast group address. If a group address is not specified, the shared tree is used for all multicast groups.
- **Group Mask** – Subnet mask that is used for the group address.

WEB INTERFACE

To configure global settings for PIM-SM:

1. Click Multicast, Multicast Routing, SM.
2. Select Configure Global from the Step list.
3. Set the register rate limit and source of register messages if required. Also specify any multicast groups which must be routed across the shared tree, instead of switching over to the SPT.
4. Click Apply.

Figure 528: Configuring Global Settings for PIM-SM



Routing Protocol > PIM > SM

Step: 1. Configure Global

Register Rate Limit (1-65535)	☑ Enabled 500 packets/sec
Register Source	☑ Enabled VLAN 1
SPT Threshold	Infinity
Group Address	224.1.0.0 (Optional)
Group Mask	255.255.0.0 (Optional)

CONFIGURING A PIM BSR CANDIDATE

Use the Routing Protocol > PIM > SM (BSR Candidate) page to configure the switch as a Bootstrap Router (BSR) candidate.

CLI REFERENCES

- "ip pim bsr-candidate" on page 1938

COMMAND USAGE

- When this router is configured as a BSR candidate, it starts sending bootstrap messages to all of its PIM-SM neighbors. The primary IP address of the designated VLAN is sent as the candidate's BSR address. Each neighbor receiving the bootstrap message compares the BSR address with the address from previous messages. If the current address is the same or a higher address, it accepts the bootstrap message and forwards it. Otherwise, it drops the message.

- This router will continue to be the BSR until it receives a bootstrap message from another candidate with a higher priority (or a higher IP address if the priorities are the same).

- To improve failover recovery, it is advisable to select at least two core routers in diverse locations, each to serve as both a candidate BSR and candidate RP. It is also preferable to set up one of these routers as both the primary BSR and RP.

PARAMETERS

These parameters are displayed:

- **BSR Candidate Status** – Configures the switch as a Bootstrap Router (BSR) candidate. (Default: Disabled)

- **VLAN ID** – Identifier of configured VLAN interface. (Range: 1-4094)

- **Hash Mask Length** – Hash mask length (in bits) used for RP selection (see "Configuring a PIM Static Rendezvous Point" on page 843 and "Configuring a PIM RP Candidate" on page 845). The portion of the hash specified by the mask length is ANDed with the group address. Therefore, when the hash function is executed on any BSR, all groups with the same seed hash will be mapped to the same RP. If the mask length is less than 32, then only the first portion of the hash is used, and a single RP will be defined for multiple groups. (Range: 0-32; Default: 10)

- **Priority** – Priority used by the candidate bootstrap router in the election process. The BSR candidate with the largest priority is preferred. If the priority values are the same, the candidate with the larger IP address is elected to be the BSR. Setting the priority to zero means that this router is not eligible to server as the BSR. At least one router in the PIM-SM domain must be set to a value greater than zero. (Range: 0-255; Default: 0)

WEB INTERFACE

To configure the switch as a BSR candidate:

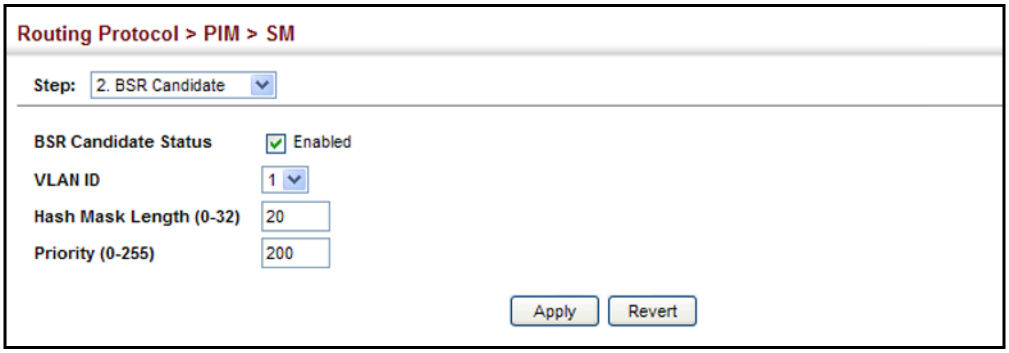
1. Click Routing Protocol, PIM, PIM-SM.

2. Select BSR Candidate from the Step list.

3. Specify the VLAN interface for which this router is bidding to become the BSR, the hash mask length that will subsequently be used for RP selection if this router is selected as the BSR, and the priority for BSR selection.

4. Click Apply.

Figure 529: Configuring a PIM-SM BSR Candidate



Routing Protocol > PIM > SM

Step: 2. BSR Candidate

BSR Candidate Status ☑ Enabled

VLAN ID 1

Hash Mask Length (0-32) 20

Priority (0-255) 200

CONFIGURING A PIM STATIC RENDEZVOUS POINT

Use the Routing Protocol > PIM > SM (RP Address) page to configure a static address as the Rendezvous Point (RP) for a particular multicast group.

CLI REFERENCES

- "ip pim rp-address" on page 1941

COMMAND USAGE

- The router will act as an RP for all multicast groups in the local PIM-SM domain if no groups are specified. A static RP can either be configured for the whole multicast group range 224/4, or for specific group ranges.

- If an IP address is specified that was previously used for an RP, then the older entry is replaced.

- Multiple RPs can be defined for different groups or group ranges. If a group is matched by more than one entry, the router will use the RP associated with the longer group prefix length. If the prefix lengths are the same, then the static RP with the highest IP address is chosen.

- Static definitions for RP addresses may be used together with RP addresses dynamically learned through the bootstrap router (BSR). If an RP address learned by the BSR and one statically configured using this command are both available for a group range, the RP address learned by the BSR is chosen over the one statically configured.

- All routers within the same PIM-SM domain must be configured with the same RP(s). Selecting an RP through the dynamic election process is therefore preferable for most situations. Using the dynamic RP election process also allows a backup RP to automatically take over if the active RP router becomes unavailable.

PARAMETERS

These parameters are displayed:

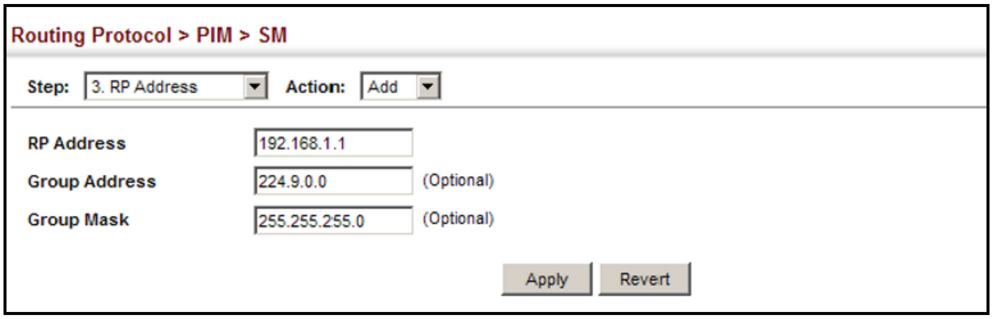
- **RP Address** – Static IP address of the router that will be an RP for the specified multicast group(s).
- **Group Address** – An IP multicast group address. If a group address is not specified, the RP is used for all multicast groups.
- **Group Mask** – Subnet mask that is used for the group address.

WEB INTERFACE

To configure a static rendezvous point:

1. Click Routing Protocol, PIM, PIM-SM.
2. Select RP Address from the Step list.
3. Specify the static RP to use for a multicast group, or a range of groups by using a subnet mask.
4. Click Apply.

Figure 530: Configuring a PIM Static Rendezvous Point



Routing Protocol > PIM > SM

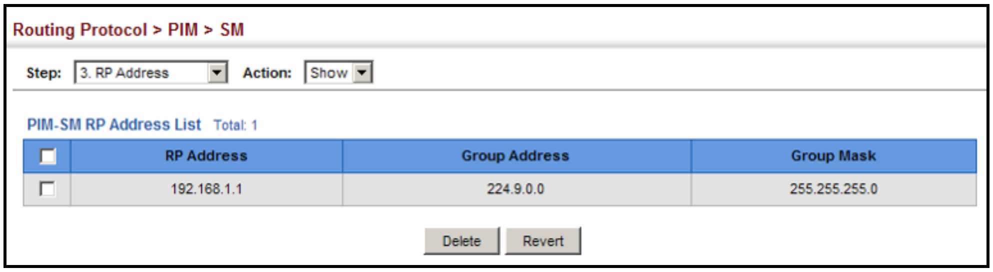
Step: 3. RP Address Action: Add

RP Address: 192.168.1.1
Group Address: 224.9.0.0 (Optional)
Group Mask: 255.255.255.0 (Optional)

To display static rendezvous points:

1. Click Routing Protocol, PIM, PIM-SM.
2. Select RP Address from the Step list.
3. Select Show from the Action list.

Figure 531: Showing PIM Static Rendezvous Points



Routing Protocol > PIM > SM

Step: 3. RP Address Action: Show

PIM-SM RP Address List Total: 1

□	RP Address	Group Address	Group Mask
□	192.168.1.1	224.9.0.0	255.255.255.0

CONFIGURING A PIM RP CANDIDATE

Use the Routing Protocol > PIM > SM (RP Candidate) page to configure the switch to advertise itself as a Rendezvous Point (RP) candidate to the bootstrap router (BSR).

CLI REFERENCES

- "ip pim rp-candidate" on page 1942

COMMAND USAGE

- When this router is configured as an RP candidate, it periodically sends PIMv2 messages to the BSR advertising itself as a candidate RP for the specified group addresses. The IP address of the designated VLAN is sent as the candidate's RP address. The BSR places information about all of the candidate RPs in subsequent bootstrap messages. The BSR uses the RP-election hash algorithm to select an active RP for each group range. The election process is performed by the BSR only for its own use. Each PIM-SM router that receives the list of RP candidates from the BSR also elects an active RP for each group range using the same election process.

- The election process for each group is based on the following criteria:

  - Find all RPs with the most specific group range.

  - Select those with the highest priority (lowest priority value).

  - Compute hash value based on the group address, RP address, priority, and hash mask included in the bootstrap messages.

  - If there is a tie, use the candidate RP with the highest IP address.

- This distributed election process provides faster convergence and minimal disruption when an RP fails. It also serves to provide load balancing by distributing groups across multiple RPs. Moreover, when an RP fails, the responsible RPs are re-elected on each router, and the groups automatically distributed to the remaining RPs.

- To improve failover recovery, it is advisable to select at least two core routers in diverse locations, each to serve as both a candidate BSR and candidate RP. It is also preferable to set up one of these routers as both the primary BSR and RP.

PARAMETERS

These parameters are displayed:

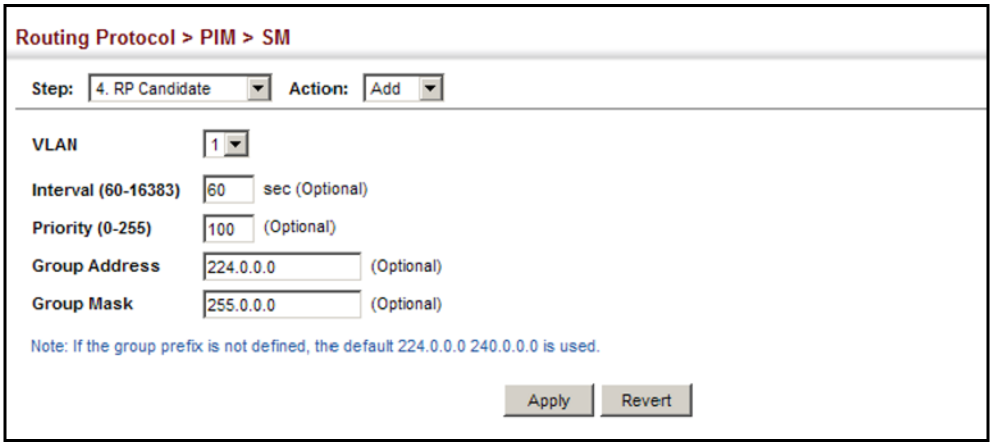
- **VLAN** – Identifier of configured VLAN interface. (Range: 1-4094)
- **Interval** – The interval at which this device advertises itself as an RP candidate. (Range: 60-16383 seconds; Default: 60 seconds)
- **Priority** – Priority used by the candidate RP in the election process. The RP candidate with the largest priority is preferred. If the priority values are the same, the candidate with the larger IP address is elected to be the RP. Setting the priority to zero means that this router is not eligible to server as the RP. (Range: 0-255; Default: 0)
- **Group Address** – An IP multicast group address. If not defined, the default address is 224.0.0.0/4, or the entire IPv4 multicast group.
- **Group Mask** – Subnet mask that is used for the group address.

WEB INTERFACE

To advertise the switch as an RP candidate:

1. Click Multicast, Multicast Routing, SM.
2. Select RP Candidate from the Step list.
3. Specify a VLAN interface, the interval at which to advertise the router as an RP candidate, the priority to use in the election process, and the multicast group address and mask indicating the groups for which this router is bidding to become the RP.
4. Click Apply.

Figure 532: Configuring a PIM RP Candidate



Routing Protocol > PIM > SM

Step: 4. RP Candidate Action: Add

VLAN: 1

Interval (60-16383): 60 sec (Optional)

Priority (0-255): 100 (Optional)

Group Address: 224.0.0.0 (Optional)

Group Mask: 255.0.0.0 (Optional)

Note: If the group prefix is not defined, the default 224.0.0.0 240.0.0.0 is used.

To display settings for an RP candidate:

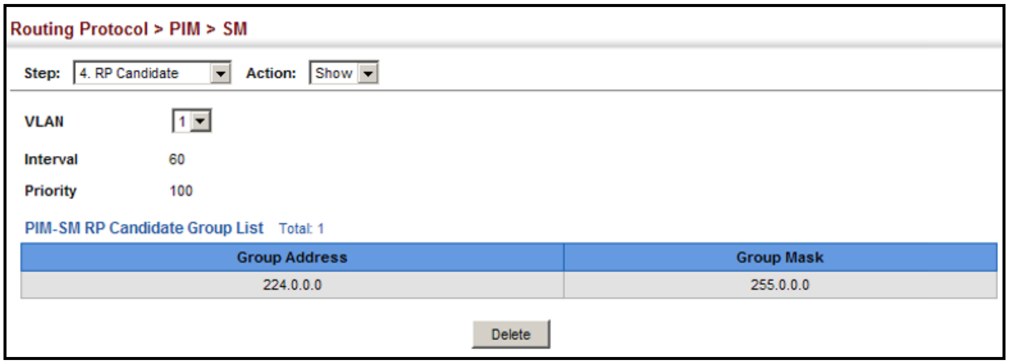
1. Click Routing Protocol, PIM, PIM-SM.

2. Select RP Candidate from the Step list.

3. Select Show from the Action list.

4. Select an interface from the VLAN list.

Figure 533: Showing Settings for a PIM RP Candidate



Routing Protocol > PIM > SM

Step: 4. RP Candidate   Action: Show

VLAN 1

Interval 60

Priority 100

PIM-SM RP Candidate Group List Total: 1

Group Address	Group Mask
224.0.0.0	255.0.0.0

DISPLAYING THE PIM BSR ROUTER

Use the Routing Protocol > PIM > SM (Show Information – Show BSR Router) page to display Information about the bootstrap router (BSR).

CLI REFERENCES

- "show ip pim bsr-router" on page 1947

PARAMETERS

These parameters are displayed:

- **IP Address** – IP address of interface configured as the BSR.

- **Uptime** – The time this BSR has been up and running.

- **Priority** – Priority value used by this BSR candidate.

- **Hash Mask Length** – The number of significant bits used in the multicast group comparison mask by this BSR candidate.

- **Expire** – The time before the BSR is declared down.

- **Role** – Candidate or non-candidate BSR.

- **State**[15] – Operation state of BSR includes:

  - No information – No information is stored for this device.

[15] These parameters are based on RFC 5059.

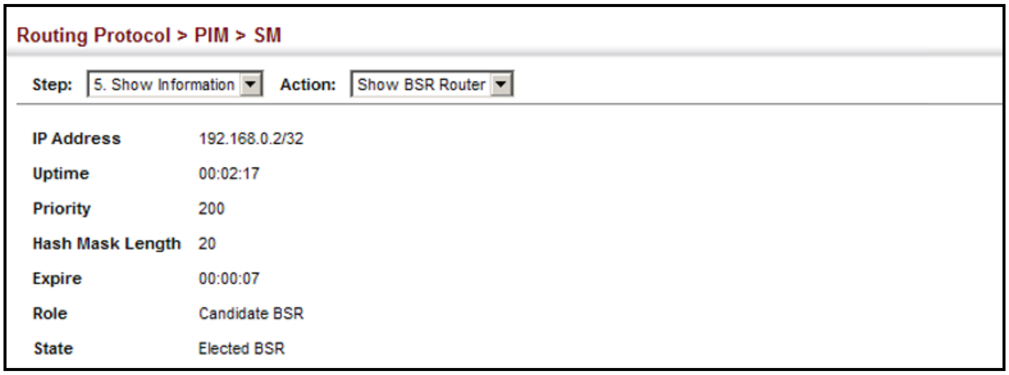
- Accept Any – The router does not know of an active BSR, and will accept the first bootstrap message it sees as giving the new BSR's identity and the RP-set.
- Accept Preferred – The router knows the identity of the current BSR, and is using the RP-set provided by that BSR. Only bootstrap messages from that BSR or from a C-BSR with higher weight than the current BSR will be accepted.
- Candidate BSR – Bidding in election process.
- Pending-BSR – The router is a candidate to be the BSR for the RP-set. Currently, no other router is the preferred BSR, but this router is not yet the elected BSR.
- Elected BSR – Elected to serve as BSR.

WEB INTERFACE

To display information about the BSR:

1. Click Routing Protocol, PIM, PIM-SM.
2. Select Show Information from the Step list.
3. Select Show BSR Router from the Action list.

Figure 534: Showing Information About the PIM BSR



Step: 5. Show Information Action: Show BSR Router

IP Address	192.168.0.2/32
Uptime	00:02:17
Priority	200
Hash Mask Length	20
Expire	00:00:07
Role	Candidate BSR
State	Elected BSR

DISPLAYING PIM RP MAPPING

Use the Routing Protocol > PIM > SM (Show Information – Show RP Mapping) page to display active RPs and associated multicast routing entries.

CLI REFERENCES

- "show ip pim rp mapping" on page 1948

PARAMETERS

These parameters are displayed:

- **Groups** – A multicast group address.

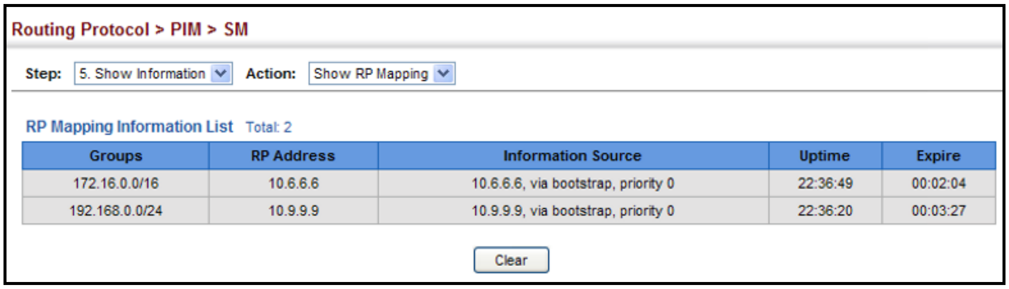
- **RP Address** – IP address of the RP for the listed multicast group.
- **Information Source** – RP that advertised the mapping, how the RP was selected (Static or Bootstrap), and the priority used in the bidding process.
- **Uptime** – The time this RP has been up and running
- **Expire** – The time before this entry will be removed.

WEB INTERFACE

To display the RPs mapped to multicast groups:

1. Click Multicast, Multicast Routing, SM.
2. Select Show Information from the Step list.
3. Select Show RP Mapping from the Action list.

Figure 535: Showing PIM RP Mapping



Step: 5. Show Information Action: Show RP Mapping

RP Mapping Information List Total: 2

Groups	RP Address	Information Source	Uptime	Expire
172.16.0.0/16	10.6.6.6	10.6.6.6, via bootstrap, priority 0	22:36:49	00:02:04
192.168.0.0/24	10.9.9.9	10.9.9.9, via bootstrap, priority 0	22:36:20	00:03:27

CONFIGURING PIMV6 FOR IPV6

This section describes how to configure PIM-DM and PIM-SM for IPv6.

ENABLING PIMV6 GLOBALLY

Use the Routing Protocol > PIM6 > General page to enable IPv6 PIM routing globally on the router.

CLI REFERENCES

- "router pim6" on page 1951

COMMAND USAGE

- This feature enables PIM-DM and PIM-SM for IPv6 globally on the router. You also need to enable PIM-DM and PIM-SM for each interface that will support multicast routing (see page 850), and make any changes necessary to the multicast protocol parameters.
- To use PIMv6, multicast routing must be enabled on the switch (see "Enabling Multicast Routing Globally" on page 828).

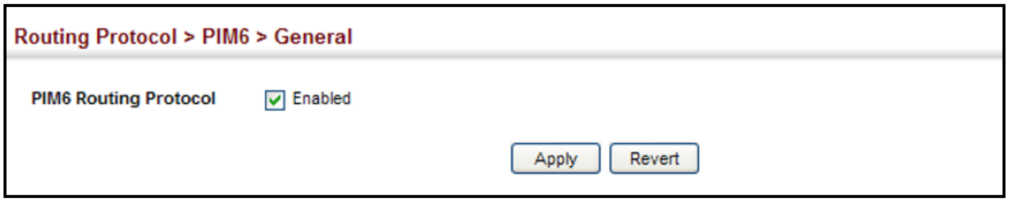
- To use multicast routing, MLD proxy cannot be enabled on any interface of the device (see "MLD Proxy Routing" on page 1533).

WEB INTERFACE

To enable PIMv6 multicast routing:

1. Click Routing Protocol, PIM6, General.
2. Enable PIM6 Routing Protocol.
3. Click Apply.

Figure 536: Enabling PIMv6 Multicast Routing



Routing Protocol > PIM6 > General

PIM6 Routing Protocol ☑ Enabled

CONFIGURING PIMV6 INTERFACE SETTINGS

Use the Routing Protocol > PIM6 > Interface page configure the routing protocol's functional attributes for each interface.

CLI REFERENCES

- "IPv6 PIM Commands" on page 1950

COMMAND USAGE

- Most of the attributes on this page are common to both PIM6-DM and PIM6-SM. Select Dense or Sparse Mode to display the common attributes, as well as those applicable to the selected mode.

- An IPv6 address must first be assigned to the required routing interface before PIMv6 can be configured on this page.

- PIMv6 and MLD proxy cannot be used at the same time. When an interface is set to use PIMv6 Dense mode, MLD proxy cannot be enabled on any interface of the device (see "MLD Proxy Routing" on page 1533). Also, when MLD proxy is enabled on an interface, PIMv6 cannot be enabled on any interface.

PIM6-DM

- PIM6-DM functions similar to DVMRP by periodically flooding the network with traffic from any active multicast server. It also uses MLD to determine the presence of multicast group members. The main difference, is that it uses the router's unicast routing table to determine if the interface through which a packet is received provides the shortest path back to the source.

- Dense-mode interfaces are subject to multicast flooding by default, and are only removed from the multicast routing table when the router determines that there are no group members or downstream routers, or when a prune message is received from a downstream router.

PIM6-SM

- A PIM6-SM interface is used to forward multicast traffic only if a join message is received from a downstream router or if group members are directly connected to the interface. When routers want to receive a multicast flow, they periodically send join messages to the RP, and are subsequently added to the shared path for the specified flow back up to the RP. If routers want to join the source path up through the SPT, they periodically send join messages toward the source. They also send prune messages toward the RP to prune the shared path once they have connected to the source through the SPT, or if there are no longer any group members connected to the interface.

Parameters

These parameters are displayed:

Common Attributes

- **VLAN** – Layer 3 VLAN interface. (Range: 1-4094)

- **Mode** – PIMv6 routing mode. (Options: Dense, Sparse, None)

  The routing mode must first be set to None, before changing between Dense and Sparse modes.

- **IPv6 Address** – IPv6 link-local address assigned to the selected VLAN.

- **Hello Holdtime** – Sets the interval to wait for hello messages from a neighboring PIM router before declaring it dead. Note that the hello holdtime should be greater than or equal to the value of Hello Interval, otherwise it will be automatically set to 3.5 x the Hello Interval. (Range: 1-65535 seconds; Default: 105 seconds, or 3.5 times the hello interval if set)

- **Hello Interval** – Sets the frequency at which PIM hello messages are transmitted out on all interfaces. (Range: 1-65535 seconds; Default: 30 seconds)

  Hello messages are sent to neighboring PIM routers from which this device has received probes, and are used to verify whether or not these neighbors are still active members of the multicast tree. PIM-SM routers use these messages not only to inform neighboring routers of their presence, but also to determine which router for each LAN segment will serve as the Designated Router (DR).

  When a router is booted or first configured to use PIM, it sends an initial hello message, and then sets its Hello timer to the configured value. If a router does not hear from a neighbor for the period specified by the Hello Holdtime, that neighbor is dropped. This hold time is included in each hello message received from a neighbor. Also note that hello messages also contain the DR priority of the router sending the message.

If the hello holdtime is already configured, and the hello interval is set to a value longer than the hello holdtime, this command will fail.

- **Join/Prune Holdtime** – Sets the hold time for the prune state. (Range: 1-65535 seconds; Default: 210 seconds)
  - PIM-DM: The multicast interface that first receives a multicast stream from a particular source forwards this traffic to all other PIM-DM interfaces on the router. If there are no requesting groups on that interface, the leaf node sends a prune message upstream and enters a prune state for this multicast stream. The prune state is maintained until the join/prune holdtime timer expires or a graft message is received for the forwarding entry.
  - PIM-SM: The multicast interface that first receives a multicast stream from a particular source forwards this traffic only to those interfaces on the router that have requests to join this group. When there are no longer any requesting groups on that interface, the leaf node sends a prune message upstream and enters a prune state for this multicast stream. The protocol maintains both the current join state and the pending RPT prune state for this (source, group) pair until the join/prune interval timer expires.

- **LAN Prune Delay** – Causes this device to inform downstream routers of how long it will wait before pruning a flow after receiving a prune request. (Default: Disabled)

  When other downstream routers on the same VLAN are notified that this upstream router has received a prune request, they must send a Join to override the prune before the prune delay expires if they want to continue receiving the flow. The message generated by this command effectively prompts any downstream neighbors with hosts receiving the flow to reply with a Join message. If no join messages are received after the prune delay expires, this router will prune the flow.

  The sum of the Override Interval and Propagation Delay are used to calculate the LAN prune delay.

- **Override Interval** – The time required for a downstream router to respond to a LAN Prune Delay message by sending back a Join message if it wants to continue receiving the flow referenced in the message. (Range: 500-6000 milliseconds; Default: 2500 milliseconds)

  The override interval and the propagation delay are used to calculate the LAN prune delay. If a downstream router has group members which want to continue receiving the flow referenced in a LAN prune delay message, then the override interval represents the time required for the downstream router to process the message and then respond by sending a Join message back to the upstream router to ensure that the flow is not terminated.

- **Propagation Delay** – The time required for a LAN prune delay message to reach downstream routers. (Range: 100-5000 milliseconds; Default: 500 milliseconds)

  The override interval and pro po gat ion delay are used to calculate the LAN prune delay. If a downstream router has group members which want to continue receiving the flow referenced in a LAN prune delay message, then the propagation delay represents the time required for the LAN prune delay message to be propagated down from the upstream router to all downstream routers attached to the same VLAN interface.

- **Trigger Hello Delay** – The maximum time before transmitting a triggered PIM Hello message after the router is rebooted or PIM is enabled on an interface. (Range: 0-5 seconds; Default: 5 seconds)

  When a router first starts or PIM is enabled on an interface, the hello delay is set to random value between 0 and the trigger hello delay. This prevents synchronization of Hello messages on multi-access links if multiple routers are powered on simultaneously.

  Also, if a Hello message is received from a new neighbor, the receiving router will send its own Hello message after a random delay between 0 and the trigger hello delay.

Dense-Mode Attributes

- **Graft Retry Interval** – The time to wait for a Graft acknowledgement before resending a Graft message. (Range: 1-10 seconds; Default: 3 seconds)

  A graft message is sent by a router to cancel a prune state. When a router receives a graft message, it must respond with an graft acknowledgement message. If this acknowledgement message is lost, the router that sent the graft message will resend it a number of times (as defined by Max. Graft Retries).

- **Max. Graft Retries** – The maximum number of times to resend a Graft message if it has not been acknowledged. (Range: 1-10; Default: 3)

- **State Refresh Origination Interval** – The interval between sending PIM-DM state refresh control messages. (Range: 1-100 seconds; Default: 60 seconds)

  The pruned state times out approximately every three minutes and the entire PIM-DM network is reflooded with multicast packets and prune messages. The state refresh feature keeps the pruned state from timing out by periodically forwarding a control message down the distribution tree, refreshing the prune state on the outgoing interfaces of each router in the tree. This also enables PIM routers to recognize topology changes (sources joining or leaving a multicast group) before the default three-minute state timeout expires.

  This command is only effectively for interfaces of first hop, PIM-DM routers that are directly connected to the sources of multicast groups.

Sparse-Mode Attributes

- **DR Priority** – Sets the priority advertised by a router when bidding to become the Designated Router (DR). (Range: 0-4294967294; Default: 1)

  More than one PIM-SM router may be connected to an Ethernet or other shared-media LAN. If multicast hosts are directly connected to the LAN, then only one of these routers is elected as the DR, and acts on behalf of these hosts, sending periodic Join/Prune messages toward a group-specific RP for each group. A single DR is elected per interface (LAN or otherwise) using a simple election process.

The router with the highest priority configured on an interface is elected as the DR. If more than one router attached to this interface uses the same priority, then the router with the highest IP address is elected to serve as the DR.

If a router does not advertise a priority in its hello messages, it is assumed to have the highest priority and is elected as the DR. If more than one router is not advertising its priority, then the router with the highest IP address is elected to serve as the DR.

- **Join/Prune Interval** – Sets the interval at which join/prune messages are sent. (Range: 1-65535 seconds; Default: 60 seconds)

  By default, the switch sends join/prune messages every 60 seconds to inform other PIM-SM routers about clients who want to join or leave a multicast group.

  Use the same join/prune message interval on all PIM-SM routers in the same PIM-SM domain, otherwise the routing protocol’s performance will be adversely affected.

  The multicast interface that first receives a multicast stream from a particular source forwards this traffic only to those interfaces on the router that have requests to join this group. When there are no longer any requesting groups on that interface, the leaf node sends a prune message upstream and enters a prune state for this multicast stream. The protocol maintains both the current join state and the pending RPT prune state for this (source, group) pair until the join/prune interval timer expires.

WEB INTERFACE

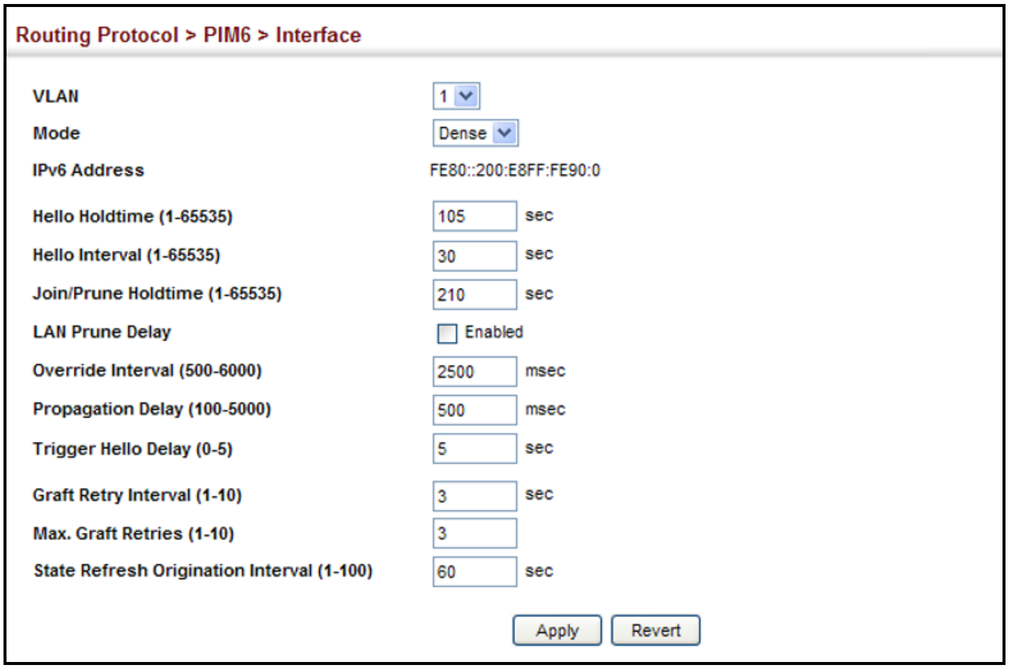
To configure PIMv6 interface settings:

1. Click Routing Protocol, PIM6, Interface.

2. Modify any of the protocol parameters as required.

3. Click Apply.

Figure 537: Configuring PIMv6 Interface Settings (Dense Mode)



Routing Protocol > PIM6 > Interface

VLAN 1

Mode Dense

IPv6 Address FE80::200:E8FF:FE90:0

Hello Holdtime (1-65535) 105 sec

Hello Interval (1-65535) 30 sec

Join/Prune Holdtime (1-65535) 210 sec

LAN Prune Delay □ Enabled

Override Interval (500-6000) 2500 msec

Propagation Delay (100-5000) 500 msec

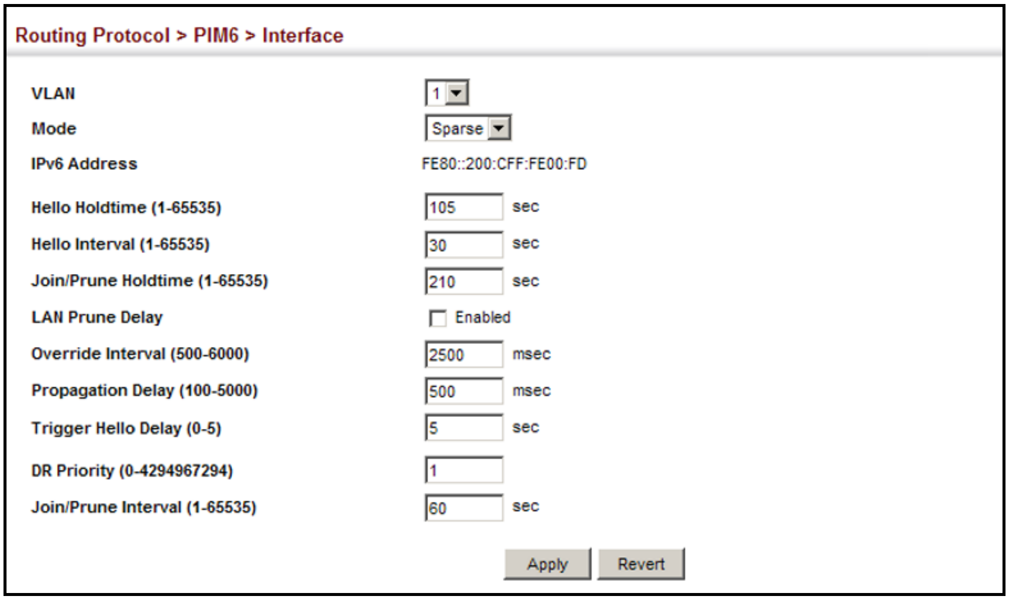
Trigger Hello Delay (0-5) 5 sec

Graft Retry Interval (1-10) 3 sec

Max. Graft Retries (1-10) 3

State Refresh Origination Interval (1-100) 60 sec

Figure 538: Configuring PIMv6 Interface Settings (Sparse Mode)



Routing Protocol > PIM6 > Interface

VLAN 1

Mode Sparse

IPv6 Address FE80::200:CFF:FE00:FD

Hello Holdtime (1-65535) 105 sec

Hello Interval (1-65535) 30 sec

Join/Prune Holdtime (1-65535) 210 sec

LAN Prune Delay □ Enabled

Override Interval (500-6000) 2500 msec

Propagation Delay (100-5000) 500 msec

Trigger Hello Delay (0-5) 5 sec

DR Priority (0-4294967294) 1

Join/Prune Interval (1-65535) 60 sec

DISPLAYING PIM6 NEIGHBOR INFORMATION

Use the Routing Protocol > PIM6 > Neighbor page to display all neighboring PIMv6 routers.

CLI REFERENCES

- "show ipv6 pim neighbor" on page 1958

PARAMETERS

These parameters are displayed:

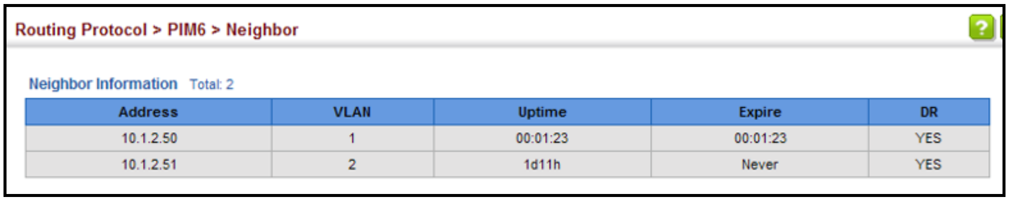
- **Address** – IP address of the next-hop router.
- **VLAN** – VLAN that is attached to this neighbor.
- **Uptime** – The duration this entry has been active.
- **Expire** – The time before this entry will be removed.
- **DR** – The designated PIM6-SM router. If multicast hosts are directly connected to the LAN, then only one of these routers is elected as the DR, and acts on behalf of these hosts, sending periodic Join/Prune messages toward a group-specific RP for each group.

WEB INTERFACE

To display neighboring PIMv6 routers:

1. Click Routing Protocol, PIM6, Neighbor.

Figure 539: Showing PIMv6 Neighbors



Routing Protocol > PIM6 > Neighbor

Neighbor Information Total: 2

Address	VLAN	Uptime	Expire	DR
10.1.2.50	1	00:01:23	00:01:23	YES
10.1.2.51	2	1d11h	Never	YES

CONFIGURING GLOBAL PIM6-SM SETTINGS

Use the Routing Protocol > PIM6 > SM (Configure Global) page to configure the rate at which register messages are sent, the source of register messages, and switchover to the Shortest Path Tree (SPT).

CLI REFERENCES

- "IPv6 PIM Commands" on page 1950

PARAMETERS

These parameters are displayed:

- **Register Rate Limit** – Configures the rate at which register messages are sent by the Designated Router (DR) for each (source, group) entry. (Range: 1-65535 packets per second: Default: disabled)

  This parameter can be used to relieve the load on the designated router (DR) and rendezvous point (RP). However, because register messages exceeding the limit are dropped, some receivers may experience data packet loss within the first few seconds in which register messages are sent from bursty sources.

- **Register Source** – Configures the IP source address of a register message to an address other than the outgoing interface address of the DR that leads back toward the RP. (Range: VLAN 1-4094; Default: The IP address of the DR's outgoing interface that leads back to the RP)

  When the source address of a register message is filtered by intermediate network devices, or is not a uniquely routed address to which the RP can send packets, the replies sent from the RP to the source address will fail to reach the DR, resulting in PIM6-SM protocol failures. This type of problem can be overcome by manually configuring the source address of register messages to an interface that leads back to the RP.

- **SPT Threshold** – Prevents the last-hop PIM-SM router from switching to Shortest Path Source Tree (SPT) mode. (Options: Infinity, Reset; Default: Reset)

  The default path for packets from a multicast source to a receiver is through the RP. However, the path through the RP is not always the shortest path. Therefore, the router uses the RP to forward only the first packet from a new multicast group to its receivers. Afterwards, it calculates the shortest path tree (SPT) directly between the receiver and source, and then uses the SPT to send all subsequent packets from the source to the receiver instead of using the shared tree. Note that when the SPT threshold is not set by this command, the PIM leaf router will join the shortest path tree immediately after receiving the first packet from a new source.

  Enable the SPT threshold to force the router to use the shared tree for all multicast groups, or just for the specified multicast groups.

- **Group Address** – An IPv6 multicast group address. If a group address is not specified, the shared tree is used for all multicast groups.

- **Group Prefix Length** – An IPv6 network prefix length for a multicast group. (Range: 8-128)

WEB INTERFACE

To configure global settings for PIM6-SM:

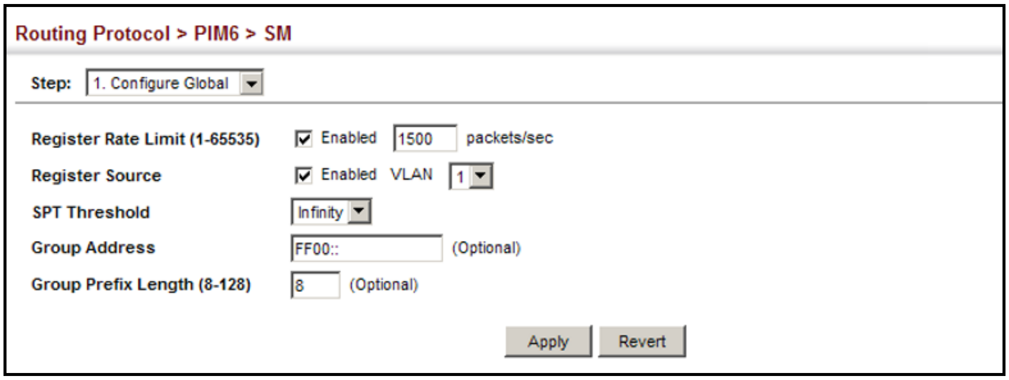
1. Click Routing Protocol, PIM6, PIM6-SM.

2. Select Configure Global from the Step list.

3. Set the register rate limit and source of register messages if required. Also specify any multicast groups which must be routed across the shared tree, instead of switching over to the SPT.

4. Click Apply.

Figure 540: Configuring Global Settings for PIM6-SM



Routing Protocol > PIM6 > SM

Step: 1. Configure Global

Register Rate Limit (1-65535) ☑ Enabled 1500 packets/sec

Register Source ☑ Enabled VLAN 1

SPT Threshold Infinity

Group Address FF00:: (Optional)

Group Prefix Length (8-128) 8 (Optional)

CONFIGURING A PIM6 BSR CANDIDATE

Use the Routing Protocol > PIM6 > SM (BSR Candidate) page to configure the switch as a Bootstrap Router (BSR) candidate.

CLI REFERENCES

- "ipv6 pim bsr-candidate" on page 1961

COMMAND USAGE

- When this router is configured as a BSR candidate, it starts sending bootstrap messages to all of its PIM6-SM neighbors. The primary IP address of the designated VLAN is sent as the candidate's BSR address. Each neighbor receiving the bootstrap message compares the BSR address with the address from previous messages. If the current address is the same or a higher address, it accepts the bootstrap message and forwards it. Otherwise, it drops the message.

- This router will continue to be the BSR until it receives a bootstrap message from another candidate with a higher priority (or a higher IP address if the priorities are the same).

- To improve failover recovery, it is advisable to select at least two core routers in diverse locations, each to serve as both a candidate BSR and candidate RP. It is also preferable to set up one of these routers as both the primary BSR and RP.

PARAMETERS

These parameters are displayed:

- **BSR Candidate Status** – Configures the switch as a Bootstrap Router (BSR) candidate. (Default: Disabled)

- **VLAN ID** – Identifier of configured VLAN interface. (Range: 1-4094)

- **Hash Mask Length** – Hash mask length (in bits) used for RP selection (see "Configuring a PIM6 Static Rendezvous Point" on page 859 and "Configuring a PIM6 RP Candidate" on page 861). The portion of the hash specified by the mask length is ANDed with the group address. Therefore, when the hash function is executed on any BSR, all groups with the same seed hash will be mapped to the same RP. If the mask length is less than 32, then only the first portion of the hash is used, and a single RP will be defined for multiple groups. (Range: 0-32; Default: 10)

- **Priority** – Priority used by the candidate bootstrap router in the election process. The BSR candidate with the largest priority is preferred. If the priority values are the same, the candidate with the larger IP address is elected to be the BSR. Setting the priority to zero means that this router is not eligible to server as the BSR. At least one router in the PIM6-SM domain must be set to a value greater than zero. (Range: 0-255; Default: 0)

WEB INTERFACE

To configure the switch as a BSR candidate:

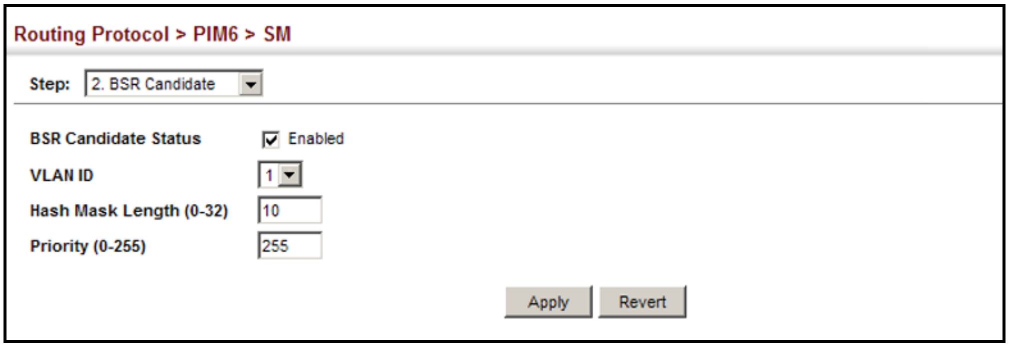
1. Click Routing Protocol, PIM6, PIM6-SM.

2. Select BSR Candidate from the Step list.

3. Specify the VLAN interface for which this router is bidding to become the BSR, the hash mask length that will subsequently be used for RP selection if this router is selected as the BSR, and the priority for BSR selection.

4. Click Apply.

Figure 541: Configuring a PIM6-SM BSR Candidate



Routing Protocol > PIM6 > SM

Step: 2. BSR Candidate

BSR Candidate Status ☑ Enabled
VLAN ID 1
Hash Mask Length (0-32) 10
Priority (0-255) 255

CONFIGURING A PIM6 STATIC RENDEZVOUS POINT

Use the Routing Protocol > PIM6 > SM (RP Address) page to configure a static address as the Rendezvous Point (RP) for a particular multicast group.

CLI REFERENCES

- "ipv6 pim rp-address" on page 1964

COMMAND USAGE

- The router will act as an RP for all multicast groups in the local PIM6-SM domain if no groups are specified. A static RP can either be configured for the whole multicast group range FF00::/8, or for specific group ranges.

- If an IP address is specified that was previously used for an RP, then the older entry is replaced.

- Multiple RPs can be defined for different groups or group ranges. If a group is matched by more than one entry, the router will use the RP associated with the longer group prefix length. If the prefix lengths are the same, then the static RP with the highest IP address is chosen.

- Static definitions for RP addresses may be used together with RP addresses dynamically learned through the bootstrap router (BSR). If an RP address learned by the BSR and one statically configured using this command are both available for a group range, the RP address learned by the BSR is chosen over the one statically configured.

- All routers within the same PIM6-SM domain must be configured with the same RP(s). Selecting an RP through the dynamic election process is therefore preferable for most situations. Using the dynamic RP election process also allows a backup RP to automatically take over if the active RP router becomes unavailable.

PARAMETERS

These parameters are displayed:

- **RP Address** – Static IP address of the router that will be an RP for the specified multicast group(s).

- **Group Address** – An IP multicast group address. If a group address is not specified, the RP is used for all multicast groups.

- **Group Prefix Length** – An IPv6 network prefix length for a multicast group. (Range: 8-128)

WEB INTERFACE

To configure a static rendezvous point:

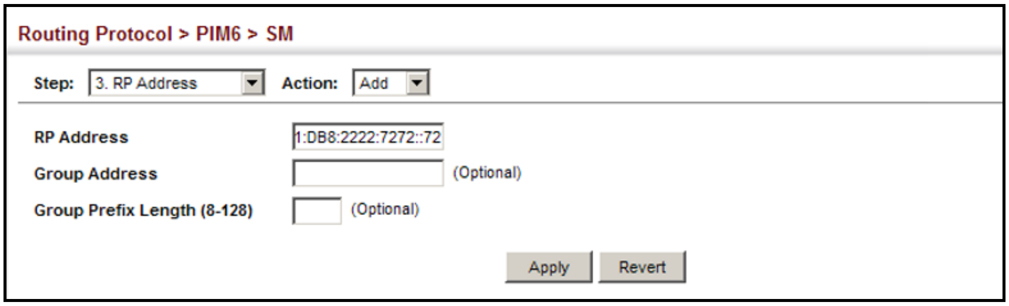
1. Click Routing Protocol, PIM6, PIM6-SM.

2. Select RP Address from the Step list.

3. Specify the static RP to use for a multicast group, or a range of groups by using a subnet mask.

4. Click Apply.

Figure 542: Configuring a PIM6 Static Rendezvous Point



Routing Protocol > PIM6 > SM

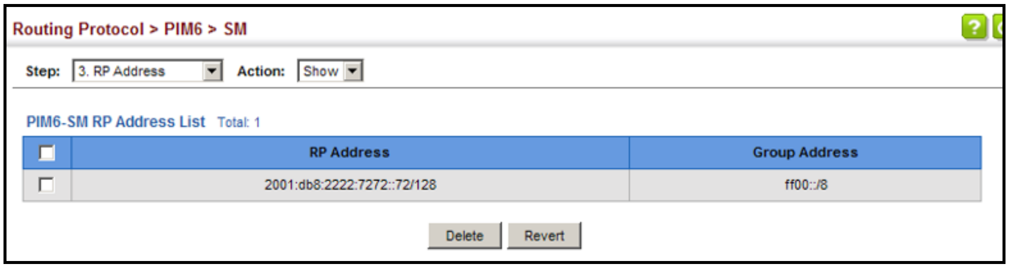
Step: 3. RP Address Action: Add

RP Address: 1:DB8:2222:7272::72
Group Address: (Optional)
Group Prefix Length (8-128): (Optional)

To display static rendezvous points:

1. Click Routing Protocol, PIM6, PIM6-SM.
2. Select RP Address from the Step list.
3. Select Show from the Action list.

Figure 543: Showing PIM6 Static Rendezvous Points



Routing Protocol > PIM6 > SM

Step: 3. RP Address Action: Show

PIM6-SM RP Address List Total: 1

□	RP Address	Group Address
□	2001:db8:2222:7272::72/128	ff00::/8

CONFIGURING A PIM6 RP CANDIDATE

Use the Routing Protocol > PIM6 > SM (RP Candidate) page to configure the switch to advertise itself as a Rendezvous Point (RP) candidate to the bootstrap router (BSR).

CLI REFERENCES

- "ipv6 pim rp-candidate" on page 1965

COMMAND USAGE

- When this router is configured as an RP candidate, it periodically sends PIMv2 messages to the BSR advertising itself as a candidate RP for the specified group addresses. The IP address of the designated VLAN is sent as the candidate’s RP address. The BSR places information about all of the candidate RPs in subsequent bootstrap messages. The BSR uses the RP-election hash algorithm to select an active RP for each group range. The election process is performed by the BSR only for its own use. Each PIM6-SM router that receives the list of RP candidates from the BSR also elects an active RP for each group range using the same election process.

- The election process for each group is based on the following criteria:

  - Find all RPs with the most specific group range.

  - Select those with the highest priority (lowest priority value).
  - Compute hash value based on the group address, RP address, priority, and hash mask included in the bootstrap messages.
  - If there is a tie, use the candidate RP with the highest IP address.

- This distributed election process provides faster convergence and minimal disruption when an RP fails. It also serves to provide load balancing by distributing groups across multiple RPs. Moreover, when an RP fails, the responsible RPs are re-elected on each router, and the groups automatically distributed to the remaining RPs.

- To improve failover recovery, it is advisable to select at least two core routers in diverse locations, each to serve as both a candidate BSR and candidate RP. It is also preferable to set up one of these routers as both the primary BSR and RP.

PARAMETERS

These parameters are displayed:

- **VLAN** – Identifier of configured VLAN interface. (Range: 1-4094)

- **Interval** – The interval at which this device advertises itself as an RP candidate. (Range: 60-16383 seconds; Default: 60 seconds)

- **Priority** – Priority used by the candidate RP in the election process. The RP candidate with the largest priority is preferred. If the priority values are the same, the candidate with the larger IP address is elected to be the RP. Setting the priority to zero means that this router is not eligible to server as the RP. (Range: 0-255; Default: 0)

- **Group Address** – An IP multicast group address. If not defined, the RP is advertised for all multicast groups.

- **Group Prefix Length** – An IPv6 network prefix length for a multicast group. (Range: 8-128)

WEB INTERFACE

To advertise the switch as an RP candidate:

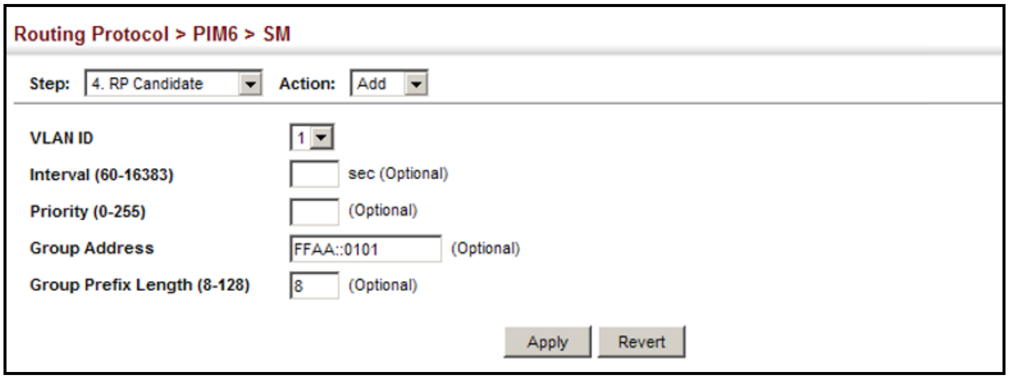
1. Click Routing Protocol, PIM6, PIM6-SM.

2. Select RP Candidate from the Step list.

3. Specify a VLAN interface, the interval at which to advertise the router as an RP candidate, the priority to use in the election process, and the multicast group address and mask indicating the groups for which this router is bidding to become the RP.

4. Click Apply.

Figure 544: Configuring a PIM6 RP Candidate



Routing Protocol > PIM6 > SM

Step: 4. RP Candidate Action: Add

VLAN ID: 1

Interval (60-16383): sec (Optional)

Priority (0-255): (Optional)

Group Address: FFAA::0101 (Optional)

Group Prefix Length (8-128): 8 (Optional)

To display settings for an RP candidate:

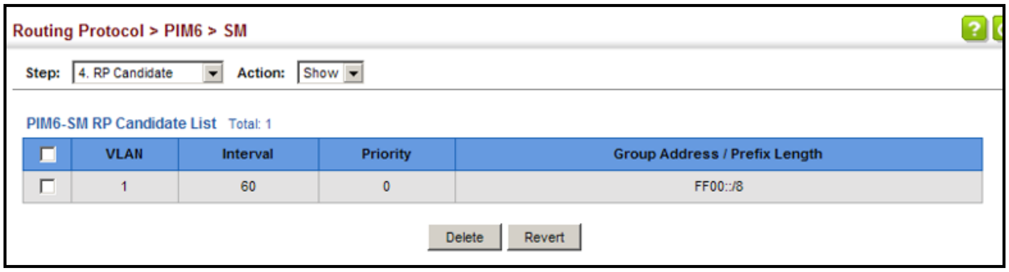
1. Click Routing Protocol, PIM6, PIM6-SM.

2. Select RP Candidate from the Step list.

3. Select Show from the Action list.

4. Select an interface from the VLAN list.

Figure 545: Showing Settings for a PIM6 RP Candidate



Routing Protocol > PIM6 > SM

Step: 4. RP Candidate Action: Show

PIM6-SM RP Candidate List Total: 1

□	VLAN	Interval	Priority	Group Address / Prefix Length
□	1	60	0	FF00::/8

DISPLAYING THE PIM6 BSR ROUTER

Use the Routing Protocol > PIM6 > SM (Show Information – Show BSR Router) page to display Information about the bootstrap router (BSR).

CLI REFERENCES

- "show ipv6 pim bsr-router" on page 1970

PARAMETERS

These parameters are displayed:

- **IP Address** – IP address of interface configured as the BSR.

- **Uptime** – The time this BSR has been up and running.

- **Priority** – Priority value used by this BSR candidate.

- **Hash Mask Length** – The number of significant bits used in the multicast group comparison mask by this BSR candidate.

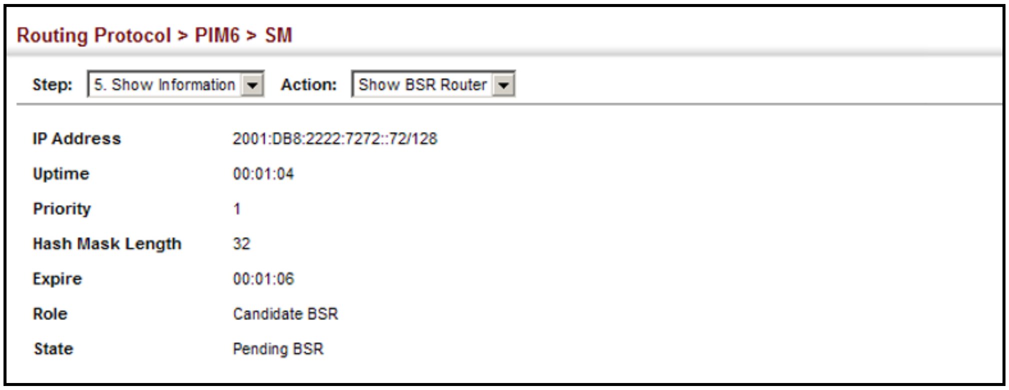
- **Expire** – The time before the BSR is declared down.
- **Role** – Candidate or non-candidate BSR.
- **State**[16] – Operation state of BSR includes:
  - No information – No information is stored for this device.
  - Accept Any – The router does not know of an active BSR, and will accept the first bootstrap message it sees as giving the new BSR's identity and the RP-set.
  - Accept Preferred – The router knows the identity of the current BSR, and is using the RP-set provided by that BSR. Only bootstrap messages from that BSR or from a C-BSR with higher weight than the current BSR will be accepted.
  - Candidate BSR – Bidding in election process.
  - Pending-BSR – The router is a candidate to be the BSR for the RP-set. Currently, no other router is the preferred BSR, but this router is not yet the elected BSR.
  - Elected BSR – Elected to serve as BSR.

WEB INTERFACE

To display information about the BSR:

1. Click Routing Protocol, PIM6, PIM6-SM.
2. Select Show Information from the Step list.
3. Select Show BSR Router from the Action list.

Figure 546: Showing Information About the PIM6 BSR



Step: 5. Show Information Action: Show BSR Router

IP Address	2001:DB8:2222:7272::72/128
Uptime	00:01:04
Priority	1
Hash Mask Length	32
Expire	00:01:06
Role	Candidate BSR
State	Pending BSR

[16] These parameters are based on RFC 5059.

DISPLAYING RP MAPPING

Use the Routing Protocol > PIM6 > SM (Show Information – Show RP Mapping) page to display active RPs and associated multicast routing entries.

CLI REFERENCES

- "show ipv6 pim rp mapping" on page 1971

PARAMETERS

These parameters are displayed:

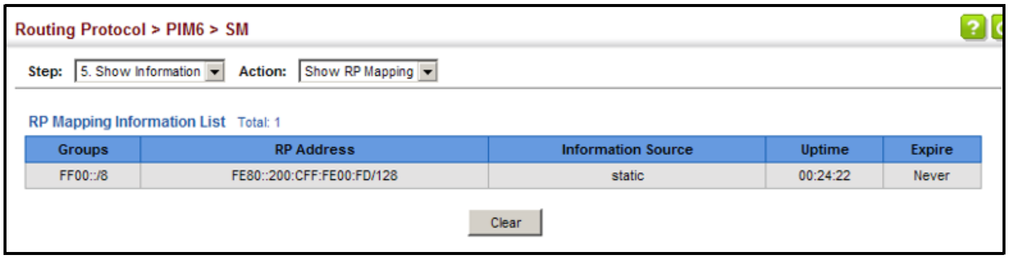
- **Groups** – A multicast group address.
- **RP Address** – IP address of the RP for the listed multicast group.
- **Information Source** – RP that advertised the mapping, how the RP was selected (Static or Bootstrap), and the priority used in the bidding process.
- **Uptime** – The time this RP has been up and running
- **Expire** – The time before this entry will be removed.

WEB INTERFACE

To display the RPs mapped to multicast groups:

1. Click Routing Protocol, PIM6, PIM6-SM.
2. Select Show Information from the Step list.
3. Select Show RP Mapping from the Action list.

Figure 547: Showing PIM6 RP Mapping



Routing Protocol > PIM6 > SM

Step: 5. Show Information Action: Show RP Mapping

RP Mapping Information List Total: 1

Groups	RP Address	Information Source	Uptime	Expire
FF00::/8	FE80::200:CFF:FE00:FD/128	static	00:24:22	Never

SECTION III

COMMAND LINE INTERFACE

This section provides a detailed description of the Command Line Interface, along with examples for all of the commands.

This section includes these chapters:

- "Using the Command Line Interface" on page 869
- "General Commands" on page 883
- "System Management Commands" on page 891
- "SNMP Commands" on page 995
- "Remote Monitoring Commands" on page 1017
- "Flow Sampling Commands" on page 1025
- "Authentication Commands" on page 1031
- "General Security Measures" on page 1089
- "Access Control Lists" on page 1163
- "Interface Commands" on page 1187
- "Link Aggregation Commands" on page 1215
- "Port Mirroring Commands" on page 1229
- "Congestion Control Commands" on page 1239
- "Loopback Detection Commands" on page 1259
- "UniDirectional Link Detection Commands" on page 1265
- "Address Table Commands" on page 1271
- "Spanning Tree Commands" on page 1277
- "ERPS Commands" on page 1305

- "VLAN Commands" on page 1337
- "Class of Service Commands" on page 1387
- "Quality of Service Commands" on page 1407
- "Multicast Filtering Commands" on page 1425
- "LLDP Commands" on page 1537
- "CFM Commands" on page 1561
- "OAM Commands" on page 1603
- "Domain Name Service Commands" on page 1615
- "DHCP Commands" on page 1625
- "IP Interface Commands" on page 1647
- "VRRP Commands" on page 1713
- "IP Routing Commands" on page 1723
- "Multicast Routing Commands" on page 1919

22 USING THE COMMAND LINE INTERFACE

This chapter describes how to use the Command Line Interface (CLI).

ACCESSING THE CLI

When accessing the management interface for the switch over a direct connection to the server's console port, or via a Telnet or Secure Shell connection (SSH), the switch can be managed by entering command keywords and parameters at the prompt. Using the switch's command-line interface (CLI) is very similar to entering commands on a UNIX system.

CONSOLE CONNECTION

To access the switch through the console port, perform these steps:

1. At the console prompt, enter the user name and password. (The default user names are "admin" and "guest" with corresponding passwords of "admin" and "guest.") When the administrator user name and password is entered, the CLI displays the "Console#" prompt and enters privileged access mode (i.e., Privileged Exec). But when the guest user name and password is entered, the CLI displays the "Console>" prompt and enters normal access mode (i.e., Normal Exec).

2. Enter the necessary commands to complete your desired tasks.

3. When finished, exit the session with the "quit" or "exit" command.

After connecting to the system through the console port, the login screen displays:

```
User Access Verification
Username: admin
Password:
  CLI session with the ECS4660-28F is opened.
  To end the CLI session, enter [Exit].
Console#
```

TELNET CONNECTION

Telnet operates over the IP transport protocol. In this environment, your management station and any network device you want to manage over the network must have a valid IP address. Valid IP addresses consist of four numbers, 0 to 255, separated by periods. Each address consists of a network portion and host portion. For example, the IP address assigned to this switch, 10.1.0.1, consists of a network portion (10.1.0) and a host portion (1).

NOTE: The IP address for this switch is obtained via DHCP by default.

To access the switch through a Telnet session, you must first set the IP address for the Master unit, and set the default gateway if you are managing the switch from a different IP subnet. For example,

```
Console(config)#interface vlan 1
Console(config-if)#ip address 10.1.0.254 255.255.255.0
Console(config-if)#exit
Console(config)#ip default-gateway 10.1.0.254
Console(config)#
```

If your corporate network is connected to another network outside your office or to the Internet, you need to apply for a registered IP address. However, if you are attached to an isolated network, then you can use any IP address that matches the network segment to which you are attached.

After you configure the switch with an IP address, you can open a Telnet session by performing these steps:

1. From the remote host, enter the Telnet command and the IP address of the device you want to access.

2. At the prompt, enter the user name and system password. The CLI will display the "Vty-*n*#" prompt for the administrator to show that you are using privileged access mode (i.e., Privileged Exec), or "Vty-*n*>" for the guest to show that you are using normal access mode (i.e., Normal Exec), where *n* indicates the number of the current Telnet session.

3. Enter the necessary commands to complete your desired tasks.

4. When finished, exit the session with the "quit" or "exit" command.

After entering the Telnet command, the login screen displays:

```
Username: admin
Password:

  CLI session with the ECS4660-28F is opened.
  To end the CLI session, enter [Exit].

Vty-0#
```

NOTE: You can open up to eight sessions to the device via Telnet or SSH.

ENTERING COMMANDS

This section describes how to enter CLI commands.

KEYWORDS AND ARGUMENTS

A CLI command is a series of keywords and arguments. Keywords identify a command, and arguments specify configuration parameters. For example, in the command "show interfaces status ethernet 1/5," **show interfaces** and **status** are keywords, **ethernet** is an argument that specifies the interface type, and **1/5** specifies the unit/port.

You can enter commands as follows:

- To enter a simple command, enter the command keyword.
- To enter multiple commands, enter each command in the required order. For example, to enable Privileged Exec command mode, and display the startup configuration, enter:

```
Console>enable
Console#show startup-config
```

- To enter commands that require parameters, enter the required parameters after the command keyword. For example, to set a password for the administrator, enter:

```
Console(config)#username admin password 0 smith
```

MINIMUM ABBREVIATION

The CLI will accept a minimum number of characters that uniquely identify a command. For example, the command "configure" can be entered as **con**. If an entry is ambiguous, the system will prompt for further input.

COMMAND COMPLETION

If you terminate input with a Tab key, the CLI will print the remaining characters of a partial keyword up to the point of ambiguity. In the "logging history" example, typing **log** followed by a tab will result in printing the command up to "**logging**."

GETTING HELP ON COMMANDS

You can display a brief description of the help system by entering the **help** command. You can also display command syntax by using the “?” character to list keywords or parameters.

SHOWING COMMANDS

If you enter a “?” at the command prompt, the system will display the first level of keywords or command groups. You can also display a list of valid keywords for a specific command. For example, the command “**show ?**” displays a list of possible show commands:

```
Console#show ?
  access-group          Access groups
  access-list           Access lists
  accounting            Uses an accounting list with this name
  alarm                 Alarm
  alarm-status          Show alarm status
  arp                   Information of ARP cache
  authorization         Enables EXEC accounting
  auto-traffic-control  Auto traffic control information
  banner                Banner info
  bridge-ext            Bridge extension information
  calendar              Date and time information
  class-map             Displays class maps
  cluster               Display cluster
  debug                 State of each debugging option
  discard               Discard packet
  dns                   DNS information
  dos-protection        Shows the system dos-protection summary information
  dot1q-tunnel          dot1q-tunnel
  dot1x                 802.1X content
  efm                   Ethernet First Mile feature
  erps                  Displays ERPS configuration
  ethernet              Specifies the ethernet
  garp                  GARP properties
  gvrp                  GVRP interface information
  history               Shows history information
  hosts                 Host information
  interfaces            Shows interface information
  ip                    IP information
  ipv6                  IPv6 information
  l2protocol-tunnel     Layer 2 protocol tunneling configuration
  lacp                  LACP statistics
  line                  TTY line information
  lldp                  LLDP
  log                   Log records
  logging               Logging setting
  loop                  Shows the information of loopback
  loopback-detection    Shows loopback detection information
  mac                   MAC access list
  mac-address-table     Configuration of the address table
  mac-vlan              MAC-based VLAN information
  management            Shows management information
  memory                Memory utilization
  mvr                   Multicast vlan registration
  mvr6                  IPv6 Multicast VLAN registration
  network-access        Shows the entries of the secure port.
  nlm                   Show notification log
  ntp                   Network Time Protocol configuration
  policy-map            Displays policy maps
  port                  Port characteristics
  port-channel          Port channel information
  pppoe                 Displays PPPoE configuration
  process               Device process
  protocol-vlan         Protocol-VLAN information
  ptp                   Displays PTP information
  public-key            Public key information
  qos                   Quality of Service
  queue                 Priority queue information
  radius-server         RADIUS server information
  reload                Shows the reload settings
  rmon                  Remote Monitoring Protocol
  route-map             Shows route-map
  rspan                 Display status of the current RSPAN configuration
  running-config        Information on the running configuration
  sflow                 Shows the sflow information
  snmp                  Simple Network Management Protocol configuration and
                          statistics
  snmp-server           Displays SNMP server configuration
  sntp                  Simple Network Time Protocol configuration
  spanning-tree         Spanning-tree configuration
  ssh                   Secure shell server connections
  startup-config        Startup system configuration
  subnet-vlan           IP subnet-based VLAN information
  synce                 Shows synchronous ethernet status
  system                System information
  tacacs-server         TACACS server information
  tech-support          Technical information
  time-range            Time range
  traffic-segmentation  Traffic segmentation information
  udld                  Displays UDLD information
  upgrade               Shows upgrade information
  users                 Information about users logged in
  version               System hardware and software versions
  vlan                  Shows virtual LAN settings
  vlan-translation      VLAN translation information
  voice                 Shows the voice VLAN information
  vrrp                  Shows VRRP
  watchdog              Displays watchdog status
  web-auth              Shows web authentication configuration
Console#show
```

The command "**show interfaces ?**" will display the following information:

```
Console#show interfaces ?
  brief                  Brief interface description
  counters               Interface counters information
  history                Historical sample of interface counters information
  protocol-vlan          Protocol-VLAN information
  status                 Shows interface status
  switchport             Shows interface switchport information
  transceiver            Interface of transceiver information
  transceiver-threshold  Interface of transceiver-threshold information
Console#
```

Show commands which display more than one page of information (e.g., **show running-config**) pause and require you to press the [Space] bar to continue displaying one more page, the [Enter] key to display one more line, or the [a] key to display the rest of the information without stopping. You can press any other key to terminate the display.

PARTIAL KEYWORD LOOKUP

If you terminate a partial keyword with a question mark, alternatives that match the initial letters are provided. (Remember not to leave a space between the command and question mark.) For example "**s?**" shows all the keywords starting with "s."

```
Console#show s?
sflow          snmp           snmp-server    sntp           spanning-tree
ssh            startup-config subnet-vlan    synce          system
Console#show s
```

NEGATING THE EFFECT OF COMMANDS

For many configuration commands you can enter the prefix keyword "**no**" to cancel the effect of a command or reset the configuration to the default value. For example, the **logging** command will log system messages to a host server. To disable logging, specify the **no logging** command. This guide describes the negation effect for all applicable commands.

USING COMMAND HISTORY

The CLI maintains a history of commands that have been entered. You can scroll back through the history of commands by pressing the up arrow key. Any command displayed in the history list can be executed again, or first modified and then executed.

Using the **show history** command displays a longer list of recently executed commands.

UNDERSTANDING COMMAND MODES

The command set is divided into Exec and Configuration classes. Exec commands generally display information on system status or clear statistical counters. Configuration commands, on the other hand, modify interface parameters or enable certain switching functions. These classes are further divided into different modes. Available commands depend on the selected mode. You can always enter a question mark "**?**" at the prompt to display a list of the commands available for the current mode. The command classes and associated modes are displayed in the following table:

Table 54: General Command Modes

Class	Mode	
Exec	Normal Privileged	
Configuration	Global*	Access Control List CFM Class Map DHCP ERPS IGMP Profile Interface Line Multiple Spanning Tree Policy Map Route Map Router Time Range VLAN Database

* You must be in Privileged Exec mode to access the Global configuration mode. You must be in Global Configuration mode to access any of the other configuration modes.

EXEC COMMANDS

When you open a new console session on the switch with the user name and password "guest," the system enters the Normal Exec command mode (or guest mode), displaying the "Console>" command prompt. Only a limited number of the commands are available in this mode. You can access all commands only from the Privileged Exec command mode (or administrator mode). To access Privilege Exec mode, open a new console session with the user name and password "admin." The system will now display the "Console#" command prompt. You can also enter Privileged Exec mode from within Normal Exec mode, by entering the enable command, followed by the privileged level password "super."

To enter Privileged Exec mode, enter the following user names and passwords:

```
Username: admin
Password: [admin login password]

  CLI session with the ECS4660-28F is opened.
  To end the CLI session, enter [Exit].

Console#
```

```
Username: guest
Password: [guest login password]

  CLI session with the ECS4660-28F is opened.
  To end the CLI session, enter [Exit].

Console>enable
Password: [privileged level password]
Console#
```

CONFIGURATION COMMANDS

Configuration commands are privileged level commands used to modify switch settings. These commands modify the running configuration only and are not saved when the switch is rebooted. To store the running configuration in non-volatile storage, use the **copy running-config startup-config** command.

The configuration commands are organized into different modes:

- Global Configuration - These commands modify the system level configuration, and include commands such as **hostname** and **snmp-server community**.
- Access Control List Configuration - These commands are used for packet filtering.
- CFM Configuration - Configures connectivity monitoring using continuity check messages, fault verification through loopback messages, and fault isolation by examining end-to-end connections between Provider Edge devices or between Customer Edge devices.
- Class Map Configuration - Creates a DiffServ class map for a specified traffic type.
- DHCP Configuration - These commands are used to configure the DHCP server.
- ERPS Configuration – These commands configure Ethernet Ring Protection Switching for increased availability of Ethernet rings commonly used in service provider networks.
- IGMP Profile - Sets a profile group and enters IGMP filter profile configuration mode.
- Interface Configuration - These commands modify the port configuration such as **speed-duplex** and **negotiation**.
- Line Configuration - These commands modify the console port and Telnet configuration, and include command such as **parity** and **databits**.
- Multiple Spanning Tree Configuration - These commands configure settings for the selected multiple spanning tree instance.
- Policy Map Configuration - Creates a DiffServ policy map for multiple interfaces.
- Route Map Configuration - These commands specify the action (next hop or silently drop) to take when a match is found.
- Router Configuration - These commands configure global settings for unicast and multicast routing protocols.
- Time Range - Sets a time range for use by other functions, such as Access Control Lists.

- VLAN Configuration - Includes the command to create VLAN groups.

To enter the Global Configuration mode, enter the command **configure** in Privileged Exec mode. The system prompt will change to “Console(config)#” which gives you access privilege to all Global Configuration commands.

```
Console#configure
Console(config)#
```

To enter the other modes, at the configuration prompt type one of the following commands. Use the **exit** or **end** command to return to the Privileged Exec mode.

Table 55: Configuration Command Modes

Mode	Command	Prompt	Page
Access Control List	access-list arp	Console(config-arp-acl)	1181
	access-list ip standard	Console(config-std-acl)	1164
	access-list ip extended	Console(config-ext-acl)	1164
	access-list ipv6 standard	Console(config-std-ipv6-acl)	1170
	access-list ipv6 extended	Console(config-ext-ipv6-acl)	1170
	access-list mac	Console(config-mac-acl)	1176
CFM	ethernet cfm domain	Console(config-ether-cfm)	1567
Class Map	class-map	Console(config-cmap)	1408
DHCP	ip dhcp pool	Console(config-dhcp)	1634
ERPS	erps domain	Console(config-erps)	1307
Interface	interface {ethernet *port* | port-channel *id*| vlan *id*}	Console(config-if)	1188
Line	line {console | vty}	Console(config-line)	924
MSTP	spanning-tree mst-configuration	Console(config-mstp)	1283
Policy Map	policy-map	Console(config-pmap)	1411
Time Range	time-range	Console(config-time-range)	957
Route Map	route-map	Console(config-route-map)	1899
Router	router {bgp | ipv6 ospf | ospf | pim | pim6 | rip}	Console(config-router)	1832 1792 1751 1928 1951 1734
Time Range	time-range	Console(config-time-range)	957
VLAN	vlan database	Console(config-vlan)	1343

For example, you can use the following commands to enter interface configuration mode, and then return to Privileged Exec mode

```
Console(config)#interface ethernet 1/5
.
.
.
Console(config-if)#exit
Console(config)#
```

COMMAND LINE PROCESSING

Commands are not case sensitive. You can abbreviate commands and parameters as long as they contain enough letters to differentiate them from any other currently available commands or parameters. You can use the Tab key to complete partial commands, or enter a partial command followed by the “?” character to display a list of possible matches. You can also use the following editing keystrokes for command-line processing:

Table 56: Keystroke Commands

Keystroke	Function
Ctrl-A	Shifts cursor to start of command line.
Ctrl-B	Shifts cursor to the left one character.
Ctrl-C	Terminates the current task and displays the command prompt.
Ctrl-E	Shifts cursor to end of command line.
Ctrl-F	Shifts cursor to the right one character.
Ctrl-K	Deletes all characters from the cursor to the end of the line.
Ctrl-L	Repeats current command line on a new line.
Ctrl-N	Enters the next command line in the history buffer.
Ctrl-P	Enters the last command.
Ctrl-R	Repeats current command line on a new line.
Ctrl-U	Deletes from the cursor to the beginning of the line.
Ctrl-W	Deletes the last word typed.
Esc-B	Moves the cursor back one word.
Esc-D	Deletes from the cursor to the end of the word.
Esc-F	Moves the cursor forward one word.
Delete key or backspace key	Erases a mistake when entering a command.

CLI COMMAND GROUPS

The system commands can be broken down into the functional groups shown below.

Table 57: Command Group Index

Command Group	Description	Page
General	Basic commands for entering privileged access mode, restarting the system, or quitting the CLI	883
System Management	Display and setting of system information, basic modes of operation, maximum frame size, file management, console port and telnet settings, system logs, SMTP alerts, the system clock, and switch clustering	891
Simple Network Management Protocol	Activates authentication failure traps; configures community access strings, and trap receivers	995
Remote Monitoring	Supports statistics, history, alarm and event groups	1017
Flow Sampling	Samples traffic flows, and forwards data to designated collector	1025
User Authentication	Configures user names and passwords, logon access using local or remote authentication, management access through the web server, Telnet server and Secure Shell; as well as port security, IEEE 802.1X port access control, restricted access based on specified IP addresses, and PPPoE Intermediate Agent	1031
General Security Measures	Segregates traffic for clients attached to common data ports; and prevents unauthorized access by configuring valid static or dynamic addresses, web authentication, MAC address authentication, filtering DHCP requests and replies, and discarding invalid ARP responses	1089
Access Control List	Provides filtering for IPv4 frames (based on address, protocol, TCP/UDP port number or TCP control code), IPv6 frames (based on address, DSCP traffic class, next header type, or flow label), or non-IP frames (based on MAC address or Ethernet type)	1163
Interface	Configures the connection parameters for all Ethernet ports, aggregated links, and VLANs	1187
Link Aggregation	Statically groups multiple ports into a single logical trunk; configures Link Aggregation Control Protocol for port trunks	1215
Mirror Port	Mirrors data to another port for analysis without affecting the data passing through or the performance of the monitored port	1229
Congestion Control	Sets the input/output rate limits, traffic storm thresholds, and thresholds for broadcast and multicast storms which can be used to trigger configured rate limits or to shut down a port.	1239
Automatic Traffic Control	Configures bounding thresholds for broadcast and multicast storms which can be used to trigger configured rate limits or to shut down a port	1207
Loopback Detection	Detects general loopback conditions caused by hardware problems or faulty protocol settings	1259
UniDirectional Link Detection	Detect and disables unidirectional links	1265
Address Table	Configures the address table for filtering specified addresses, displays current entries, clears the table, or sets the aging time	1271

Table 57: Command Group Index (Continued)

Command Group	Description	Page
Spanning Tree	Configures Spanning Tree settings for the switch	1277
ERPS	Configures Ethernet Ring Protection Switching for increased availability of Ethernet rings commonly used in service provider networks	1305
VLANs	Configures VLAN settings, and defines port membership for VLAN groups; also enables or configures private VLANs, protocol VLANs, voice VLANs, and QinQ tunneling	1337
Class of Service	Sets port priority for untagged frames, selects strict priority or weighted round robin, relative weight for each priority queue, also sets priority for TCP/UDP traffic types, IP precedence, and DSCP	1387
Quality of Service	Configures Differentiated Services	1407
Multicast Filtering	Configures IGMP multicast filtering, query, profile, and proxy parameters; specifies ports attached to a multicast router; also configures multicast VLAN registration, and IPv6 MLD snooping	1425
Link Layer Discovery Protocol	Configures LLDP settings to enable information discovery about neighbor devices	1537
Connectivity Fault Management	Configures connectivity monitoring using continuity check messages, fault verification through loopback messages, and fault isolation by examining end-to-end connections between Provider Edge devices or between Customer Edge devices	1561
OAM	Configures Operations, Administration and Maintenance remote management tools required to monitor and maintain the links to subscriber CPEs	1603
Domain Name Service	Configures DNS services.	1615
Dynamic Host Configuration Protocol	Configures DHCP client, relay and server functions	1625
Router Redundancy	Configures router redundancy to create primary and backup routers	1713
IP Interface	Configures IP address for the switch interfaces; also configures ARP parameters	1647
IP Routing	Configures static unicast routing, policy-based unicast routing for BGP, and dynamic unicast routing	1723
Multicast Routing	Configures multicast routing protocols PIM-DM and PIM-SM	1919
Debug	Displays debugging information for all key functions These commands are not described in this manual. Please refer to the prompt messages included in the CLI interface.	

The access mode shown in the following tables is indicated by these abbreviations:

ACL (Access Control List Configuration)
CFM (Connectivity Fault Management Configuration)
CM (Class Map Configuration)
DC (DHCP Server Configuration)
ERPS (Ethernet Ring Protection Switching Configuration)
GC (Global Configuration)
IC (Interface Configuration)

IPC (IGMP Profile Configuration)
LC (Line Configuration)
MST (Multiple Spanning Tree)
NE (Normal Exec)
PE (Privileged Exec)
PM (Policy Map Configuration)
RC (Router Configuration)
RM (Route Map Configuration)
VC (VLAN Database Configuration)

23 General Commands

The general commands are used to control the command access mode, configuration mode, and other basic functions.

Table 58: General Commands

Command	Function	Mode
prompt	Customizes the CLI prompt	GC
reload	Restarts the system at a specified time, after a specified delay, or at a periodic interval	GC
enable	Activates privileged mode	NE
quit	Exits a CLI session	NE, PE
show history	Shows the command history buffer	NE, PE
configure	Activates global configuration mode	PE
disable	Returns to normal mode from privileged mode	PE
reload	Restarts the system immediately	PE
show reload	Displays the current reload settings, and the time at which next scheduled reload will take place	PE
end	Returns to Privileged Exec mode	any config. mode
exit	Returns to the previous configuration mode, or exits the CLI	any mode
help	Shows how to use help	any mode
?	Shows options for command completion (context sensitive)	any mode

prompt

This command customizes the CLI prompt. Use the **no** form to restore the default prompt.

Syntax

prompt *string*

no prompt

string - Any alphanumeric string to use for the CLI prompt. (Maximum length: 255 characters)

Default Setting

Console

Command Mode

Global Configuration

EXAMPLE

```
Console(config)#prompt RD2
RD2(config)#
```

reload
(Global Configuration)

This command restarts the system at a specified time, after a specified delay, or at a periodic interval. You can reboot the system immediately, or you can configure the switch to reset after a specified amount of time. Use the **cancel** option to remove a configured setting.

SYNTAX

reload {**at** *hour minute* [{*month day* | *day month*} [*year*]] |
in {**hour** *hours* | **minute** *minutes* | **hour** *hours* **minute** *minutes*} |
regularity *hour minute* [**period** {**daily** | **weekly** *day-of-week* |
monthly *day*}] | **cancel** [**at** | **in** | **regularity**]}

reload at - A specified time at which to reload the switch.

hour - The hour at which to reload. (Range: 0-23)

minute - The minute at which to reload. (Range: 0-59)

month - The month at which to reload. (january ... december)

day - The day of the month at which to reload. (Range: 1-31)

year - The year at which to reload. (Range: 1970-2037)

reload in - An interval after which to reload the switch.

hours - The number of hours, combined with the minutes, before the switch resets. (Range: 0-576)

minutes - The number of minutes, combined with the hours, before the switch resets. (Range: 0-59)

reload regularity - A periodic interval at which to reload the switch.

hour - The hour at which to reload. (Range: 0-23)

minute - The minute at which to reload. (Range: 0-59)

day-of-week - Day of the week at which to reload.
(Range: monday ... saturday)

day - Day of the month at which to reload. (Range: 1-31)

reload cancel - Cancels the specified reload option.

DEFAULT SETTING

None

COMMAND MODE

Global Configuration

COMMAND USAGE

- This command resets the entire system.
- Any combination of reload options may be specified. If the same option is re-specified, the previous setting will be overwritten.
- When the system is restarted, it will always run the Power-On Self-Test. It will also retain all configuration information stored in non-volatile memory by the copy running-config startup-config command (See "copy" on page 914).

EXAMPLE

This example shows how to reset the switch after 30 minutes:

```
Console(config)#reload in minute 30
***
*** --- Rebooting at January  1 02:10:43 2007 ---
***

Are you sure to reboot the system at the specified time? <y/n>
```

enable

This command activates Privileged Exec mode. In privileged mode, additional commands are available, and certain commands display additional information. See "Understanding Command Modes" on page 874.

SYNTAX

enable [*level*]

level - Privilege level to log into the device.

The device has two predefined privilege levels: 0: Normal Exec, 15: Privileged Exec. Enter level 15 to access Privileged Exec mode.

DEFAULT SETTING

Level 15

COMMAND MODE

Normal Exec

COMMAND USAGE

- “super” is the default password required to change the command mode from Normal Exec to Privileged Exec. (To set this password, see the enable password command.)
- The “#” character is appended to the end of the prompt to indicate that the system is in privileged access mode.

EXAMPLE

```
Console>enable
Password: [privileged level password]
Console#
```

RELATED COMMANDS

disable (888)

enable password (1032)

quit

This command exits the configuration program.

DEFAULT SETTING

None

COMMAND MODE

Normal Exec, Privileged Exec

COMMAND USAGE

The **quit** and **exit** commands can both exit the configuration program.

EXAMPLE

This example shows how to quit a CLI session:

```
Console#quit

Press ENTER to start session

User Access Verification

Username:
```

show history

This command shows the contents of the command history buffer.

DEFAULT SETTING

None

COMMAND MODE

Normal Exec, Privileged Exec

COMMAND USAGE

The history buffer size is fixed at 10 Execution commands and 10 Configuration commands.

EXAMPLE

In this example, the show history command lists the contents of the command history buffer:

```
Console#show history
Execution command history:
 2 config
 1 show history

Configuration command history:
 4 interface vlan 1
 3 exit
 2 interface vlan 1
 1 end

Console#
```

The **!** command repeats commands from the Execution command history buffer when you are in Normal Exec or Privileged Exec Mode, and commands from the Configuration command history buffer when you are in any of the configuration modes. In this example, the **!2** command repeats the second command in the Execution history buffer (**config**).

```
Console#!2
Console#config
Console(config)#
```

configure

This command activates Global Configuration mode. You must enter this mode to modify any settings on the switch. You must also enter Global Configuration mode prior to enabling some of the other configuration modes, such as Interface Configuration, Line Configuration, and VLAN Database Configuration. See "Understanding Command Modes" on page 874.

DEFAULT SETTING

None

COMMAND MODE

Privileged Exec

EXAMPLE

```
Console#configure
Console(config)#
```

RELATED COMMANDS

end (889)

disable

This command returns to Normal Exec mode from privileged mode. In normal access mode, you can only display basic information on the switch's configuration or Ethernet statistics. To gain access to all commands, you must use the privileged mode. See "Understanding Command Modes" on page 874.

DEFAULT SETTING

None

COMMAND MODE

Privileged Exec

COMMAND USAGE

The “>” character is appended to the end of the prompt to indicate that the system is in normal access mode.

EXAMPLE

```
Console#disable
Console>
```

RELATED COMMANDS

enable (885)

reload (Privileged Exec)

This command restarts the system.

NOTE: When the system is restarted, it will always run the Power-On Self-Test. It will also retain all configuration information stored in non-volatile memory by the copy running-config startup-config command.

DEFAULT SETTING

None

COMMAND MODE

Privileged Exec

COMMAND USAGE

This command resets the entire system.

EXAMPLE

This example shows how to reset the switch:

```
Console#reload
System will be restarted, continue <y/n>? y
```

show reload

This command displays the current reload settings, and the time at which next scheduled reload will take place.

Command Mode

Privileged Exec

Example

```
Console#show reload
Reloading switch in time:                      0 hours 29 minutes.

The switch will be rebooted at January  1 02:11:50 2001.
Remaining Time: 0 days, 0 hours, 29 minutes, 52 seconds.
Console#
```

end

This command returns to Privileged Exec mode.

Default Setting

None

Command Mode

Global Configuration, Interface Configuration, Line Configuration, VLAN Database Configuration, and Multiple Spanning Tree Configuration.

Example

This example shows how to return to the Privileged Exec mode from the Interface Configuration mode:

```
Console(config-if)#end
Console#
```

exit

This command returns to the previous configuration mode or exits the configuration program.

Default Setting

None

Command Mode

Any

EXAMPLE

This example shows how to return to the Privileged Exec mode from the Global Configuration mode, and then quit the CLI session:

```
Console(config)#exit
Console#exit

Press ENTER to start session

User Access Verification

Username:
```

24 System Management Commands

The system management commands are used to control system logs, passwords, user names, management options, and display or configure a variety of other system information.

Table 59: System Management Commands

Command Group	Function
Device Designation	Configures information that uniquely identifies this switch
Banner Information	Configures administrative contact, device identification and location
System Status	Displays system configuration, active managers, and version information
Fan Control	Forces fans to full speed
Frame Size	Enables support for jumbo frames
File Management	Manages code image or switch configuration files
Line	Sets communication parameters for the serial port, including baud rate and console time-out
Event Logging	Controls logging of error messages
SMTP Alerts	Configures SMTP email alerts
Time (System Clock)	Sets the system clock automatically via NTP/SNTP server or manually
Time Range	Sets a time range for use by other functions, such as Access Control Lists
Precision Time Protocol	Configures clock synchronization for the local network
Synchronous Ethernet	Synchronizes specified links to the same frequency in order to transfer timing information to remote sites
Switch Clustering	Configures management of multiple devices via a single IP address

Device Designation

This section describes commands used to configure information that uniquely identifies the switch.

Table 60: Device Designation Commands

Command	Function	Mode
hostname	Specifies the host name for the switch	GC
snmp-server contact	Sets the system contact string	GC
snmp-server location	Sets the system location string	GC

hostname

This command specifies or modifies the host name for this device. Use the **no** form to restore the default host name.

SYNTAX

hostname *name*

no hostname

name - The name of this host. (Maximum length: 255 characters)

DEFAULT SETTING

None

COMMAND MODE

Global Configuration

EXAMPLE

```
Console(config)#hostname RD#1
Console(config)#
```

BANNER INFORMATION

These commands are used to configure and manage administrative information about the switch, its exact data center location, details of the electrical and network circuits that supply the switch, as well as contact information for the network administrator and system manager. This information is only available via the CLI and is automatically displayed before login as soon as a console or telnet connection has been established.

Table 61: Banner Commands

Command	Function	Mode
banner configure	Configures the banner information that is displayed before login	GC
banner configure company	Configures the Company information that is displayed by banner	GC
banner configure dc-power-info	Configures the DC Power information that is displayed by banner	GC
banner configure department	Configures the Department information that is displayed by banner	GC
banner configure equipment-info	Configures the Equipment information that is displayed by banner	GC
banner configure equipment-location	Configures the Equipment Location information that is displayed by banner	GC
banner configure ip-lan	Configures the IP and LAN information that is displayed by banner	GC
banner configure lp-number	Configures the LP Number information that is displayed by banner	GC

Table 61: Banner Commands (Continued)

Command	Function	Mode
banner configure manager-info	Configures the Manager contact information that is displayed by banner	GC
banner configure mux	Configures the MUX information that is displayed by banner	GC
banner configure note	Configures miscellaneous information that is displayed by banner under the Notes heading	GC
show banner	Displays all banner information	NE, PE

banner configure

This command is used to interactively specify administrative information for this device.

SYNTAX

banner configure

DEFAULT SETTING

None

COMMAND MODE

Global Configuration

COMMAND USAGE

The administrator can batch-input all details for the switch with one command. When the administrator finishes typing the company name and presses the enter key, the script prompts for the next piece of information, and so on, until all information has been entered. Pressing enter without inputting information at any prompt during the script's operation will leave the field empty. Spaces can be used during script mode because pressing the enter key signifies the end of data input. The delete and left-arrow keys terminate the script. The use of the backspace key during script mode is not supported. If, for example, a mistake is made in the company name, it can be corrected with the **banner configure company** command.

EXAMPLE

```
Console(config)#banner configure

Company: Edge-Core Networks
Responsible department: R&D Dept
Name and telephone to Contact the management people
Manager1 name: Sr. Network Admin
 phone number: 123-555-1212
Manager2 name: Jr. Network Admin
 phone number: 123-555-1213
Manager3 name: Night-shift Net Admin / Janitor
 phone number: 123-555-1214
The physical location of the equipment.
City and street address: 12 Straight St. Motown, Zimbabwe
Information about this equipment:
Manufacturer: Edge-Core Networks
ID: 123_unique_id_number
Floor: 2
```

```
Row: 7
Rack: 29
Shelf in this rack: 8
Information about DC power supply.
Floor: 2
Row: 7
Rack: 25
Electrical circuit: : ec-177743209-xb
Number of LP:12
Position of the equipment in the MUX:1/23
IP LAN:192.168.1.1
Note: This is a random note about this managed switch and can contain
  miscellaneous information.
Console(config)#
```

banner configure company

This command is used to configure company information displayed in the banner. Use the **no** form to remove the company name from the banner display.

SYNTAX

banner configure company *name*

no banner configure company

name - The name of the company.
(Maximum length: 32 characters)

DEFAULT SETTING

None

COMMAND MODE

Global Configuration

COMMAND USAGE

Input strings cannot contain spaces. The **banner configure company** command interprets spaces as data input boundaries. The use of underscores (_) or other unobtrusive non-letter characters is suggested for situations where white space is necessary for clarity.

EXAMPLE

```
Console(config)#banner configure company Big-Ben
Console(config)#
```

banner configure dc-power-info

This command is use to configure DC power information displayed in the banner. Use the **no** form to restore the default setting.

SYNTAX

banner configure dc-power-info floor *floor-id* **row** *row-id* **rack** *rack-id* **electrical-circuit** *ec-id*

no banner configure dc-power-info [**floor** | **row** | **rack** | **electrical-circuit**]

floor-id - The floor number.

row-id - The row number.

rack-id - The rack number.

ec-id - The electrical circuit ID.

Maximum length of each parameter: 32 characters

DEFAULT SETTING

None

COMMAND MODE

Global Configuration

COMMAND USAGE

Input strings cannot contain spaces. The **banner configure dc-power-info** command interprets spaces as data input boundaries. The use of underscores (_) or other unobtrusive non-letter characters is suggested for situations where white space is necessary for clarity.

EXAMPLE

```
Console(config)#banner configure dc-power-info floor 3 row 15 rack 24
  electrical-circuit 48v-id_3.15.24.2
Console(config)#
```

banner configure department

This command is used to configure the department information displayed in the banner. Use the **no** form to restore the default setting.

SYNTAX

banner configure department *dept***-***name*

no banner configure department

dept-name - The name of the department.
(Maximum length: 32 characters)

DEFAULT SETTING

None

COMMAND MODE

Global Configuration

COMMAND USAGE

Input strings cannot contain spaces. The **banner configure department** command interprets spaces as data input boundaries. The use of underscores (_) or other unobtrusive non-letter characters is suggested for situations where white space is necessary for clarity.

EXAMPLE

```
Console(config)#banner configure department R&D
Console(config)#
```

banner configure equipment-info

This command is used to configure the equipment information displayed in the banner. Use the **no** form to restore the default setting.

SYNTAX

banner configure equipment-info manufacturer-id *mfr-id* **floor** *floor-id* **row** *row-id* **rack** *rack-id* **shelf-rack** *sr-id* **manufacturer** *mfr-name*

no banner configure equipment-info [**floor** | **manufacturer** | **manufacturer-id** | **rack** | **row** | **shelf-rack**]

mfr-id - The name of the device model number.

floor-id - The floor number.

row-id - The row number.

rack-id - The rack number.

sr-id - The shelf number in the rack.

mfr-name - The name of the device manufacturer.

Maximum length of each parameter: 32 characters

DEFAULT SETTING

None

COMMAND MODE

Global Configuration

COMMAND USAGE

Input strings cannot contain spaces. The **banner configure equipment-info** command interprets spaces as data input boundaries. The use of underscores (_) or other unobtrusive non-letter characters is suggested for situations where white space is necessary for clarity.

Example

```
Console(config)#banner configure equipment-info manufacturer-id ECS4660-28F
  floor 3 row 10 rack 15 shelf-rack 12 manufacturer Edge-Core
Console(config)#
```

banner configure equipment-location

This command is used to configure the equipment location information displayed in the banner. Use the **no** form to restore the default setting.

Syntax

banner configure equipment-location *location*

no banner configure equipment-location

location - The address location of the device.
(Maximum length: 32 characters)

Default Setting

None

Command Mode

Global Configuration

Command Usage

Input strings cannot contain spaces. The **banner configure equipment-location** command interprets spaces as data input boundaries. The use of underscores (_) or other unobtrusive non-letter characters is suggested for situations where white space is necessary for clarity.

Example

```
Console(config)#banner configure equipment-location
  710_Network_Path,_Indianapolis
Console(config)#
```

banner configure ip-lan

This command is used to configure the device IP address and subnet mask information displayed in the banner. Use the **no** form to restore the default setting.

Syntax

banner configure ip-lan *ip-mask*

no banner configure ip-lan

ip-mask - The IP address and subnet mask of the device.
(Maximum length: 32 characters)

Default Setting

None

COMMAND MODE

Global Configuration

COMMAND USAGE

Input strings cannot contain spaces. The **banner configure ip-lan** command interprets spaces as data input boundaries. The use of underscores (_) or other unobtrusive non-letter characters is suggested for situations where white space is necessary for clarity.

EXAMPLE

```
Console(config)#banner configure ip-lan 192.168.1.1/255.255.255.0
Console(config)#
```

banner configure lp-number

This command is used to configure the LP number information displayed in the banner. Use the **no** form to restore the default setting.

SYNTAX

banner configure lp-number *lp-num*

no banner configure lp-number

lp-num - The LP number. (Maximum length: 32 characters)

DEFAULT SETTING

None

COMMAND MODE

Global Configuration

COMMAND USAGE

Input strings cannot contain spaces. The **banner configure lp-number** command interprets spaces as data input boundaries. The use of underscores (_) or other unobtrusive non-letter characters is suggested for situations where white space is necessary for clarity.

EXAMPLE

```
Console(config)#banner configure lp-number 12
Console(config)#
```

banner configure manager-info

This command is used to configure the manager contact information displayed in the banner. Use the **no** form to restore the default setting.

SYNTAX

banner configure manager-info
name *mgr1-name* **phone-number** *mgr1-number*
[**name2** *mgr2-name* **phone-number** *mgr2-number* |
name3 *mgr3-name* **phone-number** *mgr3-number*]

no banner configure manager-info [**name1** | **name2** | **name3**]

mgr1-name - The name of the first manager.

mgr1-number - The phone number of the first manager.

mgr2-name - The name of the second manager.

mgr2-number - The phone number of the second manager.

mgr3-name - The name of the third manager.

mgr3-number - The phone number of the third manager.

Maximum length of each parameter: 32 characters

DEFAULT SETTING

None

COMMAND MODE

Global Configuration

COMMAND USAGE

Input strings cannot contain spaces. The **banner configure manager-info** command interprets spaces as data input boundaries. The use of underscores (_) or other unobtrusive non-letter characters is suggested for situations where white space is necessary for clarity.

EXAMPLE

```
Console(config)#banner configure manager-info name Albert_Einstein phone-
  number 123-555-1212 name2 Lamar phone-number 123-555-1219
Console(config)#
```

banner configure mux

This command is used to configure the mux information displayed in the banner. Use the **no** form to restore the default setting.

SYNTAX

banner configure mux *muxinfo*

no banner configure mux

muxinfo - The circuit and PVC to which the switch is connected. (Maximum length: 32 characters)

DEFAULT SETTING

None

COMMAND MODE

Global Configuration

COMMAND USAGE

Input strings cannot contain spaces. The **banner configure mux** command interprets spaces as data input boundaries. The use of underscores (_) or other unobtrusive non-letter characters is suggested for situations where white space is necessary for clarity.

EXAMPLE

```
Console(config)#banner configure mux telco-8734212kx_PVC-1/23
Console(config)#
```

banner configure note

This command is used to configure the note displayed in the banner. Use the **no** form to restore the default setting.

SYNTAX

banner configure note *note-info*

no banner configure note

note-info - Miscellaneous information that does not fit the other banner categories, or any other information of importance to users of the switch CLI. (Maximum length: 150 characters)

DEFAULT SETTING

None

COMMAND MODE

Global Configuration

COMMAND USAGE

Input strings cannot contain spaces. The **banner configure note** command interprets spaces as data input boundaries. The use of underscores (_) or other unobtrusive non-letter characters is suggested for situations where white space is necessary for clarity.

EXAMPLE

```
Console(config)#banner configure note !!!!!ROUTINE_MAINTENANCE_firmware-
  upgrade_0100-0500_GMT-0500_20071022!!!!!_20min_network_impact_expected
Console(config)#
```

show banner

This command displays all banner information.

COMMAND MODE

Normal Exec, Privileged Exec

EXAMPLE

```
Console#show banner
Edge-Core
WARNING - MONITORED ACTIONS AND ACCESSES
R&D

Albert_Einstein - 123-555-1212
Lamar - 123-555-1219

Station's information:
710_Network_Path,_Indianapolis

 Edge-Core - ECS4660-28F
Floor / Row / Rack / Sub-Rack
 3/ 10 / 15 / 12
DC power supply:
Power Source A: Floor / Row / Rack / Electrical circuit
 3/ 15 / 24 / 48v-id_3.15.24.2
Number of LP: 12
Position MUX: telco-8734212kx_PVC-1/23
IP LAN: 192.168.1.1/255.255.255.0
Note: !!!!!ROUTINE_MAINTENANCE_firmware-upgrade_0100-0500_GMT-
  0500_20071022!!!!!_20min_network_
Console#
```

SYSTEM STATUS

This section describes commands used to display system information.

Table 62: System Status Commands

Command	Function	Mode
show access-list tcam-utilization	Shows utilization parameters for TCAM	PE
show alarm-status	Shows information for predefined alarms	PE
show memory	Shows memory utilization parameters	NE, PE
show process cpu	Shows CPU utilization parameters	NE, PE
show running-config	Displays the configuration data currently in use	PE
show startup-config	Displays the contents of the configuration file (stored in flash memory) that is used to start up the system	PE
show system	Displays system information	NE, PE
show tech-support	Displays a detailed list of system settings designed to help technical support resolve configuration or functional problems	PE
show users	Shows all active console and Telnet sessions, including user name, idle time, and IP address of Telnet clients	NE, PE
show version	Displays version information for the system	NE, PE

Table 62: System Status Commands (Continued)

Command	Function	Mode
show watchdog	Shows if watchdog debugging is enabled	PE
watchdog software	Monitors key processes, and automatically reboots the system if any of these processes are not responding correctly	PE

show access-list tcam-utilization

This command shows utilization parameters for TCAM (Ternary Content Addressable Memory), including the number policy control entries in use, the number of free entries, and the overall percentage of TCAM in use.

COMMAND MODE

Privileged Exec

COMMAND USAGE

Policy control entries (PCEs) are used by various system functions which rely on rule-based searches, including Access Control Lists (ACLs), IP Source Guard filter rules, Quality of Service (QoS) processes, or traps.

For example, when binding an ACL to a port, each rule in an ACL will use two PCEs; and when setting an IP Source Guard filter rule for a port, the system will also use two PCEs.

EXAMPLE

```
Console#show access-list tcam-utilization
  Total Policy Control Entries : 1664
  Free Policy Control Entries  : 1664
  Entries Used by System       : 0
  Entries Used by User         : 0
  TCAM Utilization             : 0.0%
Console#
```

show alarm-status

This command displays information on predefined alarms (i.e., non-configurable) and on the link-down alarm (which is displayed as a minor alarm).

Command Mode

Privileged Exec

Command Usage

- Alarms are signalled through the Alarm LEDs (Major Alarm and Minor Alarm) and the Alarm Input and Output port on the front panel. When an alarm occurs, the corresponding LEDs will not be extinguished until the alarm condition is resolved. The event that triggered the alarm can be viewed using this command. Alarms are also recorded in the system log, and can viewed using the show log command.

- The alarms supported by this switch include the internal alarms described below and various external alarms which can be sent to the switch through hard-wired connections described in the *Installation Guide*. Refer to the *Installation Guide* for information on how to use the alarm relay contacts and external site alarm inputs.

- Major alarms include the failure of all fans, both thermal detectors exceeding 65°C, or an invalid power module being installed. Minor alarms include the failure of one or two fans, or when a second power module is installed but it is not functioning.

EXAMPLE

The following shows the message types displayed when no alarms are active, and another example when both minor and major alarms occur.

```
Console#show alarm-status
Unit 1
 Asserted Alarm Input    : [NONE]
 Current Major Alarm Status:[NONE]
 Current Minor Alarm Status:[NONE]
 Current Major Alarm Output Status:[INACTIVE]
 Current Minor Alarm Output Status:[INACTIVE]
Console#
```

show memory

This command shows memory utilization parameters, and alarm thresholds.

COMMAND MODE

Normal Exec, Privileged Exec

COMMAND USAGE

This command shows the amount of memory currently free for use, the amount of memory allocated to active processes, and the total amount of system memory.

EXAMPLE

```
Console#show memory
 Status Bytes      %
 ------ ---------- ---
 Free    406712320  75
 Used    130158592  25
 Total   536870912

 Alarm Configuration
  Rising Threshold          : 90%
  Falling Threshold         : 70%

Console#
```

RELATED COMMANDS

memory (1015)

show process cpu

This command shows the CPU utilization parameters, alarm status, and alarm configuration.

COMMAND MODE

Normal Exec, Privileged Exec

EXAMPLE

```
Console#show process cpu
 CPU Utilization in the past 5 seconds : 7%

 CPU Utilization in the past 60 seconds
  Average Utilization      : 8%
  Maximum Utilization      : 9%

 Alarm Status
  Current Alarm Status     : Off
  Last Alarm Start Time    : Jun  9 15:10:09 2011
  Last Alarm Duration Time : 10 seconds

 Alarm Configuration
  Rising Threshold         : 90%
  Falling Threshold        : 70%

Console#
```

RELATED COMMANDS

process cpu (1016)

show running-config

This command displays the configuration information currently in use.

SYNTAX

show running-config

COMMAND MODE

Privileged Exec

COMMAND USAGE

- Use this command in conjunction with the **show startup-config** command to compare the information in running memory to the information stored in non-volatile memory.

- This command displays settings for key command modes. Each mode group is separated by "!" symbols, and includes the configuration mode command, and corresponding commands. This command displays the following information:
  - MAC address for the switch
  - L2 Protocol Tunnel destination MAC
  - SNMP community strings
  - Users (names, access levels, and encrypted passwords)
  - VLAN database (VLAN ID, name and state)
  - VLAN configuration settings for each interface

- Multiple spanning tree instances (name and interfaces)
- IP address configured for management VLAN
- Interface settings
- Any configured settings for the console port and Telnet

EXAMPLE

```
Console#show running-config
Building startup configuration. Please wait...
!<stackingDB>00</stackingDB>
!<stackingMac>01_00-e0-0c-00-00-fd_00</stackingMac>
!
l2protocol-tunnel tunnel-dmac 01-12-cf-00-00-00
!
snmp-server community public ro
snmp-server community private rw
!
snmp-server enable traps authentication
!
username admin access-level 15
username admin password 7 21232f297a57a5a743894a0e4a801fc3
username guest access-level 0
username guest password 7 084e0343a0486ff05530df6c705c8bb4
enable password level 15 7 1b3231655cebb7a1f783eddf27d254ca
!
vlan database
 VLAN 1 name DefaultVlan media ethernet state active
!
spanning-tree mst configuration
interface ethernet 1/1
 queue weight 1 2 4 6 8 10 12 14
⋮

!
interface ethernet 1/1
 switchport allowed vlan add 1 untagged
 switchport native vlan 1
 switchport allowed vlan add 4094 tagged
⋮

!
interface vlan 1
 ip address dhcp
!
interface craft
!
line console
!
line vty
!
end
!
Console#
```

RELATED COMMANDS

show startup-config (906)

show startup-config

This command displays the configuration file stored in non-volatile memory that is used to start up the system.

COMMAND MODE

Privileged Exec

COMMAND USAGE

- Use this command in conjunction with the **show running-config** command to compare the information in running memory to the information stored in non-volatile memory.
- This command displays settings for key command modes. Each mode group is separated by "!" symbols, and includes the configuration mode command, and corresponding commands. This command displays the following information:
  - MAC address for the switch
  - L2 Protocol Tunnel destination MAC
  - SNMP community strings
  - Users (names, access levels, and encrypted passwords)
  - VLAN database (VLAN ID, name and state)
  - VLAN configuration settings for each interface
  - Multiple spanning tree instances (name and interfaces)
  - IP address configured for management VLAN
  - Interface settings
  - Any configured settings for the console port and Telnet

EXAMPLE

Refer to the example for the running configuration file.

RELATED COMMANDS

show running-config (904)

show system

This command displays system information.

DEFAULT SETTING

None

COMMAND MODE

Normal Exec, Privileged Exec

COMMAND USAGE

- For a description of the items shown by this command, refer to "Displaying System Information" on page 149.
- There are three fans in the switch. Fans 1 - 3 are located from the font to the back of the fan tray, and provide cooling for the power supply and other internal components by forcing air out of the unit.

- There are two thermal detectors in the switch The first detector is near the air flow intake vents. The second detector is near the switch ASIC and CPU.

EXAMPLE

```
Console#show system
System Description : ECS4660-28F
System OID String  : 1.3.6.1.4.1.259.10.1.10
System Information
 System Up Time         : 0 days, 5 hours, 44 minutes, and 42.28 seconds
 System Name            :
 System Location        :
 System Contact         :
 MAC Address (Unit 1)   : 00-00-0C-00-00-FD
 Web Server             : Enabled
 Web Server Port        : 80
 Web Secure Server      : Enabled
 Web Secure Server Port : 443
 Telnet Server          : Enabled
 Telnet Server Port     : 23
 Jumbo Frame            : Disabled

System Fan:
 Force Fan Speed Full   : Disabled
Unit 1
 Fan 1: Ok                    Fan 2: Ok                    Fan 3: Ok
System Temperature:
Unit 1
 Temperature 1:  29 degrees     Temperature 2:  32 degrees

 Main Power Status      : Up
 Redundant Power Status : Not present
 Main Power Type        : [AC100~240V to +12V Module]
 Redundant Power Type   : [None]
Console#
```

show tech-support

This command displays a detailed list of system settings designed to help technical support resolve configuration or functional problems.

COMMAND MODE

Normal Exec, Privileged Exec

COMMAND USAGE

This command generates a long list of information including detailed system and interface settings. It is therefore advisable to direct the output to a file using any suitable output capture function provided with your terminal emulation program.

EXAMPLE

```
Console#show tech-support

show system:
System Description : ECS4660-28F
System OID String  : 1.3.6.1.4.1.259.10.1.10
System Information
 System Up Time:          0 days, 2 hours, 17 minutes, and 6.23 seconds
 System Name:             [NONE]
 System Location:         [NONE]
 System Contact:          [NONE]
 MAC Address (Unit1):     00-12-CF-61-24-2F
 Web Server:              Enabled
 Web Server Port:         80
 Web Secure Server:       Enabled
 Web Secure Server Port:  443
 Telnet Server:           Enable
 Telnet Server Port:      23
 Jumbo Frame:             Disabled
⋮
```

show users

Shows all active console and Telnet sessions, including user name, idle time, and IP address of Telnet client.

DEFAULT SETTING

None

COMMAND MODE

Normal Exec, Privileged Exec

COMMAND USAGE

The session used to execute this command is indicated by a "*" symbol next to the Line (i.e., session) index number.

EXAMPLE

```
Console#show users
 User Name Accounts:
  User Name Privilege Public-Key
  --------- --------- ----------
      admin        15 None
      guest         0 None
      steve        15  RSA

 Online Users:
  Line        Username Idle time (h:m:s) Remote IP addr.
  ----------- -------- ----------------- ---------------
  0   console    admin           0:14:14
* 1     VTY 0    admin           0:00:00    192.168.1.19
  2     SSH 1    steve           0:00:06    192.168.1.19

 Web Online Users:
  Line        Remote IP Addr  User Name Idle time (h:m:s)
  ----------- --------------- --------- ------------------
  1      HTTP    192.168.1.19     admin            0:00:00

Console#
```

show version

This command displays hardware and software version information for the system.

COMMAND MODE

Normal Exec, Privileged Exec

COMMAND USAGE

See "Displaying Hardware/Software Versions" on page 151 for detailed information on the items displayed by this command.

EXAMPLE

```
Console#show version
Unit 1
 Serial Number           : S123456
 Hardware Version        : R0A
 EPLD Version            : 13.08
 Number of Ports         : 28
 Main Power Status       : Up
 Redundant Power Status : Not present
 Role                    : Master
 Loader Version          : 1.3.2.3
 Linux Kernel Version    : 2.6.19.2-0.1
 Boot ROM Version        : 0.0.0.1
 Operation Code Version : 1.0.0.0

Console#
```

show watchdog

This command shows if watchdog debugging is enabled.

COMMAND MODE

Privileged Exec

EXAMPLE

```
Console#show watchdog

Software Watchdog Information
 Status :    Enabled
Console#
```

watchdog software

This command monitors key processes, and automatically reboots the system if any of these processes are not responding correctly.

SYNTAX

watchdog software {**disable** | **enable**}

DEFAULT SETTING

Disabled

COMMAND MODE

Privileged Exec

EXAMPLE

```
Console#watchdog
Console#
```

FAN CONTROL

This section describes the command used to force fan speed.

Table 63: Fan Control Commands

Command	Function	Mode
fan-speed force-full	Forces fans to full speed	GC
show system	Shows if full fan speed is enabled	NE, PE

fan-speed force-full

This command sets all fans to full speed. Use the no form to reset the fans to normal operating speed.

SYNTAX

[**no**] **fan-speed force-full**

DEFAULT SETTING

Normal speed

COMMAND MODE

Global Configuration

EXAMPLE

```
Console(config)#fan-speed force-full
Console(config)#
```

FRAME SIZE

This section describes commands used to configure the Ethernet frame size on the switch.

Table 64: Frame Size Commands

Command	Function	Mode
jumbo frame	Enables support for jumbo frames	GC

jumbo frame

This command enables support for layer 2 jumbo frames for Gigabit and 10 Gigabit Ethernet ports. Use the **no** form to disable it.

SYNTAX

[**no**] **jumbo frame**

DEFAULT SETTING

Disabled

COMMAND MODE

Global Configuration

COMMAND USAGE

- This switch provides more efficient throughput for large sequential data transfers by supporting jumbo frames on Gigabit and 10 Gigabit Ethernet ports or trunks of up to 9216 bytes. Compared to standard Ethernet frames that run only up to 1.5 KB, using jumbo frames significantly reduces the per-packet overhead required to process protocol encapsulation fields.

- To use jumbo frames, both the source and destination end nodes (such as a computer or server) must support this feature. Also, when the connection is operating at full duplex, all switches in the network between the two end nodes must be able to accept the extended frame size. And for half-duplex connections, all devices in the collision domain would need to support jumbo frames.

- This command globally enables support for jumbo frames on all Gigabit and 10 Gigabit ports and trunks. To set the MTU for a specific interface, enable jumbo frames and use the switchport mtu command to specify the required size of the MTU.

- The current setting for jumbo frames can be displayed with the show system command.

EXAMPLE

```
Console(config)#jumbo frame
Console(config)#
```

FILE MANAGEMENT

Managing Firmware

Firmware can be uploaded and downloaded to or from an FTP/TFTP server. By saving runtime code to a file on an FTP/TFTP server, that file can later be downloaded to the switch to restore operation. The switch can also be set to use new firmware without overwriting the previous version.

When downloading runtime code, the destination file name can be specified to replace the current image, or the file can be first downloaded using a different name from the current runtime code file, and then the new file set as the startup file.

Saving or Restoring Configuration Settings

Configuration settings can be uploaded and downloaded to and from an FTP/TFTP server. The configuration file can be later downloaded to restore switch settings.

The configuration file can be downloaded under a new file name and then set as the startup file, or the current startup configuration file can be specified as the destination file to directly replace it. Note that the file "Factory_Default_Config.cfg" can be copied to the FTP/TFTP server, but cannot be used as the destination on the switch.

Table 65: Flash/File Commands

Command	Function	Mode
General Commands		
boot system	Specifies the file or image used to start up the system	GC
copy	Copies a code image or a switch configuration to or from flash memory or an FTP/TFTP server	PE
delete	Deletes a file or code image	PE
dir	Displays a list of files in flash memory	PE
umount usbdisk	Prepares the USB memory device to be safely removed	PE
whichboot	Displays the files booted	PE
Automatic Code Upgrade Commands		
upgrade opcode auto	Automatically upgrades the current image when a new version is detected on the indicated server	GC
upgrade opcode path	Specifies an FTP/TFTP server and directory in which the new opcode is stored	GC
upgrade opcode reload	Reloads the switch automatically after the opcode upgrade is completed	GC
show upgrade	Shows the opcode upgrade configuration settings.	PE

General Commands

boot system

This command specifies the file or image used to start up the system.

SYNTAX

boot system {**boot-rom** | **config** | **opcode**}: *filename*

boot-rom* - Boot ROM.

config* - Configuration file.

opcode* - Run-time operation code.

filename - Name of configuration file or code image.

* The colon (:) is required.

DEFAULT SETTING

None

COMMAND MODE

Global Configuration

COMMAND USAGE

- A colon (:) is required after the specified file type.
- If the file contains an error, it cannot be set as the default file.

EXAMPLE

```
Console(config)#boot system config: startup
Console(config)#
```

RELATED COMMANDS

dir (918)
whichboot (919)

copy

This command moves (upload/download) a code image or configuration file between the switch's flash memory and an FTP/TFTP server. When you save the system code or configuration settings to a file on an FTP/TFTP server, that file can later be downloaded to the switch to restore system operation. The success of the file transfer depends on the accessibility of the FTP/TFTP server and the quality of the network connection.

SYNTAX

copy file {**file** | **ftp** | **running-config** | **startup-config** | **tftp**}
copy ftp {**add-to-running-config** | **file** | **https-certificate** | **public-key** | **running-config** | **startup-config**}
copy running-config {**file** | **ftp** | **startup-config** | **tftp**}
copy startup-config {**file** | **ftp** | **running-config** | **tftp**}
copy tftp {**add-to-running-config** | **file** | **https-certificate** | **public-key** | **running-config** | **startup-config**}
copy usbdisk file

add-to-running-config - Keyword that adds the settings listed in the specified file to the running configuration.

file - Keyword that allows you to copy to/from a file.

ftp - Keyword that allows you to copy to/from an FTP server.

https-certificate - Keyword that allows you to copy the HTTPS secure site certificate.

public-key - Keyword that allows you to copy a SSH key from a TFTP server. (See "Secure Shell" on page 1057.)

running-config - Keyword that allows you to copy to/from the current running configuration.

startup-config - The configuration used for system initialization.

tftp - Keyword that allows you to copy to/from a TFTP server.

usbdisk - Keyword that allows you to copy to/from a USB memory stick. (USB slot only supports simple data storage devices using a FAT16/32 file system with or without a partition table.)

DEFAULT SETTING

None

COMMAND MODE

Privileged Exec

COMMAND USAGE

- The system prompts for data required to complete the copy command.
- The destination file name should not contain slashes (\ or /), and the maximum length for file names is 32 characters for files on the switch or 128 characters for files on the server. (Valid characters: A-Z, a-z, 0-9, ".", "-")
- The switch supports only two operation code files, but the maximum number of user-defined configuration files is 16.

- You can use “Factory_Default_Config.cfg” as the source to copy from the factory default configuration file, but you cannot use it as the destination.

- To replace the startup configuration, you must use **startup-config** as the destination.

- The Boot ROM and Loader cannot be uploaded or downloaded from the FTP/TFTP server. You must follow the instructions in the release notes for new firmware, or contact your distributor for help.

- For information on specifying an https-certificate, see "Replacing the Default Secure-site Certificate" on page 380. For information on configuring the switch to use HTTPS for a secure connection, see the ip http secure-server command.

- When logging into an FTP server, the interface prompts for a user name and password configured on the remote server. Note that “anonymous” is set as the default user name.

EXAMPLE

The following example shows how to download new firmware from a TFTP server:

```
Console#copy tftp file
TFTP server ip address: 10.1.0.19
Choose file type:
 1. config:  2. opcode: <1-2>: 2
Source file name: m360.bix
Destination file name: m360.bix
\Write to FLASH Programming.
-Write to FLASH finish.
Success.
Console#
```

The following example shows how to upload the configuration settings to a file on the TFTP server:

```
Console#copy file tftp
Choose file type:
 1. config:  2. opcode: <1-2>: 1
Source file name: startup
TFTP server ip address: 10.1.0.99
Destination file name: startup.01
TFTP completed.
Success.

Console#
```

The following example shows how to copy the running configuration to a startup file.

```
Console#copy running-config file
destination file name: startup
Write to FLASH Programming.
\Write to FLASH finish.
Success.

Console#
```

The following example shows how to download a configuration file:

```
Console#copy tftp startup-config
TFTP server ip address: 10.1.0.99
Source configuration file name: startup.01
Startup configuration file name [startup]:
Write to FLASH Programming.

\Write to FLASH finish.
Success.

Console#
```

This example shows how to copy a secure-site certificate from an TFTP server. It then reboots the switch to activate the certificate:

```
Console#copy tftp https-certificate
TFTP server ip address: 10.1.0.19
Source certificate file name: SS-certificate
Source private file name: SS-private
Private password: ********

Success.
Console#reload
System will be restarted, continue <y/n>? y
```

This example shows how to copy a public-key used by SSH from an TFTP server. Note that public key authentication via SSH is only supported for users configured locally on the switch.

```
Console#copy tftp public-key
TFTP server IP address: 192.168.1.19
Choose public key type:
 1. RSA:  2. DSA: <1-2>: 1
Source file name: steve.pub
Username: steve
TFTP Download
Success.
Write to FLASH Programming.
Success.

Console#
```

This example shows how to copy a file to an FTP server.

```
Console#copy ftp file
FTP server IP address: 169.254.1.11
User[anonymous]: admin
Password[]: *****
Choose file type:
 1. config:  2. opcode: 2
Source file name: BLANC.BIX
Destination file name: BLANC.BIX
Console#
```

delete

This command deletes a file, image, or public key.

SYNTAX

delete {**file** | **usbdisk**} **name** *filename*} |
  public-key *username* [**dsa** | **rsa**]}

file - Keyword that allows you to delete a file.

usbdisk - Keyword indicating USB memory stick or disk.

name - Keyword indicating a file.

filename - Name of configuration file or code image.

public-key - Keyword that allows you to delete a SSH key on the switch. (See "Secure Shell" on page 1057.)

username – Name of an SSH user. (Range: 1-8 characters)

dsa – DSA public key type.

rsa – RSA public key type.

DEFAULT SETTING

None

COMMAND MODE

Privileged Exec

COMMAND USAGE

- If the file type is used for system startup, then this file cannot be deleted.
- “Factory_Default_Config.cfg” cannot be deleted.
- If the public key type is not specified, then both DSA and RSA keys will be deleted.

EXAMPLE

This example shows how to delete the test2.cfg configuration file from flash memory.

```
Console#delete file name test2.cfg
Console#
```

RELATED COMMANDS

dir (918)
delete public-key (1062)

dir

This command displays a list of files in flash memory.

SYNTAX

dir {**boot-rom:** | **config:** | **opcode:** | **usbdisk:**} [*filename*]}

boot-rom - Boot ROM (or diagnostic) image file.

config - Switch configuration file.

opcode - Run-time operation code image file.

usbdisk - System file on a USB memory stick or disk.

filename - Name of configuration file or code image. If this file exists but contains errors, information on this file cannot be shown.

DEFAULT SETTING

None

COMMAND MODE

Privileged Exec

COMMAND USAGE

- If you enter the command **dir** without any parameters, the system displays all files.

  File information is shown below:

Table 66: File Directory Information

Column Heading	Description
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.
Create Time	The date and time the file was created.
Size	The length of the file in bytes.

EXAMPLE

The following example shows how to display all file information:

```
Console#dir
        File Name                  Type  Startup Modify Time         Size(bytes)
-------------------------- -------------- ------- ------------------- ----------
 Unit 1:
ECS4660-28F_V1.2.1.4.bix         OpCode     N    2012-06-25 10:40:53   21627592
ECS4660-28F_V1.2.1.5.bix         OpCode     Y    2001-01-06 14:35:12   21627592
Factory_Default_Config.cfg       Config     N    2010-12-27 02:42:32        455
startup1.cfg                     Config     Y    2001-01-04 19:22:08       1732
 -----------------------------------------------------------------------------
                         Free space for compressed user config files:   2584576
Console#
```

umount usbdisk

This command prepares the USB memory device to be safely removed from the switch.

SYNTAX

umount usbdisk

DEFAULT SETTING

None

COMMAND MODE

Privileged Exec

COMMAND USAGE

Before disconnecting USB memory devices, you must unmount them first. This is similar to “Safely Remove Hardware” in Windows where the device will not unmount until all data transfers have been finished.

EXAMPLE

```
Console#umount usbdisk
You can safely remove your usbdisk.
Console#
```

whichboot

This command displays which files were booted when the system powered up.

SYNTAX

whichboot

DEFAULT SETTING

None

COMMAND MODE

Privileged Exec

EXAMPLE

This example shows the information displayed by the **whichboot** command. See the table under the **dir** command for a description of the file information displayed by this command.

```
Console#whichboot
        File Name                    Type   Startup Modify Time         Size(bytes)
-------------------------------- ------- ------- ------------------- -----------
 Unit 1:
ECS4660_V1.0.0.0.bix             OpCode     Y    2011-11-28 09:25:30   17732136
startup1.cfg                     Config     Y    2011-12-26 12:48:10       1629
Console#
```

Automatic Code Upgrade Commands

upgrade opcode auto

This command automatically upgrades the current operational code when a new version is detected on the server indicated by the upgrade opcode path command. Use the **no** form of this command to restore the default setting.

SYNTAX

[**no**] **upgrade opcode auto**

DEFAULT SETTING

Disabled

COMMAND MODE

Global Configuration

COMMAND USAGE

- This command is used to enable or disable automatic upgrade of the operational code. When the switch starts up and automatic image upgrade is enabled by this command, the switch will follow these steps when it boots up:

  1. It will search for a new version of the image at the location specified by upgrade opcode path command. The name for the new image stored on the TFTP server must be ECS4660_28F.bix. If the switch detects a code version newer than the one currently in use, it will download the new image. If two code images are already stored in the switch, the image not set to start up the system will be overwritten by the new version.

  2. After the image has been downloaded, the switch will send a trap message to log whether or not the upgrade operation was successful.

  3. It sets the new version as the startup image.

  4. It then restarts the system to start using the new image.

- Any changes made to the default setting can be displayed with the show running-config or show startup-config commands.

EXAMPLE

```
Console(config)#upgrade opcode auto
Console(config)#upgrade opcode path tftp://192.168.0.1/sm24/
Console(config)#
```

If a new image is found at the specified location, the following type of messages will be displayed during bootup.

```
:
Automatic Upgrade is looking for a new image
New image detected: current version 1.1.1.0; new version 1.1.1.2
Image upgrade in progress
The switch will restart after upgrade succeeds
Downloading new image
Flash programming started
Flash programming completed
The switch will now restart
:
```

upgrade opcode path

This command specifies an TFTP server and directory in which the new opcode is stored. Use the **no** form of this command to clear the current setting.

SYNTAX

upgrade opcode path *opcode-dir-url*

no upgrade opcode path

opcode-dir-url - The location of the new code.

DEFAULT SETTING

None

COMMAND MODE

Global Configuration

COMMAND USAGE

- This command is used in conjunction with the upgrade opcode auto command to facilitate automatic upgrade of new operational code stored at the location indicated by this command.

- The name for the new image stored on the TFTP server must be ecs4660-28f.bix. However, note that file name is not to be included in this command.

- When specifying a TFTP server, the following syntax must be used, where *filedir* indicates the path to the directory containing the new image:

  ```
  tftp://192.168.0.1[/filedir]/
  ```

- When specifying an FTP server, the following syntax must be used, where *filedir* indicates the path to the directory containing the new image:

  ```
  ftp://[username[:password@]]192.168.0.1[/filedir]/
  ```

  If the user name is omitted, “anonymous” will be used for the connection. If the password is omitted a null string (“”) will be used for the connection.

EXAMPLE

This shows how to specify a TFTP server where new code is stored.

```
Console(config)#upgrade opcode path tftp://192.168.0.1/sm24/
Console(config)#
```

This shows how to specify an FTP server where new code is stored.

```
Console(config)#upgrade opcode path ftp://admin:billy@192.168.0.1/sm24/
Console(config)#
```

upgrade opcode reload

This command reloads the switch automatically after the opcode upgrade is completed. Use the **no** form to disable this feature.

SYNTAX

[**no**] **upgrade opcode reload**

DEFAULT SETTING

Disabled

COMMAND MODE

Global Configuration

EXAMPLE

This shows how to specify a TFTP server where new code is stored.

```
Console(config)#upgrade opcode reload
Console(config)#
```

show upgrade

This command shows the opcode upgrade configuration settings.

COMMAND MODE

Privileged Exec

EXAMPLE

```
Console#show upgrade
Auto Image Upgrade Global Settings:
  Status     : Disabled
  Reload Status : Disabled
  Path       :
  File Name : ECS4600_28F.bix
Console#
```

LINE

You can access the onboard configuration program by attaching a VT100 compatible device to the server's serial port. These commands are used to set communication parameters for the serial port or Telnet (i.e., a virtual terminal).

Table 67: Line Commands

Command	Function	Mode
line	Identifies a specific line for configuration and starts the line configuration mode	GC
accounting exec	Applies an accounting method to local console, Telnet or SSH connections	LC
authorization exec	Applies an authorization method to local console, Telnet or SSH connections	LC
databits*	Sets the number of data bits per character that are interpreted and generated by hardware	LC
exec-timeout	Sets the interval that the command interpreter waits until user input is detected	LC
login	Enables password checking at login	LC
parity*	Defines the generation of a parity bit	LC
password	Specifies a password on a line	LC
password-thresh	Sets the password intrusion threshold, which limits the number of failed logon attempts	LC
silent-time*	Sets the amount of time the management console is inaccessible after the number of unsuccessful logon attempts exceeds the threshold set by the password-thresh command	LC
speed*	Sets the terminal baud rate	LC
stopbits*	Sets the number of the stop bits transmitted per byte	LC
timeout login response	Sets the interval that the system waits for a login attempt	LC

Table 67: Line Commands (Continued)

Command	Function	Mode
disconnect	Terminates a line connection	PE
show line	Displays a terminal line's parameters	NE, PE

* These commands only apply to the serial port.

line

This command identifies a specific line for configuration, and to process subsequent line configuration commands.

SYNTAX

line {**console** | **vty**}

console - Console terminal line.

vty - Virtual terminal for remote console access (i.e., Telnet).

DEFAULT SETTING

There is no default line.

COMMAND MODE

Global Configuration

COMMAND USAGE

Telnet is considered a virtual terminal connection and will be shown as “VTY” in screen displays such as show users. However, the serial communication parameters (e.g., databits) do not affect Telnet connections.

EXAMPLE

To enter console line mode, enter the following command:

```
Console(config)#line console
Console(config-line)#
```

RELATED COMMANDS

show line (932)
show users (908)

databits

This command sets the number of data bits per character that are interpreted and generated by the console port. Use the **no** form to restore the default value.

SYNTAX

databits {**7** | **8**}

no databits

7 - Seven data bits per character.

8 - Eight data bits per character.

DEFAULT SETTING

8 data bits per character

COMMAND MODE

Line Configuration

COMMAND USAGE

The **databits** command can be used to mask the high bit on input from devices that generate 7 data bits with parity. If parity is being generated, specify 7 data bits per character. If no parity is required, specify 8 data bits per character.

EXAMPLE

To specify 7 data bits, enter this command:

```
Console(config-line)#databits 7
Console(config-line)#
```

RELATED COMMANDS

parity (927)

exec-timeout

This command sets the interval that the system waits until user input is detected. Use the **no** form to restore the default.

SYNTAX

exec-timeout [*seconds*]

no exec-timeout

seconds - Integer that specifies the timeout interval. (Range: 60 - 65535 seconds; 0: no timeout)

DEFAULT SETTING

CLI: No timeout
Telnet: 10 minutes

COMMAND MODE

Line Configuration

COMMAND USAGE

- If user input is detected within the timeout interval, the session is kept open; otherwise the session is terminated.

- This command applies to both the local console and Telnet connections.

- The timeout for Telnet cannot be disabled.

- Using the command without specifying a timeout restores the default setting.

EXAMPLE

To set the timeout to two minutes, enter this command:

```
Console(config-line)#exec-timeout 120
Console(config-line)#
```

login

This command enables password checking at login. Use the **no** form to disable password checking and allow connections without a password.

SYNTAX

login [**local**]

no login

local - Selects local password checking. Authentication is based on the user name specified with the username command.

DEFAULT SETTING

login local

COMMAND MODE

Line Configuration

COMMAND USAGE

- There are three authentication modes provided by the switch itself at login:

  - **login** selects authentication by a single global password as specified by the password line configuration command. When using this method, the management interface starts in Normal Exec (NE) mode.

  - **login local** selects authentication via the user name and password specified by the username command (i.e., default setting). When using this method, the management interface starts in Normal Exec (NE) or Privileged Exec (PE) mode, depending on the user's privilege level (0 or 15 respectively).

  - **no login** selects no authentication. When using this method, the management interface starts in Normal Exec (NE) mode.

- This command controls login authentication via the switch itself. To configure user names and passwords for remote authentication servers, you must use the RADIUS or TACACS software installed on those servers.

EXAMPLE

```
Console(config-line)#login local
Console(config-line)#
```

RELATED COMMANDS

username (1033)
password (928)

parity

This command defines the generation of a parity bit. Use the **no** form to restore the default setting.

SYNTAX

parity {**none** | **even** | **odd**}

no parity

none - No parity

even - Even parity

odd - Odd parity

DEFAULT SETTING

No parity

COMMAND MODE

Line Configuration

COMMAND USAGE

Communication protocols provided by devices such as terminals and modems often require a specific parity bit setting.

EXAMPLE

To specify no parity, enter this command:

```
Console(config-line)#parity none
Console(config-line)#
```

password

This command specifies the password for a line. Use the **no** form to remove the password.

SYNTAX

password {**0** | **7**} *password*

no password

{**0** | **7**} - 0 means plain password, 7 means encrypted password

password - Character string that specifies the line password. (Maximum length: 32 characters plain text or encrypted, case sensitive)

DEFAULT SETTING

No password is specified.

COMMAND MODE

Line Configuration

COMMAND USAGE

- When a connection is started on a line with password protection, the system prompts for the password. If you enter the correct password, the system shows a prompt. You can use the password-thresh command to set the number of times a user can enter an incorrect password before the system terminates the line connection and returns the terminal to the idle state.

- The encrypted password is required for compatibility with legacy password settings (i.e., plain text or encrypted) when reading the configuration file during system bootup or when downloading the configuration file from a TFTP server. There is no need for you to manually configure encrypted passwords.

EXAMPLE

```
Console(config-line)#password 0 secret
Console(config-line)#
```

RELATED COMMANDS

login (926)
password-thresh (929)

password-thresh

This command sets the password intrusion threshold which limits the number of failed logon attempts. Use the **no** form to remove the threshold value.

SYNTAX

password-thresh [*threshold*]

no password-thresh

threshold - The number of allowed password attempts. (Range: 1-120; 0: no threshold)

DEFAULT SETTING

The default value is three attempts.

COMMAND MODE

Line Configuration

COMMAND USAGE

When the logon attempt threshold is reached, 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 shuts down.

EXAMPLE

To set the password threshold to five attempts, enter this command:

```
Console(config-line)#password-thresh 5
Console(config-line)#
```

RELATED COMMANDS

silent-time (929)

silent-time

This command sets the amount of time the management console is inaccessible after the number of unsuccessful logon attempts exceeds the threshold set by the password-thresh command. Use the **no** form to remove the silent time value.

SYNTAX

silent-time [*seconds*]

no silent-time

seconds - The number of seconds to disable console response. (Range: 0-65535; where 0 means disabled)

DEFAULT SETTING

The default value is no silent-time.

COMMAND MODE

Line Configuration

EXAMPLE

To set the silent time to 60 seconds, enter this command:

```
Console(config-line)#silent-time 60
Console(config-line)#
```

RELATED COMMANDS

password-thresh (929)

speed

This command sets the terminal line's baud rate. This command sets both the transmit (to terminal) and receive (from terminal) speeds. Use the **no** form to restore the default setting.

SYNTAX

speed *bps*

no speed

bps - Baud rate in bits per second.
(Options: 9600, 19200, 38400, 57600, 115200 bps)

DEFAULT SETTING

115200 bps

COMMAND MODE

Line Configuration

COMMAND USAGE

Set the speed to match the baud rate of the device connected to the serial port. Some baud rates available on devices connected to the port might not be supported. The system indicates if the speed you selected is not supported.

EXAMPLE

To specify 57600 bps, enter this command:

```
Console(config-line)#speed 57600
Console(config-line)#
```

stopbits

This command sets the number of the stop bits transmitted per byte. Use the **no** form to restore the default setting.

SYNTAX

stopbits {**1** | **2**}

no stopbits

1 - One stop bit

2 - Two stop bits

DEFAULT SETTING

1 stop bit

COMMAND MODE

Line Configuration

EXAMPLE

To specify 2 stop bits, enter this command:

```
Console(config-line)#stopbits 2
Console(config-line)#
```

timeout login response

This command sets the interval that the system waits for a user to log into the CLI. Use the **no** form to restore the default setting.

SYNTAX

timeout login response [*seconds*]

no timeout login response

seconds - Integer that specifies the timeout interval.
(Range: 10 - 300 seconds)

DEFAULT SETTING

CLI: Disabled
Telnet: 300 seconds

COMMAND MODE

Line Configuration

COMMAND USAGE

- If a login attempt is not detected within the timeout interval, the connection is terminated for the session.
- This command applies to both the local console and Telnet connections.
- The timeout for Telnet cannot be disabled.

- Using the command without specifying a timeout restores the default setting.

Example

To set the timeout to two minutes, enter this command:

```
Console(config-line)#timeout login response 120
Console(config-line)#
```

disconnect

This command terminates an SSH, Telnet, or console connection.

Syntax

disconnect *session-id*

session-id – The session identifier for an SSH, Telnet or console connection. (Range: 0-8)

Command Mode

Privileged Exec

Command Usage

Specifying session identifier "0" will disconnect the console connection. Specifying any other identifiers for an active session will disconnect an SSH or Telnet connection.

Example

```
Console#disconnect 1
Console#
```

Related Commands

show ssh (1066)
show users (908)

show line

This command displays the terminal line's parameters.

Syntax

show line [**console** | **vty**]

console - Console terminal line.

vty - Virtual terminal for remote console access (i.e., Telnet).

Default Setting

Shows all lines

Command Mode

Normal Exec, Privileged Exec

Example

To show all lines, enter this command:

```
Console#show line
 Console Configuration:
  Password Threshold : 3 times
  Inactive Timeout   : Disabled
  Login Timeout      : Disabled
  Silent Time        : Disabled
  Baud Rate          : Auto
  Data Bits          : 8
  Parity             : None
  Stop Bits          : 1

 VTY Configuration:
  Password Threshold : 3 times
  Inactive Timeout   : 600 seconds
  Login Timeout      : 300 sec.
  Silent Time        : Disabled
Console#
```

Event Logging

This section describes commands used to configure event logging on the switch.

Table 68: Event Logging Commands

Command	Function	Mode
logging facility	Sets the facility type for remote logging of syslog messages	GC
logging history	Limits syslog messages saved to switch memory based on severity	GC
logging host	Adds a syslog server host IP address that will receive logging messages	GC
logging on	Controls logging of error messages	GC
logging trap	Limits syslog messages saved to a remote server based on severity	GC
clear log	Clears messages from the logging buffer	PE
show log	Displays log messages	PE
show logging	Displays the state of logging	PE

logging facility

This command sets the facility type for remote logging of syslog messages. Use the **no** form to return the type to the default.

SYNTAX

logging facility *type*

no logging facility

type - A number that indicates the facility used by the syslog server to dispatch log messages to an appropriate service. (Range: 16-23)

DEFAULT SETTING

23

COMMAND MODE

Global Configuration

COMMAND USAGE

The command specifies the facility type tag sent in syslog messages. (See RFC 3164.) This type has no effect on the kind of messages reported by the switch. However, it may be used by the syslog server to sort messages or to store messages in the corresponding database.

EXAMPLE

```
Console(config)#logging facility 19
Console(config)#
```

logging history

This command limits syslog messages saved to switch memory based on severity. The **no** form returns the logging of syslog messages to the default level.

SYNTAX

logging history {**flash** | **ram**} *level*

no logging history {**flash** | **ram**}

flash - Event history stored in flash memory (i.e., permanent memory).

ram - Event history stored in temporary RAM (i.e., memory flushed on power reset).

level - One of the levels listed below. Messages sent include the selected level down to level 0. (Range: 0-7)

Table 69: Logging Levels

Level	Severity Name	Description
7	debugging	Debugging messages
6	informational	Informational messages only
5	notifications	Normal but significant condition, such as cold start

Table 69: Logging Levels (Continued)

Level	Severity Name	Description
4	warnings	Warning conditions (e.g., return false, unexpected return)
3	errors	Error conditions (e.g., invalid input, default used)
2	critical	Critical conditions (e.g., memory allocation, or free memory error - resource exhausted)
1	alerts	Immediate action needed
0	emergencies	System unusable

DEFAULT SETTING

Flash: errors (level 3 - 0)
RAM: debugging (level 7 - 0)

COMMAND MODE

Global Configuration

COMMAND USAGE

The message level specified for flash memory must be a higher priority (i.e., numerically lower) than that specified for RAM.

EXAMPLE

```
Console(config)#logging history ram 0
Console(config)#
```

logging host

This command adds a syslog server host IP address that will receive logging messages. Use the **no** form to remove a syslog server host.

SYNTAX

[**no**] **logging host** *host-ip-address*

host-ip-address - The IPv4 or IPv6 address of a syslog server.

DEFAULT SETTING

None

COMMAND MODE

Global Configuration

COMMAND USAGE

- Use this command more than once to build up a list of host IP addresses.
- The maximum number of host IP addresses allowed is five.

EXAMPLE

```
Console(config)#logging host 10.1.0.3
Console(config)#
```

logging on

This command controls logging of error messages, sending debug or error messages to a logging process. The **no** form disables the logging process.

SYNTAX

[**no**] **logging on**

DEFAULT SETTING

None

COMMAND MODE

Global Configuration

COMMAND USAGE

The logging process controls error messages saved to switch memory or sent to remote syslog servers. You can use the logging history command to control the type of error messages that are stored in memory. You can use the logging trap command to control the type of error messages that are sent to specified syslog servers.

EXAMPLE

```
Console(config)#logging on
Console(config)#
```

RELATED COMMANDS

logging history (934)
logging trap (936)
clear log (937)

logging trap

This command enables the logging of system messages to a remote server, or limits the syslog messages saved to a remote server based on severity. Use this command without a specified level to enable remote logging. Use the **no** form to disable remote logging.

SYNTAX

logging trap [**level** *level*]

no logging trap [**level**]

level - One of the syslog severity levels listed in the table on page 934. Messages sent include the selected level through level 0.

DEFAULT SETTING

Disabled
Level 7

COMMAND MODE

Global Configuration

COMMAND USAGE

- Using this command with a specified level enables remote logging and sets the minimum severity level to be saved.
- Using this command without a specified level also enables remote logging, but restores the minimum severity level to the default.

EXAMPLE

```
Console(config)#logging trap 4
Console(config)#
```

clear log

This command clears messages from the log buffer.

SYNTAX

clear log [**flash** | **ram**]

flash - Event history stored in flash memory (i.e., permanent memory).

ram - Event history stored in temporary RAM (i.e., memory flushed on power reset).

DEFAULT SETTING

Flash and RAM

COMMAND MODE

Privileged Exec

EXAMPLE

```
Console#clear log
Console#
```

RELATED COMMANDS

show log (938)

show log

This command displays the log messages stored in local memory.

SYNTAX

show log {**flash** | **ram**}

flash - Event history stored in flash memory (i.e., permanent memory).

ram - Event history stored in temporary RAM (i.e., memory flushed on power reset).

DEFAULT SETTING

None

COMMAND MODE

Privileged Exec

COMMAND USAGE

- All log messages are retained in RAM and Flash after a warm restart (i.e., power is reset through the command interface).
- All log messages are retained in Flash and purged from RAM after a cold restart (i.e., power is turned off and then on through the power source).

EXAMPLE

The following example shows the event message stored in RAM.

```
Console#show log ram
[1] 00:01:30 2001-01-01
   "VLAN 1 link-up notification."
   level: 6, module: 5, function: 1, and event no.: 1
[0] 00:01:30 2001-01-01
   "Unit 1, Port  1 link-up notification."
   level: 6, module: 5, function: 1, and event no.: 1
Console#
```

show logging

This command displays the configuration settings for logging messages to local switch memory, to an SMTP event handler, or to a remote syslog server.

SYNTAX

show logging {**flash** | **ram** | **sendmail** | **trap**}

flash - Displays settings for storing event messages in flash memory (i.e., permanent memory).

ram - Displays settings for storing event messages in temporary RAM (i.e., memory flushed on power reset).

sendmail - Displays settings for the SMTP event handler (page 943).

trap - Displays settings for the trap function.

DEFAULT SETTING

None

COMMAND MODE

Privileged Exec

EXAMPLE

The following example shows that system logging is enabled, the message level for flash memory is "errors" (i.e., default level 3 - 0), and the message level for RAM is "debugging" (i.e., default level 7 - 0).

```
Console#show logging flash
Syslog logging:            Enabled
History logging in FLASH: level errors
Console#show logging ram
Syslog logging:            Enabled
History logging in RAM: level debugging
Console#
```

Table 70: show logging flash/ram - display description

Field	Description
Syslog logging	Shows if system logging has been enabled via the logging on command.
History logging in FLASH	The message level(s) reported based on the logging history command.
History logging in RAM	The message level(s) reported based on the logging history command.

The following example displays settings for the trap function.

```
Console#show logging trap
Remote Log Status            : Disabled
Remote Log Facility Type     : Local use 7
Remote Log Level Type        : Debugging messages
Remote Log Server IP Address : 0.0.0.0
Remote Log Server IP Address : 0.0.0.0
Remote Log Server IP Address : 0.0.0.0
Remote Log Server IP Address : 0.0.0.0
Remote Log Server IP Address : 0.0.0.0
Console#
```

Table 71: show logging trap - display description

Field	Description
Syslog logging	Shows if system logging has been enabled via the logging on command.
REMOTELOG status	Shows if remote logging has been enabled via the logging trap command.

Table 71: show logging trap - display description (Continued)

Field	Description
REMOTELOG facility type	The facility type for remote logging of syslog messages as specified in the logging facility command.
REMOTELOG level type	The severity threshold for syslog messages sent to a remote server as specified in the logging trap command.
REMOTELOG server IP address	The address of syslog servers as specified in the logging host command.

RELATED COMMANDS

show logging sendmail (943)

SMTP ALERTS

These commands configure SMTP event handling, and forwarding of alert messages to the specified SMTP servers and email recipients.

Table 72: Event Logging Commands

Command	Function	Mode
logging sendmail	Enables SMTP event handling	GC
logging sendmail host	SMTP servers to receive alert messages	GC
logging sendmail level	Severity threshold used to trigger alert messages	GC
logging sendmail destination-email	Email recipients of alert messages	GC
logging sendmail source-email	Email address used for “From” field of alert messages	GC
show logging sendmail	Displays SMTP event handler settings	NE, PE

logging sendmail

This command enables SMTP event handling. Use the **no** form to disable this function.

SYNTAX

[**no**] **logging sendmail**

DEFAULT SETTING

Enabled

COMMAND MODE

Global Configuration

EXAMPLE

```
Console(config)#logging sendmail
Console(config)#
```

logging sendmail host

This command specifies SMTP servers that will be sent alert messages. Use the **no** form to remove an SMTP server.

SYNTAX

[**no**] **logging sendmail host** *ip-address*

ip-address - IPv4 or IPv6 address of an SMTP server that will be sent alert messages for event handling.

DEFAULT SETTING

None

COMMAND MODE

Global Configuration

COMMAND USAGE

- You can specify up to three SMTP servers for event handing. However, you must enter a separate command to specify each server.
- To send email alerts, the switch first opens a connection, sends all the email alerts waiting in the queue one by one, and finally closes the connection.
- To open a connection, the switch first selects the server that successfully sent mail during the last connection, or the first server configured by this command. If it fails to send mail, the switch selects the next server in the list and tries to send mail again. If it still fails, the system will repeat the process at a periodic interval. (A trap will be triggered if the switch cannot successfully open a connection.)

EXAMPLE

```
Console(config)#logging sendmail host 192.168.1.19
Console(config)#
```

logging sendmail level

This command sets the severity threshold used to trigger alert messages. Use the **no** form to restore the default setting.

SYNTAX

logging sendmail level *level*

no logging sendmail level

level - One of the system message levels (page 934). Messages sent include the selected level down to level 0. (Range: 0-7; Default: 7)

DEFAULT SETTING

Level 7

COMMAND MODE

Global Configuration

COMMAND USAGE

The specified level indicates an event threshold. All events at this level or higher will be sent to the configured email recipients. (For example, using Level 7 will report all events from level 7 to level 0.)

EXAMPLE

This example will send email alerts for system errors from level 3 through 0.

```
Console(config)#logging sendmail level 3
Console(config)#
```

logging sendmail destination-email

This command specifies the email recipients of alert messages. Use the **no** form to remove a recipient.

SYNTAX

[**no**] **logging sendmail destination-email** *email-address*

email-address - The source email address used in alert messages. (Range: 1-41 characters)

DEFAULT SETTING

None

COMMAND MODE

Global Configuration

COMMAND USAGE

You can specify up to five recipients for alert messages. However, you must enter a separate command to specify each recipient.

EXAMPLE

```
Console(config)#logging sendmail destination-email ted@this-company.com
Console(config)#
```

logging sendmail source-email

This command sets the email address used for the “From” field in alert messages. Use the **no** form to restore the default value.

SYNTAX

logging sendmail source-email *email-address*

no logging sendmail source-email

email-address - The source email address used in alert messages. (Range: 1-41 characters)

DEFAULT SETTING

None

COMMAND MODE

Global Configuration

COMMAND USAGE

You may use an symbolic email address that identifies the switch, or the address of an administrator responsible for the switch.

EXAMPLE

```
Console(config)#logging sendmail source-email bill@this-company.com
Console(config)#
```

show logging sendmail

This command displays the settings for the SMTP event handler.

COMMAND MODE

Normal Exec, Privileged Exec

EXAMPLE

```
Console#show logging sendmail
SMTP servers
-----------------------------------------------
192.168.1.19

SMTP Minimum Severity Level: 7

SMTP destination email addresses
-----------------------------------------------
ted@this-company.com

SMTP Source Email Address: bill@this-company.com

SMTP Status: Enabled
Console#
```

TIME

The system clock can be dynamically set by polling a set of specified time servers (NTP or SNTP). Maintaining an accurate time on the switch enables the system log to record meaningful dates and times for event entries. If the clock is not set, the switch will only record the time from the factory default set at the last bootup.

Table 73: Time Commands

Command	Function	Mode
SNTP Commands		
sntp client	Accepts time from specified time servers	GC
sntp poll	Sets the interval at which the client polls for time	GC
sntp server	Specifies one or more time servers	GC
show sntp	Shows current SNTP configuration settings	NE, PE
NTP Commands		
ntp authenticate	Enables authentication for NTP traffic	GC
ntp authentication-key	Configures authentication keys	GC
ntp client	Enables the NTP client for time updates from specified servers	GC
ntp server	Specifies NTP servers to poll for time updates	GC
show ntp	Shows current NTP configuration settings	NE, PE
Manual Configuration Commands		
clock summer-time (date)	Configures summer time* for the switch's internal clock	GC
clock summer-time (predefined)	Configures summer time* for the switch's internal clock	GC
clock summer-time (recurring)	Configures summer time* for the switch's internal clock	GC
clock timezone	Sets the time zone for the switch's internal clock	GC
calendar set	Sets the system date and time	PE
show calendar	Displays the current date and time setting	NE, PE

* Daylight savings time.

SNTP Commands

sntp client

This command enables SNTP client requests for time synchronization from NTP or SNTP time servers specified with the sntp server command. Use the **no** form to disable SNTP client requests.

SYNTAX

[**no**] **sntp client**

DEFAULT SETTING

Disabled

COMMAND MODE

Global Configuration

COMMAND USAGE

- The time acquired from time servers is used to record accurate dates and times for log events. Without SNTP, the switch only records the time starting from the factory default set at the last bootup (i.e., 00:00:00, Jan. 1, 2001).
- This command enables client time requests to time servers specified via the sntp server command. It issues time synchronization requests based on the interval set via the sntp poll command.

EXAMPLE

```
Console(config)#sntp server 10.1.0.19
Console(config)#sntp poll 60
Console(config)#sntp client
Console(config)#end
Console#show sntp
Current Time   : Apr 29 13:53:45 2011
Poll Interval  : 60 seconds
Current Mode   : Unicast
SNTP Status    : Enabled
SNTP Server    : 10.1.0.19
Current Server : 137.92.140.80
Console#
```

RELATED COMMANDS

sntp server (946)
sntp poll (946)
show sntp (947)

sntp poll

This command sets the interval between sending time requests when the switch is set to SNTP client mode. Use the **no** form to restore to the default.

Syntax

sntp poll *seconds*

no sntp poll

seconds - Interval between time requests.
(Range: 16-16384 seconds)

Default Setting

16 seconds

Command Mode

Global Configuration

Example

```
Console(config)#sntp poll 60
Console#
```

Related Commands

sntp client (945)

sntp server

This command sets the IP address of the servers to which SNTP time requests are issued. Use the this command with no arguments to clear all time servers from the current list. Use the **no** form to clear all time servers from the current list, or to clear a specific server.

Syntax

sntp server [*ip1* [*ip2* [*ip3*]]]

no sntp server [*ip1* [*ip2* [*ip3*]]]

ip - IPv4 or IPv6 address of an time server (NTP or SNTP).
(Range: 1 - 3 addresses)

Default Setting

None

Command Mode

Global Configuration

Command Usage

This command specifies time servers from which the switch will poll for time updates when set to SNTP client mode. The client will poll the time servers in the order specified until a response is received. It issues time synchronization requests based on the interval set via the sntp poll command.

EXAMPLE

```
Console(config)#sntp server 10.1.0.19
Console#
```

RELATED COMMANDS

sntp client (945)
sntp poll (946)
show sntp (947)

show sntp

This command displays the current time and configuration settings for the SNTP client, and indicates whether or not the local time has been properly updated.

COMMAND MODE

Normal Exec, Privileged Exec

COMMAND USAGE

This command displays the current time, the poll interval used for sending time synchronization requests, and the current SNTP mode (i.e., unicast).

EXAMPLE

```
Console#show sntp
Current Time   : Nov  5 18:51:22 2006
Poll Interval  : 16 seconds
Current Mode   : Unicast
SNTP Status    : Enabled
SNTP Server    : 137.92.140.80 0.0.0.0 0.0.0.0
Current Server : 137.92.140.80
Console#
```

NTP Commands

ntp authenticate

This command enables authentication for NTP client-server communications. Use the **no** form to disable authentication.

SYNTAX

[**no**] **ntp authenticate**

DEFAULT SETTING

Disabled

COMMAND MODE

Global Configuration

COMMAND USAGE

You can enable NTP authentication to ensure that reliable updates are received from only authorized NTP servers. The authentication keys and their associated key number must be centrally managed and manually distributed to NTP servers and clients. The key numbers and key values must match on both the server and client.

EXAMPLE

```
Console(config)#ntp authenticate
Console(config)#
```

RELATED COMMANDS

ntp authentication-key (948)

ntp authentication-key

This command configures authentication keys and key numbers to use when NTP authentication is enabled. Use the **no** form of the command to clear a specific authentication key or all keys from the current list.

SYNTAX

ntp authentication-key *number* **md5** *key*

no ntp authentication-key [*number*]

number - The NTP authentication key ID number. (Range: 1-65535)

md5 - Specifies that authentication is provided by using the message digest algorithm 5.

key - An MD5 authentication key string. The key string can be up to 32 case-sensitive printable ASCII characters (no spaces).

DEFAULT SETTING

None

COMMAND MODE

Global Configuration

COMMAND USAGE

- The key number specifies a key value in the NTP authentication key list. Up to 255 keys can be configured on the switch. Re-enter this command for each server you want to configure.

- Note that NTP authentication key numbers and values must match on both the server and client.

- NTP authentication is optional. When enabled with the **ntp authenticate** command, you must also configure at least one key number using this command.

- Use the **no** form of this command without an argument to clear all authentication keys in the list.

EXAMPLE

```
Console(config)#ntp authentication-key 45 md5 thisiskey45
Console(config)#
```

RELATED COMMANDS

ntp authenticate (947)

ntp client

This command enables NTP client requests for time synchronization from NTP time servers specified with the **ntp servers** command. Use the **no** form to disable NTP client requests.

SYNTAX

[**no**] **ntp client**

DEFAULT SETTING

Disabled

COMMAND MODE

Global Configuration

COMMAND USAGE

- The SNTP and NTP clients cannot be enabled at the same time. First disable the SNTP client before using this command.
- The time acquired from time servers is used to record accurate dates and times for log events. Without NTP, the switch only records the time starting from the factory default set at the last bootup (i.e., 00:00:00, Jan. 1, 2001).
- This command enables client time requests to time servers specified via the **ntp servers** command. It issues time synchronization requests based on the interval set via the **ntp poll** command.

EXAMPLE

```
Console(config)#ntp client
Console(config)#
```

RELATED COMMANDS

sntp client (945)
ntp server (950)

ntp server

This command sets the IP addresses of the servers to which NTP time requests are issued. Use the **no** form of the command to clear a specific time server or all servers from the current list.

SYNTAX

ntp server *ip-address* [**key** *key-number*]

no ntp server [*ip-address*]

ip-address - IP address of an NTP time server.

key-number - The number of an authentication key to use in communications with the server. (Range: 1-65535)

DEFAULT SETTING

Version number: 3

COMMAND MODE

Global Configuration

COMMAND USAGE

- This command specifies time servers that the switch will poll for time updates when set to NTP client mode. It issues time synchronization requests based on the interval set with the **ntp poll** command. The client will poll all the time servers configured, the responses received are filtered and compared to determine the most reliable and accurate time update for the switch.

- You can configure up to 50 NTP servers on the switch. Re-enter this command for each server you want to configure.

- NTP authentication is optional. If enabled with the **ntp authenticate** command, you must also configure at least one key number using the **ntp authentication-key** command.

- Use the **no** form of this command without an argument to clear all configured servers in the list.

EXAMPLE

```
Console(config)#ntp server 192.168.3.20
Console(config)#ntp server 192.168.3.21
Console(config)#ntp server 192.168.5.23 key 19
Console(config)#
```

RELATED COMMANDS

ntp client (949)
show ntp (951)

show ntp

This command displays the current time and configuration settings for the NTP client, and indicates whether or not the local time has been properly updated.

COMMAND MODE

Normal Exec, Privileged Exec

COMMAND USAGE

This command displays the current time, the poll interval used for sending time synchronization requests, and the current NTP mode (i.e., unicast).

EXAMPLE

```
Console#show ntp
Current Time              : Apr 29 13:57:32 2011
Polling                   : 1024 seconds
Current Mode              : unicast
NTP Status                : Disabled
NTP Authenticate Status   : Enabled
Last Update NTP Server    : 0.0.0.0        Port: 0
Last Update Time          : Jan  1 00:00:00 1970 UTC
NTP Server 192.168.3.20 version 3
NTP Server 192.168.3.21 version 3
NTP Server 192.168.4.22 version 3 key 19
NTP Authentication Key 19 md5 42V68751663T6K11P2J307210R885
Console#
```

Manual Configuration Commands

clock summer-time (date)

This command sets the start, end, and offset times of summer time (daylight savings time) for the switch on a one-time basis. Use the **no** form to disable summer time.

SYNTAX

clock summer-time *name* **date** *b-date b-month b-year b-hour b-minute e-date e-month e-year e-hour e-minute* [*offset*]

no clock summer-time

name - Name of the time zone while summer time is in effect, usually an acronym. (Range: 1-30 characters)

b-date - Day of the month when summer time will begin. (Range: 1-31)

b-month - The month when summer time will begin. (Options: **january** | **february** | **march** | **april** | **may** | **june** | **july** | **august** | **september** | **october** | **november** | **december**)

b-year- The year summer time will begin.

b-hour - The hour summer time will begin. (Range: 0-23 hours)

b-minute - The minute summer time will begin. (Range: 0-59 minutes) *e-date* - Day of the month when summer time will end. (Range: 1-31)

e-month - The month when summer time will end. (Options: **january** | **february** | **march** | **april** | **may** | **june** | **july** | **august** | **september** | **october** | **november** | **december**)

e-year - The year summer time will end.

e-hour - The hour summer time will end. (Range: 0-23 hours)

e-minute - The minute summer time will end. (Range: 0-59 minutes)

offset - Summer time offset from the regular time zone, in minutes. (Range: 0-99 minutes)

Default Setting

Disabled

Command Mode

Global Configuration

Command Usage

- In some countries or regions, clocks are adjusted through the summer months so that afternoons have more daylight and mornings have less. This is known as Summer Time, or Daylight Savings Time (DST). Typically, clocks are adjusted forward one hour at the start of spring and then adjusted backward in autumn.

- This command sets the summer-time time zone relative to the currently configured time zone. To specify a time corresponding to your local time when summer time is in effect, you must indicate the number of minutes your summer-time time zone deviates from your regular time zone.

Example

```
Console(config)#clock summer-time DEST date april 1 2007 23 23 april 23 2007
  23 23 60
Console(config)#
```

Related Commands

show sntp (947)

clock summer-time (predefined)

This command configures the summer time (daylight savings time) status and settings for the switch using predefined configurations for several major regions in the world. Use the **no** form to disable summer time.

SYNTAX

clock summer-time *name* **predefined** [**australia** | **europe** | **new-zealand** | **usa**]

no clock summer-time

name - Name of the timezone while summer time is in effect, usually an acronym. (Range: 1-30 characters)

DEFAULT SETTING

Disabled

COMMAND MODE

Global Configuration

COMMAND USAGE

- In some countries or regions, clocks are adjusted through the summer months so that afternoons have more daylight and mornings have less. This is known as Summer Time, or Daylight Savings Time (DST). Typically, clocks are adjusted forward one hour at the start of spring and then adjusted backward in autumn.

- This command sets the summer-time time relative to the configured time zone. To specify the time corresponding to your local time when summer time is in effect, select the predefined summer-time time zone appropriate for your location, or manually configure summer time if these predefined configurations do not apply to your location (see clock summer-time (date) or clock summer-time (recurring).

Table 74: Predefined Summer-Time Parameters

Region	Start Time, Day, Week, & Month	End Time, Day, Week, & Month	Rel. Offset
Australia	00:00:00, Sunday, Week 5 of October	23:59:59, Sunday, Week 5 of March	60 min
Europe	00:00:00, Sunday, Week 5 of March	23:59:59, Sunday, Week 5 of October	60 min
New Zealand	00:00:00, Sunday, Week 1 of October	23:59:59, Sunday, Week 3 of March	60 min
USA	00:00:00, Sunday, Week 2 of March	23:59:59, Sunday, Week 1 of November	60 min

EXAMPLE

```
Console(config)#clock summer-time MESZ predefined europe
Console(config)#
```

RELATED COMMANDS

show sntp (947)

clock summer-time (recurring)

This command allows the user to manually configure the start, end, and offset times of summer time (daylight savings time) for the switch on a recurring basis. Use the **no** form to disable summer-time.

SYNTAX

clock summer-time *name* **recurring** *b-week b-day b-month b-hour b-minute e-week e-day e-month e-hour e-minute* [*offset*]

no clock summer-time

name - Name of the timezone while summer time is in effect, usually an acronym. (Range: 1-30 characters)

b-week - The week of the month when summer time will begin. (Range: 1-5)

b-day - The day of the week when summer time will begin. (Options: **sunday** | **monday** | **tuesday** | **wednesday** | **thursday** | **friday** | **saturday**)

b-month - The month when summer time will begin. (Options: **january** | **february** | **march** | **april** | **may** | **june** | **july** | **august** | **september** | **october** | **november** | **december**)

b-hour - The hour when summer time will begin. (Range: 0-23 hours)

b-minute - The minute when summer time will begin. (Range: 0-59 minutes)

e-week - The week of the month when summer time will end. (Range: 1-5)

e-day - The day of the week summer time will end. (Options: **sunday** | **monday** | **tuesday** | **wednesday** | **thursday** | **friday** | **saturday**)

e-month - The month when summer time will end. (Options: **january** | **february** | **march** | **april** | **may** | **june** | **july** | **august** | **september** | **october** | **november** | **december**)

e-hour - The hour when summer time will end. (Range: 0-23 hours)

e-minute - The minute when summer time will end. (Range: 0-59 minutes)

offset - Summer-time offset from the regular time zone, in minutes. (Range: 0-99 minutes)

DEFAULT SETTING

Disabled

COMMAND MODE

Global Configuration

COMMAND USAGE

- In some countries or regions, clocks are adjusted through the summer months so that afternoons have more daylight and mornings have less. This is known as Summer Time, or Daylight Savings Time (DST).

Typically, clocks are adjusted forward one hour at the start of spring and then adjusted backward in autumn.

- This command sets the summer-time time zone relative to the currently configured time zone. To display a time corresponding to your local time when summer time is in effect, you must indicate the number of minutes your summer-time time zone deviates from your regular time zone.

EXAMPLE

```
Console(config)#clock summer-time MESZ recurring 1 friday june 23 59 3
  saturday september 2 55 60
Console(config)#
```

RELATED COMMANDS

show sntp (947)

clock timezone

This command sets the time zone for the switch's internal clock.

SYNTAX

clock timezone *name* **hour** *hours* **minute** *minutes*
{**before-utc** | **after-utc**}

name - Name of timezone, usually an acronym. (Range: 1-30 characters)

hours - Number of hours before/after UTC. (Range: 0-12 hours before UTC, 0-13 hours after UTC)

minutes - 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

None

COMMAND MODE

Global Configuration

COMMAND USAGE

This command sets the local time zone relative to the Coordinated Universal Time (UTC, formerly Greenwich Mean Time or GMT), based on the earth's prime meridian, zero degrees longitude. To display a time corresponding to your local time, you must indicate the number of hours and minutes your time zone is east (before) or west (after) of UTC.

EXAMPLE

```
Console(config)#clock timezone Japan hours 8 minute 0 after-UTC
Console(config)#
```

RELATED COMMANDS

show sntp (947)

calendar set

This command sets the system clock. It may be used if there is no time server on your network, or if you have not configured the switch to receive signals from a time server.

SYNTAX

calendar set *hour min sec* {*day month year* | *month day year*}

hour - Hour in 24-hour format. (Range: 0 - 23)

min - Minute. (Range: 0 - 59)

sec - Second. (Range: 0 - 59)

day - Day of month. (Range: 1 - 31)

month - **january** | **february** | **march** | **april** | **may** | **june** | **july** | **august** | **september** | **october** | **november** | **december**

year - Year (4-digit). (Range: 2001 - 2100)

DEFAULT SETTING

None

COMMAND MODE

Privileged Exec

COMMAND USAGE

Note that when SNTP is enabled, the system clock cannot be manually configured.

EXAMPLE

This example shows how to set the system clock to 15:12:34, February 1st, 2011.

```
Console#calendar set 15:12:34 1 February 2011
Console#
```

show calendar

This command displays the system clock.

DEFAULT SETTING

None

COMMAND MODE

Normal Exec, Privileged Exec

EXAMPLE

```
Console#show calendar
 14:13:38 August 19 2011
Console#
```

TIME RANGE

This section describes the commands used to sets a time range for use by other functions, such as Access Control Lists.

Table 75: Time Range Commands

Command	Function	Mode
time-range	Specifies the name of a time range, and enters time range configuration mode	GC
absolute	Sets the time range for the execution of a command	TR
periodic	Sets the time range for the periodic execution of a command	TR
show time-range	Shows configured time ranges.	PE

time-range

This command specifies the name of a time range, and enters time range configuration mode. Use the **no** form to remove a previously specified time range.

SYNTAX

[**no**] **time-range** *name*

name - Name of the time range. (Range: 1-16 characters)

DEFAULT SETTING

None

COMMAND MODE

Global Configuration

COMMAND USAGE

This command sets a time range for use by other functions, such as Access Control Lists.

EXAMPLE

```
Console(config)#time-range r&d
Console(config-time-range)#
```

RELATED COMMANDS

Access Control Lists (1163)

absolute

This command sets the time range for the execution of a command. Use the **no** form to remove a previously specified time.

SYNTAX

absolute start *hour minute day month year*
[**end** *hour minutes day month year*]

absolute end *hour minutes day month year*

no absolute

hour - Hour in 24-hour format. (Range: 0-23)

minute - Minute. (Range: 0-59)

day - Day of month. (Range: 1-31)

month - **january** | **february** | **march** | **april** | **may** | **june** | **july** | **august** | **september** | **october** | **november** | **december**

year - Year (4-digit). (Range: 2009-2109)

DEFAULT SETTING

None

COMMAND MODE

Time Range Configuration

COMMAND USAGE

- If a time range is already configured, you must use the **no** form of this command to remove the current entry prior to configuring a new time range.
- If both an absolute rule and one or more periodic rules are configured for the same time range (i.e., named entry), that entry will only take effect if the current time is within the absolute time range and one of the periodic time ranges.

EXAMPLE

This example configures the time for the single occurrence of an event.

```
Console(config)#time-range r&d
Console(config-time-range)#absolute start 1 1 1 april 2009 end 2 1 1 april
  2009
Console(config-time-range)#
```

periodic

This command sets the time range for the periodic execution of a command. Use the **no** form to remove a previously specified time range.

SYNTAX

[**no**] **periodic** {**daily** | **friday** | **monday** | **saturday** | **sunday** | **thursday** | **tuesday** | **wednesday** | **weekdays** | **weekend**} *hour minute* to {**daily** | **friday** | **monday** | **saturday** | **sunday** | **thursday** | **tuesday** | **wednesday** | **weekdays** | **weekend** | *hour minute*}

daily - Daily

friday - Friday

monday - Monday

saturday - Saturday

sunday - Sunday

thursday - Thursday

tuesday - Tuesday

wednesday - Wednesday

weekdays - Weekdays

weekend - Weekends

hour - Hour in 24-hour format. (Range: 0-23)

minute - Minute. (Range: 0-59)

DEFAULT SETTING

None

COMMAND MODE

Time Range Configuration

COMMAND USAGE

- If a time range is already configured, you must use the **no** form of this command to remove the current entry prior to configuring a new time range.

- If both an absolute rule and one or more periodic rules are configured for the same time range (i.e., named entry), that entry will only take effect if the current time is within the absolute time range and one of the periodic time ranges.

EXAMPLE

This example configures a time range for the periodic occurrence of an event.

```
Console(config)#time-range sales
Console(config-time-range)#periodic daily 1 1 to 2 1
Console(config-time-range)#
```

show time-range

This command shows configured time ranges.

SYNTAX

show time-range [*name*]

name - Name of the time range. (Range: 1-30 characters)

DEFAULT SETTING

None

COMMAND MODE

Privileged Exec

EXAMPLE

```
Console#show time-range r&d
 Time-range r&d:
   absolute start 01:01 01 April 2009
   periodic    Daily 01:01 to    Daily 02:01
   periodic    Daily 02:01 to    Daily 03:01
Console#
```

PRECISION TIME PROTOCOL

Precision Time Protocol (PTP) provides high-precision time synchronization at an accuracy within the sub-microsecond range. PTP Version 2 (based on IEEE 1588-2002) is used to provide clock synchronization for measurement and control systems in a local area network.

Table 76: PTP Commands

Command	Function	Mode
ptp adjust	Adjusts the system time based information in received Sync messages	GC
ptp domain-number	Specifies the PTP clock synchronization domain to which the switch belongs	GC
ptp e-latency	Specifies the egress latency added to the timestamp	GC
ptp in-latency	Specifies the ingress latency added to the timestamp	GC
ptp mode	Sets the operating mode to boundary clock or transparent clock	GC
ptp priority1	Sets a preference level used in selecting the master clock	GC
ptp priority2	Sets a secondary preference level used in selecting the master clock	GC
ptp announce-receipt-timeout	Sets the transmit timeout for PTP announcement messages	IC
ptp delay-mechanism	Sets the delay measurement method in a boundary clock to use peer-to-peer or end-to-end mode	IC
ptp log-announce-interval	Sets the announce message transmit interval	IC

Table 76: PTP Commands (Continued)

Command	Function	Mode
ptp log-min-delay-request-interval	Sets the delay request message transmit interval	IC
ptp log-min-pdelay-request-interval	Sets the peer delay request message transmit interval	IC
ptp log-sync-interval	Sets the synchronization message transmit interval	IC
ptp port-enable	Enables PTP capability on a port	IC
ptp transport	Sets the message transport method to Ethernet, IPv4 UDP, or IPv6 UDP	IC
ptp port-release	Returns a port to PTP enabled state after having been disabled by a PTP management message	PE
show ptp configuration	Shows configuration settings	PE
show ptp foreign-master	Shows PTP announcements from neighbors	PE
show ptp information	Shows configured and protocol negotiated settings	PE

ptp adjust

This command adjusts the system time based information in received Sync messages. Use the **no** form to restore the default setting.

SYNTAX

[**no**] **ptp adjust**

DEFAULT SETTING

Disabled

COMMAND MODE

Global Configuration

COMMAND USAGE

- When this command is enabled, the switch will adjust the time of the local clock to match that of the master clock.

- When synchronization is enabled with this command, the switch will exchange PTP timing messages on the communication path to the master clock. By exchanging Sync, Follow_Up, Delay_Req, and Delay_Resp messages, the switch calculates the offset of the slave’s clock with respect to the master clock. It then adjusts the time reported in the received Sync message, ensuring that the offset from the master clock listed in the Current Data Set is now zero (as displayed by the show ptp information command).

EXAMPLE

```
Console(config)#ptp adjust
Console(config)#
```

ptp domain-number

This command specifies the PTP clock synchronization domain to which the switch belongs. Use the **no** form to restore the default setting.

SYNTAX

ptp domain-number *domain-number*

no ptp domain-number

domain-number – The PTP domain number. (Range: 0-255)

DEFAULT SETTING

0

COMMAND MODE

Global Configuration

COMMAND USAGE

- A domain is a set of clocks that synchronize to one another using PTP.
- Multiple independent PTP clocking domains can be configured on a single network, but a device can only belong to one domain.

EXAMPLE

```
Console(config)#ptp domain-number 1
Console(config)#
```

ptp e-latency

This command specifies the egress latency added to the timestamp. Use the **no** form to restore the default setting.

SYNTAX

ptp e-latency *latency*

no ptp e-latency

latency – The egress latency added to the actual timestamp. (Range: 0-1000000 nanoseconds; Default: 0 nanoseconds)

DEFAULT SETTING

0 nanoseconds

COMMAND MODE

Global Configuration

COMMAND USAGE

Failure to make this correction will result in a time offset between the slave and master clocks.

Example

```
Console(config)#ptp e-latency 10
Console(config)#
```

ptp in-latency

This command specifies the ingress latency added to the timestamp. Use the **no** form to restore the default setting.

Syntax

ptp in-latency *latency*

no ptp in-latency

latency – The ingress latency added the actual timestamp. (Range: 0-1000000 nanoseconds; Default: 0 nanoseconds)

Default Setting

0 nanoseconds

Command Mode

Global Configuration

Command Usage

Failure to make this correction will result in a time offset between the slave and master clocks.

Example

```
Console(config)#ptp in-latency 10
Console(config)#
```

ptp mode

This command sets the operating mode to boundary clock or transparent clock. Use the **no** form to restore the default setting.

Syntax

ptp mode {**boundary-clock** | **disable** |
transparent-clock {**end-to-end** | **peer-to-peer**}}

no ptp mode

boundary-clock – A boundary clock can have multiple network connections and can accurately bridge synchronization from one network segment to another.

disable – Disables PTP on the switch.

transparent-clock – A transparent clock modifies PTP messages as they pass through the switch, updating the time stamps to correct for time spent traversing the network.

end-to-end – This method measures the residence time required for PTP event messages to cross from the input port to the output port, and adjusts the time stamp to compensate for this delay. The value of the correction update and checksums are specific to each output port and message since the residence time are not necessarily the same for all paths through the switch or for successive messages crossing the same path.

peer-to-peer – This method measures the delay required for PTP event messages to cross the link from the peer port on the upstream device to the input port on the switch, as well as the residence time required for PTP event messages to cross from the input port to the output port, and adjusts the time stamp to compensate for both of these delay times.

DEFAULT SETTING

Disabled

COMMAND MODE

Global Configuration

COMMAND USAGE

- Setting the switch to boundary mode allows it to participate in the selection of the best master clock. If no better clock is detected, it will become the grandmaster clock within its PTP domain, and the parent clock to all connected devices. However, if the best master clock is found to be a another clock connected to the switch, the switch will synchronize to that clock as its child, and then acts as the parent clock to devices connected to other ports. After initial synchronization, the switch and connected devices exchange timing messages to correct for time skew caused by clock offsets and network delays.

- Setting the switch to end-to-end transparent mode makes it synchronize all ports with the grand master clock connected to the switch. The switch corrects PTP message time stamps for the delay incurred passing through it. This option causes less jitter and error accumulation than that incurred when using boundary mode.

- Setting the switch to peer-to-peer transparent mode differ with end-to-end transparent mode only in the way it corrects and handles PTP timing messages. Unlike the end-to-end clock, which corrects and forwards all PTP timing messages, the peer-to-peer clock only corrects and forwards Sync and Follow_Up messages. These messages are updated for both the residence time of the Sync message and link delay on the port receiving the Sync message.

- When PTP mode is set to boundary clock, the delay mechanism is determined by the ptp delay-mechanism command. When set to transparent clock, the delay mechanism is determined by message exchanges with other clocks in the PTP domain.

EXAMPLE

```
Console(config)#ptp mode boundary-clock
Console(config)#
```

ptp priority1

This command sets a preference level used in selecting the master clock. Use the **no** form to restore the default setting.

SYNTAX

ptp priority1 *priority-value*

no ptp priority1

priority-value – Slave devices use the priority1 value when selecting a master clock. (Range: 0-255)

DEFAULT SETTING

128

COMMAND MODE

Global Configuration

COMMAND USAGE

- Specify the priority1 preference level to override the default criteria for best master clock selection. Lower values take precedence.

- The best master clock algorithm (BMC), performs a distributed selection of the best candidate clock based on the following clock properties.
  - Priority – An administratively assigned precedence hint used by the BMC to help select a grandmaster for the PTP domain.
  - Class – An attribute defining the clock’s International Atomic Time (TAI) traceability.
  - Accuracy – An attribute defining the accuracy of the clock.
  - Variance – A clock's estimate of its stability based on observation of its performance against the PTP reference.
  - Quality – Clock quality based on expected timing deviation, technology used to implement the clock or location in a stratum schema.
  - Identifier – A universally unique numeric identifier for the clock. This is typically constructed based on a device's MAC address.

- PTP uses a hierarchical selection algorithm based on the following properties in the order indicated.
  - Priority 1
  - Class
  - Accuracy
  - Variance
  - Priority 2
  - Unique identifier (tie breaker)

EXAMPLE

```
Console(config)#ptp priority1 64
Console(config)#
```

ptp priority2

This command sets a secondary preference level used in selecting the master clock. Use the **no** form to restore the default setting.

SYNTAX

ptp priority2 *priority-value*

no ptp priority2

priority-value – Slave devices use the priority2 value when selecting a master clock. (Range: 0-255)

DEFAULT SETTING

128

COMMAND MODE

Global Configuration

COMMAND USAGE

The priority2 preference is only considered when it not possible to use priority1 and other clock attributes to select a best master clock.

EXAMPLE

```
Console(config)#ptp priority2 16
Console(config)#
```

ptp announce-receipt-timeout

This command sets the transmit timeout for PTP announcement messages. Use the **no** form to restore the default setting.

SYNTAX

ptp announce-receipt-timeout *timeout-value*

no ptp announce-receipt-timeout

timeout-value – The number of PTP announce message intervals which have to expire without the receipt of a announce message before the session times out. (Range: 2-10)

DEFAULT SETTING

3

COMMAND MODE

Interface Configuration (Ethernet, Port Channel)

EXAMPLE

```
Console(config)#ptp announce-receipt-timeout 10
Console(config)#
```

RELATED COMMANDS

ptp log-announce-interval (968)

ptp delay-mechanism

This command sets the delay measurement method for a boundary clock to peer-to-peer or end-to-end mode. Use the **no** form to restore the default setting.

SYNTAX

ptp delay-mechanism {**end-to-end** | **peer-to-peer**}

no ptp delay-mechanism

end-to-end – This method measures the residence time required for PTP event messages to cross from the input port to the output port, and adjusts the time stamp to compensate for this delay. The value of the correction update and checksums are specific to each output port and message since the residence time are not necessarily the same for all paths through the switch or for successive messages crossing the same path.

peer-to-peer – This method measures the delay required for PTP event messages to cross the link from the peer port on the upstream device to the input port on the switch, as well as the residence time required for PTP event messages to cross from the input port to the output port, and adjusts the time stamp to compensate for both of these delay times.

DEFAULT SETTING

peer-to-peer

COMMAND MODE

Interface Configuration (Ethernet, Port Channel)

COMMAND USAGE

- For more information, refer to the Command Usage section under the ptp mode command.

- When PTP mode is set to boundary clock, the delay mechanism is determined by the **ptp delay-mechanism** command. When PTP mode is set to transparent clock, the delay mechanism is determined by message exchanges with other clocks in the PTP domain.

EXAMPLE

```
Console(config)#interface ethernet 1/1
Console(config-if)#ptp delay-mechanism end-to-end
Console(config-if)#
```

ptp log-announce-interval

This command sets the announcement message transmit interval. Use the **no** form to restore the default setting.

SYNTAX

ptp log-announce-interval *interval-value*

no ptp log-announce-interval

interval-value – The interval for PTP announcement messages. (Range: 0-4 in log base 2)

DEFAULT SETTING

1 (2 seconds)

COMMAND MODE

Interface Configuration (Ethernet, Port Channel)

COMMAND USAGE

- The log base 2 settings equate to the following values:
  - 0 – 1 packet every second
  - 1 – 1 packet every 2 seconds
  - 2 – 1 packet every 4 seconds
  - 3 – 1 packet every 8 seconds
  - 4 – 1 packet every 16 seconds

- It may be necessary for the announcement interval to be different in networks which employ different communication technologies, such as wired or wireless. Systems where the announcement interval varies from region to region will still function correctly. However, regions with short intervals may experience more reconfiguration events while waiting for slower regions to select master clocks.

EXAMPLE

```
Console(config)#interface ethernet 1/1
Console(config-if)#ptp log-announce-interval 0
Console(config-if)#
```

RELATED COMMANDS

ptp announce-receipt-timeout (966)

ptp log-min-delay-request-interval

This command sets the delay request message transmit interval. Use the **no** form to restore the default setting.

SYNTAX

ptp log-min-delay-request-interval *interval-value*

no ptp log-min-delay-request-interval

interval-value – The minimum interval between delay request messages sent by a slave clock to a specific port on the master clock. (Range: 0-5 in log base 2)

DEFAULT SETTING

0 (1 second)

COMMAND MODE

Interface Configuration (Ethernet, Port Channel)

COMMAND USAGE

- The log base 2 settings equate to the following values:
  - 0 – 1 packet every second
  - 1 – 1 packet every 2 seconds
  - 2 – 1 packet every 4 seconds
  - 3 – 1 packet every 8 seconds
  - 4 – 1 packet every 16 seconds
  - 5 – 1 packet every 32 seconds
- This value is determined and advertised by a master clock based on its ability to process delay request message traffic.

EXAMPLE

```
Console(config)#interface ethernet 1/1
Console(config-if)#ptp log-min-delay-request-interval 1
Console(config-if)#
```

ptp log-min-pdelay-request-interval

This command sets the peer delay request message transmit interval. Use the **no** form to restore the default setting.

SYNTAX

ptp log-min-pdelay-request-interval *interval-value*

no ptp log-min-pdelay-request-interval

interval-value – The minimum interval between peer delay request messages used to measure the link delay between two clock ports implementing the peer-to-peer delay mechanism. (Range: 0-5 in log base 2)

DEFAULT SETTING

0 (1 second)

COMMAND MODE

Interface Configuration (Ethernet, Port Channel)

COMMAND USAGE

- The log base 2 settings equate to the following values:
  - 0 – 1 packet every second
  - 1 – 1 packet every 2 seconds
  - 2 – 1 packet every 4 seconds
  - 3 – 1 packet every 8 seconds
  - 4 – 1 packet every 16 seconds
  - 5 – 1 packet every 32 seconds
- This command is only applicable for interfaces which are set to use the peer-to-peer delay mechanism with the ptp delay-mechanism command.

EXAMPLE

```
Console(config)#interface ethernet 1/1
Console(config-if)#ptp log-min-pdelay-request-interval 1
Console(config-if)#
```

ptp log-sync-interval

This command sets the synchronization message transmit interval. Use the **no** form to restore the default setting.

SYNTAX

ptp log-sync-interval *interval-value*

no ptp log-sync-interval

interval-value – The minimum interval between (multicast) synchronization messages. (Range: -1 - 1 in log base 2)

DEFAULT SETTING

0 (1 second)

COMMAND MODE

Interface Configuration (Ethernet, Port Channel)

COMMAND USAGE

- The log base 2 settings equate to the following values:
  - - 1 – 1 packet every 1/2 second
  - 0 – 1 packet every second
  - 1 – 1 packet every 2 seconds

- Synchronization messages are used to synchronize clocks within the same PTP domain. A boundary or transparent clock in slave state will synchronize to its master in the synchronization hierarchy established by the best master clock algorithm.

EXAMPLE

```
Console(config)#interface ethernet 1/1
Console(config-if)#ptp log-sync-interval 1
Console(config-if)#
```

ptp port-enable

This command enables PTP capability on a port. Use the **no** form to restore the default setting.

SYNTAX

[**no**] **ptp port-enable**

DEFAULT SETTING

Disabled

COMMAND MODE

Interface Configuration (Ethernet, Port Channel)

COMMAND USAGE

PTP is not enabled on all supported interfaces by default. You must enable PTP on individual interfaces.

EXAMPLE

```
Console(config)#interface ethernet 1/1
Console(config-if)#ptp port-enable
Console(config-if)#
```

ptp transport

This command sets the message transport method to Ethernet, UDP over IPv4, or UDP over IPv6. Use the **no** form to restore the default setting.

SYNTAX

ptp transport {**ethernet** | **udp-ipv4** | **udp-ipv6**}

no ptp transport

ethernet – PTP messages are transmitted using Ethernet format.

udp-ipv4 – PTP messages are transmitted using UDP over IPv4.

udp-ipv6 – PTP messages are transmitted using UDP over IPv6.

DEFAULT SETTING

Ethernet

COMMAND MODE

Interface Configuration (Ethernet, Port Channel)

COMMAND USAGE

- When using Ethernet as the transport mechanism, PTP messages use Ethernet formatted packets with the 88F7 Ethertype. PTP messages use MAC addresses as specified below.

Table 77: Ethernet Multicast MAC Addresses

Message Types	Address (hex)
All except peer delay mechanism messages	01-1B-19-00-00-00
Peer delay mechanism messages	01-80-C2-00-00-0E

- When using UDP over IPv4 as a transport mechanism, the following UDP destination ports are reserved values assigned to PTP.

Table 78: UDP/IPv4 Destination Port Numbers

Message Types	UDP Port Number
Event message	319
Multicast general message	320
Unicast general message addressed to a clock	320

When using UDP over IPv4 as a transport mechanism, PTP messages use the multicast addresses as specified below.

Table 79: UDP/IPv4 Multicast Addresses

Message Types	Address
All except peer delay mechanism messages	224.0.1.129
Peer delay mechanism messages	224.0.0.107

- When using UDP over IPv6 as a transport mechanism, the following UDP destination ports are reserved values assigned to PTP.

Table 80: UDP/IPv6 Destination Port Numbers

Message Types	UDP Port Number
Event message	319
Multicast general message	320
Unicast general message addressed to a clock	320

When using UDP over IPv6 as a transport mechanism, PTP messages use the multicast addresses as specified below.

Table 81: UDP/IPv6 Multicast Addresses

Message Types	Address
All except peer delay mechanism messages	FF0X:0:0:0:0:0:0:183
Peer delay mechanism messages	FF02:0:0:0:0:0:0:6B

EXAMPLE

```
Console(config)#interface ethernet 1/1
Console(config-if)#ptp transport udp-ipv4
Console(config-if)#
```

ptp port-release

This command returns a port to PTP enabled state after having been disabled by a PTP management message.

SYNTAX

ptp port-release *interface*

interface

ethernet *unit/port*

unit - Unit identifier. (Range: 1)

port - Port number. (Range: 1-28)

port-channel *channel-id* (Range: 1-8)

COMMAND MODE

Privileged Exec

COMMAND MODE

Check the “Port State” field displayed by the show ptp information command to see if a port has been disabled by a PTP management message.

EXAMPLE

```
Console#ptp port-release ethernet 1/1
Console#
```

show ptp configuration

This command shows PTP configuration settings.

SYNTAX

show ptp configuration [*interface*]

interface

ethernet *unit*/*port-list*

unit - Stack unit. (Range: 1)

port-list - Physical port number or list of port numbers. Separate nonconsecutive port numbers with a comma and no spaces; or use a hyphen to designate a range of port numbers. (Range: 1-28)

port-channel *channel-id* (Range: 1-8)

COMMAND MODE

Privileged Exec

EXAMPLE

```
Console#show ptp configuration ethernet 1/1
 Ethernet                        : 1/1
 Delay Mechanism                 : Peer-to-Peer
 Transport                       : Ethernet
 Log Sync Interval               : 0
 Log Annouce Interval            : 1
 Announce Receipt Timeout        : 3
 Log Min Pdelay Req. Interval : 0
 Log Min Delay Req. Interval  : 0
Console(config-if)#
```

show ptp foreign-master

This command shows PTP announcements from neighbors.

SYNTAX

show ptp foreign-master *interface*

interface

ethernet *unit*/*port*

unit - Unit identifier. (Range: 1)

port - Port number. (Range: 1-28)

port-channel *channel-id* (Range: 1-8)

COMMAND MODE

Privileged Exec

EXAMPLE

```
Console#show ptp foreign-master ethernet 1/1
Port     Master Identity            Master Clock Quality   Pri1 Pri2 Valid Best
-------- -------------------------- ---------------------- ---- ---- ----- ----
Eth 1/ 1 00:00:22:00:13:23:00:00  2 C1: 251 Ac: 254 Va:-1     0    0 Yes   Yes
Pch 2    00:00:22:00:13:23:00:00  2 C1: 251 Ac: 254 Va:-1     0    0 No    No
Console(config-if)#
```

Table 82: show ptp foreign-mater - display description

Field	Description
Port	Interface through which this message was received.
Master Identity	A unique 8-octet array based on the IEEE EUI-64 assigned numbers, and the port number
Master Clock Quality	The reported clock quality components include: ◆ Cl – Clock class defines the clock's International Atomic Time (TAI) traceability. ◆ Ac – Clock accuracy defines the accuracy of the clock. ◆ Va – Clock variance defines the stability of the clock
Pri1	A preference level used in selecting the master clock
Pri2	A secondary preference level used in selecting the master clock
Valid	This record is used to calculate Best master clock
Best	This record is the best record of all foreign masters

show ptp information

This command shows configured and protocol negotiated settings.

SYNTAX

show ptp information [**boundary** [**current** | **default** | **parent** | **time-properties** | *interface*]| **transparent** [*interface*]]

boundary – Shows information for a boundary clock.

current – Shows information about the number of steps (clock hops) from the grand master, time offset from the grand master, and mean path delay from the grand master.

default – Shows default PTP settings.

parent – Shows information on the parent data set and grand master clock quality.

time-properties – Shows information about the time attributes.

transparent – Shows information for a transparent clock.

interface

ethernet *unit/port-list*

unit - Stack unit. (Range: 1)

port-list - Physical port number or list of port numbers. Separate nonconsecutive port numbers with a comma and no spaces; or use a hyphen to designate a range of port numbers. (Range: 1-28)

port-channel *channel-id* (Range: 1-8)

COMMAND MODE

Privileged Exec

EXAMPLE

This example shows PTP configuration settings, negotiated settings, and default values for a boundary clock.

```
Console#show ptp information boundary
This Device is GrandMaster clock

Default Data Set:
 Two Step Flag                : Yes
 Clock Identity               : 0x00000CFFFE00FDFD
 Number Ports                 : 2
 Clock Quality                :
  Clock Class                 : 248
  Clock Accuracy              : Unknown
  Offset Scaled Log Variance  : -4000
 Priority1                    : 128
 Priority2                    : 128
 Domain Number                : 0
 Slave Only                   : No

Current Data Set:
 Steps Removed      : 0
 Offset From Master : 0 sec. 0 nano sec.
 Mean Path Delay    : 0 sec. 0 nano sec.

Parent Data Set:
 Parent Identity
  Clock Identity                     : 0X00000CFFFE0000FD
  Port Number                        : 0
 Observed Offset Scaled Log Variance : 65535
 Observed Clock Phase Change Rate    : 2147483647
 Grandmaster Identity                : 0X00000CFFFE0000FD

 Grandmaster Clock Quality           :
  Clock Class                        : 248
  Clock Accuracy                     : Unknown
  Offset Scaled Log Variance         : -4000
 Grandmaster Priority1               : 128
 Grandmaster Priority2               : 128

Time Properties Data Set:
 Current UTC Offset       : 0
 Current UTC Offset Valid : No
 Leap59                   : No
 Leap61                   : No
 Time Traceable           : No
 Frequency Traceable      : No
 PTP Timescale            : Yes
 Time Source              : Internal Oscillator

Etherent 1/1 Port Data Set:
 Port Identity                 :
  Clock Identity               : 00000CFFFE0000FD
  Port Number                  : 1
 Boundary Clock                 :
  Port State                    : Master
  Log Min Delay Req. Interval   : 0
  Peer Mean Path Delay          : 0 sec. 0 nano sec.
  Announce Receipt Timeout      : 3
  Log Announce Interval         : 1
  Log Sync Interval             : 0
  Delay Mechanism               : Peer to Peer
  Log Min Pdelay Req. Interval  : 0
  Version Number                : 2
.
.
.
```

Table 83: show ptp information - display description for boundary clock

Field	Description
Default Data Set	
Two Step Flag	Shows if this device is a two-step clock. A two-step clock sends a time stamp in a Follow_Up message, while a one-step clock sends a time stamp in a Sync message.
Clock Identity	A unique 8-octet array based on the IEEE EUI-64 assigned numbers
Number Ports	Number of PTP ports on this device
Clock Quality	A set of attributes defining the clock’s relative quality
Clock Class	An attribute defining the clock’s International Atomic Time (TAI) traceability.
Clock Accuracy	An attribute defining the accuracy of the clock
Offset Scaled Log Variance	An attribute defining the stability of the clock
Priority1	A preference level used in selecting the master clock
Priority2	A secondary preference level used in selecting the master clock
Domain Number	PTP clock synchronization domain
Slave Only	Shows if this device is operating in slave-only mode. (This operation mode is not supported by this device.)
Current Data Set	
Steps Removed	Number of steps (clock hops) from the grand master
Offset From Master	Time offset from the grand master
Mean Path Delay	Mean path delay from the grand master
Parent Data Set	
Parent Identity	Parent identity information
Clock Identity	A unique 8-octet array based on the IEEE EUI-64 assigned numbers
Port Number	Port connected to the parent clock. (This attribute indicates a number from the sequence of ports supporting PTP, not a physical port number.)
Observed Offset Scaled Log Variance	The variance of the parent’s clock phase as measured by the local clock
Observed Clock Phase Change Rate	The variance of the parent’s clock phase change rate as measured by the slave clock

Table 83: show ptp information - display description for boundary clock

Field	Description
Grandmaster Identity	A unique 8-octet array based on the IEEE EUI-64 assigned numbers
Grandmaster Clock Quality	
Clock Class	An attribute defining the clock's International Atomic Time (TAI) traceability.
Clock Accuracy	An attribute defining the accuracy of the clock
Offset Scaled Log Variance	An attribute defining the stability of the clock
Grandmaster Priority1	A preference level used in selecting the grand master clock
Grandmaster Priority2	A secondary preference level used in selecting the grand master clock
Time Properties Data Set	
Current UTC Offset	Current offset between TAI (International Atomic Time) and UTC (Coordinated Universal Time)
Current UTC Offset Valid	Indicates if the current UTC offset is known to be correct
Leap59	Indicates if the last minute of the UTC day contains 59 seconds
Leap61	Indicates if the last minute of the UTC day contains 61 seconds
Time Traceable	Indicates if the time scale of value of the current UTC offset are traceable to a primary reference
Frequency Traceable	Indicates if the frequency determining the time scale is traceable to a primary reference
PTP Timescale	Indicates if the clock time scale of the grand master clock is PTP
Time Source	The source of time used by the grand master clock
Port Data Set	
Port Identity	Port identity information
Clock Identity	A unique 8-octet array based on the IEEE EUI-64 assigned numbers
Port Number	Port on the local switch
Boundary Clock	A clock at the domain boundary used to bridge synchronization from one network segment to another
Port State	Shows if device is in master or slave state
Log Min Delay Req. Interval	Delay request message transmit interval (log value)
Peer Mean Path Delay	Mean path delay between upstream peer and this device
Announce Receipt Timeout	Transmit timeout for PTP announcement messages
Log Announce Interval	Announcement message transmit interval (log value)
Log Sync Interval	Synchronization message transmit interval (log value)
Delay Mechanism	Time delay measurement method (end-to-end or peer-to-peer)
Log Min Pdelay Req. Interval	Peer delay request message transmit interval
Version Number	PTP version number (1 or 2)

This example shows PTP configuration settings, negotiated settings, and default values for a transparent clock.

```
Console#show ptp information transparent
Transparent Default Data Set:
 Clock Identify        : 0x00000CFFFE00FDFD
 Number Ports          : 40
 Delay Mechanism       : End to End
 Primary Domain Number : 0
Console#
```

Table 84: show ptp information - display description for transparent clock

Field	Description
Clock Identity	A unique 8-octet array based on the IEEE EUI-64 assigned numbers
Number Ports	Number of ports on this device
Delay Mechanism	Time delay measurement method (end-to-end or peer-to-peer)
Primary Domain Number	The primary PTP domain to which this device belongs. (This switch can only belong to one domain.)

SYNCHRONOUS ETHERNET

Synchronous Ethernet (SyncE) is used to synchronize specified links to the same frequency in order to transfer timing information to remote sites. SyncE ensures that all nodes have a clock source traceable to a Primary Reference Clock (PRC). The commands described in this section are used to enable SyncE on specified interfaces, automatically or manually select a clock source, receive Synchronization Status Messages (SSM) used to select the clock source based on the indicated quality level.

Table 85: Sync-E Commands

Command	Function	Mode
synce	Enables SyncE on all ports that support SyncE	GC
synce ethernet	Enables SyncE on a port that supports SyncE	GC
synce ethernet clock-source	Manually sets a port as a clock source or candidate clock source at the specified priority	GC
synce auto-clock-source-selecting	Automatically selects the clock-source port with the highest priority	GC
synce force-clock-source-selecting	Sets the local clock as the active clock source, or sets a port to be the active clock source	GC
synce ssm ethernet	Configures a port to receive/send SSM messages, and sets the priority used for this port in clock source port selection	GC
synce clk-src-ssm	Uses SSM to select the clock source according to the SSM quality level, priority and port number	GC
show synce	Shows SyncE status, selection mode, clock source status, and SSM status	PE

synce

This command enables SyncE on all ports that support SyncE. Use the **no** form to disable SyncE on all ports that support SyncE.

SYNTAX

[**no**] **synce**

DEFAULT SETTING

Disabled

COMMAND MODE

Global Configuration

COMMAND USAGE

- This command enables SyncE on ports 25-28. It does not configure any of these port to be the clock source.

- SyncE must be enabled on a port before the clock selection method can be set. Selection options include manual (synce ethernet clock-source), automatic (synce auto-clock-source-selecting), or forced (synce force-clock-source-selecting).

- SyncE frequency synchronization uses physical layer Ethernet to distribute timing information. A synchronization chain is formed by using a stratum 1 traceable source at one end which is then recovered at downstream PHYs and retransmitted down the chain. Every node in the chain must be capable of recovering and re-transmitting frequency synchronization signals.

- SyncE provides timing synchronization through the physical layer, while PTP (Precision Time Protocol) uses a higher level packet protocol which can result in processing delays. However, both SyncE and PTP may be used in combination to achieve a high level of frequency synchronization with a common defined time.

- SyncE delivers a high level of frequency accuracy, but cannot deliver time-of-day information (i.e., GMT). Conversely, PTP supports time-of-day information required by billing and service level agreements.

- SyncE implementation guidelines are covered by these standards:

Table 86: Synchronous Ethernet Standards

Standard	Description
ITU G.8264/Y.1364	Distribution of timing information through packet networks
ITU G.8261/Y.1361	Timing and synchronization aspects in packet networks
ITU G.8262/Y.1362	Timing characteristics of a synchronous Ethernet equipment slave clock

EXAMPLE

```
Console(config)#synce
Console(config)#exit
Console#show synce
SyncE Status:
Port        Status     Clock Source
---------  --------   ------------
Eth  1/25  Enabled    No
Eth  1/26  Enabled    No
Eth  1/27  Enabled    No
Eth  1/28  Enabled    No
...
```

synce ethernet

This command enables SyncE on a port that supports SyncE. Use the **no** form to disable SyncE on a port.

SYNTAX

[**no**] **synce ethernet** *unit***/***port*

unit - Unit identifier. (Range: 1)

port - Port number. (Range: 25-28)

DEFAULT SETTING

Disabled

COMMAND MODE

Global Configuration

COMMAND USAGE

- This command only enables SyncE on the specified port. It does not configure the port to be the clock source.
- This command can enable SyncE on trunk member but not on a trunk.
- SyncE can only be enabled on two ports at the same time.

EXAMPLE

```
Console(config)#syncd ethernet 1/28
Console(config)#
```

synce ethernet clock-source

This command manually sets a port as a clock source, or as a candidate clock source at the specified priority when using automatic clock source selection. Use the **no** form to remove a port as a clock source.

SYNTAX

synce ethernet *unit***/***port* **clock-source** [**priority** *priority*]

no synce synce ethernet *unit***/***port* **clock-source**

unit - Unit identifier. (Range: 1)

port - Port number. (Range: 1-28)

priority - The priority used by automatic clock source selection. (Range: 1-65535)

DEFAULT SETTING

Disabled

COMMAND MODE

Global Configuration

COMMAND USAGE

- This command can enable SyncE on trunk member but not on a trunk.
- If more than one port is configured as clock source port with this command, the first configured port will be set as the active clock source port.
- If an active clock source port is removed as the clock source, no active clock source port will exist until explicitly configured.
- When no active clock-source port exists, the switch's internal clock will be used as the clock source.
- If the priority of the clock-source port is not specified, the port ID of the clock-source port will be used as the priority for automatic clock source selection (see the synce auto-clock-source-selecting command).
- Lower priority values indicate higher precedence. If more than two clock-source ports have the same priority value, the clock source-port with the lowest port ID assumes higher precedence.
- If SyncE has locked the clock source and the clock source becomes invalid, SyncE will operate in holdover mode, switching over to the local reference clock if all available clock source signals fail. If SyncE has never locked the clock source and no valid clock source exists, SyncE will operate in free-run mode. If SyncE locked the clock source, SyncE will operate in locked mode.

  Note that a clock is said to be in holdover mode if it was previously synchronized to another clock (normally the primary reference clock) but is now free-running on its own internal oscillator, whose frequency is being adjusted using data acquired while it had been synchronized to the other clock.

EXAMPLE

```
Console(config)#synce ethernet 1/25 clock-source priority 1
Console(config)#
```

synce auto-clock-source-selecting

This command automatically selects the clock source port with the highest priority. Use the **no** form to disable automatic clock source selection.

SYNTAX

[**no**] **synce auto-clock-source-selecting** [**revertive-switching**]

auto-clock-source-selecting - Chooses the clock source port based on current clock-source port status and priority.

revertive-switching - The active clock source port will be changed when a clock source port with a higher priority becomes available.

DEFAULT SETTING

Disabled

COMMAND MODE

Global Configuration

COMMAND USAGE

- The switch can only be set to automatic clock source selection mode when the current selection mode is set to manual.

- At least one clock source port must be configured before switching to auto clock source selection mode. All ports configured as clock source port in manual mode will be kept after changing to auto mode.

- If more than one port is configured as clock source port, the port with a valid clock source signal and the highest priority is selected to be the active clock source port.

- If the configured priorities for two or more clock source ports are the same, it will choose the smaller numbered port to be the active clock source port.

- If revertive switching is enabled, the active clock source port will be changed when a clock source port with a higher priority becomes available. If revertive switching is disabled, the active clock source port will not be changed unless the current active clock source becomes invalid.

- If SyncE has locked the clock source and the clock source becomes invalid, SyncE will operate in holdover mode, switching over to the local reference clock if all available clock source signals fail. If SyncE has never locked the clock source and no valid clock source exists, SyncE will operate in free-run mode. If SyncE locked the clock source, SyncE will operate in locked mode.

EXAMPLE

```
Console(config)#synce auto-clock-source-selecting revertive-switching
Console(config)#end
Console#show synce
SyncE Status:
Port       Status    Clock Source
---------  --------  ------------
Eth  1/25  Enabled   Yes
Eth  1/26  Disabled  No
Eth  1/27  Disabled  No
Eth  1/28  Disabled  No
SyncE Clock Source Selection Mode: Auto
SyncE Active Clock Source Locked: No

SyncE Clock Source Status:
Port       Priority  Active Clock Source  Clock Status
---------  --------  -------------------  ------------
Eth  1/25        25          Yes                 Bad
...
```

synce force-clock-source-selecting

This command sets the local clock as the active clock source, or sets a port to be the active clock source.

SYNTAX

synce force-clock-source-selecting [**ethernet** *unit***/***port*]

unit - Unit identifier. (Range: 1)

port - Port number. (Range: 25-28)

DEFAULT SETTING

Disabled

COMMAND MODE

Global Configuration

COMMAND USAGE

- If this command is used without specifying a clock source port, and SyncE has not been enabled on any port, then the local clock is set to be the active clock source.
- If SyncE has been enabled on more than one port, the switch will choose the clock source port based on the current clock source port status and priority.
- A port can be forced to be the clock source port regardless of the clock's signal status.

EXAMPLE

```
Console(config)#sync ethernet 1/25 clock-source priority 1
Console(config)#
```

synce ssm ethernet

This command configures a port to receive/send Synchronization Status Messages (SSM), and sets the priority used for this port in clock source port selection. Use the **no** form to stop using clock selection based on SSM.

SYNTAX

synce ssm ethernet *unit***/***port* [**priority** *priority*]

no synce ssm [**ethernet** *unit***/***port*]

unit - Unit identifier. (Range: 1)

port - Port number. (Range: 25-28)

priority - The priority used for clock source selection. (Range: 1-65535)

DEFAULT SETTING

Disabled

COMMAND MODE

Global Configuration

COMMAND USAGE

General Information

- SSM provides a mechanism for downstream SyncE devices to synchronize with the Primary Reference Clock or the highest quality clock available. If an upstream network failure breaks this link, the synchronization function can take appropriate action based on SSM and pre-set priorities to select an alternate source of synchronization.
- This command only enables a port to send/receive SSM. It does not designate a specific port to be used as the clock source port. Use the synce clk-src-ssm command to configure the clock source.
- Only SSM will be extracted from the Ethernet Synchronization Message Channel (ESMC). No other information from the ESMC will be forwarded. SSM will be sent out of the specified port indicating the clock source selected by SSM or the manually configured clock source.
- The clock source port will not itself send out SSM. The other SSM-enabled ports will only send out SSM if received on the clock source port. SSM will be sent out of the other SSM-enabled ports once a second. If SSM has not been received on the clock source port after five seconds, the other SSM-enabled ports will stop sending SSM until a new clock source is selected.
- If SSM is disabled for a port, the priority level will be restored to the default value.

Mode Changes

- The switch can only be configured to use SSM for dynamic clock source selection when the current selection mode is set to Manual. The mode cannot be changed directly from SSM mode to Auto mode, or from Auto mode to SSM mode.

- If the switch is changed from SSM mode to Manual mode, and a port has been chosen as the active clock source in SSM mode, this port will still be the active clock source in Manual mode. If no clock source port has been selected in SSM mode, the local clock will be used as the active clock source.

- If the switch is changed from Manual mode to SSM mode, and a port has been chosen as the active clock source in Manual mode, this port will no longer be the active clock source. All clock source ports configured under Manual mode will be removed. The new active clock source is determined as described under the first item in this section.

- If the switch is changed from Manual mode to SSM mode using the **no** form of this command, and a port has been chosen as the active clock source in Auto mode, this port will be the active clock source in Manual Mode. If there is no active clock source in Auto mode, the local clock will be used as clock source in Manual mode. All ports configured as clock source ports under Auto mode will be kept after changing to Manual mode.

Link State Changes

- If an SSM-enabled port links up, the new active clock source is determined as described under the first item in this section.

- If SSM-chose clock source port goes down, the switch will choose the next clock source port as described under the first item in this section. If no other port can be used as the clock source port, the local clock will be used as the active clock source.

Joining a Trunk

- If an SSM-enabled port is added to a trunk, and the trunk is not operating at 1Gbps (full duplex), this port will no longer process SSM, and cannot be used a clock source port.

EXAMPLE

```
Console(config)#synce ssm ethernet 1/25
Console(config)#synce ssm ethernet 1/26
Console(config)#synce ssm ethernet 1/27
Console(config)#synce ssm ethernet 1/28
Console(config)#
```

synce clk-src-ssm

This command uses SSM to select the clock source according to the SSM quality level, priority and port number. Use the no form to disable this function.

SYNTAX

[**no**] **synce clk-src-ssm**

DEFAULT SETTING

Disabled

COMMAND MODE

Global Configuration

COMMAND USAGE

- Use this command to configure the clock source according to the SSM Quality Level (QL), port priority (as defined under the synce ssm ethernet command), and port number.

  If the SSM QL received on more than one port is the same, the clock source port is selected according to priority.

  If SSM QL and priority are the same on more than one port, the lower port number be chosen as the clock source port.

- If the clock source port has been manually configured (i.e., the active clock source is locked), SSM clock source selection will not function.

EXAMPLE

```
Console(config)#synce ssm ethernet 1/25
Console(config)#synce ssm ethernet 1/26
Console(config)#synce ssm ethernet 1/27
Console(config)#synce ssm ethernet 1/28
Console(config)#
```

show synce

This command shows SyncE status, selection mode, clock source status, and SSM status.

COMMAND MODE

Privileged Exec

EXAMPLE

```
Console#show synce
SyncE Status:
Port       Status    Clock Source
---------  --------  ------------
Eth  1/25  Enabled   No
Eth  1/26  Enabled   No
Eth  1/27  Enabled   No
Eth  1/28  Enabled   No
SyncE Clock Source Selection Mode: SSM
SyncE Active Clock Source Locked: No

SyncE Clock Source Status:
Port       Priority  Active Clock Source  Clock Status
---------  --------  -------------------  ------------
Eth  1/25         1          Yes               Good
Eth  1/26         2          No                Bad

SyncE SSM Status:
Port      Status   Pri Tx SSM  Rx SSM
--------- -------- --- ------- -------
Eth  1/25 Enabled    0 QL_NONE QL_EEC1
Eth  1/26 Enabled    0 QL-DNU  QL_EEC1
Eth  1/27 Enabled    0 QL_NONE QL_NONE
Eth  1/28 Enabled    0 QL_NONE QL_NONE
```

Table 87: show sync - display description for sync

Field	Description
SyncE Status	
Port	Port identifier
Status	Shows if SyncE is enabled or disabled
Clock Source	Shows if port is configured as a clock source candidate
SyncE Clock Source Selection Mode	Shows the clock source selection method: ◆ Manual – Manual mode (see synce or synce ethernet command) ◆ Auto – Automatic mode (see synce auto-clock-source-selecting command) ◆ SSM – Selection based on SSM messages (see synce clk-src-ssm command)
SyncE Active Clock Source Locked	Shows if clock source port is unlocked, or locked by manual or forced mode configuration
SyncE Clock Source Status	
Port	Port identifier
Priority	The selection priority determined by the manual configuration or default setting
Active Clock Source	Shows if port is currently operating as the port actively connected to the clock source
Clock Status	Shows if the clock signal is valid or not
SyncE SSM Status	
Port	Port identifier
Status	Shows if reception/transmission of SSM is enabled or disabled
Priority	The selection priority determined by the manual configuration or default setting
Tx SSM	Shows transmitted Quality Level message type: ◆ QL-NONE: This port is not transmitting SSM or timeout information ◆ QL-EEC1: Transmitting QL-EEC1* messages ◆ QL-EEC2: Transmitting QL-EEC2* messages
Rx SSM	Shows received Quality Level message type: ◆ QL-NONE: This port is not receiving SSM or timeout information ◆ QL-DNU: This port is receiving SSM code but has not been chosen as the clock source port ◆ QL-EEC1: Receiving QL-EEC1* messages ◆ QL-EEC2: Receiving QL-EEC2* messages

* The performance characteristics of the Phase Lock Loops (PLL) used to receive and re-transmit frequency synchronization signals in a SyncE chain are governed the ITU-T G.8262 standard. It defines two possible PLL performance options: Ethernet Equipment Clock (EEC) Option 1 and 2. EEC Option 1 is based on the 2.048 kpbs hierarchy governed by G.813 Option 1 which is used in Europe and Asia. EEC Option 2 is based on the 1.544 kpbs hierarchy governed by G.812 Type IV or Stratum 3 which is predominantly used in North America.

SWITCH CLUSTERING

Switch Clustering is a method of grouping switches together to enable centralized management through a single unit. Switches that support clustering can be grouped together regardless of physical location or switch type, as long as they are connected to the same local network.

Table 88: Switch Cluster Commands

Command	Function	Mode
cluster	Configures clustering on the switch	GC
cluster commander	Configures the switch as a cluster Commander	GC
cluster ip-pool	Sets the cluster IP address pool for Members	GC
cluster member	Sets Candidate switches as cluster members	GC
rcommand	Provides configuration access to Member switches	PE
show cluster	Displays the switch clustering status	PE
show cluster members	Displays current cluster Members	PE
show cluster candidates	Displays current cluster Candidates in the network	PE

Using Switch Clustering

- A switch cluster has a primary unit called the “Commander” which is used to manage all other “Member” switches in the cluster. The management station can use either Telnet or the web interface to communicate directly with the Commander through its IP address, and then use the Commander to manage the Member switches through the cluster’s “internal” IP addresses.
- Clustered switches must be in the same Ethernet broadcast domain. In other words, clustering only functions for switches which can pass information between the Commander and potential Candidates or active Members through VLAN 4093.
- Once a switch has been configured to be a cluster Commander, it automatically discovers other cluster-enabled switches in the network. These “Candidate” switches only become cluster Members when manually selected by the administrator through the management station.

NOTE: Cluster Member switches can be managed either through a Telnet connection to the Commander, or through a web management connection to the Commander. When using a console connection, from the Commander CLI prompt, use the rcommand to connect to the Member switch.

cluster

This command enables clustering on the switch. Use the **no** form to disable clustering.

SYNTAX

[**no**] **cluster**

DEFAULT SETTING

Disabled

COMMAND MODE

Global Configuration

COMMAND USAGE

- To create a switch cluster, first be sure that clustering is enabled on the switch (the default is enabled), then set the switch as a Cluster Commander. Set a Cluster IP Pool that does not conflict with any other IP subnets in the network. Cluster IP addresses are assigned to switches when they become Members and are used for communication between Member switches and the Commander.
- Switch clusters are limited to the same Ethernet broadcast domain.
- There can be up to 100 candidates and 16 member switches in one cluster.
- A switch can only be a Member of one cluster.
- Configured switch clusters are maintained across power resets and network changes.

EXAMPLE

```
Console(config)#cluster
Console(config)#
```

cluster commander

This command enables the switch as a cluster Commander. Use the **no** form to disable the switch as cluster Commander.

SYNTAX

[**no**] **cluster commander**

DEFAULT SETTING

Disabled

COMMAND MODE

Global Configuration

COMMAND USAGE

- Once a switch has been configured to be a cluster Commander, it automatically discovers other cluster-enabled switches in the network. These "Candidate" switches only become cluster Members when manually selected by the administrator through the management station.

- Cluster Member switches can be managed through a Telnet connection to the Commander. From the Commander CLI prompt, use the rcommand id command to connect to the Member switch.

EXAMPLE

```
Console(config)#cluster commander
Console(config)#
```

cluster ip-pool

This command sets the cluster IP address pool. Use the **no** form to reset to the default address.

SYNTAX

cluster ip-pool *ip-address*

no cluster ip-pool

ip-address - The base IP address for IP addresses assigned to cluster Members. The IP address must start 10.x.x.x.

DEFAULT SETTING

10.254.254.1

COMMAND MODE

Global Configuration

COMMAND USAGE

- An "internal" IP address pool is used to assign IP addresses to Member switches in the cluster. Internal cluster IP addresses are in the form 10.*x.x.member-ID*. Only the base IP address of the pool needs to be set since Member IDs can only be between 1 and 36.

- Set a Cluster IP Pool that does not conflict with addresses in the network IP subnet. Cluster IP addresses are assigned to switches when they become Members and are used for communication between Member switches and the Commander.

- You cannot change the cluster IP pool when the switch is currently in Commander mode. Commander mode must first be disabled.

EXAMPLE

```
Console(config)#cluster ip-pool 10.2.3.4
Console(config)#
```

cluster member

This command configures a Candidate switch as a cluster Member. Use the **no** form to remove a Member switch from the cluster.

SYNTAX

cluster member mac-address *mac-address* **id** *member-id*

no cluster member id *member-id*

mac-address - The MAC address of the Candidate switch.

member-id - The ID number to assign to the Member switch. (Range: 1-16)

DEFAULT SETTING

No Members

COMMAND MODE

Global Configuration

COMMAND USAGE

- The maximum number of cluster Members is 16.
- The maximum number of cluster Candidates is 100.

EXAMPLE

```
Console(config)#cluster member mac-address 00-12-34-56-78-9a id 5
Console(config)#
```

rcommand

This command provides access to a cluster Member CLI for configuration.

SYNTAX

rcommand id *member-id*

member-id - The ID number of the Member switch. (Range: 1-16)

COMMAND MODE

Privileged Exec

COMMAND USAGE

- This command only operates through a Telnet connection to the Commander switch. Managing cluster Members using the local console CLI on the Commander is not supported.
- There is no need to enter the username and password for access to the Member switch CLI.

EXAMPLE

```
Console#rcommand id 1

      CLI session with the ECS4660-28F is opened.
      To end the CLI session, enter [Exit].

Vty-0#
```

show cluster

This command shows the switch clustering configuration.

COMMAND MODE

Privileged Exec

EXAMPLE

```
Console#show cluster
Role                    : commander
Interval Heartbeat      : 30
Heartbeat Loss Count : 3 seconds
Number of Members       : 1
Number of Candidates : 2
Console#
```

show cluster members

This command shows the current switch cluster members.

COMMAND MODE

Privileged Exec

EXAMPLE

```
Console#show cluster members
Cluster Members:
ID          : 1
Role        : Active member
IP Address  : 10.254.254.2
MAC Address : 00-E0-0C-00-00-FE
Description : ECS4660-28F
Console#
```

show cluster candidates

This command shows the discovered Candidate switches in the network.

COMMAND MODE

Privileged Exec

EXAMPLE

```
Console#show cluster candidates
Cluster Candidates:
Role            MAC Address       Description
--------------- ----------------- ----------------------------------------
Active member   00-E0-0C-00-00-FE ECS4660-28F
CANDIDATE       00-12-CF-0B-47-A0 ECS4660-28F
Console#
```

25 SNMP Commands

SNMP commands control access to this switch from management stations using the Simple Network Management Protocol (SNMP), as well as the error types sent to trap managers.

SNMP Version 3 also provides security features that cover message integrity, authentication, and encryption; as well as controlling user access to specific areas of the MIB tree. To use SNMPv3, first set an SNMP engine ID (or accept the default), specify read and write access views for the MIB tree, configure SNMP user groups with the required security model (i.e., SNMP v1, v2c or v3) and security level (i.e., authentication and privacy), and then assign SNMP users to these groups, along with their specific authentication and privacy passwords.

Table 89: SNMP Commands

Command	Function	Mode
General SNMP Commands		
snmp-server	Enables the SNMP agent	GC
snmp-server community	Sets up the community access string to permit access to SNMP commands	GC
snmp-server contact	Sets the system contact string	GC
snmp-server location	Sets the system location string	GC
show snmp	Displays the status of SNMP communications	NE, PE
SNMP Target Host Commands		
snmp-server enable traps	Enables the device to send SNMP traps (i.e., SNMP notifications)	GC
snmp-server host	Specifies the recipient of an SNMP notification operation	GC
snmp-server enable port-traps mac-notification	Enables the device to send SNMP traps (i.e., SNMP notifications) when a dynamic MAC address is added or removed	IC
show snmp-server enable port-traps	Shows if SNMP traps are enabled or disabled for the specified interfaces	PE
SNMPv3 Commands		
snmp-server engine-id	Sets the SNMP engine ID	GC
snmp-server group	Adds an SNMP group, mapping users to views	GC
snmp-server user	Adds a user to an SNMP group	GC
snmp-server view	Adds an SNMP view	GC
show snmp engine-id	Shows the SNMP engine ID	PE
show snmp group	Shows the SNMP groups	PE
show snmp user	Shows the SNMP users	PE

Table 89: SNMP Commands (Continued)

Command	Function	Mode
show snmp view	Shows the SNMP views	PE
Notification Log Commands		
nlm	Enables the specified notification log	GC
snmp-server notify-filter	Creates a notification log and specifies the target host	GC
show nlm oper-status	Shows operation status of configured notification logs	PE
show snmp notify-filter	Displays the configured notification logs	PE
ATC Trap Commands		
snmp-server enable port-traps atc broadcast-alarm-clear	Sends a trap when broadcast traffic falls beneath the lower threshold after a storm control response has been triggered	IC (Port)
snmp-server enable port-traps atc broadcast-alarm-fire	Sends a trap when broadcast traffic exceeds the upper threshold for automatic storm control	IC (Port)
snmp-server enable port-traps atc broadcast-control-apply	Sends a trap when broadcast traffic exceeds the upper threshold for automatic storm control and the apply timer expires	IC (Port)
snmp-server enable port-traps atc broadcast-control-release	Sends a trap when broadcast traffic falls beneath the lower threshold after a storm control response has been triggered and the release timer expires	IC (Port)
snmp-server enable port-traps atc multicast-alarm-clear	Sends a trap when multicast traffic falls beneath the lower threshold after a storm control response has been triggered	IC (Port)
snmp-server enable port-traps atc multicast-alarm-fire	Sends a trap when multicast traffic exceeds the upper threshold for automatic storm control	IC (Port)
snmp-server enable port-traps atc multicast-control-apply	Sends a trap when multicast traffic exceeds the upper threshold for automatic storm control and the apply timer expires	IC (Port)
Connectivity Fault Management Trap Commands		
snmp-server enable traps ethernet cfm cc	Enables SNMP traps for CFM continuity check events	GC
snmp-server enable traps ethernet cfm crosscheck	Enables SNMP traps for CFM continuity check events, in relation to the cross-check operations between statically configured MEPs and those learned via continuity check messages	GC
snmp-server enable port-traps atc multicast-control-release	Sends a trap when multicast traffic falls beneath the lower threshold after a storm control response has been triggered and the release timer expires	IC (Port)
Transceiver Power Threshold Trap Commands		
transceiver-threshold current	Sends a trap when the transceiver current falls outside the specified thresholds	IC (Port)
transceiver-threshold rx-power	Sends a trap when the power level of the received signal falls outside the specified thresholds	IC (Port)
transceiver-threshold temperature	Sends a trap when the transceiver temperature falls outside the specified thresholds	IC (Port)
transceiver-threshold tx-power	Sends a trap when the power level of the transmitted signal power outside the specified thresholds	IC (Port)
transceiver-threshold voltage	Sends a trap when the transceiver voltage falls outside the specified thresholds	IC (Port)

Table 89: SNMP Commands (Continued)

Command	Function	Mode
Additional Trap Commands		
memory	Sets the rising and falling threshold for the memory utilization alarm	GC
process cpu	Sets the rising and falling threshold for the CPU utilization alarm	GC
show memory	Shows memory utilization parameters	PE
show process cpu	Shows CPU utilization parameters	PE

General SNMP Commands

snmp-server

This command enables the SNMPv3 engine and services for all management clients (i.e., versions 1, 2c, 3). Use the **no** form to disable the server.

SYNTAX

[**no**] **snmp-server**

DEFAULT SETTING

Enabled

COMMAND MODE

Global Configuration

EXAMPLE

```
Console(config)#snmp-server
Console(config)#
```

snmp-server community

This command defines community access strings used to authorize management access by clients using SNMP v1 or v2c. Use the **no** form to remove the specified community string.

SYNTAX

snmp-server community *string* [**ro** | **rw**]

no snmp-server community *string*

string - Community string that acts like a password and permits access to the SNMP protocol. (Maximum length: 32 characters, case sensitive; Maximum number of strings: 5)

ro - Specifies read-only access. Authorized management stations are only able to retrieve MIB objects.

rw - Specifies read/write access. Authorized management stations are able to both retrieve and modify MIB objects.

DEFAULT SETTING

- public - Read-only access. Authorized management stations are only able to retrieve MIB objects.
- private - Read/write access. Authorized management stations are able to both retrieve and modify MIB objects.

COMMAND MODE

Global Configuration

EXAMPLE

```
Console(config)#snmp-server community alpha rw
Console(config)#
```

snmp-server contact

This command sets the system contact string. Use the **no** form to remove the system contact information.

SYNTAX

snmp-server contact *string*

no snmp-server contact

string - String that describes the system contact information. (Maximum length: 255 characters)

DEFAULT SETTING

None

COMMAND MODE

Global Configuration

EXAMPLE

```
Console(config)#snmp-server contact Paul
Console(config)#
```

RELATED COMMANDS

snmp-server location (998)

snmp-server location

This command sets the system location string. Use the **no** form to remove the location string.

SYNTAX

snmp-server location *text*

no snmp-server location

text - String that describes the system location. (Maximum length: 255 characters)

DEFAULT SETTING

None

COMMAND MODE

Global Configuration

EXAMPLE

```
Console(config)#snmp-server location WC-19
Console(config)#
```

RELATED COMMANDS

snmp-server contact (998)

show snmp

This command can be used to check the status of SNMP communications.

DEFAULT SETTING

None

COMMAND MODE

Normal Exec, Privileged Exec

COMMAND USAGE

This command provides information on the community access strings, counter information for SNMP input and output protocol data units, and whether or not SNMP logging has been enabled with the **snmp-server enable traps** command.

EXAMPLE

```
Console#show snmp

SNMP Agent : Enabled

SNMP Traps :
 Authentication : Enabled
 Link-up-down   : Enabled
 MAC-notification : Disabled
 MAC-notification interval : 1 second(s)

SNMP Communities :
   1. public, and the access level is read-only
   2. private, and the access level is read/write

0 SNMP packets input
    0 Bad SNMP version errors
    0 Unknown community name
    0 Illegal operation for community name supplied
    0 Encoding errors
    0 Number of requested variables
    0 Number of altered variables
    0 Get-request PDUs
    0 Get-next PDUs
    0 Set-request PDUs
```

```
0 SNMP packets output
    0 Too big errors
    0 No such name errors
    0 Bad values errors
    0 General errors
    0 Response PDUs
    0 Trap PDUs

SNMP Logging: Disabled
Console#
```

SNMP Target Host Commands

snmp-server enable traps

This command enables this device to send Simple Network Management Protocol traps or informs (i.e., SNMP notifications). Use the **no** form to disable SNMP notifications.

SYNTAX

[**no**] **snmp-server enable traps** [**authentication** | **link-up-down** | **ethernet cfm** | **mac-notification** [**interval** *seconds*]]

authentication - Keyword to issue authentication failure notifications.

link-up-down - Keyword to issue link-up or link-down notifications.

ethernet cfm - Connectivity Fault Management traps. For more information on these traps, see "CFM Commands" on page 1561.

mac-notification - Keyword to issue trap when a dynamic MAC address is added or removed.

interval - Specifies the interval between issuing two consecutive traps. (Range: 0-3600 seconds; Default: 1 second)

DEFAULT SETTING

Issue authentication and link-up-down traps.
Other traps are disabled.

COMMAND MODE

Global Configuration

COMMAND USAGE

- If you do not enter an **snmp-server enable traps** command, no notifications controlled by this command are sent. In order to configure this device to send SNMP notifications, you must enter at least one **snmp-server enable traps** command. If you enter the command with no keywords, both authentication and link-up-down notifications are enabled. If you enter the command with a keyword, only the notification type related to that keyword is enabled.

- The **snmp-server enable traps** command is used in conjunction with the snmp-server host command. Use the snmp-server host command to specify which host or hosts receive SNMP notifications. In order to send notifications, you must configure at least one snmp-server host command.

- The authentication, link-up, and link-down traps are legacy notifications, and therefore when used for SNMP Version 3 hosts, they must be enabled in conjunction with the corresponding entries in the Notify View assigned by the snmp-server group command.

EXAMPLE

```
Console(config)#snmp-server enable traps link-up-down
Console(config)#
```

RELATED COMMANDS

snmp-server host (1001)

snmp-server host

This command specifies the recipient of a Simple Network Management Protocol notification operation. Use the **no** form to remove the specified host.

SYNTAX

snmp-server host *host-addr* [**inform** [**retry** *retries* |
timeout *seconds*]] *community-string*
[**version** {**1** | **2c** | **3** {**auth** | **noauth** | **priv**} [**udp-port** *port*]}

no snmp-server host *host-addr*

host-addr - IPv4 or IPv6 address of the host (targeted recipient). (Maximum host addresses: 5 trap destination IP address entries)

inform - Notifications are sent as inform messages. Note that this option is only available for version 2c and 3 hosts. (Default: traps are used)

retries - The maximum number of times to resend an inform message if the recipient does not acknowledge receipt. (Range: 0-255; Default: 3)

seconds - The number of seconds to wait for an acknowledgment before resending an inform message. (Range: 0-2147483647 centiseconds; Default: 1500 centiseconds)

community-string - Password-like community string sent with the notification operation to SNMP V1 and V2c hosts. Although you can set this string using the **snmp-server host** command by itself, we recommend defining it with the snmp-server community command prior to using the **snmp-server host** command. (Maximum length: 32 characters)

version - Specifies whether to send notifications as SNMP Version 1, 2c or 3 traps. (Range: 1, 2c, 3; Default: 1)

auth | **noauth** | **priv** - This group uses SNMPv3 with authentication, no authentication, or with authentication and privacy. See "Simple Network Management Protocol" on page 480 for further information about these authentication and encryption options.

port - Host UDP port to use. (Range: 1-65535; Default: 162)

DEFAULT SETTING

Host Address: None
Notification Type: Traps
SNMP Version: 1
UDP Port: 162

COMMAND MODE

Global Configuration

COMMAND USAGE

- If you do not enter an **snmp-server host** command, no notifications are sent. In order to configure the switch to send SNMP notifications, you must enter at least one **snmp-server host** command. In order to enable multiple hosts, you must issue a separate **snmp-server host** command for each host.

- The **snmp-server host** command is used in conjunction with the snmp-server enable traps command. Use the snmp-server enable traps command to enable the sending of traps or informs and to specify which SNMP notifications are sent globally. For a host to receive notifications, at least one snmp-server enable traps command and the **snmp-server host** command for that host must be enabled.

- Some notification types cannot be controlled with the snmp-server enable traps command. For example, some notification types are always enabled.

- Notifications are issued by the switch as trap messages by default. The recipient of a trap message does not send a response to the switch. Traps are therefore not as reliable as inform messages, which include a request for acknowledgement of receipt. Informs can be used to ensure that critical information is received by the host. However, note that informs consume more system resources because they must be kept in memory until a response is received. Informs also add to network traffic. You should consider these effects when deciding whether to issue notifications as traps or informs.

  To send an inform to a SNMPv2c host, complete these steps:

  1. Enable the SNMP agent (page 997).
  2. Create a view with the required notification messages (page 1008).
  3. Create a group that includes the required notify view (page 1006).
  4. Allow the switch to send SNMP traps; i.e., notifications (page 1000).
  5. Specify the target host that will receive inform messages with the **snmp-server host** command as described in this section.

To send an inform to a SNMPv3 host, complete these steps:

1. Enable the SNMP agent (page 997).
2. Create a local SNMPv3 user to use in the message exchange process (page 1007).
3. Create a view with the required notification messages (page 1008).
4. Create a group that includes the required notify view (page 1006).
5. Allow the switch to send SNMP traps; i.e., notifications (page 1000).
6. Specify the target host that will receive inform messages with the **snmp-server host** command as described in this section.

- The switch can send SNMP Version 1, 2c or 3 notifications to a host IP address, depending on the SNMP version that the management station supports. If the **snmp-server host** command does not specify the SNMP version, the default is to send SNMP version 1 notifications.

- If you specify an SNMP Version 3 host, then the community string is interpreted as an SNMP user name. The user name must first be defined with the snmp-server user command. Otherwise, an SNMPv3 group will be automatically created by the **snmp-server host** command using the name of the specified community string, and default settings for the read, write, and notify view.

EXAMPLE

```
Console(config)#snmp-server host 10.1.19.23 batman
Console(config)#
```

RELATED COMMANDS

snmp-server enable traps (1000)

snmp-server enable port-traps mac-notification

This command enables the device to send SNMP traps (i.e., SNMP notifications) when a dynamic MAC address is added or removed. Use the no form to restore the default setting.

SYNTAX

[**no**] **snmp-server enable port-traps mac-notification**

mac-notification - Keyword to issue trap when a dynamic MAC address is added or removed.

DEFAULT SETTING

Disabled

COMMAND MODE

Interface Configuration (Ethernet, Port Channel)

COMMAND USAGE

This command can enable MAC authentication traps on the current interface only if they are also enabled at the global level with the snmp-server enable traps mac-authentication command.

EXAMPLE

```
Console(config)#interface ethernet 1/1
Console(config-if)#snmp-server enable port-traps mac-notification
Console(config)#
```

show snmp-server enable port-traps

This command shows if SNMP traps are enabled or disabled for the specified interfaces.

SYNTAX

show snmp-server enable port-traps interface [*interface*]

interface

ethernet *unit/port*

unit - Unit identifier. (Range: 1)

port - Port number. (Range: 1-28)

port-channel *channel-id* (Range: 1-8)

COMMAND MODE

Privileged Exec

EXAMPLE

```
Console#show snmp-server enable port-traps interface
Interface MAC Notification Trap
--------- ---------------------
Eth 1/1                      No
Eth 1/2                      No
Eth 1/3                      No
⋮
```

SNMPv3 Commands

snmp-server engine-id

This command configures an identification string for the SNMPv3 engine. Use the **no** form to restore the default.

SYNTAX

snmp-server engine-id {**local** | **remote** {*ip-address*}}
engineid-string

no snmp-server engine-id {**local** | **remote** {*ip-address*}}

local - Specifies the SNMP engine on this switch.

remote - Specifies an SNMP engine on a remote device.

ip-address - The Internet address of the remote device.

engineid-string - String identifying the engine ID. (Range: 1-26 hexadecimal characters)

Default Setting

A unique engine ID is automatically generated by the switch based on its MAC address.

Command Mode

Global Configuration

Command Usage

- An SNMP engine is an independent SNMP agent that resides either on this switch or on a remote device. This engine protects against message replay, delay, and redirection. The engine ID is also used in combination with user passwords to generate the security keys for authenticating and encrypting SNMPv3 packets.

- A remote engine ID is required when using SNMPv3 informs. (See the snmp-server host command.) The remote engine ID is used to compute the security digest for authentication and encryption of packets passed between the switch and a user on the remote host. SNMP passwords are localized using the engine ID of the authoritative agent. For informs, the authoritative SNMP agent is the remote agent. You therefore need to configure the remote agent's SNMP engine ID before you can send proxy requests or informs to it.

- Trailing zeroes need not be entered to uniquely specify a engine ID. In other words, the value "0123456789" is equivalent to "0123456789" followed by 16 zeroes for a local engine ID.

- A local engine ID is automatically generated that is unique to the switch. This is referred to as the default engine ID. If the local engine ID is deleted or changed, all SNMP users will be cleared. You will need to reconfigure all existing users (page 1007).

Example

```
Console(config)#snmp-server engine-id local 1234567890
Console(config)#snmp-server engineID remote 9876543210 192.168.1.19
Console(config)#
```

Related Commands

snmp-server host (1001)

snmp-server group

This command adds an SNMP group, mapping SNMP users to SNMP views. Use the **no** form to remove an SNMP group.

SYNTAX

snmp-server group *groupname*
{**v1** | **v2c** | **v3** {**auth** | **noauth** | **priv**}}
[**read** *readview*] [**write** *writeview*] [**notify** *notifyview*]

no snmp-server group *groupname*

groupname - Name of an SNMP group. (Range: 1-32 characters)

v1 | **v2c** | **v3** - Use SNMP version 1, 2c or 3.

auth | **noauth** | **priv** - This group uses SNMPv3 with authentication, no authentication, or with authentication and privacy. See "Simple Network Management Protocol" on page 480 for further information about these authentication and encryption options.

readview - Defines the view for read access. (1-32 characters)

writeview - Defines the view for write access. (1-32 characters)

notifyview - Defines the view for notifications. (1-32 characters)

DEFAULT SETTING

Default groups: public[17] (read only), private[18] (read/write)
readview - Every object belonging to the Internet OID space (1).
writeview - Nothing is defined.
notifyview - Nothing is defined.

COMMAND MODE

Global Configuration

COMMAND USAGE

- A group sets the access policy for the assigned users.
- When authentication is selected, the MD5 or SHA algorithm is used as specified in the snmp-server user command.
- When privacy is selected, the DES 56-bit algorithm is used for data encryption.
- For additional information on the notification messages supported by this switch, see Table 34, "Supported Notification Messages," on page 490. Also, note that the authentication, link-up and link-down messages are legacy traps and must therefore be enabled in conjunction with the snmp-server enable traps command.

[17] No view is defined.
[18] Maps to the defaultview.

EXAMPLE

```
Console(config)#snmp-server group r&d v3 auth write daily
Console(config)#
```

snmp-server user

This command adds a user to an SNMP group, restricting the user to a specific SNMP Read, Write, or Notify View. Use the **no** form to remove a user from an SNMP group.

SYNTAX

snmp-server user *username groupname* [**remote** *ip-address*]
{**v1** | **v2c** | **v3** [**encrypted**] [**auth** {**md5** | **sha**} *auth-password*
[**priv des56** *priv-password*]]

no snmp-server user *username* {**v1** | **v2c** | **v3** | **remote**}

username - Name of user connecting to the SNMP agent. (Range: 1-32 characters)

groupname - Name of an SNMP group to which the user is assigned. (Range: 1-32 characters)

remote - Specifies an SNMP engine on a remote device.

ip-address - The Internet address of the remote device.

v1 | **v2c** | **v3** - Use SNMP version 1, 2c or 3.

encrypted - Accepts the password as encrypted input.

auth - Uses SNMPv3 with authentication.

md5 | **sha** - Uses MD5 or SHA authentication.

auth-password - Authentication password. Enter as plain text if the **encrypted** option is not used. Otherwise, enter an encrypted password. (A minimum of eight characters is required.)

priv des56 - Uses SNMPv3 with privacy with DES56 encryption.

priv-password - Privacy password. Enter as plain text if the **encrypted** option is not used. Otherwise, enter an encrypted password.

DEFAULT SETTING

None

COMMAND MODE

Global Configuration

COMMAND USAGE

- Local users (i.e., the command does not specify a remote engine identifier) must be configured to authorize management access for SNMPv3 clients, or to identify the source of SNMPv3 trap messages sent from the local switch.

- Remote users (i.e., the command specifies a remote engine identifier) must be configured to identify the source of SNMPv3 inform messages sent from the local switch.

- The SNMP engine ID is used to compute the authentication/privacy digests from the password. You should therefore configure the engine ID with the snmp-server engine-id command before using this configuration command.

- Before you configure a remote user, use the snmp-server engine-id command to specify the engine ID for the remote device where the user resides. Then use the **snmp-server user** command to specify the user and the IP address for the remote device where the user resides. The remote agent's SNMP engine ID is used to compute authentication/ privacy digests from the user's password. If the remote engine ID is not first configured, the **snmp-server user** command specifying a remote user will fail.

- SNMP passwords are localized using the engine ID of the authoritative agent. For informs, the authoritative SNMP agent is the remote agent. You therefore need to configure the remote agent's SNMP engine ID before you can send proxy requests or informs to it.

EXAMPLE

```
Console(config)#snmp-server user steve group r&d v3 auth md5 greenpeace priv
  des56 einstien
Console(config)#snmp-server user mark group r&d remote 192.168.1.19 v3 auth
  md5 greenpeace priv des56 einstien
Console(config)#
```

snmp-server view

This command adds an SNMP view which controls user access to the MIB. Use the **no** form to remove an SNMP view.

SYNTAX

snmp-server view *view-name oid-tree* {**included** | **excluded**}

no snmp-server view *view-name*

view-name - Name of an SNMP view. (Range: 1-32 characters)

oid-tree - Object identifier of a branch within the MIB tree. Wild cards can be used to mask a specific portion of the OID string. (Refer to the examples.)

included - Defines an included view.

excluded - Defines an excluded view.

DEFAULT SETTING

defaultview (includes access to the entire MIB tree)

COMMAND MODE

Global Configuration

Command Usage

- Views are used in the snmp-server group command to restrict user access to specified portions of the MIB tree.
- The predefined view “defaultview” includes access to the entire MIB tree.

Examples

This view includes MIB-2.

```
Console(config)#snmp-server view mib-2 1.3.6.1.2.1 included
Console(config)#
```

This view includes the MIB-2 interfaces table, ifDescr. The wild card is used to select all the index values in this table.

```
Console(config)#snmp-server view ifEntry.2 1.3.6.1.2.1.2.2.1.*.2 included
Console(config)#
```

This view includes the MIB-2 interfaces table, and the mask selects all index entries.

```
Console(config)#snmp-server view ifEntry.a 1.3.6.1.2.1.2.2.1.1.* included
Console(config)#
```

show snmp engine-id

This command shows the SNMP engine ID.

Command Mode

Privileged Exec

Example

This example shows the default engine ID.

```
Console#show snmp engine-id
Local SNMP EngineID: 8000002a8000000000e8666672
Local SNMP EngineBoots: 1

Remote SNMP EngineID                                         IP address
80000000030004e2b316c54321                                   192.168.1.19
Console#
```

Table 90: show snmp engine-id - display description

Field	Description
Local SNMP engineID	String identifying the engine ID.
Local SNMP engineBoots	The number of times that the engine has (re-)initialized since the snmp EngineID was last configured.

Table 90: show snmp engine-id - display description (Continued)

Field	Description
Remote SNMP engineID	String identifying an engine ID on a remote device.
IP address	IP address of the device containing the corresponding remote SNMP engine.

show snmp group

Four default groups are provided – SNMPv1 read-only access and read/write access, and SNMPv2c read-only access and read/write access.

COMMAND MODE

Privileged Exec

EXAMPLE

```
Console#show snmp group
Group Name: r&d
Security Model: v3
Read View: defaultview
Write View: daily
Notify View: none
Storage Type: permanent
Row Status: active

Group Name: public
Security Model: v1
Read View: defaultview
Write View: none
Notify View: none
Storage Type: volatile
Row Status: active

Group Name: public
Security Model: v2c
Read View: defaultview
Write View: none
Notify View: none
Storage Type: volatile
Row Status: active

Group Name: private
Security Model: v1
Read View: defaultview
Write View: defaultview
Notify View: none
Storage Type: volatile
Row Status: active

Group Name: private
Security Model: v2c
Read View: defaultview
Write View: defaultview
Notify View: none
Storage Type: volatile
Row Status: active

Console#
```

Table 91: show snmp group - display description

Field	Description
groupname	Name of an SNMP group.
security model	The SNMP version.
readview	The associated read view.
writeview	The associated write view.
notifyview	The associated notify view.
storage-type	The storage type for this entry.
Row Status	The row status of this entry.

show snmp user

This command shows information on SNMP users.

COMMAND MODE

Privileged Exec

EXAMPLE

```
Console#show snmp user
EngineId: 800000ca030030f1df9ca00000
User Name: steve
Authentication Protocol: md5
Privacy Protocol: des56
Storage Type: nonvolatile
Row Status: active

SNMP remote user
EngineId: 80000000030004e2b316c54321
User Name: mark
Authentication Protocol: mdt
Privacy Protocol: des56
Storage Type: nonvolatile
Row Status: active

Console#
```

Table 92: show snmp user - display description

Field	Description
EngineId	String identifying the engine ID.
User Name	Name of user connecting to the SNMP agent.
Authentication Protocol	The authentication protocol used with SNMPv3.
Privacy Protocol	The privacy protocol used with SNMPv3.
Storage Type	The storage type for this entry.
Row Status	The row status of this entry.
SNMP remote user	A user associated with an SNMP engine on a remote device.

show snmp view

This command shows information on the SNMP views.

COMMAND MODE

Privileged Exec

EXAMPLE

```
Console#show snmp view
View Name: mib-2
Subtree OID: 1.2.2.3.6.2.1
View Type: included
Storage Type: permanent
Row Status: active

View Name: defaultview
Subtree OID: 1
View Type: included
Storage Type: volatile
Row Status: active

Console#
```

Table 93: show snmp view - display description

Field	Description
View Name	Name of an SNMP view.
Subtree OID	A branch in the MIB tree.
View Type	Indicates if the view is included or excluded.
Storage Type	The storage type for this entry.
Row Status	The row status of this entry.

Notification Log Commands

nlm

This command enables or disables the specified notification log.

SYNTAX

[**no**] **nlm** *filter-name*

filter-name - Notification log name. (Range: 1-32 characters)

DEFAULT SETTING

Enabled

COMMAND MODE

Global Configuration

COMMAND USAGE

- Notification logging is enabled by default, but will not start recording information until a logging profile specified by the snmp-server notify-filter command is enabled by the **nlm** command.

- Disabling logging with this command does not delete the entries stored in the notification log.

Example

This example enables the notification log A1.

```
Console(config)#nlm A1
Console(config)#
```

snmp-server notify-filter

This command creates an SNMP notification log. Use the **no** form to remove this log.

Syntax

[**no**] **snmp-server notify-filter** *profile-name* **remote** *ip-address*

profile-name - Notification log profile name. (Range: 1-32 characters)

ip-address - The Internet address of a remote device. The specified target host must already have been configured using the snmp-server host command.

Note: The notification log is stored locally. It is not sent to a remote device. This remote host parameter is only required to complete mandatory fields in the SNMP Notification MIB.

Default Setting

None

Command Mode

Global Configuration

Command Usage

- Systems that support SNMP often need a mechanism for recording Notification information as a hedge against lost notifications, whether there are Traps or Informs that may be exceeding retransmission limits. The Notification Log MIB (NLM, RFC 3014) provides an infrastructure in which information from other MIBs may be logged.

- Given the service provided by the NLM, individual MIBs can now bear less responsibility to record transient information associated with an event against the possibility that the Notification message is lost, and applications can poll the log to verify that they have not missed any important Notifications.

- If notification logging is not configured and enabled, when the switch reboots, some SNMP traps (such as warm start) cannot be logged.

- To avoid this problem, notification logging should be configured and enabled using the **snmp-server notify-filter** command and nlm command, and these commands stored in the startup configuration file. Then when the switch reboots, SNMP traps (such as warm start) can now be logged.

- When this command is executed, a notification log is created (with the default parameters defined in RFC 3014). Notification logging is enabled by default (see the nlm command), but will not start recording information until a logging profile specified with this command is enabled with the nlm command.

- Based on the default settings used in RFC 3014, a notification log can contain up to 256 entries, and the entry aging time is 1440 minutes. Information recorded in a notification log, and the entry aging time can only be configured using SNMP from a network management station.

- When a trap host is created with the snmp-server host command, a default notify filter will be created as shown in the example under the show snmp notify-filter command.

EXAMPLE

This example first creates an entry for a remote host, and then instructs the switch to record this device as the remote host for the specified notification log.

```
Console(config)#snmp-server host 10.1.19.23 batman
Console(config)#snmp-server notify-filter A1 remote 10.1.19.23
Console#
```

show nlm oper-status

This command shows the operational status of configured notification logs.

COMMAND MODE

Privileged Exec

EXAMPLE

```
Console#show nlm oper-status
Filter Name: A1
Oper-Status: Operational
Console#
```

show snmp notify-filter

This command displays the configured notification logs.

COMMAND MODE
Privileged Exec

EXAMPLE
This example displays the configured notification logs and associated target hosts.

```
Console#show snmp notify-filter
Filter profile name            IP address
----------------------------  ----------------
A1                             10.1.19.23
Console#
```

Additional Trap Commands

memory

This command sets an SNMP trap based on configured thresholds for memory utilization. Use the **no** form to restore the default setting.

SYNTAX

memory {**rising** *rising-threshold* | **falling** *falling-threshold*}

no memory {**rising** | **falling**}

rising-threshold - Rising threshold for memory utilization alarm expressed in percentage. (Range: 1-100)

falling-threshold - Falling threshold for memory utilization alarm expressed in percentage. (Range: 1-100)

DEFAULT SETTING
Rising Threshold: 90%
Falling Threshold: 70%

COMMAND MODE
Global Configuration

COMMAND USAGE
Once the rising alarm threshold is exceeded, utilization must drop beneath the falling threshold before the alarm is terminated, and then exceed the rising threshold again before another alarm is triggered.

EXAMPLE

```
Console(config)#memory rising 80
Console(config)#memory falling 60
Console#
```

RELATED COMMANDS
show memory (903)

process cpu

This command sets an SNMP trap based on configured thresholds for CPU utilization. Use the no form to restore the default setting.

SYNTAX

process cpu {**rising** *rising-threshold* | **falling** *falling-threshold*}

no process cpu {**rising** | **falling**}

rising-threshold - Rising threshold for CPU utilization alarm expressed in percentage. (Range: 1-100)

falling-threshold - Falling threshold for CPU utilization alarm expressed in percentage. (Range: 1-100)

DEFAULT SETTING

Rising Threshold: 90%
Falling Threshold: 70%

COMMAND MODE

Global Configuration

COMMAND USAGE

Once the rising alarm threshold is exceeded, utilization must drop beneath the falling threshold before the alarm is terminated, and then exceed the rising threshold again before another alarm is triggered.

EXAMPLE

```
Console(config)#process cpu rising 80
Console(config)#process cpu falling 60
Console#
```

RELATED COMMANDS

show process cpu (904)

26 Remote Monitoring Commands

Remote Monitoring allows a remote device to collect information or respond to specified events on an independent basis. This switch is an RMON-capable device which can independently perform a wide range of tasks, significantly reducing network management traffic. It can continuously run diagnostics and log information on network performance. If an event is triggered, it can automatically notify the network administrator of a failure and provide historical information about the event. If it cannot connect to the management agent, it will continue to perform any specified tasks and pass data back to the management station the next time it is contacted.

This switch supports mini-RMON, which consists of the Statistics, History, Event and Alarm groups. When RMON is enabled, the system gradually builds up information about its physical interfaces, storing this information in the relevant RMON database group. A management agent then periodically communicates with the switch using the SNMP protocol. However, if the switch encounters a critical event, it can automatically send a trap message to the management agent which can then respond to the event if so configured.

Table 94: RMON Commands

Command	Function	Mode
rmon alarm	Sets threshold bounds for a monitored variable	GC
rmon event	Creates a response event for an alarm	GC
rmon collection history	Periodically samples statistics	IC
rmon collection rmon1	Enables statistics collection	IC
show rmon alarms	Shows the settings for all configured alarms	PE
show rmon events	Shows the settings for all configured events	PE
show rmon history	Shows the sampling parameters for each entry	PE
show rmon statistics	Shows the collected statistics	PE

rmon alarm

This command sets threshold bounds for a monitored variable. Use the **no** form to remove an alarm.

SYNTAX

rmon alarm *index variable interval* {**absolute** | **delta**}
rising-threshold *threshold* [*event-index*]
falling-threshold *threshold* [*event-index*]
[**owner** *name*]

no rmon alarm *index*

index – Index to this entry. (Range: 1-65535)

variable – The object identifier of the MIB variable to be sampled. Only variables of the type etherStatsEntry.n.n may be sampled. Note that etherStatsEntry.n uniquely defines the MIB variable, and etherStatsEntry.n.n defines the MIB variable, plus the etherStatsIndex. For example, 1.3.6.1.2.1.16.1.1.1.6.1 denotes etherStatsBroadcastPkts, plus the etherStatsIndex of 1.

interval – The polling interval. (Range: 1-31622400 seconds)

absolute – The variable is compared directly to the thresholds at the end of the sampling period.

delta – The last sample is subtracted from the current value and the difference is then compared to the thresholds.

threshold – An alarm threshold for the sampled variable. (Range: 0-2147483647)

event-index – The index of the event to use if an alarm is triggered. If there is no corresponding entry in the event control table, then no event will be generated. (Range: 1-65535)

name – Name of the person who created this entry. (Range: 1-127 characters)

DEFAULT SETTING

1.3.6.1.2.1.16.1.1.1.6.1 - 1.3.6.1.2.1.16.1.1.1.6.28
Taking delta samples every 30 seconds,
Rising threshold is 892800, assigned to event 0
Falling threshold is 446400, assigned to event 0

COMMAND MODE

Global Configuration

COMMAND USAGE

- If an event is already defined for an index, the entry must be deleted before any changes can be made with this command.
- If the current value is greater than or equal to the rising threshold, and the last sample value was less than this threshold, then an alarm will be generated. After a rising event has been generated, another such event will not be generated until the sampled value has fallen below the rising threshold, reaches the falling threshold, and again moves back up to the rising threshold.

- If the current value is less than or equal to the falling threshold, and the last sample value was greater than this threshold, then an alarm will be generated. After a falling event has been generated, another such event will not be generated until the sampled value has risen above the falling threshold, reaches the rising threshold, and again moves back down to the failing threshold.

EXAMPLE

```
Console(config)#rmon alarm 1 1.3.6.1.2.1.16.1.1.1.6.1 15 delta
  rising-threshold 100 1 falling-threshold 30 1 owner mike
Console(config)#
```

rmon event

This command creates a response event for an alarm. Use the **no** form to remove an event.

SYNTAX

rmon event *index* [**log**] | [**trap** *community*] | [**description** *string*] | [**owner** *name*]

no rmon event *index*

index – Index to this entry. (Range: 1-65535)

log – Generates an RMON log entry when the event is triggered. Log messages are processed based on the current configuration settings for event logging (see "Event Logging" on page 933).

trap – Sends a trap message to all configured trap managers (see "snmp-server host" on page 1001).

community – A password-like community string sent with the trap operation to SNMP v1 and v2c hosts. Although this string can be set using the **rmon event** command by itself, it is recommended that the string be defined using the snmp-server community command prior to using the rmon event command. (Range: 1-32 characters)

string – A comment that describes this event.
(Range: 1-127 characters)

name – Name of the person who created this entry.
(Range: 1-127 characters)

DEFAULT SETTING

None

COMMAND MODE

Global Configuration

COMMAND USAGE

- If an event is already defined for an index, the entry must be deleted before any changes can be made with this command.

- The specified events determine the action to take when an alarm triggers this event. The response to an alarm can include logging the alarm or sending a message to a trap manager.

EXAMPLE

```
Console(config)#rmon event 2 log description urgent owner mike
Console(config)#
```

rmon collection history

This command periodically samples statistics on a physical interface. Use the no form to disable periodic sampling.

SYNTAX

rmon collection history controlEntry *index*
[[**owner** *name*] [**buckets** *number*] [**interval** *seconds*]] |
[**buckets** *number*] [**interval** *seconds*] | **interval** *seconds*

no rmon collection history controlEntry *index*

index – Index to this entry. (Range: 1-65535)

number – The number of buckets requested for this entry. (Range: 1-65536)

seconds – The polling interval. (Range: 1-3600 seconds)

name – Name of the person who created this entry. (Range: 1-127 characters)

DEFAULT SETTING

1.3.6.1.2.1.16.1.1.1.6.1 - 1.3.6.1.2.1.16.1.1.1.6.28
Buckets: 50
Interval: 30 seconds for even numbered entries,
1800 seconds for odd numbered entries

COMMAND MODE

Interface Configuration (Ethernet)

COMMAND USAGE

- By default, each index number equates to a port on the switch, but can be changed to any number not currently in use.

- If periodic sampling is already enabled on an interface, the entry must be deleted before any changes can be made with this command.

- The information collected for each sample includes:

  input octets, packets, broadcast packets, multicast packets, undersize packets, oversize packets, fragments, jabbers, CRC alignment errors, collisions, drop events, and network utilization.

- The switch reserves two controlEntry index entries for each port. If a default index entry is re-assigned to another port by this command, the show running-config command will display a message indicating that this index is not available for the port to which is normally assigned.

For example, if control entry 15 is assigned to port 5 as shown below, the **show running-config** command will indicate that this entry is not available for port 8.

```
Console(config)#interface ethernet 1/5
Console(config-if)#rmon collection history controlEntry 15
Console(config-if)#end
Console#show running-config
!
interface ethernet 1/5
 rmon collection history controlEntry 15 buckets 50 interval 1800
...
interface ethernet 1/8
 no rmon collection history controlEntry 15
```

EXAMPLE

```
Console(config)#interface ethernet 1/1
Console(config-if)#rmon collection history controlentry 21 owner mike buckets
  24 interval 60
Console(config-if)#
```

rmon collection rmon1

This command enables the collection of statistics on a physical interface. Use the no form to disable statistics collection.

SYNTAX

rmon collection rmon1 controlEntry *index* [**owner** *name*]

no rmon collection rmon1 controlEntry *index*

index – Index to this entry. (Range: 1-65535)

name – Name of the person who created this entry. (Range: 1-127 characters)

DEFAULT SETTING

Enabled

COMMAND MODE

Interface Configuration (Ethernet)

COMMAND USAGE

- By default, each index number equates to a port on the switch, but can be changed to any number not currently in use.

- If statistics collection is already enabled on an interface, the entry must be deleted before any changes can be made with this command.

- The information collected for each entry includes:

  input octets, packets, broadcast packets, multicast packets, undersize packets, oversize packets, fragments, jabbers, CRC alignment errors, collisions, drop events, and packets of specified lengths

EXAMPLE

```
Console(config)#interface ethernet 1/1
Console(config-if)#rmon collection rmon1 controlEntry 1 owner mike
Console(config-if)#
```

show rmon alarms

This command shows the settings for all configured alarms.

COMMAND MODE

Privileged Exec

EXAMPLE

```
Console#show rmon alarms
Alarm 1 is valid, owned by
 Monitors 1.3.6.1.2.1.16.1.1.1.6.1 every 30 seconds
 Taking delta samples, last value was 0
 Rising threshold is 892800, assigned to event 0
 Falling threshold is 446400, assigned to event 0
:
```

show rmon events

This command shows the settings for all configured events.

COMMAND MODE

Privileged Exec

EXAMPLE

```
Console#show rmon events
Event 2 is valid, owned by mike
 Description is urgent
 Event firing causes log and trap to community , last fired  00:00:00
Console#
```

show rmon history

This command shows the sampling parameters configured for each entry in the history group.

COMMAND MODE

Privileged Exec

EXAMPLE

```
Console#show rmon history
Entry 1 is valid, and owned by
 Monitors 1.3.6.1.2.1.2.2.1.1.1 every 1800 seconds
 Requested # of time intervals, ie buckets, is 8
 Granted # of time intervals, ie buckets, is 8
  Sample # 1 began measuring at 00:00:01
  Received 77671 octets, 1077 packets,
  61 broadcast and 978 multicast packets,
  0 undersized and 0 oversized packets,
  0 fragments and 0 jabbers packets,
  0 CRC alignment errors and 0 collisions.
  # of dropped packet events is 0
  Network utilization is estimated at 0
⋮
```

show rmon statistics

This command shows the information collected for all configured entries in the statistics group.

COMMAND MODE

Privileged Exec

EXAMPLE

```
Console#show rmon statistics
Interface 1 is valid, and owned by
 Monitors 1.3.6.1.2.1.2.2.1.1.1 which has
 Received 164289 octets, 2372 packets,
 120 broadcast and 2211 multicast packets,
 0 undersized and 0 oversized packets,
 0 fragments and 0 jabbers,
 0 CRC alignment errors and 0 collisions.
 # of dropped packet events (due to lack of resources): 0
 # of packets received of length (in octets):
  64: 2245, 65-127: 87, 128-255: 31,
  256-511: 5, 512-1023: 2, 1024-1518: 2
⋮
```

27 Flow Sampling Commands

Flow sampling (sFlow) can be used with a remote sFlow Collector to provide an accurate, detailed and real-time overview of the types and levels of traffic present on the network. The sFlow Agent samples 1 out of *n* packets from all data traversing the switch, re-encapsulates the samples as sFlow datagrams and transmits them to the sFlow Collector. This sampling occurs at the internal hardware level where all traffic is seen, whereas traditional probes only have a partial view of traffic as it is sampled at the monitored interface. Moreover, the processor and memory load imposed by the sFlow agent is minimal since local analysis does not take place.

Note: The terms “collector”, “receiver” and “owner”, in the context of this chapter, all refer to a remote server capable of receiving the sFlow datagrams generated by the sFlow agent of the switch.

Table 95: sFlow Commands

Command	Function	Mode
sflow owner	Creates an sFlow collector which the switch uses to send samples to.	PE
sflow sampling instance	Configures an sFlow sampling data source that samples periodically based on a packet count.	PE
sflow polling instance	Configures an sFlow polling data source that takes samples periodically based on time.	PE
show sflow	Shows the global and interface settings for the sFlow process	PE

sflow owner

This command creates an sFlow collector on the switch. Use the **no** form to remove the sFlow receiver.

Syntax

sflow owner *owner-name*
  timeout *timeout-value*
  [**destination** {*ipv4-address* | *ipv6-address*}]
  [**port** *destination-udp-port*]
  [**max-datagram-size** *max-datagram-size*]
  [**version** {**v4** | **v5**}]

no sflow owner *owner-name*

owner-name - Name of the collector. (Range: 1-30 alphanumeric characters) *timeout-value* - The length of time the sFlow interface is available to send samples to a receiver, after which the owner and associated polling and sampling data source instances are removed from the configuration. (Range: 30-10000000 seconds)

ipv4-address - IPv4 address of the sFlow collector. Valid IPv4 addresses consist of four decimal numbers, 0 to 255, separated by periods.

ipv6-address - IPv6 address of the sFlow collector. A full IPv6 address including the network prefix and host address bits. An IPv6 address consists of 8 colon-separated 16-bit hexadecimal values. One double colon may be used to indicate the appropriate number of zeros required to fill the undefined fields.

destination-udp-port - The UDP port on which the collector is listening for sFlow streams. (Range: 1-65535)

max-datagram-size - The maximum size of the sFlow datagram payload. (Range: 200-1500 bytes)

version {**v4** | **v5**} - Sends either v4 or v5 sFlow datagrams to the receiver.

DEFAULT SETTING

No owner is configured
UDP Port: 6343
Version: v4
Maximum Datagram Size: 1400 bytes

COMMAND MODE

Privileged Exec

COMMAND USAGE

- Use the **sflow owner** command to create an owner instance of an sFlow collector. If the socket port, maximum datagram size, and datagram version are not specified, then the default values are used.

- Once an owner is created, the **sflow owner** command can again be used to modify the owner's port number. All other parameter values for the owner will be retained if the port is modified.

- Use the **no sflow owner** command to remove the collector.

- When the **sflow owner** command is issued, it's associated timeout value will immediately begin to count down. Once the timeout value has reached zero seconds, the sFlow owner and it's associated sampling sources will be deleted from the configuration.

EXAMPLE

This example shows an sflow collector being created on the switch.

```
Console(config)#sflow owner stat_server1 timeout 100 destination
  192.168.220.225 port 22500 max-datagram-size 512 version v5
Console(config)#
```

This example shows how to modify the sFlow port number for an already configured collector.

```
Console(config)#sflow owner stat_server1 timeout 100 port 35100
Console(config)#
```

sflow sampling instance

This command enables an sFlow data source instance for a specific interface that takes samples periodically based on the number of packets processed. Use the **no** form to remove the sampling data source instance from the switch's sFlow configuration.

SYNTAX

sflow sampling {**interface** *interface*} **instance** *instance-id* **receiver** *owner-name* **sampling-rate** *sample-rate* [**max-header-size** *max-header-size*]

no sflow sample {**interface** *interface*} **instance** *instance-id*

interface - The source from which the samples will be taken and sent to a collector.

ethernet *unit/port*

unit - Stack unit. (Range: 1)

port - Port number. (Range: 1-28)

instance-id - An instance ID used to identify the sampling source. (Range: 1)

owner-name - The associated receiver, to which the samples will be sent. (Range: 1-30 alphanumeric characters)

sample-rate - The packet sampling rate, or the number of packets out of which one sample will be taken. (Range: 256-16777215 packets)

max-header-size - The maximum size of the sFlow datagram header. (Range: 64 to 256 bytes)

DEFAULT SETTING

No sFlow sampling instance id configured.
Maximu Header Size: 128 bytes

COMMAND MODE

Privileged Exec

EXAMPLE

This example enables a sampling data source on Ethernet interface 1/1, an associated receiver named "owner1", and a sampling rate of one out of 100. The maximum header size is also set to 200 bytes.

```
Console# sflow sampling interface ethernet 1/1 instance 1 receiver owner1
  sampling-rate 100 max-header-size 200
Console#
```

The following command removes a sampling data source from Ethernet interface 1/1.

```
Console# no sflow sampling interface ethernet 1/1 instance 1
Console#
```

sflow polling instance

This command enables an sFlow polling data source, for a specified interface, that polls periodically based on a specified time interval. Use the **no** form to remove the polling data source instance from the switch's sFlow configuration.

SYNTAX

sflow polling {**interface** *interface*} **instance** *instance-id* **receiver** *owner-name* **polling-interval** *seconds*

no sflow polling {**interface** *interface*} **instance** *instance-id*

interface - The source from which the samples will be taken at specified intervals and sent to a collector.

ethernet *unit/port*

unit - Stack unit. (Range: 1)

port - Port number. (Range: 1-28)

instance-id - An instance ID used to identify the sampling source. (Range: 1)

owner-name - The associated receiver, to which the samples will be sent. (Range: 1-30 alphanumeric characters)

polling-interval - The time interval at which the sFlow process adds counter values to the sample datagram. (Range: 0-10000000 seconds, 0 disables this feature)

DEFAULT SETTING

No sFlow polling instance is configured.

COMMAND MODE

Privileged Exec

COMMAND USAGE

This command enables a polling data source and configures the interval at which counter values are added to the sample datagram.

EXAMPLE

This example sets the polling interval to 10 seconds.

```
Console(config)#interface ethernet 1/9
Console(config-if)#sflow polling-interval 10
Console(config-if)#
```

show sflow

This command shows the global and interface settings for the sFlow process.

SYNTAX

show sflow [**owner** *owner-name* | **interface** *interface*]

owner-name - The associated receiver, to which the samples are sent. (Range: 1-30 alphanumeric characters)

interface

ethernet *unit*/*port*

unit - Stack unit. (Range: 1)

port - Port number. (Range: 1-28)

COMMAND MODE

Privileged Exec

EXAMPLE

```
Console#show sflow interface ethernet 1/2

  Receiver Owner Name    : stat1
  Receiver Timeout       : 99633 sec
  Receiver Destination   : 192.168.32.32
  Receiver Socket Port   : 6343
  Maximum Datagram Size : 1400 bytes
  Datagram Version       : 4

  Data Source            : Eth 1/2
  Sampling Instance ID   : 1
  Sampling Rate          : 512
  Maximum Header Size    : 128 bytes

Console#
```

28 Authentication Commands

You can configure this switch to authenticate users logging into the system for management access using local or remote authentication methods. Port-based authentication using IEEE 802.1X can also be configured to control either management access to the uplink ports or client access[19] to the data ports.

Table 96: Authentication Commands

Command Group	Function
User Accounts	Configures the basic user names and passwords for management access
Authentication Sequence	Defines logon authentication method and precedence
RADIUS Client	Configures settings for authentication via a RADIUS server
TACACS+ Client	Configures settings for authentication via a TACACS+ server
AAA	Configures authentication, authorization, and accounting for network access
Web Server	Enables management access via a web browser
Telnet Server	Enables management access via Telnet
Secure Shell	Provides secure replacement for Telnet
802.1X Port Authentication	Configures host authentication on specific ports using 802.1X
Management IP Filter	Configures IP addresses that are allowed management access
PPPoE Intermediate Agent	Configures relay parameters required for sending authentication messages between a client and broadband remote access servers

[19] For other methods of controlling client access, see "General Security Measures" on page 1089.

USER ACCOUNTS

The basic commands required for management access are listed in this section. This switch also includes other options for password checking via the console or a Telnet connection (page 923), user authentication via a remote authentication server (page 1031), and host access authentication for specific ports (page 1067).

Table 97: User Access Commands

Command	Function	Mode
enable password	Sets a password to control access to the Privileged Exec level	GC
username	Establishes a user name-based authentication system at login	GC

enable password

After initially logging onto the system, you should set the Privileged Exec password. Remember to record it in a safe place. This command controls access to the Privileged Exec level from the Normal Exec level. Use the **no** form to reset the default password.

SYNTAX

enable password [**level** *level*] {**0** | **7**} *password*

no enable password [**level** *level*]

level *level* - Level 15 for Privileged Exec. (Levels 0-14 are not used.)

{**0** | **7**} - 0 means plain password, 7 means encrypted password.

password - Password for this privilege level. (Maximum length: 32 characters plain text or encrypted, case sensitive)

DEFAULT SETTING

The default is level 15.
The default password is “super”

COMMAND MODE

Global Configuration

COMMAND USAGE

- You cannot set a null password. You will have to enter a password to change the command mode from Normal Exec to Privileged Exec with the enable command.

- The encrypted password is required for compatibility with legacy password settings (i.e., plain text or encrypted) when reading the configuration file during system bootup or when downloading the configuration file from a TFTP server. There is no need for you to manually configure encrypted passwords.

EXAMPLE

```
Console(config)#enable password level 15 0 admin
Console(config)#
```

RELATED COMMANDS

enable (885)
authentication enable (1034)

username

This command adds named users, requires authentication at login, specifies or changes a user's password (or specify that no password is required), or specifies or changes a user's access level. Use the **no** form to remove a user name.

SYNTAX

username *name* {**access-level** *level* | **nopassword** |
password {**0** | **7**} *password*}

no username *name*

name - The name of the user. (Maximum length: 32 characters, case sensitive. Maximum users: 16)

access-level *level* - Specifies the user level.
The device has two predefined privilege levels:
0: Normal Exec, **15**: Privileged Exec.

nopassword - No password is required for this user to log in.

{**0** | **7**} - 0 means plain password, 7 means encrypted password.

password *password* - The authentication password for the user. (Maximum length: 32 characters plain text or encrypted, case sensitive)

DEFAULT SETTING

The default access level is Normal Exec.
The factory defaults for the user names and passwords are:

Table 98: Default Login Settings

username	access-level	password
guest	0	guest
admin	15	admin

COMMAND MODE

Global Configuration

COMMAND USAGE

The encrypted password is required for compatibility with legacy password settings (i.e., plain text or encrypted) when reading the configuration file during system bootup or when downloading the configuration file from an FTP/TFTP server. There is no need for you to manually configure encrypted passwords.

EXAMPLE

This example shows how the set the access level and password for a user.

```
Console(config)#username bob access-level 15
Console(config)#username bob password 0 smith
Console(config)#
```

AUTHENTICATION SEQUENCE

Three authentication methods can be specified to authenticate users logging into the system for management access. The commands in this section can be used to define the authentication method and sequence.

Table 99: Authentication Sequence Commands

Command	Function	Mode
authentication enable	Defines the authentication method and precedence for command mode change	GC
authentication login	Defines logon authentication method and precedence	GC

authentication enable

This command defines the authentication method and precedence to use when changing from Exec command mode to Privileged Exec command mode with the enable command. Use the **no** form to restore the default.

SYNTAX

authentication enable {[**local**] [**radius**] [**tacacs**]}

no authentication enable

local - Use local password only.

radius - Use RADIUS server password only.

tacacs - Use TACACS server password.

DEFAULT SETTING

Local

COMMAND MODE

Global Configuration

COMMAND USAGE

- RADIUS uses UDP while TACACS+ uses TCP. UDP only offers best effort delivery, while TCP offers a connection-oriented transport. Also, note that RADIUS encrypts only the password in the access-request packet from the client to the server, while TACACS+ encrypts the entire body of the packet.

- RADIUS and TACACS+ logon authentication assigns a specific privilege level for each user name and password pair. The user name, password, and privilege level must be configured on the authentication server.

- You can specify three authentication methods in a single command to indicate the authentication sequence. For example, if you enter "**authentication enable radius tacacs local**," the user name and password on the RADIUS server is verified first. If the RADIUS server is not available, then authentication is attempted on the TACACS+ server. If the TACACS+ server is not available, the local user name and password is checked.

EXAMPLE

```
Console(config)#authentication enable radius
Console(config)#
```

RELATED COMMANDS

enable password - sets the password for changing command modes (1032)

authentication login

This command defines the login authentication method and precedence. Use the **no** form to restore the default.

SYNTAX

authentication login {[**local**] [**radius**] [**tacacs**]}

no authentication login

local - Use local password.

radius - Use RADIUS server password.

tacacs - Use TACACS server password.

DEFAULT SETTING

Local

COMMAND MODE

Global Configuration

COMMAND USAGE

- RADIUS uses UDP while TACACS+ uses TCP. UDP only offers best effort delivery, while TCP offers a connection-oriented transport. Also, note that RADIUS encrypts only the password in the access-request packet from the client to the server, while TACACS+ encrypts the entire body of the packet.

- RADIUS and TACACS+ logon authentication assigns a specific privilege level for each user name and password pair. The user name, password, and privilege level must be configured on the authentication server.

- You can specify three authentication methods in a single command to indicate the authentication sequence. For example, if you enter "**authentication login radius tacacs local**," the user name and password on the RADIUS server is verified first. If the RADIUS server is not available, then authentication is attempted on the TACACS+ server. If the TACACS+ server is not available, the local user name and password is checked.

EXAMPLE

```
Console(config)#authentication login radius
Console(config)#
```

RELATED COMMANDS

username - for setting the local user names and passwords (1033)

RADIUS CLIENT

Remote Authentication Dial-in User Service (RADIUS) is a logon authentication protocol that uses software running on a central server to control access to RADIUS-aware devices on the network. An authentication server contains a database of multiple user name/password pairs with associated privilege levels for each user or group that require management access to a switch.

Table 100: RADIUS Client Commands

Command	Function	Mode
radius-server acct-port	Sets the RADIUS server network port	GC
radius-server auth-port	Sets the RADIUS server network port	GC
radius-server host	Specifies the RADIUS server	GC
radius-server key	Sets the RADIUS encryption key	GC
radius-server retransmit	Sets the number of retries	GC
radius-server timeout	Sets the interval between sending authentication requests	GC
show radius-server	Shows the current RADIUS settings	PE

radius-server acct-port

This command sets the RADIUS server network port for accounting messages. Use the **no** form to restore the default.

SYNTAX

radius-server acct-port *port-number*

no radius-server acct-port

port-number - RADIUS server UDP port used for accounting messages. (Range: 1-65535)

DEFAULT SETTING

1813

COMMAND MODE

Global Configuration

EXAMPLE

```
Console(config)#radius-server acct-port 181
Console(config)#
```

radius-server auth-port

This command sets the RADIUS server network port. Use the **no** form to restore the default.

SYNTAX

radius-server auth-port *port-number*

no radius-server auth-port

port-number - RADIUS server UDP port used for authentication messages. (Range: 1-65535)

DEFAULT SETTING

1812

COMMAND MODE

Global Configuration

EXAMPLE

```
Console(config)#radius-server auth-port 181
Console(config)#
```

radius-server host

This command specifies primary and backup RADIUS servers, and authentication and accounting parameters that apply to each server. Use the **no** form to remove a specified server, or to restore the default values.

SYNTAX

[**no**] **radius-server** *index* **host** *host-ip-address* [**acct-port** *acct-port*] [**auth-port** *auth-port*] [**key** *key*] [**retransmit** *retransmit*] [**timeout** *timeout*]

index - Allows you to specify up to five servers. These servers are queried in sequence until a server responds or the retransmit period expires.

host-ip-address - IP address of server.

acct-port - RADIUS server UDP port used for accounting messages. (Range: 1-65535)

auth-port - RADIUS server UDP port used for authentication messages. (Range: 1-65535) *key* - Encryption key used to authenticate logon access for client. Do not use blank spaces in the string. (Maximum length: 48 characters)

retransmit - Number of times the switch will try to authenticate logon access via the RADIUS server. (Range: 1-30)

timeout - Number of seconds the switch waits for a reply before resending a request. (Range: 1-65535)

DEFAULT SETTING

auth-port - 1812
acct-port - 1813
timeout - 5 seconds
retransmit - 2

COMMAND MODE

Global Configuration

EXAMPLE

```
Console(config)#radius-server 1 host 192.168.1.20 port 181 timeout 10
  retransmit 5 key green
Console(config)#
```

radius-server key

This command sets the RADIUS encryption key. Use the **no** form to restore the default.

SYNTAX

radius-server key *key-string*

no radius-server key

key-string - Encryption key used to authenticate logon access for client. Do not use blank spaces in the string. (Maximum length: 48 characters)

DEFAULT SETTING

None

COMMAND MODE

Global Configuration

EXAMPLE

```
Console(config)#radius-server key green
Console(config)#
```

radius-server retransmit

This command sets the number of retries. Use the **no** form to restore the default.

SYNTAX

radius-server retransmit *number-of-retries*

no radius-server retransmit

number-of-retries - Number of times the switch will try to authenticate logon access via the RADIUS server. (Range: 1 - 30)

DEFAULT SETTING

2

COMMAND MODE

Global Configuration

EXAMPLE

```
Console(config)#radius-server retransmit 5
Console(config)#
```

radius-server timeout

This command sets the interval between transmitting authentication requests to the RADIUS server. Use the **no** form to restore the default.

SYNTAX

radius-server timeout *number-of-seconds*

no radius-server timeout

number-of-seconds - Number of seconds the switch waits for a reply before resending a request. (Range: 1-65535)

DEFAULT SETTING

5

COMMAND MODE

Global Configuration

EXAMPLE

```
Console(config)#radius-server timeout 10
Console(config)#
```

show radius-server

This command displays the current settings for the RADIUS server.

DEFAULT SETTING

None

COMMAND MODE

Privileged Exec

EXAMPLE

```
Console#show radius-server

Remote RADIUS Server Configuration:

Global Settings:
 Authentication Port Number : 1812
 Accounting Port Number     : 1813
 Retransmit Times           : 2
 Request Timeout            : 5

Server 1:
 Server IP Address          : 192.168.1.1
 Authentication Port Number : 1812
 Accounting Port Number     : 1813
 Retransmit Times           : 2
 Request Timeout            : 5

RADIUS Server Group:
Group Name                Member Index
------------------------- -------------
radius                    1
Console#
```

TACACS+ CLIENT

Terminal Access Controller Access Control System (TACACS+) is a logon authentication protocol that uses software running on a central server to control access to TACACS-aware devices on the network. An authentication server contains a database of multiple user name/password pairs with associated privilege levels for each user or group that require management access to a switch.

Table 101: TACACS+ Client Commands

Command	Function	Mode
tacacs-server host	Specifies the TACACS+ server and optional parameters	GC
tacacs-server key	Sets the TACACS+ encryption key	GC
tacacs-server port	Specifies the TACACS+ server network port	GC
tacacs-server retransmit	Sets the number of retries	GC
tacacs-server timeout	Sets the interval between sending authentication requests	GC
show tacacs-server	Shows the current TACACS+ settings	GC

tacacs-server host

This command specifies the TACACS+ server and other optional parameters. Use the **no** form to remove the server, or to restore the default values.

SYNTAX

tacacs-server *index* **host** *host-ip-address* [**key** *key*]
[**port** *port-number*] [**retransmit** *retransmit*] [**timeout** *timeout*]

no tacacs-server *index*

index - The index for this server. (Range: 1)

host-ip-address - IP address of a TACACS+ server.

key - Encryption key used to authenticate logon access for the client. Do not use blank spaces in the string. (Maximum length: 48 characters)

port-number - TACACS+ server TCP port used for authentication messages. (Range: 1-65535)

retransmit - Number of times the switch will try to authenticate logon access via the TACACS+ server. (Range: 1-30)

timeout - Number of seconds the switch waits for a reply before resending a request. (Range: 1-540)

DEFAULT SETTING

authentication port - 49
timeout - 5 seconds
retransmit - 2

COMMAND MODE

Global Configuration

EXAMPLE

```
Console(config)#tacacs-server 1 host 192.168.1.25 port 181 timeout 10
  retransmit 5 key green
Console(config)#
```

tacacs-server key

This command sets the TACACS+ encryption key. Use the **no** form to restore the default.

SYNTAX

tacacs-server key *key-string*

no tacacs-server key

key-string - Encryption key used to authenticate logon access for the client. Do not use blank spaces in the string.
(Maximum length: 48 characters)

DEFAULT SETTING

None

COMMAND MODE

Global Configuration

EXAMPLE

```
Console(config)#tacacs-server key green
Console(config)#
```

tacacs-server port

This command specifies the TACACS+ server network port. Use the **no** form to restore the default.

SYNTAX

tacacs-server port *port-number*

no tacacs-server port

port-number - TACACS+ server TCP port used for authentication messages. (Range: 1-65535)

DEFAULT SETTING

49

COMMAND MODE

Global Configuration

EXAMPLE

```
Console(config)#tacacs-server port 181
Console(config)#
```

tacacs-server retransmit

This command sets the number of retries. Use the **no** form to restore the default.

SYNTAX

tacacs-server retransmit *number-of-retries*

no tacacs-server retransmit

number-of-retries - Number of times the switch will try to authenticate logon access via the TACACS+ server. (Range: 1 - 30)

DEFAULT SETTING

2

COMMAND MODE

Global Configuration

EXAMPLE

```
Console(config)#tacacs-server retransmit 5
Console(config)#
```

tacacs-server timeout

This command sets the interval between transmitting authentication requests to the TACACS+ server. Use the **no** form to restore the default.

SYNTAX

tacacs-server timeout *number-of-seconds*

no tacacs-server timeout

number-of-seconds - Number of seconds the switch waits for a reply before resending a request. (Range: 1-540)

DEFAULT SETTING

5

COMMAND MODE

Global Configuration

EXAMPLE

```
Console(config)#tacacs-server timeout 10
Console(config)#
```

show tacacs-server

This command displays the current settings for the TACACS+ server.

DEFAULT SETTING

None

COMMAND MODE

Privileged Exec

EXAMPLE

```
Console#show tacacs-server

Remote TACACS+ Server Configuration:

Global Settings:
 Server Port Number : 49
 Retransmit Times   : 2
 Timeout            : 5

Server 1:
 Server IP Address  : 10.11.12.13
 Server Port Number : 49
 Retransmit Times   : 2
 Timeout            : 4
```

```
TACACS+ Server Group:
Group Name                Member Index
------------------------- -------------
tacacs+                   1

Console#
```

AAA

The Authentication, Authorization, and Accounting (AAA) feature provides the main framework for configuring access control on the switch. The AAA functions require the use of configured RADIUS or TACACS+ servers in the network.

Table 102: AAA Commands

Command	Function	Mode
aaa accounting dot1x	Enables accounting of 802.1X services	GC
aaa accounting exec	Enables accounting of Exec services	GC
aaa accounting update	Enables periodoc updates to be sent to the accounting server	GC
aaa authorization exec	Enables authorization of Exec sessions	GC
aaa group server	Groups security servers in to defined lists	GC
server	Configures the IP address of a server in a group list	SG
accounting dot1x	Applies an accounting method to an interface for 802.1X service requests	IC
accounting exec	Applies an accounting method to local console, Telnet or SSH connections	Line
authorization exec	Applies an authorization method to local console, Telnet or SSH connections	Line
show accounting	Displays all accounting information	PE

aaa accounting dot1x

This command enables the accounting of requested 802.1X services for network access. Use the **no** form to disable the accounting service.

SYNTAX

aaa accounting dot1x {**default** | *method-name*}
start-stop group {**radius** | **tacacs+** |*server-group*}

no aaa accounting dot1x {**default** | *method-name*}

default - Specifies the default accounting method for service requests.

method-name - Specifies an accounting method for service requests. (Range: 1-64 characters)

start-stop - Records accounting from starting point and stopping point.

group - Specifies the server group to use.

radius - Specifies all RADIUS hosts configure with the radius-server host command.

tacacs+ - Specifies all TACACS+ hosts configure with the tacacs-server host command.

server-group - Specifies the name of a server group configured with the aaa group server command. (Range: 1-64 characters)

DEFAULT SETTING

Accounting is not enabled
No servers are specified

COMMAND MODE

Global Configuration

COMMAND USAGE

Note that the **default** and *method-name* fields are only used to describe the accounting method(s) configured on the specified RADIUS or TACACS+ servers, and do not actually send any information to the servers about the methods to use.

EXAMPLE

```
Console(config)#aaa accounting dot1x default start-stop group radius
Console(config)#
```

aaa accounting exec

This command enables the accounting of requested Exec services for network access. Use the **no** form to disable the accounting service.

SYNTAX

aaa accounting exec {**default** | *method-name*}
start-stop group {**radius** | **tacacs+** |*server-group*}

no aaa accounting exec {**default** | *method-name*}

default - Specifies the default accounting method for service requests.

method-name - Specifies an accounting method for service requests. (Range: 1-255 characters)

start-stop - Records accounting from starting point and stopping point.

group - Specifies the server group to use.

radius - Specifies all RADIUS hosts configure with the radius-server host command.

tacacs+ - Specifies all TACACS+ hosts configure with the tacacs-server host command.

server-group - Specifies the name of a server group configured with the aaa group server command. (Range: 1-64 characters)

DEFAULT SETTING

Accounting is not enabled
No servers are specified

COMMAND MODE

Global Configuration

COMMAND USAGE

- This command runs accounting for Exec service requests for the local console and Telnet connections.
- Note that the **default** and *method-name* fields are only used to describe the accounting method(s) configured on the specified RADIUS or TACACS+ servers, and do not actually send any information to the servers about the methods to use.

EXAMPLE

```
Console(config)#aaa accounting exec default start-stop group tacacs+
Console(config)#
```

aaa accounting update

This command enables the sending of periodic updates to the accounting server. Use the **no** form to disable accounting updates.

SYNTAX

aaa accounting update [**periodic** *interval*]

no aaa accounting update

interval - Sends an interim accounting record to the server at this interval. (Range: 1-2147483647 minutes)

DEFAULT SETTING

1 minute

COMMAND MODE

Global Configuration

COMMAND USAGE

- When accounting updates are enabled, the switch issues periodic interim accounting records for all users on the system.

- Using the command without specifying an interim interval enables updates, but does not change the current interval setting.

EXAMPLE

```
Console(config)#aaa accounting update periodic 30
Console(config)#
```

aaa authorization exec

This command enables the authorization for Exec access. Use the **no** form to disable the authorization service.

SYNTAX

aaa authorization exec {**default** | *method-name*}
  group {**tacacs+** | *server-group*}

no aaa authorization exec {**default** | *method-name*}

default - Specifies the default authorization method for Exec access.

method-name - Specifies an authorization method for Exec access. (Range: 1-64 characters)

group - Specifies the server group to use.

tacacs+ - Specifies all TACACS+ hosts configured with the tacacs-server host command.

server-group - Specifies the name of a server group configured with the aaa group server command. (Range: 1-64 characters)

DEFAULT SETTING

Authorization is not enabled
No servers are specified

COMMAND MODE

Global Configuration

COMMAND USAGE

- This command performs authorization to determine if a user is allowed to run an Exec shell.

- AAA authentication must be enabled before authorization is enabled.

- If this command is issued without a specified named method, the default method list is applied to all interfaces or lines (where this authorization type applies), except those that have a named method explicitly defined.

EXAMPLE

```
Console(config)#aaa authorization exec default group tacacs+
Console(config)#
```

aaa group server

Use this command to name a group of security server hosts. To remove a server group from the configuration list, enter the **no** form of this command.

SYNTAX

[**no**] **aaa group server** {**radius** | **tacacs+**} *group-name*

radius - Defines a RADIUS server group.

tacacs+ - Defines a TACACS+ server group.

group-name - A text string that names a security server group. (Range: 1-64 characters)

DEFAULT SETTING

None

COMMAND MODE

Global Configuration

EXAMPLE

```
Console(config)#aaa group server radius tps
Console(config-sg-radius)#
```

server

This command adds a security server to an AAA server group. Use the **no** form to remove the associated server from the group.

SYNTAX

[**no**] **server** {*index* | *ip-address*}

index - Specifies the server index.
(Range: RADIUS 1-5, TACACS+ 1)

ip-address - Specifies the host IP address of a server.

DEFAULT SETTING

None

COMMAND MODE

Server Group Configuration

COMMAND USAGE

- When specifying the index for a RADIUS server, that server index must already be defined by the radius-server host command.

- When specifying the index for a TACACS+ server, that server index must already be defined by the tacacs-server host command.

EXAMPLE

```
Console(config)#aaa group server radius tps
Console(config-sg-radius)#server 10.2.68.120
Console(config-sg-radius)#
```

accounting dot1x

This command applies an accounting method for 802.1X service requests on an interface. Use the **no** form to disable accounting on the interface.

SYNTAX

accounting dot1x {**default** | *list-name*}

no accounting dot1x

default - Specifies the default method list created with the aaa accounting dot1x command.

list-name - Specifies a method list created with the aaa accounting dot1x command.

DEFAULT SETTING

None

COMMAND MODE

Interface Configuration

EXAMPLE

```
Console(config)#interface ethernet 1/2
Console(config-if)#accounting dot1x tps
Console(config-if)#
```

accounting exec

This command applies an accounting method to local console, Telnet or SSH connections. Use the **no** form to disable accounting on the line.

SYNTAX

accounting exec {**default** | *list-name*}

no accounting exec

default - Specifies the default method list created with the aaa accounting exec command.

list-name - Specifies a method list created with the aaa accounting exec command.

DEFAULT SETTING

None

COMMAND MODE

Line Configuration

EXAMPLE

```
Console(config)#line console
Console(config-line)#accounting exec tps
Console(config-line)#exit
Console(config)#line vty
Console(config-line)#accounting exec default
Console(config-line)#
```

authorization exec

This command applies an authorization method to local console, Telnet or SSH connections. Use the **no** form to disable authorization on the line.

SYNTAX

authorization exec {**default** | *list-name*}
no authorization exec

default - Specifies the default method list created with the aaa authorization exec command.

list-name - Specifies a method list created with the aaa authorization exec command.

DEFAULT SETTING

None

COMMAND MODE

Line Configuration

EXAMPLE

```
Console(config)#line console
Console(config-line)#authorization exec tps
Console(config-line)#exit
Console(config)#line vty
Console(config-line)#authorization exec default
Console(config-line)#
```

show accounting

This command displays the current accounting settings per function and per port.

SYNTAX

show accounting [**commands** [*level*]] |
[[**dot1x** [**statistics** [**username** *user-name* | **interface** *interface*]]
| **exec** [**statistics**] | **statistics**]

commands - Displays command accounting information.

level - Displays command accounting information for a specifiable command level.

dot1x - Displays dot1x accounting information.

exec - Displays Exec accounting records.

statistics - Displays accounting records.

user-name - Displays accounting records for a specifiable username.

interface

ethernet *unit/port*

unit - Unit identifier. (Range: 1)

port - Port number. (Range: 1-28)

DEFAULT SETTING

None

COMMAND MODE

Privileged Exec

EXAMPLE

```
Console#show accounting
Accounting Type : dot1x
  Method List   : default
  Group List    : radius
  Interface     : Eth 1/1

  Method List   : tps
  Group List    : radius
  Interface     : Eth 1/2

Accounting Type : EXEC
  Method List   : default
  Group List    : tacacs+
  Interface     : vty

Console#
```

WEB SERVER

This section describes commands used to configure web browser management access to the switch.

Table 103: Web Server Commands

Command	Function	Mode
ip http port	Specifies the port to be used by the web browser interface	GC
ip http server	Allows the switch to be monitored or configured from a browser	GC
ip http secure-port	Specifies the UDP port number for HTTPS	GC
ip http secure-server	Enables HTTPS (HTTP/SSL) for encrypted communications	GC

ip http port

This command specifies the TCP port number used by the web browser interface. Use the **no** form to use the default port.

SYNTAX

ip http port *port-number*

no ip http port

port-number - The TCP port to be used by the browser interface. (Range: 1-65535)

DEFAULT SETTING

80

COMMAND MODE

Global Configuration

EXAMPLE

```
Console(config)#ip http port 769
Console(config)#
```

RELATED COMMANDS

ip http server (1052)
show system (906)

ip http server

This command allows this device to be monitored or configured from a browser. Use the **no** form to disable this function.

SYNTAX

[**no**] **ip http server**

DEFAULT SETTING

Enabled

COMMAND MODE

Global Configuration

EXAMPLE

```
Console(config)#ip http server
Console(config)#
```

RELATED COMMANDS

ip http port (1052)
show system (906)

ip http secure-port

This command specifies the UDP port number used for HTTPS connection to the switch's web interface. Use the **no** form to restore the default port.

SYNTAX

ip http secure-port *port_number*

no ip http secure-port

port_number – The UDP port used for HTTPS. (Range: 1-65535)

DEFAULT SETTING

443

COMMAND MODE

Global Configuration

COMMAND USAGE

- You cannot configure the HTTP and HTTPS servers to use the same port.
- If you change the HTTPS port number, clients attempting to connect to the HTTPS server must specify the port number in the URL, in this format: **https://***device***:***port_number*

EXAMPLE

```
Console(config)#ip http secure-port 1000
Console(config)#
```

RELATED COMMANDS

ip http secure-server (1053)
show system (906)

ip http secure-server

This command enables the secure hypertext transfer protocol (HTTPS) over the Secure Socket Layer (SSL), providing secure access (i.e., an encrypted connection) to the switch's web interface. Use the **no** form to disable this function.

SYNTAX

[**no**] **ip http secure-server**

DEFAULT SETTING

Enabled

COMMAND MODE

Global Configuration

COMMAND USAGE

- Both HTTP and HTTPS service can be enabled independently on the switch. However, you cannot configure the HTTP and HTTPS servers to use the same UDP port.

- If you enable HTTPS, you must indicate this in the URL that you specify in your browser: **https**://*device*[:*port_number*]

- When you start HTTPS, the connection is established in this way:

  - The client authenticates the server using the server's digital certificate.

  - The client and server negotiate a set of security protocols to use for the connection.

  - The client and server generate session keys for encrypting and decrypting data.

- The client and server establish a secure encrypted connection.

  A padlock icon should appear in the status bar for Internet Explorer 6, Mozilla Firefox 4, or Google Chrome 29, or more recent versions.

  The following web browsers and operating systems currently support HTTPS:

Table 104: HTTPS System Support

Web Browser	Operating System
Internet Explorer 6.x or later	Windows 98,Windows NT (with service pack 6a), Windows 2000, XP, Vista, 7, 8
Mozilla Firefox 4 or later	Windows 2000, XP, Vista, 7, 8, Linux
Google Chrome 29 or later	Windows XP, Vista, 7, 8

- To specify a secure-site certificate, see "Replacing the Default Secure-site Certificate" on page 380. Also refer to the copy tftp https-certificate command.

EXAMPLE

```
Console(config)#ip http secure-server
Console(config)#
```

RELATED COMMANDS

ip http secure-port (1053)
copy tftp https-certificate (914)
show system (906)

TELNET SERVER

This section describes commands used to configure Telnet management access to the switch.

Table 105: Telnet Server Commands

Command	Function	Mode
ip telnet max-sessions	Specifies the maximum number of Telnet sessions that can simultaneously connect to this system	GC
ip telnet port	Specifies the port to be used by the Telnet interface	GC
ip telnet server	Allows the switch to be monitored or configured from Telnet	GC
show ip telnet	Displays configuration settings for the Telnet server	PE

NOTE: This switch also supports a Telnet client function. A Telnet connection can be made from this switch to another device by entering the **telnet** command at the Privileged Exec configuration level.

ip telnet max-sessions

This command specifies the maximum number of Telnet sessions that can simultaneously connect to this system. Use the **no** from to restore the default setting.

SYNTAX

ip telnet max-sessions *session-count*

no ip telnet max-sessions

session-count - The maximum number of allowed Telnet session. (Range: 0-8)

DEFAULT SETTING

4 sessions

COMMAND MODE

Global Configuration

COMMAND USAGE

A maximum of eight sessions can be concurrently opened for Telnet and Secure Shell (i.e., both Telnet and SSH share a maximum number or eight sessions).

EXAMPLE

```
Console(config)#ip telnet max-sessions 1
Console(config)#
```

ip telnet port

This command specifies the TCP port number used by the Telnet interface. Use the **no** form to use the default port.

SYNTAX

ip telnet port *port-number*

no telnet port

port-number - The TCP port number to be used by the browser interface. (Range: 1-65535)

DEFAULT SETTING

23

COMMAND MODE

Global Configuration

EXAMPLE

```
Console(config)#ip telnet port 123
Console(config)#
```

ip telnet server

This command allows this device to be monitored or configured from Telnet. Use the **no** form to disable this function.

SYNTAX

[**no**] **ip telnet server**

DEFAULT SETTING

Enabled

COMMAND MODE

Global Configuration

EXAMPLE

```
Console(config)#ip telnet server
Console(config)#
```

show ip telnet

This command displays the configuration settings for the Telnet server.

COMMAND MODE

Normal Exec, Privileged Exec

EXAMPLE

```
Console#show ip telnet
IP Telnet Configuration:

Telnet Status: Enabled
Telnet Service Port: 23
Telnet Max Session: 4
Console#
```

SECURE SHELL

This section describes the commands used to configure the SSH server. Note that you also need to install a SSH client on the management station when using this protocol to configure the switch.

NOTE: The switch supports both SSH Version 1.5 and 2.0 clients.

Table 106: Secure Shell Commands

Command	Function	Mode
ip ssh authentication-retries	Specifies the number of retries allowed by a client	GC
ip ssh server	Enables the SSH server on the switch	GC
ip ssh server-key size	Sets the SSH server key size	GC
ip ssh timeout	Specifies the authentication timeout for the SSH server	GC
copy tftp public-key	Copies the user's public key from a TFTP server to the switch	PE
delete public-key	Deletes the public key for the specified user	PE
disconnect	Terminates a line connection	PE
ip ssh crypto host-key generate	Generates the host key	PE
ip ssh crypto zeroize	Clear the host key from RAM	PE
ip ssh save host-key	Saves the host key from RAM to flash memory	PE
show ip ssh	Displays the status of the SSH server and the configured values for authentication timeout and retries	PE
show public-key	Shows the public key for the specified user or for the host	PE

Table 106: Secure Shell Commands (Continued)

Command	Function	Mode
show ssh	Displays the status of current SSH sessions	PE
show users	Shows SSH users, including privilege level and public key type	PE

Configuration Guidelines

The SSH server on this switch supports both password and public key authentication. If password authentication is specified by the SSH client, then the password can be authenticated either locally or via a RADIUS or TACACS+ remote authentication server, as specified by the authentication login command. If public key authentication is specified by the client, then you must configure authentication keys on both the client and the switch as described in the following section. Note that regardless of whether you use public key or password authentication, you still have to generate authentication keys on the switch and enable the SSH server.

To use the SSH server, complete these steps:

1. Generate a Host Key Pair – Use the ip ssh crypto host-key generate command to create a host public/private key pair.

2. Provide Host Public Key to Clients – Many SSH client programs automatically import the host public key during the initial connection setup with the switch. Otherwise, you need to manually create a known hosts file on the management station and place the host public key in it. An entry for a public key in the known hosts file would appear similar to the following example:

   ```
   10.1.0.54 1024 35
   15684995401867669259333946775054617325313674890836547254
   15020245593199868544358361651999923329781766065830956
   10825913212890233765468017262725714134287629413011961955667825
   95664104869574278881462065194174677298486546861571773939016477
   93559423035774130980227370877945452408397175264635805817671670
   9574804776117
   ```

3. Import Client's Public Key to the Switch – Use the copy tftp public-key command to copy a file containing the public key for all the SSH client's granted management access to the switch. (Note that these clients must be configured locally on the switch with the username command.) The clients are subsequently authenticated using these keys. The current firmware only accepts public key files based on standard UNIX format as shown in the following example for an RSA key:

   ```
   1024 35
   13410816856098939210409449201554253476316419218729589211431738
   80055536161631051775940838686311092912322268285192543746031009
   37187721199696317813662774141689851320491172048303392543241016
   37997592371449011938006090253948408482717819437228840253311595
   2134861022902978982721353267131629432532818915045306393916643
   steve@192.168.1.19
   ```

4. Set the Optional Parameters – Set other optional parameters, including the authentication timeout, the number of retries, and the server key size.

5. Enable SSH Service – Use the ip ssh server command to enable the SSH server on the switch.

6. *Authentication* – One of the following authentication methods is employed:

   Password Authentication (for SSH v1.5 or V2 Clients)

   a. The client sends its password to the server.
   b. The switch compares the client's password to those stored in memory.
   c. If a match is found, the connection is allowed.

NOTE: To use SSH with only password authentication, the host public key must still be given to the client, either during initial connection or manually entered into the known host file. However, you do not need to configure the client's keys.

Public Key Authentication – When an SSH client attempts to contact the switch, the SSH server uses the host key pair to negotiate a session key and encryption method. Only clients that have a private key corresponding to the public keys stored on the switch can access it. The following exchanges take place during this process:

Authenticating SSH v1.5 Clients

a. The client sends its RSA public key to the switch.
b. The switch compares the client's public key to those stored in memory.
c. If a match is found, the switch uses its secret key to generate a random 256-bit string as a challenge, encrypts this string with the user’s public key, and sends it to the client.
d. The client uses its private key to decrypt the challenge string, computes the MD5 checksum, and sends the checksum back to the switch.
e. The switch compares the checksum sent from the client against that computed for the original string it sent. If the two check sums match, this means that the client's private key corresponds to an authorized public key, and the client is authenticated.

Authenticating SSH v2 Clients

a. The client first queries the switch to determine if DSA public key authentication using a preferred algorithm is acceptable.
b. If the specified algorithm is supported by the switch, it notifies the client to proceed with the authentication process. Otherwise, it rejects the request.

c. The client sends a signature generated using the private key to the switch.

d. When the server receives this message, it checks whether the supplied key is acceptable for authentication, and if so, it then checks whether the signature is correct. If both checks succeed, the client is authenticated.

NOTE: The SSH server supports up to four client sessions. The maximum number of client sessions includes both current Telnet sessions and SSH sessions.

NOTE: The SSH server can be accessed using any configured IPv4 or IPv6 interface address on the switch.

ip ssh authentication-retries

This command configures the number of times the SSH server attempts to reauthenticate a user. Use the **no** form to restore the default setting.

SYNTAX

ip ssh authentication-retries *count*

no ip ssh authentication-retries

count – The number of authentication attempts permitted after which the interface is reset. (Range: 1-5)

DEFAULT SETTING

3

COMMAND MODE

Global Configuration

EXAMPLE

```
Console(config)#ip ssh authentication-retires 2
Console(config)#
```

RELATED COMMANDS

show ip ssh (1065)

ip ssh server

This command enables the Secure Shell (SSH) server on this switch. Use the **no** form to disable this service.

SYNTAX

[**no**] **ip ssh server**

DEFAULT SETTING

Disabled

COMMAND MODE

Global Configuration

COMMAND USAGE

- The SSH server supports up to four client sessions. The maximum number of client sessions includes both current Telnet sessions and SSH sessions.
- The SSH server uses DSA or RSA for key exchange when the client first establishes a connection with the switch, and then negotiates with the client to select either DES (56-bit) or 3DES (168-bit) for data encryption.
- You must generate DSA and RSA host keys before enabling the SSH server.

EXAMPLE

```
Console#ip ssh crypto host-key generate dsa
Console#configure
Console(config)#ip ssh server
Console(config)#
```

RELATED COMMANDS

ip ssh crypto host-key generate (1063)
show ssh (1066)

ip ssh server-key size

This command sets the SSH server key size. Use the **no** form to restore the default setting.

SYNTAX

ip ssh server-key size *key-size*

no ip ssh server-key size

key-size – The size of server key. (Range: 512-896 bits)

DEFAULT SETTING

768 bits

COMMAND MODE

Global Configuration

COMMAND USAGE

The server key is a private key that is never shared outside the switch. The host key is shared with the SSH client, and is fixed at 1024 bits.

EXAMPLE

```
Console(config)#ip ssh server-key size 512
Console(config)#
```

ip ssh timeout

This command configures the timeout for the SSH server. Use the **no** form to restore the default setting.

SYNTAX

ip ssh timeout *seconds*

no ip ssh timeout

seconds – The timeout for client response during SSH negotiation. (Range: 1-120)

DEFAULT SETTING

10 seconds

COMMAND MODE

Global Configuration

COMMAND USAGE

The **timeout** specifies the interval the switch will wait for a response from the client during the SSH negotiation phase. Once an SSH session has been established, the timeout for user input is controlled by the exec-timeout command for vty sessions.

EXAMPLE

```
Console(config)#ip ssh timeout 60
Console(config)#
```

RELATED COMMANDS

exec-timeout (925)
show ip ssh (1065)

delete public-key

This command deletes the specified user's public key.

SYNTAX

delete public-key *username* [**dsa** | **rsa**]

username – Name of an SSH user. (Range: 1-8 characters)

dsa – DSA public key type.

rsa – RSA public key type.

DEFAULT SETTING

Deletes both the DSA and RSA key.

COMMAND MODE

Privileged Exec

EXAMPLE

```
Console#delete public-key admin dsa
Console#
```

ip ssh crypto host-key generate

This command generates the host key pair (i.e., public and private).

SYNTAX

ip ssh crypto host-key generate [**dsa** | **rsa**]

dsa – DSA (Version 2) key type.

rsa – RSA (Version 1) key type.

DEFAULT SETTING

Generates both the DSA and RSA key pairs.

COMMAND MODE

Privileged Exec

COMMAND USAGE

- The switch uses only RSA Version 1 for SSHv1.5 clients and DSA Version 2 for SSHv2 clients.

- This command stores the host key pair in memory (i.e., RAM). Use the ip ssh save host-key command to save the host key pair to flash memory.

- Some SSH client programs automatically add the public key to the known hosts file as part of the configuration process. Otherwise, you must manually create a known hosts file and place the host public key in it.

- The SSH server uses this host key to negotiate a session key and encryption method with the client trying to connect to it.

EXAMPLE

```
Console#ip ssh crypto host-key generate dsa
Console#
```

RELATED COMMANDS

ip ssh crypto zeroize (1064)
ip ssh save host-key (1064)

ip ssh crypto zeroize

This command clears the host key from memory (i.e. RAM).

SYNTAX

ip ssh crypto zeroize [**dsa** | **rsa**]

dsa – DSA key type.

rsa – RSA key type.

DEFAULT SETTING

Clears both the DSA and RSA key.

COMMAND MODE

Privileged Exec

COMMAND USAGE

- This command clears the host key from volatile memory (RAM). Use the **no** ip ssh save host-key command to clear the host key from flash memory.
- The SSH server must be disabled before you can execute this command.

EXAMPLE

```
Console#ip ssh crypto zeroize dsa
Console#
```

RELATED COMMANDS

ip ssh crypto host-key generate (1063)
ip ssh save host-key (1064)
no ip ssh server (1060)

ip ssh save host-key

This command saves the host key from RAM to flash memory.

SYNTAX

ip ssh save host-key

DEFAULT SETTING

Saves both the DSA and RSA key.

COMMAND MODE

Privileged Exec

EXAMPLE

```
Console#ip ssh save host-key dsa
Console#
```

RELATED COMMANDS

ip ssh crypto host-key generate (1063)

show ip ssh

This command displays the connection settings used when authenticating client access to the SSH server.

COMMAND MODE

Privileged Exec

EXAMPLE

```
Console#show ip ssh
SSH Enabled - Version 2.0
Negotiation Timeout : 120 seconds; Authentication Retries : 3
Server Key Size     : 768 bits
Console#
```

show public-key

This command shows the public key for the specified user or for the host.

SYNTAX

show public-key [**user** [*username*]| **host**]

username – Name of an SSH user. (Range: 1-8 characters)

DEFAULT SETTING

Shows all public keys.

COMMAND MODE

Privileged Exec

COMMAND USAGE

- If no parameters are entered, all keys are displayed. If the user keyword is entered, but no user name is specified, then the public keys for all users are displayed.

- When an RSA key is displayed, the first field indicates the size of the host key (e.g., 1024), the second field is the encoded public exponent (e.g., 35), and the last string is the encoded modulus. When a DSA key is displayed, the first field indicates that the encryption method used by SSH is based on the Digital Signature Standard (DSS), and the last string is the encoded modulus.

EXAMPLE

```
Console#show public-key host
Host:
RSA:
1024 65537 13236940658254764031382795526536375927835525327972629521130241
  071942106165575942459093923609695405036277525755625100386613098939383452310
  332802149888661921595568598879891919505883940181387440468908779160305837768
  185490002831341625008348718449522087429212255691665655296328163516964040831
  5547660664151657116381
DSA:
ssh-dss AAAB3NzaC1kc3MAAACBAPWKZTPbsRIB8ydEXcxM3dyV/yrDbKStIlnzD/Dg0h2Hxc
  YV44sXZ2JXhamLK6P8bvuiyacWbUW/a4PAtp1KMSdqsKeh3hKoA3vRRSy1N2XFfAKxl5fwFfv
  JlPdOkFgzLGMinvSNYQwiQXbKTBH0Z4mUZpE85PWxDZMaCNBPjBrRAAAAFQChb4vsdfQGNIjwbv
  wrNLaQ77isiwAAAIEAsy5YWDC99ebYHNRj5kh47wY4i8cZvH+/p9cnrfwFTMU01VFDly3IR
  2G395NLy5Qd7ZDxfA9mCOfT/yyEfbobMJZi8oGCstSNOxrZZVnMqWrTYfdrKX7YKBw/Kjw6Bm
  iFq7O+jAhf1Dg45loAc27s6TLdtny1wRq/ow2eTCD5nekAAACBAJ8rMccXTxHLFAczWS7EjOy
  DbsloBfPuSAb4oAsyjKXKVYNLQkTLZfcFRu41bS2KV5LAwecsigF/+DjKGWtPNIQqabKgYCw2
  o/dVzX4Gg+yqdTlYmGA7fHGm8ARGeiG4ssFKy4Z6DmYPXFum1Yg0fhLwuHpOSKdxT3kk475S7
  w0W
Console#
```

show ssh

This command displays the current SSH server connections.

COMMAND MODE

Privileged Exec

EXAMPLE

```
Console#show ssh
Connection Version State               Username Encryption
  0          2.0   Session-Started      admin    ctos aes128-cbc-hmac-md5
                                                stoc aes128-cbc-hmac-md5
Console#
```

Table 107: show ssh - display description

Field	Description
Session	The session number. (Range: 0-3)
Version	The Secure Shell version number.
State	The authentication negotiation state. (Values: Negotiation-Started, Authentication-Started, Session-Started)
Username	The user name of the client.

802.1X PORT AUTHENTICATION

The switch supports IEEE 802.1X (dot1x) port-based access control that prevents unauthorized access to the network by requiring users to first submit credentials for authentication. Client authentication is controlled centrally by a RADIUS server using EAP (Extensible Authentication Protocol).

Table 108: 802.1X Port Authentication Commands

Command	Function	Mode
General Commands		
dot1x default	Resets all dot1x parameters to their default values	GC
dot1x eapol-pass-through	Passes EAPOL frames to all ports in STP forwarding state when dot1x is globally disabled	GC
dot1x system-auth-control	Enables dot1x globally on the switch.	GC
Authenticator Commands		
dot1x intrusion-action	Sets the port response to intrusion when authentication fails	IC
dot1x max-reauth-req	Sets the maximum number of times that the switch sends an EAP-request/identity frame to the client before restarting the authentication process	IC
dot1x max-req	Sets the maximum number of times that the switch retransmits an EAP request/identity packet to the client before it times out the authentication session	IC
dot1x operation-mode	Allows single or multiple hosts on an dot1x port	IC
dot1x port-control	Sets dot1x mode for a port interface	IC
dot1x re-authentication	Enables re-authentication for all ports	IC
dot1x timeout quiet-period	Sets the time that a switch port waits after the Max Request Count has been exceeded before attempting to acquire a new client	IC
dot1x timeout re-authperiod	Sets the time period after which a connected client must be re-authenticated	IC
dot1x timeout supp-timeout	Sets the interval for a supplicant to respond	IC
dot1x timeout tx-period	Sets the time period during an authentication session that the switch waits before re-transmitting an EAP packet	IC
dot1x re-authenticate	Forces re-authentication on specific ports	PE
Display Information Commands		
show dot1x	Shows all dot1x related information	PE

General Commands

dot1x default

This command sets all configurable dot1x global and port settings to their default values.

COMMAND MODE

Global Configuration

EXAMPLE

```
Console(config)#dot1x default
Console(config)#
```

dot1x eapol-pass-through

This command passes EAPOL frames through to all ports in STP forwarding state when dot1x is globally disabled. Use the **no** form to restore the default.

SYNTAX

[**no**] **dot1x eapol-pass-through**

DEFAULT SETTING

Discards all EAPOL frames when dot1x is globally disabled

COMMAND MODE

Global Configuration

COMMAND USAGE

- When this device is functioning as intermediate node in the network and does not need to perform dot1x authentication, the **dot1x eapol pass-through** command can be used to forward EAPOL frames from other switches on to the authentication servers, thereby allowing the authentication process to still be carried out by switches located on the edge of the network.

- When this device is functioning as an edge switch but does not require any attached clients to be authenticated, the **no dot1x eapol-pass-through** command can be used to discard unnecessary EAPOL traffic.

EXAMPLE

This example instructs the switch to pass all EAPOL frame through to any ports in STP forwarding state.

```
Console(config)#dot1x eapol-pass-through
Console(config)#
```

dot1x system-auth-control

This command enables IEEE 802.1X port authentication globally on the switch. Use the **no** form to restore the default.

SYNTAX

[**no**] **dot1x system-auth-control**

DEFAULT SETTING

Disabled

COMMAND MODE

Global Configuration

EXAMPLE

```
Console(config)#dot1x system-auth-control
Console(config)#
```

Authenticator Commands

dot1x intrusion-action

This command sets the port's response to a failed authentication, either to block all traffic, or to assign all traffic for the port to a guest VLAN. Use the **no** form to reset the default.

SYNTAX

dot1x intrusion-action {**block-traffic** | **guest-vlan**}

no dot1x intrusion-action

block-traffic - Blocks traffic on this port.

guest-vlan - Assigns the user to the Guest VLAN.

DEFAULT

block-traffic

COMMAND MODE

Interface Configuration

COMMAND USAGE

For guest VLAN assignment to be successful, the VLAN must be configured and set as active (see the vlan database command) and assigned as the guest VLAN for the port (see the network-access guest-vlan command).

EXAMPLE

```
Console(config)#interface eth 1/2
Console(config-if)#dot1x intrusion-action guest-vlan
Console(config-if)#
```

dot1x max-reauth-req

This command sets the maximum number of times that the switch sends an EAP-request/identity frame to the client before restarting the authentication process. Use the **no** form to restore the default.

SYNTAX

dot1x max-reauth-req *count*

no dot1x max-reauth-req

count – The maximum number of requests (Range: 1-10)

DEFAULT

2

COMMAND MODE

Interface Configuration

EXAMPLE

```
Console(config)#interface eth 1/2
Console(config-if)#dot1x max-reauth-req 2
Console(config-if)#
```

dot1x max-req

This command sets the maximum number of times the switch port will retransmit an EAP request/identity packet to the client before it times out the authentication session. Use the **no** form to restore the default.

SYNTAX

dot1x max-req *count*

no dot1x max-req

count – The maximum number of requests (Range: 1-10)

DEFAULT

2

COMMAND MODE

Interface Configuration

EXAMPLE

```
Console(config)#interface eth 1/2
Console(config-if)#dot1x max-req 2
Console(config-if)#
```

dot1x operation-mode

This command allows hosts (clients) to connect to an 802.1X-authorized port. Use the **no** form with no keywords to restore the default to single host. Use the **no** form with the **multi-host max-count** keywords to restore the default maximum count.

SYNTAX

dot1x operation-mode {**single-host** |
multi-host [**max-count** *count*] | **mac-based-auth**}

no dot1x operation-mode [**multi-host max-count**]

single-host – Allows only a single host to connect to this port.

multi-host – Allows multiple host to connect to this port.

max-count – Keyword for the maximum number of hosts.

count – The maximum number of hosts that can connect to a port. (Range: 1-1024; Default: 5)

mac-based – Allows multiple hosts to connect to this port, with each host needing to be authenticated.

DEFAULT

Single-host

COMMAND MODE

Interface Configuration

COMMAND USAGE

- The "max-count" parameter specified by this command is only effective if the dot1x mode is set to "auto" by the dot1x port-control command.
- In "multi-host" mode, only one host connected to a port needs to pass authentication for all other hosts to be granted network access. Similarly, a port can become unauthorized for all hosts if one attached host fails re-authentication or sends an EAPOL logoff message.
- In "mac-based-auth" mode, each host connected to a port needs to pass authentication. The number of hosts allowed access to a port operating in this mode is limited only by the available space in the secure address table (i.e., up to 1024 addresses).

EXAMPLE

```
Console(config)#interface eth 1/2
Console(config-if)#dot1x operation-mode multi-host max-count 10
Console(config-if)#
```

dot1x port-control

This command sets the dot1x mode on a port interface. Use the **no** form to restore the default.

SYNTAX

dot1x port-control {**auto** | **force-authorized** | **force-unauthorized**}

no dot1x port-control

auto – Requires a dot1x-aware connected client to be authorized by the RADIUS server. Clients that are not dot1x-aware will be denied access.

force-authorized – Configures the port to grant access to all clients, either dot1x-aware or otherwise.

force-unauthorized – Configures the port to deny access to all clients, either dot1x-aware or otherwise.

DEFAULT

force-authorized

COMMAND MODE

Interface Configuration

EXAMPLE

```
Console(config)#interface eth 1/2
Console(config-if)#dot1x port-control auto
Console(config-if)#
```

dot1x re-authentication

This command enables periodic re-authentication for a specified port. Use the **no** form to disable re-authentication.

SYNTAX

[**no**] **dot1x re-authentication**

COMMAND MODE

Interface Configuration

COMMAND USAGE

- The re-authentication process verifies the connected client’s user ID and password on the RADIUS server. During re-authentication, the client remains connected the network and the process is handled transparently by the dot1x client software. Only if re-authentication fails is the port blocked.

- The connected client is re-authenticated after the interval specified by the dot1x timeout re-authperiod command. The default is 3600 seconds.

EXAMPLE

```
Console(config)#interface eth 1/2
Console(config-if)#dot1x re-authentication
Console(config-if)#
```

RELATED COMMANDS

dot1x timeout re-authperiod (1073)

dot1x timeout quiet-period

This command sets the time that a switch port waits after the maximum request count (see page 1070) has been exceeded before attempting to acquire a new client. Use the **no** form to reset the default.

SYNTAX

dot1x timeout quiet-period *seconds*

no dot1x timeout quiet-period

seconds - The number of seconds. (Range: 1-65535)

DEFAULT

60 seconds

COMMAND MODE

Interface Configuration

EXAMPLE

```
Console(config)#interface eth 1/2
Console(config-if)#dot1x timeout quiet-period 350
Console(config-if)#
```

dot1x timeout re-authperiod

This command sets the time period after which a connected client must be re-authenticated. Use the **no** form of this command to reset the default.

SYNTAX

dot1x timeout re-authperiod *seconds*

no dot1x timeout re-authperiod

seconds - The number of seconds. (Range: 1-65535)

DEFAULT

3600 seconds

COMMAND MODE

Interface Configuration

EXAMPLE

```
Console(config)#interface eth 1/2
Console(config-if)#dot1x timeout re-authperiod 300
Console(config-if)#
```

dot1x timeout supp-timeout

This command sets the time that an interface on the switch waits for a response to an EAP request from a client before re-transmitting an EAP packet. Use the **no** form to reset to the default value.

SYNTAX

dot1x timeout supp-timeout *seconds*

no dot1x timeout supp-timeout

seconds - The number of seconds. (Range: 1-65535)

DEFAULT

30 seconds

COMMAND MODE

Interface Configuration

COMMAND USAGE

This command sets the timeout for EAP-request frames other than EAP-request/identity frames. If dot1x authentication is enabled on a port, the switch will initiate authentication when the port link state comes up. It will send an EAP-request/identity frame to the client to request its identity, followed by one or more requests for authentication information. It may also send other EAP-request frames to the client during an active connection as required for reauthentication.

EXAMPLE

```
Console(config)#interface eth 1/2
Console(config-if)#dot1x timeout supp-timeout 300
Console(config-if)#
```

dot1x timeout tx-period

This command sets the time that an interface on the switch waits during an authentication session before re-transmitting an EAP packet. Use the **no** form to reset to the default value.

SYNTAX

dot1x timeout tx-period *seconds*

no dot1x timeout tx-period

seconds - The number of seconds. (Range: 1-65535)

DEFAULT

30 seconds

COMMAND MODE

Interface Configuration

EXAMPLE

```
Console(config)#interface eth 1/2
Console(config-if)#dot1x timeout tx-period 300
Console(config-if)#
```

dot1x re-authenticate

This command forces re-authentication on all ports or a specific interface.

SYNTAX

dot1x re-authenticate [*interface*]

interface

ethernet *unit*/*port*

unit - Unit identifier. (Range: 1)

port - Port number. (Range: 1-28)

COMMAND MODE

Privileged Exec

COMMAND USAGE

The re-authentication process verifies the connected client's user ID and password on the RADIUS server. During re-authentication, the client remains connected the network and the process is handled transparently by the dot1x client software. Only if re-authentication fails is the port blocked.

EXAMPLE

```
Console#dot1x re-authenticate
Console#
```

Display Information Commands

show dot1x

This command shows general port authentication related settings on the switch or a specific interface.

SYNTAX

show dot1x [**statistics**] [**interface** *interface*]

statistics - Displays dot1x status for each port.

interface

ethernet *unit/port*

unit - Unit identifier. (Range: 1)

port - Port number. (Range: 1-28)

COMMAND MODE

Privileged Exec

COMMAND USAGE

This command displays the following information:

- *Global 802.1X Parameters* – Shows whether or not 802.1X port authentication is globally enabled on the switch (page 1069).

- *Authenticator Parameters* – Shows whether or not EAPOL pass-through is enabled (page 1068).

- *802.1X Port Summary* – Displays the port access control parameters for each interface that has enabled 802.1X, including the following items:

  - Type – Administrative state for port access control (Enabled, Authenticator, or Supplicant).
  - Operation Mode–Allows single or multiple hosts (page 1071).
  - Control Mode – Dot1x port control mode (page 1072).
  - Authorized– Authorization status (yes or n/a - not authorized).

- *802.1X Port Details* – Displays the port access control parameters for each interface, including the following items:

  - Reauthentication – Periodic re-authentication (page 1072).
  - Reauth Period – Time after which a connected client must be re-authenticated (page 1073).
  - Quiet Period – Time a port waits after Max Request Count is exceeded before attempting to acquire a new client (page 1073).
  - TX Period – Time a port waits during authentication session before re-transmitting EAP packet (page 1074).
  - Supplicant Timeout – Supplicant timeout.
  - Server Timeout – Server timeout. A RADIUS server must be set before the correct operational value of 10 seconds will be displayed in this field.

  - Reauth Max Retries – Maximum number of reauthentication attempts.
  - Max Request – Maximum number of times a port will retransmit an EAP request/identity packet to the client before it times out the authentication session (page 1070).
  - Operation Mode– Shows if single or multiple hosts (clients) can connect to an 802.1X-authorized port.
  - Port Control–Shows the dot1x mode on a port as auto, force-authorized, or force-unauthorized (page 1072).
  - Intrusion Action– Shows the port response to intrusion when authentication fails (page 1069).
  - Supplicant– MAC address of authorized client.

- *Authenticator State Machine*

  - State – Current state (including initialize, disconnected, connecting, authenticating, authenticated, aborting, held, force_authorized, force_unauthorized).
  - Reauth Count– Number of times connecting state is re-entered.
  - Current Identifier– The integer (0-255) used by the Authenticator to identify the current authentication session.

- *Backend State Machine*

  - State – Current state (including request, response, success, fail, timeout, idle, initialize).
  - Request Count– Number of EAP Request packets sent to the Supplicant without receiving a response.
  - Identifier (Server)– Identifier carried in the most recent EAP Success, Failure or Request packet received from the Authentication Server.

- *Reauthentication State Machine*

  State – Current state (including initialize, reauthenticate).

EXAMPLE

```
Console#show dot1x
Global 802.1X Parameters
 System Auth Control       : Enabled

Authenticator Parameters:
 EAPOL Pass Through        : Disabled

802.1X Port Summary

Port     Type          Operation Mode Control Mode       Authorized
-------- ------------- -------------- ------------------ ----------
Eth 1/ 1 Disabled      Single-Host    Force-Authorized   Yes
Eth 1/ 2 Disabled      Single-Host    Force-Authorized   Yes
.
.
.
Eth 1/27 Disabled      Single-Host    Force-Authorized   Yes
Eth 1/28 Enabled       Single-Host    Auto               Yes
```

```
802.1X Port Details

802.1X Authenticator is enabled on port 1/1
802.1X Supplicant is disabled on port 1/1
.
.
.
802.1X Authenticator is enabled on port 28
Reauthentication     : Enabled
Reauth Period        : 3600
Quiet Period         : 60
TX Period            : 30
Supplicant Timeout   : 30
Server Timeout       : 10
Reauth Max Retries   : 2
Max Request          : 2
Operation Mode       : Multi-host
Port Control         : Auto
Intrusion Action     : Block traffic

Supplicant           : 00-e0-29-94-34-65


 Authenticator PAE State Machine
  State                : Authenticated
  Reauth Count         : 0
  Current Identifier   : 3

 Backend State Machine
  State                : Idle
  Request Count        : 0
  Identifier(Server)   : 2

 Reauthentication State Machine
  State                : Initialize

Console#
```

MANAGEMENT IP FILTER

This section describes commands used to configure IP management access to the switch.

Table 109: Management IP Filter Commands

Command	Function	Mode
management	Configures IP addresses that are allowed management access	GC
show management	Displays the switch to be monitored or configured from a browser	PE

management

This command specifies the client IP addresses that are allowed management access to the switch through various protocols. Use the **no** form to restore the default setting.

SYNTAX

[**no**] **management** {**all-client** | **http-client** | **snmp-client** | **telnet-client**} *start-address* [*end-address*]

all-client - Adds IP address(es) to all groups.

http-client - Adds IP address(es) to the web group.

snmp-client - Adds IP address(es) to the SNMP group.

telnet-client - Adds IP address(es) to the Telnet group.

start-address - A single IP address, or the starting address of a range.

end-address - The end address of a range.

DEFAULT SETTING

All addresses

COMMAND MODE

Global Configuration

COMMAND USAGE

- If anyone tries to access a management interface on the switch from an invalid address, the switch will reject the connection, enter an event message in the system log, and send a trap message to the trap manager.
- IP address can be configured for SNMP, web, and Telnet access respectively. Each of these groups can include up to five different sets of addresses, either individual addresses or address ranges.
- When entering addresses for the same group (i.e., SNMP, web, or Telnet), the switch will not accept overlapping address ranges. When entering addresses for different groups, the switch will accept overlapping address ranges.
- You cannot delete an individual address from a specified range. You must delete the entire range, and reenter the addresses.
- You can delete an address range just by specifying the start address, or by specifying both the start address and end address.

EXAMPLE

This example restricts management access to the indicated addresses.

```
Console(config)#management all-client 192.168.1.19
Console(config)#management all-client 192.168.1.25 192.168.1.30
Console#
```

show management

This command displays the client IP addresses that are allowed management access to the switch through various protocols.

SYNTAX

show management {**all-client** | **http-client** | **snmp-client** | **telnet-client**}

all-client - Displays IP addresses for all groups.

http-client - Displays IP addresses for the web group.

snmp-client - Displays IP addresses for the SNMP group.

telnet-client - Displays IP addresses for the Telnet group.

COMMAND MODE

Privileged Exec

EXAMPLE

```
Console#show management all-client
Management Ip Filter
 HTTP-Client:
   Start IP address      End IP address
-----------------------------------------------
1. 192.168.1.19          192.168.1.19
2. 192.168.1.25          192.168.1.30

 SNMP-Client:
   Start IP address      End IP address
-----------------------------------------------
1. 192.168.1.19          192.168.1.19
2. 192.168.1.25          192.168.1.30

 TELNET-Client:
   Start IP address      End IP address
-----------------------------------------------
1. 192.168.1.19          192.168.1.19
2. 192.168.1.25          192.168.1.30

Console#
```

PPPOE INTERMEDIATE AGENT

This section describes commands used to configure the PPPoE Intermediate Agent (PPPoE IA) relay parameters required for passing authentication messages between a client and broadband remote access servers.

Table 110: PPPoE Intermediate Agent Commands

Command	Function	Mode
pppoe intermediate-agent	Enables the PPPoE IA globally on the switch	GC
pppoe intermediate-agent format-type	Sets the access node identifier and generic error message for the switch	GC
pppoe intermediate-agent port-enable	Enables the PPPoE IA on an interface	IC
pppoe intermediate-agent port-format-type	Sets the circuit-id or remote-id for an interface	IC
pppoe intermediate-agent trust	Sets the trust mode for an interface	IC
pppoe intermediate-agent vendor-tag strip	Enables the stripping of vendor tags from PPPoE Discovery packets sent from a PPPoE server	IC
clear pppoe intermediate-agent statistics	Clears PPPoE IA statistics	PE
show pppoe intermediate-agent info	Displays PPPoE IA configuration settings	PE
show pppoe intermediate-agent statistics	Displays PPPoE IA statistics	PE

pppoe intermediate-agent

This command enables the PPPoE Intermediate Agent globally on the switch. Use the **no** form to disable this feature.

SYNTAX

[**no**] **pppoe intermediate-agent**

DEFAULT SETTING

Disabled

COMMAND MODE

Global Configuration

COMMAND USAGE

- The switch inserts a tag identifying itself as a PPPoE Intermediate Agent residing between the attached client requesting network access and the ports connected to broadband remote access servers (BRAS). The switch extracts access-loop information from the client's PPPoE Active Discovery Request, and forwards this information to all trusted ports designated by the pppoe intermediate-agent trust command. The BRAS detects the presence of the subscriber's circuit-Id tag inserted by the switch during the PPPoE discovery phase, and sends this tag as a NAS-port-Id attribute in PPP authentication and AAA accounting requests to a RADIUS server.

- PPPoE IA must be enabled globally by this command before this feature can be enabled on an interface using the pppoe intermediate-agent port-enable command.

EXAMPLE

```
Console(config)#pppoe intermediate-agent
Console(config)#
```

pppoe intermediate-agent format-type

This command sets the access node identifier and generic error message for the switch. Use the **no** form to restore the default settings.

SYNTAX

pppoe intermediate-agent format-type {**access-node-identifier** *id-string* | **generic-error-message** *error-message*}

no pppoe intermediate-agent format-type {**access-node-identifier** | **generic-error-message**}

id-string - String identifying this switch as an PPPoE IA to the PPPoE server. (Range: 1-48 ASCII characters)

error-message - An error message notifying the sender that the PPPoE Discovery packet was too large.

DEFAULT SETTING

- Access Node Identifier: IP address of first IPv4 interface on the switch.
- Generic Error Message: PPPoE Discover packet too large to process. Try reducing the number of tags added.

COMMAND MODE

Global Configuration

COMMAND USAGE

- The switch uses the access-node-identifier to generate the circuit-id for PPPoE discovery stage packets sent to the BRAS, but does not modify the source or destination MAC address of these PPPoE discovery packets.
- These messages are forwarded to all trusted ports designated by the pppoe intermediate-agent trust command.

EXAMPLE

```
Console(config)#pppoe intermediate-agent format-type access-node-identifier
  billibong
Console(config)#
```

pppoe intermediate-agent port-enable

This command enables the PPPoE IA on an interface. Use the **no** form to disable this feature.

SYNTAX

[**no**] **pppoe intermediate-agent port-enable**

DEFAULT SETTING

Disabled

COMMAND MODE

Interface Configuration (Ethernet, Port Channel)

COMMAND USAGE

PPPoE IA must also be enabled globally on the switch for this command to tack effect.

EXAMPLE

```
Console(config)#int ethernet 1/5
Console(config-if)#pppoe intermediate-agent port-enable
Console(config-if)#
```

pppoe intermediate-agent port-format-type

This command sets the circuit-id or remote-id for an interface. Use the **no** form to restore the default settings.

SYNTAX

pppoe intermediate-agent port-format-type {**circuit-id** | **remote-id**} *id-string*

circuit-id - String identifying the circuit identifier (or interface) on this switch to which the user is connected. (Range: 1-10 ASCII characters)

remote-id - String identifying the remote identifier (or interface) on this switch to which the user is connected. (Range: 1-63 ASCII characters)

DEFAULT SETTING

circuit-id: unit/port:vlan-id or 0/trunk-id:vlan-id
remote-id: port MAC address

COMMAND MODE

Interface Configuration (Ethernet, Port Channel)

COMMAND USAGE

- The PPPoE server extracts the Line-Id tag from PPPoE discovery stage messages, and uses the Circuit-Id field of that tag as a NAS-Port-Id attribute in AAA access and accounting requests.

- The switch intercepts PPPoE discovery frames from the client and inserts a unique line identifier using the PPPoE Vendor-Specific tag (0x0105) to PPPoE Active Discovery Initiation (PADI) and Request (PADR) packets. The switch then forwards these packets to the PPPoE server. The tag contains the Line-Id of the customer line over which the discovery packet was received, entering the switch (or access node) where the intermediate agent resides.

- Outgoing PAD Offer (PADO) and Session-confirmation (PADS) packets sent from the PPPoE Server include the Circuit-Id tag inserted by the switch, and should be stripped out of PADO and PADS packets which are to be passed directly to end-node clients using the pppoe intermediate-agent vendor-tag strip command.

EXAMPLE

```
Console(config)#int ethernet 1/5
Console(config-if)#pppoe intermediate-agent port-format-type circuit-id
  ECS4660-28F
Console(config-if)#
```

pppoe intermediate-agent trust

This command sets an interface to trusted mode to indicate that it is connected to a PPPoE server. Use the **no** form to set an interface to untrusted mode.

SYNTAX

[**no**] **pppoe intermediate-agent trust**

DEFAULT SETTING

Untrusted

COMMAND MODE

Interface Configuration (Ethernet, Port Channel)

COMMAND USAGE

- Set any interfaces connecting the switch to a PPPoE Server as trusted. Interfaces that connect the switch to users (PPPoE clients) should be set as untrusted.

- At least one trusted interface must be configured on the switch for the PPPoE IA to function.

EXAMPLE

```
Console(config)#int ethernet 1/5
Console(config-if)#pppoe intermediate-agent trust
Console(config-if)#
```

pppoe intermediate-agent vendor-tag strip

This command enables the stripping of vendor tags from PPPoE Discovery packets sent from a PPPoE server. Use the **no** form to disable this feature.

SYNTAX

[**no**] **pppoe intermediate-agent vendor-tag strip**

DEFAULT SETTING

Disabled

COMMAND MODE

Interface Configuration (Ethernet, Port Channel)

COMMAND USAGE

This command only applies to trusted interfaces. It is used to strip off vendor-specific tags (which carry subscriber and line identification information) in PPPoE Discovery packets received from an upstream PPPoE server before forwarding them to a user.

EXAMPLE

```
Console(config)#int ethernet 1/5
Console(config-if)#pppoe intermediate-agent vendor-tag strip
Console(config-if)#
```

clear pppoe intermediate-agent statistics

This command clears statistical counters for the PPPoE Intermediate Agent.

SYNTAX

clear pppoe intermediate-agent statistics interface [*interface*]

interface

ethernet *unit*/*port*

unit - Stack unit. (Range: 1)

port - Port number. (Range: 1-28)

port-channel *channel-id* (Range: 1-8)

COMMAND MODE

Privileged Exec

EXAMPLE

```
Console#clear pppoe intermediate-agent statistics
Console#
```

show pppoe intermediate-agent info

This command displays configuration settings for the PPPoE Intermediate Agent.

SYNTAX

show pppoe intermediate-agent info [**interface** [*interface*]]

interface

ethernet *unit/port*

unit - Stack unit. (Range: 1)

port - Port number. (Range: 1-28)

port-channel *channel-id* (Range: 1-8)

COMMAND MODE

Privileged Exec

EXAMPLE

```
Console#show pppoe intermediate-agent info
PPPoE Intermediate Agent Global Status          : Enabled
PPPoE Intermediate Agent Admin Access Node Identifier : 192.168.0.2
PPPoE Intermediate Agent Oper Access Node Identifier  : 192.168.0.2
PPPoE Intermediate Agent Admin Generic Error Message  :
 PPPoE Discover packet too large to process. Try reducing the number of tags
  added.
PPPoE Intermediate Agent Oper Generic Error Message   :
 PPPoE Discover packet too large to process. Try reducing the number of tags
  added.
Consoleshow pppoe intermediate-agent info interface ethernet 1/1
Interface PPPoE IA Trusted Vendor-Tag Strip Admin Circuit-ID Admin Remote-ID
                                            Oper Circuit-ID  Oper Remote-ID
--------- -------- ------- ---------------- ------------     ----------------
Eth 1/2   Yes      No      Yes              ECS4660-28F      ECS4660-28F
                                            ECS4660-28F      ECS4660-28F

Console#
```

show pppoe intermediate-agent statistics

This command displays statistics for the PPPoE Intermediate Agent.

SYNTAX

show pppoe intermediate-agent statistics interface [*interface*]

interface

ethernet *unit/port*

unit - Stack unit. (Range: 1)

port - Port number. (Range: 1-28)

port-channel *channel-id* (Range: 1-8)

COMMAND MODE

Privileged Exec

EXAMPLE

```
Console#show pppoe intermediate-agent statistics interface ethernet 1/1
Eth 1/1 statistics
-----------------------------------------------------------------------------
 Received :        All       PADI       PADO       PADR       PADS       PADT
            ---------- ---------- ---------- ---------- ---------- ----------
                     3          0          0          0          0          3

 Dropped  : Response from untrusted  Request towards untrusted  Malformed
            -----------------------  -------------------------  ---------
                                  0                          0          0
Console#
```

Table 111: show pppoe intermediate-agent statistics - display description

Field	Description
Received	
PADI	PPPoE Active Discovery Initiation
PADO	PPPoE Active Discovery Offer
PADR	PPPoE Active Discovery Request
PADS	PPPoE Active Discovery Session-Confirmation
PADT	PPPoE Active Discovery Terminate
Dropped	
Response from untrusted	Response from an interface which not been configured as trusted.
Request towards untrusted	Request sent to an interface which not been configured as trusted.
Malformed	Corrupted PPPoE message.

29 General Security Measures

This switch supports many methods of segregating traffic for clients attached to each of the data ports, and for ensuring that only authorized clients gain access to the network. Port-based authentication using IEEE 802.1X is commonly used for these purposes. In addition to these method, several other options of providing client security are described in this chapter. These include port-based authentication, which can be configured to allow network client access by specifying a fixed set of MAC addresses. The addresses assigned to DHCP clients can also be carefully controlled with IP Source Guard and DHCP Snooping commands.

Table 112: General Security Commands

Command Group	Function
Port Security*	Configures secure addresses for a port
802.1X Port Authentication*	Configures host authentication on specific ports using 802.1X
Network Access*	Configures MAC authentication and dynamic VLAN assignment
Web Authentication*	Configures Web authentication
Access Control Lists*	Provides filtering for IP frames (based on address, protocol, TCP/UDP port number or TCP control code) or non-IP frames (based on MAC address or Ethernet type)
DHCPv4 Snooping*	Filters untrusted DHCP messages on unsecure ports by building and maintaining a DHCP snooping binding table
DHCPv6 Snooping*	Filters untrusted DHCPv6 messages on unsecure ports by building and maintaining a DHCPv6 snooping binding table
IPv4 Source Guard*	Filters IPv4 traffic on insecure ports for which the source address cannot be identified via DHCPv4 snooping nor static source bindings
IPv6 Source Guard*	Filters IPv6 traffic on insecure ports for which the source address cannot be identified via DHCPv6 snooping nor static source bindings
ND Snooping	Maintains IPv6 prefix table and user address binding table which can be used for stateless address auto-configuration or for address filtering by IPv6 Source Guard
ARP Inspection	Validates the MAC-to-IP address bindings in ARP packets
DoS Protection	Protects against Denial-of-Service attacks
Port-based Traffic Segmentation	Configures traffic segmentation for different client sessions based on specified downlink and uplink ports

* The priority of execution for these filtering commands is Port Security, Port Authentication, Network Access, Web Authentication, Access Control Lists, DHCP Snooping, and then IP Source Guard.

PORT SECURITY

These commands can be used to enable port security on a port.

When MAC address learning is disabled on an interface, only incoming traffic with source addresses already stored in the dynamic or static address table for this port will be authorized to access the network.

When using port security, the switch stops learning new MAC addresses on the specified port when it has reached a configured maximum number. Only incoming traffic with source addresses already stored in the dynamic or static address table for this port will be authorized to access the network. The port will drop any incoming frames with a source MAC address that is unknown or has been previously learned from another port. If a device with an unauthorized MAC address attempts to use the switch port, the intrusion will be detected and the switch can automatically take action by disabling the port and sending a trap message.

Table 113: Management IP Filter Commands

Command	Function	Mode
mac-address-table static	Maps a static address to a port in a VLAN	GC
mac-learning	Enables MAC address learning on the selected physical interface or VLAN	IC
port security	Configures a secure port	IC
port security mac-address-as-permanent	Saves the MAC addresses learned by port security as static entries.	IC
show mac-address-table	Displays entries in the bridge-forwarding database	PE
show port security	Displays port security status and secure address count	PE

mac-learning

This command enables MAC address learning on the selected interface. Use the **no** form to disable MAC address learning.

SYNTAX

[**no**] **mac-learning**

DEFAULT SETTING

Enabled

COMMAND MODE

Interface Configuration (Ethernet or Port Channel)

COMMAND USAGE

- The **no mac-learning** command immediately stops the switch from learning new MAC addresses on the specified port or trunk. Only incoming traffic with source addresses stored in the static address table will be accepted. Note that the dynamic addresses stored in the address table when MAC address learning is disabled are flushed from the system, and no dynamic addresses are subsequently learned until MAC address learning has been re-enabled.

- The mac-learning commands cannot be used if 802.1X Port Authentication has been globally enabled on the switch with the dot1x system-auth-control command, or if MAC Address Security has been enabled by the port security command on the same interface.

EXAMPLE

The following example disables MAC address learning for port 2.

```
Console(config)#interface ethernet 1/2
Console(config-if)#no mac-learning
Console(config-if)#
```

RELATED COMMANDS

show interfaces status (1202)

port security

This command enables or configures port security. Use the **no** form without any keywords to disable port security. Use the **no** form with the appropriate keyword to restore the default settings for a response to security violation or for the maximum number of allowed addresses.

SYNTAX

port security [**action** {**shutdown** | **trap** | **trap-and-shutdown**} | **max-mac-count** *address-count*]

no port security [**action** | **max-mac-count**]

action - Response to take when port security is violated.

shutdown - Disable port only.

trap - Issue SNMP trap message only.

trap-and-shutdown - Issue SNMP trap message and disable port.

max-mac-count

address-count - The maximum number of MAC addresses that can be learned on a port. (Range: 0 - 1024, where 0 means disabled)

DEFAULT SETTING

Status: Disabled
Action: None
Maximum Addresses: 0

COMMAND MODE

Interface Configuration (Ethernet)

Command Usage

- The default maximum number of MAC addresses allowed on a secure port is zero (that is, port security is disabled). To use port security, you must configure the maximum number of addresses allowed on a port using the **port security max-mac-count** command.

- When port security is enabled using the **port security** command, or the maximum number or allowed addresses is set to value lower than the current limit after port security has been enabled, the switch first clears all dynamically learned entries from the address table. It then starts learning new MAC addresses on the specified port, and stops learning addresses when it reaches a configured maximum number. Only incoming traffic with source addresses already stored in the dynamic or static address table will be accepted.

- To configure the maximum number of address entries which can be learned on a port, specify the maximum number of dynamic addresses allowed. The switch will learn up to the maximum number of allowed address pairs <source MAC address, VLAN> for frames received on the port. (The specified maximum address count is effective when port security is enabled or disabled.) Note that you can manually add additional secure addresses to a port using the mac-address-table static command. When the port has reached the maximum number of MAC addresses, the port will stop learning new addresses. The MAC addresses already in the address table will be retained and will not be aged out.

- MAC addresses that port security has learned, can be saved in the configuration file as static entries. See the port security mac-address-as-permanent command.

- If port security is enabled, and the maximum number of allowed addresses are set to a non-zero value, any device not in the address table that attempts to use the port will be prevented from accessing the switch.

- If a port is disabled due to a security violation, it must be manually re-enabled using the no shutdown command.

- A secure port has the following restrictions:
  - Cannot be connected to a network interconnection device.
  - Cannot be a trunk port.

Example

The following example enables port security for port 5, and sets the response to a security violation to issue a trap message:

```
Console(config)#interface ethernet 1/5
Console(config-if)#port security action trap
```

RELATED COMMANDS

show interfaces status (1202)
shutdown (1194)
mac-address-table static (1272)

port security mac-address-as-permanent

This command saves the MAC addresses that port security has learned as static entries.

SYNTAX

port security mac-address-as-permanent [**interface** *interface*]

interface - Specifies a port interface.

ethernet *unit*/*port*

unit - This is unit 1.

port - Port number. (Range: 1-28)

COMMAND MODE

Privileged Exec

EXAMPLE

This example shows the switch saving the MAC addresses learned by port security on ethernet port 3.

```
Console#port security mac-address-as-permanent interface ethernet 1/3
Console#
```

show port security

This command displays port security status and the secure address count.

SYNTAX

show port security [**interface** *interface*]

interface - Specifies a port interface.

ethernet *unit*/*port*

unit - This is unit 1.

port - Port number. (Range: 1-28)

COMMAND MODE

Privileged Exec

EXAMPLE

This example shows the port security settings and number of secure addresses for all ports.

```
Console#show port security
Global Port Security Parameters
 Secure MAC Aging Mode : Disabled

Port Security Port Summary
 Port     Port Security Port Status  Intrusion Action  MaxMacCnt CurrMacCnt
 --------------------------------------------------------------------------
 Eth 1/ 1 Disabled      Secure/Down  None              0         2
 Eth 1/ 2 Enabled       Secure/Up    None              10        0
 Eth 1/ 3 Disabled      Secure/Down  None              0         0
 Eth 1/ 4 Disabled      Secure/Down  None              0         0
 Eth 1/ 5 Disabled      Secure/Down  None              0         0
 Eth 1/ 6 Disabled      Secure/Down  None              0         0
 Eth 1/ 7 Disabled      Secure/Down  None              0         0
 Eth 1/ 8 Disabled      Secure/Down  None              0         0
 Eth 1/ 9 Disabled      Secure/Down  None              0         0
 Eth 1/10 Disabled      Secure/Down  None              0         0
 Eth 1/11 Disabled      Secure/Down  None              0         0
 Eth 1/12 Disabled      Secure/Down  None              0         0
Console#
```

Table 114: show port security - display description

Field	Description
Port Security	The configured status (enabled or disabled).
Port Status	The operational status: ◆ Secure/Down – Port security is disabled. ◆ Secure/Up – Port security is enabled. ◆ Shutdown – Port is shut down due to a response to a port security violation.
Intrusion Action	The configured intrusion response.
MaxMacCnt	The maximum number of addresses which can be stored in the address table for this interface (either dynamic or static).
CurrMacCnt	The current number of secure entries in the address table.

The following example shows the port security settings and number of secure addresses for a specific port. The Last Intrusion MAC and Last Time Detected Intrusion MAC fields show information about the last detected intrusion MAC address. These fields are not applicable if no intrusion has been detected or port security is disabled. The MAC Filter ID field is configured by the network-access port-mac-filter command. If this field displays Disabled, then any unknown source MAC address can be learned as a secure MAC address. If it displays a filter identifier, then only source

MAC address entries in MAC Filter table can be learned as secure MAC addresses.

```
Console#show port security interface ethernet 1/2
Global Port Security Parameters
 Secure MAC aging mode : Disabled

Port Security Details
 Port                                  : 1/2
 Port Security                         : Enabled
 Port Status                           : Secure/Up
 Intrusion Action                      : None
 Max-MAC-Count                         : 0
 Current MAC Count                     : 0
 MAC Filter ID                         : Disabled
 Last Intrusion MAC                    : NA
 Last Time Detected Intrusion MAC      : NA
Console#
```

This example shows information about a detected intrusion.

```
Console#show port security interface ethernet 1/2
Global Port Security Parameters
 Secure MAC aging mode : Disabled

Port Security Details
 Port                                  : 1/2
 Port Security                         : Enabled
 Port Status                           : Secure/Up
 Intrusion Action                      : None
 Max-MAC-Count                         : 0
 Current MAC Count                     : 0
 MAC Filter                            : Enabled
 MAC Filter ID                         : 1
 Last Intrusion MAC                    : 00-10-22-00-00-01
 Last Time Detected Intrusion MAC      : 2010/7/29 15:13:03
Console#
```

NETWORK ACCESS (MAC ADDRESS AUTHENTICATION)

Network Access authentication controls access to the network by authenticating the MAC address of each host that attempts to connect to a switch port. Traffic received from a specific MAC address is forwarded by the switch only if the source MAC address is successfully authenticated by a central RADIUS server. While authentication for a MAC address is in progress, all traffic is blocked until authentication is completed. Once successfully authenticated, the RADIUS server may optionally assign VLAN and QoS settings for the switch port.

Table 115: Network Access Commands

Command	Function	Mode
network-access aging	Enables MAC address aging	GC
network-access mac-filter	Adds a MAC address to a filter table	GC

Table 115: Network Access Commands (Continued)

Command	Function	Mode
mac-authentication reauth-time	Sets the time period after which a connected MAC address must be re-authenticated	GC
network-access dynamic-qos	Enables the dynamic quality of service feature	IC
network-access dynamic-vlan	Enables dynamic VLAN assignment from a RADIUS server	IC
network-access guest-vlan	Specifies the guest VLAN	IC
network-access link-detection	Enables the link detection feature	IC
network-access link-detection link-down	Configures the link detection feature to detect and act upon link-down events	IC
network-access link-detection link-up	Configures the link detection feature to detect and act upon link-up events	IC
network-access link-detection link-up-down	Configures the link detection feature to detect and act upon both link-up and link-down events	IC
network-access max-mac-count	Sets the maximum number of MAC addresses that can be authenticated on a port via all forms of authentication	IC
network-access mode mac-authentication	Enables MAC authentication on an interface	IC
network-access port-mac-filter	Enables the specified MAC address filter	IC
mac-authentication intrusion-action	Determines the port response when a connected host fails MAC authentication.	IC
mac-authentication max-mac-count	Sets the maximum number of MAC addresses that can be authenticated on a port via MAC authentication	IC
clear network-access	Clears authenticated MAC addresses from the address table	PE
show network-access	Displays the MAC authentication settings for port interfaces	PE
show network-access mac-address-table	Displays information for entries in the secure MAC address table	PE
show network-access mac-filter	Displays information for entries in the MAC filter tables	PE

network-access aging

Use this command to enable aging for authenticated MAC addresses stored in the secure MAC address table. Use the **no** form of this command to disable address aging.

SYNTAX

[**no**] **network-access aging**

DEFAULT SETTING

Disabled

COMMAND MODE

Global Configuration

COMMAND USAGE

- Authenticated MAC addresses are stored as dynamic entries in the switch's secure MAC address table and are removed when the aging time expires. The address aging time is determined by the mac-address-table aging-time command.

- This parameter applies to authenticated MAC addresses configured by the MAC Address Authentication process described in this section, as well as to any secure MAC addresses authenticated by 802.1X, regardless of the 802.1X Operation Mode (Single-Host, Multi-Host, or MAC-Based authentication as described on page 1071).

- The maximum number of secure MAC addresses supported for the switch system is 1024.

EXAMPLE

```
Console(config-if)#network-access aging
Console(config-if)#
```

network-access mac-filter

Use this command to add a MAC address into a filter table. Use the **no** form of this command to remove the specified MAC address.

SYNTAX

[**no**] **network-access mac-filter** *filter-id*
mac-address *mac-address* [**mask** *mask-address*]

filter-id - Specifies a MAC address filter table. (Range: 1-64)

mac-address - Specifies a MAC address entry.
(Format: xx-xx-xx-xx-xx-xx)

mask - Specifies a MAC address bit mask for a range of addresses.

DEFAULT SETTING

Disabled

COMMAND MODE

Global Configuration

COMMAND USAGE

- Specified addresses are exempt from network access authentication.

- This command is different from configuring static addresses with the mac-address-table static command in that it allows you configure a range of addresses when using a mask, and then to assign these addresses to one or more ports with the network-access port-mac-filter command.

- Up to 64 filter tables can be defined.

- There is no limitation on the number of entries that can entered in a filter table.

EXAMPLE

```
Console(config)#network-access mac-filter 1 mac-address 11-22-33-44-55-66
Console(config)#
```

mac-authentication reauth-time

Use this command to set the time period after which a connected MAC address must be re-authenticated. Use the **no** form of this command to restore the default value.

SYNTAX

mac-authentication reauth-time *seconds*

no mac-authentication reauth-time

seconds - The reauthentication time period. (Range: 120-1000000 seconds)

DEFAULT SETTING

1800

COMMAND MODE

Global Configuration

COMMAND USAGE

- The reauthentication time is a global setting and applies to all ports.
- When the reauthentication time expires for a secure MAC address it is reauthenticated with the RADIUS server. During the reauthentication process traffic through the port remains unaffected.

EXAMPLE

```
Console(config)#mac-authentication reauth-time 300
Console(config)#
```

network-access dynamic-qos

Use this command to enable the dynamic QoS feature for an authenticated port. Use the **no** form to restore the default.

SYNTAX

[**no**] **network-access dynamic-qos**

DEFAULT SETTING

Disabled

Command Mode

Interface Configuration

Command Usage

- The RADIUS server may optionally return dynamic QoS assignments to be applied to a switch port for an authenticated user. The “Filter-ID” attribute (attribute 11) can be configured on the RADIUS server to pass the following QoS information:

Table 116: Dynamic QoS Profiles

Profile	Attribute Syntax	Example
DiffServ	**service-policy-in**=*policy-map-name*	service-policy-in=p1
Rate Limit	**rate-limit-input**=*rate*	rate-limit-input=100 (Kbps)
802.1p	**switchport-priority-default**=*value*	switchport-priority-default=2
IP ACL	**ip-access-group-in**=*ip-acl-name*	ip-access-group-in=ipv4acl
IPv6 ACL	**ipv6-access-group-in**=*ipv6-acl-name*	ipv6-access-group-in=ipv6acl
MAC ACL	**mac-access-group-in**=*mac-acl-name*	mac-access-group-in=macAcl

- When the last user logs off of a port with a dynamic QoS assignment, the switch restores the original QoS configuration for the port.

- When a user attempts to log into the network with a returned dynamic QoS profile that is different from users already logged on to the same port, the user is denied access.

- While a port has an assigned dynamic QoS profile, any manual QoS configuration changes only take effect after all users have logged off of the port.

Note: Any configuration changes for dynamic QoS are not saved to the switch configuration file.

Example

The following example enables the dynamic QoS feature on port 1.

```
Console(config)#interface ethernet 1/1
Console(config-if)#network-access dynamic-qos
Console(config-if)#
```

network-access dynamic-vlan

Use this command to enable dynamic VLAN assignment for an authenticated port. Use the **no** form to disable dynamic VLAN assignment.

SYNTAX

[**no**] **network-access dynamic-vlan**

DEFAULT SETTING

Enabled

COMMAND MODE

Interface Configuration

COMMAND USAGE

- When enabled, the VLAN identifiers returned by the RADIUS server through the 802.1X authentication process will be applied to the port, providing the VLANs have already been created on the switch. GVRP is not used to create the VLANs.
- The VLAN settings specified by the first authenticated MAC address are implemented for a port. Other authenticated MAC addresses on the port must have same VLAN configuration, or they are treated as an authentication failure.
- If dynamic VLAN assignment is enabled on a port and the RADIUS server returns no VLAN configuration, the authentication is still treated as a success, and the host assigned to the default untagged VLAN.
- When the dynamic VLAN assignment status is changed on a port, all authenticated addresses are cleared from the secure MAC address table.

EXAMPLE

The following example enables dynamic VLAN assignment on port 1.

```
Console(config)#interface ethernet 1/1
Console(config-if)#network-access dynamic-vlan
Console(config-if)#
```

network-access guest-vlan

Use this command to assign all traffic on a port to a guest VLAN when 802.1x authentication is rejected. Use the **no** form of this command to disable guest VLAN assignment.

SYNTAX

network-access guest-vlan *vlan-id*

no network-access guest-vlan

vlan-id - VLAN ID (Range: 1-4094)

Default Setting

Disabled

Command Mode

Interface Configuration

Command Usage

- The VLAN to be used as the guest VLAN must be defined and set as active (See the vlan database command).
- When used with 802.1X authentication, the intrusion-action must be set for “guest-vlan” to be effective (see the dot1x intrusion-action command).

Example

```
Console(config)#interface ethernet 1/1
Console(config-if)#network-access guest-vlan 25
Console(config-if)#
```

network-access link-detection

Use this command to enable link detection for the selected port. Use the **no** form of this command to restore the default.

Syntax

[**no**] **network-access link-detection**

Default Setting

Disabled

Command Mode

Interface Configuration

Example

```
Console(config)#interface ethernet 1/1
Console(config-if)#network-access link-detection
Console(config-if)#
```

network-access link-detection link-down

Use this command to detect link-down events. When detected, the switch can shut down the port, send an SNMP trap, or both. Use the **no** form of this command to disable this feature.

SYNTAX

network-access link-detection link-down
action [**shutdown** | **trap** | **trap-and-shutdown**]

no network-access link-detection

action - Response to take when port security is violated.

shutdown - Disable port only.

trap - Issue SNMP trap message only.

trap-and-shutdown - Issue SNMP trap message and disable the port.

DEFAULT SETTING

Disabled

COMMAND MODE

Interface Configuration

EXAMPLE

```
Console(config)#interface ethernet 1/1
Console(config-if)#network-access link-detection link-down action trap
Console(config-if)#
```

network-access link-detection link-up

Use this command to detect link-up events. When detected, the switch can shut down the port, send an SNMP trap, or both. Use the **no** form of this command to disable this feature.

SYNTAX

network-access link-detection link-up
action [**shutdown** | **trap** | **trap-and-shutdown**]

no network-access link-detection

action - Response to take when port security is violated.

shutdown - Disable port only.

trap - Issue SNMP trap message only.

trap-and-shutdown - Issue SNMP trap message and disable the port.

DEFAULT SETTING

Disabled

COMMAND MODE

Interface Configuration

EXAMPLE

```
Console(config)#interface ethernet 1/1
Console(config-if)#network-access link-detection link-up action trap
Console(config-if)#
```

network-access link-detection link-up-down

Use this command to detect link-up and link-down events. When either event is detected, the switch can shut down the port, send an SNMP trap, or both. Use the **no** form of this command to disable this feature.

SYNTAX

network-access link-detection link-up-down
action [**shutdown** | **trap** | **trap-and-shutdown**]

no network-access link-detection

action - Response to take when port security is violated.

shutdown - Disable port only.

trap - Issue SNMP trap message only.

trap-and-shutdown - Issue SNMP trap message and disable the port.

DEFAULT SETTING

Disabled

COMMAND MODE

Interface Configuration

EXAMPLE

```
Console(config)#interface ethernet 1/1
Console(config-if)#network-access link-detection link-up-down action trap
Console(config-if)#
```

network-access max-mac-count

Use this command to set the maximum number of MAC addresses that can be authenticated on a port interface via all forms of authentication. Use the **no** form of this command to restore the default.

SYNTAX

network-access max-mac-count *count*

no network-access max-mac-count

count - The maximum number of authenticated IEEE 802.1X and MAC addresses allowed. (Range: 0-1024; 0 for unlimited)

DEFAULT SETTING

1024

COMMAND MODE

Interface Configuration

COMMAND USAGE

The maximum number of MAC addresses per port is 1024, and the maximum number of secure MAC addresses supported for the switch system is 1024. When the limit is reached, all new MAC addresses are treated as authentication failures.

EXAMPLE

```
Console(config-if)#network-access max-mac-count 5
Console(config-if)#
```

network-access mode mac-authentication

Use this command to enable network access authentication on a port. Use the **no** form of this command to disable network access authentication.

SYNTAX

[**no**] **network-access mode mac-authentication**

DEFAULT SETTING

Disabled

COMMAND MODE

Interface Configuration

COMMAND USAGE

- When enabled on a port, the authentication process sends a Password Authentication Protocol (PAP) request to a configured RADIUS server. The user name and password are both equal to the MAC address being authenticated.

- On the RADIUS server, PAP user name and passwords must be configured in the MAC address format XX-XX-XX-XX-XX-XX (all in upper case).

- Authenticated MAC addresses are stored as dynamic entries in the switch secure MAC address table and are removed when the aging time expires. The maximum number of secure MAC addresses supported for the switch system is 1024.

- Configured static MAC addresses are added to the secure address table when seen on a switch port. Static addresses are treated as authenticated without sending a request to a RADIUS server.

- MAC authentication, 802.1X, and port security cannot be configured together on the same port. Only one security mechanism can be applied.

- MAC authentication cannot be configured on trunk ports.

- When port status changes to down, all MAC addresses are cleared from the secure MAC address table. Static VLAN assignments are not restored.

- The RADIUS server may optionally return a VLAN identifier list. VLAN identifier list is carried in the "Tunnel-Private-Group-ID" attribute. The VLAN list can contain multiple VLAN identifiers in the format "1u,2t," where "u" indicates untagged VLAN and "t" tagged VLAN. The "Tunnel-Type" attribute should be set to "VLAN," and the "Tunnel-Medium-Type" attribute set to "802."

EXAMPLE

```
Console(config-if)#network-access mode mac-authentication
Console(config-if)#
```

network-access port-mac-filter

Use this command to enable the specified MAC address filter. Use the **no** form of this command to disable the specified MAC address filter.

SYNTAX

network-access port-mac-filter *filter-id*

no network-access port-mac-filter

filter-id - Specifies a MAC address filter table. (Range: 1-64)

DEFAULT SETTING

None

COMMAND MODE

Interface Configuration

COMMAND MODE

- Entries in the MAC address filter table can be configured with the network-access mac-filter command.

- Only one filter table can be assigned to a port.

EXAMPLE

```
Console(config)#interface ethernet 1/1
Console(config-if)#network-access port-mac-filter 1
Console(config-if)#
```

mac-authentication intrusion-action

Use this command to configure the port response to a host MAC authentication failure. Use the **no** form of this command to restore the default.

SYNTAX

mac-authentication intrusion-action {**block traffic** | **pass traffic**}

no mac-authentication intrusion-action

DEFAULT SETTING

Block Traffic

COMMAND MODE

Interface Con figuration

EXAMPLE

```
Console(config-if)#mac-authentication intrusion-action block-traffic
Console(config-if)#
```

mac-authentication max-mac-count

Use this command to set the maximum number of MAC addresses that can be authenticated on a port via MAC authentication. Use the **no** form of this command to restore the default.

SYNTAX

mac-authentication max-mac-count *count*

no mac-authentication max-mac-count

count - The maximum number of MAC-authenticated MAC addresses allowed. (Range: 1-1024)

DEFAULT SETTING

1024

COMMAND MODE

Interface Configuration

EXAMPLE

```
Console(config-if)#mac-authentication max-mac-count 32
Console(config-if)#
```

clear network-access

Use this command to clear entries from the secure MAC addresses table.

SYNTAX

clear network-access mac-address-table [**static** | **dynamic**] [**address** *mac-address*] [**interface** *interface*]

static - Specifies static address entries.

dynamic - Specifies dynamic address entries.

mac-address - Specifies a MAC address entry. (Format: xx-xx-xx-xx-xx-xx)

interface - Specifies a port interface.

ethernet *unit/port*

unit - This is unit 1.

port - Port number. (Range: 1-28)

DEFAULT SETTING

None

COMMAND MODE

Privileged Exec

EXAMPLE

```
Console#clear network-access mac-address-table interface ethernet 1/1
Console#
```

show network-access

Use this command to display the MAC authentication settings for port interfaces.

SYNTAX

show network-access [**interface** *interface*]

interface - Specifies a port interface.

ethernet *unit/port*

unit - Unit identifier. (Range: 1)

port - Port number. (Range: 1-28)

DEFAULT SETTING

Displays the settings for all interfaces.

COMMAND MODE

Privileged Exec

EXAMPLE

```
Console#show network-access interface ethernet 1/1
Global secure port information
Reauthentication Time                      : 1800
MAC Address Aging                          : Enabled

Port : 1/1
MAC Authentication                         : Disabled
MAC Authentication Intrusion Action        : Block traffic
MAC Authentication Maximum MAC Counts      : 1024
Maximum MAC Counts                         : 2048
Dynamic VLAN Assignment                    : Enabled
Dynamic QoS Assignment                     : Disabled
MAC Filter ID                              : Disabled
Guest VLAN                                 : Disabled
Link Detection                             : Disabled
Detection Mode                             : Link-down
Detection Action                           : Trap
Console#
```

show network-access mac-address-table

Use this command to display secure MAC address table entries.

SYNTAX

show network-access mac-address-table [**static** | **dynamic**]
[**address** *mac-address* [*mask*]] [**interface** *interface*]
[**sort** {**address** | **interface**}]

static - Specifies static address entries.

dynamic - Specifies dynamic address entries.

mac-address - Specifies a MAC address entry.
(Format: xx-xx-xx-xx-xx-xx)

mask - Specifies a MAC address bit mask for filtering displayed addresses.

interface - Specifies a port interface.

ethernet *unit*/*port*

unit - Unit identifier. (Range: 1)

port - Port number. (Range: 1-28)

sort - Sorts displayed entries by either MAC address or interface.

DEFAULT SETTING

Displays all filters.

COMMAND MODE

Privileged Exec

COMMAND USAGE

When using a bit mask to filter displayed MAC addresses, a 1 means “care” and a 0 means “don't care”. For example, a MAC of 00-00-01-02-03-04 and mask FF-FF-FF-00-00-00 would result in all MACs in the range 00-00-01-

00-00-00 to 00-00-01-FF-FF-FF to be displayed. All other MACs would be filtered out.

EXAMPLE

```
Console#show network-access mac-address-table
---- ----------------- --------------- --------- -------------------------
Port MAC-Address       RADIUS-Server   Attribute Time
---- ----------------- --------------- --------- -------------------------
1/1  00-00-01-02-03-04 172.155.120.17  Static    00d06h32m50s
1/1  00-00-01-02-03-05 172.155.120.17  Dynamic   00d06h33m20s
1/1  00-00-01-02-03-06 172.155.120.17  Static    00d06h35m10s
1/3  00-00-01-02-03-07 172.155.120.17  Dynamic   00d06h34m20s

Console#
```

show network-access mac-filter

Use this command to display information for entries in the MAC filter tables.

SYNTAX

show network-access mac-filter [*filter-id*]

filter-id - Specifies a MAC address filter table. (Range: 1-64)

DEFAULT SETTING

Displays all filters.

COMMAND MODE

Privileged Exec

EXAMPLE

```
Console#show network-access mac-filter
Filter ID MAC Address       MAC Mask
--------- ----------------- -----------------
        1 00-00-01-02-03-08 FF-FF-FF-FF-FF-FF
Console#
```

WEB AUTHENTICATION

Web authentication allows stations to authenticate and access the network in situations where 802.1X or Network Access authentication are infeasible or impractical. The web authentication feature allows unauthenticated hosts to request and receive a DHCP assigned IP address and perform DNS queries. All other traffic, except for HTTP protocol traffic, is blocked. The switch intercepts HTTP protocol traffic and redirects it to a switch-generated web page that facilitates user name and password authentication via RADIUS. Once authentication is successful, the web browser is forwarded on to the originally requested web page. Successful authentication is valid for all hosts connected to the port.

NOTE: RADIUS authentication must be activated and configured for the web authentication feature to work properly (see "Authentication Sequence" on page 1034).

NOTE: Web authentication cannot be configured on trunk ports.

Table 117: Web Authentication

Command	Function	Mode
web-auth login-attempts	Defines the limit for failed web authentication login attempts	GC
web-auth quiet-period	Defines the amount of time to wait after the limit for failed login attempts is exceeded.	GC
web-auth session-timeout	Defines the amount of time a session remains valid	GC
web-auth system-auth-control	Enables web authentication globally for the switch	GC
web-auth	Enables web authentication for an interface	IC
web-auth re-authenticate (Port)	Ends all web authentication sessions on the port and forces the users to re-authenticate	PE
web-auth re-authenticate (IP)	Ends the web authentication session associated with the designated IP address and forces the user to re-authenticate	PE
show web-auth	Displays global web authentication parameters	PE
show web-auth interface	Displays interface-specific web authentication parameters and statistics	PE
show web-auth summary	Displays a summary of web authentication port parameters and statistics	PE

web-auth login-attempts

This command defines the limit for failed web authentication login attempts. After the limit is reached, the switch refuses further login attempts until the quiet time expires. Use the **no** form to restore the default.

SYNTAX

web-auth login-attempts *count*

no web-auth login-attempts

count - The limit of allowed failed login attempts. (Range: 1-3)

DEFAULT SETTING

3 login attempts

COMMAND MODE

Global Configuration

EXAMPLE

```
Console(config)#web-auth login-attempts 2
Console(config)#
```

web-auth quiet-period

This command defines the amount of time a host must wait after exceeding the limit for failed login attempts, before it may attempt web authentication again. Use the **no** form to restore the default.

SYNTAX

web-auth quiet-period *time*

no web-auth quiet period

time - The amount of time the host must wait before attempting authentication again. (Range: 1-180 seconds)

DEFAULT SETTING

60 seconds

COMMAND MODE

Global Configuration

EXAMPLE

```
Console(config)#web-auth quiet-period 120
Console(config)#
```

web-auth session-timeout

This command defines the amount of time a web-authentication session remains valid. When the session timeout has been reached, the host is logged off and must re-authenticate itself the next time data transmission takes place. Use the **no** form to restore the default.

SYNTAX

web-auth session-timeout *timeout*

no web-auth session timeout

timeout - The amount of time that an authenticated session remains valid. (Range: 300-3600 seconds)

DEFAULT SETTING

3600 seconds

COMMAND MODE

Global Configuration

EXAMPLE

```
Console(config)#web-auth session-timeout 1800
Console(config)#
```

web-auth system-auth-control

This command globally enables web authentication for the switch. Use the **no** form to restore the default.

SYNTAX

[**no**] **web-auth system-auth-control**

DEFAULT SETTING

Disabled

COMMAND MODE

Global Configuration

COMMAND USAGE

Both **web-auth system-auth-control** for the switch and web-auth for an interface must be enabled for the web authentication feature to be active.

EXAMPLE

```
Console(config)#web-auth system-auth-control
Console(config)#
```

web-auth

This command enables web authentication for an interface. Use the no form to restore the default.

SYNTAX

[**no**] **web-auth**

DEFAULT SETTING

Disabled

COMMAND MODE

Interface Configuration

COMMAND USAGE

Both web-auth system-auth-control for the switch and **web-auth** for a port must be enabled for the web authentication feature to be active.

EXAMPLE

```
Console(config-if)#web-auth
Console(config-if)#
```

web-auth re-authenticate (Port)

This command ends all web authentication sessions connected to the port and forces the users to re-authenticate.

SYNTAX

web-auth re-authenticate interface *interface*

interface - Specifies a port interface.

ethernet *unit*/*port*

unit - This is unit 1.

port - Port number. (Range: 1-28)

DEFAULT SETTING

None

COMMAND MODE

Privileged Exec

EXAMPLE

```
Console#web-auth re-authenticate interface ethernet 1/2
Console#
```

web-auth re-authenticate (IP)

This command ends the web authentication session associated with the designated IP address and forces the user to re-authenticate.

SYNTAX

web-auth re-authenticate interface *interface ip*

interface - Specifies a port interface.

ethernet *unit*/*port*

unit - This is unit 1.

port - Port number. (Range: 1-28)

ip - IPv4 formatted IP address

DEFAULT SETTING

None

COMMAND MODE

Privileged Exec

EXAMPLE

```
Console#web-auth re-authenticate interface ethernet 1/2 192.168.1.5
Console#
```

show web-auth

This command displays global web authentication parameters.

COMMAND MODE

Privileged Exec

EXAMPLE

```
Console#show web-auth
Global Web-Auth Parameters
  System Auth Control       : Enabled
  Session Timeout           : 3600
  Quiet Period              : 60
  Max Login Attempts        : 3
Console#
```

show web-auth interface

This command displays interface-specific web authentication parameters and statistics.

SYNTAX

show web-auth interface *interface*

interface - Specifies a port interface.

ethernet *unit*/*port*

unit - This is unit 1.

port - Port number. (Range: 1-28)

COMMAND MODE

Privileged Exec

EXAMPLE

```
Console#show web-auth interface ethernet 1/2
Web Auth Status      : Enabled

Host Summary

IP address      Web-Auth-State Remaining-Session-Time
--------------- -------------- ----------------------
1.1.1.1         Authenticated  295
1.1.1.2         Authenticated  111
Console#
```

show web-auth summary

This command displays a summary of web authentication port parameters and statistics.

COMMAND MODE

Privileged Exec

EXAMPLE

```
Console#show web-auth summary
Global Web-Auth Parameters
  System Auth Control      : Enabled
Port       Status         Authenticated Host Count
----       ------         ------------------------
1/ 1       Disabled       0
1/ 2       Enabled        8
1/ 3       Disabled       0
1/ 4       Disabled       0
1/ 5       Disabled       0
 ⋮
```

DHCPV4 SNOOPING

DHCPv4 snooping allows a switch to protect a network from rogue DHCPv4 servers or other devices which send port-related information to a DHCPv4 server. This information can be useful in tracking an IP address back to a physical port. This section describes commands used to configure DHCPv4 snooping.

Table 118: DHCP Snooping Commands

Command	Function	Mode
ip dhcp snooping	Enables DHCP snooping globally	GC
ip dhcp snooping information option	Enables or disables the use of DHCP Option 82 information, and specifies frame format for the remote-id	GC
ip dhcp snooping information policy	Sets the information option policy for DHCP client packets that include Option 82 information	GC
ip dhcp snooping verify mac-address	Verifies the client’s hardware address stored in the DHCP packet against the source MAC address in the Ethernet header	GC
ip dhcp snooping vlan	Enables DHCP snooping on the specified VLAN	GC
ip dhcp snooping information option circuit-id	Specifies DHCP Option 82 circuit-id suboption information	IC
ip dhcp snooping trust	Configures the specified interface as trusted	IC
clear ip dhcp snooping binding	Clears DHCP snooping binding table entries from RAM	PE
clear ip dhcp snooping database flash	Removes all dynamically learned snooping entries from flash memory.	PE
ip dhcp snooping database flash	Writes all dynamically learned snooping entries to flash memory	PE

Table 118: DHCP Snooping Commands (Continued)

Command	Function	Mode
show ip dhcp snooping	Shows the DHCP snooping configuration settings	PE
show ip dhcp snooping binding	Shows the DHCP snooping binding table entries	PE

ip dhcp snooping

This command enables DHCP snooping globally. Use the **no** form to restore the default setting.

SYNTAX

[no] ip dhcp snooping

DEFAULT SETTING

Disabled

COMMAND MODE

Global Configuration

COMMAND USAGE

- Network traffic may be disrupted when malicious DHCP messages are received from an outside source. DHCP snooping is used to filter DHCP messages received on an unsecure interface from outside the network or fire wall. When DHCP snooping is enabled globally by this command, and enabled on a VLAN interface by the ip dhcp snooping vlan command, DHCP messages received on an untrusted interface (as specified by the no ip dhcp snooping trust command) from a device not listed in the DHCP snooping table will be dropped.

- When enabled, DHCP messages entering an untrusted interface are filtered based upon dynamic entries learned via DHCP snooping.

- Table entries are only learned for trusted interfaces. Each entry includes a MAC address, IP address, lease time, VLAN identifier, and port identifier.

- When DHCP snooping is enabled, the rate limit for the number of DHCP messages that can be processed by the switch is 100 packets per second. Any DHCP packets in excess of this limit are dropped.

- Filtering rules are implemented as follows:

  - If global DHCP snooping is disabled, all DHCP packets are forwarded.

  - If DHCP snooping is enabled globally, and also enabled on the VLAN where the DHCP packet is received, all DHCP packets are forwarded for a *trusted* port. If the received packet is a DHCP ACK message, a dynamic DHCP snooping entry is also added to the binding table.

  - If DHCP snooping is enabled globally, and also enabled on the VLAN where the DHCP packet is received, but the port is *not trusted*, it is processed as follows:

    - If the DHCP packet is a reply packet from a DHCP server (including OFFER, ACK or NAK messages), the packet is dropped.
    - If the DHCP packet is from a client, such as a DECLINE or RELEASE message, the switch forwards the packet only if the corresponding entry is found in the binding table.
    - If the DHCP packet is from client, such as a DISCOVER, REQUEST, INFORM, DECLINE or RELEASE message, the packet is forwarded if MAC address verification is disabled (as specified by the ip dhcp snooping verify mac-address command). However, if MAC address verification is enabled, then the packet will only be forwarded if the client's hardware address stored in the DHCP packet is the same as the source MAC address in the Ethernet header.
    - If the DHCP packet is not a recognizable type, it is dropped.

  - If a DHCP packet from a client passes the filtering criteria above, it will only be forwarded to trusted ports in the same VLAN.

  - If a DHCP packet is from server is received on a trusted port, it will be forwarded to both trusted and untrusted ports in the same VLAN.

- If DHCP snooping is globally disabled, all dynamic bindings are removed from the binding table.

- *Additional considerations when the switch itself is a DHCP client* – The port(s) through which the switch submits a client request to the DHCP server must be configured as trusted (using the ip dhcp snooping trust command). Note that the switch will not add a dynamic entry for itself to the binding table when it receives an ACK message from a DHCP server. Also, when the switch sends out DHCP client packets for itself, no filtering takes place. However, when the switch receives any messages from a DHCP server, any packets received from untrusted ports are dropped.

EXAMPLE

This example enables DHCP snooping globally for the switch.

```
Console(config)#ip dhcp snooping
Console(config)#
```

RELATED COMMANDS

ip dhcp snooping vlan (1121)
ip dhcp snooping trust (1123)

ip dhcp snooping information option

This command enables the use of DHCP Option 82 information for the switch, and specifies the frame format to use for the remote-id when Option 82 information is generated by the switch. Use the **no** form without any keywords to disable this function, the **no** form with the **encode no-subtype** keyword to enable use of sub-type and sub-length in CID/RID fields, or the **no** form with the **remote-id** keyword to set the remote ID to the switch's MAC address encoded in hexadecimal.

SYNTAX

ip dhcp snooping information option
[**encode no-subtype**]
[**remote-id** {**ip-address** [**encode** {**ascii** | **hex**}] |
mac-address [**encode** {**ascii** | **hex**}] | **string** *string*}]

no ip dhcp snooping information option [**encode no-subtype**]
[**remote-id** [**ip-address encode**] | [**mac-address encode**]]

encode no-subtype - Disables use of sub-type and sub-length fields in circuit-ID (CID) and remote-ID (RID) in Option 82 information.

mac-address - Inserts a MAC address in the remote ID sub-option for the DHCP snooping agent (that is, the MAC address of the switch's CPU).

ip-address - Inserts an IP address in the remote ID sub-option for the DHCP snooping agent (that is, the IP address of the management interface).

encode - Indicates encoding in ASCII or hexadecimal.

string - An arbitrary string inserted into the remote identifier field. (Range: 1-32 characters)

DEFAULT SETTING

Option 82: Disabled
CID/RID sub-type: Enabled
Remote ID: MAC address (hexadecimal)

COMMAND MODE

Global Configuration

COMMAND USAGE

- DHCP provides a relay mechanism for sending information about the switch and its DHCP clients to the DHCP server. Known as DHCP Option 82, it allows compatible DHCP servers to use the information when assigning IP addresses, or to set other services or policies for clients.

- When the DHCP Snooping Information Option 82 is enabled, the requesting client (or an intermediate relay agent that has used the information fields to describe itself) can be identified in the DHCP request packets forwarded by the switch and in reply packets sent back from the DHCP server.

- When the DHCP Snooping Information Option is enabled, clients can be identified by the switch port to which they are connected rather than just their MAC address. DHCP client-server exchange messages are then forwarded directly between the server and client without having to flood them to the entire VLAN.

- DHCP snooping must be enabled for the DHCP Option 82 information to be inserted into packets. When enabled, the switch will only add/ remove option 82 information in incoming DCHP packets but not relay them. Packets are processed as follows:
  - If an incoming packet is a DHCP request packet with option 82 information, it will modify the option 82 information according to settings specified with ip dhcp snooping information policy command.
  - If an incoming packet is a DHCP request packet without option 82 information, enabling the DHCP snooping information option will add option 82 information to the packet.
  - If an incoming packet is a DHCP reply packet with option 82 information, enabling the DHCP snooping information option will remove option 82 information from the packet.

EXAMPLE

This example enables the DHCP Snooping Information Option.

```
Console(config)#ip dhcp snooping information option
Console(config)#
```

ip dhcp snooping information policy

This command sets the DHCP snooping information option policy for DHCP client packets that include Option 82 information.

SYNTAX

ip dhcp snooping information policy {**drop** | **keep** | **replace**}

drop - Drops the client’s request packet instead of relaying it.

keep - Retains the Option 82 information in the client request, and forwards the packets to trusted ports.

replace - Replaces the Option 82 information circuit-id and remote-id fields in the client’s request with information about the relay agent itself, inserts the relay agent’s address (when DHCP snooping is enabled), and forwards the packets to trusted ports.

DEFAULT SETTING

replace

COMMAND MODE

Global Configuration

COMMAND USAGE

When the switch receives DHCP packets from clients that already include DHCP Option 82 information, the switch can be configured to set the action policy for these packets. The switch can either drop the DHCP packets, keep the existing information, or replace it with the switch's relay information.

EXAMPLE

```
Console(config)#ip dhcp snooping information policy drop
Console(config)#
```

ip dhcp snooping verify mac-address

This command verifies the client's hardware address stored in the DHCP packet against the source MAC address in the Ethernet header. Use the **no** form to disable this function.

SYNTAX

[**no**] **ip dhcp binding verify mac-address**

DEFAULT SETTING

Enabled

COMMAND MODE

Global Configuration

COMMAND USAGE

If MAC address verification is enabled, and the source MAC address in the Ethernet header of the packet is not same as the client's hardware address in the DHCP packet, the packet is dropped.

EXAMPLE

This example enables MAC address verification.

```
Console(config)#ip dhcp snooping verify mac-address
Console(config)#
```

RELATED COMMANDS

ip dhcp snooping (1116)
ip dhcp snooping vlan (1121)
ip dhcp snooping trust (1123)

ip dhcp snooping vlan

This command enables DHCP snooping on the specified VLAN. Use the **no** form to restore the default setting.

SYNTAX

[**no**] **ip dhcp snooping vlan** *vlan-id*

vlan-id - ID of a configured VLAN (Range: 1-4094)

DEFAULT SETTING

Disabled

COMMAND MODE

Global Configuration

COMMAND USAGE

- When DHCP snooping is enabled globally using the ip dhcp snooping command, and enabled on a VLAN with this command, DHCP packet filtering will be performed on any untrusted ports within the VLAN as specified by the ip dhcp snooping trust command.

- When the DHCP snooping is globally disabled, DHCP snooping can still be configured for specific VLANs, but the changes will not take effect until DHCP snooping is globally re-enabled.

- When DHCP snooping is globally enabled, and then disabled on a specific VLAN, all dynamic bindings learned for this VLAN are removed from the binding table.

EXAMPLE

This example enables DHCP snooping for VLAN 1.

```
Console(config)#ip dhcp snooping vlan 1
Console(config)#
```

RELATED COMMANDS

ip dhcp snooping (1116)
ip dhcp snooping trust (1123)

ip dhcp snooping information option circuit-id

This command specifies DHCP Option 82 circuit-id suboption information. Use the **no** form to use the default settings.

SYNTAX

ip dhcp snooping information option circuit-id string *string*

no dhcp snooping information option circuit-id

string - An arbitrary string inserted into the circuit identifier field. (Range: 1-32 characters)

DEFAULT SETTING

VLAN-Unit-Port

COMMAND MODE

Interface Configuration (Ethernet, Port Channel)

COMMAND USAGE

- DHCP provides a relay mechanism for sending information about the switch and its DHCP clients to the DHCP server. DHCP Option 82 allows compatible DHCP servers to use the information when assigning IP addresses, to set other services or policies for clients. For more information of this process, refer to the Command Usage section under the ip dhcp snooping information option command.

- Option 82 information generated by the switch is based on TR-101 syntax as shown below:

  Table 119: Option 82 information

82	3-69	1	1-67	x1	x2	x3	x4	x5	x63
opt82	opt-len	sub-opt1	string-len	R-124 string					

  The circuit identifier used by this switch starts at sub-option1 and goes to the end of the R-124 string. The R-124 string includes the following information:

  - sub-type - Distinguishes different types of circuit IDs.
  - sub-length - Length of the circuit ID type
  - access node identifier - ASCII string. Default is the MAC address of the switch's CPU. This field is set by the ip dhcp snooping information option command,
  - eth - The second field is the fixed string "eth"
  - slot - The slot represents the stack unit for this system.
  - port - The port which received the DHCP request. If the packet arrives over a trunk, the value is the ifIndex of the trunk.
  - vlan - Tag of the VLAN which received the DHCP request.

    Note that the sub-type and sub-length fields can be enabled or disabled using the ip dhcp snooping information option command.

- The **ip dhcp snooping information option circuit-id** command can be used to modify the default settings described above.

EXAMPLE

This example sets the DHCP Snooping Information circuit-id suboption string.

```
Console(config)#interface ethernet 1/1
Console(config-if)#ip dhcp snooping information option circuit-id string 4500
Console(config-if)#
```

ip dhcp snooping trust

This command configures the specified interface as trusted. Use the **no** form to restore the default setting.

SYNTAX

[**no**] **ip dhcp snooping trust**

DEFAULT SETTING

All interfaces are untrusted

COMMAND MODE

Interface Configuration (Ethernet, Port Channel)

COMMAND USAGE

- A trusted interface is an interface that is configured to receive only messages from within the network. An untrusted interface is an interface that is configured to receive messages from outside the network or fire wall.

- Set all ports connected to DHCP servers within the local network or fire wall to trusted, and all other ports outside the local network or fire wall to untrusted.

- When DHCP snooping is enabled globally using the ip dhcp snooping command, and enabled on a VLAN with ip dhcp snooping vlan command, DHCP packet filtering will be performed on any untrusted ports within the VLAN according to the default status, or as specifically configured for an interface with the **no ip dhcp snooping trust** command.

- When an untrusted port is changed to a trusted port, all the dynamic DHCP snooping bindings associated with this port are removed.

- *Additional considerations when the switch itself is a DHCP client* – The port(s) through which it submits a client request to the DHCP server must be configured as trusted.

EXAMPLE

This example sets port 5 to untrusted.

```
Console(config)#interface ethernet 1/5
Console(config-if)#no ip dhcp snooping trust
Console(config-if)#
```

RELATED COMMANDS

ip dhcp snooping (1116)
ip dhcp snooping vlan (1121)

clear ip dhcp snooping binding

This command clears DHCP snooping binding table entries from RAM. Use this command without any optional keywords to clear all entries from the binding table.

SYNTAX

clear ip dhcp snooping binding [*mac-address* **vlan** *vlan-id*]

mac-address - Specifies a MAC address entry. (Format: xx-xx-xx-xx-xx-xx)

vlan-id - ID of a configured VLAN (Range: 1-4094)

COMMAND MODE

Privileged Exec

EXAMPLE

```
Console(config)#clear ip dhcp snooping binding 11-22-33-44-55-66 vlan 1
Console(config)#
```

clear ip dhcp snooping database flash

This command removes all dynamically learned snooping entries from flash memory.

COMMAND MODE

Privileged Exec

EXAMPLE

```
Console(config)#clear ip dhcp snooping database flash
Console(config)#
```

ip dhcp snooping database flash

This command writes all dynamically learned snooping entries to flash memory.

COMMAND MODE

Privileged Exec

COMMAND USAGE

This command can be used to store the currently learned dynamic DHCP snooping entries to flash memory. These entries will be restored to the snooping table when the switch is reset. However, note that the lease time shown for a dynamic entry that has been restored from flash memory will no longer be valid.

EXAMPLE

```
Console#ip dhcp snooping database flash
Console#
```

show ip dhcp snooping

This command shows the DHCP snooping configuration settings.

COMMAND MODE

Privileged Exec

EXAMPLE

```
Console#show ip dhcp snooping
Global DHCP Snooping Status: enabled
DHCP Snooping Information Option Status: enabled
DHCP Snooping Information Option Sub-option Format: extra subtype included
DHCP Snooping Information Option Remote ID: MAC Address (ascii encoded)
DHCP Snooping Information Policy: replace
DHCP Snooping is configured on the following VLANs:
   1,
Verify Source MAC-Address: enabled
Interface           Trusted       Circuit-ID Value
----------          ----------    --------------------------------
Eth 1/1             Yes           park 19
Eth 1/2             No            ---
Eth 1/3             No            ---
Eth 1/4             No            ---
Eth 1/5             No            ---
.
.
.
```

show ip dhcp snooping binding

This command shows the DHCP snooping binding table entries.

COMMAND MODE

Privileged Exec

EXAMPLE

```
Console#show ip dhcp snooping binding
MAC Address       IP Address      Lease(sec) Type                 VLAN Interface
----------------- --------------- ---------- -------------------- ---- ---------
11-22-33-44-55-66 192.168.0.99             0 Dynamic-DHCPSNP         1 Eth 1/5
Console#
```

DHCPv6 SNOOPING

DHCPv6 snooping allows a switch to protect a network from rogue DHCPv6 servers or other devices which send port-related information to a DHCPv6 server. This information can be useful in tracking an IP address back to a physical port. This section describes commands used to configure DHCPv6 snooping.

Table 120: DHCP Snooping Commands

Command	Function	Mode
ipv6 dhcp snooping	Enables DHCPv6 snooping globally	GC
ipv6 dhcp snooping vlan	Enables DHCPv6 snooping on the specified VLAN	GC
ipv6 dhcp snooping max-binding	Sets the maximum number of entries which can be stored in the binding database for an interface	IC
ipv6 dhcp snooping trust	Configures the specified interface as trusted	IC
clear ipv6 dhcp snooping binding	Clears DHCPv6 snooping binding table entries from RAM	PE
clear ipv6 dhcp snooping statistics	Clears statistical counters for DHCPv6 snooping client, server and relay packets	PE
show ipv6 dhcp snooping	Shows the DHCPv6 snooping configuration settings	PE
show ipv6 dhcp snooping binding	Shows the DHCPv6 snooping binding table entries	PE
show ipv6 dhcp snooping statistics	Shows statistics for DHCPv6 snooping client, server and relay packets	PE

ipv6 dhcp snooping

This command enables DHCPv6 snooping globally. Use the **no** form to restore the default setting.

SYNTAX

[**no**] **ipv6 dhcp snooping**

DEFAULT SETTING

Disabled

COMMAND MODE

Global Configuration

COMMAND USAGE

- Network traffic may be disrupted when malicious DHCPv6 messages are received from an outside source. DHCPv6 snooping is used to filter DHCPv6 messages received on an unsecure interface from outside the network or fire wall. When DHCPv6 snooping is enabled globally by this command, and enabled on a VLAN interface by the ipv6 dhcp snooping vlan command, DHCP messages received on an untrusted interface (as specified by the no ipv6 dhcp snooping trust command) from a device not listed in the DHCPv6 snooping table will be dropped.

- When enabled, DHCPv6 messages entering an untrusted interface are filtered based upon dynamic entries learned via DHCPv6 snooping.

- Table entries are only learned for trusted interfaces. Each entry includes a MAC address, IPv6 address, lease time, binding type, VLAN identifier, and port identifier.

- When DHCPv6 snooping is enabled, the rate limit for the number of DHCPv6 messages that can be processed by the switch is 100 packets per second. Any DHCPv6 packets in excess of this limit are dropped.

- Filtering rules are implemented as follows:

  - If global DHCPv6 snooping is disabled, all DHCPv6 packets are forwarded.

  - If DHCPv6 snooping is enabled globally, and also enabled on the VLAN where the DHCPv6 packet is received, DHCPv6 packets are forwarded for a *trusted* port as described below.

  - If DHCPv6 snooping is enabled globally, and also enabled on the VLAN where the DHCP packet is received, but the port is *not trusted*, DHCP packets are processed according to message type as follows:

    DHCP Client Packet

    - Request: Update entry in binding cache, recording client's DHCPv6 Unique Identifier (DUID), server's DUID, Identity Association (IA) type, IA Identifier, and address (4 message exchanges to get IPv6 address), and forward to trusted port.
    - Solicit: Add new entry in binding cache, recording client's DUID, IA type, IA ID (2 message exchanges to get IPv6 address with rapid commit option, otherwise 4 message exchanges), and forward to trusted port.
    - Decline: If no matching entry is found in binding cache, drop this packet.
    - Renew, Rebind, Release, Confirm: If no matching entry is found in binding cache, drop this packet.
    - If the DHCPv6 packet is not a recognizable type, it is dropped.

If a DHCPv6 packet from a client passes the filtering criteria above, it will only be forwarded to trusted ports in the same VLAN.

DHCP Server Packet

- If a DHCP server packet is received on an *untrusted* port, drop this packet and add a log entry in the system.
- If a DHCPv6 Reply packet is received from a server on a *trusted* port, it will be processed in the following manner:

  A. Check if IPv6 address in IA option is found in binding table:

  - If yes, continue to C.
  - If not, continue to B.

  B. Check if IPv6 address in IA option is found in binding cache:

  - If yes, continue to C.
  - If not, check failed, and forward packet to trusted port.

  C. Check status code in IA option:

  - If successful, and entry is in binding table, update lease time and forward to original destination.
  - If successful, and entry is in binding cache, move entry from binding cache to binding table, update lease time and forward to original destination.
  - Otherwise, remove binding entry. and check failed.

- If a DHCPv6 Relay packet is received, check the relay message option in Relay-Forward or Relay-Reply packet, and process client and server packets as described above.

◆ If DHCPv6 snooping is globally disabled, all dynamic bindings are removed from the binding table.

◆ *Additional considerations when the switch itself is a DHCPv6 client* – The port(s) through which the switch submits a client request to the DHCPv6 server must be configured as trusted (using the ipv6 dhcp snooping trust command). Note that the switch will not add a dynamic entry for itself to the binding table when it receives an ACK message from a DHCPv6 server. Also, when the switch sends out DHCPv6 client packets for itself, no filtering takes place. However, when the switch receives any messages from a DHCPv6 server, any packets received from untrusted ports are dropped.

EXAMPLE

This example enables DHCPv6 snooping globally for the switch.

```
Console(config)#ipv6 dhcp snooping
Console(config)#
```

RELATED COMMANDS

ipv6 dhcp snooping vlan (1129)
ipv6 dhcp snooping trust (1130)

ipv6 dhcp snooping vlan

This command enables DHCPv6 snooping on the specified VLAN. Use the **no** form to restore the default setting.

SYNTAX

[**no**] **ipv6 dhcp snooping vlan** {*vlan-id* | *vlan-range*}

vlan-id - ID of a configured VLAN (Range: 1-4094)

vlan-range - A consecutive range of VLANs indicated by the use a hyphen, or a random group of VLANs with each entry separated by a comma.

DEFAULT SETTING

Disabled

COMMAND MODE

Global Configuration

COMMAND USAGE

- When DHCPv6 snooping enabled globally using the ipv6 dhcp snooping command, and enabled on a VLAN with this command, DHCPv6 packet filtering will be performed on any untrusted ports within the VLAN as specified by the ipv6 dhcp snooping trust command.

- When the DHCPv6 snooping is globally disabled, DHCPv6 snooping can still be configured for specific VLANs, but the changes will not take effect until DHCPv6 snooping is globally re-enabled.

- When DHCPv6 snooping is enabled globally, and then disabled on a VLAN, all dynamic bindings learned for this VLAN are removed from the binding table.

EXAMPLE

This example enables DHCP6 snooping for VLAN 1.

```
Console(config)#ipv6 dhcp snooping vlan 1
Console(config)#
```

RELATED COMMANDS

ipv6 dhcp snooping (1126)
ipv6 dhcp snooping trust (1130)

ipv6 dhcp snooping max-binding

This command sets the maximum number of entries which can be stored in the binding database for an interface. Use the **no** form to restore the default setting.

SYNTAX

ipv6 dhcp snooping max-binding *count*

no ipv6 dhcp snooping max-binding

count - Maximum number of entries. (Range: 1-5)

DEFAULT SETTING

5

COMMAND MODE

Interface Configuration (Ethernet, Port Channel)

EXAMPLE

This example sets the maximum number of binding entries to 1.

```
Console(config)#interface ethernet 1/1
Console(config-if)#ipv6 dhcp snooping max-binding 1
Console(config-if)#
```

ipv6 dhcp snooping trust

This command configures the specified interface as trusted. Use the **no** form to restore the default setting.

SYNTAX

[**no**] **ipv6 dhcp snooping trust**

DEFAULT SETTING

All interfaces are untrusted

COMMAND MODE

Interface Configuration (Ethernet, Port Channel)

COMMAND USAGE

- A trusted interface is an interface that is configured to receive only messages from within the network. An untrusted interface is an interface that is configured to receive messages from outside the network or fire wall.

- Set all ports connected to DHCv6 servers within the local network or fire wall to trusted, and all other ports outside the local network or fire wall to untrusted.

- When DHCPv6 snooping is enabled globally using the ipv6 dhcp snooping command, and enabled on a VLAN with ipv6 dhcp snooping vlan command, DHCPv6 packet filtering will be performed on any untrusted ports within the VLAN according to the default status, or as specifically configured for an interface with the **no ipv6 dhcp snooping trust** command.

- When an untrusted port is changed to a trusted port, all the dynamic DHCPv6 snooping bindings associated with this port are removed.

- *Additional considerations when the switch itself is a DHCPv6 client* – The port(s) through which it submits a client request to the DHCPv6 server must be configured as trusted.

EXAMPLE

This example sets port 5 to untrusted.

```
Console(config)#interface ethernet 1/5
Console(config-if)#no ipv6 dhcp snooping trust
Console(config-if)#
```

RELATED COMMANDS

ipv6 dhcp snooping (1126)
ipv6 dhcp snooping vlan (1129)

clear ipv6 dhcp snooping binding

This command clears DHCPv6 snooping binding table entries from RAM. Use this command without any optional keywords to clear all entries from the binding table.

SYNTAX

clear ipv6 dhcp snooping binding [*mac-address ipv6-address*]

mac-address - Specifies a MAC address entry. (Format: xx-xx-xx-xx-xx-xx)

ipv6-address - Corresponding IPv6 address. This address must be entered according to RFC 2373 “IPv6 Addressing Architecture,” using 8 colon-separated 16-bit hexadecimal values. One double colon may be used in the address to indicate the appropriate number of zeros required to fill the undefined fields.

COMMAND MODE

Privileged Exec

EXAMPLE

```
Console(config)#clear ipv6 dhcp snooping binding 00-12-cf-01-02-03 2001::1
Console(config)#
```

clear ipv6 dhcp snooping statistics

This command clears statistical counters for DHCPv6 snooping client, server and relay packets.

COMMAND MODE

Privileged Exec

EXAMPLE

```
Console(config)#clear ipv6 dhcp snooping statistics
Console(config)#
```

show ipv6 dhcp snooping

This command shows the DHCPv6 snooping configuration settings.

COMMAND MODE

Privileged Exec

EXAMPLE

```
Console#show ipv6 dhcp snooping
Global DHCPv6 Snooping status: disabled
DHCPv6 Snooping is configured on the following VLANs:
   1,
Interface           Trusted       Max-binding  Current-binding
---------           ---------     -----------  ---------------
Eth 1/1             No                      5                0
Eth 1/2             No                      5                0
Eth 1/3             No                      5                0
Eth 1/4             No                      5                0
Eth 1/5             Yes                     5                0
.
.
.
```

show ipv6 dhcp snooping binding

This command shows the DHCPv6 snooping binding table entries.

COMMAND MODE

Privileged Exec

EXAMPLE

```
Console#show ipv6 dhcp snooping binding
NA - Non-temporary address
TA - Temporary address
-------------------------------------- ----------- ---- ------- ----
Link-layer Address: 00-13-49-aa-39-26
IPv6 Address                            Lifetime   VLAN Port    Type
--------------------------------------- ---------- ---- ------- ----
2001:b021:1435:5612:ab3c:6792:a452:6712    2591998    1 Eth 1/5   NA
--------------------------------------- ---------- ---- ------- ----
Link-layer Address: 00-12-cf-01-02-03
IPv6 Address                            Lifetime   VLAN Port    Type
--------------------------------------- ---------- ---- ------- ----
                           2001:b000::1    2591912    1 Eth 1/3   NA
Console#
```

show ipv6 dhcp snooping statistics

This command shows statistics for DHCPv6 snooping client, server and relay packets.

COMMAND MODE

Privileged Exec

EXAMPLE

```
Console#show ipv6 dhcp snooping statistics
DHCPv6 Snooping Statistics:
    Client Packet: Solicit, Request, Confirm, Renew, Rebind,
                         Decline, Release, Information-request
    Server Packet: Advertise, Reply, Reconfigure
    Relay  Packet: Relay-forward, Relay-reply
State     Client    Server    Relay     Total
--------  --------  --------  --------  --------
Received        10         9         0        19
Sent             9         9         0        18
Droped           1         0         0         1

Console#
```

IPV4 SOURCE GUARD

IPv4 Source Guard is a security feature that filters IPv4 traffic on network interfaces based on manually configured entries in the IPv4 Source Guard table, or dynamic entries in the DHCPv4 Snooping table when enabled (see "DHCPv4 Snooping" on page 1115). IPv4 source guard can be used to prevent traffic attacks caused when a host tries to use the IPv4 address of a neighbor to access the network. This section describes commands used to configure IPv4 Source Guard.

Table 121: IPv4 Source Guard Commands

Command	Function	Mode
ip source-guard binding	Adds a static address to the source-guard binding table	GC
ip source-guard	Configures the switch to filter inbound traffic based on source IP address, or source IP address and corresponding MAC address	IC
ip source-guard max-binding	Sets the maximum number of entries that can be bound to an interface	IC
ip source-guard mode	Sets the source-guard learning mode to search for addresses in the ACL binding table or the MAC address binding table	IC
clear ip source-guard binding blocked	Remove all blocked records	IC
show ip source-guard	Shows whether source guard is enabled or disabled on each interface	PE
show ip source-guard binding	Shows the source guard binding table	PE

ip source-guard binding

This command adds a static address to the source-guard ACL or MAC address binding table. Use the **no** form to remove a static entry.

SYNTAX

ip source-guard binding [**mode** {**acl** | **mac**}] *mac-address* **vlan** *vlan-id ip-address* **interface ethernet** *unit/port*

no ip source-guard binding [**mode** {**acl** | **mac**}] *mac-address* **vlan** *vlan-id*

mode - Specifies the binding mode.

acl - Adds binding to ACL table.

mac - Adds binding to MAC address

mac-address - A valid unicast MAC address table.

vlan-id - ID of a configured VLAN (Range: 1-4094)

ip-address - A valid unicast IP address, including classful types A, B or C.

unit - Unit identifier. (Range: 1)

port - Port number. (Range: 1-28)

DEFAULT SETTING

No configured entries

COMMAND MODE

Global Configuration

COMMAND USAGE

- If the binding mode is not specified in this command, the entry is bound to the ACL table by default.

- Table entries include a MAC address, IP address, lease time, entry type (Static-IP-SG-Binding, Dynamic-DHCP-Binding), VLAN identifier, and port identifier.

- All static entries are configured with an infinite lease time, which is indicated with a value of zero by the show ip source-guard command (page 1139).

- When source guard is enabled, traffic is filtered based upon dynamic entries learned via DHCP snooping, or static addresses configured in the source guard binding table with this command.

- Static bindings are processed as follows:

  - If there is no entry with same VLAN ID and MAC address, a new entry is added to binding table using the type of static IP source guard binding.

- If there is an entry with same VLAN ID and MAC address, and the type of entry is static IP source guard binding, then the new entry will replace the old one.
- If there is an entry with same VLAN ID and MAC address, and the type of the entry is dynamic DHCP snooping binding, then the new entry will replace the old one and the entry type will be changed to static IP source guard binding.

EXAMPLE

This example configures a static source-guard binding on port 5. Since the binding mode is not specified, the entry is bound to the ACL table by default.

```
Console(config)#ip source-guard binding 00-ab-11-cd-23-45 vlan 1 192.168.0.99
  interface ethernet 1/5
Console(config)#
```

RELATED COMMANDS

ip source-guard (1135)
ip dhcp snooping (1116)
ip dhcp snooping vlan (1121)

ip source-guard

This command configures the switch to filter inbound traffic based on source IP address, or source IP address and corresponding MAC address. Use the **no** form to disable this function.

SYNTAX

ip source-guard {**sip** | **sip-mac**}

no ip source-guard

sip - Filters traffic based on IP addresses stored in the binding table.

sip-mac - Filters traffic based on IP addresses and corresponding MAC addresses stored in the binding table.

DEFAULT SETTING

Disabled

COMMAND MODE

Interface Configuration (Ethernet)

COMMAND USAGE

- Source guard is used to filter traffic on an insecure port which receives messages from outside the network or fire wall, and therefore may be subject to traffic attacks caused by a host trying to use the IP address of a neighbor.

- Setting source guard mode to “sip” or “sip-mac” enables this function on the selected port. Use the “sip” option to check the VLAN ID, source IP address, and port number against all entries in the binding table. Use the “sip-mac” option to check these same parameters, plus the source MAC address. Use the **no ip source guard** command to disable this function on the selected port.

- When enabled, traffic is filtered based upon dynamic entries learned via DHCP snooping, or static addresses configured in the source guard binding table.

- Table entries include a MAC address, IP address, lease time, entry type (Static-IP-SG-Binding, Dynamic-DHCP-Binding, VLAN identifier, and port identifier.

- Static addresses entered in the source guard binding table with the ip source-guard binding command are automatically configured with an infinite lease time. Dynamic entries learned via DHCP snooping are configured by the DHCP server itself.

- If the IP source guard is enabled, an inbound packet’s IP address (sip option) or both its IP address and corresponding MAC address (sip-mac option) will be checked against the binding table. If no matching entry is found, the packet will be dropped.

- Filtering rules are implemented as follows:

  - If DHCPv4 snooping is disabled (see page 1116), IP source guard will check the VLAN ID, source IP address, port number, and source MAC address (for the sip-mac option). If a matching entry is found in the binding table and the entry type is static IP source guard binding, the packet will be forwarded.

  - If the DHCP snooping is enabled, IP source guard will check the VLAN ID, source IP address, port number, and source MAC address (for the sip-mac option). If a matching entry is found in the binding table and the entry type is static IP source guard binding, or dynamic DHCP snooping binding, the packet will be forwarded.

  - If IP source guard if enabled on an interface for which IP source bindings (dynamically learned via DHCP snooping or manually configured) are not yet configured, the switch will drop all IP traffic on that port, except for DHCP packets.

  - Only unicast addresses are accepted for static bindings.

EXAMPLE

This example enables IP source guard on port 5.

```
Console(config)#interface ethernet 1/5
Console(config-if)#ip source-guard sip
Console(config-if)#
```

RELATED COMMANDS

ip source-guard binding (1134)
ip dhcp snooping (1116)
ip dhcp snooping vlan (1121)

ip source-guard max-binding

This command sets the maximum number of entries that can be bound to an interface. Use the **no** form to restore the default setting.

SYNTAX

ip source-guard [**mode** {**acl** | **mac**}] **max-binding** *number*

no ip source-guard [**mode** {**acl** | **mac**}] **max-binding**

mode - Specifies the learning mode.

acl - Searches for addresses in the ACL table.

mac - Searches for addresses in the MAC address table.

number - The maximum number of IP addresses that can be mapped to an interface in the binding table. (Range: 1-5 for ACL mode; 1-1024 for MAC mode)

DEFAULT SETTING

Mode: ACL
Maximum bindings: 5 for ACL mode, 1024 for MAC mode

COMMAND MODE

Interface Configuration (Ethernet)

COMMAND USAGE

This command sets the maximum number of address entries that can be mapped to an interface in the binding table, including both dynamic entries discovered by DHCP snooping and static entries set by the ip source-guard command.

EXAMPLE

This example sets the maximum number of allowed entries in the binding table for port 5 to one entry. The mode is not specified, and therefore defaults to the ACL binding table.

```
Console(config)#interface ethernet 1/5
Console(config-if)#ip source-guard max-binding 1
Console(config-if)#
```

ip source-guard mode

This command sets the source-guard learning mode to search for addresses in the ACL binding table or the MAC address binding table. Use the **no** form to restore the default setting.

SYNTAX

ip source-guard mode {**acl** | **mac**}

no ip source-guard mode

mode - Specifies the learning mode.

acl - Searches for addresses in the ACL table.

mac - Searches for addresses in the MAC address table.

DEFAULT SETTING

ACL

COMMAND MODE

Interface Configuration (Ethernet)

EXAMPLE

This command sets the binding table mode for the specified interface to MAC mode:

```
Console(config)#interface ethernet 1/5
Console(config-if)#ip source-guard mode mac
Console(config-if)#
```

clear ip source-guard binding blocked

This command remove all blocked records.

SYNTAX

clear ip source-guard binding blocked

COMMAND MODE

Privileged Exec

COMMAND USAGE

When IP Source-Guard detects an invalid packet it creates a blocked record. These records can be viewed using the show ip source-guard binding blocked command. A maximum of 512 blocked records can be stored before the switch overwrites the oldest record with new blocked records. Use the **clear ip source-guard binding blocked** command to clear this table.

EXAMPLE

This command clears the blocked record table.

```
Console(config)#clear ip source-guard binding blocked
Console(config)#
```

show ip source-guard

This command shows whether source guard is enabled or disabled on each interface.

COMMAND MODE

Privileged Exec

EXAMPLE

```
Console#show ip source-guard
                                         ACL Table     MAC Table
Interface   Filter-type   Filter-table   Max-binding   Max-binding
---------   -----------   ------------   -----------   -----------
Eth 1/1     DISABLED      ACL                      5          1024
Eth 1/2     DISABLED      ACL                      5          1024
Eth 1/3     DISABLED      ACL                      5          1024
Eth 1/4     DISABLED      ACL                      5          1024
Eth 1/5     DISABLED      ACL                      5          1024
⋮
```

show ip source-guard binding

This command shows the source guard binding table.

SYNTAX

show ip source-guard binding [**dhcp-snooping** |
static [**acl** | **mac**] | **blocked** [**vlan** *vlan-id* | **interface** *interface*]

dhcp-snooping - Shows dynamic entries configured with DHCP Snooping commands (see page 1115)

static - Shows static entries configured with the ip source-guard binding command (see page 1134).

acl - Shows static entries in the ACL binding table.

mac - Shows static entries in the MAC address binding table.

blocked - Shows blocked records of invalid packets.

vlan-id (Range: 1-4094)

interface

ethernet *unit/port*

unit - Unit identifier. (Range: 1)

port - Port number. (Range: 1-28)

COMMAND MODE

Privileged Exec

EXAMPLE

```
Console#show ip source-guard binding
MAC Address       IP Address      Lease(sec) Type           VLAN      Interface
----------------- --------------- ---------- -------------- --------- ---------
00-ab-11-cd-23-45 192.168.0.99             0 static-acl             1 Eth 1/5
Console#
```

IPV6 SOURCE GUARD

IPv6 Source Guard is a security feature that filters IPv6 traffic on non-routed, Layer 2 network interfaces based on manually configured entries in the IPv6 Source Guard table, or dynamic entries in the Neighbor Discovery Snooping table or DHCPv6 Snooping table when either snooping protocol is enabled (see "DHCPv6 Snooping" on page 1126). IPv6 source guard can be used to prevent traffic attacks caused when a host tries to use the IPv6 address of a neighbor to access the network. This section describes commands used to configure IPv6 Source Guard.

Table 122: IPv6 Source Guard Commands

Command	Function	Mode
ipv6 source-guard binding	Adds a static address to the source-guard binding table	GC
ipv6 source-guard	Configures the switch to filter inbound traffic based on source IP address	IC
ipv6 source-guard max-binding	Sets the maximum number of entries that can be bound to an interface	IC
show ipv6 source-guard	Shows whether source guard is enabled or disabled on each interface	PE
show ipv6 source-guard binding	Shows the source guard binding table	PE

ipv6 source-guard binding

This command adds a static address to the source-guard binding table. Use the **no** form to remove a static entry.

SYNTAX

ipv6 source-guard binding *mac-address* **vlan** *vlan-id ipv6-address* **interface** *interface*

no ipv6 source-guard binding *mac-address* **vlan** *vlan-id*

mac-address - A valid unicast MAC address.

vlan-id - ID of a configured VLAN (Range: 1-4094)

ipv6-address - Corresponding IPv6 address. This address must be entered according to RFC 2373 “IPv6 Addressing Architecture,” using 8 colon-separated 16-bit hexadecimal values. One double colon may be used in the address to indicate the appropriate number of zeros required to fill the undefined fields.

interface

ethernet *unit*/*port*

unit - Unit identifier. (Range: 1)

port - Port number. (Range: 1-28)

DEFAULT SETTING

No configured entries

COMMAND MODE

Global Configuration

COMMAND USAGE

- Table entries include an associated MAC address, IPv6 global unicast address, lease time, entry type (Static-IP-SG-Binding, Dynamic-ND-Binding, Dynamic-DHCPv6-Binding), VLAN identifier, and port identifier.

- Traffic filtering is based only on the source IPv6 address, VLAN ID, and port number.

- All static entries are configured with an infinite lease time, which is indicated with a value of zero by the show ipv6 source-guard command (page 1144).

- When source guard is enabled, traffic is filtered based upon dynamic entries learned via ND snooping, DHCPv6 snooping, or static addresses configured in the source guard binding table with this command.

- Static bindings are processed as follows:

  - If there is no entry with same and MAC address and IPv6 address, a new entry is added to binding table using static IP source guard binding.

  - If there is an entry with same MAC address and IPv6 address, and the type of entry is static IP source guard binding, then the new entry will replace the old one.

  - If there is an entry with same MAC address and IPv6 address, and the type of the entry is either a dynamic ND snooping binding or DHCPv6 snooping binding, then the new entry will replace the old one and the entry type will be changed to static IP source guard binding.

EXAMPLE

This example configures a static source-guard binding on port 5.

```
Console(config)#ipv6 source-guard binding 00-ab-11-cd-23-45 vlan 1 2001::1
  interface ethernet 1/5
Console(config)#
```

RELATED COMMANDS

ipv6 source-guard (1142)
ipv6 dhcp snooping (1126)
ipv6 dhcp snooping vlan (1129)

ipv6 source-guard

This command configures the switch to filter inbound traffic based on the source IP address stored in the binding table. Use the **no** form to disable this function.

SYNTAX

ipv6 source-guard sip

no ipv6 source-guard

DEFAULT SETTING

Disabled

COMMAND MODE

Interface Configuration (Ethernet)

COMMAND USAGE

- Source guard is used to filter traffic on an insecure port which receives messages from outside the network or fire wall, and therefore may be subject to traffic attacks caused by a host trying to use the IP address of a neighbor.

- This command checks the VLAN ID, IPv6 global unicast source IP address, and port number against all entries in the binding table. Use the **no ipv6 source guard** command to disable this function on the selected port.

- After IPv6 source guard is enabled on an interface, the switch initially blocks all IPv6 traffic received on that interface, except for ND packets allowed by ND snooping and DHCPv6 packets allowed by DHCPv6 snooping. A port access control list (ACL) is applied to the interface. Traffic is then filtered based upon dynamic entries learned via ND snooping or DHCPv6 snooping, or static addresses configured in the source guard binding table. The port allows only IPv6 traffic with a matching entry in the binding table and denies all other IPv6 traffic.

- Table entries include a MAC address, IPv6 global unicast address, lease time, entry type (Static-IP-SG-Binding, Dynamic-ND-Binding, Dynamic-DHCPv6-Binding), VLAN identifier, and port identifier.

- Static addresses entered in the source guard binding table with the ipv6 source-guard binding command are automatically configured with an infinite lease time. Dynamic entries learned via DHCPv6 snooping are configured by the DHCPv6 server itself.

- If IP source guard is enabled, an inbound packet's source IPv6 address will be checked against the binding table. If no matching entry is found, the packet will be dropped.

- Filtering rules are implemented as follows:
  - If ND snooping and DHCPv6 snooping are disabled, IP source guard will check the VLAN ID, source IPv6 address, and port number. If a matching entry is found in the binding table and the entry type is static IP source guard binding, the packet will be forwarded.
  - If ND snooping or DHCP snooping is enabled, IP source guard will check the VLAN ID, source IP address, and port number. If a matching entry is found in the binding table and the entry type is static IP source guard binding, dynamic ND snooping binding, or dynamic DHCPv6 snooping binding, the packet will be forwarded.
  - If IP source guard if enabled on an interface for which IPv6 source bindings (dynamically learned via ND snooping or DHCP snooping, or manually configured) are not yet configured, the switch will drop all IPv6 traffic on that port, except for ND packets and DHCPv6 packets.
  - Only IPv6 global unicast addresses are accepted for static bindings.

EXAMPLE

This example enables IP source guard on port 5.

```
Console(config)#interface ethernet 1/5
Console(config-if)#ipv6 source-guard sip
Console(config-if)#
```

RELATED COMMANDS

ipv6 source-guard binding (1140)
ipv6 dhcp snooping (1126)
ipv6 dhcp snooping vlan (1129)

ipv6 source-guard max-binding

This command sets the maximum number of entries that can be bound to an interface. Use the **no** form to restore the default setting.

SYNTAX

ipv6 source-guard max-binding *number*

no ipv6 source-guard max-binding

number - The maximum number of IPv6 addresses that can be mapped to an interface in the binding table. (Range: 1-5)

DEFAULT SETTING

5

COMMAND MODE

Interface Configuration (Ethernet)

COMMAND USAGE

- This command sets the maximum number of address entries that can be mapped to an interface in the binding table, including both dynamic entries discovered by ND snooping, DHCPv6 snooping, and static entries set by the ipv6 source-guard command.

- IPv6 source guard maximum bindings must be set to a value higher than DHCPv6 snooping maximum bindings and ND snooping maximum bindings.

- If IPv6 source guard, ND snooping, and DHCPv6 snooping are enabled on a port, the dynamic bindings used by ND snooping, DHCPv6 snooping, and IPv6 source guard static bindings cannot exceed the maximum allowed bindings set by the **ipv6 source-guard max-binding** command. In other words, no new entries will be added to the IPv6 source guard binding table.

- If IPv6 source guard is enabled on a port, and the maximum number of allowed bindings is changed to a lower value, precedence is given to deleting entries learned through DHCPv6 snooping, ND snooping, and then manually configured IPv6 source guard static bindings, until the number of entries in the binding table reaches the newly configured maximum number of allowed bindings.

EXAMPLE

This example sets the maximum number of allowed entries in the binding table for port 5 to one entry.

```
Console(config)#interface ethernet 1/5
Console(config-if)#ipv6 source-guard max-binding 1
Console(config-if)#
```

show ipv6 source-guard

This command shows whether IPv6 source guard is enabled or disabled on each interface, and the maximum allowed bindings.

COMMAND MODE

Privileged Exec

EXAMPLE

```
Console#show ipv6 source-guard
Interface   Filter-type   Max-binding
---------   -----------   -----------
Eth 1/1     DISABLED                5
Eth 1/2     DISABLED                5
Eth 1/3     DISABLED                5
Eth 1/4     DISABLED                5
Eth 1/5     SIP                     1
Eth 1/6     DISABLED                5
 ⋮
```

show ipv6 source-guard binding

This command shows the source guard binding table.

SYNTAX

show ipv6 source-guard binding [**dynamic** | **static**]

dynamic - Shows dynamic entries configured with ND Snooping or DHCPv6 Snooping commands (see page 1126)

static - Shows static entries configured with the ipv6 source-guard binding command.

COMMAND MODE

Privileged Exec

EXAMPLE

```
Console#show ipv6 source-guard binding
MAC Address    IPv6 Address                            VLAN Interface Type
-------------- --------------------------------------- ---- --------- ----
00AB-11CD-2345                                 2001::1    1  Eth 1/5   STA
Console#
```

ARP INSPECTION

ARP Inspection validates the MAC-to-IP address bindings in Address Resolution Protocol (ARP) packets. It protects against ARP traffic with invalid address bindings, which forms the basis for certain “man-in-the-middle” attacks. This is accomplished by intercepting all ARP requests and responses and verifying each of these packets before the local ARP cache is updated or the packet is forwarded to the appropriate destination, dropping any invalid ARP packets.

ARP Inspection determines the validity of an ARP packet based on valid IP-to-MAC address bindings stored in a trusted database – the DHCP snooping binding database. ARP Inspection can also validate ARP packets against user-configured ARP access control lists (ACLs) for hosts with statically configured IP addresses.

This section describes commands used to configure ARP Inspection.

Table 123: ARP Inspection Commands

Command	Function	Mode
ip arp inspection	Enables ARP Inspection globally on the switch	GC
ip arp inspection filter	Specifies an ARP ACL to apply to one or more VLANs	GC
ip arp inspection log-buffer logs	Sets the maximum number of entries saved in a log message, and the rate at these messages are sent	GC
ip arp inspection validate	Specifies additional validation of address components in an ARP packet	GC
ip arp inspection vlan	Enables ARP Inspection for a specified VLAN or range of VLANs	GC

Table 123: ARP Inspection Commands (Continued)

Command	Function	Mode
ip arp inspection limit	Sets a rate limit for the ARP packets received on a port	IC
ip arp inspection trust	Sets a port as trusted, and thus exempted from ARP Inspection	IC
show ip arp inspection configuration	Displays the global configuration settings for ARP Inspection	PE
show ip arp inspection interface	Shows the trust status and inspection rate limit for ports	PE
show ip arp inspection log	Shows information about entries stored in the log, including the associated VLAN, port, and address components	PE
show ip arp inspection statistics	Shows statistics about the number of ARP packets processed, or dropped for various reasons	PE
show ip arp inspection vlan	Shows configuration setting for VLANs, including ARP Inspection status, the ARP ACL name, and if the DHCP Snooping database is used after ACL validation is completed	PE

ip arp inspection

This command enables ARP Inspection globally on the switch. Use the **no** form to disable this function.

SYNTAX

[**no**] **ip arp inspection**

DEFAULT SETTING

Disabled

COMMAND MODE

Global Configuration

COMMAND USAGE

- When ARP Inspection is enabled globally with this command, it becomes active only on those VLANs where it has been enabled with the ip arp inspection vlan command.
- When ARP Inspection is enabled globally and enabled on selected VLANs, all ARP request and reply packets on those VLANs are redirected to the CPU and their switching is handled by the ARP Inspection engine.
- When ARP Inspection is disabled globally, it becomes inactive for all VLANs, including those where ARP Inspection is enabled.
- When ARP Inspection is disabled, all ARP request and reply packets bypass the ARP Inspection engine and their manner of switching matches that of all other packets.
- Disabling and then re-enabling global ARP Inspection will not affect the ARP Inspection configuration for any VLANs.

- When ARP Inspection is disabled globally, it is still possible to configure ARP Inspection for individual VLANs. These configuration changes will only become active after ARP Inspection is globally enabled again.

EXAMPLE

```
Console(config)#ip arp inspection
Console(config)#
```

ip arp inspection filter

This command specifies an ARP ACL to apply to one or more VLANs. Use the **no** form to remove an ACL binding.

SYNTAX

ip arp inspection filter *arp-acl-name* **vlan** {*vlan-id* | *vlan-range*} [**static**]

arp-acl-name - Name of an ARP ACL.
(Maximum length: 16 characters)

vlan-id - VLAN ID. (Range: 1-4094)

vlan-range - A consecutive range of VLANs indicated by the use a hyphen, or a random group of VLANs with each entry separated by a comma.

static - ARP packets are only validated against the specified ACL, address bindings in the DHCP snooping database is not checked.

DEFAULT SETTING

ARP ACLs are not bound to any VLAN
Static mode is not enabled

COMMAND MODE

Global Configuration

COMMAND USAGE

- ARP ACLs are configured with the commands described on page 406.

- If static mode is enabled, the switch compares ARP packets to the specified ARP ACLs. Packets matching an IP-to-MAC address binding in a permit or deny rule are processed accordingly. Packets not matching any of the ACL rules are dropped. Address bindings in the DHCP snooping database are not checked.

- If static mode is not enabled, packets are first validated against the specified ARP ACL. Packets matching a deny rule are dropped. All remaining packets are validated against the address bindings in the DHCP snooping database.

EXAMPLE

```
Console(config)#ip arp inspection filter sales vlan 1
Console(config)#
```

ip arp inspection log-buffer logs

This command sets the maximum number of entries saved in a log message, and the rate at which these messages are sent. Use the **no** form to restore the default settings.

SYNTAX

ip arp inspection log-buffer logs *message-number* **interval** *seconds*

no ip arp inspection log-buffer logs

message-number - The maximum number of entries saved in a log message. (Range: 0-256, where 0 means no events are saved)

seconds - The interval at which log messages are sent. (Range: 0-86400)

DEFAULT SETTING

Message Number: 5
Interval: 1 second

COMMAND MODE

Global Configuration

COMMAND USAGE

- ARP Inspection must be enabled with the ip arp inspection command before this command will be accepted by the switch.
- By default, logging is active for ARP Inspection, and cannot be disabled.
- When the switch drops a packet, it places an entry in the log buffer. Each entry contains flow information, such as the receiving VLAN, the port number, the source and destination IP addresses, and the source and destination MAC addresses.
- If multiple, identical invalid ARP packets are received consecutively on the same VLAN, then the logging facility will only generate one entry in the log buffer and one corresponding system message.
- The maximum number of entries that can be stored in the log buffer is determined by the *message-number* parameter. If the log buffer fills up before a message is sent, the oldest entry will be replaced with the newest one.
- The switch generates a system message on a rate-controlled basis determined by the *seconds* values. After the system message is generated, all entries are cleared from the log buffer.

EXAMPLE

```
Console(config)#ip arp inspection log-buffer logs 1 interval 10
Console(config)#
```

ip arp inspection validate

This command specifies additional validation of address components in an ARP packet. Use the **no** form to restore the default setting.

SYNTAX

ip arp inspection validate
{**dst-mac** [**ip** [**allow-zeros**] [**src-mac**]] |
ip [**allow-zeros**] [**src-mac**]] | **src-mac**}

no ip arp inspection validate

dst-mac - Checks the destination MAC address in the Ethernet header against the target MAC address in the ARP body. This check is performed for ARP responses. When enabled, packets with different MAC addresses are classified as invalid and are dropped.

ip - Checks the ARP body for invalid and unexpected IP addresses. Addresses include 0.0.0.0, 255.255.255.255, and all IP multicast addresses. Sender IP addresses are checked in all ARP requests and responses, while target IP addresses are checked only in ARP responses.

allow-zeros - Allows sender IP address to be 0.0.0.0.

src-mac - Checks the source MAC address in the Ethernet header against the sender MAC address in the ARP body. This check is performed on both ARP requests and responses. When enabled, packets with different MAC addresses are classified as invalid and are dropped.

DEFAULT SETTING

No additional validation is performed

COMMAND MODE

Global Configuration

COMMAND USAGE

By default, ARP Inspection only checks the IP-to-MAC address bindings specified in an ARP ACL or in the DHCP Snooping database.

EXAMPLE

```
Console(config)#ip arp inspection validate dst-mac
Console(config)#
```

ip arp inspection vlan

This command enables ARP Inspection for a specified VLAN or range of VLANs. Use the **no** form to disable this function.

SYNTAX

[**no**] **ip arp inspection vlan** {*vlan-id* | *vlan-range*}

vlan-id - VLAN ID. (Range: 1-4094)

vlan-range - A consecutive range of VLANs indicated by the use a hyphen, or a random group of VLANs with each entry separated by a comma.

DEFAULT SETTING

Disabled on all VLANs

COMMAND MODE

Global Configuration

COMMAND USAGE

- When ARP Inspection is enabled globally with the ip arp inspection command, it becomes active only on those VLANs where it has been enabled with this command.

- When ARP Inspection is enabled globally and enabled on selected VLANs, all ARP request and reply packets on those VLANs are redirected to the CPU and their switching is handled by the ARP Inspection engine.

- When ARP Inspection is disabled globally, it becomes inactive for all VLANs, including those where ARP Inspection is enabled.

- When ARP Inspection is disabled, all ARP request and reply packets bypass the ARP Inspection engine and their manner of switching matches that of all other packets.

- Disabling and then re-enabling global ARP Inspection will not affect the ARP Inspection configuration for any VLANs.

- When ARP Inspection is disabled globally, it is still possible to configure ARP Inspection for individual VLANs. These configuration changes will only become active after ARP Inspection is globally enabled again.

EXAMPLE

```
Console(config)#ip arp inspection vlan 1,2
Console(config)#
```

ip arp inspection limit

This command sets a rate limit for the ARP packets received on a port. Use the **no** form to restore the default setting.

SYNTAX

ip arp inspection limit {**rate** *pps* | **none**}

no ip arp inspection limit

pps - The maximum number of ARP packets that can be processed by the CPU per second. (Range: 0-2048, where 0 means that no ARP packets can be forwarded)

none - There is no limit on the number of ARP packets that can be processed by the CPU.

DEFAULT SETTING

15

COMMAND MODE

Interface Configuration (Port, Static Aggregation)

COMMAND USAGE

- This command applies to both trusted and untrusted ports.
- When the rate of incoming ARP packets exceeds the configured limit, the switch drops all ARP packets in excess of the limit.

EXAMPLE

```
Console(config)#interface ethernet 1/1
Console(config-if)#ip arp inspection limit rate 150
Console(config-if)#
```

ip arp inspection trust

This command sets a port as trusted, and thus exempted from ARP Inspection. Use the **no** form to restore the default setting.

SYNTAX

[**no**] **ip arp inspection trust**

DEFAULT SETTING

Untrusted

COMMAND MODE

Interface Configuration (Port, Static Aggregation)

COMMAND USAGE

Packets arriving on untrusted ports are subject to any configured ARP Inspection and additional validation checks. Packets arriving on trusted ports bypass all of these checks, and are forwarded according to normal switching rules.

EXAMPLE

```
Console(config)#interface ethernet 1/1
Console(config-if)#ip arp inspection trust
Console(config-if)#
```

show ip arp inspection configuration

This command displays the global configuration settings for ARP Inspection.

COMMAND MODE

Privileged Exec

EXAMPLE

```
Console#show ip arp inspection configuration

ARP Inspection Global Information:

Global IP ARP Inspection Status : disabled
Log Message Interval            : 10 s
Log Message Number              : 1
Need Additional Validation(s)   : Yes
Additional Validation Type      : Destination MAC address
Console#
```

show ip arp inspection interface

This command shows the trust status and ARP Inspection rate limit for ports.

SYNTAX

show ip arp inspection interface [*interface*]

interface

ethernet *unit*/*port*

unit - Unit identifier. (Range: 1)

port - Port number. (Range: 1-28)

COMMAND MODE

Privileged Exec

EXAMPLE

```
Console#show ip arp inspection interface ethernet 1/1

Port Number        Trust Status             Rate Limit (pps)
-------------   --------------------    ------------------------------
Eth 1/1            Trusted                    150
Console#
```

show ip arp inspection log

This command shows information about entries stored in the log, including the associated VLAN, port, and address components.

COMMAND MODE

Privileged Exec

EXAMPLE

```
Console#show ip arp inspection log
Total log entries number is 1

Num VLAN Port Src IP Address  Dst IP Address  Src MAC Address  Dst MAC Address
--- ---- ---- --------------  --------------  ---------------  --------------
1   1     11  192.168.2.2     192.168.2.1     00-04-E2-A0-E2-7C FF-FF-FF-FF-FF-FF
Console#
```

show ip arp inspection statistics

This command shows statistics about the number of ARP packets processed, or dropped for various reasons.

COMMAND MODE

Privileged Exec

EXAMPLE

```
Console#show ip arp inspection statistics

ARP packets received before rate limit                                : 150
ARP packets dropped due to rate limt                                  : 5
Total ARP packets processed by ARP Inspection                         : 150
ARP packets dropped by additional validation (source MAC address)     : 0
ARP packets dropped by additional validation (destination MAC address): 0
ARP packets dropped by additional validation (IP address)             : 0
ARP packets dropped by ARP ACLs                                       : 0
ARP packets dropped by DHCP snooping                                  : 0

Console#
```

show ip arp inspection vlan

This command shows the configuration settings for VLANs, including ARP Inspection status, the ARP ACL name, and if the DHCP Snooping database is used after ARP ACL validation is completed.

SYNTAX

show ip arp inspection vlan [*vlan-id* | *vlan-range*]

vlan-id - VLAN ID. (Range: 1-4094)

vlan-range - A consecutive range of VLANs indicated by the use a hyphen, or a random group of VLANs with each entry separated by a comma.

COMMAND MODE

Privileged Exec

EXAMPLE

```
Console#show ip arp inspection vlan 1

VLAN ID     DAI Status             ACL Name             ACL Status
--------   ---------------    --------------------    --------------------
1           disabled               sales               static
Console#
```

DENIAL OF SERVICE PROTECTION

A denial-of-service attack (DoS attack) is an attempt to block the services provided by a computer or network resource. This kind of attack tries to prevent an Internet site or service from functioning efficiently or at all. In general, DoS attacks are implemented by either forcing the target to reset, to consume most of its resources so that it can no longer provide its intended service, or to obstruct the communication media between the intended users and the target so that they can no longer communicate adequately.

This section describes commands used to protect against DoS attacks.

Table 124: DoS Protection Commands

Command	Function	Mode
dos-protection land	Protects against DoS LAND attacks	GC
dos-protection tcp-null-scan	Protects against DoS TCP-null-scan attacks	GC
dos-protection tcp-syn-fin-scan	Protects against DoS TCP-SYN/FIN-scan attacks	GC
dos-protection tcp-xmas-scan	Protects against DoS TCP-XMAS-scan attacks	GC
show dos-protection	Shows the configuration settings for DoS protection	PE

dos-protection land

This command protects against DoS LAND (Local Area Network Denial) attacks in which hackers send spoofed-IP packets where the source and destination address are the same, thereby causing the target to reply to itself continuously. Use the **no** form to disable this feature.

SYNTAX

[**no**] **dos-protection land**

DEFAULT SETTING

Enabled

COMMAND MODE

Global Configuration

EXAMPLE

```
Console(config)#dos-protection land
Console(config)#
```

dos-protection tcp-null-scan

This command protects against DoS TCP-null-scan attacks in which a TCP NULL scan message is used to identify listening TCP ports. The scan uses a series of strangely configured TCP packets which contain a sequence number of 0 and no flags. If the target's TCP port is closed, the target replies with a TCP RST (reset) packet. If the target TCP port is open, it simply discards the TCP NULL scan. Use the **no** form to disable this feature.

SYNTAX

[**no**] **dos-protection tcp-null-scan**

DEFAULT SETTING

Enabled

COMMAND MODE

Global Configuration

EXAMPLE

```
Console(config)#dos-protection tcp-null-scan
Console(config)#
```

dos-protection tcp-syn-fin-scan

This command protects against DoS TCP-SYN/FIN-scan attacks in which a TCP SYN/FIN scan message is used to identify listening TCP ports. The scan uses a series of strangely configured TCP packets which contain SYN (synchronize) and FIN (finish) flags. If the target's TCP port is closed, the target replies with a TCP RST (reset) packet. If the target TCP port is open, it simply discards the TCP SYN FIN scan. Use the **no** form to disable this feature.

SYNTAX

[**no**] **dos-protection syn-fin-scan**

DEFAULT SETTING

Enabled

COMMAND MODE

Global Configuration

EXAMPLE

```
Console(config)#dos-protection syn-fin-scan
Console(config)#
```

dos-protection tcp-xmas-scan

This command protects against DoS TCP-xmas-scan in which a so-called TCP XMAS scan message is used to identify listening TCP ports. This scan uses a series of strangely configured TCP packets which contain a sequence number of 0 and the URG, PSH and FIN flags. If the target's TCP port is closed, the target replies with a TCP RST packet. If the target TCP port is open, it simply discards the TCP XMAS scan. Use the **no** form to disable this feature.

SYNTAX

[**no**] **dos-protection tcp-xmas-scan**

DEFAULT SETTING

Enabled

COMMAND MODE

Global Configuration

EXAMPLE

```
Console(config)#dos-protection tcp-xmas-scan
Console(config)#
```

show dos-protection

This command shows the configuration settings for the DoS protection commands.

COMMAND MODE

Privileged Exec

EXAMPLE

```
Console#show dos-protection
Global DoS Protections:

 LAND Attack          : Enabled
 TCP Null Scan        : Enabled
 TCP SYN/FIN Scan     : Enabled
 TCP XMAS Scan        : Enabled
Console#
```

CONFIGURING PORT-BASED TRAFFIC SEGMENTATION

If tighter security is required for passing traffic from different clients through downlink ports on the local network and over uplink ports to the service provider, port-based traffic segmentation can be used to isolate traffic for individual clients.

Traffic belonging to each client is isolated to the allocated downlink ports. But the switch can be configured to either isolate traffic passing across a client's allocated uplink ports from the uplink ports assigned to other clients, or to forward traffic through the uplink ports used by other clients, allowing different clients to share access to their uplink ports where security is less likely to be compromised.

Table 125: Commands for Configuring Traffic Segmentation

Command	Function	Mode
traffic-segmentation	Enables traffic segmentation	GC
traffic-segmentation session	Creates a client session	GC
traffic-segmentation uplink/downlink	Configures uplink/downlink ports for client sessions	GC
traffic-segmentation uplink-to-uplink	Specifies whether or not traffic can be forwarded between uplink ports assigned to different client sessions	GC
show traffic-segmentation	Displays the configured traffic segments	PE

traffic-segmentation

This command enables traffic segmentation. Use the **no** form to disable traffic segmentation.

SYNTAX

[**no**] **traffic-segmentation**

DEFAULT SETTING

Disabled

COMMAND MODE

Global Configuration

COMMAND USAGE

- Traffic segmentation provides port-based security and isolation between ports within the VLAN. Data traffic on the downlink ports can only be forwarded to, and from, the designated uplink port(s). Data cannot pass between downlink ports in the same segmented group, nor to ports which do not belong to the same group.

- Traffic segmentation and normal VLANs can exist simultaneously within the same switch. Traffic may pass freely between uplink ports in segmented groups and ports in normal VLANs.

- When traffic segmentation is enabled, the forwarding state for the uplink and downlink ports assigned to different client sessions is shown below.

Table 126: Traffic Segmentation Forwarding

Destination Source	Session #1 Downlinks	Session #1 Uplinks	Session #2 Downlinks	Session #2 Uplinks	Normal Ports
Session #1 Downlink Ports	Blocking	Forwarding	Blocking	Blocking	Blocking
Session #1 Uplink Ports	Forwarding	Forwarding	Blocking	Blocking/ Forwarding*	Forwarding
Session #2 Downlink Ports	Blocking	Blocking	Blocking	Forwarding	Blocking
Session #2 Uplink Ports	Blocking	Blocking/ Forwarding*	Forwarding	Forwarding	Forwarding
Normal Ports	Forwarding	Forwarding	Forwarding	Forwarding	Forwarding

* The forwarding state for uplink-to-uplink ports is configured by the traffic-segmentation uplink-to-uplink command.

- When traffic segmentation is disabled, all ports operate in normal forwarding mode based on the settings specified by other functions such as VLANs and spanning tree protocol.

- Enter the **traffic-segmentation** command without any parameters to enable traffic segmentation. Then set the interface members for segmented groups using the traffic-segmentation uplink/downlink command.

- Enter **no traffic-segmentation** to disable traffic segmentation and clear the configuration settings for segmented groups.

EXAMPLE

This example enables traffic segmentation globally on the switch.

```
Console(config)#traffic-segmentation
Console(config)#
```

traffic-segmentation session

This command creates a traffic-segmentation client session. Use the **no** form to remove a client session.

SYNTAX

[**no**] **pvlan session** *session-id*

session-id – Traffic segmentation session. (Range: 1-4)

DEFAULT SETTING

None

COMMAND MODE

Global Configuration

Command Usage

- Use this command to create a new traffic-segmentation client session.

- Using the **no** form of this command will remove any assigned uplink or downlink ports, restoring these interfaces to normal operating mode.

Example

```
Console(config)#traffic-segmentation session 1
Console(config)#
```

traffic-segmentation uplink/downlink

This command configures the uplink and down-link ports for a segmented group of ports. Use the **no** form to remove a port from the segmented group.

SYNTAX

[**no**] **traffic-segmentation** [**session** *session-id*] {**uplink** *interface-list* [**downlink** *interface-list*] | **downlink** *interface-list*}

session-id – Traffic segmentation session. (Range: 1-4)

uplink – Specifies an uplink interface.

downlink – Specifies a downlink interface.

interface-list – One or more ports. Use a hyphen to indicate a consecutive list of ports or a comma between non-consecutive ports.

ethernet *unit*/*port*

unit - Unit identifier. (Range: 1)

port - Port number. (Range: 1-28)

port-channel *channel-id* (Range: 1-8)

DEFAULT SETTING

Session 1 if not defined
No segmented port groups are defined.

COMMAND MODE

Global Configuration

COMMAND USAGE

- A port cannot be configured in both an uplink and downlink list.

- A port can only be assigned to one traffic-segmentation session.

- When specifying an uplink or downlink, a list of ports may be entered by using a hyphen or comma in the *port* field. Note that lists are not supported for the *channel-id* field.

- A downlink port can only communicate with an uplink port in the same session. Therefore, if an uplink port is not configured for a session, the assigned downlink ports will not be able to communicate with any other ports.
- If a downlink port is not configured for the session, the assigned uplink ports will operate as normal ports.

EXAMPLE

This example enables traffic segmentation, and then sets port 10 as the uplink and ports 5-8 as downlinks.

```
Console(config)#traffic-segmentation
Console(config)#traffic-segmentation uplink ethernet 1/10
  downlink ethernet 1/5-8
Console(config)#
```

traffic-segmentation uplink-to-uplink

This command specifies whether or not traffic can be forwarded between uplink ports assigned to different client sessions. Use the **no** form to restore the default.

SYNTAX

[**no**] **traffic-segmentation uplink-to-uplink** {**blocking** | **forwarding**}

blocking – Blocks traffic between uplink ports assigned to different sessions.

forwarding – Forwards traffic between uplink ports assigned to different sessions.

DEFAULT SETTING

Blocking

COMMAND MODE

Global Configuration

EXAMPLE

This example enables forwarding of traffic between uplink ports assigned to different client sessions.

```
Console(config)#traffic-segmentation uplink-to-uplink forwarding
Console(config)#
```

show traffic-segmentation

This command displays the configured traffic segments.

COMMAND MODE

Privileged Exec

EXAMPLE

```
Console#show traffic-segmentation

 Private VLAN Status   :                  Enabled
 Uplink-to-Uplink Mode :                  Forwarding

 Session   Uplink Ports                   Downlink Ports
--------- ------------------------------ -----------------------------
    1      Ethernet  1/1                  Ethernet  1/2
                                          Ethernet  1/3
                                          Ethernet  1/4
Console#
```

30 Access Control Lists

Access Control Lists (ACL) provide packet filtering for IPv4 frames (based on address, protocol, Layer 4 protocol port number or TCP control code), IPv6 frames (based on address, DSCP traffic class, next header type, or flow label), or any frames (based on MAC address or Ethernet type). To filter packets, first create an access list, add the required rules, and then bind the list to a specific port. This section describes the Access Control List commands.

Table 127: Access Control List Commands

Command Group	Function
IPv4 ACLs	Configures ACLs based on IPv4 addresses, TCP/UDP port number, protocol type, and TCP control code
IPv6 ACLs	Configures ACLs based on IPv6 addresses, DSCP traffic class, next header type, or flow label
MAC ACLs	Configures ACLs based on hardware addresses, packet format, and Ethernet type
ARP ACLs	Configures ACLs based on ARP messages addresses
ACL Information	Displays ACLs and associated rules; shows ACLs assigned to each port

IPv4 ACLs

The commands in this section configure ACLs based on IPv4 addresses, TCP/UDP port number, protocol type, and TCP control code. To configure IPv4 ACLs, first create an access list containing the required permit or deny rules, and then bind the access list to one or more ports.

Table 128: IPv4 ACL Commands

Command	Function	Mode
access-list ip	Creates an IP ACL and enters configuration mode for standard or extended IPv4 ACLs	GC
permit, deny	Filters packets matching a specified source IPv4 address	IPv4-STD-ACL
permit, deny	Filters packets meeting the specified criteria, including source and destination IPv4 address, TCP/UDP port number, protocol type, and TCP control code	IPv4-EXT-ACL
ip access-group	Binds an IPv4 ACL to a port	IC
show ip access-group	Shows port assignments for IPv4 ACLs	PE
show ip access-list	Displays the rules for configured IPv4 ACLs	PE

access-list ip

This command adds an IP access list and enters configuration mode for standard or extended IPv4 ACLs. Use the **no** form to remove the specified ACL.

SYNTAX

[**no**] **access-list ip** {**standard** | **extended**} *acl-name*

standard – Specifies an ACL that filters packets based on the source IP address.

extended – Specifies an ACL that filters packets based on the source or destination IP address, and other more specific criteria.

acl-name – Name of the ACL. (Maximum length: 32 characters, no spaces or other special characters)

DEFAULT SETTING

None

COMMAND MODE

Global Configuration

COMMAND USAGE

- When you create a new ACL or enter configuration mode for an existing ACL, use the **permit** or **deny** command to add new rules to the bottom of the list.
- To remove a rule, use the **no permit** or **no deny** command followed by the exact text of a previously configured rule.
- An ACL can contain up to 64 rules.

EXAMPLE

```
Console(config)#access-list ip standard david
Console(config-std-acl)#
```

RELATED COMMANDS

permit, deny (1165)
ip access-group (1168)
show ip access-list (1169)

permit, deny (Standard IP ACL)

This command adds a rule to a Standard IPv4 ACL. The rule sets a filter condition for packets emanating from the specified source. Use the **no** form to remove a rule.

SYNTAX

{**permit** | **deny**} {**any** | *source bitmask* | **host** *source*}
[**time-range** *time-range-name*]

no {**permit** | **deny**} {**any** | *source bitmask* | **host** *source*}

any – Any source IP address.

source – Source IP address.

bitmask – Dotted decimal number representing the address bits to match.

host – Keyword followed by a specific IP address.

time-range-name - Name of the time range.
(Range: 1-30 characters)

DEFAULT SETTING

None

COMMAND MODE

Standard IPv4 ACL

COMMAND USAGE

- New rules are appended to the end of the list.
- Address bit masks are similar to a subnet mask, containing four integers from 0 to 255, each separated by a period. The binary mask uses 1 bits to indicate "match" and 0 bits to indicate "ignore." The bitmask is bitwise ANDed with the specified source IP address, and then compared with the address for each IP packet entering the port(s) to which this ACL has been assigned.

EXAMPLE

This example configures one permit rule for the specific address 10.1.1.21 and another rule for the address range 168.92.16.x – 168.92.31.x using a bitmask.

```
Console(config-std-acl)#permit host 10.1.1.21
Console(config-std-acl)#permit 168.92.16.0 255.255.240.0
Console(config-std-acl)#
```

RELATED COMMANDS

access-list ip (1164)
Time Range (957)

permit, deny (Extended IPv4 ACL)

This command adds a rule to an Extended IPv4 ACL. The rule sets a filter condition for packets with specific source or destination IP addresses, protocol types, source or destination protocol ports, or TCP control codes. Use the **no** form to remove a rule.

SYNTAX

```
{permit | deny} [protocol-number | udp]
    {any | source address-bitmask | host source}
    {any | destination address-bitmask | host destination}
    [precedence precedence] [tos tos] [dscp dscp]
    [source-port sport [bitmask]]
    [destination-port dport [port-bitmask]]
    [time-range time-range-name]

no {permit | deny} [protocol-number | udp]
    {any | source address-bitmask | host source}
    {any | destination address-bitmask | host destination}
    [precedence precedence] [tos tos] [dscp dscp]
    [source-port sport [bitmask]]
    [destination-port dport [port-bitmask]]

{permit | deny} tcp
    {any | source address-bitmask | host source}
    {any | destination address-bitmask | host destination}
    [precedence precedence] [tos tos] [dscp dscp]
    [source-port sport [bitmask]]
    [destination-port dport [port-bitmask]]
    [control-flag control-flags flag-bitmask]
    [time-range time-range-name]

no {permit | deny} tcp
    {any | source address-bitmask | host source}
    {any | destination address-bitmask | host destination}
    [precedence precedence] [tos tos] [dscp dscp]
    [source-port sport [bitmask]]
    [destination-port dport [port-bitmask]]
    [control-flag control-flags flag-bitmask]
```

protocol-number – A specific protocol number. (Range: 0-255)

source – Source IP address.

destination – Destination IP address.

address-bitmask – Decimal number representing the address bits to match.

host – Keyword followed by a specific IP address.

precedence – IP precedence level. (Range: 0-7)

tos – Type of Service level. (Range: 0-15)

dscp – DSCP priority level. (Range: 0-63)

sport – Protocol[20] source port number. (Range: 0-65535)

dport – Protocol[20] destination port number. (Range: 0-65535)

[20] Includes TCP, UDP or other protocol types.

port-bitmask – Decimal number representing the port bits to match. (Range: 0-65535)

control-flags – Decimal number (representing a bit string) that specifies flag bits in byte 14 of the TCP header. (Range: 0-63)

flag-bitmask – Decimal number representing the code bits to match.

time-range-name - Name of the time range.
(Range: 1-30 characters)

DEFAULT SETTING

None

COMMAND MODE

Extended IPv4 ACL

COMMAND USAGE

- All new rules are appended to the end of the list.
- Address bit masks are similar to a subnet mask, containing four integers from 0 to 255, each separated by a period. The binary mask uses 1 bits to indicate "match" and 0 bits to indicate "ignore." The bit mask is bitwise ANDed with the specified source IP address, and then compared with the address for each IP packet entering the port(s) to which this ACL has been assigned.
- You can specify both Precedence and ToS in the same rule. However, if DSCP is used, then neither Precedence nor ToS can be specified.
- The control-code bitmask is a decimal number (representing an equivalent bit mask) that is applied to the control code. Enter a decimal number, where the equivalent binary bit "1" means to match a bit and "0" means to ignore a bit. The following bits may be specified:

  - 1 (fin) – Finish
  - 2 (syn) – Synchronize
  - 4 (rst) – Reset
  - 8 (psh) – Push
  - 16 (ack) – Acknowledgement
  - 32 (urg) – Urgent pointer

  For example, use the code value and mask below to catch packets with the following flags set:

  - SYN flag valid, use "control-code 2 2"
  - Both SYN and ACK valid, use "control-code 18 18"
  - SYN valid and ACK invalid, use "control-code 2 18"

EXAMPLE

This example accepts any incoming packets if the source address is within subnet 10.7.1.x. For example, if the rule is matched; i.e., the rule (10.7.1.0 & 255.255.255.0) equals the masked address (10.7.1.2 & 255.255.255.0), the packet passes through.

```
Console(config-ext-acl)#permit 10.7.1.1 255.255.255.0 any
Console(config-ext-acl)#
```

This allows TCP packets from class C addresses 192.168.1.0 to any destination address when set for destination TCP port 80 (i.e., HTTP).

```
Console(config-ext-acl)#permit 192.168.1.0 255.255.255.0 any destination-port
  80
Console(config-ext-acl)#
```

This permits all TCP packets from class C addresses 192.168.1.0 with the TCP control code set to “SYN.”

```
Console(config-ext-acl)#permit tcp 192.168.1.0 255.255.255.0 any control-
  flag 2 2
Console(config-ext-acl)#
```

RELATED COMMANDS

access-list ip (1164)
Time Range (957)

ip access-group

This command binds an IPv4 ACL to a port. Use the **no** form to remove the port.

SYNTAX

ip access-group *acl-name* {**in** | **out**}
[**time-range** *time-range-name*] [**counter**]

no ip access-group *acl-name* {**in** | **out**}

acl-name – Name of the ACL. (Maximum length: 16 characters)

in – Indicates that this list applies to ingress packets.

out – Indicates that this list applies to egress packets.

time-range-name - Name of the time range.
(Range: 1-30 characters)

counter – Enables counter for ACL statistics.

DEFAULT SETTING

None

COMMAND MODE

Interface Configuration (Ethernet)

COMMAND USAGE

If an ACL is already bound to a port and you bind a different ACL to it, the switch will replace the old binding with the new one.

EXAMPLE

```
Console(config)#int eth 1/2
Console(config-if)#ip access-group david in
Console(config-if)#
```

RELATED COMMANDS

show ip access-list (1169)
Time Range (957)

show ip access-group

This command shows the ports assigned to IP ACLs.

COMMAND MODE

Privileged Exec

EXAMPLE

```
Console#show ip access-group
Interface ethernet 1/2
 IP access-list david in
Console#
```

RELATED COMMANDS

ip access-group (1168)

show ip access-list

This command displays the rules for configured IPv4 ACLs.

SYNTAX

show ip access-list {**standard** | **extended**} [*acl-name*]

standard – Specifies a standard IP ACL.

extended – Specifies an extended IP ACL.

acl-name – Name of the ACL. (Maximum length: 16 characters)

COMMAND MODE

Privileged Exec

EXAMPLE

```
Console#show ip access-list standard
IP standard access-list david:
  permit host 10.1.1.21
  permit 168.92.0.0 255.255.15.0
Console#
```

RELATED COMMANDS

permit, deny (1165)
ip access-group (1168)

IPV6 ACLS

The commands in this section configure ACLs based on IPv6 address, DSCP traffic class, next header type, or flow label. To configure IPv6 ACLs, first create an access list containing the required permit or deny rules, and then bind the access list to one or more ports.

Table 129: IPv6 ACL Commands

Command	Function	Mode
access-list ipv6	Creates an IPv6 ACL and enters configuration mode for standard or extended IPv6 ACLs	GC
permit, deny	Filters packets matching a specified source IPv6 address	IPv6-STD-ACL
permit, deny	Filters packets meeting the specified criteria, including destination IPv6 address, DSCP traffic class, next header type, or flow label	IPv6-EXT-ACL
ipv6 access-group	Adds a port to an IPv6 ACL	IC
show ipv6 access-group	Shows port assignments for IPv6 ACLs	PE
show ipv6 access-list	Displays the rules for configured IPv6 ACLs	PE

access-list ipv6

This command adds an IP access list and enters configuration mode for standard or extended IPv6 ACLs. Use the **no** form to remove the specified ACL.

SYNTAX

[**no**] **access-list ipv6** {**standard** | **extended**} *acl-name*

standard – Specifies an ACL that filters packets based on the source IP address.

extended – Specifies an ACL that filters packets based on the destination IP address, and other more specific criteria.

acl-name – Name of the ACL. (Maximum length: 32 characters)

DEFAULT SETTING

None

Command Mode

Global Configuration

Command Usage

- When you create a new ACL or enter configuration mode for an existing ACL, use the **permit** or **deny** command to add new rules to the bottom of the list. To create an ACL, you must add at least one rule to the list.
- To remove a rule, use the **no permit** or **no deny** command followed by the exact text of a previously configured rule.
- An ACL can contain up to 64 rules.

Example

```
Console(config)#access-list ipv6 standard david
Console(config-std-ipv6-acl)#
```

Related Commands

permit, deny (Standard IPv6 ACL) (1171)
permit, deny (Extended IPv6 ACL) (1172)
ipv6 access-group (1174)
show ipv6 access-list (1175)

permit, deny (Standard IPv6 ACL)

This command adds a rule to a Standard IPv6 ACL. The rule sets a filter condition for packets emanating from the specified source. Use the **no** form to remove a rule.

Syntax

{**permit** | **deny**} {**any** | **host** *source-ipv6-address* |
source-ipv6-address[/*prefix-length*]}
[**time-range** *time-range-name*]

no {**permit** | **deny**} {**any** | **host** *source-ipv6-address* |
source-ipv6-address[/*prefix-length*]}

any – Any source IP address.

host – Keyword followed by a specific IP address.

source-ipv6-address - An IPv6 source address or network class. The address must be formatted according to RFC 2373 “IPv6 Addressing Architecture,” using 8 colon-separated 16-bit hexadecimal values. One double colon may be used in the address to indicate the appropriate number of zeros required to fill the undefined fields.

prefix-length - A decimal value indicating how many contiguous bits (from the left) of the address comprise the prefix; i.e., the network portion of the address. (Range: 0-128)

time-range-name - Name of the time range.
(Range: 1-30 characters)

DEFAULT SETTING

None

COMMAND MODE

Standard IPv6 ACL

COMMAND USAGE

New rules are appended to the end of the list.

EXAMPLE

This example configures one permit rule for the specific address 2009:DB9:2229::79 and another rule for the addresses with the network prefix 2009:DB9:2229:5::/64.

```
Console(config-std-ipv6-acl)#permit host 2009:DB9:2229::79
Console(config-std-ipv6-acl)#permit 2009:DB9:2229:5::/64
Console(config-std-ipv6-acl)#
```

RELATED COMMANDS

access-list ipv6 (1170)
Time Range (957)

permit, deny (Extended IPv6 ACL)

This command adds a rule to an Extended IPv6 ACL. The rule sets a filter condition for packets with specific destination IP addresses, next header type, or flow label. Use the **no** form to remove a rule.

SYNTAX

{**permit** | **deny**} {**any** | **host** *destination-ipv6-address* |
destination-ipv6-address[*/prefix-length*]}
[**dscp** *dscp*] [**flow-label** *flow-label*] [**next-header** *next-header*]
[**time-range** *time-range-name*]

no {**permit** | **deny**} {**any** | **host** *destination-ipv6-address* |
destination-ipv6-address[*/prefix-length*]}
[**dscp** *dscp*] [**flow-label** *flow-label*] [**next-header** *next-header*]

any – Any IP address (an abbreviation for the IPv6 prefix ::/0).

host – Keyword followed by a specific destination IP address.

destination-ipv6-address - An IPv6 destination address or network class. The address must be formatted according to RFC 2373 “IPv6 Addressing Architecture,” using 8 colon-separated 16-bit hexadecimal values. One double colon may be used in the address to indicate the appropriate number of zeros required to fill the undefined fields.

prefix-length - A decimal value indicating how many contiguous bits (from the left) of the address comprise the prefix; i.e., the network portion of the address. (Range: 0-64)

dscp – DSCP traffic class. (Range: 0-63) *flow-label* – A label for packets belonging to a particular traffic “flow” for which the sender requests special handling by IPv6 routers, such as non-default quality of service or “real-time” service (see RFC 2460). (Range: 0-16777215)

next-header – Identifies the type of header immediately following the IPv6 header. (Range: 0-255)

time-range-name - Name of the time range. (Range: 1-30 characters)

DEFAULT SETTING

None

COMMAND MODE

Extended IPv6 ACL

COMMAND USAGE

- All new rules are appended to the end of the list.

- A flow label is assigned to a flow by the flow's source node. New flow labels must be chosen pseudo-randomly and uniformly from the range 1 to FFFFF hexadecimal. The purpose of the random allocation is to make any set of bits within the Flow Label field suitable for use as a hash key by routers, for looking up the state associated with the flow.

  A flow identifies a sequence of packets sent from a particular source to a particular (unicast or multicast) destination for which the source desires special handling by the intervening routers. The nature of that special handling might be conveyed to the routers by a control protocol, such as a resource reservation protocol, or by information within the flow's packets themselves, e.g., in a hop-by-hop option. A flow is uniquely identified by the combination of a source address and a non-zero flow label. Packets that do not belong to a flow carry a flow label of zero.

  Hosts or routers that do not support the functions specified by the flow label must set the field to zero when originating a packet, pass the field on unchanged when forwarding a packet, and ignore the field when receiving a packet.

- Optional internet-layer information is encoded in separate headers that may be placed between the IPv6 header and the upper-layer header in a packet. There are a small number of such extension headers, each identified by a distinct Next Header value. IPv6 supports the values defined for the IPv4 Protocol field in RFC 1700, including these commonly used headers:

0	: Hop-by-Hop Options	(RFC 2460)
6	: TCP Upper-layer Header	(RFC 1700)
17	: UDP Upper-layer Header	(RFC 1700)
43	: Routing	(RFC 2460)
44	: Fragment	(RFC 2460)
51	: Authentication	(RFC 2402)
50	: Encapsulating Security Payload	(RFC 2406)
60	: Destination Options	(RFC 2460)

EXAMPLE

This example accepts any incoming packets if the destination address is 2009:DB9:2229::79/8.

```
Console(config-ext-ipv6-acl)#permit 2009:DB9:2229::79/8
Console(config-ext-ipv6-acl)#
```

This allows packets to any destination address when the DSCP value is 5.

```
Console(config-ext-ipv6-acl)#permit any dscp 5
Console(config-ext-ipv6-acl)#
```

This allows any packets sent to the destination 2009:DB9:2229::79/48 when the flow label is 43."

```
Console(config-ext-ipv6-acl)#permit 2009:DB9:2229::79/48 flow-label 43
Console(config-ext-ipv6-acl)#
```

This allows any packets sent to the destination 2009:DB9:2229::79/48 when the next header is 43."

```
Console(config-ext-ipv6-acl)#permit 2009:DB9:2229::79/48 next-header 43
Console(config-ext-ipv6-acl)#
```

RELATED COMMANDS

access-list ipv6 (1170)
Time Range (957)

ipv6 access-group

This command binds a port to an IPv6 ACL. Use the **no** form to remove the port.

SYNTAX

ipv6 access-group *acl-name* {**in** | **out**}
[**time-range** *time-range-name*] [**counter**]

no ipv6 access-group *acl-name* {**in** | **out**}

acl-name – Name of the ACL. (Maximum length: 16 characters)

in – Indicates that this list applies to ingress packets.

out – Indicates that this list applies to egress packets.

time-range-name - Name of the time range.
(Range: 1-30 characters)

counter – Enables counter for ACL statistics.

Default Setting

None

Command Mode

Interface Configuration (Ethernet)

Command Usage

If a port is already bound to an ACL and you bind it to a different ACL, the switch will replace the old binding with the new one.

Example

```
Console(config)#interface ethernet 1/2
Console(config-if)#ipv6 access-group standard david in
Console(config-if)#
```

Related Commands

show ipv6 access-list (1175)
Time Range (957)

show ipv6 access-group

This command shows the ports assigned to IPv6 ACLs.

Command Mode

Privileged Exec

Example

```
Console#show ipv6 access-group
Interface ethernet 1/2
 IPv6 standard access-list david in
Console#
```

Related Commands

ipv6 access-group (1174)

show ipv6 access-list

This command displays the rules for configured IPv6 ACLs.

Syntax

show ipv6 access-list {**standard** | **extended**} [*acl-name*]

standard – Specifies a standard IPv6 ACL.

extended – Specifies an extended IPv6 ACL.

acl-name – Name of the ACL. (Maximum length: 16 characters)

Command Mode

Privileged Exec

EXAMPLE

```
Console#show ipv6 access-list standard
IPv6 standard access-list david:
  permit host 2009:DB9:2229::79
  permit 2009:DB9:2229:5::/64
Console#
```

MAC ACLS

The commands in this section configure ACLs based on hardware addresses, packet format, and Ethernet type. To configure MAC ACLs, first create an access list containing the required permit or deny rules, and then bind the access list to one or more ports.

Table 130: MAC ACL Commands

Command	Function	Mode
access-list mac	Creates a MAC ACL and enters configuration mode	GC
permit, deny	Filters packets matching a specified source and destination address, packet format, and Ethernet type	MAC-ACL
mac access-group	Binds a MAC ACL to a port	IC
show mac access-group	Shows port assignments for MAC ACLs	PE
show mac access-list	Displays the rules for configured MAC ACLs	PE

access-list mac

This command adds a MAC access list and enters MAC ACL configuration mode. Use the **no** form to remove the specified ACL.

SYNTAX

[**no**] **access-list mac** *acl-name*

acl-name – Name of the ACL. (Maximum length: 16 characters, no spaces or other special characters)

DEFAULT SETTING

None

COMMAND MODE

Global Configuration

COMMAND USAGE

- When you create a new ACL or enter configuration mode for an existing ACL, use the **permit** or **deny** command to add new rules to the bottom of the list.
- To remove a rule, use the **no permit** or **no deny** command followed by the exact text of a previously configured rule.

- An ACL can contain up to 128 rules.

EXAMPLE

```
Console(config)#access-list mac jerry
Console(config-mac-acl)#
```

RELATED COMMANDS

permit, deny (1177)
mac access-group (1179)
show mac access-list (1180)

permit, deny (MAC ACL)

This command adds a rule to a MAC ACL. The rule filters packets matching a specified MAC source or destination address (i.e., physical layer address), or Ethernet protocol type. Use the **no** form to remove a rule.

SYNTAX

{**permit** | **deny**}
{**any** | **host** *source* | *source address-bitmask*}
{**any** | **host** *destination* | *destination address-bitmask*}
[**vid** *vid vid-bitmask*] [**ethertype** *protocol* [*protocol-bitmask*]]
[**time-range** *time-range-name*]

no {**permit** | **deny**}
{**any** | **host** *source* | *source address-bitmask*}
{**any** | **host** *destination* | *destination address-bitmask*}
[**vid** *vid vid-bitmask*] [**ethertype** *protocol* [*protocol-bitmask*]]

NOTE: The default is for Ethernet II packets.

{**permit** | **deny**} **tagged-eth2**
{**any** | **host** *source* | *source address-bitmask*}
{**any** | **host** *destination* | *destination address-bitmask*}
[**vid** *vid vid-bitmask*] [**ethertype** *protocol* [*protocol-bitmask*]]
[**time-range** *time-range-name*]

no {**permit** | **deny**} **tagged-eth2**
{**any** | **host** *source* | *source address-bitmask*}
{**any** | **host** *destination* | *destination address-bitmask*}
[**vid** *vid vid-bitmask*] [**ethertype** *protocol* [*protocol-bitmask*]]

{**permit** | **deny**} **untagged-eth2**
{**any** | **host** *source* | *source address-bitmask*}
{**any** | **host** *destination* | *destination address-bitmask*}
[**ethertype** *protocol* [*protocol-bitmask*]]
[**time-range** *time-range-name*]

no {**permit** | **deny**} **untagged-eth2**
{**any** | **host** *source* | *source address-bitmask*}
{**any** | **host** *destination* | *destination address-bitmask*}
[**ethertype** *protocol* [*protocol-bitmask*]]

{**permit** | **deny**} **tagged-802.3**
{**any** | **host** *source* | *source address-bitmask*}
{**any** | **host** *destination* | *destination address-bitmask*}
[**vid** *vid vid-bitmask*] [**time-range** *time-range-name*]

no {**permit** | **deny**} **tagged-802.3**
{**any** | **host** *source* | *source address-bitmask*}
{**any** | **host** *destination* | *destination address-bitmask*}
[**vid** *vid vid-bitmask*]

{**permit** | **deny**} **untagged-802.3**
{**any** | **host** *source* | *source address-bitmask*}
{**any** | **host** *destination* | *destination address-bitmask*}
[**time-range** *time-range-name*]

no {**permit** | **deny**} **untagged-802.3**
{**any** | **host** *source* | *source address-bitmask*}
{**any** | **host** *destination* | *destination address-bitmask*}

tagged-eth2 – Tagged Ethernet II packets.

untagged-eth2 – Untagged Ethernet II packets.

tagged-802.3 – Tagged Ethernet 802.3 packets.

untagged-802.3 – Untagged Ethernet 802.3 packets.

any – Any MAC source or destination address.

host – A specific MAC address.

source – Source MAC address.

destination – Destination MAC address range with bitmask.

address-bitmask[21] – Bitmask for MAC address (in hexadecimal format).

vid – VLAN ID. (Range: 1-4094)

vid-bitmask[21] – VLAN bitmask. (Range: 1-4095)

protocol – A specific Ethernet protocol number. (Range: 0-ffff hex.)

protocol-bitmask[21] – Protocol bitmask. (Range: 0-ffff hex.)

time-range-name - Name of the time range.
(Range: 1-30 characters)

DEFAULT SETTING

None

COMMAND MODE

MAC ACL

COMMAND USAGE

- New rules are added to the end of the list.
- The **ethertype** option can only be used to filter Ethernet II formatted packets.

[21] For all bitmasks, “1” means relevant and “0” means ignore.

- A detailed listing of Ethernet protocol types can be found in RFC 1060. A few of the more common types include the following:
  - 0800 - IP
  - 0806 - ARP
  - 8137 - IPX

Example

This rule permits packets from any source MAC address to the destination address 00-e0-29-94-34-de where the Ethernet type is 0800.

```
Console(config-mac-acl)#permit any host 00-e0-29-94-34-de ethertype 0800
Console(config-mac-acl)#
```

Related Commands

access-list mac (1176)
Time Range (957)

mac access-group

This command binds a MAC ACL to a port. Use the **no** form to remove the port.

Syntax

mac access-group *acl-name* {**in** | **out**}
[**time-range** *time-range-name*] [**counter**]

no mac access-group *acl-name* {**in** | **out**}

acl-name – Name of the ACL. (Maximum length: 16 characters)

in – Indicates that this list applies to ingress packets.

out – Indicates that this list applies to egress packets.

time-range-name - Name of the time range. (Range: 1-30 characters)

counter – Enables counter for ACL statistics.

Default Setting

None

Command Mode

Interface Configuration (Ethernet)

Command Usage

If an ACL is already bound to a port and you bind a different ACL to it, the switch will replace the old binding with the new one.

Example

```
Console(config)#interface ethernet 1/2
Console(config-if)#mac access-group jerry in
Console(config-if)#
```

RELATED COMMANDS

show mac access-list (1180)
Time Range (957)

show mac access-group

This command shows the ports assigned to MAC ACLs.

COMMAND MODE

Privileged Exec

EXAMPLE

```
Console#show mac access-group
Interface ethernet 1/5
 MAC access-list M5 in
Console#
```

RELATED COMMANDS

mac access-group (1179)

show mac access-list

This command displays the rules for configured MAC ACLs.

SYNTAX

show mac access-list [*acl-name*]

acl-name – Name of the ACL. (Maximum length: 16 characters)

COMMAND MODE

Privileged Exec

EXAMPLE

```
Console#show mac access-list
MAC access-list jerry:
  permit any 00-e0-29-94-34-de ethertype 0800
Console#
```

RELATED COMMANDS

permit, deny (1177)
mac access-group (1179)

ARP ACLs

The commands in this section configure ACLs based on the IP or MAC address contained in ARP request and reply messages. To configure ARP ACLs, first create an access list containing the required permit or deny rules, and then bind the access list to one or more VLANs using the ip arp inspection vlan command.

Table 131: ARP ACL Commands

Command	Function	Mode
access-list arp	Creates a ARP ACL and enters configuration mode	GC
permit, deny	Filters packets matching a specified source or destination address in ARP messages	ARP-ACL
show access-list arp	Displays the rules for configured ARP ACLs	PE

access-list arp

This command adds an ARP access list and enters ARP ACL configuration mode. Use the **no** form to remove the specified ACL.

Syntax

[**no**] **access-list arp** *acl-name*

acl-name – Name of the ACL. (Maximum length: 16 characters)

Default Setting

None

Command Mode

Global Configuration

Command Usage

- When you create a new ACL or enter configuration mode for an existing ACL, use the **permit** or **deny** command to add new rules to the bottom of the list. To create an ACL, you must add at least one rule to the list.
- To remove a rule, use the **no permit** or **no deny** command followed by the exact text of a previously configured rule.
- An ACL can contain up to 128 rules.

Example

```
Console(config)#access-list arp factory
Console(config-arp-acl)#
```

Related Commands

permit, deny (1182)
show access-list arp (1183)

permit, deny (ARP ACL)

This command adds a rule to an ARP ACL. The rule filters packets matching a specified source or destination address in ARP messages. Use the **no** form to remove a rule.

SYNTAX

[**no**] {**permit** | **deny**}
ip {**any** | **host** *source-ip* | *source-ip ip-address-bitmask*}
mac {**any** | **host** *source-mac* | *source-mac mac-address-bitmask*}
[**log**]

This form indicates either request or response packets.

[**no**] {**permit** | **deny**} **request**
ip {**any** | **host** *source-ip* | *source-ip ip-address-bitmask*}
mac {**any** | **host** *source-mac* | *source-mac mac-address-bitmask*}
[**log**]

[**no**] {**permit** | **deny**} **response**
ip {**any** | **host** *source-ip* | *source-ip ip-address-bitmask*}
{**any** | **host** *destination-ip* | *destination-ip ip-address-bitmask*}
mac {**any** | **host** *source-mac* | *source-mac mac-address-bitmask*}
[**any** | **host** *destination-mac* | *destination-mac mac-address-bitmask*] [**log**]

source-ip – Source IP address.

destination-ip – Destination IP address with bitmask.

ip-address-bitmask[22] – IPv4 number representing the address bits to match.

source-mac – Source MAC address.

destination-mac – Destination MAC address range with bitmask.

mac-address-bitmask[22] – Bitmask for MAC address (in hexadecimal format).

log - Logs a packet when it matches the access control entry.

DEFAULT SETTING

None

COMMAND MODE

ARP ACL

COMMAND USAGE

New rules are added to the end of the list.

[22] For all bitmasks, binary “1” means relevant and “0” means ignore.

EXAMPLE

This rule permits packets from any source IP and MAC address to the destination subnet address 192.168.0.0.

```
Console(config-arp-acl)#$permit response ip any 192.168.0.0 255.255.0.0 mac
  any any
Console(config-mac-acl)#
```

RELATED COMMANDS

access-list arp (1181)

show access-list arp

This command displays the rules for configured ARP ACLs.

SYNTAX

show access-list arp [*acl-name*]

acl-name – Name of the ACL. (Maximum length: 16 characters)

COMMAND MODE

Privileged Exec

EXAMPLE

```
Console#show access-list arp
ARP access-list factory:
  permit response ip any 192.168.0.0 255.255.0.0 mac any any
Console#
```

RELATED COMMANDS

permit, deny (1182)

ACL INFORMATION

This section describes commands used to display ACL information.

Table 132: ACL Information Commands

Command	Function	Mode
clear access-list hardware counters	Clears hit counter for rules in all ACLs, or in a specified ACL.	PE
show access-group	Shows the ACLs assigned to each port	PE
show access-list	Show all ACLs and associated rules	PE

clear access-list hardware counters

This command clears the hit counter for the rules in all ACLs, or for the rules in a specified ACL.

SYNTAX

clear access-list hardware counters
[**direction** {**in** | **out**} [**interface** *interface*]] |
[**interface** *interface*] | [**name** *acl-name*]

in – Clears counter for ingress rules.

out – Clears counter for egress rules.

interface

ethernet *unit/port*

unit - Unit identifier. (Range: 1)

port - Port number. (Range: 1-28)

acl-name – Name of the ACL. (Maximum length: 16 characters)

COMMAND MODE

Privileged Exec

EXAMPLE

```
Console#clear access-list hardware counters
Console#
```

show access-group

This command shows the port assignments of ACLs.

COMMAND MODE

Privileged Executive

EXAMPLE

```
Console#show access-group
Interface ethernet 1/2
 IP access-list david
 MAC access-list jerry
Console#
```

show access-list

This command shows all ACLs and associated rules.

SYNTAX

show access-list
[[**arp** [*acl-name*]] |
[**ip** [**extended** [*acl-name*] | **standard** [*acl-name*]] |
[**ipv6** [**extended** [*acl-name*] | **standard** [*acl-name*]] |
[**mac** [*acl-name*]] | [**tcam-utilization**] | [**hardware counters**]]

arp – Shows ingress or egress rules for ARP ACLs.

hardware counters – Shows statistics for all ACLs.[23]

ip extended – Shows ingress/egress rules for Extended IPv4 ACLs.

ip standard – Shows ingress/egress rules for Standard IPv4 ACLs.

ipv6 extended – Shows ingress/egress rules for Extended IPv6 ACLs.

ipv6 standard – Shows ingress/egress rules for Standard IPv6 ACLs.

mac – Shows ingress/egress rules for MAC ACLs.

tcam-utilization – Shows the percentage of user configured ACL rules as a percentage of total ACL rules

acl-name – Name of the ACL. (Maximum length: 16 characters)

COMMAND MODE

Privileged Exec

EXAMPLE

```
Console#show access-list
IP standard access-list david:
  permit host 10.1.1.21
  permit 168.92.0.0 255.255.15.0
IP extended access-list bob:
  permit 10.7.1.1 255.255.255.0 any
  permit 192.168.1.0 255.255.255.0 any destination-port 80 80
  permit 192.168.1.0 255.255.255.0 any protocol tcp control-code 2 2
MAC access-list jerry:
  permit any host 00-30-29-94-34-de ethertype 800 800
IP extended access-list A6:
  deny tcp any any control-flag 2 2
  permit any any
Console#
```

[23] Due to a hardware limitation, this option only displays statistics for permit rules.

31 Interface Commands

These commands are used to display or set communication parameters for an Ethernet port, aggregated link, or VLAN; or perform cable diagnostics on the specified interface.

Table 133: Interface Commands

Command	Function	Mode
Interface Configuration		
interface	Configures an interface type and enters interface configuration mode	GC
alias	Configures an alias name for the interface	IC
capabilities	Advertises the capabilities of a given interface for use in autonegotiation	IC
description	Adds a description to an interface configuration	IC
discard	Discards CDP or PVST packets	IC
flowcontrol	Enables flow control on a given interface	IC
history	Configures a periodic sampling of statistics, specifying the sampling interval and number of samples	IC
media-type	Forces transceiver mode to use for SFP ports	IC
negotiation	Enables autonegotiation of a given interface	IC
shutdown	Disables an interface	IC
switchport mtu	Sets the maximum transfer unit for an interface	IC
clear counters	Clears statistics on an interface	PE
show discard	Displays if CDP and PVST packets are being discarded	PE
show interfaces brief	Displays a summary of key information, including operational status, native VLAN ID, default priority, speed/duplex mode, and port type	PE
show interfaces counters	Displays statistics for the specified interfaces	NE, PE
show interfaces history	Displays statistical history for the specified interfaces	PE
show interfaces status	Displays status for the specified interface	NE, PE
show interfaces switchport	Displays the administrative and operational status of an interface	NE, PE
Transceiver Threshold Configuration		
transceiver-threshold-auto	Uses default threshold settings obtained from the transceiver to determine when an alarm or trap message should be sent	IC
transceiver-threshold-monitor	Sends a trap when any of the transceiver's operational values fall outside specified thresholds	IC
transceiver-threshold current	Sends a trap when the transceiver current falls outside the specified thresholds	IC

Table 133: Interface Commands (Continued)

Command	Function	Mode
transceiver-threshold rx-power	Sends a trap when the power level of the received signal power falls outside the specified thresholds	IC
transceiver-threshold temperature	Sends a trap when the transceiver temperature falls outside the specified thresholds	IC
transceiver-threshold tx-power	Sends a trap when the power level of the transmitted signal power outside the specified thresholds	IC
transceiver-threshold voltage	Sends a trap when the transceiver voltage falls outside the specified thresholds	IC
show interfaces transceiver	Displays the temperature, voltage, bias current, transmit power, and receive power	PE
show interfaces transceiver-threshold	Displays the alarm/warning thresholds for temperature, voltage, bias current, transmit power, and receive power	PE

Interface Configuration

interface

This command configures an interface type and enters interface configuration mode. Use the **no** form with a trunk to remove an inactive interface.

SYNTAX

[**no**] **interface** *interface*

interface

craft - Management port on the front panel.

ethernet *unit/port*

unit - Unit identifier. (Range: 1)

port - Port number. (Range: 1-28)

port-channel *channel-id* (Range: 1-8)

vlan *vlan-id* (Range: 1-4094)

DEFAULT SETTING

None

COMMAND MODE

Global Configuration

COMMAND USAGE

The craft interface is provided as an out-of-band management connection which is isolated from all other ports on the switch. This interface must first be configured with an IPv4 or IPv6 address before a connection can be made through Telnet, SSH, or HTTP.

EXAMPLE

To specify port 4, enter the following command:

```
Console(config)#interface ethernet 1/4
Console(config-if)#
```

alias

This command configures an alias name for the interface. Use the **no** form to remove the alias name.

SYNTAX

alias *string*

no alias

string - A mnemonic name to help you remember what is attached to this interface. (Range: 1-64 characters)

DEFAULT SETTING

None

COMMAND MODE

Interface Configuration (Ethernet, Port Channel)

COMMAND USAGE

The alias is displayed in the running-configuration file. An example of the value which a network manager might store in this object for a WAN interface is the (Telco's) circuit number/identifier of the interface.

EXAMPLE

The following example adds an alias to port 4.

```
Console(config)#interface ethernet 1/4
Console(config-if)#alias finance
Console(config-if)#
```

capabilities

This command advertises the port capabilities of a given interface during auto-negotiation. Use the **no** form with parameters to remove an advertised capability, or the **no** form without parameters to restore the default values.

SYNTAX

[**no**] **capabilities** {**flowcontrol** | **symmetric**}

flowcontrol - Supports flow control

symmetric (Gigabit and 10 Gigabit only) - When specified, the port transmits and receives symmetric pause frames.

DEFAULT SETTING

100Base-FX (SFP) – 100full
1000BASE-SX/LX/LH (SFP): 1000full
10GBASE-SR/LR/ER (XFP/SFP+): 10Gfull

COMMAND MODE

Interface Configuration (Ethernet, Port Channel)

COMMAND USAGE

- 100Base-FX (SFP) connections are fixed at 100Mbps, full duplex; 1000BASE-SFP connections at 1000Mbps, full duplex; and 10GBASE-XFP and 10GBASE-SFP+ connections at 10G, full duplex.

- When auto-negotiation is enabled, the only attributes which can be advertised include flow control and symmetric pause frames.

- When auto-negotiation is enabled with the negotiation command, the switch will negotiate the best settings for a link based on the **capabilities** command. When auto-negotiation is disabled, you must manually specify the link attributes with the flowcontrol command.

EXAMPLE

The following example configures Ethernet port 5 capabilities to include flow control.

```
Console(config)#interface ethernet 1/5
Console(config-if)#capabilities flowcontrol
Console(config-if)#
```

RELATED COMMANDS

negotiation (1194)
flowcontrol (1191)

description

This command adds a description to an interface. Use the **no** form to remove the description.

SYNTAX

description *string*

no description

string - Comment or a description to help you remember what is attached to this interface. (Range: 1-64 characters)

DEFAULT SETTING

None

COMMAND MODE

Interface Configuration (Ethernet, Port Channel)

COMMAND USAGE

The description is displayed by the show interfaces status command and in the running-configuration file. An example of the value which a network manager might store in this object is the name of the manufacturer, and the product name.

EXAMPLE

The following example adds a description to port 4.

```
Console(config)#interface ethernet 1/4
Console(config-if)#description RD-SW#3
Console(config-if)#
```

discard

This command discards CDP or PVST packets. Use the **no** form to forward the specified packet type to other ports configured the same way.

SYNTAX

[**no**] **discard** {**cdp** | **pvst**}

cdp – Cisco Discovery Protocol

pvst – Per-VLAN Spanning Tree

DEFAULT SETTING

Default - Forward CDP and PVST packets

COMMAND MODE

Interface Configuration (Ethernet)

COMMAND USAGE

Use the no discard command to allow CDP or PVST packets to be forwarded to other ports in the same VLAN which are also configured to forward the specified packet type.

EXAMPLE

The following example forwards CDP packets entering port 5.

```
Console(config)#interface ethernet 1/5
Console(config-if)#no discard cdp
Console(config-if)#
```

flowcontrol

This command enables flow control. Use the **no** form to disable flow control.

SYNTAX

[**no**] **flowcontrol**

DEFAULT SETTING

Disabled

COMMAND MODE

Interface Configuration (Ethernet, Port Channel)

COMMAND USAGE

- Flow control can eliminate frame loss by "blocking" traffic from end stations or segments connected directly to the switch when its buffers fill. When enabled, back pressure is used for half-duplex operation and IEEE 802.3-2002 (formally IEEE 802.3x) for full-duplex operation.

- To force flow control on or off (with the **flowcontrol** or **no flowcontrol** command), use the **no negotiation** command to disable auto-negotiation on the selected interface.

- When using the negotiation command to enable auto-negotiation, the optimal settings will be determined by the capabilities command. To enable flow control under auto-negotiation, "flowcontrol" must be included in the capabilities list for any port

EXAMPLE

The following example enables flow control on port 5.

```
Console(config)#interface ethernet 1/5
Console(config-if)#flowcontrol
Console(config-if)#no negotiation
Console(config-if)#
```

RELATED COMMANDS

negotiation (1194)
capabilities (flowcontrol, symmetric) (1189)

history

This command configures a periodic sampling of statistics, specifying the sampling interval and number of samples. Use the **no** form to remove a named entry from the sampling table.

SYNTAX

history *name interval buckets*

no history *name*

name - A symbolic name for this entry in the sampling table. (Range: 1-32 characters)

interval - The interval for sampling statistics. (Range: 1-1440 minutes.

buckets - The number of samples to take. (Range: 1-96)

DEFAULT SETTING

15min - 15 minute interval, 96 buckets

1day - 1 day interval, 7 buckets

COMMAND MODE

Interface Configuration (Ethernet, Port Channel)

EXAMPLE

This example sets a interval of 15 minutes for sampling standard statisical values on port 1.

```
Console(config)#interface ethernet 1/1
Console(config-if)#history 15min 15 10
Console(config-if)#
```

media-type

This command forces the transceiver mode to use for SFP ports. Use the **no** form to restore the default mode.

SYNTAX

media-type sfp-forced [*mode*]

no media-type

sfp-forced - Forces transceiver mode for the SFP port.

mode

1000sfp - Always uses 1000BASE SFP mode.

100fx - Always uses 100BASE-FX mode.

10gsfp - Always uses 10GBASE SFP mode

DEFAULT SETTING

None - Mode is not forced.

COMMAND MODE

Interface Configuration (Ethernet)

Command Usage

Available modes include:
SFP: 1000spf, 100fx
10G SFP+, XFP: 1000spf, 100fx, 10gsfp

EXAMPLE

This forces the switch to use 1000BASE SFP mode for port 25.

```
Console(config)#interface ethernet 1/25
Console(config-if)#media-type sfp-forced 1000sfp
Console(config-if)#
```

negotiation

This command enables auto-negotiation for a given interface. Use the **no** form to disable auto-negotiation.

SYNTAX

[**no**] **negotiation**

DEFAULT SETTING

Enabled

COMMAND MODE

Interface Configuration (Ethernet, Port Channel)

COMMAND USAGE

- When auto-negotiation is enabled the switch will negotiate the best settings for a link based on the capabilities command. When auto-negotiation is disabled, you must manually specify the link attributes with the flowcontrol command.

Note: Auto-negotiation is not supported for 1000BASE SFP transceivers used in 10G SFP+ Ports 51 to 52.

EXAMPLE

The following example configures port 10 to use auto-negotiation.

```
Console(config)#interface ethernet 1/10
Console(config-if)#negotiation
Console(config-if)#
```

RELATED COMMANDS

capabilities (1189)

shutdown

This command disables an interface. To restart a disabled interface, use the **no** form.

SYNTAX

[**no**] **shutdown**

DEFAULT SETTING

All interfaces are enabled.

COMMAND MODE

Interface Configuration (Ethernet, Port Channel)

COMMAND USAGE

This command allows you to disable a port due to abnormal behavior (e.g., excessive collisions), and then re-enable it after the problem has been resolved. You may also want to disable a port for security reasons.

EXAMPLE

The following example disables port 5.

```
Console(config)#interface ethernet 1/5
Console(config-if)#shutdown
Console(config-if)#
```

switchport mtu

This command configures the maximum transfer unit (MTU) allowed for layer 2 packets crossing a Gigabit or 10 Gigabit Ethernet port or trunk. Use the **no** form to restore the default setting.

SYNTAX

switchport mtu *size*

no switchport mtu

size - Specifies the maximum transfer unit (or frame size) for a Gigabit and 10 Gigabit Ethernet port or trunk. (Range: 1500-9216 bytes)

DEFAULT SETTING

1518 bytes

COMMAND MODE

Interface Configuration (Ethernet, Port Channel)

COMMAND USAGE

- Use the jumbo frame command to enable or disable jumbo frames for all Gigabit and 10 Gigabit Ethernet ports. To set the MTU for a specific interface, enable jumbo frames and use this command to specify the required size of the MTU.

- The comparison of packet size against the configured port MTU considers only the incoming packet size, and is not affected by the fact that an ingress port is a tagged port or a QinQ ingress port. In other words, any additional size (for example, a tagged field of 4 bytes added by the chip) will not be considered when comparing the egress packet's size against the configured MTU.

- When pinging the switch from an external device, information added for the Ethernet header can increase the packet size by at least 42 bytes for an untagged packet, and 46 bytes for a tagged packet. If the adjusted frame size exceeds the configured port MTU, the switch will not respond to the ping message.

- For other traffic types, calculation of overall frame size is basically the same, including the additional header fields SA(6) + DA(6) + Type(2) + VLAN-Tag(4) (for tagged packets, for untaqged packets, the 4-byte field will not be added by switch), and the payload. This should all be less than the configured port MTU, including the CRC at the end of the frame.

- For QinQ, the overall frame size is still calculated as described above, and does not add the length of the second tag to the frame.

- The port MTU size can be displayed with the show show interfaces status command.

EXAMPLE

The following first enables jumbo frames for layer 2 packets, and then sets the MTU for port 1:

```
Console(config)#jumbo frame
Console(config)#interface ethernet 1/1
Console(config-if)#switchport mtu 9216
Console(config-if)#
```

RELATED COMMANDS

jumbo frame (911)
show interfaces status (1202)

clear counters

This command clears statistics on an interface.

SYNTAX

clear counters *interface*

interface

ethernet *unit/port*

unit - Unit identifier. (Range: 1)

port - Port number. (Range: 1-28)

port-channel *channel-id* (Range: 1-8)

vlan *vlan-id* (Range: 1-4094)

DEFAULT SETTING

None

COMMAND MODE

Privileged Exec

COMMAND USAGE

Statistics are only initialized for a power reset. This command sets the base value for displayed statistics to zero for the current management session. However, if you log out and back into the management interface, the statistics displayed will show the absolute value accumulated since the last power reset.

EXAMPLE

The following example clears statistics on port 5.

```
Console#clear counters ethernet 1/5
Console#
```

show discard

This command displays whether or not CDP and PVST packets are being discarded.

COMMAND MODE

Privileged Exec

EXAMPLE

In this example, “Default” means that the packets are not discarded.

```
Console#show discard
Port     CDP     PVST
-------- ------- -------
Eth 1/ 1 Default Default
Eth 1/ 2 Default Default
Eth 1/ 3 Default Default
Eth 1/ 4 Default Default
Eth 1/ 7 Default Default
Eth 1/ 8 Default Default
Eth 1/ 9 Default Default
Eth 1/10 Default Default
Eth 1/11 Default Default
Eth 1/12 Default Default
Console#
```

show interfaces brief

This command displays a summary of key information, including operational status, native VLAN ID, default priority, speed/duplex mode, and port type for all ports.

COMMAND MODE

Privileged Exec

EXAMPLE

```
Console#show interfaces brief
Interface Name              Status   PVID Pri Speed/Duplex  Type        Trunk
--------- ------------------ -------- ---- --- ------------- ------------ ---
Eth 1/ 1                    Up          1   0 Auto-1000full 1000Base SFP None
Eth 1/ 2                    Down        1   0 Auto          1000Base SFP None
Eth 1/ 3                    Down        1   0 Auto          1000Base SFP None
 ⋮
```

show interfaces counters

This command displays interface statistics.

SYNTAX

show interfaces counters [*interface*]

interface

ethernet *unit/port*

unit - Unit identifier. (Range: 1)

port - Port number. (Range: 1-28)

port-channel *channel-id* (Range: 1-8)

vlan *vlan-id* (Range: 1-4094)

DEFAULT SETTING

Shows the counters for all interfaces.

COMMAND MODE

Normal Exec, Privileged Exec

COMMAND USAGE

If no interface is specified, information on all interfaces is displayed. For a description of the items displayed by this command, see "Showing Port or Trunk Statistics" on page 192.

EXAMPLE

```
Console#show interfaces counters ethernet 1/1
Ethernet 1/ 1
 ===== IF table Stats =====
                2166458 Octets Input
               14734059 Octets Output
                  14707 Unicast Input
                  19806 Unicast Output
                      0 Discard Input
                      0 Discard Output
                      0 Error Input
                      0 Error Output
                      0 Unknown Protocols Input
                      0 QLen Output
 ===== Extended Iftable Stats =====
                     23 Multi-cast Input
                   5525 Multi-cast Output
                    170 Broadcast Input
                     11 Broadcast Output
 ===== Ether-like Stats =====
                      0 Alignment Errors
                      0 FCS Errors
                      0 Single Collision Frames
                      0 Multiple Collision Frames
                      0 SQE Test Errors
                      0 Deferred Transmissions
                      0 Late Collisions
                      0 Excessive Collisions
                      0 Internal Mac Transmit Errors
                      0 Internal Mac Receive Errors
                      0 Frames Too Long
                      0 Carrier Sense Errors
```

```
                       0 Symbol Errors
                       0 Pause Frames Input
                       0 Pause Frames Output
 ===== RMON Stats =====
                       0 Drop Events
                16900558 Octets
                   40243 Packets
                     170 Broadcast PKTS
                      23 Multi-cast PKTS
                       0 Undersize PKTS
                       0 Oversize PKTS
                       0 Fragments
                       0 Jabbers
                       0 CRC Align Errors
                       0 Collisions
                   21065 Packet Size <= 64 Octets
                    3805 Packet Size 65 to 127 Octets
                    2448 Packet Size 128 to 255 Octets
                     797 Packet Size 256 to 511 Octets
                    2941 Packet Size 512 to 1023 Octets
                    9187 Packet Size 1024 to 1518 Octets
 ===== Port Utilization =====
                     111 Octets Input per seconds
                       0 Packets Input per seconds
                    0.00 % Input Utilization
                     606 Octets Output per seconds
                       1 Packets Output per second
                    0.00 % Output Utilization
Console#show interfaces counters vlan 1
VLAN 1
                   21462 Octets Input
                      93 Packets Input
Console#
```

show interfaces history

This command displays statistical history for the specified interfaces.

show interfaces history [*interface* [*name* [**current** | **previous** *index count*] [**input** | **output**]]]

interface

ethernet *unit*/*port*

unit - Unit identifier. (Range: 1)

port - Port number. (Range: 1-28)

port-channel *channel-id* (Range: 1-8)

name - Name of sample as defined in the history command. (Range: 1-32 characters)

current - Statistics recorded in current interval.

previous - Statistics recorded in previous intervals.

index - An index into the buckets containing previous samples. (Range: 1-96)

count - The number of historical samples to display. (Range: 1-96)

input - Ingress traffic.

output - Egress traffic.

DEFAULT SETTING

Shows historical statistics for all interfaces, intervals, ingress traffic, and egress traffic.

COMMAND MODE

Privileged Exec

COMMAND USAGE

If no interface is specified, information on all interfaces is displayed. For a description of the items displayed by this command, see "Showing Port or Trunk Statistics" on page 192.

EXAMPLE

This example shows the statistics recorded for all named entries in the sampling table.

```
Console#show interfaces history ethernet 1/1
Interface         : Eth 1/ 1
Name              : 1min
Interval          : 1 minute(s)
Buckets Requested : 15
Buckets Granted   : 15
Status            : Active

Current Entries

 Start Time   Octets Input    Unicast       Multicast     Broadcast
 ------------ --------------- ------------- ------------- -------------
 00d 02:50:52        15059355         80275         43750          2304

                              Discards      Errors        Unknown Proto
                              ------------- ------------- -------------
                                          0             0             0

              Octets Output   Unicast       Multicast     Broadcast
              --------------- ------------- ------------- -------------
                     84493398        106787         47232          1158

                              Discards      Errors
                              ------------- -------------
                                          0             0

Interface         : Eth 1/ 1
Name              : 15min
Interval          : 15 minute(s)
Buckets Requested : 96
Buckets Granted   : 11
Status            : Active

Current Entries

 Start Time   Octets Input    Unicast       Multicast     Broadcast
 ------------ --------------- ------------- ------------- -------------
 00d 02:45:07       116003318        616894        336491         17899

                              Discards      Errors        Unknown Proto
                              ------------- ------------- -------------
                                          0             0             0
              Octets Output   Unicast       Multicast     Broadcast
              --------------- ------------- ------------- -------------
                    648387890        819696        358285          8921

                              Discards      Errors
                              ------------- -------------
                                          0             0

Interface         : Eth 1/ 1
Name              : 1day
Interval          : 1440 minute(s)
Buckets Requested : 7
Buckets Granted   : 0
Status            : Active

Current Entries

 Start Time   Octets Input    Unicast       Multicast     Broadcast
 ------------ --------------- ------------- ------------- -------------
 00d 00:00:01      1563328011       8391643       4440171        241090

                              Discards      Errors        Unknown Proto
                              ------------- ------------- -------------
                                          0             0             0

              Octets Output   Unicast       Multicast     Broadcast
              --------------- ------------- ------------- -------------
                   8896498997      11151669       4734465        119595

                              Discards      Errors
                              ------------- -------------
                                          0             0

Console#
```

This example shows the statistics recorded for a named entry in the sampling table.

```
Console#show interfaces history ethernet 1/1 1min
Interface         : Eth 1/ 1
Name              : 1min
Interval          : 1 minute(s)
Buckets Requested : 10
Buckets Granted   : 3
Status            : Active

Current Entries

 Start Time   Octets Input    Unicast       Multicast     Broadcast
 ------------ --------------- ------------- ------------- -------------
 00d 00:08:40         1042759          6932          1653            54

                              Discards      Errors        Unknown Proto
                              ------------- ------------- -------------
                                          0             0             0

              Octets Output   Unicast       Multicast     Broadcast
              --------------- ------------- ------------- -------------
                      5095864          7894          1776            18
```

```
                              Discards      Errors
                              ------------- -------------
                                          0             0

Previous Entries

 Start Time   Octets Input    Unicast       Multicast     Broadcast
 ------------ --------------- ------------- ------------- -------------
 00d 00:05:37         1400912          9381          1895            50
 00d 00:06:37         1566090         10660          2195            50
 00d 00:07:37         1754781         11786          2674            59

 Start Time   Octets Input    Discards      Errors        Unknown Proto
 ------------ --------------- ------------- ------------- -------------
 00d 00:05:37         1400912             0             0             0
 00d 00:06:37         1566090             0             0             0
 00d 00:07:37         1754781             0             0             0

 Start Time   Octets Output   Unicast       Multicast     Broadcast
 ------------ --------------- ------------- ------------- -------------
 00d 00:05:37         6827866         10563          2042            30
 00d 00:06:37         7572668         12040          2362            30
 00d 00:07:37         8548505         13380          2879            30

 Start Time   Octets Output   Discards      Errors
 ------------ --------------- ------------- -------------
 00d 00:05:37         6827866             0             0
 00d 00:06:37         7572668             0             0
 00d 00:07:37         8548505             0             0

Console#
```

show interfaces status

This command displays the status for an interface.

SYNTAX

show interfaces status [*interface*]

interface

ethernet *unit*/*port*

unit - Unit identifier. (Range: 1)

port - Port number. (Range: 1-28)

port-channel *channel-id* (Range: 1-8)

vlan *vlan-id* (Range: 1-4094)

DEFAULT SETTING

Shows the status for all interfaces.

COMMAND MODE

Normal Exec, Privileged Exec

COMMAND USAGE

If no interface is specified, information on all interfaces is displayed. For a description of the items displayed by this command, see "Displaying Connection Status" on page 185.

EXAMPLE

```
Console#show interfaces status ethernet 1/1
Information of Eth 1/1
 Basic Information:
  Port Type                 : 1000Base SFP
  MAC Address               : 00-00-0C-00-00-FE
 Configuration:
  Name                      :
  Port Admin                : Up
  Speed-duplex              : Auto
  Capabilities              : 1000full
  Broadcast Storm           : Enabled
  Broadcast Storm Limit     : 500 packets/second
  Multicast Storm           : Disabled
  Multicast Storm Limit     : 262143 packets/second
  Unknown Unicast Storm          : Disabled
  Unknown Unicast Storm Limit : 262143 packets/second
  Flow Control              : Disabled
  VLAN Trunking             : Disabled
  LACP                      : Disabled
  MAC-Learning              : Yes
  Media Type                : SFP forced
  MTU                       : 1518
 Current Status:
  Link Status               : Up
  Port Operation Status     : Up
  Operation Speed-duplex    : 1000full
  Up Time                   : 0w 0d 1h 41m 8s (6068 seconds)
  Flow Control Type         : None
  Max Frame Size            : 1518 bytes (1522 bytes for tagged frames)
  MAC Learning Status       : Enabled
Console#
```

show interfaces switchport

This command displays the administrative and operational status of the specified interfaces.

SYNTAX

show interfaces switchport [*interface*]

interface

ethernet *unit*/*port*

unit - Unit identifier. (Range: 1)

port - Port number. (Range: 1-28)

port-channel *channel-id* (Range: 1-8)

DEFAULT SETTING

Shows all interfaces.

COMMAND MODE

Normal Exec, Privileged Exec

COMMAND USAGE

If no interface is specified, information on all interfaces is displayed.

EXAMPLE

This example shows the configuration setting for port 1.

```
Console#show interfaces switchport ethernet 1/1
Information of Eth 1/1
 Broadcast Threshold             : Enabled, 500 packets/second
 Multicast Threshold             : Disabled
 Unknown Unicast Threshold       : Disabled
 LACP Status                     : Disabled
 Ingress Rate Limit              : Disabled, 1000000 Kbits per second
 Egress Rate Limit               : Disabled, 1000000 Kbits per second
 VLAN Membership Mode            : Hybrid
 Ingress Rule                    : Disabled
 Acceptable Frame Type           : All frames
 Native VLAN                     : 1
 Priority for Untagged Traffic : 0
 GVRP Status                     : Disabled
 Allowed VLAN                    :     1(u)
 Forbidden VLAN                  :
 Private-VLAN Mode               : None
 Private-VLAN host-association : None
 Private-VLAN Mapping            : None
 802.1Q Tunnel Status            : Disabled
 802.1Q Tunnel Mode              : Normal
 802.1Q Tunnel TPID              : 8100 (Hex)
 Layer 2 Protocol Tunnel         : None
 Broadcast Block                 : Disabled
 Unknown Multicast Block         : Disabled
 Unknown Unicast Block           : Disabled
Console#
```

Table 134: show interfaces switchport - display description

Field	Description
Broadcast Threshold	Shows if broadcast storm suppression is enabled or disabled; if enabled it also shows the threshold level (page 1241).
Multicast Threshold	Shows if multicast storm suppression is enabled or disabled; if enabled it also shows the threshold level (page 1241).
Unknown Unicast Threshold	Shows if unknown unicast storm suppression is enabled or disabled; if enabled it also shows the threshold level (page 1241).
LACP Status	Shows if Link Aggregation Control Protocol has been enabled or disabled (page 1218).
Ingress/Egress Rate Limit	Shows if rate limiting is enabled, and the current rate limit (page 1205).
VLAN Membership Mode	Indicates membership mode as Trunk or Hybrid (page 1349).
Ingress Rule	Shows if ingress filtering is enabled or disabled (page 1348).
Acceptable Frame Type	Shows if acceptable VLAN frames include all types or tagged frames only (page 1346).
Native VLAN	Indicates the default Port VLAN ID (page 1350).
Priority for Untagged Traffic	Indicates the default priority for untagged frames (page 1390).
GVRP Status	Shows if GARP VLAN Registration Protocol is enabled or disabled (page 1340).

Table 134: show interfaces switchport - display description (Continued)

Field	Description
Allowed VLAN	Shows the VLANs this interface has joined, where "(u)" indicates untagged and "(t)" indicates tagged (page 1347).
Forbidden VLAN	Shows the VLANs this interface can not dynamically join via GVRP (page 1340).
Private-VLAN Mode	Shows the private VLAN mode as host, promiscuous, or none (1369).
Private VLAN host-association	Shows the secondary (or community) VLAN with which this port is associated (1368).
Private VLAN mapping	Shows the primary VLAN mapping for a promiscuous port (1370).
802.1Q-tunnel Status	Shows if 802.1Q tunnel is enabled on this interface (page 1354).
802.1Q-tunnel Mode	Shows the tunnel mode as Normal, 802.1Q Tunnel or 802.1Q Tunnel Uplink (page 1355).
802.1Q-tunnel TPID	Shows the Tag Protocol Identifier used for learning and switching packets (page 1358).
Layer 2 Protocol Tunnel	Shows if L2 Protocol Tunnel is enabled for spanning tree protocol (page 1363).
Broadcast Block	Shows if the broadcast packets are blocked (page 1242).
Unknown Multicast Block	Shows if the unknown multicast packets are blocked (page 1242).
Unknown Unicast Block	Shows if the unknown unicast packets are blocked (page 1242).

Transceiver Threshold Configuration

transceiver-threshold-auto

This command uses default threshold settings obtained from the transceiver to determine when an alarm or warning message should be sent. Use the **no** form to disable this feature.

SYNTAX

transceiver-threshold-auto

DEFAULT SETTING

Enabled

COMMAND MODE

Interface Configuration (Ethernet)

EXAMPLE

```
Console(config)interface ethernet 1/11
Console(config-if)#transceiver-threshold-auto
Console#
```

transceiver-threshold-monitor

This command sends a trap when any of the transceiver's operational values fall outside of specified thresholds. Use the **no** form to disable trap messages.

Syntax

transceiver-monitor

Default Setting

Enabled

Command Mode

Interface Configuration (Ethernet)

Example

```
Console(config)interface ethernet 1/11
Console(config-if)#transceiver-monitor
Console#
```

transceiver-threshold current

This command sets thresholds for transceiver current which can be used to trigger an alarm or warning message.

Syntax

transceiver-threshold current {**high-alarm** | **high-warning** | **low-alarm** | **low-warning**} *threshold-value*

high-alarm – Sets the high current threshold for an alarm message.

high-warning – Sets the high current threshold for a warning message.

low-alarm – Sets the low current threshold for an alarm message.

low-warning – Sets the low current threshold for a warning message.

threshold-value – The threshold of the transceiver current. (Range: 100-25500 in units of 0.01 mA)

Default Setting

High Alarm: 100 mA
HIgh Warning: 90 mA
Low Warning: 7 mA
Low Alarm: 6 mA

Command Mode

Interface Configuration (Ethernet)

Command Usage

- If trap messages are enabled with the transceiver-threshold-monitor command, and a high-threshold alarm or warning message is sent if the current value is greater than or equal to the threshold, and the last sample value was less than the threshold. After a rising event has been generated, another such event will not be generated until the sampled value has fallen below the high threshold and reaches the low threshold.

- If trap messages are enabled with the transceiver-threshold-monitor command, and a low-threshold alarm or warning message is sent if the current value is less than or equal to the threshold, and the last sample value was greater than the threshold. After a falling event has been generated, another such event will not be generated until the sampled value has risen above the low threshold and reaches the high threshold.

- Threshold events are triggered as described above to avoid a hysteresis effect which would continuously trigger event messages if the power level were to fluctuate just above and below either the high threshold or the low threshold.

- Trap messages enabled by the transceiver-threshold-monitor command are sent to any management station configured by the snmp-server host command.

EXAMPLE

The following example sets alarm thresholds for the transceiver current at port 1.

```
Console(config)interface ethernet 1/1
Console(config-if)#transceiver-threshold current low-alarm 100
Console(config-if)#transceiver-threshold rx-power high-alarm 700
Console#
```

transceiver-threshold rx-power

This command sets thresholds for the transceiver power level of the received signal which can be used to trigger an alarm or warning message.

SYNTAX

transceiver-threshold rx-power {**high-alarm** | **high-warning** | **low-alarm** | **low-warning**} *threshold-value*

high-alarm – Sets the high power threshold for an alarm message.

high-warning – Sets the high power threshold for a warning message.

low-alarm – Sets the low power threshold for an alarm message.

low-warning – Sets the low power threshold for a warning message.

threshold-value – The power threshold of the received signal. (Range: -9999 - 9999 in units of 0.01 dBm)

DEFAULT SETTING

High Alarm: -3.00 dBm
HIgh Warning: -3.50 dBm
Low Warning: -21.00 dBm
Low Alarm: -21.50 dBm

COMMAND MODE

Interface Configuration (Ethernet)

COMMAND USAGE

- The threshold value is the power ratio in decibels (dB) of the measured power referenced to one milliwatt (mW).

- Refer to the Command Usage section under the transceiver-threshold current command for more information on configuring transceiver thresholds.

- Trap messages enabled by the transceiver-threshold-monitor command are sent to any management station configured by the snmp-server host command.

EXAMPLE

The following example sets alarm thresholds for the signal power received at port 1.

```
Console(config)interface ethernet 1/1
Console(config-if)#transceiver-threshold rx-power low-alarm -21
Console(config-if)#transceiver-threshold rx-power high-alarm -3
Console#
```

transceiver-threshold temperature

This command sets thresholds for the transceiver temperature which can be used to trigger an alarm or warning message.

SYNTAX

transceiver-threshold temperature {**high-alarm** | **high-warning** | **low-alarm** | **low-warning**} *threshold-value*

high-alarm – Sets the high temperature threshold for an alarm message.

high-warning – Sets the high temperature threshold for a warning message.

low-alarm – Sets the low temperature threshold for an alarm message.

low-warning – Sets the low temperature threshold for a warning message.

threshold-value – The threshold of the transceiver temperature. (Range: -20000 - 20000 in units of 0.01 Celsius)

DEFAULT SETTING

High Alarm: 75.00 °C
HIgh Warning: 70.00 °C
Low Alarm: -123.00 °C
Low Warning: 0.00 °C

COMMAND MODE

Interface Configuration (Ethernet)

COMMAND USAGE

- Refer to the Command Usage section under the transceiver-threshold current command for more information on configuring transceiver thresholds.
- Trap messages enabled by the transceiver-threshold-monitor command are sent to any management station configured by the snmp-server host command.

EXAMPLE

The following example sets alarm thresholds for the transceiver temperature at port 1.

```
Console(config)interface ethernet 1/1
Console(config-if)#transceiver-threshold temperature low-alarm 97
Console(config-if)#transceiver-threshold temperature high-alarm -83
Console#
```

transceiver-threshold tx-power

This command sets thresholds for the transceiver power level of the transmitted signal which can be used to trigger an alarm or warning message.

SYNTAX

transceiver-threshold tx-power {**high-alarm** | **high-warning** | **low-alarm** | **low-warning**} *threshold-value*

high-alarm – Sets the high power threshold for an alarm message.

high-warning – Sets the high power threshold for a warning message.

low-alarm – Sets the low power threshold for an alarm message.

low-warning – Sets the low power threshold for a warning message.

threshold-value – The power threshold of the transmitted signal. (Range: -9999 - 9999 in units of 0.01 dBm)

DEFAULT SETTING

High Alarm: -9.00 dBm
HIgh Warning: -9.50 dBm

Low Warning: -21.00 dBm
Low Alarm: -21.50 dBm

COMMAND MODE

Interface Configuration (Ethernet)

COMMAND USAGE

- The threshold value is the power ratio in decibels (dB) of the measured power referenced to one milliwatt (mW).

- Refer to the Command Usage section under the transceiver-threshold current command for more information on configuring transceiver thresholds.

- Trap messages enabled by the transceiver-threshold-monitor command are sent to any management station configured by the snmp-server host command.

EXAMPLE

The following example sets alarm thresholds for the signal power transmitted at port 1.

```
Console(config)interface ethernet 1/1
Console(config-if)#transceiver-threshold tx-power low-alarm 8
Console(config-if)#transceiver-threshold tx-power high-alarm -3
Console#
```

transceiver-threshold voltage

This command sets thresholds for the transceiver voltage which can be used to trigger an alarm or warning message.

SYNTAX

transceiver-threshold voltage {**high-alarm** | **high-warning** | **low-alarm** | **low-warning**} *threshold-value*

high-alarm – Sets the high voltage threshold for an alarm message.

high-warning – Sets the high voltage threshold for a warning message.

low-alarm – Sets the low voltage threshold for an alarm message.

low-warning – Sets the low voltage threshold for a warning message.

threshold-value – The threshold of the transceiver voltage. (Range: 100-25500 in units of 0.01 Volt)

DEFAULT SETTING

High Alarm: 3.50 Volts
HIgh Warning: 3.45 Volts
Low Warning: 3.15 Volts
Low Alarm: 3.10 Volts

Command Mode

Interface Configuration (Ethernet)

Command Usage

- Refer to the Command Usage section under the transceiver-threshold current command for more information on configuring transceiver thresholds.
- Trap messages enabled by the transceiver-threshold-monitor command are sent to any management station configured by the snmp-server host command.

Example

The following example sets alarm thresholds for the transceiver voltage at port 1.

```
Console(config)interface ethernet 1/1
Console(config-if)#transceiver-threshold voltage low-alarm 4
Console(config-if)#transceiver-threshold voltage high-alarm 2
Console#
```

show interfaces transceiver

This command displays identifying information for the specified transceiver, including connector type and vendor-related parameters, as well as the temperature, voltage, bias current, transmit power, and receive power.

Syntax

show interfaces transceiver [*interface*]

interface

ethernet *unit*/*port*

unit - Unit identifier. (Range: 1)

port - Port number. (Range: 1-28)

Default Setting

Shows all SFP interfaces.

Command Mode

Privileged Exec

Command Usage

The switch can display diagnostic information for SFP modules which support the SFF-8472 Specification for Diagnostic Monitoring Interface for Optical Transceivers. This information allows administrators to remotely diagnose problems with optical devices. This feature, referred to as Digital Diagnostic Monitoring (DDM) in the command display, provides information on transceiver parameters including temperature, supply voltage, laser bias current, laser power, received optical power, and related alarm thresholds.

EXAMPLE

```
Console#show interfaces transceiver ethernet 1/25
Information of Eth 1/25
 Connector Type          : LC
 Fiber Type              : Multimode 50um (M5), Multimode 62.5um (M6)
 Eth Compliance Codes    : 1000BASE-SX
 Baud Rate               : 2100 MBd
 Vendor OUI              : 00-90-65
 Vendor Name             : FINISAR CORP.
 Vendor PN               : FTLF8519P2BNL
 Vendor Rev              : A
 Vendor SN               : PFS4U5F
 Date Code               : 09-07-02
 DDM Info
   Temperature           : 11.54 degree C
   Vcc                   : 3.25 V
   Bias Current          : 7.21 mA
   TX Power              : -4.37 dBm
   RX Power              : -31.55 dBm
 DDM Thresholds
                              Low Alarm  Low Warning  High Warning    High Alarm
   -----------            ------------ ------------ ------------  ------------
   Temperature(Celsius)        -123.00         0.00        70.00         75.00
   Voltage(Volts)                 3.10         3.15         3.45          3.50
   Current(mA)                    6.00         7.00        90.00        100.00
   TxPower(dBm)                 -12.00       -11.50        -9.50!        -9.00!
   RxPower(dBm)                 -21.50!      -21.00!       -3.50         -3.00
Console#
```

show interfaces transceiver-threshold

This command Displays the alarm/warning thresholds for temperature, voltage, bias current, transmit power, and receive power. **SYNTAX**

SYNTAX

show interfaces transceiver-threshold [*interface*]

interface

ethernet *unit*/*port*

unit - Unit identifier. (Range: 1)

port - Port number. (Range: 1-28)

DEFAULT SETTING

Shows all SFP interfaces.

COMMAND MODE

Privileged Exec

COMMAND USAGE

- The switch can display diagnostic information for SFP modules which support the SFF-8472 Specification for Diagnostic Monitoring Interface for Optical Transceivers. This information allows administrators to remotely diagnose problems with optical devices. This feature, referred to as Digital Diagnostic Monitoring (DDM) in the command display, provides information on transceiver parameters including temperature, supply voltage, laser bias current, laser power, received optical power, and related alarm thresholds.

- The DDM thresholds displayed by this command only apply to ports which have a DDM-compliant transceiver inserted.

EXAMPLE

```
Console#show interfaces transceiver-threshold ethernet 1/25
Information of Eth 1/25
 DDM Thresholds
 Transceiver-monitor        : Disabled
 Transceiver-threshold-auto : Enabled
                            Low Alarm   Low Warning  High Warning    High Alarm
   -----------           ------------  ------------  ------------  ------------
   Temperature(Celsius)       -123.00         0.00        70.00        75.00
   Voltage(Volts)                3.10         3.15         3.45         3.50
   Current(mA)                   6.00         7.00        90.00       100.00
   TxPower(dBm)                -12.00       -11.50        -9.50        -9.00
   RxPower(dBm)                -21.50       -21.00        -3.50        -3.00
Console#
```

32 Link Aggregation Commands

Ports can be statically grouped into an aggregate link (i.e., trunk) to increase the bandwidth of a network connection or to ensure fault recovery. Or you can use the Link Aggregation Control Protocol (LACP) to automatically negotiate a trunk link between this switch and another network device. For static trunks, the switches have to comply with the Cisco EtherChannel standard. For dynamic trunks, the switches have to comply with LACP. This switch supports up to 8 trunks. For example, a trunk consisting of two 1000 Mbps ports can support an aggregate bandwidth of 4 Gbps when operating at full duplex.

Table 135: Link Aggregation Commands

Command	Function	Mode
Manual Configuration Commands		
interface port-channel	Configures a trunk and enters interface configuration mode for the trunk	GC
port channel load-balance	Sets the load-distribution method among ports in aggregated links	GC
channel-group	Adds a port to a trunk	IC (Ethernet)
Dynamic Configuration Commands		
lacp	Configures LACP for the current interface	IC (Ethernet)
lacp admin-key	Configures a port's administration key	IC (Ethernet)
lacp port-priority	Configures a port's LACP port priority	IC (Ethernet)
lacp system-priority	Configures a port's LACP system priority	IC (Ethernet)
lacp admin-key	Configures an port channel’s administration key	IC (Port Channel)
lacp timeout	Configures the timeout to wait for next LACPDU	IC (Port Channel)
Trunk Status Display Commands		
show interfaces status port-channel	Shows trunk information	NE, PE
show lacp	Shows LACP information	PE
show port-channel load-balance	Shows the load-distribution method used on aggregated links	PE

Guidelines for Creating Trunks

General Guidelines –

- Finish configuring trunks before you connect the corresponding network cables between switches to avoid creating a loop.
- A trunk can have up to 8 ports.

- The ports at both ends of a connection must be configured as trunk ports.
- All ports in a trunk must be configured in an identical manner, including communication mode (i.e., speed and duplex mode), VLAN assignments, and CoS settings.
- Any of the Gigabit ports on the front panel can be trunked together, including ports of different media types.
- All the ports in a trunk have to be treated as a whole when moved from/to, added or deleted from a VLAN via the specified port-channel.
- STP, VLAN, and IGMP settings can only be made for the entire trunk via the specified port-channel.

Dynamically Creating a Port Channel –

Ports assigned to a common port channel must meet the following criteria:

- Ports must have the same LACP system priority.
- Ports must have the same port admin key (Ethernet Interface).
- If the port channel admin key (lacp admin key - Port Channel) is not set when a channel group is formed (i.e., it has the null value of 0), this key is set to the same value as the port admin key (lacp admin key - Ethernet Interface) used by the interfaces that joined the group.
- However, if the port channel admin key is set, then the port admin key must be set to the same value for a port to be allowed to join a channel group.
- If a link goes down, LACP port priority is used to select the backup link.

Manual Configuration Commands

port channel load-balance

This command sets the load-distribution method among ports in aggregated links (for both static and dynamic trunks). Use the **no** form to restore the default setting.

SYNTAX

port channel load-balance {**dst-ip** | **dst-mac** | **src-dst-ip** | **src-dst-mac** | **src-ip** | **src-mac**}

no port channel load-balance

dst-ip - Load balancing based on destination IP address.

dst-mac - Load balancing based on destination MAC address.

src-dst-ip - Load balancing based on source and destination IP address.

src-dst-mac - Load balancing based on source and destination MAC address.

src-ip - Load balancing based on source IP address.

src-mac - Load balancing based on source MAC address.

DEFAULT SETTING

src-dst-ip

COMMAND MODE

Global Configuration

COMMAND USAGE

- This command applies to all static and dynamic trunks on the switch.
- To ensure that the switch traffic load is distributed evenly across all links in a trunk, select the source and destination addresses used in the load-balance calculation to provide the best result for trunk connections:
  - **dst-ip**: All traffic with the same destination IP address is output on the same link in a trunk. This mode works best for switch-to-router trunk links where traffic through the switch is destined for many different hosts. Do not use this mode for switch-to-server trunk links where the destination IP address is the same for all traffic.
  - **dst-mac**: All traffic with the same destination MAC address is output on the same link in a trunk. This mode works best for switch-to-switch trunk links where traffic through the switch is destined for many different hosts. Do not use this mode for switch-to-router trunk links where the destination MAC address is the same for all traffic.
  - **src-dst-ip**: All traffic with the same source and destination IP address is output on the same link in a trunk. This mode works best for switch-to-router trunk links where traffic through the switch is received from and destined for many different hosts.
  - **src-dst-mac**: All traffic with the same source and destination MAC address is output on the same link in a trunk. This mode works best for switch-to-switch trunk links where traffic through the switch is received from and destined for many different hosts.
  - **src-ip**: All traffic with the same source IP address is output on the same link in a trunk. This mode works best for switch-to-router or switch-to-server trunk links where traffic through the switch is received from many different hosts.
  - **src-mac**: All traffic with the same source MAC address is output on the same link in a trunk. This mode works best for switch-to-switch trunk links where traffic through the switch is received from many different hosts.

EXAMPLE

```
Console(config)#port-channel load-balance dst-ip
Console(config)#
```

channel-group

This command adds a port to a trunk. Use the **no** form to remove a port from a trunk.

SYNTAX

channel-group *channel-id*

no channel-group

channel-id - Trunk index (Range: 1-8)

DEFAULT SETTING

The current port will be added to this trunk.

COMMAND MODE

Interface Configuration (Ethernet)

COMMAND USAGE

- When configuring static trunks, the switches must comply with the Cisco EtherChannel standard.
- Use **no channel-group** to remove a port group from a trunk.
- Use no interface port-channel to remove a trunk from the switch.

EXAMPLE

The following example creates trunk 1 and then adds port 10:

```
Console(config)#interface port-channel 1
Console(config-if)#exit
Console(config)#interface ethernet 1/10
Console(config-if)#channel-group 1
Console(config-if)#
```

Dynamic Configuration Commands

lacp

This command enables 802.3ad Link Aggregation Control Protocol (LACP) for the current interface. Use the **no** form to disable it.

SYNTAX

[**no**] **lacp**

DEFAULT SETTING

Disabled

COMMAND MODE

Interface Configuration (Ethernet)

COMMAND USAGE

- The ports on both ends of an LACP trunk must be configured for full duplex, either by forced mode or auto-negotiation.
- A trunk formed with another switch using LACP will automatically be assigned the next available port-channel ID.
- If the target switch has also enabled LACP on the connected ports, the trunk will be activated automatically.
- If more than eight ports attached to the same target switch have LACP enabled, the additional ports will be placed in standby mode, and will only be enabled if one of the active links fails.

EXAMPLE

The following shows LACP enabled on ports 1-3. Because LACP has also been enabled on the ports at the other end of the links, the show interfaces status port-channel 1 command shows that Trunk1 has been established.

```
Console(config)#interface ethernet 1/1
Console(config-if)#lacp
Console(config-if)#interface ethernet 1/2
Console(config-if)#lacp
Console(config-if)#interface ethernet 1/3
Console(config-if)#lacp
Console(config-if)#end
Console#show interfaces status port-channel 1
Information of Trunk 1
 Basic Information:
  Port Type                : 1000Base SFP
  MAC Address              : 12-34-12-34-12-3F
Configuration:
  Name                     :
  Port Admin               : Up
  Speed-duplex             : Auto
  Capabilities             : 1000full
  Broadcast Storm          : Enabled
  Broadcast Storm Limit    : 500 packets/second
  Multicast Storm          : Disabled
  Multicast Storm Limit    : 64 Kbits/second
  Unknown Unicast Storm         : Disabled
  Unknown Unicast Storm Limit : 64 Kbits/second
  Flow Control             : Disabled
  VLAN Trunking            : Disabled
  MAC Learning             : Yes
  MTU                      : 1518
 Current status:
  Created By               : LACP
  Link Status              : Up
  Port Operation Status    : Up
  Operation speed-duplex   : 1000full
  Up Time                  : 0w 0d 0h 14s (14 seconds)
  Flow control Type        : None
  Max Frame Size           : 1518 bytes (1522 bytes for tagged frames)
  Member Ports             : Eth1/1, Eth1/2, Eth1/3,
Console#
```

lacp admin-key (Ethernet Interface)

This command configures a port's LACP administration key. Use the **no** form to restore the default setting.

SYNTAX

lacp {**actor** | **partner**} **admin-key** *key*

no lacp {**actor** | **partner**} **admin-key**

actor - The local side an aggregate link.

partner - The remote side of an aggregate link.

key - The port admin key must be set to the same value for ports that belong to the same link aggregation group (LAG).
(Range: 0-65535)

DEFAULT SETTING

Actor: 1, Partner: 0

COMMAND MODE

Interface Configuration (Ethernet)

COMMAND USAGE

- Ports are only allowed to join the same LAG if (1) the LACP system priority matches, (2) the LACP port admin key matches, and (3) the LACP port channel key matches (if configured).
- If the port channel admin key (lacp admin key - Port Channel) is not set when a channel group is formed (i.e., it has the null value of 0), this key is set to the same value as the port admin key (**lacp admin key** - Ethernet Interface) used by the interfaces that joined the group.
- Once the remote side of a link has been established, LACP operational settings are already in use on that side. Configuring LACP settings for the partner only applies to its administrative state, not its operational state.

EXAMPLE

```
Console(config)#interface ethernet 1/5
Console(config-if)#lacp actor admin-key 120
Console(config-if)#
```

lacp port-priority

This command configures LACP port priority. Use the **no** form to restore the default setting.

SYNTAX

lacp {**actor** | **partner**} **port-priority** *priority*

no lacp {**actor** | **partner**} **port-priority**

actor - The local side an aggregate link.

partner - The remote side of an aggregate link.

priority - LACP port priority is used to select a backup link. (Range: 0-65535)

DEFAULT SETTING

32768

COMMAND MODE

Interface Configuration (Ethernet)

COMMAND USAGE

- Setting a lower value indicates a higher effective priority.

- If an active port link goes down, the backup port with the highest priority is selected to replace the downed link. However, if two or more ports have the same LACP port priority, the port with the lowest physical port number will be selected as the backup port.

- If an LAG already exists with the maximum number of allowed port members, and LACP is subsequently enabled on another port using a higher priority than an existing member, the newly configured port will replace an existing port member that has a lower priority.

- Once the remote side of a link has been established, LACP operational settings are already in use on that side. Configuring LACP settings for the partner only applies to its administrative state, not its operational state, and will only take effect the next time an aggregate link is established with the partner.

EXAMPLE

```
Console(config)#interface ethernet 1/5
Console(config-if)#lacp actor port-priority 128
```

lacp system-priority

This command configures a port's LACP system priority. Use the **no** form to restore the default setting.

SYNTAX

lacp {**actor** | **partner**} **system-priority** *priority*

no lacp {**actor** | **partner**} **system-priority**

actor - The local side an aggregate link.

partner - The remote side of an aggregate link.

priority - This priority is used to determine link aggregation group (LAG) membership, and to identify this device to other switches during LAG negotiations. (Range: 0-65535)

DEFAULT SETTING

32768

COMMAND MODE

Interface Configuration (Ethernet)

COMMAND USAGE

- Port must be configured with the same system priority to join the same LAG.
- System priority is combined with the switch’s MAC address to form the LAG identifier. This identifier is used to indicate a specific LAG during LACP negotiations with other systems.
- Once the remote side of a link has been established, LACP operational settings are already in use on that side. Configuring LACP settings for the partner only applies to its administrative state, not its operational state, and will only take effect the next time an aggregate link is established with the partner.

EXAMPLE

```
Console(config)#interface ethernet 1/5
Console(config-if)#lacp actor system-priority 3
Console(config-if)#
```

lacp admin-key (Port Channel)

This command configures a port channel's LACP administration key string. Use the **no** form to restore the default setting.

SYNTAX

lacp admin-key *key*

no lacp admin-key

key - The port channel admin key is used to identify a specific link aggregation group (LAG) during local LACP setup on this switch. (Range: 0-65535)

DEFAULT SETTING

0

COMMAND MODE

Interface Configuration (Port Channel)

COMMAND USAGE

- Ports are only allowed to join the same LAG if (1) the LACP system priority matches, (2) the LACP port admin key matches, and (3) the LACP port channel key matches (if configured).

- If the port channel admin key (**lacp admin key** - Port Channel) is not set when a channel group is formed (i.e., it has the null value of 0), this key is set to the same value as the port admin key (lacp admin key - Ethernet Interface) used by the interfaces that joined the group. Note that when the LAG is no longer used, the port channel admin key is reset to 0.

EXAMPLE

```
Console(config)#interface port-channel 1
Console(config-if)#lacp admin-key 3
Console(config-if)#
```

lacp timeout

This command configures the timeout to wait for the next LACP data unit (LACPDU). Use the no form to restore the default setting.

SYNTAX

lacp timeout {**long** | **short**}

no lacp timeout

long - Specifies a slow timeout of 90 seconds.

short - Specifies a fast timeout of 3 seconds.

DEFAULT SETTING

long

COMMAND MODE

Interface Configuration (Port Channel)

COMMAND USAGE

- The timeout configured by this command is set in the LACP timeout bit of the Actor State field in transmitted LACPDUs. When the partner switch receives an LACPDU set with a short timeout from the actor switch, the partner adjusts the transmit LACPDU interval to 1 second. When it receives an LACPDU set with a long timeout from the actor, it adjusts the transmit LACPDU interval to 30 seconds.

- If the actor does not receive an LACPDU from its partner before the configured timeout expires, the partner port information will be deleted from the LACP group.
- When a dynamic port-channel member leaves a port-channel, the default timeout value will be restored on that port.
- When a dynamic port-channel is torn down, the configured timeout value will be retained. When the dynamic port-channel is constructed again, that timeout value will be used.

EXAMPLE

```
Console(config)#interface port-channel 1
Console(config-if)#lacp timeout short
Console(config-if)#
```

Trunk Status Display Commands

show lacp

This command displays LACP information.

SYNTAX

show lacp [*port-channel*] {**counters** | **internal** | **neighbors** | **sys-id**}

port-channel - Local identifier for a link aggregation group. (Range: 1-8)

counters - Statistics for LACP protocol messages.

internal - Configuration settings and operational state for local side.

neighbors - Configuration settings and operational state for remote side.

sys-id - Summary of system priority and MAC address for all channel groups.

DEFAULT SETTING

Port Channel: all

COMMAND MODE

Privileged Exec

EXAMPLE

```
Console#show lacp 1 counters
Port Channel: 1
-------------------------------------------------------------------------
Eth 1/ 2
-------------------------------------------------------------------------
  LACPDUs Sent          : 12
  LACPDUs Received      : 6
  Marker Sent           : 0
  Marker Received       : 0
  LACPDUs Unknown Pkts : 0
  LACPDUs Illegal Pkts : 0
⋮
```

Table 136: show lacp counters - display description

Field	Description
LACPDUs Sent	Number of valid LACPDUs transmitted from this channel group.
LACPDUs Received	Number of valid LACPDUs received on this channel group.
Marker Sent	Number of valid Marker PDUs transmitted from this channel group.
Marker Received	Number of valid Marker PDUs received by this channel group.
LACPDUs Unknown Pkts	Number of frames received that either (1) Carry the Slow Protocols Ethernet Type value, but contain an unknown PDU, or (2) are addressed to the Slow Protocols group MAC Address, but do not carry the Slow Protocols Ethernet Type.
LACPDUs Illegal Pkts	Number of frames that carry the Slow Protocols Ethernet Type value, but contain a badly formed PDU or an illegal value of Protocol Subtype.

```
Console#show lacp 1 internal
Port Channel : 1
-------------------------------------------------------------------------
Oper Key  : 3
Admin Key : 0
Timeout   : long

Eth 1/ 1
-------------------------------------------------------------------------
  LACPDUs Internal      : 30 seconds
  LACP System Priority : 32768
  LACP Port Priority   : 32768
  Admin Key             : 3
  Oper Key              : 3
  Admin State           : defaulted, aggregation, long timeout, LACP-activity
  Oper State            : distributing, collecting, synchronization,
                          aggregation, long timeout, LACP-activity
⋮
```

Table 137: show lacp internal - display description

Field	Description
Oper Key	Current operational value of the key for the aggregation port.
Admin Key	Current administrative value of the key for the aggregation port.
LACPDUs Internal	Number of seconds before invalidating received LACPDU information.

Table 137: show lacp internal - display description (Continued)

Field	Description
LACP System Priority	LACP system priority assigned to this port channel.
LACP Port Priority	LACP port priority assigned to this interface within the channel group.
Admin State, Oper State	Administrative or operational values of the actor's state parameters: ◆ Expired – The actor's receive machine is in the expired state; ◆ Defaulted – The actor's receive machine is using defaulted operational partner information, administratively configured for the partner. ◆ Distributing – If false, distribution of outgoing frames on this link is disabled; i.e., distribution is currently disabled and is not expected to be enabled in the absence of administrative changes or changes in received protocol information. ◆ Collecting – Collection of incoming frames on this link is enabled; i.e., collection is currently enabled and is not expected to be disabled in the absence of administrative changes or changes in received protocol information. ◆ Synchronization – The System considers this link to be IN_SYNC; i.e., it has been allocated to the correct Link Aggregation Group, the group has been associated with a compatible Aggregator, and the identity of the Link Aggregation Group is consistent with the System ID and operational Key information transmitted. ◆ Aggregation – The system considers this link to be aggregatable; i.e., a potential candidate for aggregation. ◆ Long timeout – Periodic transmission of LACPDUs uses a slow transmission rate. ◆ LACP-Activity – Activity control value with regard to this link. (0: Passive; 1: Active)

```
Console#show lacp 1 neighbors
Port Channel 1 neighbors
-------------------------------------------------------------------------
Eth 1/ 1
-------------------------------------------------------------------------
  Partner Admin System ID   : 32768, 00-00-00-00-00-00
  Partner Oper System ID    : 32768, 00-12-CF-61-24-2F
  Partner Admin Port Number : 1
  Partner Oper Port Number  : 1
  Port Admin Priority       : 32768
  Port Oper Priority        : 32768
  Admin Key                 : 0
  Oper Key                  : 3
  Admin State:               defaulted, distributing, collecting,
                             synchronization, long timeout,
  Oper State:                distributing, collecting, synchronization,
                             aggregation, long timeout, LACP-activity
⋮
```

Table 138: show lacp neighbors - display description

Field	Description
Partner Admin System ID	LAG partner's system ID assigned by the user.
Partner Oper System ID	LAG partner's system ID assigned by the LACP protocol.
Partner Admin Port Number	Current administrative value of the port number for the protocol Partner.

Table 138: show lacp neighbors - display description (Continued)

Field	Description
Partner Oper Port Number	Operational port number assigned to this aggregation port by the port's protocol partner.
Port Admin Priority	Current administrative value of the port priority for the protocol partner.
Port Oper Priority	Priority value assigned to this aggregation port by the partner.
Admin Key	Current administrative value of the Key for the protocol partner.
Oper Key	Current operational value of the Key for the protocol partner.
Admin State	Administrative values of the partner's state parameters. (See preceding table.)
Oper State	Operational values of the partner's state parameters. (See preceding table.)

```
 Console#show lacp sysid
Port Channel     System Priority    System MAC Address
--------------------------------------------------------------------------
            1              32768     00-30-F1-8F-2C-A7
            2              32768     00-30-F1-8F-2C-A7
            3              32768     00-30-F1-8F-2C-A7
            4              32768     00-30-F1-8F-2C-A7
            5              32768     00-30-F1-8F-2C-A7
            6              32768     00-30-F1-8F-2C-A7
            7              32768     00-30-F1-D4-73-A0
            8              32768     00-30-F1-D4-73-A0
            9              32768     00-30-F1-D4-73-A0
           10              32768     00-30-F1-D4-73-A0
           11              32768     00-30-F1-D4-73-A0
           12              32768     00-30-F1-D4-73-A0
⋮
```

Table 139: show lacp sysid - display description

Field	Description
Channel group	A link aggregation group configured on this switch.
System Priority*	LACP system priority for this channel group.
System MAC Address*	System MAC address.

* The LACP system priority and system MAC address are concatenated to form the LAG system ID.

show port-channel load-balance

This command shows the load-distribution method used on aggregated links.

COMMAND MODE

Privileged Exec

EXAMPLE

```
Console#show port-channel load-balance
Trunk Load Balance Mode: Destination IP address
Console#
```

33 Port Mirroring Commands

Data can be mirrored from a local port on the same switch or from a remote port on another switch for analysis at the target port using software monitoring tools or a hardware probe. This switch supports the following mirroring modes.

Table 140: Port Mirroring Commands

Command	Function
Local Port Mirroring	Mirrors data to another port for analysis without affecting the data passing through or the performance of the monitored port
RSPAN Mirroring	Mirrors data from remote switches over a dedicated VLAN

Local Port Mirroring Commands

This section describes how to mirror traffic from a source port to a target port.

Table 141: Mirror Port Commands

Command	Function	Mode
port monitor	Configures a mirror session	IC
show port monitor	Shows the configuration for a mirror port	PE

port monitor

This command configures a mirror session. Use the **no** form to clear a mirror session.

Syntax

port monitor *interface* [**rx** | **tx** | **both**]

no port monitor *interface*

interface - **ethernet** *unit/port* (source port)

unit - Unit identifier. (Range: 1)

port - Port number. (Range: 1-28)

rx - Mirror received packets.

tx - Mirror transmitted packets.

both - Mirror both received and transmitted packets.

DEFAULT SETTING

- No mirror session is defined.
- When enabled for an interface, default mirroring is for both received and transmitted packets.

COMMAND MODE

Interface Configuration (Ethernet, destination port)

COMMAND USAGE

- You can mirror traffic from any source port to a destination port for real-time analysis. You can then attach a logic analyzer or RMON probe to the destination port and study the traffic crossing the source port in a completely unobtrusive manner.
- Set the destination port by specifying an Ethernet interface with the interface configuration command, and then use the **port monitor** command to specify the source of the traffic to mirror.
- When mirroring traffic from a port, the mirror port and monitor port speeds should match, otherwise traffic may be dropped from the monitor port. When mirroring traffic from a VLAN, traffic may also be dropped under heavy loads.
- Note that Spanning Tree BPDU packets are not mirrored to the target port.
- You can create multiple mirror sessions, but all sessions must share the same destination port.
- The destination port cannot be a trunk or trunk member port.

EXAMPLE

The following example configures the switch to mirror all packets from port 6 to 5:

```
Console(config)#interface ethernet 1/5
Console(config-if)#port monitor ethernet 1/6 both
Console(config-if)#
```

show port monitor

This command displays mirror information.

SYNTAX

show port monitor [*interface* | **vlan** *vlan-id* |
mac-address *mac-address*]

interface - **ethernet** *unit/port* (source port)

unit - Unit identifier. (Range: 1)

port - Port number. (Range: 1-28)

vlan-id - VLAN ID (Range: 1-4094)

mac-address - MAC address in the form of xx-xx-xx-xx-xx-xx or xxxxxxxxxxxx.

DEFAULT SETTING

Shows all sessions.

COMMAND MODE

Privileged Exec

COMMAND USAGE

This command displays the currently configured source port, destination port, and mirror mode (i.e., RX, TX, RX/TX).

EXAMPLE

The following shows mirroring configured from port 6 to port 5:

```
Console(config)#interface ethernet 1/5
Console(config-if)#port monitor ethernet 1/6
Console(config-if)#end
Console#show port monitor
Port Mirroring
-------------------------------------
 Destination Port (listen port):Eth1/5
 Source Port (monitored port)  :Eth1/6
 Mode                          :RX/TX
Console#
```

RSPAN MIRRORING COMMANDS

Remote Switched Port Analyzer (RSPAN) allows you to mirror traffic from remote switches for analysis on a local destination port.

Table 142: RSPAN Commands

Command	Function	Mode
vlan rspan	Creates a VLAN dedicated to carrying RSPAN traffic	VC
rspan source	Specifies the source port and traffic type to be mirrored	GC
rspan destination	Specifies the destination port to monitor the mirrored traffic	GC
rspan remote vlan	Specifies the RSPAN VLAN, switch role (source, intermediate or destination), and the uplink ports	GC
no rspan session	Deletes a configured RSPAN session	GC
show rspan	Displays the configuration settings for an RSPAN session	PE

Configuration Guidelines

Take the following steps to configure an RSPAN session:

1. Use the vlan rspan command to configure a VLAN to use for RSPAN. (Default VLAN 1 and switch cluster VLAN 4093 are prohibited.)

2. Use the rspan source command to specify the interfaces and the traffic type (RX, TX or both) to be monitored.

3. Use the rspan destination command to specify the destination port for the traffic mirrored by an RSPAN session.

4. Use the rspan remote vlan command to specify the VLAN to be used for an RSPAN session, to specify the switch's role as a source, intermediate relay, or destination of the mirrored traffic, and to configure the uplink ports designated to carry this traffic.

RSPAN Limitations

The following limitations apply to the use of RSPAN on this switch:

- *RSPAN Ports* – Only ports can be configured as an RSPAN source, destination, or uplink; static and dynamic trunks are not allowed. A port can only be configured as one type of RSPAN interface – source, destination, or uplink. Also, note that the source port and destination port cannot be configured on the same switch.

- *Local/Remote Mirror* – The destination of a local mirror session (created with the port monitor command) cannot be used as the destination for RSPAN traffic.

  Only two mirror sessions are allowed. Both sessions can be allocated to remote mirroring, unless local mirroring is enabled (which is limited to a single session).

- *Spanning Tree* – If the spanning tree is disabled, BPDUs will not be flooded onto the RSPAN VLAN.

  MAC address learning is not supported on RSPAN uplink ports when RSPAN is enabled on the switch. Therefore, even if spanning tree is enabled after RSPAN has been configured, MAC address learning will still not be re-started on the RSPAN uplink ports.

- *IEEE 802.1X* – RSPAN and 802.1X are mutually exclusive functions. When 802.1X is enabled globally, RSPAN uplink ports cannot be configured, even though RSPAN source and destination ports can still be configured. When RSPAN uplink ports are enabled on the switch, 802.1X cannot be enabled globally.

  RSPAN uplink ports cannot be configured to use IEEE 802.1X Port Authentication, but RSPAN source ports and destination ports can be configured to use it

- *Port Security* – If port security is enabled on any port, that port cannot be set as an RSPAN uplink port, even though it can still be configured as an RSPAN source or destination port. Also, when a port is configured as an RSPAN uplink port, port security cannot be enabled on that port.

rspan source

Use this command to specify the source port and traffic type to be mirrored remotely. Use the **no** form to disable RSPAN on the specified port, or with a traffic type keyword to disable mirroring for the specified type.

SYNTAX

[**no**] **rspan session** *session-id* **source interface** *interface-list* [**rx** | **tx** | **both**]

session-id – A number identifying this RSPAN session. (Range: 1-2)

Only two mirror sessions are allowed, including both local and remote mirroring. If local mirroring is enabled with the port monitor command, then there is only one session available for RSPAN.

interface-list – One or more source ports. Use a hyphen to indicate a consecutive list of ports or a comma between non-consecutive ports.

ethernet *unit*/*port*

unit - Unit identifier. (Range: 1)

port - Port number. (Range: 1-28)

rx - Mirror received packets.

tx - Mirror transmitted packets.

both - Mirror both received and transmitted packets.

DEFAULT SETTING

Both TX and RX traffic is mirrored

COMMAND MODE

Global Configuration

COMMAND USAGE

- One or more source ports can be assigned to the same RSPAN session, either on the same switch or on different switches.
- Only ports can be configured as an RSPAN source – static and dynamic trunks are not allowed.
- The source port and destination port cannot be configured on the same switch.

EXAMPLE

The following example configures the switch to mirror received packets from port 2 and 3:

```
Console(config)#rspan session 1 source interface ethernet 1/2
Console(config)#rspan session 1 source interface ethernet 1/3
Console(config)#
```

rspan destination

Use this command to specify the destination port to monitor the mirrored traffic. Use the **no** form to disable RSPAN on the specified port.

SYNTAX

rspan session *session-id* **destination interface** *interface* [**tagged** | **untagged**]

no rspan session *session-id* **destination interface** *interface*

session-id – A number identifying this RSPAN session. (Range: 1-2)

Only two mirror sessions are allowed, including both local and remote mirroring. If local mirroring is enabled with the port monitor command, then there is only one session available for RSPAN.

interface - **ethernet** *unit/port*

unit - Unit identifier. (Range: 1)

port - Port number. (Range: 1-28)

tagged - Traffic exiting the destination port carries the RSPAN VLAN tag.

untagged - Traffic exiting the destination port is untagged.

DEFAULT SETTING

Traffic exiting the destination port is untagged.

COMMAND MODE

Global Configuration

COMMAND USAGE

- Only one destination port can be configured on the same switch per session, but a destination port can be configured on more than one switch for the same session.

- Only ports can be configured as an RSPAN destination – static and dynamic trunks are not allowed.

- The source port and destination port cannot be configured on the same switch.

- A destination port can still send and receive switched traffic, and participate in any Layer 2 protocols to which it has been assigned.

EXAMPLE

The following example configures port 4 to receive mirrored RSPAN traffic:

```
Console(config)#rspan session 1 destination interface ethernet 1/2
Console(config)#
```

rspan remote vlan

Use this command to specify the RSPAN VLAN, switch role (source, intermediate or destination), and the uplink ports. Use the **no** form to disable the RSPAN on the specified VLAN.

SYNTAX

[**no**] **rspan session** *session-id* **remote vlan** *vlan-id*
{**source** | **intermediate** | **destination**} **uplink** *interface*

session-id – A number identifying this RSPAN session. (Range: 1-2)

Only two mirror sessions are allowed, including both local and remote mirroring. If local mirroring is enabled with the port monitor command, then there is only one session available for RSPAN.

vlan-id - ID of configured RSPAN VLAN. (Range: 2-4092)
Use the vlan rspan command to reserve a VLAN for RSPAN mirroring before enabling RSPAN with this command.

source - Specifies this device as the source of remotely mirrored traffic.

intermediate - Specifies this device as an intermediate switch, transparently passing mirrored traffic from one or more sources to one or more destinations.

destination - Specifies this device as a switch configured with a destination port which is to receive mirrored traffic for this session.

uplink - A port configured to receive or transmit remotely mirrored traffic.

interface - **ethernet** *unit/port*

ethernet *unit/port*

unit - Unit identifier. (Range: 1)

port - Port number. (Range: 1-28)

DEFAULT SETTING

None

COMMAND MODE

Global Configuration

COMMAND USAGE

- Only 802.1Q trunk or hybrid (i.e., general use) ports can be configured as an RSPAN uplink port – access ports are not allowed (see switchport mode).

- Only one uplink port can be configured on a source switch, but there is no limitation on the number of uplink ports configured on an intermediate or destination switch.

- Only destination and uplink ports will be assigned by the switch as members of this VLAN. Ports cannot be manually assigned to an RSPAN VLAN with the switchport allowed vlan command. Nor can GVRP dynamically add port members to an RSPAN VLAN. Also, note that the show vlan command will not display any members for an RSPAN VLAN, but will only show configured RSPAN VLAN identifiers.

EXAMPLE

The following example enables RSPAN on VLAN 2, specifies this device as an RSPAN destination switch, and the uplink interface as port 3:

```
Console(config)#rspan session 1 remote vlan 2 destination uplink ethernet 1/3
Console(config)#
```

no rspan session

Use this command to delete a configured RSPAN session.

SYNTAX

no rspan session *session-id*

session-id – A number identifying this RSPAN session. (Range: 1-2)

Only two mirror sessions are allowed, including both local and remote mirroring. If local mirroring is enabled with the port monitor command, then there is only one session available for RSPAN.

COMMAND MODE

Global Configuration

COMMAND USAGE

The **no rspan session** command must be used to disable an RSPAN VLAN before it can be deleted from the VLAN database (see the vlan command).

EXAMPLE

```
Console(config)#no rspan session 1
Console(config)#
```

show rspan

Use this command to displays the configuration settings for an RSPAN session.

SYNTAX

show rspan session [*session-id*]

session-id – A number identifying this RSPAN session. (Range: 1-2)

Only two mirror sessions are allowed, including both local and remote mirroring. If local mirroring is enabled with the port monitor command, then there is only one session available for RSPAN.

COMMAND MODE

Privileged Exec

EXAMPLE

```
Console#show rspan session
RSPAN Session ID                  : 1
Source Ports (mirrored ports)     : None
  RX Only                         : None
  TX Only                         : None
  BOTH                            : None
Destination Port (monitor port) : Eth 1/2
Destination Tagged Mode           : Untagged
Switch Role                       : Destination
RSPAN VLAN                        : 2
RSPAN Uplink Ports                : Eth 1/3
Operation Status                  : Up
Console#
```

34 Congestion Control Commands

The switch can set the maximum upload or download data transfer rate for any port. It can control traffic storms by setting a maximum threshold for broadcast traffic or multicast traffic. It can also set bounding thresholds for broadcast and multicast storms which can be used to automatically trigger rate limits or to shut down a port.

Table 143: Congestion Control Commands

Command Group	Function
Rate Limiting	Sets the input and output rate limits for a port.
Storm Control	Sets the traffic storm threshold for each port.
Automatic Traffic Control	Sets thresholds for broadcast and multicast storms which can be used to trigger configured rate limits or to shut down a port.

Rate Limit Commands

Rate limit commands allow the network manager to control the maximum rate for traffic transmitted or received on an interface. Rate limiting is configured on interfaces at the edge of a network to limit traffic into or out of the network. Packets that exceed the acceptable amount of traffic are dropped.

Rate limiting can be applied to individual ports or trunks. When an interface is configured with this feature, the traffic rate will be monitored by the hardware to verify conformity. Non-conforming traffic is dropped.

Table 144: Rate Limit Commands

Command	Function	Mode
rate-limit	Configures the maximum input or output rate for an interface	IC

rate-limit

This command defines the rate limit for a specific interface. Use this command without specifying a rate to restore the default rate. Use the **no** form to restore the default status of disabled.

SYNTAX

rate-limit {**input** | **output**} [*rate*]

no rate-limit {**input** | **output**}

input – Input rate for specified interface

output – Output rate for specified interface

rate – Maximum value in Kbps.
(Range: 64 - 1,000,000 Kbits per second for Gigabit Ethernet ports;
64 - 10,000,000 Kbits per second for 10G Ethernet ports)

DEFAULT SETTING

Disabled

COMMAND MODE

Interface Configuration (Ethernet, Port Channel)

COMMAND USAGE

Using both rate limiting and storm control on the same interface may lead to unexpected results. It is therefore not advisable to use both of these commands on the same interface.

EXAMPLE

```
Console(config)#interface ethernet 1/1
Console(config-if)#rate-limit input 64
Console(config-if)#
```

RELATED COMMAND

show interfaces switchport (1203)

STORM CONTROL COMMANDS

Storm control commands can be used to configure broadcast, multicast, and unknown unicast storm control thresholds. Traffic storms may occur when a device on your network is malfunctioning, or if application programs are not well designed or properly configured. If there is too much traffic on your network, performance can be severely degraded or everything can come to complete halt.

You can protect your network from traffic storms by setting a threshold for broadcast, multicast or unknown unicast traffic. Any packets exceeding the specified threshold will then be dropped.

Table 145: Rate Limit Commands

Command	Function	Mode
switchport packet-rate*	Configures broadcast, multicast, and unknown unicast storm control thresholds	IC
switchport block	Prevents flooding of broadcast, unknown multicast, or unknown unicast packets	IC
show interfaces switchport	Displays the administrative and operational status of an interface	NE, PE

* Enabling hardware-level storm control with this command on a port will disable software-level automatic storm control on the same port if configured by the auto-traffic-control command.

switchport packet-rate

This command configures broadcast, multicast and unknown unicast storm control. Use the **no** form to restore the default setting.

SYNTAX

switchport {**broadcast** | **multicast** | **unicast**} **packet-rate** *rate*

no switchport {**broadcast** | **multicast** | **unicast**}

broadcast - Specifies storm control for broadcast traffic.

multicast - Specifies storm control for multicast traffic.

unicast - Specifies storm control for unknown unicast traffic.

rate - Threshold level as a rate; i.e., kilobits per second.
(Range: 500-14880000 pps)

DEFAULT SETTING

Broadcast Storm Control: Enabled, 500 pps
Multicast Storm Control: Disabled
Unknown Unicast Storm Control: Disabled

COMMAND MODE

Interface Configuration (Ethernet, Port Channel)

COMMAND USAGE

- When traffic exceeds the threshold specified for broadcast and multicast or unknown unicast traffic, packets exceeding the threshold are dropped until the rate falls back down beneath the threshold.
- Traffic storms can be controlled at the hardware level using this command or at the software level using the auto-traffic-control command. However, only one of these control types can be applied to a port. Enabling hardware-level storm control on a port will disable automatic storm control on that port.
- The rate limits set by this command are also used by automatic storm control when the control response is set to rate limiting by the auto-traffic-control action command.
- Using both rate limiting and storm control on the same interface may lead to unexpected results. It is therefore not advisable to use both of these commands on the same interface.

EXAMPLE

The following shows how to configure broadcast storm control at 600 packets per second:

```
Console(config)#interface ethernet 1/5
Console(config-if)#switchport broadcast packet-rate 600
Console(config-if)#
```

switchport block

This command prevents the flooding of broadcast, unknown multicast, or unknown unicast packets onto an interface. Use the **no** form to restore the default setting.

SYNTAX

[**no**] **switchport block** {**broadcast** | **multicast** | **unicast**}

broadcast - Specifies broadcast packets.

multicast - Specifies unknown multicast packets.

unicast - Specifies unknown unicast packets.

COMMAND MODE

Interface Configuration (Ethernet, Port Channel)

DEFAULT SETTING

Disabled

COMMAND USAGE

By default, broadcast, unknown multicast, and unknown unicast traffic is flooded to all ports. This occurs if a MAC address has been timed out or not yet learned by the switch. If this kind of traffic is flooded to an isolated port on a private VLAN, there could be security issues.

EXAMPLE

The following example blocks unknown multicast traffic on port 5:

```
Console(config)#interface ethernet 1/5
Console(config-if)#switchport switchport block multicast
Console(config-if)#
```

AUTOMATIC TRAFFIC CONTROL COMMANDS

Automatic Traffic Control (ATC) configures bounding thresholds for broadcast and multicast storms which can be used to trigger configured rate limits or to shut down a port.

Table 146: ATC Commands

Command	Function	Mode
Threshold Commands		
auto-traffic-control apply-timer	Sets the time at which to apply the control response after ingress traffic has exceeded the upper threshold	GC
auto-traffic-control release-timer	Sets the time at which to release the control response after ingress traffic has fallen beneath the lower threshold	GC
auto-traffic-control*	Enables automatic traffic control for broadcast or multicast storms	IC (Port)
auto-traffic-control action	Sets the control action to limit ingress traffic or shut down the offending port	IC (Port)
auto-traffic-control alarm-clear-threshold	Sets the lower threshold for ingress traffic beneath which a cleared storm control trap is sent	IC (Port)
auto-traffic-control alarm-fire-threshold	Sets the upper threshold for ingress traffic beyond which a storm control response is triggered after the apply timer expires	IC (Port)
auto-traffic-control auto-control-release	Automatically releases a control response	IC (Port)
auto-traffic-control control-release	Manually releases a control response	IC (Port)
SNMP Trap Commands		
snmp-server enable port-traps atc broadcast-alarm-clear	Sends a trap when broadcast traffic falls beneath the lower threshold after a storm control response has been triggered	IC (Port)
snmp-server enable port-traps atc broadcast-alarm-fire	Sends a trap when broadcast traffic exceeds the upper threshold for automatic storm control	IC (Port)
snmp-server enable port-traps atc broadcast-control-apply	Sends a trap when broadcast traffic exceeds the upper threshold for automatic storm control and the apply timer expires	IC (Port)
snmp-server enable port-traps atc broadcast-control-release	Sends a trap when broadcast traffic falls beneath the lower threshold after a storm control response has been triggered and the release timer expires	IC (Port)

Table 146: ATC Commands (Continued)

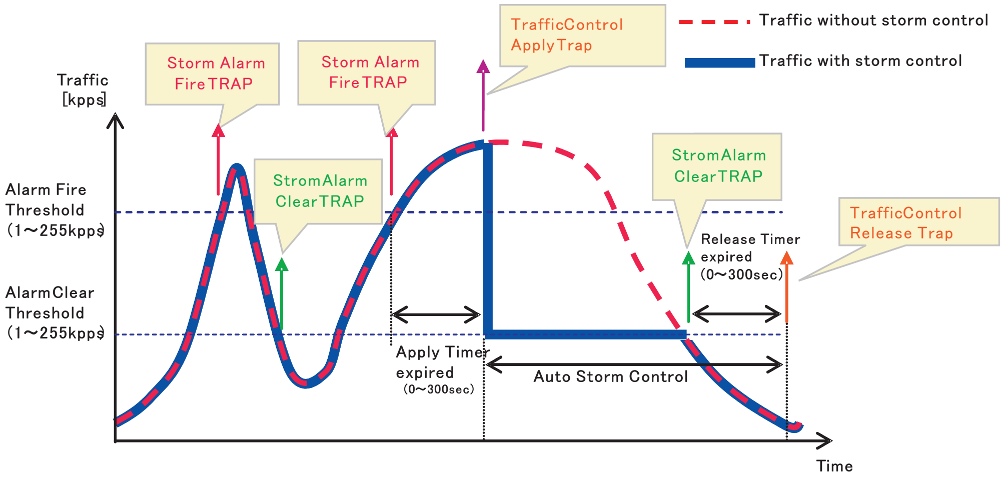
Command	Function	Mode
snmp-server enable port-traps atc multicast-alarm-clear	Sends a trap when multicast traffic falls beneath the lower threshold after a storm control response has been triggered	IC (Port)
snmp-server enable port-traps atc multicast-alarm-fire	Sends a trap when multicast traffic exceeds the upper threshold for automatic storm control	IC (Port)
snmp-server enable port-traps atc multicast-control-apply	Sends a trap when multicast traffic exceeds the upper threshold for automatic storm control and the apply timer expires	IC (Port)
snmp-server enable port-traps atc multicast-control-release	Sends a trap when multicast traffic falls beneath the lower threshold after a storm control response has been triggered and the release timer expires	IC (Port)
ATC Display Commands		
show auto-traffic-control	Shows global configuration settings for automatic storm control	PE
show auto-traffic-control interface	Shows interface configuration settings and storm control status for the specified port	PE

* Enabling automatic storm control on a port will disable hardware-level storm control on the same port if configured by the switchport packet-rate command.

USAGE GUIDELINES

ATC includes storm control for broadcast or multicast traffic. The control response for either of these traffic types is the same, as shown in the following diagrams.

Figure 548: Storm Control by Limiting the Traffic Rate


TrafficControl Apply Trap
Traffic without storm control
Traffic with storm control
Storm Alarm Fire TRAP
Storm Alarm Fire TRAP
Traffic [kpps]
Alarm Fire Threshold (1～255kpps)
StromAlarm ClearTRAP
StromAlarm ClearTRAP
TrafficControl Release Trap
Release Timer expired (0～300sec)
AlarmClear Threshold (1～255kpps)
Apply Timer expired (0～300sec)
Auto Storm Control
Time

The key elements of this diagram are described below:

- ◆ Alarm Fire Threshold – The highest acceptable traffic rate. When ingress traffic exceeds the threshold, ATC sends a Storm Alarm Fire Trap and logs it.

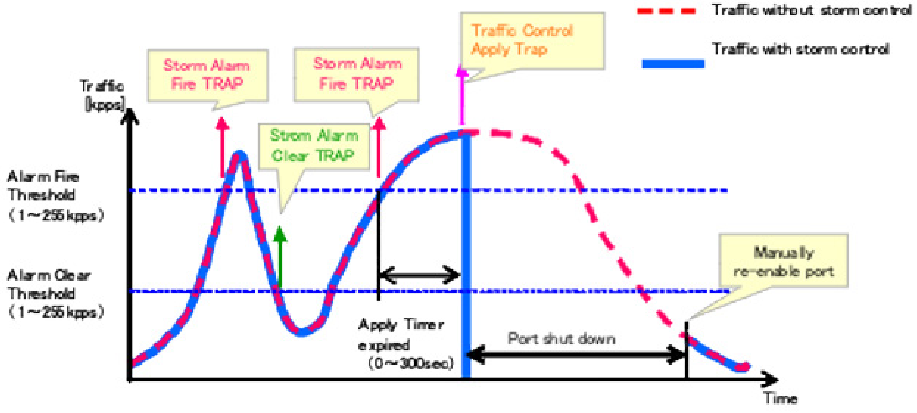
- When traffic exceeds the alarm fire threshold and the apply timer expires, a traffic control response is applied, and a Traffic Control Apply Trap is sent and logged.

- Alarm Clear Threshold – The lower threshold beneath which a control response can be automatically terminated after the release timer expires. When ingress traffic falls below this threshold, ATC sends a Storm Alarm Clear Trap and logs it.

- When traffic falls below the alarm clear threshold after the release timer expires, traffic control (for rate limiting) will be stopped and a Traffic Control Release Trap sent and logged. Note that if the control action has shut down a port, it can only be manually re-enabled using the auto-traffic-control control-release command).

- The traffic control response of rate limiting can be released automatically or manually. The control response of shutting down a port can only be released manually.

Figure 549: Storm Control by Shutting Down a Port



The key elements of this diagram are the same as that described in the preceding diagram, except that automatic release of the control response is not provided. When traffic control is applied, you must manually re-enable the port.

FUNCTIONAL LIMITATIONS

Automatic storm control is a software level control function. Traffic storms can also be controlled at the hardware level using the switchport packet-rate command. However, only one of these control types can be applied to a port. Enabling automatic storm control on a port will disable hardware-level storm control on that port.

Threshold Commands

auto-traffic-control apply-timer

This command sets the time at which to apply the control response after ingress traffic has exceeded the upper threshold. Use the **no** form to restore the default setting.

SYNTAX

auto-traffic-control {**broadcast** | **multicast**} **apply-timer** *seconds*

no auto-traffic-control {**broadcast** | **multicast**} **apply-timer**

broadcast - Specifies automatic storm control for broadcast traffic.

multicast - Specifies automatic storm control for multicast traffic.

seconds - The interval after the upper threshold has been exceeded at which to apply the control response. (Range: 1-300 seconds)

DEFAULT SETTING

300 seconds

COMMAND MODE

Global Configuration

COMMAND USAGE

After the apply timer expires, a control action may be triggered as specified by the auto-traffic-control action command and a trap message sent as specified by the snmp-server enable port-traps atc broadcast-control-apply command or snmp-server enable port-traps atc multicast-control-apply command.

EXAMPLE

This example sets the apply timer to 200 seconds for all ports.

```
Console(config)#auto-traffic-control broadcast apply-timer 200
Console(config)#
```

auto-traffic-control release-timer

This command sets the time at which to release the control response after ingress traffic has fallen beneath the lower threshold. Use the **no** form to restore the default setting.

SYNTAX

auto-traffic-control {**broadcast** | **multicast**} **release-timer** *seconds*

no auto-traffic-control {**broadcast** | **multicast**} **release-timer**

broadcast - Specifies automatic storm control for broadcast traffic.

multicast - Specifies automatic storm control for multicast traffic.

seconds - The time at which to release the control response after ingress traffic has fallen beneath the lower threshold. (Range: 1-900 seconds)

DEFAULT SETTING

900 seconds

COMMAND MODE

Global Configuration

COMMAND USAGE

This command sets the delay after which the control response can be terminated. The auto-traffic-control auto-control-release command must be used to enable or disable the automatic release of a control response of rate-limiting. To re-enable a port which has been shut down by automatic traffic control, you must manually re-enable the port using the auto-traffic-control control-release command.

EXAMPLE

This example sets the release timer to 800 seconds for all ports.

```
Console(config)#auto-traffic-control broadcast release-timer 800
Console(config)#
```

auto-traffic-control

This command enables automatic traffic control for broadcast or multicast storms. Use the **no** form to disable this feature.

SYNTAX

[**no**] **auto-traffic-control** {**broadcast** | **multicast**}

broadcast - Specifies automatic storm control for broadcast traffic.

multicast - Specifies automatic storm control for multicast traffic.

DEFAULT SETTING

Disabled

COMMAND MODE

Interface Configuration (Ethernet)

COMMAND USAGE

- Automatic storm control can be enabled for either broadcast or multicast traffic. It cannot be enabled for both of these traffic types at the same time.

- Automatic storm control is a software level control function. Traffic storms can also be controlled at the hardware level using the switchport packet-rate command. However, only one of these control types can be applied to a port. Enabling automatic storm control on a port will disable hardware-level storm control on that port.

EXAMPLE

This example enables automatic storm control for broadcast traffic on port 1.

```
Console(config)#interface ethernet 1/1
Console(config-if)#auto-traffic-control broadcast
Console(config-if)#
```

auto-traffic-control action

This command sets the control action to limit ingress traffic or shut down the offending port. Use the **no** form to restore the default setting.

SYNTAX

auto-traffic-control {**broadcast** | **multicast**} **action** {**rate-control** | **shutdown**}

no auto-traffic-control {**broadcast** | **multicast**} **action**

broadcast - Specifies automatic storm control for broadcast traffic.

multicast - Specifies automatic storm control for multicast traffic.

rate-control - If a control response is triggered, the rate of ingress traffic is limited based on the threshold configured by the auto-traffic-control alarm-clear-threshold command.

shutdown - If a control response is triggered, the port is administratively disabled. A port disabled by automatic traffic control can only be manually re-enabled.

DEFAULT SETTING

rate-control

COMMAND MODE

Interface Configuration (Ethernet)

COMMAND USAGE

- When the upper threshold is exceeded and the apply timer expires, a control response will be triggered based on this command.

- When the control response is set to rate limiting by this command, the rate limits are determined by the auto-traffic-control alarm-clear-threshold command.

- If the control response is to limit the rate of ingress traffic, it can be automatically terminated once the traffic rate has fallen beneath the lower threshold and the release timer has expired.

- If a port has been shut down by a control response, it will not be re-enabled by automatic traffic control. It can only be manually re-enabled using the auto-traffic-control control-release command.

EXAMPLE

This example sets the control response for broadcast traffic on port 1.

```
Console(config)#interface ethernet 1/1
Console(config-if)#auto-traffic-control broadcast action shutdown
Console(config-if)#
```

auto-traffic-control alarm-clear-threshold

This command sets the lower threshold for ingress traffic beneath which a control response for rate limiting will be released after the Release Timer expires, if so configured by the auto-traffic-control auto-control-release command. Use the **no** form to restore the default setting.

SYNTAX

auto-traffic-control {**broadcast** | **multicast**} **alarm-clear-threshold** *threshold*

no auto-traffic-control {**broadcast** | **multicast**} **alarm-clear-threshold**

broadcast - Specifies automatic storm control for broadcast traffic.

multicast - Specifies automatic storm control for multicast traffic.

threshold - The lower threshold for ingress traffic beneath which a cleared storm control trap is sent. (Range: 1-255 kilo-packets per second)

DEFAULT SETTING

128 kilo-packets per second

COMMAND MODE

Interface Configuration (Ethernet)

COMMAND USAGE

- Once the traffic rate falls beneath the lower threshold, a trap message may be sent if configured by the snmp-server enable port-traps atc broadcast-alarm-clear command or snmp-server enable port-traps atc multicast-alarm-clear command.

- If rate limiting has been configured as a control response, it will be discontinued after the traffic rate has fallen beneath the lower threshold, and the release timer has expired. Note that if a port has been shut down by a control response, it will not be re-enabled by automatic traffic control. It can only be manually re-enabled using the auto-traffic-control control-release command.

EXAMPLE

This example sets the clear threshold for automatic storm control for broadcast traffic on port 1.

```
Console(config)#interface ethernet 1/1
Console(config-if)#auto-traffic-control broadcast alarm-clear-threshold 155
Console(config-if)#
```

auto-traffic-control alarm-fire-threshold

This command sets the upper threshold for ingress traffic beyond which a storm control response is triggered after the apply timer expires. Use the **no** form to restore the default setting.

SYNTAX

auto-traffic-control {**broadcast** | **multicast**} **alarm-fire-threshold** *threshold*

no auto-traffic-control {**broadcast** | **multicast**} **alarm-fire-threshold**

broadcast - Specifies automatic storm control for broadcast traffic.

multicast - Specifies automatic storm control for multicast traffic.

threshold - The upper threshold for ingress traffic beyond which a storm control response is triggered after the apply timer expires. (Range: 1-255 kilo-packets per second)

DEFAULT SETTING

128 kilo-packets per second

COMMAND MODE

Interface Configuration (Ethernet)

COMMAND USAGE

- Once the upper threshold is exceeded, a trap message may be sent if configured by the snmp-server enable port-traps atc broadcast-alarm-fire command or snmp-server enable port-traps atc multicast-alarm-fire command.

- After the upper threshold is exceeded, the control timer must first expire as configured by the auto-traffic-control apply-timer command before a control response is triggered if configured by the auto-traffic-control action command.

EXAMPLE

This example sets the trigger threshold for automatic storm control for broadcast traffic on port 1.

```
Console(config)#interface ethernet 1/1
Console(config-if)#auto-traffic-control broadcast alarm-fire-threshold 255
Console(config-if)#
```

auto-traffic-control auto-control-release

This command automatically releases a control response of rate-limiting after the time specified in the auto-traffic-control release-timer command has expired.

SYNTAX

auto-traffic-control {**broadcast** | **multicast**} **auto-control-release**

broadcast - Specifies automatic storm control for broadcast traffic.

multicast - Specifies automatic storm control for multicast traffic.

COMMAND MODE

Interface Configuration (Ethernet)

COMMAND USAGE

- This command can be used to automatically stop a control response of rate-limiting after the specified action has been triggered and the release timer has expired.
- To release a control response which has shut down a port after the specified action has been triggered and the release timer has expired, use the auto-traffic-control control-release command.

EXAMPLE

```
Console(config)#interface ethernet 1/1
Console(config-if)#auto-traffic-control broadcast auto-control-release
Console(config-if)#
```

auto-traffic-control control-release

This command manually releases a control response.

SYNTAX

auto-traffic-control {**broadcast** | **multicast**} **control-release**

broadcast - Specifies automatic storm control for broadcast traffic.

multicast - Specifies automatic storm control for multicast traffic.

COMMAND MODE

Interface Configuration (Ethernet)

COMMAND USAGE

This command can be used to manually stop a control response of rate-limiting or port shutdown any time after the specified action has been triggered.

EXAMPLE

```
Console(config)#interface ethernet 1/1
Console(config-if)#auto-traffic-control broadcast control-release
Console#(config-if)
```

SNMP Trap Commands

snmp-server enable port-traps atc broadcast-alarm-clear

This command sends a trap when broadcast traffic falls beneath the lower threshold after a storm control response has been triggered. Use the **no** form to disable this trap.

SYNTAX

[**no**] **snmp-server enable port-traps atc broadcast-alarm-clear**

DEFAULT SETTING

Disabled

COMMAND MODE

Interface Configuration (Ethernet)

EXAMPLE

```
Console(config)#interface ethernet 1/1
Console(config-if)#snmp-server enable port-traps atc broadcast-alarm-clear
Console(config-if)#
```

RELATED COMMANDS

auto-traffic-control action (1248)
auto-traffic-control alarm-clear-threshold (1249)

snmp-server enable port-traps atc broadcast-alarm-fire

This command sends a trap when broadcast traffic exceeds the upper threshold for automatic storm control. Use the **no** form to disable this trap.

SYNTAX

[**no**] **snmp-server enable port-traps atc broadcast-alarm-fire**

DEFAULT SETTING

Disabled

COMMAND MODE

Interface Configuration (Ethernet)

EXAMPLE

```
Console(config)#interface ethernet 1/1
Console(config-if)#snmp-server enable port-traps atc broadcast-alarm-fire
Console(config-if)#
```

RELATED COMMANDS

auto-traffic-control alarm-fire-threshold (1250)

snmp-server enable port-traps atc broadcast-control-apply

This command sends a trap when broadcast traffic exceeds the upper threshold for automatic storm control and the apply timer expires. Use the **no** form to disable this trap.

SYNTAX

[**no**] **snmp-server enable port-traps atc broadcast-control-apply**

DEFAULT SETTING

Disabled

COMMAND MODE

Interface Configuration (Ethernet)

EXAMPLE

```
Console(config)#interface ethernet 1/1
Console(config-if)#snmp-server enable port-traps atc broadcast-control-apply
Console(config-if)#
```

RELATED COMMANDS

auto-traffic-control alarm-fire-threshold (1250)
auto-traffic-control apply-timer (1246)

snmp-server enable port-traps atc broadcast-control-release

This command sends a trap when broadcast traffic falls beneath the lower threshold after a storm control response has been triggered and the release timer expires. Use the **no** form to disable this trap.

SYNTAX

[**no**] **snmp-server enable port-traps atc broadcast-control-release**

DEFAULT SETTING

Disabled

COMMAND MODE

Interface Configuration (Ethernet)

EXAMPLE

```
Console(config)#interface ethernet 1/1
Console(config-if)#snmp-server enable port-traps atc broadcast-control-
  release
Console(config-if)#
```

RELATED COMMANDS

auto-traffic-control alarm-clear-threshold (1249)
auto-traffic-control action (1248)
auto-traffic-control release-timer (1246)

snmp-server enable port-traps atc multicast-alarm-clear

This command sends a trap when multicast traffic falls beneath the lower threshold after a storm control response has been triggered. Use the **no** form to disable this trap.

SYNTAX

[**no**] **snmp-server enable port-traps atc multicast-alarm-clear**

DEFAULT SETTING

Disabled

COMMAND MODE

Interface Configuration (Ethernet)

EXAMPLE

```
Console(config)#interface ethernet 1/1
Console(config-if)#snmp-server enable port-traps atc multicast-alarm-clear
Console(config-if)#
```

RELATED COMMANDS

auto-traffic-control action (1248)
auto-traffic-control alarm-clear-threshold (1249)

snmp-server enable port-traps atc multicast-alarm-fire

This command sends a trap when multicast traffic exceeds the upper threshold for automatic storm control. Use the **no** form to disable this trap.

SYNTAX

[**no**] **snmp-server enable port-traps atc multicast-alarm-fire**

DEFAULT SETTING

Disabled

COMMAND MODE

Interface Configuration (Ethernet)

EXAMPLE

```
Console(config)#interface ethernet 1/1
Console(config-if)#snmp-server enable port-traps atc multicast-alarm-fire
Console(config-if)#
```

RELATED COMMANDS

auto-traffic-control alarm-fire-threshold (1250)

snmp-server enable port-traps atc multicast-control-apply

This command sends a trap when multicast traffic exceeds the upper threshold for automatic storm control and the apply timer expires. Use the **no** form to disable this trap.

SYNTAX

[**no**] **snmp-server enable port-traps atc multicast-control-apply**

DEFAULT SETTING

Disabled

COMMAND MODE

Interface Configuration (Ethernet)

EXAMPLE

```
Console(config)#interface ethernet 1/1
Console(config-if)#snmp-server enable port-traps atc multicast-control-apply
Console(config-if)#
```

RELATED COMMANDS

auto-traffic-control alarm-fire-threshold (1250)
auto-traffic-control apply-timer (1246)

snmp-server enable port-traps atc multicast-control-release

This command sends a trap when multicast traffic falls beneath the lower threshold after a storm control response has been triggered and the release timer expires. Use the **no** form to disable this trap.

SYNTAX

[**no**] **snmp-server enable port-traps atc multicast-control-release**

DEFAULT SETTING

Disabled

COMMAND MODE

Interface Configuration (Ethernet)

EXAMPLE

```
Console(config)#interface ethernet 1/1
Console(config-if)#snmp-server enable port-traps atc multicast-control-
  release
Console(config-if)#
```

RELATED COMMANDS

auto-traffic-control alarm-clear-threshold (1249)
auto-traffic-control action (1248)
auto-traffic-control release-timer (1246)

ATC Display Commands

show auto-traffic-control

This command shows global configuration settings for automatic storm control.

COMMAND MODE

Privileged Exec

EXAMPLE

```
Console#show auto-traffic-control

Storm-control: Broadcast
 Apply-timer (sec)    : 300
 release-timer (sec) : 900

Storm-control: Multicast
 Apply-timer(sec)     : 300
 release-timer(sec)   : 900
Console#
```

show auto-traffic-control interface

This command shows interface configuration settings and storm control status for the specified port.

SYNTAX

show auto-traffic-control interface [*interface*]

interface

ethernet *unit*/*port*

unit - Unit identifier. (Range: 1)

port - Port number. (Range: 1-28)

COMMAND MODE

Privileged Exec

EXAMPLE

```
Console#show auto-traffic-control interface ethernet 1/1
Eth 1/1 Information
------------------------------------------------------------------------
Storm Control:              Broadcast                    Multicast
State:                      Disabled                     Disabled
Action:                     rate-control                 rate-control
Auto Release Control:       Disabled                     Disabled
Alarm Fire Threshold(Kpps): 128                          128
Alarm Clear Threshold(Kpps):128                          128
Trap Storm Fire:            Disabled                     Disabled
Trap Storm Clear:           Disabled                     Disabled
Trap Traffic Apply:         Disabled                     Disabled
Trap Traffic Release:       Disabled                     Disabled

Console#
```

35 Loopback Detection Commands

The switch can be configured to detect general loopback conditions caused by hardware problems or faulty protocol settings. When enabled, a control frame is transmitted on the participating ports, and the switch monitors inbound traffic to see if the frame is looped back.

Table 147: Loopback Detection Commands

Command	Function	Mode
loopback-detection	Enables loopback detection globally on the switch or on a specified interface	GC, IC
loopback-detection action	Specifies the response to take for a detected loopback condition	GC
loopback-detection recover-time	Specifies the interval to wait before releasing an interface from shutdown state	GC
loopback-detection transmit-interval	Specifies the interval at which to transmit loopback detection control frames	GC
loopback detection trap	Configures the switch to send a trap when a loopback condition is detected or the switch recover from a loopback	GC
loopback-detection release	Manually releases all interfaces currently shut down by the loopback detection feature	PE
show loopback-detection	Shows loopback detection configuration settings for the switch or for a specified interface	PE

Usage Guidelines

- The default settings for the control frame transmit interval and recover time may be adjusted to improve performance for your specific environment. The shutdown mode may also need to be changed once you determine what kind of packets are being looped back.

- General loopback detection provided by the command described in this section and loopback detection provided by the spanning tree protocol cannot both be enabled at the same time. If loopback detection is enabled for the spanning tree protocol, general loopback detection cannot be enabled on the same interface.

- When a loopback event is detected on an interface or when an interface is released from a shutdown state caused by a loopback event, a trap message is sent and the event recorded in the system log.

- Loopback detection must be enabled both globally and on an interface for loopback detection to take effect.

loopback-detection

This command enables loopback detection globally on the switch or on a specified interface. Use the **no** form to disable loopback detection.

SYNTAX

[**no**] **loopback-detection**

DEFAULT SETTING

Disabled

COMMAND MODE

Global Configuration
Interface Configuration (Ethernet, Port Channel)

COMMAND USAGE

Loopback detection must be enabled globally for the switch by this command and enabled for a specific interface for this function to take effect.

EXAMPLE

This example enables general loopback detection on the switch, disables loopback detection provided for the spanning tree protocol on port 1, and then enables general loopback detection for that port.

```
Console(config)#loopback-detection
Console(config)#interface ethernet 1/1
Console(config-if)#no spanning-tree loopback-detection
Console(config-if)#loopback-detection
Console(config)#
```

loopback-detection action

This command specifies the protective action the switch takes when a loopback condition is detected. Use the no form to restore the default setting. Use the **no** form to restore the default setting.

SYNTAX

loopback-detection action {**block** | **none** | **shutdown**}

no loopback-detection action

block - When a loopback is detected on a port which a member of a specific VLAN, packets belonging to that VLAN are dropped at the offending port.

none - No action is taken.

shutdown - Shuts down the interface.

DEFAULT SETTING

Shut down

COMMAND MODE

Global Configuration

COMMAND USAGE

- When the response to a detected loopback condition is set to block user traffic, loopback detection control frames may untagged or tagged depending on the port's VLAN membership type.
- When the response to a detected loopback condition is set to block user traffic, ingress filtering for the port is enabled automatically if not already enabled by the switchport ingress-filtering command. The port's original setting for ingress filtering will be restored when loopback detection is disabled.
- Use the loopback-detection recover-time command to set the time to wait before re-enabling an interface shut down by the loopback detection process.
- When the loopback detection response is changed, any ports placed in shutdown state by the loopback detection process will be immediately restored to operation regardless of the remaining recover time.

EXAMPLE

This example sets the loopback detection mode to block user traffic.

```
Console(config)#loopback-detection action block
Console(config)#
```

loopback-detection recover-time

This command specifies the interval to wait before the switch automatically releases an interface from shutdown state. Use the **no** form to restore the default setting.

SYNTAX

loopback-detection recover-time *seconds*

no loopback-detection recover-time

seconds - Recovery time from shutdown state.
(Range: 60-1,000,000 seconds, or 0 to disable automatic recovery)

DEFAULT SETTING

60 seconds

COMMAND MODE

Global Configuration

COMMAND USAGE

- When the loopback detection mode is changed, any ports placed in shutdown state by the loopback detection process will be immediately restored to operation regardless of the remaining recover time.
- If the recovery time is set to zero, all ports placed in shutdown state can be restored to operation using the loopback-detection release command. To restore a specific port, use the no shutdown command.

EXAMPLE

```
Console(config)#loopback-detection recover-time 120
Console(config-if)#
```

loopback-detection transmit-interval

This command specifies the interval at which to transmit loopback detection control frames. Use the **no** form to restore the default setting.

SYNTAX

loopback-detection transmit-interval *seconds*

no loopback-detection transmit-interval

seconds - The transmission interval for loopback detection control frames. (Range: 1-32767 seconds)

DEFAULT SETTING

10 seconds

COMMAND MODE

Global Configuration

EXAMPLE

```
Console(config)#loopback-detection transmit-interval 60
Console(config)#
```

loopback detection trap

This command sends a trap when a loopback condition is detected, or when the switch recovers from a loopback condition. Use the no form to restore the default state.

SYNTAX

loopback-detection trap [**both** | **detect** | **none** | **recover**]

no loopback-detection trap

both - Sends an SNMP trap message when a loopback condition is detected, or when the switch recovers from a loopback condition.

detect - Sends an SNMP trap message when a loopback condition is detected.

none - Does not send an SNMP trap for loopback detection or recovery.

recover - Sends an SNMP trap message when the switch recovers from a loopback condition.

DEFAULT SETTING

None

COMMAND MODE

Global Configuration

COMMAND USAGE

Refer to the loopback-detection recover-time command for information on conditions which constitute loopback recovery.

EXAMPLE

```
Console(config)#loopback-detection trap both
Console(config)#
```

loopback-detection release

This command releases all interfaces currently shut down by the loopback detection feature.

SYNTAX

loopback-detection release

COMMAND MODE

Privileged Exec

EXAMPLE

```
Console#loopback-detection release
Console(config)#
```

show loopback-detection

This command shows loopback detection configuration settings for the switch or for a specified interface.

SYNTAX

show loopback-detection [*interface*]

interface

ethernet *unit*/*port*

unit - Unit identifier. (Range: 1)

port - Port number. (Range: 1-28)

COMMAND MODE

Privileged Exec

EXAMPLE

```
Console#show loopback-detection
Loopback Detection Global Information
 Global Status     : Enabled
 Transmit Interval : 10
 Recover Time      : 60
 Action            : Shutdown
 Trap              : None
Loopback Detection Port Information
 Port      Admin State  Oper State
 --------  -----------  ----------
 Eth 1/ 1  Enabled      Normal
 Eth 1/ 2  Disabled     Disabled
 Eth 1/ 3  Disabled     Disabled
:
Console#show loopback-detection ethernet 1/1
Loopback Detection Information of Eth 1/1
 Admin State : Enabled
 Oper State  : Normal
 Looped VLAN : None
Console#
```

36 UniDirectional Link Detection Commands

The switch can be configured to detect and disable unidirectional Ethernet fiber or copper links. When enabled, the protocol advertises a port's identity and learns about its neighbors on a specific LAN segment; and stores information about its neighbors in a cache. It can also send out a train of echo messages under circumstances that require fast notifications or re-synchronization of the cached information.

Table 148: UniDirectional Link Detection Commands

Command	Function	Mode
udld message-interval	Configures the message interval between UDLD probe messages	GC
udld aggressive	Sets UDLD to aggressive mode on an interface	IC
udld port	Enables UDLD on an interface	IC
show udld	Shows UDLD configuration settings and operational status	PE

udld message-interval

This command configures the message interval between UDLD probe messages for ports in advertisement phase and determined to be bidirectional. Use the **no** form to restore the default setting.

Syntax

udld message-interval *message-interval*

no message-interval

message-interval – The interval at which a port sends UDLD probe messages after linkup or detection phases. (Range: 7-90 seconds)

Default Setting

15 seconds

Command Mode

Global Configuration

Command Usage

During the detection phase, messages are exchanged at the maximum rate of one per second. After that, if the protocol reaches a stable state and determines that the link is bidirectional, the message interval is increased to a configurable value based on a curve known as M1(t), a time-based function described in RFC 5171.

If the link is deemed anything other than bidirectional at the end of the detection phase, this curve becomes a flat line with a fixed value of Mfast (7 seconds).

If the link is instead deemed bidirectional, the curve will use Mfast for the first four subsequent message transmissions and then transition to an Mslow value for all other steady-state transmissions. Mslow is the value configured by this command.

EXAMPLE

This example sets the message interval to 10 seconds.

```
Console(config)#udld message-interval 10
Console(config)#
```

udld aggressive

This command sets UDLD to aggressive mode on an interface. Use the **no** form to restore the default setting.

SYNTAX

[**no**] **udld aggressive**

DEFAULT SETTING

Disabled

COMMAND MODE

Interface Configuration (Ethernet Port)

COMMAND USAGE

UDLD can function in two modes: normal mode and aggressive mode.

- In normal mode, determination of link status at the end of the detection process is always based on information received in UDLD messages: whether that’s information about the exchange of proper neighbor identification or the absence of such. Hence, albeit bound by a timer, normal mode determinations are always based on gleaned information, and as such are “event-based.” If no such information can be obtained (e.g., because of a bidirectional loss of connectivity), UDLD follows a conservative approach minimize false positives during the detection process and deems a port to be in “undetermined” state. In other words, normal mode will shut down a port only if it can explicitly determine that the associated link is faulty for an extended period of time.

- In aggressive mode, UDLD will also shut down a port if it loses bidirectional connectivity with the neighbor for the same extended period of time (as that mentioned above for normal mode) and subsequently fails repeated last-resort attempts to re-establish communication with the other end of the link. This mode of operation assumes that loss of communication with the neighbor is a meaningful network event in itself, and a symptom of a serious connectivity problem. Because this type of detection can be event-less, and lack of information cannot always be associated to an actual malfunction of the link, this mode is optional and is recommended only in certain scenarios (typically only on point-to-point links where no communication failure between two neighbors is admissible).

EXAMPLE

This example enables UDLD aggressive mode on port 1.

```
Console(config)#interface ethernet 1/1
Console(config-if)#udld aggressive
Console(config-if)#
```

udld port

This command enables UDLD on an interface. Use the **no** form to disable UDLD on an interface.

SYNTAX

[**no**] **udld port**

DEFAULT SETTING

Disabled

COMMAND MODE

Interface Configuration (Ethernet Port)

COMMAND USAGE

- UDLD requires that all the devices connected to the same LAN segment be running the protocol in order for a potential mis-configuration to be detected and for prompt corrective action to be taken.

- Whenever a UDLD device learns about a new neighbor or receives a re-synchronization request from an out-of-synch neighbor, it (re)starts the detection process on its side of the connection and sends N echo messages in reply. (This mechanism implicitly assumes that N packets are sufficient to get through a link and reach the other end, even though some of them might get dropped during the transmission.)

  Since this behavior must be the same on all the neighbors, the sender of the echoes expects to receive an echo in reply. If the detection process ends without the proper echo information being received, the link is considered to be unidirectional.

EXAMPLE

```
Console(config)#interface ethernet 1/1
Console(config-if)#udld port
Console(config-if)#
```

show udld

This command shows UDLD configuration settings and operational status for the switch or for a specified interface.

SYNTAX

show udld [**interface** *interface*]

interface

ethernet *unit*/*port*

unit - Unit identifier. (Range: 1)

port - Port number. (Range: 1-28)

COMMAND MODE

Privileged Exec

EXAMPLE

```
Console#show udld
Message Interval : 15

Interface UDLD     Mode       Oper State                            Msg Invl
                              Port State                            Timeout
--------- -------- ---------- ------------------------------------- --------
Eth 1/ 1  Enabled  Aggressive Advertisement                             15 s
                              Bidirectional                              5 s
Eth 1/ 2  Disabled Normal     Disabled                                   7 s
                              Unknown                                    5 s
Eth 1/ 3  Disabled Normal     Disabled                                   7 s
                              Unknown                                    5 s
Eth 1/ 4  Disabled Normal     Disabled                                   7 s
                              Unknown                                    5 s
Eth 1/ 5  Disabled Normal     Disabled                                   7 s
                              Unknown                                    5 s
⋮
Console#show udld interface ethernet 1/1
Interface UDLD     Mode       Oper State                            Msg Invl
                              Port State                            Timeout
--------- -------- ---------- ------------------------------------- --------
Eth 1/ 1  Enabled  Aggressive Advertisement                             15 s
                              Bidirectional                              5 s
Console#
```

Table 149: show udld - display description

Field	Description
Message Interval	The interval between UDLD probe messages for ports in advertisement phase
UDLD	Shows if UDLD is enabled or disabled on a port
Mode	Shows if UDLD is functioning in Normal or Aggressive mode
Oper State	Shows the UDLD operational state (Disabled, Link down, Link up, Advertisement, Detection, Disabled port, Advertisement - Single neighbor, Advertisement - Multiple neighbors)

Table 149: show udld - display description (Continued)

Field	Description
Port State	Shows the UDLD port state (Unknown, Bidirectional, Unidirectional, Transmit-to-receive loop, Mismatch with neighbor state reported, Neighbor's echo is empty) The state is Unknown if the link is down or not connected to a UDLD-capable device. The state is Bidirectional if the link has a normal two-way connection to a UDLD-capable device. All other states indicate mis-wiring.
Msg Invl	The interval between UDLD probe messages used for the indicated operational state
Timeout	The time that UDLD waits for echoes from a neighbor device during the detection window

37 Address Table Commands

These commands are used to configure the address table for filtering specified addresses, displaying current entries, clearing the table, or setting the aging time.

Table 150: Address Table Commands

Command	Function	Mode
mac-address-table aging-time	Sets the aging time of the address table	GC
mac-address-table static	Maps a static address to a port in a VLAN	GC
clear mac-address-table dynamic	Removes any learned entries from the forwarding database	PE
show mac-address-table	Displays entries in the bridge-forwarding database	PE
show mac-address-table aging-time	Shows the aging time for the address table	PE
show mac-address-table count	Shows the number of MAC addresses used and the number of available MAC addresses	PE

mac-address-table aging-time

This command sets the aging time for entries in the address table. Use the **no** form to restore the default aging time.

Syntax

mac-address-table aging-time *seconds*

no mac-address-table aging-time

seconds - Aging time. (Range: 10-1000000 seconds; 0 to disable aging)

Default Setting

300 seconds

Command Mode

Global Configuration

Command Usage

The aging time is used to age out dynamically learned forwarding information.

EXAMPLE

```
Console(config)#mac-address-table aging-time 100
Console(config)#
```

mac-address-table static

This command maps a static address to a destination port in a VLAN. Use the **no** form to remove an address.

SYNTAX

mac-address-table static *mac-address* **interface** *interface*
vlan *vlan-id* [*action*]

no mac-address-table static *mac-address* **vlan** *vlan-id*

mac-address - MAC address.

interface

ethernet *unit/port*

unit - Unit identifier. (Range: 1)

port - Port number. (Range: 1-28)

port-channel *channel-id* (Range: 1-8)

vlan-id - VLAN ID (Range: 1-4094)

action -

delete-on-reset - Assignment lasts until the switch is reset.

permanent - Assignment is permanent.

DEFAULT SETTING

No static addresses are defined. The default mode is **permanent**.

COMMAND MODE

Global Configuration

COMMAND USAGE

The static address for a host device can be assigned to a specific port within a specific VLAN. Use this command to add static addresses to the MAC Address Table. Static addresses have the following characteristics:

- Static addresses will not be removed from the address table when a given interface link is down.

- Static addresses are bound to the assigned interface and will not be moved. When a static address is seen on another interface, the address will be ignored and will not be written to the address table.

- A static address cannot be learned on another port until the address is removed with the **no** form of this command.

EXAMPLE

```
Console(config)#mac-address-table static 00-e0-29-94-34-de interface ethernet
  1/1 vlan 1 delete-on-reset
Console(config)#
```

clear mac-address-table dynamic

This command removes any learned entries from the forwarding database.

DEFAULT SETTING

None

COMMAND MODE

Privileged Exec

EXAMPLE

```
Console#clear mac-address-table dynamic
Console#
```

show mac-address-table

This command shows classes of entries in the bridge-forwarding database.

SYNTAX

show mac-address-table [**address** *mac-address* [*mask*]]
[**interface** *interface*] [**vlan** *vlan-id*]
[**sort** {**address** | **vlan** | **interface**}]

mac-address - MAC address.

mask - Bits to match in the address.

interface

ethernet *unit/port*

unit - Unit identifier. (Range: 1)

port - Port number. (Range: 1-28)

port-channel *channel-id* (Range: 1-8)

vlan-id - VLAN ID (Range: 1-4094)

sort - Sort by address, vlan or interface.

DEFAULT SETTING

None

COMMAND MODE

Privileged Exec

COMMAND USAGE

- The MAC Address Table contains the MAC addresses associated with each interface. Note that the Type field may include the following types:
  - Learn - Dynamic address entries
  - Config - Static entry
- The mask should be hexadecimal numbers (representing an equivalent bit mask) in the form xx-xx-xx-xx-xx-xx that is applied to the specified MAC address. Enter hexadecimal numbers, where an equivalent binary bit “0” means to match a bit and “1” means to ignore a bit. For example, a mask of 00-00-00-00-00-00 means an exact match, and a mask of FF-FF-FF-FF-FF-FF means “any.”
- The maximum number of address entries is 16K.

EXAMPLE

```
Console#show mac-address-table
 Interface MAC Address       VLAN Type     Life Time
 --------- ----------------- ---- -------- -----------------
  CPU      00-00-0C-00-00-FD    1 CPU      Delete on Reset
  Eth 1/ 1 00-E0-29-94-34-DE    1 Config   Delete on Reset
  Eth 1/21 00-01-EC-F8-D8-D9    1 Learn    Delete on Timeout
Console#
```

show mac-address-table aging-time

This command shows the aging time for entries in the address table.

DEFAULT SETTING

None

COMMAND MODE

Privileged Exec

EXAMPLE

```
Console#show mac-address-table aging-time
 Aging Status : Enabled
 Aging Time: 300 sec.
Console#
```

show mac-address-table count

This command shows the number of MAC addresses used and the number of available MAC addresses for the overall system or for an interface.

SYNTAX

show mac-address-table count [**interface** *interface*]

interface

ethernet *unit*/*port*

unit - Unit identifier. (Range: 1)

port - Port number. (Range: 1-28)

port-channel *channel-id* (Range: 1-8)

DEFAULT SETTING

None

COMMAND MODE

Privileged Exec

EXAMPLE

```
Console#show mac-address-table count interface ethernet 1/1

MAC Entries for Eth 1/1
Total Address Count       :3
Static Address Count      :0
Dynamic Address Count     :3

Console#show mac-address-table count

Compute the number of MAC Address...

Maximum number of MAC Address which can be created in the system:
Total Number of MAC Address       : 32768
Number of Static MAC Address      : 1024

Current number of entries which have been created in the system:
Total Number of MAC Address       : 6
Number of Static MAC Address      : 1
Number of Dynamic MAC Address     : 5

Console#
```

38 Spanning Tree Commands

This section includes commands that configure the Spanning Tree Algorithm (STA) globally for the switch, and commands that configure STA for the selected interface.

Table 151: Spanning Tree Commands

Command	Function	Mode
spanning-tree	Enables the spanning tree protocol	GC
spanning-tree forward-time	Configures the spanning tree bridge forward time	GC
spanning-tree hello-time	Configures the spanning tree bridge hello time	GC
spanning-tree max-age	Configures the spanning tree bridge maximum age	GC
spanning-tree mode	Configures STP, RSTP or MSTP mode	GC
spanning-tree pathcost method	Configures the path cost method for RSTP/MSTP	GC
spanning-tree priority	Configures the spanning tree bridge priority	GC
spanning-tree mst configuration	Changes to MSTP configuration mode	GC
spanning-tree system-bpdu-flooding	Floods BPDUs to all other ports or just to all other ports in the same VLAN when global spanning tree is disabled	GC
spanning-tree transmission-limit	Configures the transmission limit for RSTP/MSTP	GC
max-hops	Configures the maximum number of hops allowed in the region before a BPDU is discarded	MST
mst priority	Configures the priority of a spanning tree instance	MST
mst vlan	Adds VLANs to a spanning tree instance	MST
name	Configures the name for the multiple spanning tree	MST
revision	Configures the revision number for the multiple spanning tree	MST
spanning-tree bpdu-filter	Filters BPDUs for edge ports	IC
spanning-tree bpdu-guard	Shuts down an edge port if it receives a BPDU	IC
spanning-tree cost	Configures the spanning tree path cost of an interface	IC
spanning-tree edge-port	Enables fast forwarding for edge ports	IC
spanning-tree link-type	Configures the link type for RSTP/MSTP	IC
spanning-tree loopback-detection	Enables BPDU loopback detection for a port	IC
spanning-tree loopback-detection action	Configures the response for loopback detection to block user traffic or shut down the interface	IC
spanning-tree loopback-detection release-mode	Configures loopback release mode for a port	IC

Table 151: Spanning Tree Commands (Continued)

Command	Function	Mode
spanning-tree loopback-detection trap	Enables BPDU loopback SNMP trap notification for a port	IC
spanning-tree mst cost	Configures the path cost of an instance in the MST	IC
spanning-tree mst port-priority	Configures the priority of an instance in the MST	IC
spanning-tree port-bpdu-flooding	Floods BPDUs to other ports when global spanning tree is disabled	IC
spanning-tree port-priority	Configures the spanning tree priority of an interface	IC
spanning-tree root-guard	Prevents a designated port from passing superior BPDUs	IC
spanning-tree spanning-disabled	Disables spanning tree for an interface	IC
spanning-tree tc-prop-stop	Stops propagation of topology change information	IC
spanning-tree loopback-detection release	Manually releases a port placed in discarding state by loopback-detection	PE
spanning-tree protocol-migration	Re-checks the appropriate BPDU format	PE
show spanning-tree	Shows spanning tree configuration for the common spanning tree (i.e., overall bridge), a selected interface, or an instance within the multiple spanning tree	PE
show spanning-tree mst configuration	Shows the multiple spanning tree configuration	PE

spanning-tree

This command enables the Spanning Tree Algorithm globally for the switch. Use the **no** form to disable it.

SYNTAX

[**no**] **spanning-tree**

DEFAULT SETTING

Spanning tree is enabled.

COMMAND MODE

Global Configuration

COMMAND USAGE

The Spanning Tree Algorithm (STA) can be used to detect and disable network loops, and to provide backup links between switches, bridges or routers. This allows the switch to interact with other bridging devices (that is, an STA-compliant switch, bridge or router) in your network to ensure that only one route exists between any two stations on the network, and provide backup links which automatically take over when a primary link goes down.

EXAMPLE

This example shows how to enable the Spanning Tree Algorithm for the switch:

```
Console(config)#spanning-tree
Console(config)#
```

spanning-tree forward-time

This command configures the spanning tree bridge forward time globally for this switch. Use the **no** form to restore the default.

SYNTAX

spanning-tree forward-time *seconds*

no spanning-tree forward-time

seconds - Time in seconds. (Range: 4 - 30 seconds)
The minimum value is the higher of 4 or [(max-age / 2) + 1].

DEFAULT SETTING

15 seconds

COMMAND MODE

Global Configuration

COMMAND USAGE

This command sets the maximum time (in seconds) a port will wait before changing states (i.e., discarding to learning to forwarding). This delay is required because every device must receive information about topology changes before it starts to forward frames. In addition, each port needs time to listen for conflicting information that would make it return to the discarding state; otherwise, temporary data loops might result.

EXAMPLE

```
Console(config)#spanning-tree forward-time 20
Console(config)#
```

spanning-tree hello-time

This command configures the spanning tree bridge hello time globally for this switch. Use the **no** form to restore the default.

SYNTAX

spanning-tree hello-time *time*

no spanning-tree hello-time

time - Time in seconds. (Range: 1-10 seconds).
The maximum value is the lower of 10 or [(max-age / 2) - 1].

DEFAULT SETTING

2 seconds

COMMAND MODE

Global Configuration

COMMAND USAGE

This command sets the time interval (in seconds) at which the root device transmits a configuration message.

EXAMPLE

```
Console(config)#spanning-tree hello-time 5
Console(config)#
```

RELATED COMMANDS

spanning-tree forward-time (1279)
spanning-tree max-age (1280)

spanning-tree max-age

This command configures the spanning tree bridge maximum age globally for this switch. Use the **no** form to restore the default.

SYNTAX

spanning-tree max-age *seconds*

no spanning-tree max-age

seconds - Time in seconds. (Range: 6-40 seconds)
The minimum value is the higher of 6 or [2 x (hello-time + 1)].
The maximum value is the lower of 40 or [2 x (forward-time - 1)].

DEFAULT SETTING

20 seconds

COMMAND MODE

Global Configuration

COMMAND USAGE

This command sets the maximum time (in seconds) a device can wait without receiving a configuration message before attempting to reconfigure. All device ports (except for designated ports) should receive configuration messages at regular intervals. Any port that ages out STA information (provided in the last configuration message) becomes the designated port for the attached LAN. If it is a root port, a new root port is selected from among the device ports attached to the network.

EXAMPLE

```
Console(config)#spanning-tree max-age 40
Console(config)#
```

RELATED COMMANDS

spanning-tree forward-time (1279)
spanning-tree hello-time (1279)

spanning-tree mode

This command selects the spanning tree mode for this switch. Use the **no** form to restore the default.

SYNTAX

spanning-tree mode {**stp** | **rstp** | **mstp**}

no spanning-tree mode

stp - Spanning Tree Protocol (IEEE 802.1D)

rstp - Rapid Spanning Tree Protocol (IEEE 802.1w)

mstp - Multiple Spanning Tree (IEEE 802.1s)

DEFAULT SETTING

rstp

COMMAND MODE

Global Configuration

COMMAND USAGE

- Spanning Tree Protocol
  This option uses RSTP set to STP forced compatibility mode. It uses RSTP for the internal state machine, but sends only 802.1D BPDUs. This creates one spanning tree instance for the entire network. If multiple VLANs are implemented on a network, the path between specific VLAN members may be inadvertently disabled to prevent network loops, thus isolating group members. When operating multiple VLANs, we recommend selecting the MSTP option.

- Rapid Spanning Tree Protocol
  RSTP supports connections to either STP or RSTP nodes by monitoring the incoming protocol messages and dynamically adjusting the type of protocol messages the RSTP node transmits, as described below:

  - STP Mode – If the switch receives an 802.1D BPDU after a port’s migration delay timer expires, the switch assumes it is connected to an 802.1D bridge and starts using only 802.1D BPDUs.

  - RSTP Mode – If RSTP is using 802.1D BPDUs on a port and receives an RSTP BPDU after the migration delay expires, RSTP restarts the migration delay timer and begins using RSTP BPDUs on that port.

- Multiple Spanning Tree Protocol

  - To allow multiple spanning trees to operate over the network, you must configure a related set of bridges with the same MSTP configuration, allowing them to participate in a specific set of spanning tree instances.

- A spanning tree instance can exist only on bridges that have compatible VLAN instance assignments.
- Be careful when switching between spanning tree modes. Changing modes stops all spanning-tree instances for the previous mode and restarts the system in the new mode, temporarily disrupting user traffic.

EXAMPLE

The following example configures the switch to use Rapid Spanning Tree:

```
Console(config)#spanning-tree mode rstp
Console(config)#
```

spanning-tree pathcost method

This command configures the path cost method used for Rapid Spanning Tree and Multiple Spanning Tree. Use the **no** form to restore the default.

SYNTAX

spanning-tree pathcost method {**long** | **short**}

no spanning-tree pathcost method

long - Specifies 32-bit based values that range from 1-200,000,000. This method is based on the IEEE 802.1w Rapid Spanning Tree Protocol.

short - Specifies 16-bit based values that range from 1-65535. This method is based on the IEEE 802.1 Spanning Tree Protocol.

DEFAULT SETTING

Long method

COMMAND MODE

Global Configuration

COMMAND USAGE

- The path cost method is used to determine the best path between devices. Therefore, lower values should be assigned to ports attached to faster media, and higher values assigned to ports with slower media. Note that path cost (page 1290) takes precedence over port priority (page 1298).
- The path cost methods apply to all spanning tree modes (STP, RSTP and MSTP). Specifically, the long method can be applied to STP since this mode is supported by a backward compatible mode of RSTP.

EXAMPLE

```
Console(config)#spanning-tree pathcost method long
Console(config)#
```

spanning-tree priority

This command configures the spanning tree priority globally for this switch. Use the **no** form to restore the default.

SYNTAX

spanning-tree priority *priority*

no spanning-tree priority

priority - Priority of the bridge. (Range – 0-61440, in steps of 4096; Options: 0, 4096, 8192, 12288, 16384, 20480, 24576, 28672, 32768, 36864, 40960, 45056, 49152, 53248, 57344, 61440)

DEFAULT SETTING

32768

COMMAND MODE

Global Configuration

COMMAND USAGE

Bridge priority is used in selecting the root device, root port, and designated port. The device with the highest priority (i.e., lower numeric value) becomes the STA root device. However, if all devices have the same priority, the device with the lowest MAC address will then become the root device.

EXAMPLE

```
Console(config)#spanning-tree priority 40000
Console(config)#
```

spanning-tree mst configuration

This command changes to Multiple Spanning Tree (MST) configuration mode.

DEFAULT SETTING

No VLANs are mapped to any MST instance.
The region name is set the switch’s MAC address.

COMMAND MODE

Global Configuration

EXAMPLE

```
Console(config)#spanning-tree mst configuration
Console(config-mstp)#
```

RELATED COMMANDS

mst vlan (1286)
mst priority (1286)
name (1287)

revision (1288)
max-hops (1285)

spanning-tree system-bpdu-flooding

This command configures the system to flood BPDUs to all other ports on the switch or just to all other ports in the same VLAN when spanning tree is disabled globally on the switch or disabled on a specific port. Use the **no** form to restore the default.

SYNTAX

spanning-tree system-bpdu-flooding {**to-all** | **to-vlan**}

no spanning-tree system-bpdu-flooding

to-all - Floods BPDUs to all other ports on the switch.

to-vlan - Floods BPDUs to all other ports within the receiving port's native VLAN (i.e., as determined by port's PVID).

DEFAULT SETTING

Floods to all other ports in the same VLAN.

COMMAND MODE

Global Configuration

COMMAND USAGE

The **spanning-tree system-bpdu-flooding** command has no effect if BPDU flooding is disabled on a port (see the spanning-tree port-bpdu-flooding command).

EXAMPLE

```
Console(config)#spanning-tree system-bpdu-flooding
Console(config)#
```

spanning-tree transmission-limit

This command configures the minimum interval between the transmission of consecutive RSTP/MSTP BPDUs. Use the **no** form to restore the default.

SYNTAX

spanning-tree transmission-limit *count*

no spanning-tree transmission-limit

count - The transmission limit in seconds. (Range: 1-10)

DEFAULT SETTING

3

COMMAND MODE

Global Configuration

COMMAND USAGE

This command limits the maximum transmission rate for BPDUs.

EXAMPLE

```
Console(config)#spanning-tree transmission-limit 4
Console(config)#
```

max-hops

This command configures the maximum number of hops in the region before a BPDU is discarded. Use the **no** form to restore the default.

SYNTAX

max-hops *hop-number*

hop-number - Maximum hop number for multiple spanning tree. (Range: 1-40)

DEFAULT SETTING

20

COMMAND MODE

MST Configuration

COMMAND USAGE

An MSTI region is treated as a single node by the STP and RSTP protocols. Therefore, the message age for BPDUs inside an MSTI region is never changed. However, each spanning tree instance within a region, and the internal spanning tree (IST) that connects these instances use a hop count to specify the maximum number of bridges that will propagate a BPDU. Each bridge decrements the hop count by one before passing on the BPDU. When the hop count reaches zero, the message is dropped.

EXAMPLE

```
Console(config-mstp)#max-hops 30
Console(config-mstp)#
```

mst priority

This command configures the priority of a spanning tree instance. Use the **no** form to restore the default.

SYNTAX

mst *instance-id* **priority** *priority*

no mst *instance-id* **priority**

instance-id - Instance identifier of the spanning tree. (Range: 0-4094)

priority - Priority of the a spanning tree instance. (Range: 0-61440 in steps of 4096; Options: 0, 4096, 8192, 12288, 16384, 20480, 24576, 28672, 32768, 36864, 40960, 45056, 49152, 53248, 57344, 61440)

DEFAULT SETTING

32768

COMMAND MODE

MST Configuration

COMMAND USAGE

- MST priority is used in selecting the root bridge and alternate bridge of the specified instance. The device with the highest priority (i.e., lowest numerical value) becomes the MSTI root device. However, if all devices have the same priority, the device with the lowest MAC address will then become the root device.
- You can set this switch to act as the MSTI root device by specifying a priority of 0, or as the MSTI alternate device by specifying a priority of 16384.

EXAMPLE

```
Console(config-mstp)#mst 1 priority 4096
Console(config-mstp)#
```

mst vlan

This command adds VLANs to a spanning tree instance. Use the **no** form to remove the specified VLANs. Using the **no** form without any VLAN parameters to remove all VLANs.

SYNTAX

[**no**] **mst** *instance-id* **vlan** *vlan-range*

instance-id - Instance identifier of the spanning tree. (Range: 0-4094)

vlan-range - Range of VLANs. (Range: 1-4094)

DEFAULT SETTING

none

COMMAND MODE

MST Configuration

COMMAND USAGE

- Use this command to group VLANs into spanning tree instances. MSTP generates a unique spanning tree for each instance. This provides multiple pathways across the network, thereby balancing the traffic load, preventing wide-scale disruption when a bridge node in a single instance fails, and allowing for faster convergence of a new topology for the failed instance.

- By default all VLANs are assigned to the Internal Spanning Tree (MSTI 0) that connects all bridges and LANs within the MST region. This switch supports up to 32 instances. You should try to group VLANs which cover the same general area of your network. However, remember that you must configure all bridges within the same MSTI Region (page 1287) with the same set of instances, and the same instance (on each bridge) with the same set of VLANs. Also, note that RSTP treats each MSTI region as a single node, connecting all regions to the Common Spanning Tree.

EXAMPLE

```
Console(config-mstp)#mst 1 vlan 2-5
Console(config-mstp)#
```

name

This command configures the name for the multiple spanning tree region in which this switch is located. Use the **no** form to clear the name.

SYNTAX

name *name*

name - Name of the spanning tree.

DEFAULT SETTING

Switch’s MAC address

COMMAND MODE

MST Configuration

COMMAND USAGE

The MST region name and revision number (page 1288) are used to designate a unique MST region. A bridge (i.e., spanning-tree compliant device such as this switch) can only belong to one MST region. And all bridges in the same region must be configured with the same MST instances.

EXAMPLE

```
Console(config-mstp)#name R&D
Console(config-mstp)#
```

RELATED COMMANDS

revision (1288)

revision

This command configures the revision number for this multiple spanning tree configuration of this switch. Use the **no** form to restore the default.

SYNTAX

revision *number*

number - Revision number of the spanning tree. (Range: 0-65535)

DEFAULT SETTING

0

COMMAND MODE

MST Configuration

COMMAND USAGE

The MST region name (page 1287) and revision number are used to designate a unique MST region. A bridge (i.e., spanning-tree compliant device such as this switch) can only belong to one MST region. And all bridges in the same region must be configured with the same MST instances.

EXAMPLE

```
Console(config-mstp)#revision 1
Console(config-mstp)#
```

RELATED COMMANDS

name (1287)

spanning-tree bpdu-filter

This command filters all BPDUs received on an edge port. Use the **no** form to disable this feature.

SYNTAX

[**no**] **spanning-tree bpdu-filter**

DEFAULT SETTING

Disabled

COMMAND MODE

Interface Configuration (Ethernet, Port Channel)

COMMAND USAGE

- This command filters all Bridge Protocol Data Units (BPDUs) received on an interface to save CPU processing time. This function is designed to work in conjunction with edge ports which should only connect end stations to the switch, and therefore do not need to process BPDUs. However, note that if a trunking port connected to another switch or bridging device is mistakenly configured as an edge port, and BPDU filtering is enabled on this port, this might cause a loop in the spanning tree.

- Before enabling BPDU Filter, the interface must first be configured as an edge port with the spanning-tree edge-port command.

EXAMPLE

```
Console(config)#interface ethernet 1/5
Console(config-if)#spanning-tree edge-port
Console(config-if)#spanning-tree bpdu-filter
Console(config-if)#
```

RELATED COMMANDS

spanning-tree edge-port (1291)

spanning-tree bpdu-guard

This command shuts down an edge port (i.e., an interface set for fast forwarding) if it receives a BPDU. Use the **no** form without any keywords to disable this feature, or with a keyword to restore the default settings.

SYNTAX

spanning-tree bpdu-guard [**auto-recovery** [**interval** *interval*]]

no spanning-tree bpdu-guard [**auto-recovery** [**interval**]]

auto-recovery - Automatically re-enables an interface after the specified interval.

interval - The time to wait before re-enabling an interface. (Range: 30-86400 seconds)

DEFAULT SETTING

BPDU Guard: Disabled
Auto-Recovery: Disabled
Auto-Recovery Interval: 300 seconds

COMMAND MODE

Interface Configuration (Ethernet, Port Channel)

COMMAND USAGE

- An edge port should only be connected to end nodes which do not generate BPDUs. If a BPDU is received on an edge port, this indicates an invalid network configuration, or that the switch may be under attack by a hacker. If an interface is shut down by BPDU Guard, it must be manually re-enabled using the no spanning-tree spanning-disabled command if the auto-recovery interval is not specified.

- Before enabling BPDU Guard, the interface must be configured as an edge port with the spanning-tree edge-port command. Also note that if the edge port attribute is disabled on an interface, BPDU Guard will also be disabled on that interface.

EXAMPLE

```
Console(config)#interface ethernet 1/5
Console(config-if)#spanning-tree edge-port
Console(config-if)#spanning-tree bpdu-guard
Console(config-if)#
```

RELATED COMMANDS

spanning-tree edge-port (1291)
spanning-tree spanning-disabled (1299)

spanning-tree cost

This command configures the spanning tree path cost for the specified interface. Use the **no** form to restore the default auto-configuration mode.

SYNTAX

spanning-tree cost *cost*

no spanning-tree cost

cost - The path cost for the port. (Range: 0 for auto-configuration, 1-65535 for short path cost method[24], 1-200,000,000 for long path cost method)

Table 152: Recommended STA Path Cost Range

Port Type	Short Path Cost (IEEE 802.1D-1998)	Long Path Cost (802.1D-2004)
Ethernet	50-600	200,000-20,000,000
Fast Ethernet	10-60	20,000-2,000,000
Gigabit Ethernet	3-10	2,000-200,000
10G Ethernet	1-5	200-20,000

DEFAULT SETTING

By default, the system automatically detects the speed and duplex mode used on each port, and configures the path cost according to the values shown below. Path cost “0” is used to indicate auto-configuration mode. When the short path cost method is selected and the default path cost recommended by the IEEE 8021w standard exceeds 65,535, the default is set to 65,535.

[24] Use the spanning-tree pathcost method command on page 1282 to set the path cost method.

Table 153: Default STA Path Costs

Port Type	Short Path Cost (IEEE 802.1D-1998)	Long Path Cost (802.1D-2004)
Ethernet	65,535	1,000,000
Fast Ethernet	65,535	100,000
Gigabit Ethernet	10,000	10,000
10G Ethernet	1,000	1,000

COMMAND MODE

Interface Configuration (Ethernet, Port Channel)

COMMAND USAGE

- This command is used by the Spanning Tree Algorithm to determine the best path between devices. Therefore, lower values should be assigned to ports attached to faster media, and higher values assigned to ports with slower media.
- Path cost takes precedence over port priority.
- When the path cost method (page 1282) is set to short, the maximum value for path cost is 65,535.

EXAMPLE

```
Console(config)#interface ethernet 1/5
Console(config-if)#spanning-tree cost 50
Console(config-if)#
```

spanning-tree edge-port

This command specifies an interface as an edge port. Use the **no** form to restore the default.

SYNTAX

spanning-tree edge-port [**auto**]

no spanning-tree edge-port

auto - Automatically determines if an interface is an edge port.

DEFAULT SETTING

Auto

COMMAND MODE

Interface Configuration (Ethernet, Port Channel)

COMMAND USAGE

You can enable this option if an interface is attached to a LAN segment that is at the end of a bridged LAN or to an end node. Since end nodes cannot cause forwarding loops, they can pass directly through to the spanning tree forwarding state. Specifying Edge Ports provides quicker convergence for devices such as workstations or servers, retains the current forwarding database to reduce the amount of frame flooding required to rebuild address tables during reconfiguration events, does not cause the spanning tree to initiate reconfiguration when the interface changes state, and also overcomes other STA-related time out problems. However, remember that Edge Port should only be enabled for ports connected to an end-node device.

EXAMPLE

```
Console(config)#interface ethernet 1/5
Console(config-if)#spanning-tree edge-port
Console(config-if)#
```

spanning-tree link-type

This command configures the link type for Rapid Spanning Tree and Multiple Spanning Tree. Use the **no** form to restore the default.

SYNTAX

spanning-tree link-type {**auto** | **point-to-point** | **shared**}

no spanning-tree link-type

auto - Automatically derived from the duplex mode setting.

point-to-point - Point-to-point link.

shared - Shared medium.

DEFAULT SETTING

auto

COMMAND MODE

Interface Configuration (Ethernet, Port Channel)

COMMAND USAGE

- Specify a point-to-point link if the interface can only be connected to exactly one other bridge, or a shared link if it can be connected to two or more bridges.

- When automatic detection is selected, the switch derives the link type from the duplex mode. A full-duplex interface is considered a point-to-point link, while a half-duplex interface is assumed to be on a shared link.

- RSTP only works on point-to-point links between two bridges. If you designate a port as a shared link, RSTP is forbidden. Since MSTP is an extension of RSTP, this same restriction applies.

EXAMPLE

```
Console(config)#interface ethernet 1/5
Console(config-if)#spanning-tree link-type point-to-point
```

spanning-tree loopback-detection

This command enables the detection and response to Spanning Tree loopback BPDU packets on the port. Use the **no** form to disable this feature.

SYNTAX

[**no**] **spanning-tree loopback-detection**

DEFAULT SETTING

Enabled

COMMAND MODE

Interface Configuration (Ethernet, Port Channel)

COMMAND USAGE

- If Port Loopback Detection is not enabled and a port receives it's own BPDU, then the port will drop the loopback BPDU according to IEEE Standard 802.1W-2001 9.3.4 (Note 1).
- Port Loopback Detection will not be active if Spanning Tree is disabled on the switch.

EXAMPLE

```
Console(config)#interface ethernet 1/5
Console(config-if)#spanning-tree loopback-detection
```

spanning-tree loopback-detection action

This command configures the response for loopback detection to block user traffic or shut down the interface. Use the **no** form to restore the default.

SYNTAX

spanning-tree loopback-detection action
{**block** | **shutdown** *duration*}

no spanning-tree loopback-detection action

block - Blocks user traffic.

shutdown - Shuts down the interface.

duration - The duration to shut down the interface. (Range: 60-86400 seconds)

DEFAULT SETTING

block

COMMAND MODE

Interface Configuration (Ethernet, Port Channel)

COMMAND USAGE

- If an interface is shut down by this command, and the release mode is set to "auto" with the spanning-tree loopback-detection release-mode command, the selected interface will be automatically enabled when the shutdown interval has expired.

- If an interface is shut down by this command, and the release mode is set to “manual,” the interface can be re-enabled using the spanning-tree loopback-detection release command.

EXAMPLE

```
Console(config)#interface ethernet 1/5
Console(config-if)#spanning-tree loopback-detection action shutdown 600
```

spanning-tree loopback-detection release-mode

This command configures the release mode for a port that was placed in the discarding state because a loopback BPDU was received. Use the **no** form to restore the default.

SYNTAX

spanning-tree loopback-detection release-mode {**auto** | **manual**}

no spanning-tree loopback-detection release-mode

auto - Allows a port to automatically be released from the discarding state when the loopback state ends.

manual - The port can only be released from the discarding state manually.

DEFAULT SETTING

auto

COMMAND MODE

Interface Configuration (Ethernet, Port Channel)

COMMAND USAGE

- If the port is configured for automatic loopback release, then the port will only be returned to the forwarding state if one of the following conditions is satisfied:
  - The port receives any other BPDU except for it’s own, or;
  - The port’s link status changes to link down and then link up again, or;
  - The port ceases to receive it’s own BPDUs in a forward delay interval.
- If Port Loopback Detection is not enabled and a port receives it’s own BPDU, then the port will drop the loopback BPDU according to IEEE Standard 802.1W-2001 9.3.4 (Note 1).
- Port Loopback Detection will not be active if Spanning Tree is disabled on the switch.

- When configured for manual release mode, then a link down / up event will not release the port from the discarding state. It can only be released using the spanning-tree loopback-detection release command.

EXAMPLE

```
Console(config)#interface ethernet 1/5
Console(config-if)#spanning-tree loopback-detection release-mode manual
Console(config-if)#
```

spanning-tree loopback-detection trap

This command enables SNMP trap notification for Spanning Tree loopback BPDU detections. Use the **no** form to restore the default.

SYNTAX

[**no**] **spanning-tree loopback-detection trap**

DEFAULT SETTING

Disabled

COMMAND MODE

Interface Configuration (Ethernet, Port Channel)

EXAMPLE

```
Console(config)#interface ethernet 1/5
Console(config-if)#spanning-tree loopback-detection trap
```

spanning-tree mst cost

This command configures the path cost on a spanning instance in the Multiple Spanning Tree. Use the **no** form to restore the default auto-configuration mode.

SYNTAX

spanning-tree mst *instance-id* **cost** *cost*

no spanning-tree mst *instance-id* **cost**

instance-id - Instance identifier of the spanning tree. (Range: 0-4094)

cost - Path cost for an interface. (Range: 0 for auto-configuration, 1-65535 for short path cost method[25], 1-200,000,000 for long path cost method)

The recommended path cost range is listed in Table 152 on page 1290.

DEFAULT SETTING

By default, the system automatically detects the speed and duplex mode used on each port, and configures the path cost according to the values

[25] Use the spanning-tree pathcost method command to set the path cost method.

shown below. Path cost "0" is used to indicate auto-configuration mode. When the short path cost method is selected and the default path cost recommended by the IEEE 8021w standard exceeds 65,535, the default is set to 65,535. The default path costs are listed in Table 153 on page 1291.

COMMAND MODE

Interface Configuration (Ethernet, Port Channel)

COMMAND USAGE

- Each spanning-tree instance is associated with a unique set of VLAN IDs.
- This command is used by the multiple spanning-tree algorithm to determine the best path between devices. Therefore, lower values should be assigned to interfaces attached to faster media, and higher values assigned to interfaces with slower media.
- Use the **no spanning-tree mst cost** command to specify auto-configuration mode.
- Path cost takes precedence over interface priority.

EXAMPLE

```
Console(config)#interface Ethernet 1/5
Console(config-if)#spanning-tree mst 1 cost 50
Console(config-if)#
```

RELATED COMMANDS

spanning-tree mst port-priority (1296)

spanning-tree mst port-priority

This command configures the interface priority on a spanning instance in the Multiple Spanning Tree. Use the **no** form to restore the default.

SYNTAX

spanning-tree mst *instance-id* **port-priority** *priority*

no spanning-tree mst ***instance-id*** **port-priority**

instance-id - Instance identifier of the spanning tree. (Range: 0-4094)

priority - Priority for an interface. (Range: 0-240 in steps of 16)

DEFAULT SETTING

128

COMMAND MODE

Interface Configuration (Ethernet, Port Channel)

COMMAND USAGE

- This command defines the priority for the use of an interface in the multiple spanning-tree. If the path cost for all interfaces on a switch are the same, the interface with the highest priority (that is, lowest value) will be configured as an active link in the spanning tree.
- Where more than one interface is assigned the highest priority, the interface with lowest numeric identifier will be enabled.

EXAMPLE

```
Console(config)#interface Ethernet 1/5
Console(config-if)#spanning-tree mst 1 port-priority 0
Console(config-if)#
```

RELATED COMMANDS

spanning-tree mst cost (1295)

spanning-tree port-bpdu-flooding

This command floods BPDUs to other ports when spanning tree is disabled globally or disabled on a specific port. Use the **no** form to restore the default setting.

SYNTAX

[**no**] **spanning-tree port-bpdu-flooding**

DEFAULT SETTING

Enabled

COMMAND MODE

Interface Configuration (Ethernet, Port Channel)

COMMAND USAGE

- When enabled, BPDUs are flooded to all other ports on the switch or to all other ports within the receiving port's native VLAN as specified by the spanning-tree system-bpdu-flooding command.
- The spanning-tree system-bpdu-flooding command has no effect if BPDU flooding is disabled on a port by the **spanning-tree port-bpdu-flooding** command.

EXAMPLE

```
Console(config)#interface ethernet 1/5
Console(config-if)#spanning-tree port-bpdu-flooding
Console(config-if)#
```

spanning-tree port-priority

This command configures the priority for the specified interface. Use the **no** form to restore the default.

SYNTAX

spanning-tree port-priority *priority*

no spanning-tree port-priority

priority - The priority for a port. (Range: 0-240, in steps of 16)

DEFAULT SETTING

128

COMMAND MODE

Interface Configuration (Ethernet, Port Channel)

COMMAND USAGE

- This command defines the priority for the use of a port in the Spanning Tree Algorithm. If the path cost for all ports on a switch are the same, the port with the highest priority (that is, lowest value) will be configured as an active link in the spanning tree.

- Where more than one port is assigned the highest priority, the port with lowest numeric identifier will be enabled.

EXAMPLE

```
Console(config)#interface ethernet 1/5
Console(config-if)#spanning-tree port-priority 0
```

RELATED COMMANDS

spanning-tree cost (1290)

spanning-tree root-guard

This command prevents a designated port[26] from taking superior BPDUs into account and allowing a new STP root port to be elected. Use the **no** form to disable this feature.

SYNTAX

[**no**] **spanning-tree root-guard**

DEFAULT SETTING

Disabled

COMMAND MODE

Interface Configuration (Ethernet, Port Channel)

[26] See Port Role under "Displaying Interface Settings for STA" on page 286.

COMMAND USAGE

- A bridge with a lower bridge identifier (or same identifier and lower MAC address) can take over as the root bridge at any time.
- When Root Guard is enabled, and the switch receives a superior BPDU on this port, it is set to the Discarding state until it stops receiving superior BPDUs for a fixed recovery period. While in the discarding state, no traffic is forwarded across the port.
- Root Guard can be used to ensure that the root bridge is not formed at a suboptimal location. Root Guard should be enabled on any designated port connected to low-speed bridges which could potentially overload a slower link by taking over as the root port and forming a new spanning tree topology. It could also be used to form a border around part of the network where the root bridge is allowed.
- When spanning tree is initialized globally on the switch or on an interface, the switch will wait for 20 seconds to ensure that the spanning tree has converged before enabling Root Guard.

EXAMPLE

```
Console(config)#interface ethernet 1/5
Console(config-if)#spanning-tree edge-port
Console(config-if)#spanning-tree root-guard
Console(config-if)#
```

spanning-tree spanning-disabled

This command disables the spanning tree algorithm for the specified interface. Use the **no** form to re-enable the spanning tree algorithm for the specified interface.

SYNTAX

[**no**] **spanning-tree spanning-disabled**

DEFAULT SETTING

Enabled

COMMAND MODE

Interface Configuration (Ethernet, Port Channel)

EXAMPLE

This example disables the spanning tree algorithm for port 5.

```
Console(config)#interface ethernet 1/5
Console(config-if)#spanning-tree spanning-disabled
Console(config-if)#
```

spanning-tree tc-prop-stop

This command stops the propagation of topology change notifications (TCN). Use the **no** form to allow propagation of TCN messages.

SYNTAX

[**no**] **spanning-tree tc-prop-stop**

DEFAULT SETTING

Disabled

COMMAND MODE

Interface Configuration (Ethernet, Port Channel)

COMMAND USAGE

- When this command is enabled on an interface, topology change information originating from the interface will still be propagated.

- This command should not be used on an interface which is purposely configured in a ring topology.

EXAMPLE

```
Console(config)#interface ethernet 1/1
Console(config-if)#spanning-tree tc-prop-stop
Console(config-if)#
```

spanning-tree loopback-detection release

This command manually releases a port placed in discarding state by loopback-detection.

SYNTAX

spanning-tree loopback-detection release *interface*

interface

ethernet *unit/port*

unit - Unit identifier. (Range: 1)

port - Port number. (Range: 1-28)

port-channel *channel-id* (Range: 1-8)

COMMAND MODE

Privileged Exec

COMMAND USAGE

Use this command to release an interface from discarding state if loopback detection release mode is set to "manual" by the spanning-tree loopback-detection release-mode command and BPDU loopback occurs.

EXAMPLE

```
Console#spanning-tree loopback-detection release ethernet 1/1
Console#
```

spanning-tree protocol-migration

This command re-checks the appropriate BPDU format to send on the selected interface.

SYNTAX

spanning-tree protocol-migration *interface*

interface

ethernet *unit/port*

unit - Unit identifier. (Range: 1)

port - Port number. (Range: 1-28)

port-channel *channel-id* (Range: 1-8)

COMMAND MODE

Privileged Exec

COMMAND USAGE

If at any time the switch detects STP BPDUs, including Configuration or Topology Change Notification BPDUs, it will automatically set the selected interface to forced STP-compatible mode. However, you can also use the **spanning-tree protocol-migration** command at any time to manually re-check the appropriate BPDU format to send on the selected interfaces (i.e., RSTP or STP-compatible).

EXAMPLE

```
Console#spanning-tree protocol-migration eth 1/5
Console#
```

show spanning-tree

This command shows the configuration for the common spanning tree (CST), for all instances within the multiple spanning tree (MST), or for a specific instance within the multiple spanning tree (MST).

SYNTAX

show spanning-tree [*interface* | **mst** *instance-id*]

interface

ethernet *unit/port*

unit - Unit identifier. (Range: 1)

port - Port number. (Range: 1-28)

port-channel *channel-id* (Range: 1-8)

instance-id - Instance identifier of the multiple spanning tree. (Range: 0-4094)

DEFAULT SETTING

None

COMMAND MODE

Privileged Exec

COMMAND USAGE

- Use the **show spanning-tree** command with no parameters to display the spanning tree configuration for the switch for the Common Spanning Tree (CST) and for every interface in the tree.

- Use the **show spanning-tree** *interface* command to display the spanning tree configuration for an interface within the Common Spanning Tree (CST).

- Use the **show spanning-tree mst** command to display the spanning tree configuration for all instances within the Multiple Spanning Tree (MST), including global settings and settings for active interfaces.

- Use the **show spanning-tree mst** *instance-id* command to display the spanning tree configuration for an instance within the Multiple Spanning Tree (MST), including global settings and settings for all interfaces.

- For a description of the items displayed under “Spanning-tree information,” see "Configuring Global Settings for STA" on page 276. For a description of the items displayed for specific interfaces, see "Displaying Interface Settings for STA" on page 286.

EXAMPLE

```
Console#show spanning-tree
Spanning Tree Information
---------------------------------------------------------------
 Spanning Tree Mode                : MSTP
 Spanning Tree Enabled/Disabled    : Enabled
 Instance                          : 0
 VLANs Configured                : 1-4094
 Priority                        : 32768
 Bridge Hello Time (sec.)        : 2
 Bridge Max. Age (sec.)          : 20
 Bridge Forward Delay (sec.)     : 15
 Root Hello Time (sec.)          : 2
 Root Max. Age (sec.)            : 20
 Root Forward Delay (sec.)       : 15
 Max. Hops                       : 20
 Remaining Hops                  : 20
 Designated Root                 : 32768.0.0001ECF8D8C6
 Current Root Port               : 21
 Current Root Cost               : 100000
 Number of Topology Changes      : 5
 Last Topology Change Time (sec.): 11409
 Transmission Limit              : 3
 Path Cost Method                : Long
 Flooding Behavior               : To VLAN
---------------------------------------------------------------
Eth  1/ 1 information
---------------------------------------------------------------
 Admin Status                      : Enabled
 Role                              : Disabled
 State                             : Discarding
 External Admin Path Cost          : 0
 Internal Admin Path Cost          : 0
 External Oper Path Cost           : 100000
 Internal Oper Path Cost           : 100000
 Priority                          : 128
 Designated Cost                   : 100000
 Designated Port                   : 128.1
 Designated Root                   : 32768.0.0001ECF8D8C6
 Designated Bridge                 : 32768.0.123412341234
 Forward Transitions               : 4
 Admin Edge Port                   : Disabled
 Oper Edge Port                    : Disabled
 Admin Link Type                   : Auto
 Oper Link Type                    : Point-to-point
 Flooding Behavior                 : Enabled
 Spanning-Tree Status              : Enabled
 Loopback Detection Status         : Enabled
 Loopback Detection Release Mode   : Auto
 Loopback Detection Trap           : Disabled
 Loopback Detection Action         : Block
 Root Guard Status                 : Disabled
 BPDU Guard Status                 : Disabled
 BPDU Guard Auto Recovery          : Disabled
 BPDU Guard Auto Recovery Interval : 300
 BPDU Filter Status                : Disabled
.
.
.
```

show spanning-tree mst configuration

This command shows the configuration of the multiple spanning tree.

COMMAND MODE

Privileged Exec

EXAMPLE

```
Console#show spanning-tree mst configuration
Mstp Configuration Information
--------------------------------------------------------------
 Configuration Name : R&D
 Revision Level     :0

 Instance VLANs
--------------------------------------------------------------
     0    1-4094
Console#
```

39 ERPS COMMANDS

The G.8032 recommendation, also referred to as Ethernet Ring Protection Switching (ERPS), can be used to increase the availability and robustness of Ethernet rings.

This chapter describes commands used to configure ERPS.

Table 154: ERPS Commands

Command	Function	Mode
erps	Enables ERPS globally on the switch	GC
erps domain	Creates an ERPS ring and enters ERPS configuration mode	GC
control-vlan	Adds a Control VLAN to an ERPS ring	ERPS
enable	Activates the current ERPS ring	ERPS
guard-timer	Sets the timer to prevent ring nodes from receiving outdated R-APS messages	ERPS
holdoff-timer	Sets the timer to filter out intermittent link faults	ERPS
major-domain	Specifies the ERPS ring used for sending control packets	ERPS
meg-level	Sets the Maintenance Entity Group level for a ring	ERPS
mep-monitor	Specifies the CCM MEPs used to monitor the link on a ring node	ERPS
node-id	Sets the MAC address for a ring node	ERPS
non-erps-dev-protect	Sends non-standard health-check packets when in protection state	ERPS
non-revertive	Enables non-revertive mode, which requires the protection state on the RPL to manually cleared	ERPS
propagate-tc	Enables propagation of topology change messages from a secondary ring to the primary ring	ERPS
raps-def-mac	Sets the switch's MAC address to be used as the node identifier in R-APS messages	ERPS
raps-without-vc	Terminates the R-APS channel at the primary ring to sub-ring interconnection nodes	ERPS
ring-port	Configures a node's connection to the ring through the east or west interface	ERPS
rpl neighbor	Configures a ring node to be the RPL neighbor	ERPS
rpl owner	Configures a ring node to be the RPL owner	ERPS
version	Specifies compatibility with ERPS version 1 or 2	ERPS
wtr-timer	Sets timer to verify that the ring has stabilized before blocking the RPL after recovery from a signal failure	ERPS
clear erps statistics	Clears statistics, including SF, NR, NR-RB, FS, MS, Event, and Health protocol messages	PE

Table 154: ERPS Commands(Continued)

Command	Function	Mode
erps clear	Manually clears protection state which has been invoked by a Forced Switch or Manual Switch command, and the node is operating under non-revertive mode; or before the WTR or WTB timer expires when the node is operating in revertive mode	PE
erps forced-switch	Blocks the specified ring port	PE
erps manual-switch	Blocks the specified ring port, in the absence of a failure or an erps forced-switch command	PE
show erps	Displays status information for all configured rings, or for a specified ring	PE

Configuration Guidelines for ERPS

1. Create an ERPS ring: Create a ring using the erps domain command. The ring name is used as an index in the G.8032 database.

2. Configure the east and west interfaces: Each node on the ring connects to it through two ring ports. Use the ring-port command to configure one port connected to the next node in the ring to the east (or clockwise direction); and then use the ring-port command again to configure another port facing west in the ring.

3. Configure the RPL owner: Configure one node in the ring as the Ring Protection Link (RPL) owner using the rpl owner command. When this switch is configured as the RPL owner, the west ring port is set as being connected to the RPL. Under normal operations (Idle state), the RPL is blocked to ensure that a loop cannot form in the ring. If a signal failure brings down any other link in the ring, the RPL will be unblocked (Protection state) to ensure proper connectivity among all ring nodes until the failure is recovered.

4. Configure ERPS timers: Use the guard-timer command to set the timer is used to prevent ring nodes from receiving outdated R-APS messages, the holdoff-timer command to filter out intermittent link faults, and the wtr-timer command to verify that the ring has stabilized before blocking the RPL after recovery from a signal failure.

5. Configure the ERPS Control VLAN (CVLAN): Use the control-vlan command to create the VLAN used to pass R-APS ring maintenance commands. The CVLAN must NOT be configured with an IP address. In addition, only ring ports may be added to the CVLAN (prior to configuring the VLAN as a CVLAN). No other ports can be members of this VLAN (once set as a CVLAN). Also, the ring ports of the CVLAN must be tagged. Failure to observe these restrictions can result in a loop in the network.

6. Enable ERPS: Before enabling a ring as described in the next step, first use the erps command to globally enable ERPS on the switch. If ERPS has not yet been enabled or has been disabled with the no erps command, no ERPS rings will work.

7. Enable an ERPS ring: Before an ERPS ring can work, it must be enabled using the enable command. When configuration is completed and the ring enabled, R-APS messages will start flowing in the control VLAN, and normal traffic will begin to flow in the data VLANs. To stop a ring, it can be disabled on any node using the no enable command.

8. Display ERPS status information: Use the show erps command to display general ERPS status information or detailed ERPS status information for a specific ring.

erps

This command enables ERPS on the switch. Use the **no** form to disable this feature.

SYNTAX

[**no**] **erps**

DEFAULT SETTING

Disabled

COMMAND MODE

Global Configuration

COMMAND USAGE

ERPS must be enabled globally on the switch before it can enabled on an ERPS ring using the enable command.

EXAMPLE

```
Console(config)#erps
Console(config)#
```

RELATED COMMANDS

enable (1309)

erps domain

This command creates an ERPS ring and enters ERPS configuration mode for the specified domain. Use the **no** form to delete a ring.

SYNTAX

[**no**] **erps domain** *ring-name* [**id** *ring-id*]

ring-name - Name of a specific ERPS ring. (Range: 1-12 characters)

ring-id - ERPS ring identifier used in R-APS messages. (Range: 1-255)

DEFAULT SETTING

None

COMMAND MODE

Global Configuration

COMMAND USAGE

- Service Instances within each ring are based on a unique maintenance association for the specific users, distinguished by the ring name, maintenance level, maintenance association's name, and assigned VLAN. Up to 6 ERPS rings can be configured on the switch.

- R-APS information is carried in an R-APS PDUs. The last octet of the MAC address is designated as the Ring ID (01-19-A7-00-00-[Ring ID]). If use of the default MAC address is disabled with the no raps-def-mac command, then the Ring ID configured by the **erps domain** command will be used in R-APS PDUs.

EXAMPLE

```
Console(config)#erps domain r&d id 1
Console(config-erps)#
```

control-vlan

This command specifies a dedicated VLAN used for sending and receiving ERPS protocol messages. Use the **no** form to remove the Control VLAN.

SYNTAX

[**no**] **control-vlan** *vlan-id*

vlan-id - VLAN ID (Range: 1-4094)

DEFAULT SETTING

None

COMMAND MODE

ERPS Configuration

COMMAND USAGE

- Configure one control VLAN for each ERPS ring. First create the VLAN to be used as the control VLAN (vlan, page 1344), add the ring ports for the east and west interface as tagged members to this VLAN (switchport allowed vlan, page 1347), and then use the control-vlan command to add it to the ring.

- The following restrictions are recommended to avoid creating a loop in the network or other problems which may occur under some situations:
  - The Control VLAN must not be configured as a Layer 3 interface (with an IP address), a dynamic VLAN (with GVRP enabled), nor as a private VLAN.
  - In addition, only ring ports may be added to the Control VLAN. No other ports can be members of this VLAN.
  - Also, the ring ports of the Control VLAN must be tagged.

- Once the ring has been activated with the enable command, the configuration of the control VLAN cannot be modified. Use the no enable command to stop the ERPS ring before making any configuration changes to the control VLAN.

EXAMPLE

```
Console(config)#vlan database
Console(config-vlan)#vlan 2 name rdc media ethernet state active
Console(config-vlan)#exit
Console(config)#interface ethernet 1/12
Console(config-if)#switchport allowed vlan add 2 tagged
Console(config-if)#interface ethernet 1/11
Console(config-if)#switchport allowed vlan add 2 tagged
Console(config-if)#exit
Console(config)#erps domain rd1
Console(config-erps)#control-vlan 2
Console(config-erps)#
```

enable

This command activates the current ERPS ring. Use the **no** form to disable the current ring.

SYNTAX

[**no**] **enable**

DEFAULT SETTING

Disabled

COMMAND MODE

ERPS Configuration

COMMAND USAGE

- Before enabling a ring, the global ERPS function should be enabled with the erps command, the east and west ring ports configured on each node with the ring-port command, the RPL owner specified with the rpl owner command, and the control VLAN configured with the control-vlan command.

- Once enabled, the RPL owner node and non-owner node state machines will start, and the ring will enter idle state if no signal failures are detected.

EXAMPLE

```
Console(config-erps)#enable
Console(config-erps)#
```

RELATED COMMANDS

erps (1307)

guard-timer

This command sets the guard timer to prevent ring nodes from receiving outdated R-APS messages. Use the **no** form to restore the default setting.

SYNTAX

guard-timer *milliseconds*

milliseconds - The guard timer is used to prevent ring nodes from receiving outdated R-APS messages. During the duration of the guard timer, all received R-APS messages are ignored by the ring protection control process, giving time for old messages still circulating on the ring to expire. (Range: 10-2000 milliseconds, in steps of 10 milliseconds)

DEFAULT SETTING

500 milliseconds

COMMAND MODE

ERPS Configuration

COMMAND USAGE

The guard timer duration should be greater than the maximum expected forwarding delay for an R-APS message to pass around the ring. A side-effect of the guard timer is that during its duration, a node will be unaware of new or existing ring requests transmitted from other nodes.

EXAMPLE

```
Console(config-erps)#guard-timer 300
Console(config-erps)#
```

holdoff-timer

This command sets the timer to filter out intermittent link faults. Use the **no** form to restore the default setting.

SYNTAX

holdoff-timer *milliseconds*

milliseconds - The hold-off timer is used to filter out intermittent link faults. Faults will only be reported to the ring protection mechanism if this timer expires. (Range: 0-10000 milliseconds, in steps of 100 milliseconds)

DEFAULT SETTING

0 milliseconds

COMMAND MODE

ERPS Configuration

COMMAND USAGE

In order to coordinate timing of protection switches at multiple layers, a hold-off timer may be required. Its purpose is to allow, for example, a server layer protection switch to have a chance to fix the problem before switching at a client layer.

When a new defect or more severe defect occurs (new Signal Failure), this event will not be reported immediately to the protection switching mechanism if the provisioned hold-off timer value is non-zero. Instead, the hold-off timer will be started. When the timer expires, whether a defect still exists or not, the timer will be checked. If one does exist, that defect will be reported to the protection switching mechanism. The reported defect need not be the same one that started the timer.

Example

```
Console(config-erps)#holdoff-timer 300
Console(config-erps)#
```

major-domain

This command specifies the ERPS ring used for sending control packets. Use the **no** form to remove the current setting.

Syntax

major-domain *name*

no major-domain

name - Name of the ERPS ring used for sending control packets. (Range: 1-32 characters)

Default Setting

None

Command Mode

ERPS Configuration

Command Usage

- This switch can support up to thirteen rings. However, ERPS control packets can only be sent on one ring. This command is used to indicate that the current ring is a secondary ring, and to specify the major ring which will be used to send ERPS control packets.

- The Ring Protection Link (RPL) is the west port and can not be configured. So the physical port on a secondary ring must be the west port. In other words, if a domain has two physical ring ports, this ring can only be a major ring, not a secondary ring (or sub-domain) which can have only one physical ring port. This command will therefore fail if the east port is already configured (see the ring-port command).

Example

```
Console(config-erps)#major-domain rd0
Console(config-erps)#
```

meg-level

This command sets the Maintenance Entity Group level for a ring. Use the **no** form to restore the default setting.

SYNTAX

meg-level *level*

level - The maintenance entity group (MEG) level which provides a communication channel for ring automatic protection switching (R-APS) information. (Range: 0-7)

DEFAULT SETTING

1

COMMAND MODE

ERPS Configuration

COMMAND USAGE

- This parameter is used to ensure that received R-APS PDUs are directed for this ring. A unique level should be configured for each local ring if there are many R-APS PDUs passing through this switch.

- If CFM continuity check messages are used to monitor the link status of an ERPS ring node as specified by the mep-monitor command, then the MEG level set by the **meg-level** command must match the authorized maintenance level of the CFM domain to which the specified MEP belongs. The MEP’s primary VLAN must also be the same as that used for the ERPS ring’s control VLAN.

EXAMPLE

```
Console(config-erps)#meg-level 0
Console(config-erps)#
```

RELATED COMMANDS

ethernet cfm domain (1567)
ethernet cfm mep (1571)

mep-monitor

This command specifies the CFM MEPs used to monitor the link on a ring node. Use the **no** form to restore the default setting.

SYNTAX

mep-monitor {**east** | **west**} **mep** *mpid*

east - Connects to next ring node to the east.

west - Connects to next ring node to the west.

mpid – Maintenance end point identifier. (Range: 1-8191)

DEFAULT SETTING

None

COMMAND MODE

ERPS Configuration

COMMAND USAGE

- If this command is used to monitor the link status of an ERPS node with CFM continuity check messages, then the MEG level set by the meg-level command must match the authorized maintenance level of the CFM domain to which the specified MEP belongs.

- To ensure complete monitoring of a ring node, use the **mep-monitor** command to specify the CFM MEPs used to monitor both the east and west ports of the ring node.

- If CFM determines that a MEP node which has been configured to monitor a ring port with this command has gone down, this information is passed to ERPS, which in turn processes it as a ring node failure. For more information on how ERPS recovers from a node failure, refer to "Ethernet Ring Protection Switching" on page 523.

EXAMPLE

```
Console(config-erps)#mep-monitor east mep 1
Console(config-erps)#
```

RELATED COMMANDS

ethernet cfm domain (1567)
ethernet cfm mep (1571)

node-id

This command sets the MAC address for a ring node. Use the **no** form to restore the default setting.

SYNTAX

node-id *mac-address*

> *mac-address* – A MAC address unique to the ring node. The MAC address must be specified in the format xx-xx-xx-xx-xx-xx or xxxxxxxxxxxx.

DEFAULT SETTING

CPU MAC address

COMMAND MODE

ERPS Configuration

COMMAND USAGE

- The ring node identifier is used to identify a node in R-APS messages for both automatic and manual switching recovery operations.

For example, a node that has one ring port in SF condition and detects that the condition has been cleared, will continuously transmit R-APS (NR) messages with its own Node ID as priority information over both ring ports, informing its neighbors that no request is present at this node. When another recovered node holding the link blocked receives this message, it compares the Node ID information with its own. If the received R-APS (NR) message has a higher priority, this unblocks its ring ports. Otherwise, the block remains unchanged.

- The node identifier may also be used for debugging, such as to distinguish messages when a node is connected to more than one ring.

EXAMPLE

```
Console(config-erps)#node-id 00-12-CF-61-24-2D
Console(config-erps)#
```

non-erps-dev-protect

This command sends non-standard health-check packets when an owner node enters protection state without any link down event having been detected through SF messages. Use the **no** form to disable this feature.

SYNTAX

[**no**] **non-erps-dev-protect**

DEFAULT SETTING

Disabled

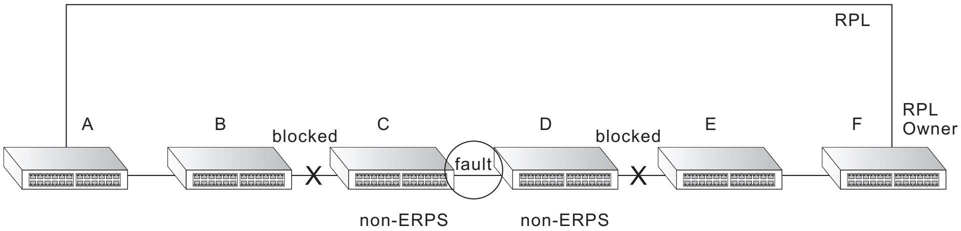
COMMAND MODE

ERPS Configuration

COMMAND USAGE

- The RPL owner node detects a failed link when it receives R-APS (SF - signal fault) messages from nodes adjacent to the failed link. The owner then enters protection state by unblocking the RPL. However, using this standard recovery procedure may cause a non-EPRS device to become isolated when the ERPS device adjacent to it detects a continuity check message (CCM) loss event and blocks the link between the non-ERPS device and ERPS device.

  CCMs are propagated by the Connectivity Fault Management (CFM) protocol as described under "CFM Commands" on page 1561. If the standard recovery procedure were used as shown in the following figure, and node E detected CCM loss, it would send an R-APS (SF) message to the RPL owner and block the link to node D, isolating that non-ERPS device.



When non-ERPS device protection is enabled on the ring, the ring ports on the RPL owner node and non-owner nodes will not be blocked when signal loss is detected by CCM loss events.

- When non-ERPS device protection is enabled on an RPL owner node, it will send non-standard health-check packets to poll the ring health when it enters the protection state. It does not use the normal procedure of waiting to receive an R-APS (NR - no request) message from nodes adjacent to the recovered link. Instead, it waits to see if the non-standard health-check packets loop back. If they do, indicating that the fault has been resolved, the RPL will be blocked.

  After blocking the RPL, the owner node will still transmit an R-APS (NR, RB - ring blocked) message. ERPS-compliant nodes receiving this message flush their forwarding database and unblock previously blocked ports. The ring is now returned to Idle state.

EXAMPLE

```
Console(config-erps)#non-erps-dev-protect
Console(config-erps)#
```

non-revertive

This command enables non-revertive mode, which requires the protection state on the RPL to manually cleared. Use the **no** form to restore the default revertive mode.

SYNTAX

[**no**] **non-revertive**

DEFAULT SETTING

Disabled

COMMAND MODE

ERPS Configuration

COMMAND USAGE

- Revertive behavior allows the switch to automatically return the RPL from Protection state to Idle state through the exchange of protocol messages.

  Non-revertive behavior for Protection, Forced Switch, and Manual Switch states are basically the same. Non-revertive behavior requires the erps clear command to used to return the RPL from Protection state to Idle state.

- Recovery for Protection Switching – A ring node that has one or more ring ports in an SF (Signal Fail) condition, upon detecting the SF condition cleared, keeps at least one of its ring ports blocked for the traffic channel and for the R-APS channel, until the RPL is blocked as a result of ring protection reversion, or until there is another higher priority request (e.g., an SF condition) in the ring.

  A ring node that has one ring port in an SF condition and detects the SF condition cleared, continuously transmits the R-APS (NR – no request) message with its own Node ID as the priority information over both ring ports, informing that no request is present at this ring node and initiates a guard timer. When another recovered ring node (or nodes) holding the link block receives this message, it compares the Node ID information with its own Node ID. If the received R-APS (NR) message has the higher priority, this ring node unblocks its ring ports. Otherwise, the block remains unchanged. As a result, there is only one link with one end blocked.

  The ring nodes stop transmitting R-APS (NR) messages when they accept an R-APS (NR, RB – RPL Blocked), or when another higher priority request is received.

  - Recovery with Revertive Mode – When all ring links and ring nodes have recovered and no external requests are active, reversion is handled in the following way:

    a. The reception of an R-APS (NR) message causes the RPL Owner Node to start the WTR (Wait-to-Restore) timer.

    b. The WTR timer is cancelled if during the WTR period a higher priority request than NR is accepted by the RPL Owner Node or is declared locally at the RPL Owner Node.

    c. When the WTR timer expires, without the presence of any other higher priority request, the RPL Owner Node initiates reversion by blocking its traffic channel over the RPL, transmitting an R-APS (NR, RB) message over both ring ports, informing the ring that the RPL is blocked, and performing a flush FDB action.

    d. The acceptance of the R-APS (NR, RB) message causes all ring nodes to unblock any blocked non-RPL link that does not have an SF condition. If it is an R-APS (NR, RB) message without a DNF (do not flush) indication, all ring nodes flush the FDB.

  - Recovery with Non-revertive Mode – In non-revertive operation, the ring does not automatically revert when all ring links and ring nodes have recovered and no external requests are active. Non-revertive operation is handled in the following way:

    a. The RPL Owner Node does not generate a response on reception of an R-APS (NR) messages.

    b. When other healthy ring nodes receive the NR (Node ID) message, no action is taken in response to the message.

c. When the operator issues the erps clear command for non-revertive mode at the RPL Owner Node, the non-revertive operation is cleared, the RPL Owner Node blocks its RPL port, and transmits an R-APS (NR, RB) message in both directions, repeatedly.

d. Upon receiving an R-APS (NR, RB) message, any blocking node should unblock its non-failed ring port. If it is an R-APS (NR, RB) message without a DNF indication, all ring nodes flush the FDB.

- Recovery for Forced Switching – An erps forced-switch command is removed by issuing the erps clear command to the same ring node where Forced Switch mode is in effect. The clear command removes any existing local operator commands, and triggers reversion if the ring is in revertive behavior mode.

  The ring node where the Forced Switch was cleared keeps the ring port blocked for the traffic channel and for the R-APS channel, due to the previous Forced Switch command. This ring port is kept blocked until the RPL is blocked as a result of ring protection reversion, or until there is another higher priority request (e.g., an SF condition) in the ring.

  The ring node where the Forced Switch was cleared continuously transmits the R-APS (NR) message on both ring ports, informing other nodes that no request is present at this ring node. The ring nodes stop transmitting R-APS (NR) messages when they accept an RAPS (NR, RB) message, or when another higher priority request is received.

  If the ring node where the Forced Switch was cleared receives an R-APS (NR) message with a Node ID higher than its own Node ID, it unblocks any ring port which does not have an SF condition and stops transmitting R-APS (NR) message over both ring ports.

  - Recovery with revertive mode is handled in the following way:

    a. The reception of an R-APS (NR) message causes the RPL Owner Node to start the WTB timer.

    b. The WTB timer is cancelled if during the WTB period a higher priority request than NR is accepted by the RPL Owner Node or is declared locally at the RPL Owner Node.

    c. When the WTB timer expires, in the absence of any other higher priority request, the RPL Owner Node initiates reversion by blocking the traffic channel over the RPL, transmitting an R-APS (NR, RB) message over both ring ports, informing the ring that the RPL is blocked, and flushes the FDB.

    d. The acceptance of the R-APS (NR, RB) message causes all ring nodes to unblock any blocked non-RPL that does not have an SF condition. If it is an R-APS (NR, RB) message without a DNF indication, all ring nodes flush their FDB. This action unblocks the ring port which was blocked as a result of an operator command.

- Recovery with non-revertive mode is handled in the following way:

  a. The RPL Owner Node, upon reception of an R-APS(NR) message and in the absence of any other higher priority request does not perform any action.

  b. Then, after the operator issues the erps clear command at the RPL Owner Node, this ring node blocks the ring port attached to the RPL, transmits an R-APS (NR, RB) message on both ring ports, informing the ring that the RPL is blocked, and flushes its FDB.

  c. The acceptance of the R-APS (NR, RB) message triggers all ring nodes to unblock any blocked non-RPL which does not have an SF condition. If it is an R-APS (NR, RB) message without a DNF indication, all ring nodes flush their FDB. This action unblocks the ring port which was blocked as result of an operator command.

- Recovery for Manual Switching – An erps manual-switch command is removed by issuing the erps clear command at the same ring node where the Manual Switch is in effect. The clear command removes any existing local operator commands, and triggers reversion if the ring is in revertive behavior mode.

  The ring node where the Manual Switch was cleared keeps the ring port blocked for the traffic channel and for the R-APS channel, due to the previous Manual Switch command. This ring port is kept blocked until the RPL is blocked as a result of ring protection reversion, or until there is another higher priority request (e.g., an SF condition) in the ring.

  The Ethernet Ring Node where the Manual Switch was cleared continuously transmits the R-APS (NR) message on both ring ports, informing that no request is present at this ring node. The ring nodes stop transmitting R-APS (NR) messages when they accept an RAPS (NR, RB) message, or when another higher priority request is received.

  If the ring node where the Manual Switch was cleared receives an R-APS (NR) message with a Node ID higher than its own Node ID, it unblocks any ring port which does not have an SF condition and stops transmitting R-APS (NR) message on both ring ports.

  - Recovery with revertive mode is handled in the following way:

    a. The RPL Owner Node, upon reception of an R-APS (NR) message and in the absence of any other higher priority request, starts the WTB timer and waits for it to expire. While the WTB timer is running, any latent R-APS (MS) message is ignored due to the higher priority of the WTB running signal.

    b. When the WTB timer expires, it generates the WTB expire signal. The RPL Owner Node, upon reception of this signal, initiates reversion by blocking the traffic channel on the RPL, transmitting an R-APS (NR, RB) message over both ring ports, informing the ring that the RPL is blocked, and flushes its FDB.

    c. The acceptance of the R-APS (NR, RB) message causes all ring nodes to unblock any blocked non-RPL that does not have an SF condition. If it is an R-APS (NR, RB) message without a DNF indication, all Ethernet Ring Nodes flush their FDB. This action unblocks the ring port which was blocked as a result of an operator command.

- Recovery with non-revertive mode is handled in the following way:

  a. The RPL Owner Node, upon reception of an R-APS (NR) message and in the absence of any other higher priority request does not perform any action.

  b. Then, after the operator issues the erps clear command at the RPL Owner Node, this ring node blocks the ring port attached to the RPL, transmits an R-APS (NR, RB) message over both ring ports, informing the ring that the RPL is blocked, and flushes its FDB.

  c. The acceptance of the R-APS (NR, RB) message triggers all ring nodes to unblock any blocked non-RPL which does not have an SF condition. If it is an R-APS (NR, RB) message without a DNF indication, all ring nodes flush their FDB. This action unblocks the ring port which was blocked as result of an operator command.

EXAMPLE

```
Console(config-erps)#non-revertive
Console(config-erps)#
```

propagate-tc

This command enables propagation of topology change messages for a secondary ring to the primary ring. Use the **no** form to disable this feature.

SYNTAX

[**no**] **propagate-tc**

DEFAULT SETTING

Disabled

COMMAND MODE

ERPS Configuration

COMMAND USAGE

- When a secondary ring detects a topology change, it can pass a message about this event to the major ring. When the major ring receives this kind of message from a secondary ring, it can clear the MAC addresses on its ring ports to help the secondary ring restore its connections more quickly through protection switching.

- When the MAC addresses are cleared, data traffic may flood onto the major ring. The data traffic will become stable after the MAC addresses are learned again. The major ring will not be broken, but the bandwidth of data traffic on the major ring may suffer for a short period of time due to this flooding behavior.

Example

```
Console(config-erps)#propagate-tc
Console(config-erps)#
```

raps-def-mac

This command sets the switch’s MAC address to be used as the node identifier in R-APS messages. Use the **no** form to use the node identifier specified in the G8032 standards.

Syntax

[**no**] **raps-def-mac**

Default Setting

Enabled

Command Mode

ERPS Configuration

Command Usage

- When ring nodes running ERPSv1 and ERPSv2 co-exist on the same ring, the Ring ID of each ring node must be configured as “1”.
- If this command is disabled, the following strings are used as the node identifier:
  - ERPSv1: 01-19-A7-00-00-01
  - ERPSv2: 01-19-A7-00-00-[Ring ID]

Example

```
Console(config-erps)#propagate-tc
Console(config-erps)#
```

raps-without-vc

This command terminates the R-APS channel at the primary ring to sub-ring interconnection nodes. Use the **no** form to restore the default setting.

Syntax

[**no**] **raps-without-vc**

Default Setting

R-APS with Virtual Channel

Command Mode

ERPS Configuration

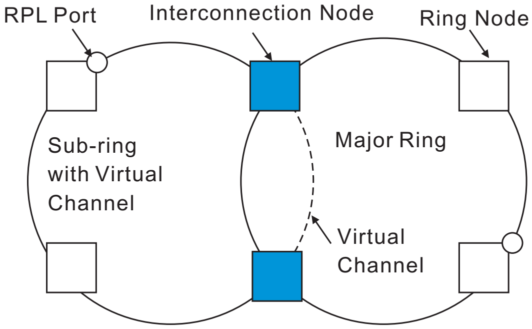
COMMAND USAGE

- A sub-ring may be attached to a primary ring with or without a virtual channel. A virtual channel is used to connect two interconnection points on the sub-ring, tunneling R-APS control messages across an arbitrary Ethernet network topology. If a virtual channel is not used to cross the intermediate Ethernet network, data in the traffic channel will still flow across the network, but the all R-APS messages will be terminated at the interconnection points.

- Sub-ring with R-APS Virtual Channel – When using a virtual channel to tunnel R-APS messages between interconnection points on a sub-ring, the R-APS virtual channel may or may not follow the same path as the traffic channel over the network. R-APS messages that are forwarded over the sub-ring's virtual channel are broadcast or multicast over the interconnected network. For this reason the broadcast/multicast domain of the virtual channel should be limited to the necessary links and nodes. For example, the virtual channel could span only the interconnecting rings or sub-rings that are necessary for forwarding R-APS messages of this sub-ring. Care must also be taken to ensure that the local RAPS messages of the sub-ring being transported over the virtual channel into the interconnected network can be uniquely distinguished from those of other interconnected ring R-APS messages. This can be achieved by, for example, by using separate VIDs for the virtual channels of different sub-rings.

  Note that the R-APS virtual channel requires a certain amount of bandwidth to forward R-APS messages on the interconnected Ethernet network where a sub-ring is attached. Also note that the protection switching time of the sub-ring may be affected if R-APS messages traverse a long distance over an R-APS virtual channel.

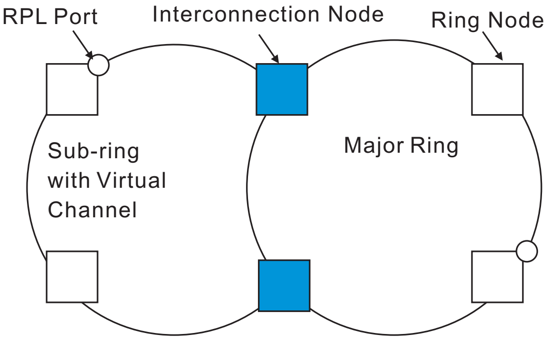
  Figure 550: Sub-ring with Virtual Channel



- Sub-ring without R-APS Virtual Channel – Under certain circumstances it may not be desirable to use a virtual channel to interconnect the sub-ring over an arbitrary Ethernet network. In this situation, the R-APS messages are terminated on the interconnection points. Since the sub-ring does not provide an R-APS channel nor R-APS virtual channel beyond the interconnection points, R-APS channel blocking is not employed on the normal ring links to avoid channel segmentation. As a result, a failure at any ring link in the sub-ring will cause the R-APS channel of the sub-ring to be segmented, thus preventing R-APS message exchange between some of the sub-ring's ring nodes.

No R-APS messages are inserted or extracted by other rings or sub-rings at the interconnection nodes where a sub-ring is attached. Hence there is no need for either additional bandwidth or for different VIDs/Ring IDs for the ring interconnection. Furthermore, protection switching time for a sub-ring is independent from the configuration or topology of the interconnected rings. In addition, this option always ensures that an interconnected network forms a tree topology regardless of its interconnection configuration. This means that it is not necessary to take precautions against forming a loop which is potentially composed of a whole interconnected network.

Figure 551: Sub-ring without Virtual Channel



EXAMPLE

```
Console(config-erps)#raps-without-vc
Console(config-erps)#
```

ring-port

This command configures a node’s connection to the ring through the east or west interface. Use the **no** form to disassociate a node from the ring.

SYNTAX

ring-port {**east** | **west**} **interface** *interface*

east - Connects to next ring node to the east.

west - Connects to next ring node to the west.

interface

ethernet *unit/port*

unit - Unit identifier. (Range: 1)

port - Port number. (Range: 1-28)

port-channel *channel-id* (Range: 1-8)

DEFAULT SETTING

Not associated

COMMAND MODE

ERPS Configuration

COMMAND USAGE

- Each node must be connected to two neighbors on the ring. For convenience, the ports connected are referred to as east and west ports. Alternatively, the closest neighbor to the east should be the next node in the ring in a clockwise direction, and the closest neighbor to the west should be the next node in the ring in a counter-clockwise direction.
- Note that a ring port cannot be configured as a member of a spanning tree, a dynamic trunk, or a static trunk.
- If a port channel (static trunk) is specified as a ring port, it can not be destroyed before it is removed from the domain configuration.
- A static trunk will be treated as a signal fault, if it contains no member ports or all of its member ports are in signal fault.
- If a static trunk is configured as a ring port prior to assigning any member ports, spanning tree will be disabled for the first member port assigned to the static trunk.

EXAMPLE

```
Console(config-erps)#ring-port east interface ethernet 1/12
Console(config-erps)#
```

rpl neighbor

This command configures a ring node to be the Ring Protection Link (RPL) neighbor. Use the **no** form to restore the default setting.

SYNTAX

rpl neighbor

no rpl

DEFAULT SETTING

None (that is, neither owner nor neighbor)

COMMAND MODE

ERPS Configuration

COMMAND USAGE

- The RPL neighbor node, when configured, is a ring node adjacent to the RPL that is responsible for blocking its end of the RPL under normal conditions (i.e., the ring is established and no requests are present in the ring) in addition to the block at the other end by the RPL Owner Node. The RPL neighbor node may participate in blocking or unblocking its end of the RPL, but is not responsible for activating the reversion behavior.
- Only one RPL owner can be configured on a ring. If the switch is set as the RPL owner for an ERPS domain, the west ring port is set as one end

of the RPL. If the switch is set as the RPL neighbor for an ERPS domain, the east ring port is set as the other end of the RPL.

- The east and west connections to the ring must be specified for all ring nodes using the ring-port command. When this switch is configured as the RPL neighbor, the east ring port is set as being connected to the RPL.

- Note that is not mandatory to declare a RPL neighbor.

EXAMPLE

```
Console(config-erps)#rpl neighbor
Console(config-erps)#
```

rpl owner

This command configures a ring node to be the Ring Protection Link (RPL) owner. Use the **no** form to restore the default setting.

SYNTAX

rpl owner

no rpl

DEFAULT SETTING

None (that is, neither owner nor neighbor)

COMMAND MODE

ERPS Configuration

COMMAND USAGE

- Only one RPL owner can be configured on a ring. The owner blocks traffic on the RPL during Idle state, and unblocks it during Protection state (that is, when a signal fault is detected on the ring or the protection state is enabled with the erps forced-switch or erps manual-switch command).

- The east and west connections to the ring must be specified for all ring nodes using the ring-port command. When this switch is configured as the RPL owner, the west ring port is automatically set as being connected to the RPL.

EXAMPLE

```
Console(config-erps)#rpl owner
Console(config-erps)#
```

version

This command specifies compatibility with ERPS version 1 or 2.

Syntax

version {**1** | **2**}

1 - ERPS version 1 based on ITU-T G.8032/Y.1344.

2 - ERPS version 2 based on ITU-T G.8032/Y.1344 Version 2.

Default Setting

2

Command Mode

ERPS Configuration

Command Usage

- In addition to the basic features provided by version 1, version 2 also supports:
  - Multi-ring/ladder network support
  - Revertive/Non-revertive recovery
  - Forced Switch (FS) and Manual Switch (MS) commands for manually blocking a particular ring port
  - Flush FDB (forwarding database) logic which reduces amount of flush FDB operations in the ring
  - Support of multiple ERP instances on a single ring
- Version 2 is backward compatible with Version 1. If version 2 is specified, the inputs and commands are forwarded transparently. If set to version 1, MS and FS operator commands are filtered, and the switch set to revertive mode.
- The version number is automatically set to “1” when a ring node, supporting only the functionalities of G.8032v1, exists on the same ring with other nodes that support G.8032v2.
- When ring nodes running G.8032v1 and G.8032v2 co-exist on a ring, the ring ID of each node is configured as “1”.
- In version 1, the MAC address 01-19-A7-00-00-01 is used for the node identifier. The raps-def-mac command has no effect.

Example

```
Console(config-erps)#version 1
Console(config-erps)#
```

wtr-timer

This command sets the wait-to-restore timer which is used to verify that the ring has stabilized before blocking the RPL after recovery from a signal failure. Use the **no** form to restore the default setting.

SYNTAX

wtr-timer *minutes*

minutes - The wait-to-restore timer is used to verify that the ring has stabilized before blocking the RPL after recovery from a signal failure. (Range: 5-12 minutes)

DEFAULT SETTING

5 minutes

COMMAND MODE

ERPS Configuration

COMMAND USAGE

If the switch goes into ring protection state due to a signal failure, after the failure condition is cleared, the RPL owner will start the wait-to-restore timer and wait until it expires to verify that the ring has stabilized before blocking the RPL and returning to the Idle (normal operating) state.

EXAMPLE

```
Console(config-erps)#wtr-timer 10
Console(config-erps)#
```

clear erps statistics

This command clears statistics, including SF, NR, NR-RB, FS, MS, Event, and Health protocol messages.

SYNTAX

clear erps statistics [**domain** *ring-name*]

ring-name - Name of a specific ERPS ring. (Range: 1-12 characters)

COMMAND MODE

Privileged Exec

EXAMPLE

```
Console#clear erps statistics domain r&d
Console#
```

erps clear

This command manually clears the protection state which has been invoked by a forced switch or manual switch command, and the node is operating under non-revertive mode; or before the WTR or WTB timer expires when the node is operating in revertive mode.

SYNTAX

erps clear domain *ring-name*

ring-name - Name of a specific ERPS ring. (Range: 1-12 characters)

COMMAND MODE

Privileged Exec

COMMAND USAGE

- Two steps are required to make a ring operating in non-revertive mode return to Idle state from forced switch or manual switch state:

  1. Issue an **erps clear** command to remove the forced switch command on the node where a local forced switch command is active.

  2. Issue an **erps clear** command on the RPL owner node to trigger the reversion.

- The **erps clear** command will also stop the WTR and WTB delay timers and reset their values.

- More detailed information about using this command for non-revertive mode is included under the Command Usage section for the non-revertive command.

EXAMPLE

```
Console#erps clear domain r&d
Console#
```

erps forced-switch

This command blocks the specified ring port.

SYNTAX

erps forced-switch [**domain** *ring-name*] {**east** | **west**}

ring-name - Name of a specific ERPS ring. (Range: 1-12 characters)

east - East ring port.

west - West ring port.

COMMAND MODE

Privileged Exec

COMMAND USAGE

- A ring with no pending request has a logical topology with the traffic channel blocked at the RPL and unblocked on all other ring links. In this situation, the **erps forced-switch** command triggers protection switching as follows:

  a. The ring node where a forced switch command was issued blocks the traffic channel and R-APS channel on the ring port to which the command was issued, and unblocks the other ring port.

  b. The ring node where the forced switch command was issued transmits R-APS messages indicating FS over both ring ports. R-APS (FS) messages are continuously transmitted by this ring node while the local FS command is the ring node's highest priority command (see Table 155 on page 1328). The R-APS (FS) message informs other ring nodes of the FS command and that the traffic channel is blocked on one ring port.

  c. A ring node accepting an R-APS (FS) message, without any local higher priority requests unblocks any blocked ring port. This action subsequently unblocks the traffic channel over the RPL.

  d. The ring node accepting an R-APS (FS) message, without any local higher priority requests stops transmission of R-APS messages.

  e. The ring node receiving an R-APS (FS) message flushes its FDB.

- Protection switching on a forced switch request is completed when the above actions are performed by each ring node. At this point, traffic flows around the ring are resumed. From this point on the following rules apply regarding processing of further forced switch commands:

  While an existing forced switch request is present in a ring, any new forced switch request is accepted, except on a ring node having a prior local forced switch request. The ring nodes where further forced switch commands are issued block the traffic channel and R-APS channel on the ring port at which the forced switch was issued. The ring node where the forced switch command was issued transmits an R-APS message over both ring ports indicating FS. R-APS (FS) messages are continuously transmitted by this ring node while the local FS command is the ring node's highest priority command. As such, two or more forced switches are allowed in the ring, which may inadvertently cause the segmentation of an ring. It is the responsibility of the operator to prevent this effect if it is undesirable.

  Ring protection requests, commands and R-APS signals have the priorities as specified in the following table.

Table 155: ERPS Request/State Priority

Request / State and Status	Type	Priority
Clear	local	highest
FS	local	|

Table 155: ERPS Request/State Priority (Continued)

Request / State and Status	Type	Priority
R-APS (FS)	remote	|
local SF*	local	|
local clear SF	local	|
R-APS (SF)	remote	|
R-APS (MS)	remote	|
MS	local	|
WTR Expires	local	|
WTR Running	local	|
WTB Expires	local	|
WTB Running	local	|
R-APS (NR, RB)	remote	|
R-APS (NR)	remote	lowest

* If an Ethernet Ring Node is in the Forced Switch state, local SF is ignored.

- Recovery for forced switching under revertive and non-revertive mode is described under the Command Usage section for the non-revertive command.

- When a ring is under an FS condition, and the node at which an FS command was issued is removed or fails, the ring remains in FS state because the FS command can only be cleared at node where the FS command was issued. This results in an unrecoverable FS condition.

  When performing a maintenance procedure (e.g., replacing, upgrading) on a ring node (or a ring link), it is recommended that FS commands be issued at the two adjacent ring nodes instead of directly issuing a FS command at the ring node under maintenance in order to avoid falling into the above mentioned unrecoverable situation.

EXAMPLE

```
Console#erps forced-switch domain r&d west
Console#
```

erps manual-switch

This command blocks the specified ring port, in the absence of a failure or an erps forced-switch command.

SYNTAX

erps manual-switch [**domain** *ring-name*] {**east** | **west**}

ring-name - Name of a specific ERPS ring. (Range: 1-12 characters)

east - East ring port.

west - West ring port.

COMMAND MODE

Privileged Exec

COMMAND USAGE

- A ring with no request has a logical topology with the traffic channel blocked at the RPL and unblocked on all other ring links. In this situation, the **erps manual-switch** command triggers protection switching as follows:

  a. If no other higher priority commands exist, the ring node, where a manual switch command was issued, blocks the traffic channel and R-APS channel on the ring port to which the command was issued, and unblocks the other ring port.

  b. If no other higher priority commands exist, the ring node where the manual switch command was issued transmits R-APS messages over both ring ports indicating MS. R-APS (MS) message are continuously transmitted by this ring node while the local MS command is the ring node's highest priority command (see Table 155 on page 1328). The R-APS (MS) message informs other ring nodes of the MS command and that the traffic channel is blocked on one ring port.

  c. If no other higher priority commands exist and assuming the ring node was in Idle state before the manual switch command was issued, the ring node flushes its local FDB.

  d. A ring node accepting an R-APS (MS) message, without any local higher priority requests unblocks any blocked ring port which does not have an SF condition. This action subsequently unblocks the traffic channel over the RPL.

  e. A ring node accepting an R-APS (MS) message, without any local higher priority requests stops transmitting R-APS messages.

  f. A ring node receiving an R-APS (MS) message flushes its FDB.

- Protection switching on a manual switch request is completed when the above actions are performed by each ring node. At this point, traffic flows around the ring are resumed. From this point on, the following rules apply regarding processing of further manual switch commands:

  a. While an existing manual switch request is present in the ring, any new manual switch request is rejected. The request is rejected at the ring node where the new request is issued and a notification is generated to inform the operator that the new MS request was not accepted.

  b. A ring node with a local manual switch command which receives an R-APS (MS) message with a different Node ID clears its manual switch request and starts transmitting R-APS (NR) messages. The ring node keeps the ring port blocked due to the previous manual switch command.

c. An ring node with a local manual switch command that receives an R-APS message or a local request of higher priority than R-APS (MS) clear its manual switch request. The ring node then processes the new higher priority request.

- Recovery for manual switching under revertive and non-revertive mode is described under the Command Usage section for the non-revertive command.

EXAMPLE

```
Console#erps manual-switch domain r&d west
Console#
```

show erps

This command displays status information for all configured rings, or for a specified ring

SYNTAX

show erps [**domain** *ring-name*] [**statistics**]

domain - Keyword to display ERPS ring configuration settings.

ring-name - Name of a specific ERPS ring. (Range: 1-32 characters)

statistics - Keyword to display ERPS ring statistics.

COMMAND MODE

Privileged Exec

EXAMPLE

This example displays a summary of all the ERPS rings configured on the switch.

```
Console#show erps
ERPS Status             : Enabled
Number of ERPS Domains  : 1

Domain       ID  Enabled Ver MEL Ctrl VLAN State      Type         Revertive
------------ --- ------- --- --- --------- ---------- ------------ ---------
r&d            1 Yes       2   1         1 Idle       RPL Owner    Yes

             W/E  Interface Port State Local SF Local FS Local MS MEP  RPL
             ---- --------- ---------- -------- -------- -------- ---- ---
             West Eth 1/ 1  Blocking   No       No       No            Yes
             East Eth 1/ 3  Forwarding No       No       No            No


Console#
```

Table 156: **show erps** - summary display description

Field	**Description**
Node Information	
ERPS Status	Shows whether ERPS is enabled on the switch.
Number of ERPS Domains	Shows the number of ERPS rings configured on the switch.
Domain	Displays the name of each ring followed by a brief list of status information
ID	ERPS ring identifier used in R-APS messages.
Enabled	Shows if the specified ring is enabled.
Ver	Shows the ERPS version.
MEL	The maintenance entity group (MEG) level providing a communication channel for ring automatic protection switching (R-APS) information.
Ctrl VLAN	Shows the Control VLAN ID.
State	Shows the following ERPS states: Init – The ERPS ring has started but has not yet determined the status of the ring. Idle – If all nodes in a ring are in this state, it means that all the links in the ring are up. This state will switch to protection state if a link failure occurs. Protection – If a node in this state, it means that a link failure has occurred. This state will switch to idle state if all the failed links recover.
Type	Shows ERPS node type as None, RPL Owner or RPL Neighbor.
Revertive	Shows if revertive or non-revertive recovery is selected.
Interface Information	
W/E	Shows information on the west and east ring port for this node.
Interface	The port or trunk which is configured as a ring port.
Port State	The operational state: Blocking – The transmission and reception of traffic is blocked and the forwarding of R-APS messages is blocked, but the transmission of locally generated R-APS messages is allowed and the reception of all R-APS messages is allowed. Forwarding – The transmission and reception of traffic is allowed; transmission, reception and forwarding of R-APS messages is allowed. Unknown – The interface is not in a known state (includes the domain being disabled).
Local SF	A signal fault generated on a link to the local node.
Local FS	Shows if a forced switch command was issued on this interface.
Local MS	Shows if a manual switch command was issued on this interface.
MEP	The CFM MEP used to monitor the status on this link.
RPL	Shows if this node is connected to the RPL.

This example displays detailed information for the specified ERPS ring.

```
Console#show erps domain rd1
Domain       ID  Enabled Ver MEL Ctrl VLAN State      Type         Revertive
------------ --- ------- --- --- --------- ---------- ------------ ---------
r&d            1 Yes       2   1         1 Idle       RPL Owner    Yes

             Major Domain Node ID           R-APS With VC
             ------------ ----------------- -------------
                          00-E0-0C-00-00-FD Yes

             R-APS Def MAC Propagate TC Non-ERPS Device Protect
             ------------- ------------ -----------------------
             Yes           No           No

             Holdoff  Guard   WTB     WTR     WTB Expire WTR Expire
             -------- ------- ------- ------- ---------- ----------
                 0 ms  500 ms 5500 ms   5 min

             W/E  Interface Port State Local SF Local FS Local MS MEP  RPL
             ---- --------- ---------- -------- -------- -------- ---- ---
             West Eth 1/ 1  Blocking   No       No       No             Yes
             East Eth 1/ 3  Forwarding No       No       No             No

Console#
```

Table 156 on page 1332 describes most of the parameters shown by **show erps domain** command. The following table includes the remaining parameters.

Table 157: **show erps domain** - detailed display description

Field	Description
Major Domain	Name of the ERPS major domain.
Node ID	A MAC address unique to this ring node.
R-APS with VC	The R-APS Virtual Channel is the R-APS channel connection used to tunnel R-APS messages between two interconnection nodes of a sub-ring in another Ethernet ring or network.
R-APS Def MAC	Indicates if the switch’s MAC address is used to identify the node in R-APS messages.
Propagate TC	Shows if the ring is configured to propagate topology change notification messages.
Non-ERPS Device Protect	Shows if the RPL owner node is configured to send non-standard health-check packets when it enters protection state without any link down event having been detected through SF messages
Holdoff	The hold-off timer interval used to filter out intermittent link faults.
Guard	The guard timer interval used to prevent ring nodes from receiving outdated R-APS messages.
WTB	The wait-to-block timer interval used to delay reversion after a Forced Switch or Manual Switch has been cleared.
WTR	The wait-to-restore timer interval used to verify that the ring has stabilized before blocking the RPL after recovery from a signal failure.

Table 157: **show erps domain** - detailed display description (Continued)

Field	Description
WTB Expire	The time before the wait-to-block timer expires.
WTR Expire	The time before the wait-to-restore timer expires.

This example displays statistics for all configured ERPS rings.

```
Console#show erps statistics
ERPS statistics for domain r&d :
Interface    Local SF   Local Clear SF
------------ ---------- --------------
(W) Eth 1/ 1 0          0
             SF         NR         NR-RB      FS         MS
             ---------- ---------- ---------- ---------- ----------
    Sent              0         62        948          0          0
    Received          0          0          0          0          0
    Ignored           0          0          0          0          0
             EVENT      HEALTH
             ---------- ----------
    Sent              0          0
    Received          0          0
    Ignored           0          0

Interface    Local SF   Local Clear SF
------------ ---------- --------------
(E) Eth 1/ 3 0          0
             SF         NR         NR-RB      FS         MS
             ---------- ---------- ---------- ---------- ----------
    Sent              0         62        948          0          0
    Received          0          0          0          0          0
    Ignored           0          0          0          0          0
             EVENT      HEALTH
             ---------- ----------
    Sent              0          0
    Received          0          0
    Ignored           0          0

Console#
```

Table 158: **show erps statistics** - detailed display description

Field	Description
Interface	The direction, and port or trunk which is configured as a ring port.
Local SF	A signal fault generated on a link to the local node.
Local Clear SF	The number of times a clear command was issued to terminate protection state entered through a forced switch or manual switch
SF	The number of signal fault messages
NR	The number of no request messages
NR-RB	The number no request - RPL blocked messages
FS	The number of forced switch messages
MS	The number of manual switch messages

Table 158: **show erps statistics** - detailed display description (Continued)

Field	**Description**
EVENT	Any request/state message, excluding FS, SF, MS, and NR
HEALTH	The number of non-standard health-check messages

40 VLAN Commands

A VLAN is a group of ports that can be located anywhere in the network, but communicate as though they belong to the same physical segment. This section describes commands used to create VLAN groups, add port members, specify how VLAN tagging is used, and enable automatic VLAN registration for the selected interface.

Table 159: VLAN Commands

Command Group	Function
GVRP and Bridge Extension Commands	Configures GVRP settings that permit automatic VLAN learning; shows the configuration for bridge extension MIB
Editing VLAN Groups	Sets up VLAN groups, including name, VID and state
Configuring VLAN Interfaces	Configures VLAN interface parameters, including ingress and egress tagging mode, ingress filtering, PVID, and GVRP
Displaying VLAN Information	Displays VLAN groups, status, port members, and MAC addresses
Configuring IEEE 802.1Q Tunneling	Configures 802.1Q Tunneling (QinQ Tunneling)
Configuring L2CP Tunneling*	Configures Layer 2 Control Protocol (L2CP) tunneling, either by discarding, processing, or transparently passing control packets across a QinQ tunnel
Configuring VLAN Translation*	Maps VLAN ID between customer and service provider for networks that do not support IEEE 802.1Q tunneling
Configuring Private VLANs	Configures private VLANs, including uplink and downlink ports
Configuring Protocol-based VLANs	Configures protocol-based VLANs based on frame type and protocol
Configuring IP Subnet VLANs	Configures IP Subnet-based VLANs
Configuring MAC Based VLANs	Configures MAC-based VLANs
Configuring Voice VLANs	Configures VoIP traffic detection and enables a Voice VLAN

* These functions are not compatible.

GVRP AND BRIDGE EXTENSION COMMANDS

GARP VLAN Registration Protocol defines a way for switches to exchange VLAN information in order to automatically register VLAN members on interfaces across the network. This section describes how to enable GVRP for individual interfaces and globally for the switch, as well as how to display default configuration settings for the Bridge Extension MIB.

Table 160: GVRP and Bridge Extension Commands

Command	Function	Mode
bridge-ext gvrp	Enables GVRP globally for the switch	GC
garp timer	Sets the GARP timer for the selected function	IC
switchport forbidden vlan	Configures forbidden VLANs for an interface	IC
switchport gvrp	Enables GVRP for an interface	IC
show bridge-ext	Shows the global bridge extension configuration	PE
show garp timer	Shows the GARP timer for the selected function	NE, PE
show gvrp configuration	Displays GVRP configuration for the selected interface	NE, PE

bridge-ext gvrp

This command enables GVRP globally for the switch. Use the **no** form to disable it.

SYNTAX

[**no**] **bridge-ext gvrp**

DEFAULT SETTING

Disabled

COMMAND MODE

Global Configuration

COMMAND USAGE

GVRP defines a way for switches to exchange VLAN information in order to register VLAN members on ports across the network. This function should be enabled to permit automatic VLAN registration, and to support VLANs which extend beyond the local switch.

EXAMPLE

```
Console(config)#bridge-ext gvrp
Console(config)#
```

garp timer

This command sets the values for the join, leave and leaveall timers. Use the **no** form to restore the timers' default values.

SYNTAX

garp timer {**join** | **leave** | **leaveall**} *timer-value*

no garp timer {**join** | **leave** | **leaveall**}

{**join** | **leave** | **leaveall**} - Timer to set.

timer-value - Value of timer.
Ranges:
join: 20-1000 centiseconds
leave: 60-3000 centiseconds
leaveall: 500-18000 centiseconds

DEFAULT SETTING

join: 20 centiseconds
leave: 60 centiseconds
leaveall: 1000 centiseconds

COMMAND MODE

Interface Configuration (Ethernet, Port Channel)

COMMAND USAGE

- Group Address Registration Protocol is used by GVRP and GMRP to register or deregister client attributes for client services within a bridged LAN. The default values for the GARP timers are independent of the media access method or data rate. These values should not be changed unless you are experiencing difficulties with GMRP or GVRP registration/deregistration.
- Timer values are applied to GVRP for all the ports on all VLANs.
- Timer values must meet the following restrictions:
  - leave >= (3 x join)
  - leaveall > leave

NOTE: Set GVRP timers on all Layer 2 devices connected in the same network to the same values. Otherwise, GVRP may not operate successfully.

EXAMPLE

```
Console(config)#interface ethernet 1/1
Console(config-if)#garp timer join 100
Console(config-if)#
```

RELATED COMMANDS

show garp timer (1341)

switchport forbidden vlan

This command configures forbidden VLANs. Use the **no** form to remove the list of forbidden VLANs.

SYNTAX

switchport forbidden vlan {**add** *vlan-list* | **remove** *vlan-list*}

no switchport forbidden vlan

add *vlan-list* - List of VLAN identifiers to add.

remove *vlan-list* - List of VLAN identifiers to remove.

vlan-list - Separate nonconsecutive VLAN identifiers with a comma and no spaces; use a hyphen to designate a range of IDs. (Range: 1-4094).

DEFAULT SETTING

No VLANs are included in the forbidden list.

COMMAND MODE

Interface Configuration (Ethernet, Port Channel)

COMMAND USAGE

- This command prevents a VLAN from being automatically added to the specified interface via GVRP.
- If a VLAN has been added to the set of allowed VLANs for an interface, then you cannot add it to the set of forbidden VLANs for that same interface.

EXAMPLE

The following example shows how to prevent port 1 from being added to VLAN 3:

```
Console(config)#interface ethernet 1/1
Console(config-if)#switchport forbidden vlan add 3
Console(config-if)#
```

switchport gvrp

This command enables GVRP for a port. Use the **no** form to disable it.

SYNTAX

[**no**] **switchport gvrp**

DEFAULT SETTING

Disabled

COMMAND MODE

Interface Configuration (Ethernet, Port Channel)

EXAMPLE

```
Console(config)#interface ethernet 1/1
Console(config-if)#switchport gvrp
Console(config-if)#
```

show bridge-ext

This command shows the configuration for bridge extension commands.

DEFAULT SETTING

None

COMMAND MODE

Privileged Exec

COMMAND USAGE

See "Displaying Bridge Extension Capabilities" on page 153 for a description of the displayed items.

EXAMPLE

```
Console#show bridge-ext
 Maximum Supported VLAN Numbers         : 4094
 Maximum Supported VLAN ID              : 4094
 Extended Multicast Filtering Services : No
 Static Entry Individual Port           : Yes
 VLAN Learning                          : IVL
 Configurable PVID Tagging              : Yes
 Local VLAN Capable                     : No
 Traffic Classes                        : Enabled
 Global GVRP Status                     : Disabled
Console#
```

show garp timer

This command shows the GARP timers for the selected interface.

SYNTAX

show garp timer [*interface*]

interface

ethernet *unit*/*port*

unit - Unit identifier. (Range: 1)

port - Port number. (Range: 1-28)

port-channel *channel-id* (Range: 1-8)

DEFAULT SETTING

Shows all GARP timers.

COMMAND MODE

Normal Exec, Privileged Exec

EXAMPLE

```
Console#show garp timer ethernet 1/1
Eth 1/ 1 GARP Timer Status:
 Join Timer      : 20 centiseconds
 Leave Timer     : 60 centiseconds
 Leave All Timer : 1000 centiseconds
Console#
```

RELATED COMMANDS

garp timer (1339)

show gvrp configuration

This command shows if GVRP is enabled.

SYNTAX

show gvrp configuration [*interface*]

interface

ethernet *unit*/*port*

unit - Unit identifier. (Range: 1)

port - Port number. (Range: 1-28)

port-channel *channel-id* (Range: 1-8)

DEFAULT SETTING

Shows both global and interface-specific configuration.

COMMAND MODE

Normal Exec, Privileged Exec

EXAMPLE

```
Console#show gvrp configuration ethernet 1/7
Eth 1/ 7:
 GVRP Configuration : Disabled
Console#
```

EDITING VLAN GROUPS

Table 161: Commands for Editing VLAN Groups

Command	Function	Mode
vlan database	Enters VLAN database mode to add, change, and delete VLANs	GC
vlan	Configures a VLAN, including VID, name and state	VC

vlan database

This command enters VLAN database mode. All commands in this mode will take effect immediately.

DEFAULT SETTING

None

COMMAND MODE

Global Configuration

COMMAND USAGE

- Use the VLAN database command mode to add, change, and delete VLANs. After finishing configuration changes, you can display the VLAN settings by entering the show vlan command.

- Use the interface vlan command mode to define the port membership mode and add or remove ports from a VLAN. The results of these commands are written to the running-configuration file, and you can display this file by entering the show running-config command.

EXAMPLE

```
Console(config)#vlan database
Console(config-vlan)#
```

RELATED COMMANDS

show vlan (1352)

vlan

This command configures a VLAN. Use the **no** form to restore the default settings or delete a VLAN.

SYNTAX

vlan *vlan-id* [**name** *vlan-name*] **media ethernet**
[**state** {**active** | **suspend**}] [**rspan**]

no vlan *vlan-id* [**name** | **state**]

vlan-id - VLAN ID, specified as a single number, a range of consecutive numbers separated by a hyphen, or multiple numbers separated by commas. (Range: 1-4094)

name - Keyword to be followed by the VLAN name.

vlan-name - ASCII string from 1 to 32 characters.

media ethernet - Ethernet media type.

state - Keyword to be followed by the VLAN state.

active - VLAN is operational.

suspend - VLAN is suspended. Suspended VLANs do not pass packets.

rspan - Keyword to create a VLAN used for mirroring traffic from remote switches. The VLAN used for RSPAN cannot include VLAN 1 (the switch's default VLAN). For more information on configuring RSPAN through the CLI, see "RSPAN Mirroring Commands" on page 1231.

DEFAULT SETTING

By default only VLAN 1 exists and is active.

COMMAND MODE

VLAN Database Configuration

COMMAND USAGE

- **no vlan** *vlan-id* deletes the VLAN.
- **no vlan** *vlan-id* **name** removes the VLAN name.
- **no vlan** *vlan-id* **state** returns the VLAN to the default state (i.e., active).
- You can configure up to 4094 VLANs on the switch.

NOTE: The switch allows 256 user-manageable VLANs.

EXAMPLE

The following example adds a VLAN, using VLAN ID 105 and name RD5. The VLAN is activated by default.

```
Console(config)#vlan database
Console(config-vlan)#vlan 105 name RD5 media ethernet
Console(config-vlan)#
```

RELATED COMMANDS

show vlan (1352)

CONFIGURING VLAN INTERFACES

Table 162: Commands for Configuring VLAN Interfaces

Command	Function	Mode
interface vlan	Enters interface configuration mode for a specified VLAN	IC
switchport acceptable-frame-types	Configures frame types to be accepted by an interface	IC
switchport allowed vlan	Configures the VLANs associated with an interface	IC
switchport forbidden vlan	Configures forbidden VLANs for an interface	IC
switchport gvrp	Enables GVRP for an interface	IC
switchport ingress-filtering	Enables ingress filtering on an interface	IC
switchport mode	Configures VLAN membership mode for an interface	IC
switchport native vlan	Configures the PVID (native VLAN) of an interface	IC
switchport priority default	Sets a port priority for incoming untagged frames	IC
vlan-trunking	Allows unknown VLANs to cross the switch	IC

interface vlan

This command enters interface configuration mode for VLANs, which is used to configure VLAN parameters for a physical interface. Use the **no** form to change a Layer 3 normal VLAN back to a Layer 2 interface.

SYNTAX

[**no**] **interface vlan** *vlan-id*

vlan-id - ID of the configured VLAN. (Range: 1-4094)

DEFAULT SETTING

None

COMMAND MODE

Global Configuration

Command Usage

- Creating a "normal" VLAN with the vlan command initializes it as a Layer 2 interface. To change it to a Layer 3 interface, use the interface command to enter interface configuration for the desired VLAN, enter any Layer 3 configuration commands, and save the configuration settings.
- To change a Layer 3 normal VLAN back to a Layer 2 VLAN, use the no interface command.

Example

The following example shows how to set the interface configuration mode to VLAN 1, and then assign an IP address to the VLAN:

```
Console(config)#interface vlan 1
Console(config-if)#ip address 192.168.1.254 255.255.255.0
Console(config-if)#
```

Related Commands

shutdown (1194)
interface (1188)
vlan (1344)

switchport acceptable-frame-types

This command configures the acceptable frame types for a port. Use the **no** form to restore the default.

Syntax

switchport acceptable-frame-types {**all** | **tagged**}

no switchport acceptable-frame-types

all - The port accepts all frames, tagged or untagged.

tagged - The port only receives tagged frames.

Default Setting

All frame types

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

When set to receive all frame types, any received frames that are untagged are assigned to the default VLAN.

EXAMPLE

The following example shows how to restrict the traffic received on port 1 to tagged frames:

```
Console(config)#interface ethernet 1/1
Console(config-if)#switchport acceptable-frame-types tagged
Console(config-if)#
```

RELATED COMMANDS

switchport mode (1349)

switchport allowed vlan

This command configures VLAN groups on the selected interface. Use the **no** form to restore the default.

SYNTAX

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

no switchport allowed vlan

add *vlan-list* - List of VLAN identifiers to add.

remove *vlan-list* - List of VLAN identifiers to remove.

vlan-list - Separate nonconsecutive VLAN identifiers with a comma and no spaces; use a hyphen to designate a range of IDs. Do not enter leading zeros. (Range: 1-4094).

DEFAULT SETTING

All ports are assigned to VLAN 1 by default.
The default frame type is untagged.

COMMAND MODE

Interface Configuration (Ethernet, Port Channel)

COMMAND USAGE

- A port, or a trunk with switchport mode set to **hybrid**, must be assigned to at least one VLAN as untagged.
- If a trunk has switchport mode set to **trunk** (i.e., 1Q Trunk), then you can only assign an interface to VLAN groups as a tagged member.
- Frames are always tagged within the switch. The tagged/untagged parameter used when adding a VLAN to an interface tells the switch whether to keep or remove the tag from a frame on egress.
- If none of the intermediate network devices nor the host at the other end of the connection supports VLANs, the interface should be added to these VLANs as an untagged member. Otherwise, it is only necessary to add at most one VLAN as untagged, and this should correspond to the native VLAN for the interface.

- If a VLAN on the forbidden list for an interface is manually added to that interface, the VLAN is automatically removed from the forbidden list for that interface.

EXAMPLE

The following example shows how to add VLANs 1, 2, 5 and 6 to the allowed list as tagged VLANs for port 1:

```
Console(config)#interface ethernet 1/1
Console(config-if)#switchport allowed vlan add 1,2,5,6 tagged
Console(config-if)#
```

switchport ingress-filtering

This command enables ingress filtering for an interface. Use the **no** form to restore the default.

SYNTAX

[**no**] **switchport ingress-filtering**

DEFAULT SETTING

Disabled

COMMAND MODE

Interface Configuration (Ethernet, Port Channel)

COMMAND USAGE

- Ingress filtering only affects tagged frames.
- If ingress filtering is disabled and a port receives frames tagged for VLANs for which it is not a member, these frames will be flooded to all other ports (except for those VLANs explicitly forbidden on this port).
- If ingress filtering is enabled and a port receives frames tagged for VLANs for which it is not a member, these frames will be discarded.
- Ingress filtering does not affect VLAN independent BPDU frames, such as GVRP or STA. However, they do affect VLAN dependent BPDU frames, such as GMRP.

EXAMPLE

The following example shows how to set the interface to port 1 and then enable ingress filtering:

```
Console(config)#interface ethernet 1/1
Console(config-if)#switchport ingress-filtering
Console(config-if)#
```

switchport mode

This command configures the VLAN membership mode for a port. Use the **no** form to restore the default.

SYNTAX

switchport mode {**hybrid** | **trunk** | **private-vlan**}

no switchport mode

hybrid - Specifies a hybrid VLAN interface. The port may transmit tagged or untagged frames.

trunk - Specifies a port as an end-point for a VLAN trunk. A trunk is a direct link between two switches, so the port transmits tagged frames that identify the source VLAN. Note that frames belonging to the port's default VLAN (i.e., associated with the PVID) are also transmitted as tagged frames.

private-vlan - For an explanation of this command see the switchport mode private-vlan command.

DEFAULT SETTING

All ports are in hybrid mode with the PVID set to VLAN 1.

COMMAND MODE

Interface Configuration (Ethernet, Port Channel)

EXAMPLE

The following shows how to set the configuration mode to port 1, and then set the switchport mode to hybrid:

```
Console(config)#interface ethernet 1/1
Console(config-if)#switchport mode hybrid
Console(config-if)#
```

RELATED COMMANDS

switchport acceptable-frame-types (1346)

switchport native vlan

This command configures the PVID (i.e., default VLAN ID) for a port. Use the **no** form to restore the default.

SYNTAX

switchport native vlan *vlan-id*

no switchport native vlan

vlan-id - Default VLAN ID for a port. (Range: 1-4094)

DEFAULT SETTING

VLAN 1

COMMAND MODE

Interface Configuration (Ethernet, Port Channel)

COMMAND USAGE

- When using Access mode, and an interface is assigned to a new VLAN, its PVID is automatically set to the identifier for that VLAN. When using Hybrid mode, the PVID for an interface can be set to any VLAN for which it is an untagged member.
- If acceptable frame types is set to **all** or switchport mode is set to **hybrid**, the PVID will be inserted into all untagged frames entering the ingress port.

EXAMPLE

The following example shows how to set the PVID for port 1 to VLAN 3:

```
Console(config)#interface ethernet 1/1
Console(config-if)#switchport native vlan 3
Console(config-if)#
```

vlan-trunking

This command allows unknown VLAN groups to pass through the specified interface. Use the **no** form to disable this feature.

SYNTAX

[**no**] **vlan-trunking**

DEFAULT SETTING

Disabled

COMMAND MODE

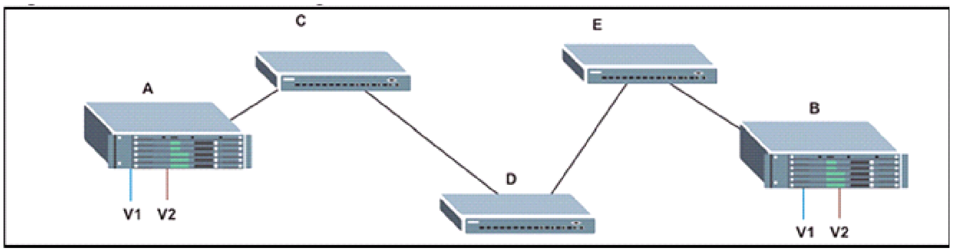
Interface Configuration (Ethernet, Port Channel)

COMMAND USAGE

- Use this command to configure a tunnel across one or more intermediate switches which pass traffic for VLAN groups to which they do not belong.

The following figure shows VLANs 1 and 2 configured on switches A and B, with VLAN trunking being used to pass traffic for these VLAN groups across switches C, D and E.

Figure 552: Configuring VLAN Trunking



Without VLAN trunking, you would have to configure VLANs 1 and 2 on all intermediate switches – C, D and E; otherwise these switches would drop any frames with unknown VLAN group tags. However, by enabling VLAN trunking on the intermediate switch ports along the path connecting VLANs 1 and 2, you only need to create these VLAN groups in switches A and B. Switches C, D and E automatically allow frames with VLAN group tags 1 and 2 (groups that are unknown to those switches) to pass through their VLAN trunking ports.

- To prevent loops from forming in the spanning tree, all unknown VLANs will be bound to a single instance (either STP/RSTP or an MSTP instance, depending on the selected STA mode).

- If both VLAN trunking and ingress filtering are disabled on an interface, packets with unknown VLAN tags will still be allowed to enter this interface and will be flooded to all other ports where VLAN trunking is enabled. (In other words, VLAN trunking will still be effectively enabled for the unknown VLAN).

EXAMPLE

The following example enables VLAN trunking on ports 9 and 10 to establish a path across the switch for unknown VLAN groups:

```
Console(config)#interface ethernet 1/9
Console(config-if)#vlan-trunking
Console(config-if)#interface ethernet 1/10
Console(config-if)#vlan-trunking
Console(config-if)#
```

DISPLAYING VLAN INFORMATION

This section describes commands used to display VLAN information.

Table 163: Commands for Displaying VLAN Information

Command	Function	Mode
show interfaces status vlan	Displays status for the specified VLAN interface	NE, PE
show interfaces switchport	Displays the administrative and operational status of an interface	NE, PE
show vlan	Shows VLAN information	NE, PE

show vlan

This command shows VLAN information.

SYNTAX

show vlan [**id** *vlan-id* | **name** *vlan-name* |
private-vlan *private-vlan-type*]

id - Keyword to be followed by the VLAN ID.

vlan-id - ID of the configured VLAN. (Range: 1-4094)

name - Keyword to be followed by the VLAN name.

vlan-name - ASCII string from 1 to 32 characters.

private-vlan - For an explanation of this command see the show vlan private-vlan command.

private-vlan-type - Indicates the private VLAN type. (Options: community, primary)

DEFAULT SETTING

Shows all VLANs.

COMMAND MODE

Normal Exec, Privileged Exec

EXAMPLE

The following example shows how to display information for VLAN 1:

```
Console#show vlan id 1

VLAN ID             : 1
Type                : Static
Name                : DefaultVlan
Status              : Active
Ports/Port Channels : Eth1/ 1(S) Eth1/ 2(S) Eth1/ 3(S) Eth1/ 4(S) Eth1/ 5(S)
                      Eth1/ 6(S) Eth1/ 7(S) Eth1/ 8(S) Eth1/ 9(S) Eth1/10(S)
                      Eth1/11(S) Eth1/12(S) Eth1/13(S) Eth1/14(S) Eth1/15(S)
                      Eth1/16(S) Eth1/17(S) Eth1/18(S) Eth1/19(S) Eth1/20(S)
                      Eth1/21(S) Eth1/22(S) Eth1/23(S) Eth1/24(S) Eth1/25(S)
                      Eth1/26(S) Eth1/27(S) Eth1/28(S)
```

```
Console#
```

CONFIGURING IEEE 802.1Q TUNNELING

IEEE 802.1Q tunneling (QinQ tunneling) uses a single Service Provider VLAN (SPVLAN) for customers who have multiple VLANs. Customer VLAN IDs are preserved and traffic from different customers is segregated within the service provider's network even when they use the same customer-specific VLAN IDs. QinQ tunneling expands VLAN space by using a VLAN-in-VLAN hierarchy, preserving the customer's original tagged packets, and adding SPVLAN tags to each frame (also called double tagging).

This section describes commands used to configure QinQ tunneling.

Table 164: 802.1Q Tunneling Commands

Command	Function	Mode
dot1q-tunnel system-tunnel-control	Configures the switch to operate in normal mode or QinQ mode	GC
switchport dot1q-tunnel mode	Configures an interface as a QinQ tunnel port	IC
switchport dot1q-tunnel service match cvid	Creates a CVLAN to SPVLAN mapping entry	IC
switchport dot1q-tunnel tpid	Sets the Tag Protocol Identifier (TPID) value of a tunnel port	IC
show dot1q-tunnel	Displays the configuration of QinQ tunnel ports	PE
show interfaces switchport	Displays port QinQ operational status	PE

General Configuration Guidelines for QinQ

1. Configure the switch to QinQ mode (dot1q-tunnel system-tunnel-control).

2. Create a SPVLAN (vlan).

3. Configure the QinQ tunnel access port to dot1Q-tunnel access mode (switchport dot1q-tunnel mode).

4. Set the Tag Protocol Identifier (TPID) value of the tunnel access port. This step is required if the attached client is using a nonstandard 2-byte ethertype to identify 802.1Q tagged frames. The standard ethertype value is 0x8100. (See switchport dot1q-tunnel tpid.)

5. Configure the QinQ tunnel access port to join the SPVLAN as an untagged member (switchport allowed vlan).

6. Configure the SPVLAN ID as the native VID on the QinQ tunnel access port (switchport native vlan).

7. Configure the QinQ tunnel uplink port to dot1Q-tunnel uplink mode (switchport dot1q-tunnel mode).

8. Configure the QinQ tunnel uplink port to join the SPVLAN as a tagged member (switchport allowed vlan).

Limitations for QinQ

- The native VLAN for the tunnel uplink ports and tunnel access ports cannot be the same. However, the same service VLANs can be set on both tunnel port types.

- IGMP Snooping should not be enabled on a tunnel access port.

- If the spanning tree protocol is enabled, be aware that a tunnel access or tunnel uplink port may be disabled if the spanning tree structure is automatically reconfigured to overcome a break in the tree. It is therefore advisable to disable spanning tree on these ports.

dot1q-tunnel system-tunnel-control

This command sets the switch to operate in QinQ mode. Use the **no** form to disable QinQ operating mode.

SYNTAX

[**no**] **dot1q-tunnel system-tunnel-control**

DEFAULT SETTING

Disabled

COMMAND MODE

Global Configuration

COMMAND USAGE

QinQ tunnel mode must be enabled on the switch for QinQ interface settings to be functional.

EXAMPLE

```
Console(config)#dot1q-tunnel system-tunnel-control
Console(config)#
```

RELATED COMMANDS

show dot1q-tunnel (1359)
show interfaces switchport (1203)

switchport dot1q-tunnel mode

This command configures an interface as a QinQ tunnel port. Use the **no** form to disable QinQ on the interface.

SYNTAX

switchport dot1q-tunnel mode {**access** | **uplink**}

no switchport dot1q-tunnel mode

access – Sets the port as an 802.1Q tunnel access port.

uplink – Sets the port as an 802.1Q tunnel uplink port.

DEFAULT SETTING

Disabled

COMMAND MODE

Interface Configuration (Ethernet, Port Channel)

COMMAND USAGE

- QinQ tunneling must be enabled on the switch using the dot1q-tunnel system-tunnel-control command before the **switchport dot1q-tunnel mode** interface command can take effect.

- When a tunnel uplink port receives a packet from a customer, the customer tag (regardless of whether there are one or more tag layers) is retained in the inner tag, and the service provider's tag added to the outer tag.

- When a tunnel uplink port receives a packet from the service provider, the outer service provider's tag is stripped off, and the packet passed on to the VLAN indicated by the inner tag. If no inner tag is found, the packet is passed onto the native VLAN defined for the uplink port.

EXAMPLE

```
Console(config)#interface ethernet 1/1
Console(config-if)#switchport dot1q-tunnel mode access
Console(config-if)#
```

RELATED COMMANDS

show dot1q-tunnel (1359)
show interfaces switchport (1203)

switchport dot1q-tunnel service match cvid

This command creates a CVLAN to SPVLAN mapping entry. Use the **no** form to delete a VLAN mapping entry.

SYNTAX

switchport dot1q-tunnel service *svid* **match cvid** *cvid* [**remove-ctag**]

svid - VLAN ID for the outer VLAN tag (Service Provider VID). (Range: 1-4094)

cvid - VLAN ID for the inner VLAN tag (Customer VID). (Range: 1-4094)

remove-ctag - Removes the customer's VLAN tag.

DEFAULT SETTING

Default mapping uses the PVID of the ingress port on the edge router for the SPVID.

COMMAND MODE

Interface Configuration (Ethernet, Port Channel)

COMMAND USAGE

- The inner VLAN tag of a customer packet entering the edge router of a service provider's network is mapped to an outer tag indicating the service provider VLAN that will carry this traffic across the 802.1Q tunnel. This process is performed in a transparent manner as described under "IEEE 802.1Q Tunneling" on page 243.

- When priority bits are found in the inner tag, these are also copied to the outer tag. This allows the service provider to differentiate service based on the indicated priority and appropriate methods of queue management at intermediate nodes across the tunnel.

- Rather than relying on standard service paths and priority queuing, QinQ VLAN mapping can be used to further enhance service by defining a set of differentiated service pathways to follow across the service provider's network for traffic arriving from specified inbound customer VLANs.

- Note that all customer interfaces should be configured as access interfaces (that is, a user-to-network interface) and service provider interfaces as uplink interfaces (that is, a network-to-network interface). Use the switchport dot1q-tunnel mode uplink command to set an interface to access or uplink mode.

- When the **remove-ctag** option is specified, the inner-tag containing the customer's VID is removed, and the outer-tag containing the service provider's VID remains in place.

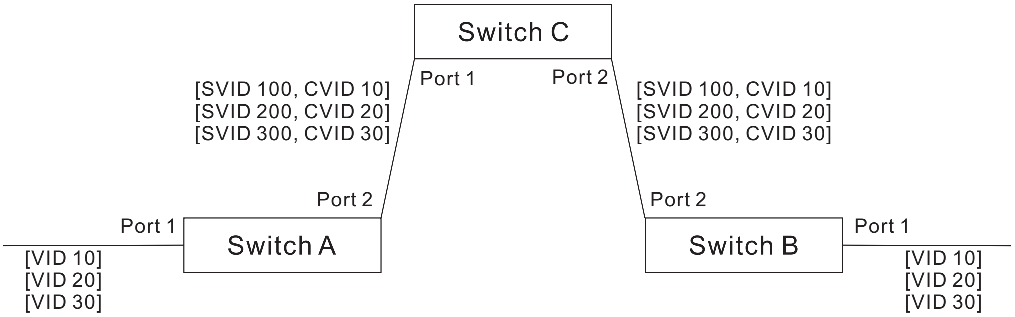
EXAMPLE

This example sets the SVID to 99 in the outer tag for egress packets exiting port 1 when the packet’s CVID is 2.

```
Console(config)#interface ethernet 1/1
Console(config-if)#switchport dot1q-tunnel service 99 match cvid 2
Console(config-if)#
```

The following example maps C-VLAN 10 to S-VLAN 100, C-VLAN 20 to S-VLAN 200 and C-VLAN 30 to S-VLAN 300 for ingress traffic on port 1 of Switches A and B.

Figure 553: Mapping QinQ Service VLAN to Customer VLAN



Step 1. Configure Switch A and B.

1. Create VLANs 100, 200 and 300.

   ```
   Console(config)#vlan database
   Console(config-vlan)#vlan 100,200,300 media ethernet state active
   ```

2. Enable QinQ.

   ```
   Console(config)#dot1q-tunnel system-tunnel-control
   ```

3. Configure port 2 as a tagged member of VLANs 100, 200 and 300 using uplink mode.

   ```
   Console(config)#interface ethernet 1/2
   Console(config-if)#switchport allowed vlan add 100,200,300 tagged
   Console(config-if)#switchport dot1q-tunnel mode uplink
   ```

4. Configures port 1 as an untagged member of VLANs 100, 200 and 300 using access mode.

   ```
   Console(config)#interface ethernet 1/1
   Console(config-if)#switchport allowed vlan add 100,200,300 untagged
   Console(config-if)#switchport dot1q-tunnel mode access
   ```

5. Configure the following selective QinQ mapping entries.

   ```
   Console(config)#interface ethernet 1/1
   Console(config-if)#switchport dot1q-tunnel service 100 match cvid 10
   Console(config-if)#switchport dot1q-tunnel service 200 match cvid 20
   Console(config-if)#switchport dot1q-tunnel service 300 match cvid 30
   ```

6. Configures port 1 as member of VLANs 10, 20 and 30 to avoid filtering out incoming frames tagged with VID 10, 20 or 30 on port 1

   ```
   Console(config)#interface ethernet 1/1
   Console(config-if)#switchport allowed vlan add 10,20,30
   ```

7. Verify configuration settings.

```
Console#show dot1q-tunnel service
802.1Q Tunnel Service Subscriptions

 Port     Match C-VID S-VID
 -------- ----------- -----
 Eth 1/ 1          10   100
 Eth 1/ 1          20   200
 Eth 1/ 1          30   300
```

Step 2. Configure Switch C.

1. Create VLAN 100, 200 and 300.

```
Console(config)#vlan database
Console(config-vlan)#vlan 100,200,300 media ethernet state active
```

2. Configure port 1 and port 2 as tagged members of VLAN 100, 200 and 300.

```
Console(config)#interface ethernet 1/1,2
Console(config-if)#switchport allowed vlan add 100,200,300 tagged
```

switchport dot1q-tunnel tpid

This command sets the Tag Protocol Identifier (TPID) value of a tunnel port. Use the **no** form to restore the default setting.

SYNTAX

switchport dot1q-tunnel tpid *tpid*

no switchport dot1q-tunnel tpid

tpid – Sets the ethertype value for 802.1Q encapsulation. This identifier is used to select a nonstandard 2-byte ethertype to identify 802.1Q tagged frames. The standard ethertype value is 0x8100. (Range: 0800-FFFF hexadecimal)

DEFAULT SETTING

0x8100

COMMAND MODE

Interface Configuration (Ethernet, Port Channel)

COMMAND USAGE

- Use the **switchport dot1q-tunnel tpid** command to set a custom 802.1Q ethertype value on the selected interface. This feature allows the switch to interoperate with third-party switches that do not use the standard 0x8100 ethertype to identify 802.1Q-tagged frames. For example, 0x1234 is set as the custom 802.1Q ethertype on a trunk port, incoming frames containing that ethertype are assigned to the VLAN contained in the tag following the ethertype field, as they would be with a standard 802.1Q trunk. Frames arriving on the port containing any other ethertype are looked upon as untagged frames, and assigned to the native VLAN of that port.

- The specified ethertype only applies to ports configured in Uplink mode using the switchport dot1q-tunnel mode command. If the port is in normal mode (i.e, unspecified), the TPID is always 8100. If the port is in Access mode, received packets are processes as untagged packets.

EXAMPLE

```
Console(config)#interface ethernet 1/1
Console(config-if)#switchport dot1q-tunnel tpid 9100
Console(config-if)#
```

RELATED COMMANDS

show interfaces switchport (1203)

show dot1q-tunnel

This command displays information about QinQ tunnel ports.

SYNTAX

show dot1q-tunnel [**interface** *interface* [**service** *svid*] | **service** [*svid*]]

interface

ethernet *unit*/*port*

unit - Stack unit. (Range: 1)

port - Port number. (Range: 1-28)

port-channel *channel-id* (Range: 1-8)

svid - VLAN ID for the outer VLAN tag (SPVID). (Range: 1-4094)

COMMAND MODE

Privileged Exec

EXAMPLE

```
Console(config)#dot1q-tunnel system-tunnel-control
Console(config)#interface ethernet 1/1
Console(config-if)#switchport dot1q-tunnel mode access
Console(config-if)#interface ethernet 1/2
Console(config-if)#switchport dot1q-tunnel mode uplink
Console(config-if)#end
Console#show dot1q-tunnel
802.1Q Tunnel Status : Enabled

Port     Mode   TPID (hex)
-------- ------ ----------
Eth 1/ 1 Access       8100
Eth 1/ 2 Uplink       8100
Eth 1/ 3 Normal       8100
:
Console#show dot1q-tunnel interface ethernet 1/5
802.1Q Tunnel Service Subscriptions

 Port     Match C-VID S-VID Remove C-Tag
 -------- ----------- ----- ------------
 Eth 1/ 5           1   100 Disabled
```

```
Console#show dot1q-tunnel service 100
802.1Q Tunnel Service Subscriptions

 Port     Match C-VID S-VID Remove C-Tag
 -------- ----------- ----- ------------
 Eth 1/ 5           1   100 Disabled
 Eth 1/ 6           1   100 Enabled

Console#
```

RELATED COMMANDS

switchport dot1q-tunnel mode (1355)

CONFIGURING L2CP TUNNELING

This section describes the commands used to configure Layer 2 Protocol Tunneling (L2PT).

Table 165: L2 Protocol Tunnel Commands

Command	Function	Mode
l2protocol-tunnel tunnel-dmac	Configures the destination address for Layer 2 Protocol Tunneling	GC
switchport l2protocol-tunnel	Enables Layer 2 Protocol Tunneling for the specified protocol	IC
show l2protocol-tunnel	Shows settings for Layer 2 Protocol Tunneling	PE

l2protocol-tunnel tunnel-dmac

This command configures the destination address for Layer 2 Protocol Tunneling (L2PT). Use the **no** form to restore the default setting.

SYNTAX

l2protocol-tunnel tunnel-dmac *mac-address*

mac-address – The switch rewrites the destination MAC address in all upstream L2PT protocol packets (i.e, STP BPDUs) to this value, and forwards them on to uplink ports. The MAC address must be specified in the format xx-xx-xx-xx-xx-xx or xxxxxxxxxxxx.

DEFAULT SETTING

01-12-CF-.00-00-02, proprietary tunnel address

COMMAND MODE

Global Configuration

COMMAND USAGE

- When L2PT is not used, protocol packets (such as STP) are flooded to 802.1Q access ports on the same edge switch, but filtered from 802.1Q tunnel ports. This creates disconnected protocol domains in the customer's network.

- L2PT can be used to pass various types of protocol packets belonging to the same customer transparently across a service provider's network. In this way, normally segregated network segments can be configured to function inside a common protocol domain.

- L2PT encapsulates protocol packets entering ingress ports on the service provider's edge switch, replacing the destination MAC address with a proprietary MAC address (for example, the spanning tree protocol uses 10-12-CF-00-00-02), a reserved address for other specified protocol types (as defined in IEEE 802.1ad – Provider Bridges), or a user-defined address. All intermediate switches carrying this traffic across the service provider's network treat these encapsulated packets in the same way as normal data, forwarding them across to the tunnel's egress port. The egress port decapsulates these packets, restores the proper protocol and MAC address information, and then floods them onto the same VLANs at the customer's remote site (via all of the appropriate tunnel ports and access ports[27] connected to the same metro VLAN).

- The way in which L2PT processes packets is based on the following criteria – (1) packet is received on a QinQ uplink port, (2) packet is received on a QinQ access port, or (3) received packet is Cisco-compatible L2PT (i.e., as indicated by a proprietary MAC address).

Processing protocol packets defined in IEEE 802.1ad – Provider Bridges

- When an IEEE 802.1ad protocol packet is received on an uplink port (i.e., an 802.1Q tunnel ingress port connecting the edge switch to the service provider network)

  - with the destination address 01-80-C2-00-00-00,0B~0F (C-VLAN tag), it is forwarded to all QinQ uplink ports and QinQ access ports in the same S-VLAN for which L2PT is enabled for that protocol.

  - with the destination address 01-80-C2-00-00-01~0A (S-VLAN tag), it is filtered, decapsulated, and processed locally by the switch if the protocol is supported.

- When a protocol packet is received on an access port (i.e., an 802.1Q trunk port connecting the edge switch to the local customer network)

  - with the destination address 01-80-C2-00-00-00,0B~0F (C-VLAN), and

    - L2PT is enabled on the port, the frame is forwarded to all QinQ uplink ports and QinQ access ports on which L2PT is enabled for that protocol in the same S-VLAN.

    - L2PT is disabled on the port, the frame is decapsulated and processed locally by the switch if the protocol is supported.

[27] Access ports in this context are 802.1Q trunk ports.

  - with destination address 01-80-C2-00-00-01~0A (S-VLAN), the frame is filtered, decapsulated, and processed locally by the switch if the protocol is supported.

Processing Cisco-compatible protocol packets

- When a Cisco-compatible L2PT packet is received on an uplink port, and
  - recognized as a CDP/VTP/STP/PVST+ protocol packet (where STP means STP/RSTP/MSTP), it is forwarded to the following ports in the same S-VLAN: (a) all access ports for which L2PT has been disabled, and (b) all uplink ports.
  - recognized as a Generic Bridge PDU Tunneling (GBPT) protocol packet (i.e., having the destination address 01-00-0C-CD-CD-D0), it is forwarded to the following ports in the same S-VLAN:
    - other access ports for which L2PT is enabled after decapsulating the packet and restoring the proper protocol and MAC address information.
    - all uplink ports.
- When a Cisco-compatible L2PT packet is received on an access port, and
  - recognized as a CDP/VTP/STP/PVST+ protocol packet, and
    - L2PT is enabled on this port, it is forwarded to the following ports in the same S-VLAN: (a) other access ports for which L2PT is enabled, and (b) uplink ports after rewriting the destination address to make it a GBPT protocol packet (i.e., setting the destination address to 01-00-0C-CD-CD-D0).
    - L2PT is disabled on this port, it is forwarded to the following ports in the same S-VLAN: (a) other access ports for which L2PT is disabled, and (b) all uplink ports.
  - recognized as a GBPT protocol packet (i.e., having the destination address 01-00-0C-CD-CD-D0), and
    - L2PT is enabled on this port, it is forwarded to other access ports in the same S-VLAN for which L2PT is enabled
    - L2PT is disabled on this port, it is forwarded to the following ports in the same S-VLAN: (a) other access ports for which L2PT is disabled, and (b) all uplink ports.
- For L2PT to function properly, QinQ must be enabled on the switch using the dot1q-tunnel system-tunnel-control command, and the interface configured to 802.1Q tunnel mode using the switchport dot1q-tunnel mode command.

EXAMPLE

```
Console(config)#dot1q-tunnel system-tunnel-control
Console(config)#l2protocol-tunnel tunnel-dmac 01-80-C2-00-00-01
Console(config-)#
```

switchport l2protocol-tunnel

This command enables Layer 2 Protocol Tunneling (L2PT) for the specified protocol. Use the **no** form to disable L2PT for the specified protocol.

SYNTAX

switchport l2protocol-tunnel {**cdp** | **lldp** | **pvst+** | **spanning-tree** | **vtp**}

cdp - Cisco Discovery Protocol

lldp - Link Layer Discovery Protocol

pvst+ - Cisco Per VLAN Spanning Tree Plus

spanning-tree - Spanning Tree (STP, RSTP, MSTP)

vtp - Cisco VLAN Trunking Protocol

DEFAULT SETTING

Disabled for all protocols

COMMAND MODE

Interface Configuration (Ethernet, Port Channel)

COMMAND USAGE

- Refer to the Command Usage section for the l2protocol-tunnel tunnel-dmac command.

- For L2PT to function properly, QinQ must be enabled on the switch using the dot1q-tunnel system-tunnel-control command, and the interface configured to 802.1Q tunnel mode using the switchport dot1q-tunnel mode command.

EXAMPLE

```
Console(config)#dot1q-tunnel system-tunnel-control
Console(config)#interface ethernet 1/1
Console(config-if)#switchport dot1q-tunnel mode access
Console(config-if)#switchport l2protocol-tunnel spanning-tree
Console(config-if)#
```

show l2protocol-tunnel

This command shows settings for Layer 2 Protocol Tunneling (L2PT).

COMMAND MODE

Privileged Exec

EXAMPLE

```
Console#show l2protocol-tunnel
Layer 2 Protocol Tunnel

Tunnel MAC Address : 01-12-CF-00-00-00

Interface  Protocol
----------------------------------------------------------
Eth 1/ 1   Spanning Tree

Console#
```

CONFIGURING VLAN TRANSLATION

QinQ tunneling uses double tagging to preserve the customer's VLAN tags on traffic crossing the service provider's network. However, if any switch in the path crossing the service provider's network does not support this feature, then the switches directly connected to that device can be configured to swap the customer's VLAN ID with the service provider's VLAN ID for upstream traffic, or the service provider's VLAN ID with the customer's VLAN ID for downstream traffic.

This section describes commands used to configure VLAN translation.

Table 166: VLAN Translation Commands

Command	Function	Mode
switchport vlan-translation	Maps VLAN IDs between the customer and service provider	IC
show vlan-translation	Displays the configuration settings for VLAN translation	PE

switchport vlan-translation

This command maps VLAN IDs between the customer and service provider.

SYNTAX

switchport vlan-translation *original-vlan new-vlan*

no switchport vlan-translation *original-vlan*

original-vlan - The original VLAN ID. (Range: 1-4094)

new-vlan - The new VLAN ID. (Range: 1-4094)

DEFAULT SETTING

Disabled

COMMAND MODE

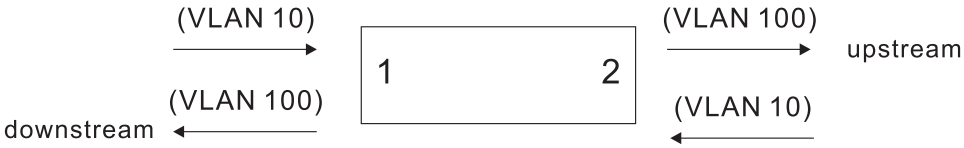
Interface Configuration (Ethernet)

COMMAND USAGE

- If the next switch upstream does not support QinQ tunneling, then use this command to map the customer's VLAN ID to the service provider's VLAN ID for the upstream port. Similarly, if the next switch downstream does not support QinQ tunneling, then use this command to map the service provider's VLAN ID to the customer's VLAN ID for the downstream port. Note that one command maps both the *original-vlan* to *new-vlan* for ingress traffic and the *new-vlan* to *original-vlan* for egress traffic on the specified port.

  For example, assume that the upstream switch does not support QinQ tunneling. If the command **switchport vlan-translation 10 100** is used to map VLAN 10 to VLAN 100 for upstream traffic entering port 1, and VLAN 100 to VLAN 10 for downstream traffic leaving port 1, then the VLAN IDs will be swapped as shown below.

  Figure 554: Configuring VLAN Translation



- The maximum number of VLAN translation entries is 8 per port, and up to 96 for the system. However, note that configuring a large number of entries may degrade the performance of other processes that also use the TCAM, such as IP Source Guard filter rules, Quality of Service (QoS) processes, QinQ, MAC-based VLANs, VLAN translation, or traps.

- If VLAN translation is set on an interface with this command, and the same interface is also configured as a QinQ access port with the switchport dot1q-tunnel mode command, VLAN tag assignments will be determined by the QinQ process, not by VLAN translation.

EXAMPLE

This example configures VLAN translation for Port 1 as described in the Command Usage section above.

```
Console(config)#vlan database
Console(config-vlan)#vlan 10 media ethernet state active
Console(config-vlan)#vlan 100 media ethernet state active
Console(config-vlan)#exit
Console(config)#interface ethernet 1/1,2
Console(config-if)#switchport allowed vlan add 10 tagged
Console(config-if)#switchport allowed vlan add 100 tagged
Console(config-if)#interface ethernet 1/1
Console(config-if)#switchport vlan-translation 10 100
Console(config-if)#end
Console#show vlan-translation

Interface Old VID New VID
--------- ------- -------
Eth 1/ 1       10     100
```

```
Console#
```

show vlan-translation

This command displays the configuration settings for VLAN translation.

SYNTAX

show vlan-translation [**interface** *interface*]

interface

ethernet *unit/port*

unit - Stack unit. (Range: 1)

port - Port number. (Range: 1-28)

COMMAND MODE

Privileged Exec

EXAMPLE

```
Console#show vlan-translation

Interface Old VID New VID
--------- ------- -------
Eth 1/ 1       10     100

Console#
```

CONFIGURING PRIVATE VLANS

Private VLANs provide port-based security and isolation of local ports contained within different private VLAN groups. This switch supports two types of private VLANs – primary and community groups. A primary VLAN contains promiscuous ports that can communicate with all other ports in the associated private VLAN groups, while a community (or secondary) VLAN contains community ports that can only communicate with other hosts within the community VLAN and with any of the promiscuous ports in the associated primary VLAN. The promiscuous ports are designed to provide open access to an external network such as the Internet, while the community ports provide restricted access to local users.

Multiple primary VLANs can be configured on this switch, and multiple community VLANs can be associated with each primary VLAN. (Note that private VLANs and normal VLANs can exist simultaneously within the same switch.)

This section describes commands used to configure private VLANs.

.
Table 167: Private VLAN Commands

Command	Function	Mode
Edit Private VLAN Groups		
private-vlan	Adds or deletes primary or community VLANs	VC
private vlan association	Associates a community VLAN with a primary VLAN	VC
Configure Private VLAN Interfaces		
switchport mode private-vlan	Sets an interface to host mode or promiscuous mode	IC
switchport private-vlan host-association	Associates an interface with a secondary VLAN	IC
switchport private-vlan mapping	Maps an interface to a primary VLAN	IC
Display Private VLAN Information		
show vlan private-vlan	Shows private VLAN information	NE, PE

To configure private VLANs, follow these steps:

1. Use the private-vlan command to designate one or more community VLANs and the primary VLAN that will channel traffic outside of the community groups.

2. Use the private vlan association command to map the community VLAN(s) to the primary VLAN.

3. Use the switchport mode private-vlan command to configure ports as promiscuous (i.e., having access to all ports in the primary VLAN) or host (i.e., community port).

4. Use the switchport private-vlan host-association command to assign a port to a community VLAN.

5. Use the switchport private-vlan mapping command to assign a port to a primary VLAN.

6. Use the show vlan private-vlan command to verify your configuration settings.

private-vlan

Use this command to create a primary or community private VLAN. Use the **no** form to remove the specified private VLAN.

SYNTAX

private-vlan *vlan-id* {**community** | **primary**}

no private-vlan *vlan-id*

vlan-id - ID of private VLAN. (Range: 1-4094)

community - A VLAN in which traffic is restricted to host members in the same VLAN and to promiscuous ports in the associate primary VLAN.

primary - A VLAN which can contain one or more community VLANs, and serves to channel traffic between community VLANs and other locations.

DEFAULT SETTING

None

COMMAND MODE

VLAN Configuration

COMMAND USAGE

- Private VLANs are used to restrict traffic to ports within the same community, and channel traffic passing outside the community through promiscuous ports. When using community VLANs, they must be mapped to an associated "primary" VLAN that contains promiscuous ports.
- Port membership for private VLANs is static. Once a port has been assigned to a private VLAN, it cannot be dynamically moved to another VLAN via GVRP.
- Private VLAN ports cannot be set to trunked mode. (See "switchport mode" on page 1349.)

EXAMPLE

```
Console(config)#vlan database
Console(config-vlan)#private-vlan 2 primary
Console(config-vlan)#private-vlan 3 community
Console(config)#
```

private vlan association

Use this command to associate a primary VLAN with a secondary (i.e., community) VLAN. Use the **no** form to remove all associations for the specified primary VLAN.

SYNTAX

private-vlan *primary-vlan-id* **association** {*secondary-vlan-id* | **add** *secondary-vlan-id* | **remove** *secondary-vlan-id*}

no private-vlan *primary-vlan-id* **association**

primary-vlan-id - ID of primary VLAN. (Range: 1-4094)

secondary-vlan-id - ID of secondary (i.e, community) VLAN. (Range: 1-4094).

DEFAULT SETTING

None

COMMAND MODE

VLAN Configuration

COMMAND USAGE

Secondary VLANs provide security for group members. The associated primary VLAN provides a common interface for access to other network resources within the primary VLAN (e.g., servers configured with promiscuous ports) and to resources outside of the primary VLAN (via promiscuous ports).

EXAMPLE

```
Console(config-vlan)#private-vlan 2 association 3
Console(config)#
```

switchport mode private-vlan

Use this command to set the private VLAN mode for an interface. Use the **no** form to restore the default setting.

SYNTAX

switchport mode private-vlan {**host** | **promiscuous**}

no switchport mode private-vlan

host – This port type can subsequently be assigned to a community VLAN.

promiscuous – This port type can communicate with all other promiscuous ports in the same primary VLAN, as well as with all the ports in the associated secondary VLANs.

DEFAULT SETTING

Normal VLAN

COMMAND MODE

Interface Configuration (Ethernet, Port Channel)

COMMAND USAGE

To assign a promiscuous port to a primary VLAN, use the switchport private-vlan mapping command. To assign a host port to a community VLAN, use the switchport private-vlan host-association command.

EXAMPLE

```
Console(config)#interface ethernet 1/2
Console(config-if)#switchport mode private-vlan promiscuous
Console(config-if)#exit
Console(config)#interface ethernet 1/3
Console(config-if)#switchport mode private-vlan host
Console(config-if)#
```

switchport private-vlan host-association

Use this command to associate an interface with a secondary VLAN. Use the **no** form to remove this association.

Syntax

switchport private-vlan host-association *secondary-vlan-id*

no switchport private-vlan host-association

secondary-vlan-id - ID of secondary (i.e., community) VLAN. (Range: 1-4094)

Default Setting

None

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

All ports assigned to a secondary (i.e., community) VLAN can pass traffic between group members, but must communicate with resources outside of the group via promiscuous ports in the associated primary VLAN.

Example

```
Console(config)#interface ethernet 1/3
Console(config-if)#switchport private-vlan host-association 3
Console(config-if)#
```

switchport private-vlan mapping

Use this command to map an interface to a primary VLAN. Use the **no** form to remove this mapping.

Syntax

switchport private-vlan mapping *primary-vlan-id*

no switchport private-vlan mapping

primary-vlan-id – ID of primary VLAN. (Range: 1-4094)

Default Setting

None

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

Promiscuous ports assigned to a primary VLAN can communicate with any other promiscuous ports in the same VLAN, and with the group members within any associated secondary VLANs.

EXAMPLE

```
Console(config)#interface ethernet 1/2
Console(config-if)#switchport private-vlan mapping 2
Console(config-if)#
```

show vlan private-vlan

Use this command to show the private VLAN configuration settings on this switch.

SYNTAX

show vlan private-vlan [**community** | **primary**]

community – Displays all community VLANs, along with their associated primary VLAN and assigned host interfaces.

primary – Displays all primary VLANs, along with any assigned promiscuous interfaces.

DEFAULT SETTING

None

COMMAND MODE

Privileged Executive

EXAMPLE

```
Console#show vlan private-vlan
Primary   Secondary       Type       Interfaces
--------  -----------  ----------  ------------------------------
     5                 primary     Eth1/ 3
     5         6       community   Eth1/ 4 Eth1/ 5
Console#
```

CONFIGURING PROTOCOL-BASED VLANS

The network devices required to support multiple protocols cannot be easily grouped into a common VLAN. This may require non-standard devices to pass traffic between different VLANs in order to encompass all the devices participating in a specific protocol. This kind of configuration deprives users of the basic benefits of VLANs, including security and easy accessibility.

To avoid these problems, you can configure this switch with protocol-based VLANs that divide the physical network into logical VLAN groups for each required protocol. When a frame is received at a port, its VLAN membership can then be determined based on the protocol type in use by the inbound packets.

Table 168: Protocol-based VLAN Commands

Command	Function	Mode
protocol-vlan protocol-group	Create a protocol group, specifying the supported protocols	GC
protocol-vlan protocol-group	Maps a protocol group to a VLAN	IC
show protocol-vlan protocol-group	Shows the configuration of protocol groups	PE
show interfaces protocol-vlan protocol-group	Shows the interfaces mapped to a protocol group and the corresponding VLAN	PE

To configure protocol-based VLANs, follow these steps:

1. First configure VLAN groups for the protocols you want to use (page 1344). Although not mandatory, we suggest configuring a separate VLAN for each major protocol running on your network. Do not add port members at this time.

2. Create a protocol group for each of the protocols you want to assign to a VLAN using the protocol-vlan protocol-group command (Global Configuration mode).

3. Then map the protocol for each interface to the appropriate VLAN using the protocol-vlan protocol-group command (Interface Configuration mode).

protocol-vlan protocol-group (Configuring Groups)

This command creates a protocol group, or to add specific protocols to a group. Use the **no** form to remove a protocol group.

SYNTAX

protocol-vlan protocol-group *group-id* [{**add** | **remove**}
frame-type *frame* **protocol-type** *protocol*]

no protocol-vlan protocol-group *group-id*

group-id - Group identifier of this protocol group. (Range: 1-2147483647)

frame[28] - Frame type used by this protocol. (Options: ethernet, rfc_1042, llc_other)

protocol - Protocol type. The only option for the llc_other frame type is ipx_raw. The options for all other frames types include: arp, ip, ipv6, rarp, ipv6.

DEFAULT SETTING

No protocol groups are configured.

[28] SNAP frame types are not supported by this switch due to hardware limitations.

COMMAND MODE

Global Configuration

EXAMPLE

The following creates protocol group 1, and specifies Ethernet frames with IP and ARP protocol types:

```
Console(config)#protocol-vlan protocol-group 1 add frame-type ethernet
  protocol-type ip
Console(config)#protocol-vlan protocol-group 1 add frame-type ethernet
  protocol-type arp
Console(config)#
```

protocol-vlan protocol-group (Configuring Interfaces)

This command maps a protocol group to a VLAN for the current interface. Use the **no** form to remove the protocol mapping for this interface.

SYNTAX

protocol-vlan protocol-group *group-id* **vlan** *vlan-id*

no protocol-vlan protocol-group *group-id* **vlan**

group-id - Group identifier of this protocol group. (Range: 1-2147483647)

vlan-id - VLAN to which matching protocol traffic is forwarded. (Range: 1-4094)

DEFAULT SETTING

No protocol groups are mapped for any interface.

COMMAND MODE

Interface Configuration (Ethernet, Port Channel)

COMMAND USAGE

- When creating a protocol-based VLAN, only assign interfaces via this command. If you assign interfaces using any of the other VLAN commands (such as the vlan command), these interfaces will admit traffic of any protocol type into the associated VLAN.

- When a frame enters a port that has been assigned to a protocol VLAN, it is processed in the following manner:

  - If the frame is tagged, it will be processed according to the standard rules applied to tagged frames.

  - If the frame is untagged and the protocol type matches, the frame is forwarded to the appropriate VLAN.

  - If the frame is untagged but the protocol type does not match, the frame is forwarded to the default VLAN for this interface.

EXAMPLE

The following example maps the traffic entering Port 1 which matches the protocol type specified in protocol group 1 to VLAN 2.

```
Console(config)#interface ethernet 1/1
Console(config-if)#protocol-vlan protocol-group 1 vlan 2
Console(config-if)#
```

show protocol-vlan protocol-group

This command shows the frame and protocol type associated with protocol groups.

SYNTAX

show protocol-vlan protocol-group [*group-id*]

group-id - Group identifier for a protocol group.
(Range: 1-2147483647)

DEFAULT SETTING

All protocol groups are displayed.

COMMAND MODE

Privileged Exec

EXAMPLE

This shows protocol group 1 configured for IP over Ethernet:

```
Console#show protocol-vlan protocol-group

 Protocol Group ID   Frame Type    Protocol Type
------------------ ------------- ---------------
                 1      ethernet     08 00
Console#
```

show interfaces protocol-vlan protocol-group

This command shows the mapping from protocol groups to VLANs for the selected interfaces.

SYNTAX

show interfaces protocol-vlan protocol-group [*interface*]

interface

ethernet *unit/port*

unit - Unit identifier. (Range: 1)

port - Port number. (Range: 1-28)

port-channel *channel-id* (Range: 1-8)

DEFAULT SETTING

The mapping for all interfaces is displayed.

COMMAND MODE

Privileged Exec

EXAMPLE

This shows that traffic entering Port 1 that matches the specifications for protocol group 1 will be mapped to VLAN 2:

```
Console#show interfaces protocol-vlan protocol-group

   Port     ProtocolGroup ID    VLAN ID
---------- ------------------ -----------
   Eth 1/1                  1       vlan2
Console#
```

CONFIGURING IP SUBNET VLANS

When using IEEE 802.1Q port-based VLAN classification, all untagged frames received by a port are classified as belonging to the VLAN whose VID (PVID) is associated with that port.

When IP subnet-based VLAN classification is enabled, the source address of untagged ingress frames are checked against the IP subnet-to-VLAN mapping table. If an entry is found for that subnet, these frames are assigned to the VLAN indicated in the entry. If no IP subnet is matched, the untagged frames are classified as belonging to the receiving port's VLAN ID (PVID).

Table 169: IP Subnet VLAN Commands

Command	Function	Mode
subnet-vlan	Defines the IP Subnet VLANs	GC
show subnet-vlan	Displays IP Subnet VLAN settings	PE

subnet-vlan

This command configures IP Subnet VLAN assignments. Use the **no** form to remove an IP subnet-to-VLAN assignment.

SYNTAX

subnet-vlan subnet *ip-address mask* **vlan** *vlan-id* [**priority** *priority*]

no subnet-vlan subnet {*ip-address mask* | **all**}

ip-address – The IP address that defines the subnet. Valid IP addresses consist of four decimal numbers, 0 to 255, separated by periods.

mask – This mask identifies the host address bits of the IP subnet.

vlan-id – VLAN to which matching IP subnet traffic is forwarded. (Range: 1-4094)

priority – The priority assigned to untagged ingress traffic. (Range: 0-7, where 7 is the highest priority)

DEFAULT SETTING

Priority: 0

COMMAND MODE

Global Configuration

COMMAND USAGE

- Each IP subnet can be mapped to only one VLAN ID. An IP subnet consists of an IP address and a subnet mask. The specified VLAN need not be an existing VLAN.
- When an untagged frame is received by a port, the source IP address is checked against the IP subnet-to-VLAN mapping table, and if an entry is found, the corresponding VLAN ID is assigned to the frame. If no mapping is found, the PVID of the receiving port is assigned to the frame.
- The IP subnet cannot be a broadcast or multicast IP address.
- When MAC-based, IP subnet-based, and protocol-based VLANs are supported concurrently, priority is applied in this sequence, and then port-based VLANs last.

EXAMPLE

The following example assigns traffic for the subnet 192.168.12.192, mask 255.255.255.224, to VLAN 4.

```
Console(config)#subnet-vlan subnet 192.168.12.192 255.255.255.224 vlan 4
Console(config)#
```

show subnet-vlan

This command displays IP Subnet VLAN assignments.

COMMAND MODE

Privileged Exec

COMMAND USAGE

- Use this command to display subnet-to-VLAN mappings.
- The last matched entry is used if more than one entry can be matched.

EXAMPLE

The following example displays all configured IP subnet-based VLANs.

```
Console#show subnet-vlan
IP Address       Mask             VLAN ID  Priority
---------------  ---------------  -------  --------
192.168.12.0     255.255.255.128        1         0
192.168.12.128   255.255.255.192        3         0
192.168.12.192   255.255.255.224        4         0
192.168.12.224   255.255.255.240        5         0
192.168.12.240   255.255.255.248        6         0
192.168.12.248   255.255.255.252        7         0
192.168.12.252   255.255.255.254        8         0
192.168.12.254   255.255.255.255        9         0
192.168.12.255   255.255.255.255       10         0
Console#
```

CONFIGURING MAC BASED VLANS

When using IEEE 802.1Q port-based VLAN classification, all untagged frames received by a port are classified as belonging to the VLAN whose VID (PVID) is associated with that port.

When MAC-based VLAN classification is enabled, the source address of untagged ingress frames are checked against the MAC address-to-VLAN mapping table. If an entry is found for that address, these frames are assigned to the VLAN indicated in the entry. If no MAC address is matched, the untagged frames are classified as belonging to the receiving port's VLAN ID (PVID).

Table 170: MAC Based VLAN Commands

Command	Function	Mode
mac-vlan	Defines the IP Subnet VLANs	GC
show mac-vlan	Displays IP Subnet VLAN settings	PE

mac-vlan

This command configures MAC address-to-VLAN mapping. Use the **no** form to remove an assignment.

SYNTAX

mac-vlan mac-address *mac-address* **vlan** *vlan-id* [**priority** *priority*]

no mac-vlan mac-address {*mac-address* | **all**}

mac-address – The source MAC address to be matched. Configured MAC addresses can only be unicast addresses. The MAC address must be specified in the format xx-xx-xx-xx-xx-xx or xxxxxxxxxxxx.

vlan-id – VLAN to which the matching source MAC address traffic is forwarded. (Range: 1-4094)

priority – The priority assigned to untagged ingress traffic. (Range: 0-7, where 7 is the highest priority)

DEFAULT SETTING

None

COMMAND MODE

Global Configuration

COMMAND USAGE

- The MAC-to-VLAN mapping applies to all ports on the switch.
- Source MAC addresses can be mapped to only one VLAN ID.
- Configured MAC addresses cannot be broadcast or multicast addresses.
- When MAC-based, IP subnet-based, and protocol-based VLANs are supported concurrently, priority is applied in this sequence, and then port-based VLANs last.

EXAMPLE

The following example assigns traffic from source MAC address 00-00-00-11-22-33 to VLAN 10.

```
Console(config)#mac-vlan mac-address 00-00-00-11-22-33 vlan 10
Console(config)#
```

show mac-vlan

This command displays MAC address-to-VLAN assignments.

COMMAND MODE

Privileged Exec

COMMAND USAGE

Use this command to display MAC address-to-VLAN mappings.

EXAMPLE

The following example displays all configured MAC address-based VLANs.

```
Console#show mac-vlan
MAC Address        VLAN ID   Priority
-----------------  --------  --------
00-00-00-11-22-33        10         0
Console#
```

CONFIGURING VOICE VLANS

The switch allows you to specify a Voice VLAN for the network and set a CoS priority for the VoIP traffic. VoIP traffic can be detected on switch ports by using the source MAC address of packets, or by using LLDP (IEEE 802.1AB) to discover connected VoIP devices. When VoIP traffic is detected on a configured port, the switch automatically assigns the port to the Voice VLAN. Alternatively, switch ports can be manually configured.

Table 171: Voice VLAN Commands

Command	Function	Mode
voice vlan	Defines the Voice VLAN ID	GC
voice vlan aging	Configures the aging time for Voice VLAN ports	GC
voice vlan mac-address	Configures VoIP device MAC addresses	GC
switchport voice vlan	Sets the Voice VLAN port mode	IC
switchport voice vlan priority	Sets the VoIP traffic priority for ports	IC
switchport voice vlan rule	Sets the automatic VoIP traffic detection method for ports	IC
switchport voice vlan security	Enables Voice VLAN security on ports	IC
show voice vlan	Displays Voice VLAN settings	PE

voice vlan

This command enables VoIP traffic detection and defines the Voice VLAN ID. Use the **no** form to disable the Voice VLAN.

SYNTAX

voice vlan *voice-vlan-id*

no voice vlan

voice-vlan-id - Specifies the voice VLAN ID. (Range: 1-4094)

DEFAULT SETTING

Disabled

COMMAND MODE

Global Configuration

COMMAND USAGE

- When IP telephony is deployed in an enterprise network, it is recommended to isolate the Voice over IP (VoIP) network traffic from other data traffic. Traffic isolation helps prevent excessive packet delays, packet loss, and jitter, which results in higher voice quality. This is best achieved by assigning all VoIP traffic to a single VLAN.

- VoIP traffic can be detected on switch ports by using the source MAC address of packets, or by using LLDP (IEEE 802.1AB) to discover connected VoIP devices. When VoIP traffic is detected on a configured port, the switch automatically assigns the port as a tagged member of the Voice VLAN.

- Only one Voice VLAN is supported and it must already be created on the switch before it can be specified as the Voice VLAN.

- The Voice VLAN ID cannot be modified when the global auto-detection status is enabled (see the switchport voice vlan command.

EXAMPLE

The following example enables VoIP traffic detection and specifies the Voice VLAN ID as 1234.

```
Console(config)#voice vlan 1234
Console(config)#
```

voice vlan aging

This command sets the Voice VLAN ID time out. Use the **no** form to restore the default.

SYNTAX

voice vlan aging *minutes*

no voice vlan

minutes - Specifies the port Voice VLAN membership time out. (Range: 5-43200 minutes)

DEFAULT SETTING

1440 minutes

COMMAND MODE

Global Configuration

COMMAND USAGE

The Voice VLAN aging time is the time after which a port is removed from the Voice VLAN when VoIP traffic is no longer received on the port.

The Remaining Age starts to count down when the OUI's MAC address expires from the MAC address table. Therefore, the MAC address aging time should be added to the overall aging time. For example, if you configure the MAC address table aging time to 30 seconds, and the voice VLAN aging time to 5 minutes, then after 5.5 minutes, a port will be removed from voice VLAN when VoIP traffic is no longer received on the port. Alternatively, if you clear the MAC address table manually, then the switch will also start counting down the Remaining Age.

EXAMPLE

The following example configures the Voice VLAN aging time as 3000 minutes.

```
Console(config)#voice vlan aging 3000
Console(config)#
```

voice vlan mac-address

This command specifies MAC address ranges to add to the OUI Telephony list. Use the **no** form to remove an entry from the list.

SYNTAX

voice vlan mac-address *mac-address* **mask** *mask-address* [**description** *description*]

no voice vlan mac-address *mac-address* **mask** *mask-address*

mac-address - Defines a MAC address OUI that identifies VoIP devices in the network. (For example, 01-23-45-00-00-00)

mask-address - Identifies a range of MAC addresses. (Range: 80-00-00-00-00-00 to FF-FF-FF-FF-FF-FF)

description - User-defined text that identifies the VoIP devices. (Range: 1-32 characters)

DEFAULT SETTING

None

COMMAND MODE

Global Configuration

COMMAND USAGE

- VoIP devices attached to the switch can be identified by the manufacturer's Organizational Unique Identifier (OUI) in the source MAC address of received packets. OUI numbers are assigned to manufacturers and form the first three octets of device MAC addresses. The MAC OUI numbers for VoIP equipment can be configured on the switch so that traffic from these devices is recognized as VoIP.

- Setting a mask of FF-FF-FF-00-00-00 identifies all devices with the same OUI (the first three octets). Other masks restrict the MAC address range. Setting FF-FF-FF-FF-FF-FF specifies a single MAC address.

EXAMPLE

The following example adds a MAC OUI to the OUI Telephony list.

```
Console(config)#voice vlan mac-address 00-12-34-56-78-90 mask ff-ff-ff-00-00-
  00 description A new phone
Console(config)#
```

switchport voice vlan

This command specifies the Voice VLAN mode for ports. Use the **no** form to disable the Voice VLAN feature on the port.

SYNTAX

switchport voice vlan {**manual** | **auto**}

no switchport voice vlan

manual - The Voice VLAN feature is enabled on the port, but the port must be manually added to the Voice VLAN.

auto - The port will be added as a tagged member to the Voice VLAN when VoIP traffic is detected on the port.

DEFAULT SETTING

Disabled

COMMAND MODE

Interface Configuration

COMMAND USAGE

When auto is selected, you must select the method to use for detecting VoIP traffic, either OUI or 802.1ab (LLDP) using the switchport voice vlan rule command. When OUI is selected, be sure to configure the MAC address ranges in the Telephony OUI list using the voice vlan mac-address command.

EXAMPLE

The following example sets port 1 to Voice VLAN auto mode.

```
Console(config)#interface ethernet 1/1
Console(config-if)#switchport voice vlan auto
Console(config-if)#
```

switchport voice vlan priority

This command specifies a CoS priority for VoIP traffic on a port. Use the **no** form to restore the default priority on a port.

SYNTAX

switchport voice vlan priority *priority-value*

no switchport voice vlan priority

priority-value - The CoS priority value. (Range: 0-6)

DEFAULT SETTING

6

COMMAND MODE

Interface Configuration

COMMAND USAGE

Specifies a CoS priority to apply to the port VoIP traffic on the Voice VLAN. The priority of any received VoIP packet is overwritten with the new priority when the Voice VLAN feature is active for the port.

EXAMPLE

The following example sets the CoS priority to 5 on port 1.

```
Console(config)#interface ethernet 1/1
Console(config-if)#switchport voice vlan priority 5
Console(config-if)#
```

switchport voice vlan rule

This command selects a method for detecting VoIP traffic on a port. Use the **no** form to disable the detection method on the port.

SYNTAX

[**no**] **switchport voice vlan rule** {**oui** | **lldp**}

oui - Traffic from VoIP devices is detected by the Organizationally Unique Identifier (OUI) of the source MAC address.

lldp - Uses LLDP to discover VoIP devices attached to the port.

DEFAULT SETTING

OUI: Enabled
LLDP: Disabled

COMMAND MODE

Interface Configuration

COMMAND USAGE

- When OUI is selected, be sure to configure the MAC address ranges in the Telephony OUI list (see the voice vlan mac-address command. MAC address OUI numbers must be configured in the Telephony OUI list so that the switch recognizes the traffic as being from a VoIP device.

- LLDP checks that the “telephone bit” in the system capability TLV is turned on. See "LLDP Commands" on page 1537 for more information on LLDP.

EXAMPLE

The following example enables the OUI method on port 1 for detecting VoIP traffic.

```
Console(config)#interface ethernet 1/1
Console(config-if)#switchport voice vlan rule oui
Console(config-if)#
```

switchport voice vlan security

This command enables security filtering for VoIP traffic on a port. Use the **no** form to disable filtering on a port.

SYNTAX

[**no**] **switchport voice vlan security**

DEFAULT SETTING

Disabled

COMMAND MODE

Interface Configuration

COMMAND USAGE

- Security filtering discards any non-VoIP packets received on the port that are tagged with the voice VLAN ID. VoIP traffic is identified by source MAC addresses configured in the Telephony OUI list, or through LLDP that discovers VoIP devices attached to the switch. Packets received from non-VoIP sources are dropped.

- When enabled, be sure the MAC address ranges for VoIP devices are configured in the Telephony OUI list (voice vlan mac-address).

EXAMPLE

The following example enables security filtering on port 1.

```
Console(config)#interface ethernet 1/1
Console(config-if)#switchport voice vlan security
Console(config-if)#
```

show voice vlan

This command displays the Voice VLAN settings on the switch and the OUI Telephony list.

SYNTAX

show voice vlan {**oui** | **status**}

oui - Displays the OUI Telephony list.

status - Displays the global and port Voice VLAN settings.

DEFAULT SETTING

None

COMMAND MODE

Privileged Exec

EXAMPLE

```
Console#show voice vlan status
Global Voice VLAN Status
Voice VLAN Status      : Enabled
Voice VLAN ID          : 1234
Voice VLAN aging time : 1440 minutes

Voice VLAN Port Summary
Port     Mode     Security Rule      Priority Remaining Age
                                                (minutes)
-------- -------- -------- --------- -------- -------------
Eth 1/ 1 Auto     Enabled  OUI              6 100
Eth 1/ 2 Disabled Disabled OUI              6 NA
Eth 1/ 3 Manual   Enabled  OUI              5 100
Eth 1/ 4 Auto     Enabled  OUI              6 100
Eth 1/ 5 Disabled Disabled OUI              6 NA
Eth 1/ 6 Disabled Disabled OUI              6 NA
Eth 1/ 7 Disabled Disabled OUI              6 NA
Eth 1/ 8 Disabled Disabled OUI              6 NA
Eth 1/ 9 Disabled Disabled OUI              6 NA
Eth 1/10 Disabled Disabled OUI              6 NA

Console#show voice vlan oui
OUI Address       Mask              Description
----------------- ----------------- ------------------------------
00-12-34-56-78-9A FF-FF-FF-00-00-00 old phones
00-11-22-33-44-55 FF-FF-FF-00-00-00 new phones
00-98-76-54-32-10 FF-FF-FF-FF-FF-FF Chris' phone

Console#
```

41 Class of Service Commands

The commands described in this section allow you to specify which data packets have greater precedence when traffic is buffered in the switch due to congestion. This switch supports CoS with eight priority queues for each port. Data packets in a port's high-priority queue will be transmitted before those in the lower-priority queues. The default priority can be set for each interface, also the queue service mode and the mapping of frame priority tags to the switch's priority queues can be configured.

Table 172: Priority Commands

Command Group	Function
Priority Commands (Layer 2)	Configures the queue mode, queue weights, and default priority for untagged frames
Priority Commands (Layer 3 and 4)	Sets the default priority processing method (CoS or DSCP), maps priority tags for internal processing, maps values from internal priority table to CoS values used in tagged egress packets for Layer 2 interfaces, maps internal per hop behavior to hardware queues

Priority Commands (Layer 2)

This section describes commands used to configure Layer 2 traffic priority on the switch.

Table 173: Priority Commands (Layer 2)

Command	Function	Mode
queue mode	Sets the queue mode to strict priority, Weighted Round-Robin (WRR), or a combination of strict and weighted queuing	IC
queue weight	Assigns round-robin weights to the priority queues	IC
switchport priority default	Sets a port priority for incoming untagged frames	IC
show interfaces switchport	Displays the administrative and operational status of an interface	PE
show queue mode	Shows the current queue mode	PE
show queue weight	Shows weights assigned to the weighted queues	PE

queue mode

This command sets the scheduling mode used for processing each of the class of service (CoS) priority queues. The options include strict priority, Weighted Round-Robin (WRR), or a combination of strict and weighted queuing. Use the **no** form to restore the default value.

SYNTAX

queue mode {**strict** | **wrr** | **strict-wrr** [*queue-type-list*]}

no queue mode

strict - Services the egress queues in sequential order, transmitting all traffic in the higher priority queues before servicing lower priority queues. This ensures that the highest priority packets are always serviced first, ahead of all other traffic.

wrr - Weighted Round-Robin shares bandwidth at the egress ports by using scheduling weights (based on the queue weight command), and servicing each queue in a round-robin fashion.

strict-wrr - Strict priority is used for the high-priority queues and WRR for the rest of the queues.

queue-type-list - Indicates if the queue is a normal or strict type. (Options: 0 indicates a normal queue, 1 indicates a strict queue)

DEFAULT SETTING

WRR

COMMAND MODE

Interface Configuration (Ethernet, Port Channel)

COMMAND USAGE

- The switch can be set to service the port queues based on strict priority, WRR, or a combination of strict and weighted queueing.
- Strict priority requires all traffic in a higher priority queue to be processed before lower priority queues are serviced.
- Weighted Round Robin (WRR) uses a predefined relative weight for each queue that determines the percentage of service time the switch services each queue before moving on to the next queue. This prevents the head-of-line blocking that can occur with strict priority queuing. Use the queue weight command to assign weights for WRR queuing to the eight priority queues.
- If Strict and WRR mode is selected, a combination of strict service is used for the high priority queues and weighted service for the remaining queues. The queues assigned to use strict priority should be specified using the Strict Mode field parameter.
- A weight can be assigned to each of the weighted queues (and thereby to the corresponding traffic priorities). This weight sets the frequency at which each queue is polled for service, and subsequently affects the response time for software applications assigned a specific priority value.

- Service time is shared at the egress ports by defining scheduling weights for WRR, or for the queuing mode that uses a combination of strict and weighted queuing. Service time is allocated to each queue by calculating a precise number of bytes per second that will be serviced on each round.

- The specified queue mode applies to all interfaces.

- Protocols used to synchronize distributed switches use packets of 1588 bytes to control the synchronization process. This switch therefore assigns packets of this size to the highest priority queue to ensure quick passage.

EXAMPLE

The following example sets the queue mode to strict priority service mode:

```
Console(config)#queue mode strict
Console(config)#
```

RELATED COMMANDS

queue weight (1389)
show queue mode (1391)

queue weight

This command assigns weights to the eight class of service (CoS) priority queues when using weighted queuing, or one of the queuing modes that use a combination of strict and weighted queuing. Use the **no** form to restore the default weights.

SYNTAX

queue weight *weight0...weight7*

no queue weight

weight0...weight7 - The ratio of weights for queues 0 - 7 determines the weights used by the WRR scheduler. (Range: 1-15)

DEFAULT SETTING

Weights 1, 2, 4, 6, 8, 10, 12, 14 are assigned to queues 0 - 7 respectively.

COMMAND MODE

Interface Configuration (Ethernet, Port Channel)

COMMAND USAGE

- This command shares bandwidth at the egress port by defining scheduling weights for Weighted Round-Robin, or for the queuing mode that uses a combination of strict and weighted queuing (page 1388).

- Bandwidth is allocated to each queue by calculating a precise number of bytes per second that will be serviced on each round.

EXAMPLE

The following example shows how to assign round-robin weights of 1 - 8 to the CoS priority queues 0 - 7.

```
Console(config)#queue weight 1 2 3 4 5 6 7 8
Console(config)#
```

RELATED COMMANDS

queue mode (1388)
show queue weight (1391)

switchport priority default

This command sets a priority for incoming untagged frames. Use the **no** form to restore the default value.

SYNTAX

switchport priority default *default-priority-id*

no switchport priority default

default-priority-id - The priority number for untagged ingress traffic. The priority is a number from 0 to 7. Seven is the highest priority.

DEFAULT SETTING

The priority is not set, and the default value for untagged frames received on the interface is zero.

COMMAND MODE

Interface Configuration (Ethernet, Port Channel)

COMMAND USAGE

- The precedence for priority mapping is IP Port, IP Precedence or IP DSCP, and then default switchport priority.
- The default priority applies for an untagged frame received on a port set to accept all frame types (i.e, receives both untagged and tagged frames). This priority does not apply to IEEE 802.1Q VLAN tagged frames. If the incoming frame is an IEEE 802.1Q VLAN tagged frame, the IEEE 802.1p User Priority bits will be used.
- The switch provides eight priority queues for each port. It can be configured to use strict priority queuing, Weighted Round Robin (WRR), or a combination of strict and weighted queuing using the queue mode command. Inbound frames that do not have VLAN tags are tagged with the input port's default ingress user priority, and then placed in the appropriate priority queue at the output port. The default priority for all ingress ports is zero. Therefore, any inbound frames that do not have priority tags will be placed in queue 2 of the output port. (Note that if the output port is an untagged member of the associated VLAN, these frames are stripped of all VLAN tags prior to transmission.)

EXAMPLE

The following example shows how to set a default priority on port 3 to 5:

```
Console(config)#interface ethernet 1/3
Console(config-if)#switchport priority default 5
Console(config-if)#
```

RELATED COMMANDS

show interfaces switchport (1203)

show queue mode

This command shows the current queue mode.

SYNTAX

show queue mode *interface*

interface

ethernet *unit/port*

unit - Stack unit. (Range: 1)

port - Port number. (Range: 1-28)

COMMAND MODE

Privileged Exec

EXAMPLE

```
Console#show queue mode ethernet 1/1
Unit   Port   queue mode
----   ----   ---------------
   1      1   Weighted Round Robin
Console#
```

show queue weight

This command displays the weights used for the weighted queues.

SYNTAX

show queue mode *interface*

interface

ethernet *unit/port*

unit - Stack unit. (Range: 1)

port - Port number. (Range: 1-28)

port-channel *channel-id* (Range: 1-8)

COMMAND MODE

Privileged Exec

EXAMPLE

```
Console#show queue weight
Information of Eth 1/1
 Queue ID  Weight
 --------  ------
        0       1
        1       2
        2       4
        3       6
        4       8
        5      10
        6      12
        7      14
⋮
```

PRIORITY COMMANDS (LAYER 3 AND 4)

This section describes commands used to configure Layer 3 and 4 traffic priority mapping on the switch.

Table 174: Priority Commands (Layer 3 and 4)

Command	Function	Mode
qos map cos-dscp	Maps CoS/CFI values in incoming packets to per-hop behavior and drop precedence values for internal priority processing	IC
qos map default-drop-precedence	Maps the per-hop behavior to default drop precedence	IC
qos map dscp-cos	Maps internal per-hop behavior and drop precedence value pairs to CoS values used in tagged egress packets on a Layer 2 interface	IC
qos map dscp-mutation	Maps DSCP values in incoming packets to per-hop behavior and drop precedence values for internal priority processing	IC
qos map ip-port-dscp	Maps the destination TCP/UDP port in incoming packets to per-hop behavior and drop precedence values for internal priority processing	IC
qos map ip-prec-dscp	Maps IP Precedence values in incoming packets to per-hop behavior and drop precedence values for internal priority processing	IC
qos map phb-queue	Maps internal per-hop behavior values to hardware queues	IC
qos map trust-mode	Sets QoS mapping to DSCP or CoS	IC
show qos map cos-dscp	Shows ingress CoS to internal DSCP map	PE
show qos map dscp-cos	Shows internal DSCP to egress CoS map	PE
show qos map dscp-mutation	Shows ingress DSCP to internal DSCP map	PE
show qos map ip-port-dscp	Shows destination TCP/UDP port to internal DSCP map	PE
show qos map ip-prec-dscp	Shows ingress IP Precedence to internal DSCP map	PE

Table 174: Priority Commands (Layer 3 and 4)

Command	Function	Mode
show qos map phb-queue	Shows internal per-hop behavior to hardware queue map	PE
show qos map trust-mode	Shows the QoS mapping mode	PE

* The default settings used for mapping priority values to internal DSCP values and back to the hardware queues are designed to optimize priority services for the majority of network applications. It should not be necessary to modify any of the default settings unless a queuing problem occurs with a particular application.

qos map cos-dscp

This command maps CoS/CFI values in incoming packets to per-hop behavior and drop precedence values for priority processing. Use the **no** form to restore the default settings.

SYNTAX

qos map cos-dscp *phb drop-precedence* **from** *cos0 cfi0...cos7 cfi7*

no qos map cos-dscp *cos0 cfi0...cos7 cfi7*

phb - Per-hop behavior, or the priority used for this router hop. (Range: 0-7)

drop-precedence - Drop precedence used for controlling traffic congestion. (Range: 0 - Green, 3 - Yellow, 1 - Red)

cos - CoS value in ingress packets. (Range: 0-7)

cfi - Canonical Format Indicator. Set to this parameter to “0” to indicate that the MAC address information carried in the frame is in canonical format. (Range: 0-1)

DEFAULT SETTING.

Table 175: Default Mapping of CoS/CFI to Internal PHB/Drop Precedence

CoS	CFI	0	1
0		(0,0)	(0,0)
1		(1,0)	(1,0)
2		(2,0)	(2,0)
3		(3,0)	(3,0)
4		(4,0)	(4,0)
5		(5,0)	(5,0)
6		(6,0)	(6,0)
7		(7,0)	(7,0)

COMMAND MODE

Interface Configuration (Port)

COMMAND USAGE

- The default mapping of CoS to PHB values shown in Table 175 is based on the recommended settings in IEEE 802.1p for mapping CoS values to output queues.
- Enter a value pair for the internal per-hop behavior and drop precedence, followed by the keyword "from" and then up to eight CoS/ CFI paired values separated by spaces.
- If a packet arrives with a 802.1Q header but it is not an IP packet, then the CoS/CFI-to-PHB/Drop Precedence mapping table is used to generate priority and drop precedence values for internal processing. Note that priority tags in the original packet are not modified by this command.
- The internal DSCP consists of three bits for per-hop behavior (PHB) which determines the queue to which a packet is sent; and two bits for drop precedence (namely color) which is used to control traffic congestion.
- The specified mapping applies to all interfaces.

EXAMPLE

```
Console(config)#interface ethernet 1/5
Console(config-if)#qos map cos-dscp 0 0 from 0 1
Console(config-if)#
```

qos map default-drop-precedence

This command maps the internal per-hop behavior (based on packet priority) to a default drop precedence for internal processing of untagged packets. Use the **no** form to restore the default settings.

SYNTAX

qos map default-drop-precedence *drop-precedence* **from** *phb0* ... *phb7*

no map default-drop-precedence *phb0* ... *phb7*

drop-precedence - Drop precedence used for controlling traffic congestion.
(Range: 0 - Green, 3 - Yellow, 1 - Red)

phb - Per-hop behavior, or the priority used for this router hop.
(Range: 0-7)

DEFAULT SETTING.

Table 176: Mapping Per-hop Behavior to Drop Precedence

Per-hop Behavior	0	1	2	3	4	5	6	7
Drop Precedence	0	0	0	0	0	0	0	0

COMMAND MODE

Interface Configuration (Port)

COMMAND USAGE

- Enter a drop precedence, followed by the keyword “from” and then up to four per-hop behavior values separated by spaces.
- This command only applies to Layer 2 untagged ingress packets. The drop precedence for any priority tagged ingress packets will be based on the other corresponding QoS mapping schemes described in those sections.

EXAMPLE

```
Console(config)#interface ethernet 1/5
Console(config-if)#qos map default-drop-precedence 1 from 0 1 2
Console(config-if)#qos map default-drop-precedence 3 from 3 4 5
Console(config-if)#qos map default-drop-precedence 0 from 6 7
Console(config-if)#
```

qos map dscp-cos

This command maps internal per-hop behavior and drop precedence value pairs to CoS/CFI values used in tagged egress packets on a Layer 2 interface. Use the **no** form to restore the default settings.

SYNTAX

qos map dscp-cos *cos-value cfi-value* **from** *phb0 drop-precedence0* ... *phb7 drop-precedence7*

no map ip dscp *phb0 drop-precedence0 ... phb7 drop-precedence7*

cos-value - CoS value in ingress packets. (Range: 0 7)

cfi-value - Canonical Format Indicator. Set to this parameter to “0” to indicate that the MAC address information carried in the frame is in canonical format. (Range: 0-1)

phb - Per-hop behavior, or the priority used for this router hop. (Range: 0-7)

drop-precedence - Drop precedence used for controlling traffic congestion. (Range: 0 - Green, 3 - Yellow, 1 - Red)

DEFAULT SETTING

Table 177: Mapping Internal PHB/Drop Precedence to CoS/CFI Values

Drop Precedence	0 (green)	1 (red)	3 (yellow)
Per-hop Behavior			
0	(0,0)	(0,0)	(0,0)
1	(1,0)	(1,0)	(1,0)
2	(2,0)	(2,0)	(2,0)
3	(3,0)	(3,0)	(3,0)
4	(4,0)	(4,0)	(4,0)

Table 177: Mapping Internal PHB/Drop Precedence to CoS/CFI Values

Drop Precedence	0 (green)	1 (red)	3 (yellow)
Per-hop Behavior			
5	(5,0)	(5,0)	(5,0)
6	(6,0)	(6,0)	(6,0)
7	(7,0)	(7,0)	(7,0)

COMMAND MODE

Interface Configuration (Port)

COMMAND USAGE

- Enter a CoS/CFI value pair, followed by the keyword "from" and then four internal per-hop behavior and drop precedence value pairs separated by spaces.
- If the packet is forwarded with an 8021.Q tag, the priority value in the egress packet is modified based on the table shown above, or on similar values as modified by this command.

EXAMPLE

```
Console(config)#interface ethernet 1/5
Console(config-if)#qos map dscp-cos 1 0 from 1 2
Console(config-if)#
```

qos map dscp-mutation

This command maps DSCP values in incoming packets to per-hop behavior and drop precedence values for priority processing. Use the **no** form to restore the default settings.

SYNTAX

qos map dscp-mutation *phb drop-precedence* **from** *dscp0* ... *dscp7*

no qos map dscp-mutation *dscp0* ... *dscp7*

phb - Per-hop behavior, or the priority used for this router hop. (Range: 0-7)

drop-precedence - Drop precedence used for in controlling traffic congestion. (Range: 0 - Green, 3 - Yellow, 1 - Red)

dscp - DSCP value in ingress packets. (Range: 0-63)

DEFAULT SETTING.

Table 178: Default Mapping of DSCP Values to Internal PHB/Drop Values

ingress-dscp1	0	1	2	3	4	5	6	7	8	9
ingress-dscp10										
0	0,0	0,1	0,0	0,3	0,0	0,1	0,0	0,3	1,0	1,1
1	1,0	1,3	1,0	1,1	1,0	1,3	2,0	2,1	2,0	2,3
2	2,0	2,1	2,0	2,3	3,0	3,1	3,0	3,3	3.0	3,1
3	3,0	3,3	4,0	4,1	4,0	4,3	4,0	4,1	4.0	4,3
4	5,0	5,1	5,0	5,3	5,0	5,1	6,0	5,3	6,0	6,1
5	6,0	6,3	6,0	6,1	6,0	6,3	7,0	7,1	7.0	7,3
6	7,0	7,1	7,0	7,3						

The ingress DSCP is composed of ingress-dscp10 (most significant digit in the left column) and ingress-dscp1 (least significant digit in the top row (in other words, ingress-dscp = ingress-dscp10 * 10 + ingress-dscp1); and the corresponding internal-dscp is shown at the intersecting cell in the table.

The ingress DSCP is bitwise ANDed with the binary value 11 to determine the drop precedence. If the resulting value is 10 binary, then the drop precedence is set to 0.

COMMAND MODE

Interface Configuration (Port)

COMMAND USAGE

- Enter a value pair for the internal per-hop behavior and drop precedence, followed by the keyword “from” and then up to eight DSCP values separated by spaces.
- This map is only used when the QoS mapping mode is set to “DSCP” by the qos map trust-mode command, and the ingress packet type is IPv4.
- Two QoS domains can have different DSCP definitions, so the DSCP-to-PHB/Drop Precedence mutation map can be used to modify one set of DSCP values to match the definition of another domain. The mutation map should be applied at the receiving port (ingress mutation) at the boundary of a QoS administrative domain.
- The specified mapping applies to all interfaces.

EXAMPLE

This example changes the priority for all packets entering port 1 which contain a DSCP value of 1 to a per-hop behavior of 3 and a drop precedence of 1. Referring to Table 178, note that the DSCP value for these packets is now set to 25 (3x2^3+1) and passed on to the egress interface.

```
Console(config)#interface ethernet 1/5
Console(config-if)#qos map dscp-mutation 3 1 from 1
Console(config-if)#
```

qos map ip-port-dscp

This command maps the destination TCP/UDP destination port in incoming packets to per-hop behavior and drop precedence values for priority processing. Use the **no** form to remove the mapped values for a TCP/UDP port.

SYNTAX

qos map ip-port-dscp {**tcp** | **udp**} *port-number* **to** *phb drop-precedence*

no qos map cos-dscp {**tcp** | **udp**} *port-number*

phb - Per-hop behavior, or the priority used for this router hop. (Range: 0-7)

drop-precedence - Drop precedence used for controlling traffic congestion. (Range: 0 - Green, 3 - Yellow, 1 - Red)

tcp - Transport Control Protocol

udp - User Datagram Protocol

port-number - 16-bit TCP/UDP destination port number. (Range: 0-65535)

DEFAULT SETTING

None

COMMAND MODE

Interface Configuration (Port)

COMMAND USAGE

- This mapping table is only used if the protocol type of the arriving packet is TCP or UDP.

EXAMPLE

```
Console(config)#interface ethernet 1/5
Console(config-if)#qos map ip-port-dscp tcp 21 to 1 0
Console(config-if)#
```

qos map ip-prec-dscp

This command maps IP precedence values in incoming packets to per-hop behavior and drop precedence values for priority processing. Use the **no** form to restore the default settings.

SYNTAX

qos map ip-prec-dscp *phb0 drop-precedence0* ... *phb7 drop-precedence7*

no map ip-prec-dscp

phb - Per-hop behavior, or the priority used for this router hop. (Range: 0-7)

drop-precedence - Drop precedence used for controlling traffic congestion. (Range: 0 - Green, 3 - Yellow, 1 - Red)

DEFAULT SETTING

Table 179: Default Mapping of IP Precedence to Internal PHB/Drop Values

IP Precedence Value	0	1	2	3	4	5	6	7
Per-hop Behavior	0	1	2	3	4	5	6	7
Drop Precedence	0	0	0	0	0	0	0	0

COMMAND MODE

Interface Configuration (Port)

COMMAND USAGE

- Enter up to eight paired values for per-hop behavior and drop precedence separated by spaces. These values are used for internal priority processing, and correspond to IP Precedence values 0 - 7.
- If the QoS mapping mode is set the IP Precedence and the ingress packet type is IPv4, then the IP Precedence-to-DSCP mapping table is used to generate priority and drop precedence values for internal processing.

EXAMPLE

```
Console(config)#interface ethernet 1/5
Console(config-if)#qos map ip-prec-dscp 7 0 6 0 5 0 4 0 3 0 2 1 1 1 0 1
Console(config-if)#
```

qos map phb-queue

This command determines the hardware output queues to use based on the internal per-hop behavior value. Use the **no** form to restore the default settings.

SYNTAX

qos map phb-queue *queue-id* **from** *phb0 ... phb7*

no map phb-queue *phb0 ... phb7*

phb - Per-hop behavior, or the priority used for this router hop. (Range: 0-7)

queue-id - The ID of the priority queue. (Range: 0-7, where 7 is the highest priority queue)

DEFAULT SETTING.

Table 180: Mapping Internal Per-hop Behavior to Hardware Queues

Per-hop Behavior	0	1	2	3	4	5	6	7
Hardware Queues	2	0	1	3	4	5	6	7

COMMAND MODE

Interface Configuration (Port)

COMMAND USAGE

- Enter a queue identifier, followed by the keyword "from" and then up to eight internal per-hop behavior values separated by spaces.

- Egress packets are placed into the hardware queues according to the mapping defined by this command.

EXAMPLE

```
Console(config)#interface ethernet 1/5
Console(config-if)#qos map phb-queue 0 from 1 2 3
Console(config-if)#
```

qos map trust-mode

This command sets QoS mapping to DSCP or CoS. Use the **no** form to restore the default setting.

SYNTAX

qos map trust-mode {**cos** | **dscp** | **ip-prec**}

no qos map trust-mode

cos - Sets the QoS mapping mode to CoS.

dscp - Sets the QoS mapping mode to DSCP.

ip-prec - Sets the QoS mapping mode to IP Precedence.

DEFAULT SETTING

CoS

COMMAND MODE

Interface Configuration (Port)

COMMAND USAGE

- If the QoS mapping mode is set to IP Precedence with this command, and the ingress packet type is IPv4, then priority processing will be based on the IP Precedence value in the ingress packet.

- If the QoS mapping mode is set to DSCP with this command, and the ingress packet type is IPv4, then priority processing will be based on the DSCP value in the ingress packet.

- If the QoS mapping mode is set to either IP Precedence or DSCP, and a non-IP packet is received, the packet's CoS and CFI (Canonical Format Indicator) values are used for priority processing if the packet is tagged. For an untagged packet, the default port priority (see page 1390) is used for priority processing.

- If the QoS mapping mode is set to CoS with this command, and the ingress packet type is IPv4, then priority processing will be based on the CoS and CFI values in the ingress packet.

For an untagged packet, the default port priority (see page 1390) is used for priority processing.

EXAMPLE

This example sets the QoS priority mapping mode to use DSCP based on the conditions described in the Command Usage section.

```
Console(config)#interface ge1/1
Console(config-if)#qos map trust-mode dscp
Console(config-if)#
```

show qos map cos-dscp

This command shows ingress CoS/CFI to internal DSCP map.

SYNTAX

show qos map cos-dscp interface *interface*

interface

ethernet *unit/port*

unit - Unit identifier. (Range: 1)

port - Port number. (Range: 1-28)

COMMAND MODE

Privileged Exec

EXAMPLE

```
Console#show qos map cos-dscp interface ethernet 1/5
CoS Information of Eth 1/5
 CoS-DSCP map.(x,y),x: phb,y: drop precedence:
 CoS  : CFI  0          1
 ---------------------------------
 0            (0,0)       (0,0)
 1            (1,0)       (1,0)
 2            (2,0)       (2,0)
 3            (3,0)       (3,0)
 4            (4,0)       (4,0)
 5            (5,0)       (5,0)
 6            (6,0)       (6,0)
 7            (7,0)       (7,0)
Console#
```

show qos map dscp-cos

This command shows the internal DSCP to egress CoS map, which converts internal PHB/Drop Precedence to CoS values.

SYNTAX

show qos map dscp-cos interface *interface*

interface

ethernet *unit*/*port*

unit - Stack unit. (Range: 1)

port - Port number. (Range: 1-28)

COMMAND MODE

Privileged Exec

COMMAND USAGE

This map is only used if the packet is forwarded with a 8021.Q tag.

EXAMPLE

```
Console#show qos map dscp-cos interface ethernet 1/5
Information of Eth 1/5
 dscp-cos map:
 phb:  drop precedence   0(green)   1(red)     3(yellow)
 -------------------------------------------------------
 0   :                    (0,0)       (0,0)       (0,0)
 1   :                    (1,0)       (1,0)       (1,0)
 2   :                    (2,0)       (2,0)       (2,0)
 3   :                    (3,0)       (3,0)       (3,0)
 4   :                    (4,0)       (4,0)       (4,0)
 5   :                    (5,0)       (5,0)       (5,0)
 6   :                    (6,0)       (6,0)       (6,0)
 7   :                    (7,0)       (7,0)       (7,0)
Console#
```

show qos map dscp-mutation

This command shows the ingress DSCP to internal DSCP map.

SYNTAX

show qos map dscp-mutation interface *interface*

interface

ethernet *unit*/*port*

unit - Unit identifier. (Range: 1)

port - Port number. (Range: 1-28)

COMMAND MODE

Privileged Exec

Command Usage

This map is only used when the QoS mapping mode is set to "DSCP" by the qos map trust-mode command, and the ingress packet type is IPv4.

Example

The ingress DSCP is composed of "d1" (most significant digit in the left column) and "d2" (least significant digit in the top row (in other words, ingress DSCP = d1 * 10 + d2); and the corresponding Internal DSCP and drop precedence is shown at the intersecting cell in the table.

```
Console#show qos map dscp-mutation interface ethernet 1/5
Information of Eth 1/5
 DSCP mutation map.(x,y),x: PHB,y: drop precedence:
 d1: d2 0     1     2     3     4     5     6     7     8     9
 -----------------------------------------------------------------
 0 :    (0,0) (0,1) (0,0) (0,3) (0,0) (0,1) (0,0) (0,3) (1,0) (1,1)
 1 :    (1,0) (1,3) (1,0) (1,1) (1,0) (1,3) (2,0) (2,1) (2,0) (2,3)
 2 :    (2,0) (2,1) (2,0) (2,3) (3,0) (3,1) (3,0) (3,3) (3,0) (3,1)
 3 :    (3,0) (3,3) (4,0) (4,1) (4,0) (4,3) (4,0) (4,1) (4,0) (4,3)
 4 :    (5,0) (5,1) (5,0) (5,3) (5,0) (5,1) (6,0) (5,3) (6,0) (6,1)
 5 :    (6,0) (6,3) (6,0) (6,1) (6,0) (6,3) (7,0) (7,1) (7,0) (7,3)
 6 :    (7,0) (7,1) (7,0) (7,3)
Console#
```

show qos map ip-port-dscp

This command shows the ingress TCP/UDP port to internal DSCP map.

Syntax

show qos map ip-port-dscp interface *interface*

interface

ethernet *unit/port*

unit - Stack unit. (Range: 1)

port - Port number. (Range: 1-28)

Command Mode

Privileged Exec

Command Usage

The IP Port-to-DSCP mapping table is only used if the protocol type of the arriving packet is TCP or UDP.

Example

```
Console#show qos map ip-port-dscp interface ethernet 1/5
Information of Eth 1/5
 ip-port-dscp map:
 (ip protocol,destination port) :  phb     drop precedence
 -----------------------------------------------------------
 (TCP, 21)    :                    0       0
 (UDP, 12)    :                    1       0
Console#
```

show qos map ip-prec-dscp

This command shows the ingress IP precedence to internal DSCP map.

SYNTAX

show qos map ip-prec-dscp interface *interface*

interface

ethernet *unit/port*

unit - Stack unit. (Range: 1)

port - Port number. (Range: 1-28)

COMMAND MODE

Privileged Exec

COMMAND USAGE

If the QoS mapping mode is set to IP Precedence and the ingress packet type is IPv4, then the IP Precedence-to-DSCP mapping table is used to generate per-hop behavior and drop precedence values for internal processing.

EXAMPLE

```
Console#show qos map ip-prec-dscp interface ethernet 1/5
Information of Eth 1/5
 IP-prec-DSCP map:
 IP-prec:         0     1     2     3     4     5     6     7
 ------------------------------------------------------------
 PHB:             0     1     2     3     4     5     6     7
 drop precedence: 0     0     0     0     0     0     0     0
Console#
```

show qos map phb-queue

This command shows internal per-hop behavior to hardware queue map.

SYNTAX

show qos map phb-queue interface *interface*

interface

ethernet *unit/port*

unit - Unit identifier. (Range: 1)

port - Port number. (Range: 1-28)

COMMAND MODE

Privileged Exec

EXAMPLE

```
Console#show qos map phb-queue interface ethernet 1/5
Information of Eth 1/5
 PHB-queue map:
 PHB:       0     1     2     3     4     5     6     7
 -------------------------------------------------------
 queue:     2     0     1     3     4     5     6     7
Console#
```

show qos map trust-mode

This command shows the QoS mapping mode.

SYNTAX

show qos map trust-mode interface *interface*

interface

ethernet *unit*/*port*

unit - Unit identifier. (Range: 1)

port - Port number. (Range: 1-28)

COMMAND MODE

Privileged Exec

EXAMPLE

The following shows that the trust mode is set to CoS:

```
Console#show qos map trust-mode interface ethernet 1/5
Information of Eth 1/5
  CoS Map Mode:          CoS mode
Console#
```

42 QUALITY OF SERVICE COMMANDS

The commands described in this section are used to configure Differentiated Services (DiffServ) classification criteria and service policies. You can classify traffic based on access lists, IP Precedence or DSCP values, or VLANs. Using access lists allows you select traffic based on Layer 2, Layer 3, or Layer 4 information contained in each packet.

Table 181: Quality of Service Commands

Command	Function	Mode
class-map	Creates a class map for a type of traffic	GC
description	Specifies the description of a class map	CM
match	Defines the criteria used to classify traffic	CM
rename	Redefines the name of a class map	CM
policy-map	Creates a policy map for multiple interfaces	GC
description	Specifies the description of a policy map	PM
class	Defines a traffic classification for the policy to act on	PM
rename	Redefines the name of a policy map	PM
police flow	Defines an enforcer for classified traffic based on a metered flow rate	PM-C
police srtcm-color	Defines an enforcer for classified traffic based on a single rate three color meter	PM-C
police trtcm-color	Defines an enforcer for classified traffic based on a two rate three color meter	PM-C
set cos	Services IP traffic by setting a class of service value for matching packets for internal processing	PM-C
set phb	Services IP traffic by setting a per-hop behavior value for matching packets for internal processing	PM-C
service-policy	Applies a policy map defined by the policy-map command to the input of a particular interface	IC
show class-map	Displays the QoS class maps which define matching criteria used for classifying traffic	PE
show policy-map	Displays the QoS policy maps which define classification criteria for incoming traffic, and may include policers for bandwidth limitations	PE
show policy-map interface	Displays the configuration of all classes configured for all service policies on the specified interface	PE

To create a service policy for a specific category of ingress traffic, follow these steps:

1. Use the class-map command to designate a class name for a specific category of traffic, and enter the Class Map configuration mode.
2. Use the match command to select a specific type of traffic based on an access list, an IPv4 DSCP value, IPv4 Precedence value, IPv6 DSCP value, a VLAN, or a CoS value.
3. Use the policy-map command to designate a policy name for a specific manner in which ingress traffic will be handled, and enter the Policy Map configuration mode.
4. Use the class command to identify the class map, and enter Policy Map Class configuration mode. A policy map can contain up to 16 class maps.
5. Use the set phb or set cos command to modify the per-hop behavior, the class of service value in the VLAN tag for the matching traffic class, and use one of the **police** commands to monitor parameters such as the average flow and burst rate, and drop any traffic that exceeds the specified rate, or just reduce the DSCP service level for traffic exceeding the specified rate.
6. Use the service-policy command to assign a policy map to a specific interface.

NOTE: Create a Class Map before creating a Policy Map.

class-map

This command creates a class map used for matching packets to the specified class, and enters Class Map configuration mode. Use the **no** form to delete a class map.

SYNTAX

[**no**] **class-map** *class-map-name* **match-any**

class-map-name - Name of the class map. (Range: 1-32 characters)

match-any - Match any condition within a class map.

DEFAULT SETTING

None

COMMAND MODE

Global Configuration

COMMAND USAGE

- First enter this command to designate a class map and enter the Class Map configuration mode. Then use match commands to specify the criteria for ingress traffic that will be classified under this class map.
- One or more class maps can be assigned to a policy map (page 1411). The policy map is then bound by a service policy to an interface (page 1421). A service policy defines packet classification, service tagging, and bandwidth policing. Once a policy map has been bound to an interface, no additional class maps may be added to the policy map, nor any changes made to the assigned class maps with the match or **set** commands.

EXAMPLE

This example creates a class map call "rd-class," and sets it to match packets marked for DSCP service value 3:

```
Console(config)#class-map rd-class match-any
Console(config-cmap)#match ip dscp 3
Console(config-cmap)#
```

RELATED COMMANDS

show class-map (1422)

description

This command specifies the description of a class map or policy map.

SYNTAX

description *string*

string - Description of the class map or policy map. (Range: 1-64 characters)

COMMAND MODE

Class Map Configuration
Policy Map Configuration

EXAMPLE

```
Console(config)#class-map rd-class#1
Console(config-cmap)#description matches packets marked for DSCP service
  value 3
Console(config-cmap)#
```

match

This command defines the criteria used to classify traffic. Use the **no** form to delete the matching criteria.

SYNTAX

[**no**] **match** {**access-list** *acl-name* | **cos** *cos* | **ip dscp** *dscp* |
ip precedence *ip-precedence* | **ipv6 dscp** *dscp* | **vlan** *vlan*}

acl-name - Name of the access control list. Any type of ACL can be specified, including standard or extended IPv4/IPv6 ACLs and MAC ACLs. (Range: 1-16 characters)

cos - A Class of Service value. (Range: 0-7)

dscp - A Differentiated Service Code Point value. (Range: 0-63)

ip-precedence - An IP Precedence value. (Range: 0-7)

vlan - A VLAN. (Range:1-4094)

DEFAULT SETTING

None

COMMAND MODE

Class Map Configuration

COMMAND USAGE

- First enter the class-map command to designate a class map and enter the Class Map configuration mode. Then use **match** commands to specify the fields within ingress packets that must match to qualify for this class map.

- If an ingress packet matches an ACL specified by this command, any deny rules included in the ACL will be ignored.

- If match criteria includes an IP ACL or IP priority rule, then a VLAN rule cannot be included in the same class map.

- If match criteria includes a MAC ACL or VLAN rule, then neither an IP ACL nor IP priority rule can be included in the same class map.

- Up to 16 match entries can be included in a class map.

EXAMPLE

This example creates a class map called "rd-class#1," and sets it to match packets marked for DSCP service value 3.

```
Console(config)#class-map rd-class#1 match-any
Console(config-cmap)#match ip dscp 3
Console(config-cmap)#
```

This example creates a class map call “rd-class#2,” and sets it to match packets marked for IP Precedence service value 5.

```
Console(config)#class-map rd-class#2 match-any
Console(config-cmap)#match ip precedence 5
Console(config-cmap)#
```

This example creates a class map call “rd-class#3,” and sets it to match packets marked for VLAN 1.

```
Console(config)#class-map rd-class#3 match-any
Console(config-cmap)#match vlan 1
Console(config-cmap)#
```

rename

This command redefines the name of a class map or policy map.

SYNTAX

rename *map-name*

map-name - Name of the class map or policy map. (Range: 1-32 characters)

COMMAND MODE

Class Map Configuration
Policy Map Configuration

EXAMPLE

```
Console(config)#class-map rd-class#1
Console(config-cmap)#rename rd-class#9
Console(config-cmap)#
```

policy-map

This command creates a policy map that can be attached to multiple interfaces, and enters Policy Map configuration mode. Use the **no** form to delete a policy map.

SYNTAX

[**no**] **policy-map** *policy-map-name*

policy-map-name - Name of the policy map. (Range: 1-32 characters)

DEFAULT SETTING

None

COMMAND MODE

Global Configuration

COMMAND USAGE

- Use the **policy-map** command to specify the name of the policy map, and then use the class command to configure policies for traffic that matches the criteria defined in a class map.
- A policy map can contain multiple class statements that can be applied to the same interface with the service-policy command.
- Create a Class Map (page 1411) before assigning it to a Policy Map.

EXAMPLE

This example creates a policy called "rd-policy," uses the class command to specify the previously defined "rd-class," uses the **set** command to classify the service that incoming packets will receive, and then uses the police flow command to limit the average bandwidth to 100,000 Kbps, the burst rate to 4000 bytes, and configure the response to drop any violating packets.

```
Console(config)#policy-map rd-policy
Console(config-pmap)#class rd-class
Console(config-pmap-c)#set cos 0
Console(config-pmap-c)#police flow 10000 4000 conform-action transmit
  violate-action drop
Console(config-pmap-c)#
```

class

This command defines a traffic classification upon which a policy can act, and enters Policy Map Class configuration mode. Use the **no** form to delete a class map.

SYNTAX

[**no**] **class** *class-map-name*

class-map-name - Name of the class map. (Range: 1-32 characters)

DEFAULT SETTING

None

COMMAND MODE

Policy Map Configuration

COMMAND USAGE

- Use the policy-map command to specify a policy map and enter Policy Map configuration mode. Then use the **class** command to enter Policy Map Class configuration mode. And finally, use the **set** command and one of the **police** commands to specify the match criteria, where the:
  - set phb command sets the per-hop behavior value in matching packets. (This modifies packet priority for internal processing only.)
  - set cos command sets the class of service value in matching packets. (This modifies packet priority in the VLAN tag.)

- **police** commands define parameters such as the maximum throughput, burst rate, and response to non-conforming traffic.

- Up to 16 classes can be included in a policy map.

EXAMPLE

This example creates a policy called "rd-policy," uses the **class** command to specify the previously defined "rd-class," uses the set phb command to classify the service that incoming packets will receive, and then uses the police flow command to limit the average bandwidth to 100,000 Kbps, the burst rate to 4,000 bytes, and configure the response to drop any violating packets.

```
Console(config)#policy-map rd-policy
Console(config-pmap)#class rd-class
Console(config-pmap-c)#set phb 3
Console(config-pmap-c)#police flow 10000 4000 conform-action transmit
  violate-action drop
Console(config-pmap-c)#
```

police flow

This command defines an enforcer for classified traffic based on the metered flow rate. Use the no form to remove a policer.

SYNTAX

[**no**] **police flow** *committed-rate committed-burst*
conform-action {**transmit** | *new-dscp*}
violate-action {**drop**| *new-dscp*}

committed-rate - Committed information rate (CIR) in kilobits per second. (Range: 0-1000000 kbps or maximum port speed, whichever is lower)

committed-burst - Committed burst size (BC) in bytes. (Range: 0-524288 bytes)

conform-action - Action to take when packet is within the CIR and BC. (There are enough tokens to service the packet, the packet is set green).

violate-action - Action to take when packet exceeds the CIR and BC. (There are not enough tokens to service the packet, the packet is set red).

transmit - Transmits without taking any action.

drop - Drops packet as required by violate-action.

new-dscp - Differentiated Service Code Point (DSCP) value. (Range: 0-63)

DEFAULT SETTING

None

COMMAND MODE

Policy Map Class Configuration

COMMAND USAGE

- You can configure up to 16 policers (i.e., class maps) for ingress ports.

- The *committed-rate* cannot exceed the configured interface speed, and the *committed-burst* cannot exceed 16 Mbytes.

- Policing is based on a token bucket, where bucket depth (i.e., the maximum burst before the bucket overflows) is by specified the *committed-burst* field, and the average rate tokens are added to the bucket is by specified by the *committed-rate* option. Note that the token bucket functions similar to that described in RFC 2697 and RFC 2698.

- The behavior of the meter is specified in terms of one token bucket (C), the rate at which the tokens are incremented (CIR – Committed Information Rate), and the maximum size of the token bucket (BC – Committed Burst Size).

  The token bucket C is initially full, that is, the token count Tc(0) = BC. Thereafter, the token count Tc is updated CIR times per second as follows:

  - If Tc is less than BC, Tc is incremented by one, else
  - Tc is not incremented.

  When a packet of size B bytes arrives at time t, the following happens:

  - If Tc(t)-B ≥ 0, the packet is green and Tc is decremented by B down to the minimum value of 0, else
  - else the packet is red and Tc is not decremented.

EXAMPLE

This example creates a policy called "rd-policy," uses the class command to specify the previously defined "rd-class," uses the set phb command to classify the service that incoming packets will receive, and then uses the **police flow** command to limit the average bandwidth to 100,000 Kbps, the burst rate to 4000 bytes, and configure the response to drop any violating packets.

```
Console(config)#policy-map rd-policy
Console(config-pmap)#class rd-class
Console(config-pmap-c)#set phb 3
Console(config-pmap-c)#police flow 100000 4000 conform-action transmit
  violate-action drop
Console(config-pmap-c)#
```

police srtcm-color

This command defines an enforcer for classified traffic based on a single rate three color meter (srTCM). Use the **no** form to remove a policer.

SYNTAX

[**no**] **police** {**srtcm-color-blind** | **srtcm-color-aware**}
committed-rate committed-burst excess-burst
conform-action {**transmit** | *new-dscp*}
exceed-action {**drop** | *new-dscp*}
violate action {**drop** | *new-dscp*}

srtcm-color-blind - Single rate three color meter in color-blind mode.

srtcm-color-aware - Single rate three color meter in color-aware mode.

committed-rate - Committed information rate (CIR) in kilobits per second. (Range: 0-1000000 kbps or maximum port speed, whichever is lower)

committed-burst - Committed burst size (BC) in bytes. (Range: 0-524288 bytes)

excess-burst - Excess burst size (BE) in bytes. (Range: 0-524288 bytes)

conform-action - Action to take when rate is within the CIR and BC. (There are enough tokens in bucket BC to service the packet, packet is set green).

exceed-action - Action to take when rate exceeds the CIR and BC but is within the BE. (There are enough tokens in bucket BE to service the packet, the packet is set yellow.)

violate-action - Action to take when rate exceeds the BE. (There are not enough tokens in bucket BE to service the packet, the packet is set red.)

transmit - Transmits without taking any action.

drop - Drops packet as required by exceed-action or violate-action.

new-dscp - Differentiated Service Code Point (DSCP) value. (Range: 0-63)

DEFAULT SETTING

None

COMMAND MODE

Policy Map Class Configuration

COMMAND USAGE

- You can configure up to 16 policers (i.e., class maps) for ingress ports.

- The *committed-rate* cannot exceed the configured interface speed, and the *committed-burst* and *excess-burst* cannot exceed 16 Mbytes.

- The srTCM as defined in RFC 2697 meters a traffic stream and processes its packets according to three traffic parameters – Committed Information Rate (CIR), Committed Burst Size (BC), and Excess Burst Size (BE).

- The PHB label is composed of five bits, three bits for per-hop behavior, and two bits for the color scheme used to control queue congestion. A packet is marked green if it doesn't exceed the CIR and BC, yellow if it does exceed the CIR and BC, but not the BE, and red otherwise.

- The meter operates in one of two modes. In the color-blind mode, the meter assumes that the packet stream is uncolored. In color-aware mode the meter assumes that some preceding entity has pre-colored the incoming packet stream so that each packet is either green, yellow, or red. The marker (re)colors an IP packet according to the results of the meter. The color is coded in the DS field [RFC 2474] of the packet.

- The behavior of the meter is specified in terms of its mode and two token buckets, C and E, which both share the common rate CIR. The maximum size of the token bucket C is BC and the maximum size of the token bucket E is BE.

  The token buckets C and E are initially full, that is, the token count Tc(0) = BC and the token count Te(0) = BE. Thereafter, the token counts Tc and Te are updated CIR times per second as follows:

  - If Tc is less than BC, Tc is incremented by one, else
  - if Te is less then BE, Te is incremented by one, else
  - neither Tc nor Te is incremented.

  When a packet of size B bytes arrives at time t, the following happens if srTCM is configured to operate in color-blind mode:

  - If Tc(t)-B ≥ 0, the packet is green and Tc is decremented by B down to the minimum value of 0, else
  - if Te(t)-B ≥ 0, the packets is yellow and Te is decremented by B down to the minimum value of 0,
  - else the packet is red and neither Tc nor Te is decremented.

  When a packet of size B bytes arrives at time t, the following happens if srTCM is configured to operate in color-aware mode:

  - If the packet has been precolored as green and Tc(t)-B ≥ 0, the packet is green and Tc is decremented by B down to the minimum value of 0, else
  - If the packet has been precolored as yellow or green and if
  - Te(t)-B ≥ 0, the packets is yellow and Te is decremented by B down to the minimum value of 0, else the packet is red and neither Tc nor Te is decremented.

  The metering policy guarantees a deterministic behavior where the volume of green packets is never smaller than what has been determined by the CIR and BC, that is, tokens of a given color are always spent on packets of that color. Refer to RFC 2697 for more information on other aspects of srTCM.

EXAMPLE

This example creates a policy called “rd-policy,” uses the class command to specify the previously defined “rd-class,” uses the set phb command to classify the service that incoming packets will receive, and then uses the **police srtcm-color-blind** command to limit the average bandwidth to 100,000 Kbps, the committed burst rate to 4000 bytes, the excess burst rate to 6000 bytes, to remark any packets exceeding the committed burst size, and to drop any packets exceeding the excess burst size.

```
Console(config)#policy-map rd-policy
Console(config-pmap)#class rd-class
Console(config-pmap-c)#set phb 3
Console(config-pmap-c)#police srtcm-color-blind 100000 4000 6000 conform-
  action transmit exceed-action 0 violate-action drop
Console(config-pmap-c)#
```

police trtcm-color

This command defines an enforcer for classified traffic based on a two rate three color meter (trTCM). Use the **no** form to remove a policer.

SYNTAX

[**no**] **police** {**trtcm-color-blind** | **trtcm-color-aware**}
committed-rate committed-burst peak-rate peak-burst
conform-action {**transmit** | *new-dscp*}
exceed-action {**drop** | *new-dscp*}
violate action {**drop** | *new-dscp*}

trtcm-color-blind - Two rate three color meter in color-blind mode.

trtcm-color-aware - Two rate three color meter in color-aware mode.

committed-rate - Committed information rate (CIR) in kilobits per second. (Range: 0-1000000 kbps or maximum port speed, whichever is lower)

committed-burst - Committed burst size (BC) in bytes. (Range: 0-524288 bytes)

peak-rate - Peak information rate (PIR) in kilobits per second. (Range: 0-1000000 kbps or maximum port speed, whichever is lower)

peak-burst - Peak burst size (BP) in bytes. (Range: 0-524288 bytes)

conform-action - Action to take when rate is within the CIR and BP. (Packet size does not exceed BP and there are enough tokens in bucket BC to service the packet, the packet is set green.)

exceed-action - Action to take when rate exceeds the CIR but is within the PIR. (Packet size exceeds BC but there are enough tokens in bucket BP to service the packet, the packet is set yellow.)

violate-action - Action to take when rate exceeds the PIR. (There are not enough tokens in bucket BP to service the packet, the packet is set red.)

drop - Drops packet as required by exceed-action or violate-action.

transmit - Transmits without taking any action.

new-dscp - Differentiated Service Code Point (DSCP) value. (Range: 0-63)

DEFAULT SETTING

None

COMMAND MODE

Policy Map Class Configuration

COMMAND USAGE

- You can configure up to 16 policers (i.e., class maps) for ingress ports.
- The *committed-rate* and *peak-rate* cannot exceed the configured interface speed, and the *committed-burst* and *peak-burst* cannot exceed 16 Mbytes.
- The trTCM as defined in RFC 2698 meters a traffic stream and processes its packets based on two rates – Committed Information Rate (CIR) and Peak Information Rate (PIR), and their associated burst sizes - Committed Burst Size (BC) and Peak Burst Size (BP).
- The PHB label is composed of five bits, three bits for per-hop behavior, and two bits for the color scheme used to control queue congestion. A packet is marked red if it exceeds the PIR. Otherwise it is marked either yellow or green depending on whether it exceeds or doesn't exceed the CIR.

  The trTCM is useful for ingress policing of a service, where a peak rate needs to be enforced separately from a committed rate.
- The meter operates in one of two modes. In the color-blind mode, the meter assumes that the packet stream is uncolored. In color-aware mode the meter assumes that some preceding entity has pre-colored the incoming packet stream so that each packet is either green, yellow, or red. The marker (re)colors an IP packet according to the results of the meter. The color is coded in the DS field [RFC 2474] of the packet.
- The behavior of the meter is specified in terms of its mode and two token buckets, P and C, which are based on the rates PIR and CIR, respectively. The maximum size of the token bucket P is BP and the maximum size of the token bucket C is BC.
- The token buckets P and C are initially (at time 0) full, that is, the token count Tp(0) = BP and the token count Tc(0) = BC. Thereafter, the token count Tp is incremented by one PIR times per second up to BP and the token count Tc is incremented by one CIR times per second up to BC.

When a packet of size B bytes arrives at time t, the following happens if trTCM is configured to operate in color-blind mode:

- If Tp(t)-B < 0, the packet is red, else
- if Tc(t)-B < 0, the packet is yellow and Tp is decremented by B, else
- the packet is green and both Tp and Tc are decremented by B.

When a packet of size B bytes arrives at time t, the following happens if trTCM is configured to operate in color-aware mode:

- If the packet has been precolored as red or if Tp(t)-B < 0, the packet is red, else
- if the packet has been precolored as yellow or if Tc(t)-B < 0, the packet is yellow and Tp is decremented by B, else
- the packet is green and both Tp and Tc are decremented by B.

◆ The trTCM can be used to mark a IP packet stream in a service, where different, decreasing levels of assurances (either absolute or relative) are given to packets which are green, yellow, or red. Refer to RFC 2698 for more information on other aspects of trTCM.

EXAMPLE

This example creates a policy called "rd-policy," uses the class command to specify the previously defined "rd-class," uses the set phb command to classify the service that incoming packets will receive, and then uses the **police trtcm-color-blind** command to limit the average bandwidth to 100,000 Kbps, the committed burst rate to 4000 bytes, the peak information rate to 1,000,000 kbps, the peak burst size to 6000, to remark any packets exceeding the committed burst size, and to drop any packets exceeding the peak information rate.

```
Console(config)#policy-map rd-policy
Console(config-pmap)#class rd-class
Console(config-pmap-c)#set phb 3
Console(config-pmap-c)#police trtcm-color-blind 100000 4000 100000 6000
  conform-action transmit exceed-action 0 violate-action drop
Console(config-pmap-c)#
```

set cos

This command modifies the class of service (CoS) value for a matching packet (as specified by the match command) in the packet's VLAN tag. Use the **no** form to remove this setting.

SYNTAX

[**no**] **set cos** *cos-value*

cos-value - Class of Service value. (Range: 0-7)

DEFAULT SETTING

None

COMMAND MODE

Policy Map Class Configuration

COMMAND USAGE

- The **set cos** command is used to set the CoS value in the VLAN tag for matching packets.
- The **set cos** and set phb command function at the same level of priority. Therefore setting either of these commands will overwrite any action already configured by the other command.

EXAMPLE

This example creates a policy called "rd-policy," uses the class command to specify the previously defined "rd-class," uses the **set cos** command to classify the service that incoming packets will receive, and then uses the police flow command to limit the average bandwidth to 100,000 Kbps, the burst rate to 4000 bytes, and configure the response to drop any violating packets.

```
Console(config)#policy-map rd-policy
Console(config-pmap)#class rd-class
Console(config-pmap-c)#set cos 3
Console(config-pmap-c)#police flow 10000 4000 conform-action transmit
  violate-action drop
Console(config-pmap-c)#
```

set phb

This command services IP traffic by setting a per-hop behavior value for a matching packet (as specified by the match command) for internal processing. Use the **no** form to remove this setting.

SYNTAX

[**no**] **set phb** *phb-value*

phb-value - Per-hop behavior value. (Range: 0-7)

DEFAULT SETTING

None

COMMAND MODE

Policy Map Class Configuration

COMMAND USAGE

- The **set phb** command is used to set an internal QoS value in hardware for matching packets (see Table 175, "Default Mapping of CoS/CFI to Internal PHB/Drop Precedence"). The QoS label is composed of five bits, three bits for per-hop behavior, and two bits for the color scheme used to control queue congestion by the police srtcm-color command and police trtcm-color command.
- The set cos and **set phb** command function at the same level of priority. Therefore setting either of these commands will overwrite any action already configured by the other command.

EXAMPLE

This example creates a policy called “rd-policy,” uses the class command to specify the previously defined “rd-class,” uses the **set phb** command to classify the service that incoming packets will receive, and then uses the police flow command to limit the average bandwidth to 100,000 Kbps, the burst rate to 4000 bytes, and configure the response to drop any violating packets.

```
Console(config)#policy-map rd-policy
Console(config-pmap)#class rd-class
Console(config-pmap-c)#set phb 3
Console(config-pmap-c)#police flow 10000 4000 conform-action transmit
  violate-action drop
Console(config-pmap-c)#
```

service-policy

This command applies a policy map defined by the **policy-map** command to the ingress or egress side of a particular interface. Use the **no** form to remove this mapping.

SYNTAX

[**no**] **service-policy input** *policy-map-name*

input - Apply to the input traffic.

output - Apply to the output traffic.

policy-map-name - Name of the policy map for this interface. (Range: 1-32 characters)

DEFAULT SETTING

No policy map is attached to an interface.

COMMAND MODE

Interface Configuration (Ethernet, Port Channel)

COMMAND USAGE

- Only one policy map can be assigned to an interface.

- First define a class map, then define a policy map, and finally use the **service-policy** command to bind the policy map to the required interface.

EXAMPLE

This example applies a service policy to an ingress interface.

```
Console(config)#interface ethernet 1/1
Console(config-if)#service-policy input rd-policy
Console(config-if)#
```

show class-map

This command displays the QoS class maps which define matching criteria used for classifying traffic.

SYNTAX

show class-map [*class-map-name*]

class-map-name - Name of the class map. (Range: 1-32 characters)

DEFAULT SETTING

Displays all class maps.

COMMAND MODE

Privileged Exec

EXAMPLE

```
Console#show class-map
Class Map match-any rd-class#1
Description:
 Match IP DSCP 10
 Match access-list rd-access
 Match IP DSCP 0

Class Map match-any rd-class#2
 Match IP Precedence 5

Class Map match-any rd-class#3
 Match VLAN 1

Console#
```

show policy-map

This command displays the QoS policy maps which define classification criteria for incoming traffic, and may include policers for bandwidth limitations.

SYNTAX

show policy-map [*policy-map-name* [**class** *class-map-name*]]

policy-map-name - Name of the policy map.
(Range: 1-32 characters)

class-map-name - Name of the class map. (Range: 1-32 characters)

DEFAULT SETTING

Displays all policy maps and all classes.

COMMAND MODE

Privileged Exec

EXAMPLE

```
Console#show policy-map
Policy Map rd-policy
```

```
Description:
 class rd-class
 set phb 3
Console#show policy-map rd-policy class rd-class
Policy Map rd-policy
 class rd-class
 set phb 3
Console#
```

show policy-map interface

This command displays the service policy assigned to the specified interface.

SYNTAX

show policy-map interface *interface* **input**

interface

unit/port

unit - Unit identifier. (Range: 1)

port - Port number. (Range: 1-28)

port-channel *channel-id* (Range: 1-8)

COMMAND MODE

Privileged Exec

EXAMPLE

```
Console#show policy-map interface 1/5 input
Service-policy rd-policy
Console#
```

43 Multicast Filtering Commands

This switch uses IGMP (Internet Group Management Protocol) to check for any attached hosts that want to receive a specific multicast service. It identifies the ports containing hosts requesting a service and sends data out to those ports only. It then propagates the service request up to any neighboring multicast switch/router to ensure that it will continue to receive the multicast service.

Note that IGMP query can be enabled globally at Layer 2, or enabled for specific VLAN interfaces at Layer 3. (Layer 2 query is disabled if Layer 3 query is enabled.)

Table 182: Multicast Filtering Commands

Command Group	Function
IGMP Snooping	Configures multicast groups via IGMP snooping or static assignment, sets the IGMP version, enables proxy reporting, displays current snooping settings, and displays the multicast service and group members
Static Multicast Routing	Configures static multicast router ports which forward all inbound multicast traffic to the attached VLANs
IGMP Filtering and Throttling	Configures IGMP filtering and throttling
MLD Snooping	Configures multicast snooping for IPv6
MLD Filtering and Throttling	Configures MLD filtering and throttling for IPv6.
MVR for IPv4	Configures a single network-wide multicast VLAN shared by hosts residing in other standard or private VLAN groups, preserving security and data isolation for normal traffic
MVR for IPv6	Configures a single network-wide multicast VLAN shared by hosts residing in other standard or private VLAN groups, preserving security and data isolation for normal traffic
IGMP (Layer 3)	Configures the IGMP protocol used with multicast routing in IPv4 networks
IGMP Proxy Routing	Collects and sends multicast group membership information onto the upstream interface based on IGMP messages monitored on downstream interfaces, and forwards multicast traffic based on that information
MLD (Layer 3)	Configures the MLD protocol used with multicast routing in IPv6 networks
MLD Proxy Routing	Collects and sends multicast group membership information onto the upstream interface based on MLD messages monitored on downstream interfaces, and forwards multicast traffic based on that information

IGMP SNOOPING

This section describes commands used to configure IGMP snooping on the switch.

Table 183: IGMP Snooping Commands

Command	Function	Mode
ip igmp snooping	Enables IGMP snooping	GC
ip igmp snooping priority	Assigns a priority to all multicast traffic	GC
ip igmp snooping proxy-reporting	Enables IGMP Snooping with Proxy Reporting	GC
ip igmp snooping querier	Allows this device to act as the querier for IGMP snooping	GC
ip igmp snooping router-alert-option-check	Discards any IGMPv2/v3 packets that do not include the Router Alert option	GC
ip igmp snooping router-port-expire-time	Configures the querier timeout	GC
ip igmp snooping tcn-flood	Floods multicast traffic when a Spanning Tree topology change occurs	GC
ip igmp snooping tcn-query-solicit	Sends an IGMP Query Solicitation when a Spanning Tree topology change occurs	GC
ip igmp snooping unregistered-data-flood	Floods unregistered multicast traffic into the attached VLAN	GC
ip igmp snooping unsolicited-report-interval	Specifies how often the upstream interface should transmit unsolicited IGMP reports (when proxy reporting is enabled)	GC
ip igmp snooping version	Configures the IGMP version for snooping	GC
ip igmp snooping version-exclusive	Discards received IGMP messages which use a version different to that currently configured	GC
ip igmp snooping vlan general-query-suppression	Suppresses general queries except for ports attached to downstream multicast hosts	GC
ip igmp snooping vlan immediate-leave	Immediately deletes a member port of a multicast service if a leave packet is received at that port and immediate-leave is enabled for the parent VLAN	GC
ip igmp snooping vlan last-memb-query-count	Configures the number of IGMP proxy query messages that are sent out before the system assumes there are no local members	GC
ip igmp snooping vlan last-memb-query-intvl	Configures the last-member-query interval	GC
ip igmp snooping vlan mrd	Sends multicast router solicitation messages	GC
ip igmp snooping vlan proxy-address	Configures a static address for proxy IGMP query and reporting	GC
ip igmp snooping vlan proxy-reporting	Enables IGMP Snooping with Proxy Reporting	GC
ip igmp snooping vlan query-interval	Configures the interval between sending IGMP general queries	GC
ip igmp snooping vlan query-resp-intvl	Configures the maximum time the system waits for a response to general queries	GC

Table 183: IGMP Snooping Commands (Continued)

Command	Function	Mode
ip igmp snooping vlan static	Adds an interface as a member of a multicast group	GC
ip igmp snooping vlan version	Configures the IGMP version for snooping	GC
ip igmp snooping vlan version-exclusive	Discards received IGMP messages which use a version different to that currently configured	GC
show ip igmp snooping	Shows the IGMP snooping, proxy, and query configuration	PE
show ip igmp snooping group	Shows known multicast group, source, and host port mapping	PE
show ip igmp snooping statistics	Shows IGMP snooping protocol statistics for the specified interface	PE

ip igmp snooping

This command enables IGMP snooping globally on the switch or on a selected VLAN interface. Use the **no** form to disable it.

SYNTAX

[**no**] **ip igmp snooping** [**vlan** *vlan-id*]

vlan-id - VLAN ID (Range: 1-4094)

DEFAULT SETTING

Enabled

COMMAND MODE

Global Configuration

COMMAND USAGE

- When IGMP snooping is enabled globally, the per VLAN interface settings for IGMP snooping take precedence.

- When IGMP snooping is disabled globally, snooping can still be configured per VLAN interface, but the interface settings will not take effect until snooping is re-enabled globally.

EXAMPLE

The following example enables IGMP snooping globally.

```
Console(config)#ip igmp snooping
Console(config)#
```

ip igmp snooping priority

This command assigns a priority to all multicast traffic. Use the **no** form to restore the default setting.

SYNTAX

ip igmp snooping priority *priority*

no ip igmp snooping priority

priority - The CoS priority assigned to all multicast traffic. (Range: 0-7, where 7 is the highest priority)

DEFAULT SETTING

2

COMMAND MODE

Global Configuration

COMMAND USAGE

This command can be used to set a high priority for low-latency multicast traffic such as a video-conference, or to set a low priority for normal multicast traffic not sensitive to latency.

EXAMPLE

```
Console(config)#ip igmp snooping priority 6
Console(config)#
```

RELATED COMMANDS

show ip igmp snooping (1442)

ip igmp snooping proxy-reporting

This command enables IGMP Snooping with Proxy Reporting. Use the **no** form to restore the default setting.

SYNTAX

[**no**] **ip igmp snooping proxy-reporting**

ip igmp snooping vlan *vlan-id* **proxy-reporting** {**enable** | **disable**}
no ip igmp snooping vlan *vlan-id* **proxy-reporting**

vlan-id - VLAN ID (Range: 1-4094)

enable - Enable on the specified VLAN.

disable - Disable on the specified VLAN.

DEFAULT SETTING

Global: Enabled
VLAN: Based on global setting

COMMAND MODE

Global Configuration

COMMAND USAGE

- When proxy reporting is enabled with this command, the switch performs "IGMP Snooping with Proxy Reporting" (as defined in DSL Forum TR-101, April 2006), including last leave, and query suppression. Last leave sends out a proxy query when the last member leaves a multicast group, and query suppression means that specific queries are not forwarded from an upstream multicast router to hosts downstream from this device.

- If the IGMP proxy reporting is configured on a VLAN, this setting takes precedence over the global configuration.

EXAMPLE

```
Console(config)#ip igmp snooping proxy-reporting
Console(config)#
```

ip igmp snooping querier

This command enables the switch as an IGMP querier. Use the **no** form to disable it.

SYNTAX

[**no**] **ip igmp snooping querier**

DEFAULT SETTING

Enabled

COMMAND MODE

Global Configuration

COMMAND USAGE

- IGMP snooping querier is not supported for IGMPv3 snooping (see ip igmp snooping version).

- If enabled, the switch will serve as querier if elected. The querier is responsible for asking hosts if they want to receive multicast traffic.

EXAMPLE

```
Console(config)#ip igmp snooping querier
Console(config)#
```

ip igmp snooping router-alert-option-check

This command discards any IGMPv2/v3 packets that do not include the Router Alert option. Use the **no** form to ignore the Router Alert Option when receiving IGMP messages.

SYNTAX

[**no**] **ip igmp snooping router-alert-option-check**

DEFAULT SETTING

Disabled

COMMAND MODE

Global Configuration

COMMAND USAGE

As described in Section 9.1 of RFC 3376 for IGMP Version 3, the Router Alert Option can be used to protect against DOS attacks. One common method of attack is launched by an intruder who takes over the role of querier, and starts overloading multicast hosts by sending a large number of group-and-source-specific queries, each with a large source list and the Maximum Response Time set to a large value.

To protect against this kind of attack, (1) routers should not forward queries. This is easier to accomplish if the query carries the Router Alert option. (2) Also, when the switch is acting in the role of a multicast host (such as when using proxy routing), it should ignore version 2 or 3 queries that do not contain the Router Alert option.

EXAMPLE

```
Console(config)#ip igmp snooping router-alert-option-check
Console(config)#
```

ip igmp snooping router-port-expire-time

This command configures the querier timeout. Use the **no** form to restore the default.

SYNTAX

ip igmp snooping router-port-expire-time *seconds*

no ip igmp snooping router-port-expire-time

seconds - The time the switch waits after the previous querier stops before it considers it to have expired. (Range: 1-65535; Recommended Range: 300-500)

DEFAULT SETTING

300 seconds

COMMAND MODE

Global Configuration

EXAMPLE

The following shows how to configure the timeout to 400 seconds:

```
Console(config)#ip igmp snooping router-port-expire-time 400
Console(config)#
```

ip igmp snooping tcn-flood

This command enables flooding of multicast traffic if a spanning tree topology change notification (TCN) occurs. Use the **no** form to disable flooding.

SYNTAX

[**no**] **ip igmp snooping tcn-flood**

DEFAULT SETTING

Disabled

COMMAND MODE

Global Configuration

COMMAND USAGE

- When a spanning tree topology change occurs, the multicast membership information learned by the switch may be out of date. For example, a host linked to one port before the topology change (TC) may be moved to another port after the change. To ensure that multicast data is delivered to all receivers, by default, a switch in a VLAN (with IGMP snooping enabled) that receives a Bridge Protocol Data Unit (BPDU) with the TC bit set (by the root bridge) will enter into "multicast flooding mode" for a period of time until the topology has stabilized and the new locations of all multicast receivers are learned.

- If a topology change notification (TCN) is received, and all the uplink ports are subsequently deleted, a timeout mechanism is used to delete all of the currently learned multicast channels.

- When a new uplink port starts up, the switch sends unsolicited reports for all current learned channels out through the new uplink port.

- By default, the switch immediately enters into "multicast flooding mode" when a spanning tree topology change occurs. In this mode, multicast traffic will be flooded to all VLAN ports. If many ports have subscribed to different multicast groups, flooding may cause excessive loading on the link between the switch and the end host. Flooding may be disabled to avoid this, causing multicast traffic to be delivered only to those ports on which multicast group members have been learned.

- When the spanning tree topology changes, the root bridge sends a proxy query to quickly re-learn the host membership/port relations for multicast channels. The root bridge also sends an unsolicited Multicast Router Discover (MRD) request to quickly locate the multicast routers in this VLAN.

  The proxy query and unsolicited MRD request are flooded to all VLAN ports except for the receiving port when the switch receives such packets.

EXAMPLE

The following example enables TCN flooding.

```
Console(config)#ip igmp snooping tcn-flood
Console(config)#
```

ip igmp snooping tcn-query-solicit

This command instructs the switch to send out an IGMP general query solicitation when a spanning tree topology change notification (TCN) occurs. Use the **no** form to disable this feature.

SYNTAX

[**no**] **ip igmp snooping tcn-query-solicit**

DEFAULT SETTING

Disabled

COMMAND MODE

Global Configuration

COMMAND USAGE

- When the root bridge in a spanning tree receives a topology change notification for a VLAN where IGMP snooping is enabled, it issues a global IGMP leave message (query solicitation). When a switch receives this solicitation, it floods it to all ports in the VLAN where the spanning tree change occurred. When an upstream multicast router receives this solicitation, it will also immediately issues an IGMP general query.

- The **ip igmp snooping tcn query-solicit** command can be used to send a query solicitation whenever it notices a topology change, even if the switch is not the root bridge in the spanning tree.

EXAMPLE

The following example instructs the switch to issue an IGMP general query whenever it receives a spanning tree topology change notification.

```
Console(config)#ip igmp snooping tcn query-solicit
Console(config)#
```

ip igmp snooping unregistered-data-flood

This command floods unregistered multicast traffic into the attached VLAN. Use the **no** form to drop unregistered multicast traffic.

SYNTAX

[**no**] **ip igmp snooping unregistered-data-flood**

DEFAULT SETTING

Disabled

COMMAND MODE

Global Configuration

COMMAND USAGE

Once the table used to store multicast entries for IGMP snooping and multicast routing is filled, no new entries are learned. If no router port is configured in the attached VLAN, and unregistered-flooding is disabled, any subsequent multicast traffic not found in the table is dropped, otherwise it is flooded throughout the VLAN.

EXAMPLE

```
Console(config)#ip igmp snooping unregistered-data-flood
Console(config)#
```

ip igmp snooping unsolicited-report-interval

This command specifies how often the upstream interface should transmit unsolicited IGMP reports when proxy reporting is enabled. Use the **no** form to restore the default value.

SYNTAX

ip igmp snooping unsolicited-report-interval *seconds*

no ip igmp snooping version-exclusive

seconds - The interval at which to issue unsolicited reports. (Range: 1-65535 seconds)

DEFAULT SETTING

400 seconds

COMMAND MODE

Global Configuration

COMMAND USAGE

- When a new upstream interface (that is, uplink port) starts up, the switch sends unsolicited reports for all currently learned multicast channels out through the new upstream interface.

- This command only applies when proxy reporting is enabled (see page 1428).

EXAMPLE

```
Console(config)#ip igmp snooping unsolicited-report-interval 5
Console(config)#
```

ip igmp snooping version

This command configures the IGMP snooping version. Use the **no** form to restore the default.

SYNTAX

ip igmp snooping [**vlan** *vlan-id*] **version** {**1** | **2** | **3**}

no ip igmp snooping version

vlan-id - VLAN ID (Range: 1-4094)

1 - IGMP Version 1

2 - IGMP Version 2

3 - IGMP Version 3

DEFAULT SETTING

Global: IGMP Version 2
VLAN: Not configured, based on global setting

COMMAND MODE

Global Configuration

COMMAND USAGE

- This command configures the IGMP report/query version used by IGMP snooping. Versions 1 - 3 are all supported, and versions 2 and 3 are backward compatible, so the switch can operate with other devices, regardless of the snooping version employed.

- If the IGMP snooping version is configured on a VLAN, this setting takes precedence over the global configuration.

EXAMPLE

The following configures the global setting for IGMP snooping to version 1.

```
Console(config)#ip igmp snooping version 1
Console(config)#
```

ip igmp snooping version-exclusive

This command discards any received IGMP messages (except for multicast protocol packets) which use a version different to that currently configured by the ip igmp snooping version command. Use the **no** form to disable this feature.

SYNTAX

ip igmp snooping [**vlan** *vlan-id*] **version-exclusive**

no ip igmp snooping version-exclusive

vlan-id - VLAN ID (Range: 1-4094)

DEFAULT SETTING

Global: Disabled
VLAN: Disabled

COMMAND MODE

Global Configuration

COMMAND USAGE

- If version exclusive is disabled on a VLAN, then this setting is based on the global setting. If it is enabled on a VLAN, then this setting takes precedence over the global setting.

- When this function is disabled, the currently selected version is backward compatible (see the ip igmp snooping version command.

EXAMPLE

```
Console(config)#ip igmp snooping version-exclusive
Console(config)#
```

ip igmp snooping vlan general-query-suppression

This command suppresses general queries except for ports attached to downstream multicast hosts. Use the **no** form to flood general queries to all ports except for the multicast router port.

SYNTAX

[**no**] **ip igmp snooping vlan** *vlan-id* **general-query-suppression**

vlan-id - VLAN ID (Range: 1-4094)

DEFAULT SETTING

Disabled

COMMAND MODE

Global Configuration

COMMAND USAGE

- By default, general query messages are flooded to all ports, except for the multicast router through which they are received.

- If general query suppression is enabled, then these messages are forwarded only to downstream ports which have joined a multicast service.

EXAMPLE

```
Console(config)#ip igmp snooping vlan 1 general-query-suppression
Console(config)#
```

ip igmp snooping vlan immediate-leave

This command immediately deletes a member port of a multicast service if a leave packet is received at that port and immediate-leave is enabled for the parent VLAN. Use the **no** form to restore the default.

Syntax

[**no**] **ip igmp snooping vlan** *vlan-id* **immediate-leave**

vlan-id - VLAN ID (Range: 1-4094)

Default Setting

Disabled

Command Mode

Global Configuration

Command Usage

- If immediate-leave is *not* used, a multicast router (or querier) will send a group-specific query message when an IGMPv2/v3 group leave message is received. The router/querier stops forwarding traffic for that group only if no host replies to the query within the timeout period. (The timeout for this release is currently defined by ip igmp snooping vlan last-memb-query-intvl * ip igmp robustval.

- If immediate-leave is enabled, the switch assumes that only one host is connected to the interface. Therefore, immediate leave should only be enabled on an interface if it is connected to only one IGMP-enabled device, either a service host or a neighbor running IGMP snooping.

- This command is only effective if IGMP snooping is enabled, and IGMPv2 or IGMPv3 snooping is used.

Example

The following shows how to enable immediate leave.

```
Console(config)#ip igmp snooping vlan 1 immediate-leave
Console(config)#
```

ip igmp snooping vlan last-memb-query-count

This command configures the number of IGMP proxy group-specific or group-and-source-specific query messages that are sent out before the system assumes there are no more local members. Use the **no** form to restore the default.

SYNTAX

ip igmp snooping vlan *vlan-id* **last-memb-query-count** *count*

no ip igmp snooping vlan *vlan-id* **last-memb-query-count**

vlan-id - VLAN ID (Range: 1-4094)

count - The number of proxy group-specific or group-and-source-specific query messages to issue before assuming that there are no more group members. (Range: 1-255)

DEFAULT SETTING

2

COMMAND MODE

Global Configuration

COMMAND USAGE

This command will take effect only if IGMP snooping proxy reporting or IGMP querier is enabled (page 1428).

EXAMPLE

```
Console(config)#ip igmp snooping vlan 1 last-memb-query-count 7
Console(config)#
```

ip igmp snooping vlan last-memb-query-intvl

This command configures the last-member-query interval. Use the **no** form to restore the default.

SYNTAX

ip igmp snooping vlan *vlan-id* **last-memb-query-intvl** *interval*

no ip igmp snooping vlan *vlan-id* **last-memb-query-intvl**

vlan-id - VLAN ID (Range: 1-4094)

interval - The interval to wait for a response to a group-specific or group-and-source-specific query message. (Range: 1-31744 tenths of a second)

DEFAULT SETTING

10 (1 second)

COMMAND MODE

Global Configuration

COMMAND USAGE

- When a multicast host leaves a group, it sends an IGMP leave message. When the leave message is received by the switch, it checks to see if this host is the last to leave the group by sending out an IGMP group-specific or group-and-source-specific query message, and starts a timer. If no reports are received before the timer expires, the group record is deleted, and a report is sent to the upstream multicast router.

- A reduced value will result in reduced time to detect the loss of the last member of a group or source, but may generate more bursty traffic.

- This command will take effect only if IGMP snooping proxy reporting is enabled (page 1428).

EXAMPLE

```
Console(config)#ip igmp snooping vlan 1 last-memb-query-intvl 700
Console(config)#
```

ip igmp snooping vlan mrd

This command enables sending of multicast router solicitation messages. Use the **no** form to disable these messages.

SYNTAX

[**no**] **ip igmp snooping vlan** *vlan-id* **mrd**

vlan-id - VLAN ID (Range: 1-4094)

DEFAULT SETTING

Disabled

COMMAND MODE

Global Configuration

COMMAND USAGE

- Multicast Router Discovery (MRD) uses multicast router advertisement, multicast router solicitation, and multicast router termination messages to discover multicast routers. Devices send solicitation messages in order to solicit advertisement messages from multicast routers. These messages are used to discover multicast routers on a directly attached link. Solicitation messages are also sent whenever a multicast forwarding interface is initialized or re-initialized. Upon receiving a solicitation on an interface with IP multicast forwarding and MRD enabled, a router will respond with an advertisement.

- Advertisements are sent by routers to advertise that IP multicast forwarding is enabled. These messages are sent unsolicited periodically on all router interfaces on which multicast forwarding is enabled. They are sent upon the expiration of a periodic timer, as a part of a router's start up procedure, during the restart of a multicast forwarding interface, and on receipt of a solicitation message. When the multicast services provided to a VLAN is relatively stable, the use of solicitation messages is not required and may be disabled using the **no ip igmp snooping vlan mrd** command.

- This command may also be used to disable multicast router solicitation messages when the upstream router does not support MRD, to reduce the loading on a busy upstream router, or when IGMP snooping is disabled in a VLAN.

EXAMPLE

This example disables sending of multicast router solicitation messages on VLAN 1.

```
Console(config)#no ip igmp snooping vlan 1 mrd
Console(config)#
```

ip igmp snooping vlan proxy-address

This command configures a static source address for locally generated query and report messages used by IGMP proxy reporting. Use the **no** form to restore the default source address.

SYNTAX

[**no**] **ip igmp snooping vlan** *vlan-id* **proxy-address** *source-address*

vlan-id - VLAN ID (Range: 1-4094)

source-address - The source address used for proxied IGMP query and report, and leave messages. (Any valid IP unicast address)

DEFAULT SETTING

0.0.0.0

COMMAND MODE

Global Configuration

COMMAND USAGE

IGMP Snooping uses a null IP address of 0.0.0.0 for the source of IGMP query messages which are proxied to downstream hosts to indicate that it is not the elected querier, but is only proxying these messages as defined in RFC 4541. The switch also uses a null address in IGMP reports sent to upstream ports.

Many hosts do not implement RFC 4541, and therefore do not understand query messages with the source address of 0.0.0.0. These hosts will therefore not reply to the queries, causing the multicast router to stop sending traffic to them.

To resolve this problem, the source address in proxied IGMP query and report messages can be replaced with any valid unicast address (other than the router's own address) using this command.

Rules Used for Proxy Reporting

When IGMP Proxy Reporting is disabled, the switch will use a null IP address for the source of IGMP query and report messages unless a proxy query address has been set.

When IGMP Proxy Reporting is enabled, the source address is based on the following criteria:

- If a proxy query address is configured, the switch will use that address as the source IP address in general and group-specific query messages sent to downstream hosts, and in report and leave messages sent upstream from the multicast router port.
- If a proxy query address is not configured, the switch will use the VLAN's IP address as the IP source address in general and group-specific query messages sent downstream, and use the source address of the last IGMP message received from a downstream host in report and leave messages sent upstream from the multicast router port.

EXAMPLE

The following example sets the source address for proxied IGMP query messages to 10.0.1.8.

```
Console(config)#ip igmp snooping vlan 1 proxy-address 10.0.1.8
Console(config)#
```

ip igmp snooping vlan query-interval

This command configures the interval between sending IGMP general queries. Use the **no** form to restore the default.

SYNTAX

ip igmp snooping vlan *vlan-id* **query-interval** *interval*

no ip igmp snooping vlan *vlan-id* **query-interval**

vlan-id - VLAN ID (Range: 1-4094)

interval - The interval between sending IGMP general queries. (Range: 10-31744 seconds)

DEFAULT SETTING

100 (10 seconds)

COMMAND MODE

Global Configuration

COMMAND USAGE

- An IGMP general query message is sent by the switch at the interval specified by this command. When this message is received by downstream hosts, all receivers build an IGMP report for the multicast groups they have joined.

- This command applies when the switch is serving as the querier (page 1429), or as a proxy host when IGMP snooping proxy reporting is enabled (page 1428).

EXAMPLE

```
Console(config)#ip igmp snooping vlan 1 query-interval 150
Console(config)#
```

ip igmp snooping vlan query-resp-intvl

This command configures the maximum time the system waits for a response to general queries. Use the **no** form to restore the default.

SYNTAX

ip igmp snooping vlan *vlan-id* **query-resp-intvl** *interval*

no ip igmp snooping vlan *vlan-id* **query-resp-intvl**

vlan-id - VLAN ID (Range: 1-4094)

interval - The maximum time the system waits for a response to general queries. (Range: 10-31740 tenths of a second)

DEFAULT SETTING

100 (10 seconds)

COMMAND MODE

Global Configuration

COMMAND USAGE

This command applies when the switch is serving as the querier (page 1429), or as a proxy host when IGMP snooping proxy reporting is enabled (page 1428).

EXAMPLE

```
Console(config)#ip igmp snooping vlan 1 query-resp-intvl 20
Console(config)#
```

ip igmp snooping vlan static

This command adds a port to a multicast group. Use the **no** form to remove the port.

SYNTAX

[**no**] **ip igmp snooping vlan** *vlan-id* **static** *ip-address interface*

vlan-id - VLAN ID (Range: 1-4094)

ip-address - IP address for multicast group

interface

ethernet *unit/port*

unit - Unit identifier. (Range: 1)

port - Port number. (Range: 1-28)

port-channel *channel-id* (Range: 1-8)

DEFAULT SETTING

None

COMMAND MODE

Global Configuration

COMMAND USAGE

- Static multicast entries are never aged out.
- When a multicast entry is assigned to an interface in a specific VLAN, the corresponding traffic can only be forwarded to ports within that VLAN.

EXAMPLE

The following shows how to statically configure a multicast group on a port.

```
Console(config)#ip igmp snooping vlan 1 static 224.0.0.12 ethernet 1/5
Console(config)#
```

show ip igmp snooping

This command shows the IGMP snooping, proxy, and query configuration settings.

SYNTAX

show ip igmp snooping [**vlan** *vlan-id*]

vlan-id - VLAN ID (1-4094)

COMMAND MODE

Privileged Exec

COMMAND USAGE

This command displays global and VLAN-specific IGMP configuration settings. See "Configuring IGMP Snooping and Query Parameters" on page 613 for a description of the displayed items.

EXAMPLE

The following shows the current IGMP snooping configuration:

```
Console#show ip igmp snooping
 IGMP Snooping                        : Enabled
 Router Port Expire Time              : 300 s
 Router Alert Check                   : Disabled
 TCN Flood                            : Disabled
 TCN Query Solicit                    : Disabled
 Unregistered Data Flood              : Disabled
 Unsolicited Report Interval          : 400 s
 Version Exclusive                    : Disabled
 Version                              : 2
 Proxy Reporting                      : Enabled
 Querier                              : Disabled

 VLAN 1:
 --------
 IGMP Snooping                        : Enabled
 IGMP Snooping Running Status         : Inactive
 Version                              : Using global version (2)
 Version Exclusive                    : Using global status (Disabled)
 Immediate Leave                      : Disabled
 Last Member Query Interval           : 10 (1/10s)
 Last Member Query Count              : 2
 General Query Suppression            : Disabled
 Query Interval                       : 125
 Query Response Interval              : 100 (1/10s)
 Proxy Query Address                  : 0.0.0.0
 Proxy Reporting                      : Using global status (Enabled)
 Multicast Router Discovery           : Enabled
⋮
```

show ip igmp snooping group

This command shows known multicast group, source, and host port mappings for the specified VLAN interface, or for all interfaces if none is specified.

SYNTAX

show ip igmp snooping group [**host-ip-addr** *ip-address interface* | **igmpsnp** | **sort-by-port** | **user** | **vlan** *vlan-id* [**user** | **igmpsnp**]]

ip-address - IP address for multicast group

interface

ethernet *unit/port*

unit - Unit identifier. (Range: 1)

port - Port number. (Range: 1-28)

port-channel *channel-id* (Range: 1-8)

igmpsnp - Display only entries learned through IGMP snooping.

sort-by-port - Display entries sorted by port.

user - Display only the user-configured multicast entries.

vlan-id - VLAN ID (1-4094)

DEFAULT SETTING

None

COMMAND MODE

Privileged Exec

COMMAND USAGE

Member types displayed include IGMP or USER, depending on selected options.

EXAMPLE

The following shows the multicast entries learned through IGMP snooping for VLAN 1.

```
Console#show ip igmp snooping group vlan 1
Bridge Multicast Forwarding Entry Count:1
Flag: R - Router port, M - Group member port
      H - Host counts (number of hosts join the group on this port).
      P - Port counts (number of ports join the group).
 Up time: Group elapsed time (d:h:m:s).
 Expire : Group remaining time (m:s).

VLAN Group           Port        Up time     Expire Count
---- --------------- ----------- ----------- ------ --------
   1 224.1.1.1                   00:00:00:37           2(P)
                     Eth 1/ 1(R)
                     Eth 1/ 2(M)                       0(H)
Console#
```

show ip igmp snooping statistics

This command shows IGMP snooping protocol statistics for the specified interface.

SYNTAX

show ip igmp snooping statistics
{**input** [**interface** *interface*] | **output** [**interface** *interface*] | **query** [**vlan** *vlan-id*]}

interface

ethernet *unit/port*

unit - Unit identifier. (Range: 1)

port - Port number. (Range: 1-28)

port-channel *channel-id* (Range: 1-8)

vlan *vlan-id* - VLAN ID (Range: 1-4094)

query - Displays IGMP snooping-related statistics.

DEFAULT SETTING

None

COMMAND MODE

Privileged Exec

EXAMPLE

The following shows IGMP protocol statistics input:

```
Console#show ip igmp snooping statistics input interface ethernet 1/1
 Interface Report   Leave    G Query  G(-S)-S Query Drop     Join Succ Group
 --------- -------- -------- -------- ------------- -------- --------- ------
 Eth 1/ 1        23       11        4            10        5        14      5
Console#
```

Table 184: show ip igmp snooping statistics input - display description

Field	Description
Interface	Shows interface.
Report	The number of IGMP membership reports received on this interface.
Leave	The number of leave messages received on this interface.
G Query	The number of general query messages received on this interface.
G(-S)-S Query	The number of group specific or group-and-source specific query messages received on this interface.
Drop	The number of times a report, leave or query was dropped. Packets may be dropped due to invalid format, rate limiting, or packet content not allowed.
Join Succ	The number of times a multicast group was successfully joined.
Group	The number of multicast groups active on this interface.

The following shows IGMP protocol statistics output:

```
Console#show ip igmp snooping statistics output interface ethernet 1/1
 Output Statistics:
 Interface Report   Leave    G Query  G(-S)-S Query
 --------- -------- -------- -------- -------------
 Eth 1/ 1        12        0        1             0
Console#
```

Table 185: show ip igmp snooping statistics output - display description

Field	Description
Interface	Shows interface.
Report	The number of IGMP membership reports sent from this interface.
Leave	The number of leave messages sent from this interface.

Table 185: show ip igmp snooping statistics output - display description

Field	Description
G Query	The number of general query messages sent from this interface.
G(-S)-S Query	The number of group specific or group-and-source specific query messages sent from this interface.

The following shows IGMP query-related statistics for VLAN 1:

```
Console#show ip igmp snooping statistics query vlan 1
 Querier IP Address         : 192.168.1.1
 Querier Expire Time        : 00:00:30
 General Query Received     : 10
 General Query Sent         : 0
 Specific Query Received    : 2
 Specific Query Sent        : 0
 Number of Reports Sent     : 2
 Number of Leaves Sent      : 0
Console#
```

Table 186: show ip igmp snooping statistics vlan query - display description

Field	Description
Querier IP Address	The IP address of the querier on this interface.
Querier Expire Time	The time after which this querier is assumed to have expired.
General Query Received	The number of general queries received on this interface.
General Query Sent	The number of general queries sent from this interface.
Specific Query Received	The number of specific queries received on this interface.
Specific Query Sent	The number of specific queries sent from this interface.
Number of Reports Sent	The number of reports sent from this interface.
Number of Leaves Sent	The number of leaves sent from this interface.

STATIC MULTICAST ROUTING

This section describes commands used to configure static multicast routing on the switch.

Table 187: Static Multicast Interface Commands

Command	Function	Mode
ip igmp snooping vlan mrouter	Adds a multicast router port	GC
show ip igmp snooping mrouter	Shows multicast router ports	PE

ip igmp snooping vlan mrouter

This command statically configures a (Layer 2) multicast router port on the specified VLAN. Use the **no** form to remove the configuration.

SYNTAX

[**no**] **ip igmp snooping vlan** *vlan-id* **mrouter** *interface*

vlan-id - VLAN ID (Range: 1-4094)

interface

ethernet *unit/port*

unit - Unit identifier. (Range: 1)

port - Port number. (Range: 1-28)

port-channel *channel-id* (Range: 1-8)

DEFAULT SETTING

No static multicast router ports are configured.

COMMAND MODE

Global Configuration

COMMAND USAGE

- Depending on your network connections, IGMP snooping may not always be able to locate the IGMP querier. Therefore, if the IGMP querier is a known multicast router or switch connected over the network to an interface (port or trunk) on this switch, that interface can be manually configured to join all the current multicast groups.

- IGMP Snooping must be enabled globally on the switch (using the ip igmp snooping command) before a multicast router port can take effect.

EXAMPLE

The following shows how to configure port 10 as a multicast router port within VLAN 1.

```
Console(config)#ip igmp snooping vlan 1 mrouter ethernet 1/10
Console(config)#
```

show ip igmp snooping mrouter

This command displays information on statically configured and dynamically learned multicast router ports.

SYNTAX

show ip igmp snooping mrouter [**vlan** *vlan-id*]

vlan-id - VLAN ID (Range: 1-4094)

DEFAULT SETTING

Displays multicast router ports for all configured VLANs.

COMMAND MODE

Privileged Exec

COMMAND USAGE

Multicast router port types displayed include Static or Dynamic.

EXAMPLE

The following shows the ports in VLAN 1 which are attached to multicast routers.

```
Console#show ip igmp snooping mrouter vlan 1
 VLAN M'cast Router Port Type    Expire
 ---- ------------------ ------- --------
 1    Eth 1/1             Static
Console#
```

IGMP FILTERING AND THROTTLING

In certain switch applications, the administrator may want to control the multicast services that are available to end users. For example, an IP/TV service based on a specific subscription plan. The IGMP filtering feature fulfills this requirement by restricting access to specified multicast services on a switch port, and IGMP throttling limits the number of simultaneous multicast groups a port can join.

Table 188: IGMP Filtering and Throttling Commands

Command	Function	Mode
ip igmp filter	Enables IGMP filtering and throttling on the switch	GC
ip igmp profile	Sets a profile number and enters IGMP filter profile configuration mode	GC
permit, deny	Sets a profile access mode to permit or deny	IPC
range	Specifies one or a range of multicast addresses for a profile	IPC
ip igmp authentication	Enables RADIUS authentication for IGMP JOIN requests.	IC
ip igmp filter	Assigns an IGMP filter profile to an interface	IC
ip igmp max-groups	Specifies an IGMP throttling number for an interface	IC
ip igmp max-groups action	Sets the IGMP throttling action for an interface	IC
ip igmp query-drop	Drops any received IGMP query packets	IC
ip multicast-data-drop	Drops all multicast data packets	IC
show ip igmp authentication	Displays IGMP authentication settings for interfaces	PE
show ip igmp filter	Displays the IGMP filtering status	PE
show ip igmp profile	Displays IGMP profiles and settings	PE

Table 188: IGMP Filtering and Throttling Commands (Continued)

Command	Function	Mode
show ip igmp query-drop	Shows if the interface is configured to drop IGMP query packets	PE
show ip igmp throttle interface	Displays the IGMP throttling setting for interfaces	PE
show ip multicast-data-drop	Shows if the interface is configured to drop multicast data packets	PE

ip igmp filter (Global Configuration)

This command globally enables IGMP filtering and throttling on the switch. Use the **no** form to disable the feature.

Syntax

[**no**] **ip igmp filter**

Default Setting

Disabled

Command Mode

Global Configuration

Command Usage

- IGMP filtering enables you to assign a profile to a switch port that specifies multicast groups that are permitted or denied on the port. An IGMP filter profile can contain one or more, or a range of multicast addresses; but only one profile can be assigned to a port. When enabled, IGMP join reports received on the port are checked against the filter profile. If a requested multicast group is permitted, the IGMP join report is forwarded as normal. If a requested multicast group is denied, the IGMP join report is dropped.

- IGMP filtering and throttling only applies to dynamically learned multicast groups, it does not apply to statically configured groups.

- The IGMP filtering feature operates in the same manner when MVR is used to forward multicast traffic.

Example

```
Console(config)#ip igmp filter
Console(config)#
```

ip igmp profile

This command creates an IGMP filter profile number and enters IGMP profile configuration mode. Use the **no** form to delete a profile number.

SYNTAX

[**no**] **ip igmp profile** *profile-number*

profile-number - An IGMP filter profile number. (Range: 1-4294967295)

DEFAULT SETTING

Disabled

COMMAND MODE

Global Configuration

COMMAND USAGE

A profile defines the multicast groups that a subscriber is permitted or denied to join. The same profile can be applied to many interfaces, but only one profile can be assigned to one interface. Each profile has only one access mode; either permit or deny.

EXAMPLE

```
Console(config)#ip igmp profile 19
Console(config-igmp-profile)#
```

permit, deny

This command sets the access mode for an IGMP filter profile. Use the **no** form to delete a profile number.

SYNTAX

{**permit** | **deny**}

DEFAULT SETTING

Deny

COMMAND MODE

IGMP Profile Configuration

COMMAND USAGE

- Each profile has only one access mode; either permit or deny.

- When the access mode is set to permit, IGMP join reports are processed when a multicast group falls within the controlled range. When the access mode is set to deny, IGMP join reports are only processed when a multicast group is not in the controlled range.

EXAMPLE

```
Console(config)#ip igmp profile 19
Console(config-igmp-profile)#permit
Console(config-igmp-profile)#
```

range

This command specifies multicast group addresses for a profile. Use the **no** form to delete addresses from a profile.

SYNTAX

[**no**] **range** *low-ip-address* [*high-ip-address*]

low-ip-address - A valid IP address of a multicast group or start of a group range.

high-ip-address - A valid IP address for the end of a multicast group range.

DEFAULT SETTING

None

COMMAND MODE

IGMP Profile Configuration

COMMAND USAGE

Enter this command multiple times to specify more than one multicast address or address range for a profile.

EXAMPLE

```
Console(config)#ip igmp profile 19
Console(config-igmp-profile)#range 239.1.1.1
Console(config-igmp-profile)#range 239.2.3.1 239.2.3.100
Console(config-igmp-profile)#
```

ip igmp authentication

This command enables IGMP authentication on the specified interface. When enabled and an IGMP JOIN request is received, an authentication request is sent to a configured RADIUS server. Use the **no** form to disable IGMP authentication.

SYNTAX

[**no**] **ip igmp authentication**

DEFAULT SETTING

Disabled

COMMAND MODE

Interface Configuration(Ethernet, Port Channel)

COMMAND USAGE

- If IGMP authentication is enabled on an interface, and a join report is received on the interface, the switch will send an access request to the RADIUS server to perform authentication.
- Only when the RADIUS server responds with an authentication success message will the switch learn the group report. Once the group is learned, the switch will not send an access request to the RADIUS server when receiving the same report again within a one (1) day period.
- If the RADIUS server responds that authentication failed or the timer expires, the report will be dropped and the group will not be learned. The entry (host MAC, port number, VLAN ID, and group IP) will be put in the "authentication failed list".
- The "authentication failed list" is valid for the period of the interval defined by command ip igmp snooping vlan query-interval. When receiving the same report during this interval, the switch will not send the access request to the RADIUS server.
- If the interface leaves the group and subsequently rejoins the same group, the join report needs to again be authenticated.
- When receiving an IGMP v3 report message, the switch will send the access request to the RADIUS server only when the record type is either IS_EX or TO_EX, and the source list is empty. Other types of packets will not initiate RADIUS authentication.
- When a report is received for the first time and is being authenticated, whether authentication succeeds or fails, the report will still be sent to the multicast-router port.
- The following table shows the RADIUS server Attribute Value Pairs used for authentication:

Table 189: IGMP Authentication RADIUS Attribute Value Pairs

Attribute Name	AVP Type	Entry
USER_NAME	1	User MAC address
USER_PASSWORD	2	User MAC address
NAS_IP_ADDRESS	4	Switch IP address
NAS_PORT	5	User Port Number
FRAMED_IP_ADDRESS	8	Multicast Group ID

EXAMPLE

This example shows how to enable IGMP Authentication on all of the switch's Ethernet interfaces.

```
Console(config)#interface ethernet 1/1-28
Console(config-if)#ip igmp authentication
Console#
```

RELATED COMMANDS

show ip igmp authentication

ip igmp filter (Interface Configuration)

This command assigns an IGMP filtering profile to an interface on the switch. Use the **no** form to remove a profile from an interface.

SYNTAX

[**no**] **ip igmp filter** *profile-number*

profile-number - An IGMP filter profile number. (Range: 1-4294967295)

DEFAULT SETTING

None

COMMAND MODE

Interface Configuration

COMMAND USAGE

- The IGMP filtering profile must first be created with the ip igmp profile command before being able to assign it to an interface.

- Only one profile can be assigned to an interface.

- A profile can also be assigned to a trunk interface. When ports are configured as trunk members, the trunk uses the filtering profile assigned to the first port member in the trunk.

EXAMPLE

```
Console(config)#interface ethernet 1/1
Console(config-if)#ip igmp filter 19
Console(config-if)#
```

ip igmp max-groups

This command sets the IGMP throttling number for an interface on the switch. Use the **no** form to restore the default setting.

SYNTAX

ip igmp max-groups *number*

no ip igmp max-groups

number - The maximum number of multicast groups an interface can join at the same time. (Range: 1-1024)

DEFAULT SETTING

1024

COMMAND MODE

Interface Configuration (Ethernet)

COMMAND USAGE

- IGMP throttling sets a maximum number of multicast groups that a port can join at the same time. When the maximum number of groups is reached on a port, the switch can take one of two actions; either “deny” or “replace.” If the action is set to deny, any new IGMP join reports will be dropped. If the action is set to replace, the switch randomly removes an existing group and replaces it with the new multicast group.

- IGMP throttling can also be set on a trunk interface. When ports are configured as trunk members, the trunk uses the throttling settings of the first port member in the trunk.

EXAMPLE

```
Console(config)#interface ethernet 1/1
Console(config-if)#ip igmp max-groups 10
Console(config-if)#
```

ip igmp max-groups action

This command sets the IGMP throttling action for an interface on the switch.

SYNTAX

ip igmp max-groups action {**deny** | **replace**}

deny - The new multicast group join report is dropped.

replace - The new multicast group replaces an existing group.

DEFAULT SETTING

Deny

COMMAND MODE

Interface Configuration (Ethernet)

COMMAND USAGE

When the maximum number of groups is reached on a port, the switch can take one of two actions; either “deny” or “replace.” If the action is set to deny, any new IGMP join reports will be dropped. If the action is set to replace, the switch randomly removes an existing group and replaces it with the new multicast group.

EXAMPLE

```
Console(config)#interface ethernet 1/1
Console(config-if)#ip igmp max-groups action replace
Console(config-if)#
```

ip igmp query-drop

This command drops any received IGMP query packets. Use the no form to restore the default setting.

SYNTAX

[**no**] **ip igmp query-drop**

DEFAULT SETTING

Disabled

COMMAND MODE

Interface Configuration (Ethernet)

COMMAND USAGE

This command can be used to drop any query packets received on the specified interface. If this switch is acting as a Querier, this prevents it from being affected by messages received from another Querier.

EXAMPLE

```
Console(config)#interface ethernet 1/1
Console(config-if)#ip igmp query-drop
Console(config-if)#
```

ip multicast-data-drop

This command drops all multicast data packets

SYNTAX

[**no**] **ip multicast-data-drop**

DEFAULT SETTING

Disabled

COMMAND MODE

Interface Configuration (Ethernet)

COMMAND USAGE

This command can be used to stop multicast services from being forwarded to users attached to the downstream port (i.e., the interfaces specified by this command).

EXAMPLE

```
Console(config)#interface ethernet 1/1
Console(config-if)#ip multicast-data-drop
Console(config-if)#
```

show ip igmp authentication

This command displays the interface settings for IGMP authentication.

SYNTAX

show ip igmp authentication interface [*interface*]

interface

ethernet *unit*/*port*

unit - Unit identifier. (Range: 1)

port - Port number. (Range: 1-28)

port-channel *channel-id* (Range: 1-8)

DEFAULT SETTING

None

COMMAND MODE

Privileged Exec

COMMAND USAGE

Using this command without specifying an interface displays information for all interfaces.

EXAMPLE

```
Console#show ip igmp authentication
Ethernet 1/1: Enabled
Ethernet 1/2: Enabled
Ethernet 1/3: Enabled
⋮
Ethernet 1/27: Enabled
Ethernet 1/28: Enabled
Console#
```

show ip igmp filter

This command displays the global and interface settings for IGMP filtering.

SYNTAX

show ip igmp filter [**interface** *interface*]

interface

ethernet *unit/port*

unit - Unit identifier. (Range: 1)

port - Port number. (Range: 1-28)

port-channel *channel-id* (Range: 1-8)

DEFAULT SETTING

None

COMMAND MODE

Privileged Exec

EXAMPLE

```
Console#show ip igmp filter
IGMP filter enabled
Console#show ip igmp filter interface ethernet 1/1
Ethernet 1/1 information
---------------------------------
 IGMP Profile 19
  Deny
  Range 239.1.1.1 239.1.1.1
  Range 239.2.3.1 239.2.3.100
Console#
```

show ip igmp profile

This command displays IGMP filtering profiles created on the switch.

SYNTAX

show ip igmp profile [*profile-number*]

profile-number - An existing IGMP filter profile number.
(Range: 1-4294967295)

DEFAULT SETTING

None

COMMAND MODE

Privileged Exec

EXAMPLE

```
Console#show ip igmp profile
IGMP Profile 19
IGMP Profile 50
Console#show ip igmp profile 19
IGMP Profile 19
```

```
  Deny
  Range 239.1.1.1 239.1.1.1
  Range 239.2.3.1 239.2.3.100
Console#
```

show ip igmp query-drop

This command shows if the specified interface is configured to drop IGMP query packets.

Syntax

show ip igmp throttle interface [*interface*]

interface

ethernet *unit*/*port*

unit - Unit identifier. (Range: 1)

port - Port number. (Range: 1-28)

port-channel *channel-id* (Range: 1-8)

Default Setting

None

Command Mode

Privileged Exec

Command Usage

Using this command without specifying an interface displays all interfaces.

Example

```
Console#show ip igmp query-drop interface ethernet 1/1
Ethernet 1/1: Enabled
Console#
```

show ip igmp throttle interface

This command displays the interface settings for IGMP throttling.

Syntax

show ip igmp throttle interface [*interface*]

interface

ethernet *unit*/*port*

unit - Unit identifier. (Range: 1)

port - Port number. (Range: 1-28)

port-channel *channel-id* (Range: 1-8)

Default Setting

None

COMMAND MODE

Privileged Exec

COMMAND USAGE

Using this command without specifying an interface displays information for all interfaces.

EXAMPLE

```
Console#show ip igmp throttle interface ethernet 1/1
Eth  1/1 Information
  Status : TRUE
  Action : Deny
  Max Multicast Groups : 32
  Current Multicast Groups : 0

Console#
```

show ip multicast-data-drop

This command shows if the specified interface is configured to drop multicast data packets.

SYNTAX

show ip igmp throttle interface [*interface*]

interface

ethernet *unit*/*port*

unit - Unit identifier. (Range: 1)

port - Port number. (Range: 1-28)

port-channel *channel-id* (Range: 1-8)

DEFAULT SETTING

None

COMMAND MODE

Privileged Exec

COMMAND USAGE

Using this command without specifying an interface displays all interfaces.

EXAMPLE

```
Console#show ip multicast-data-drop interface ethernet 1/1
Ethernet 1/1: Enabled
Console#
```

MLD SNOOPING

Multicast Listener Discovery (MLD) snooping operates on IPv6 traffic and performs a similar function to IGMP snooping for IPv4. That is, MLD snooping dynamically configures switch ports to limit IPv6 multicast traffic so that it is forwarded only to ports with users that want to receive it. This reduces the flooding of IPv6 multicast packets in the specified VLANs.

There are two versions of the MLD protocol, version 1 and version 2. MLDv1 control packets include Listener Query, Listener Report, and Listener Done messages (equivalent to IGMPv2 query, report, and leave messages). MLDv2 control packets include MLDv2 query and report messages, as well as MLDv1 report and done messages.

Remember that IGMP Snooping and MLD Snooping are independent functions, and can therefore both function at the same time.

Table 190: MLD Snooping Commands

Command	Function	Mode
ipv6 mld snooping	Enables MLD Snooping globally	GC
ipv6 mld snooping querier	Allows the switch to act as the querier for MLD snooping	GC
ipv6 mld snooping query-interval	Configures the interval between sending MLD general query messages	GC
ipv6 mld snooping query-max-response-time	Configures the maximum response time for a general queries	GC
ipv6 mld snooping robustness	Configures the robustness variable	GC
ipv6 mld snooping router-port-expire-time	Configures the router port expire time	GC
ipv6 mld snooping unknown-multicast mode	Sets an action for unknown multicast packets	GC
ipv6 mld snooping version	Configures the MLD Snooping version	GC
ipv6 mld snooping vlan immediate-leave	Removes a member port of an IPv6 multicast service if a leave packet is received at that port and MLD immediate-leave is enabled for the parent VLAN	GC
ipv6 mld snooping vlan mrouter	Adds an IPv6 multicast router port	GC
ipv6 mld snooping vlan static	Adds an interface as a member of a multicast group	GC
show ipv6 mld snooping	Displays MLD Snooping configuration	PE
show ipv6 mld snooping group	Displays the learned groups	PE
show ipv6 mld snooping group source-list	Displays the learned groups and corresponding source list	PE
show ipv6 mld snooping mrouter	Displays the information of multicast router ports	PE

ipv6 mld snooping

This command enables MLD Snooping globally on the switch. Use the **no** form to disable MLD Snooping.

SYNTAX

[**no**] **ipv6 mld snooping**

DEFAULT SETTING

Disabled

COMMAND MODE

Global Configuration

EXAMPLE

The following example enables MLD Snooping:

```
Console(config)#ipv6 mld snooping
Console(config)#
```

ipv6 mld snooping querier

This command allows the switch to act as the querier for MLDv2 snooping. Use the no form to disable this feature.

SYNTAX

[**no**] **ipv6 mld snooping querier**

DEFAULT SETTING

Disabled

COMMAND MODE

Global Configuration

COMMAND USAGE

- If enabled, the switch will serve as querier if elected. The querier is responsible for asking hosts if they want to receive multicast traffic.
- An IPv6 address must be configured on the VLAN interface from which the querier will act if elected. When serving as the querier, the switch uses this IPv6 address as the query source address.
- The querier will not start or will disable itself after having started if it detects an IPv6 multicast router on the network.

EXAMPLE

```
Console(config)#ipv6 mld snooping querier
Console(config)#
```

ipv6 mld snooping query-interval

This command configures the interval between sending MLD general queries. Use the **no** form to restore the default.

SYNTAX

ipv6 mld snooping query-interval *interval*

no ipv6 mld snooping query-interval

interval - The interval between sending MLD general queries. (Range: 60-125 seconds)

DEFAULT SETTING

125 seconds

COMMAND MODE

Global Configuration

COMMAND USAGE

- This command applies when the switch is serving as the querier.
- An MLD general query message is sent by the switch at the interval specified by this command. When this message is received by downstream hosts, all receivers build an MLD report for the multicast groups they have joined.

EXAMPLE

```
Console(config)#ipv6 mld snooping query-interval 150
Console(config)#
```

ipv6 mld snooping query-max-response-time

This command configures the maximum response time advertised in MLD general queries. Use the **no** form to restore the default.

SYNTAX

ipv6 mld snooping query-max-response-time *seconds*

no ipv6 mld snooping query-max-response-time

seconds - The maximum response time allowed for MLD general queries. (Range: 5-25 seconds)

DEFAULT SETTING

10 seconds

COMMAND MODE

Global Configuration

COMMAND USAGE

This command controls how long the host has to respond to an MLD Query message before the switch deletes the group if it is the last member.

EXAMPLE

```
Console(config)#ipv6 mld snooping query-max-response-time seconds 15
Console(config)#
```

ipv6 mld snooping robustness

This command configures the MLD Snooping robustness variable. Use the **no** form to restore the default value.

SYNTAX

ipv6 mld snooping robustness *value*

no ipv6 mld snooping robustness

value - The number of the robustness variable. (Range: 2-10)

DEFAULT SETTING

2

COMMAND MODE

Global Configuration

COMMAND USAGE

A port will be removed from the receiver list for a multicast service when no MLD reports are detected in response to a number of MLD queries. The robustness variable sets the number of queries on ports for which there is no report.

EXAMPLE

```
Console(config)#ipv6 mld snooping robustness 2
Console(config)#
```

ipv6 mld snooping router-port-expire-time

This command configures the MLD query timeout. Use the **no** form to restore the default.

SYNTAX

ipv6 mld snooping router-port-expire-time *time*

no ipv6 mld snooping router-port-expire-time

time - Specifies the timeout of a dynamically learned router port. (Range: 300-500 seconds)

DEFAULT SETTING

300 seconds

COMMAND MODE

Global Configuration

COMMAND USAGE

The router port expire time is the time the switch waits after the previous querier stops before it considers the router port (i.e., the interface that had been receiving query packets) to have expired.

EXAMPLE

```
Console(config)#ipv6 mld snooping router-port-expire-time 300
Console(config)#
```

ipv6 mld snooping unknown-multicast mode

This command sets the action for dealing with unknown multicast packets. Use the **no** form to restore the default.

SYNTAX

ipv6 mld snooping unknown-multicast mode {**flood** | **to-router-port**}

[**no**] **ipv6 mld snooping unknown-multicast mode**

flood - Floods the unknown multicast data packets to all ports.

to-router-port - Forwards the unknown multicast data packets to router ports.

DEFAULT SETTING

to-router-port

COMMAND MODE

Global Configuration

COMMAND USAGE

- When set to “flood,” any received IPv6 multicast packets that have not been requested by a host are flooded to all ports in the VLAN.
- When set to “router-port,” any received IPv6 multicast packets that have not been requested by a host are forwarded to ports that are connected to a detected multicast router.

EXAMPLE

```
Console(config)#ipv6 mld snooping unknown-multicast mode flood
Console(config)#
```

ipv6 mld snooping version

This command configures the MLD snooping version. Use the **no** form to restore the default.

SYNTAX

ipv6 mld snooping version {**1** | **2**}

1 - MLD version 1.

2 - MLD version 2.

DEFAULT SETTING

Version 2

COMMAND MODE

Global Configuration

EXAMPLE

```
Console(config)#ipv6 mld snooping version 1
Console(config)#
```

ipv6 mld snooping vlan mrouter

This command statically configures an IPv6 multicast router port. Use the **no** form to remove the configuration.

SYNTAX

[**no**] **ipv6 mld snooping vlan** *vlan-id* **mrouter** *interface*

vlan-id - VLAN ID (Range: 1-4094)

interface

ethernet *unit/port*

unit - Stack unit. (Range: 1)

port - Port number. (Range: 1-28)

port-channel *channel-id* (Range: 1-8)

DEFAULT SETTING

No static multicast router ports are configured.

COMMAND MODE

Global Configuration

COMMAND USAGE

Depending on your network connections, MLD snooping may not always be able to locate the MLD querier. Therefore, if the MLD querier is a known multicast router/switch connected over the network to an interface (port or trunk) on the switch, you can manually configure that interface to join all the current multicast groups.

EXAMPLE

The following shows how to configure port 1 as a multicast router port within VLAN 1:

```
Console(config)#ipv6 mld snooping vlan 1 mrouter ethernet 1/1
Console(config)#
```

ipv6 mld snooping vlan static

This command adds a port to an IPv6 multicast group. Use the **no** form to remove the port.

SYNTAX

[**no**] **ipv6 mld snooping vlan** *vlan-id* **static** *ipv6-address interface*

vlan - VLAN ID (Range: 1-4094)

ipv6-address - An IPv6 address of a multicast group.
(Format: X:X:X:X::X)

interface

ethernet *unit/port*

unit - Stack unit. (Range: 1)

port - Port number. (Range: 1-28)

port-channel *channel-id* (Range: 1-8)

DEFAULT SETTING

None

COMMAND MODE

Global Configuration

EXAMPLE

```
Console(config)#ipv6 mld snooping vlan 1 static FF00:0:0:0:0:0:0:10C ethernet
  1/6
Console(config)#
```

ipv6 mld snooping vlan immediate-leave

This command immediately deletes a member port of an IPv6 multicast service when a leave packet is received at that port and immediate-leave is enabled for the parent VLAN. Use the **no** form to restore the default.

SYNTAX

[**no**] **ipv6 mld snooping vlan** *vlan-id* **immediate-leave**

vlan-id - A VLAN identification number. (Range: 1-4094)

DEFAULT SETTING

Disabled

COMMAND MODE

Global Configuration

COMMAND USAGE

- If MLD immediate-leave is *not* used, a multicast router (or querier) will send a group-specific query message when an MLD group leave message is received. The router/querier stops forwarding traffic for that group only if no host replies to the query within the specified timeout period.

- If MLD immediate-leave is enabled, the switch assumes that only one host is connected to the interface. Therefore, immediate leave should only be enabled on an interface if it is connected to only one MLD-enabled device, either a service host or a neighbor running MLD snooping.

EXAMPLE

The following shows how to enable MLD immediate leave.

```
Console(config)#interface vlan 1
Console(config-if)#ipv6 mld snooping immediate-leave
Console(config-if)#
```

show ipv6 mld snooping

This command shows the current MLD Snooping configuration.

SYNTAX

show ipv6 mld snooping

COMMAND MODE

Privileged Exec

EXAMPLE

The following shows MLD Snooping configuration information

```
Console#show ipv6 mld snooping
 Service Status                : Disabled
 Querier Status                : Disabled
 Robustness                    : 2
 Query Interval                : 125 sec
 Query Max Response Time       : 10 sec
 Router Port Expiry Time       : 300 sec
 Immediate Leave               : Disabled on all VLAN
 Unknown Flood Behavior        : To Router Port
 MLD Snooping Version          : Version 2
Console#
```

show ipv6 mld snooping group

This command shows known multicast groups, member ports, and the means by which each group was learned.

SYNTAX

show ipv6 mld snooping group

COMMAND MODE

Privileged Exec

EXAMPLE

The following shows MLD Snooping group configuration information:

```
Console#show ipv6 mld snooping group

VLAN Multicast IPv6 Address                  Member port Type
---- --------------------------------------- ----------- ---------------
   1 FF02::01:01:01:01                       Eth 1/1     MLD Snooping
   1 FF02::01:01:01:02                       Eth 1/1     Multicast Data
   1 FF02::01:01:01:02                       Eth 1/1     User

Console#
```

show ipv6 mld snooping group source-list

This command shows known multicast groups, member ports, the means by which each group was learned, and the corresponding source list.

SYNTAX

show ipv6 mld snooping group source-list

COMMAND MODE

Privileged Exec

EXAMPLE

The following shows MLD Snooping group mapping information:

```
Console#show ipv6 mld snooping group source-list

Console#show ipv6 mld snooping group source-list
VLAN ID                     : 1
Mutlicast IPv6 Address      : FF02::01:01:01:01
Member Port                 : Eth 1/1
Type                        : MLD Snooping
Filter Mode                 : Include
(if exclude filter mode)
Filter Timer elapse         : 10 sec.
Request List                : ::01:02:03:04, ::01:02:03:05, ::01:02:03:06,
                              ::01:02:03:07
Exclude List                : ::02:02:03:04, ::02:02:03:05, ::02:02:03:06,
                              ::02:02:03:07
(if include filter mode)
Include List                : ::02:02:03:04, ::02:02:03:05, ::02:02:03:06,
                              ::02:02:03:06
```

```
Option:
 Filter Mode: Include, Exclude

Console#
```

show ipv6 mld snooping mrouter

This command shows MLD Snooping multicast router information.

SYNTAX

show ipv6 mld snooping mrouter vlan *vlan-id*

vlan-id - A VLAN identification number. (Range: 1-4094)

COMMAND MODE

Privileged Exec

EXAMPLE

```
Console#show ipv6 mld snooping mrouter vlan 1
 VLAN Multicast Router Port Type      Expire
 ---- --------------------- --------- ------
    1 Eth 1/ 2              Static

Console#
```

MLD FILTERING AND THROTTLING

In certain switch applications, the administrator may want to control the multicast services that are available to end users. For example, an IP/TV service based on a specific subscription plan. The MLD filtering feature fulfills this requirement by restricting access to specified multicast services on a switch port, and MLD throttling limits the number of simultaneous multicast groups a port can join.

Table 191: MLD Filtering and Throttling Commands

Command	Function	Mode
ipv6 mld filter	Enables MLD filtering and throttling on the switch	GC
ipv6 mld profile	Sets a profile number and enters MLD filter profile configuration mode	GC
permit, deny	Sets a profile access mode to permit or deny	IPC
range	Specifies one or a range of multicast addresses for a profile	IPC
ipv6 mld filter	Assigns an MLD filter profile to an interface	IC
ipv6 mld max-groups	Specifies an M:D throttling number for an interface	IC
ipv6 mld max-groups action	Sets the MLD throttling action for an interface	IC
ipv6 mld query-drop	Drops any received MLD query packets	IC
ipv6 multicast-data-drop	Enable multicast data guard mode on a port interface	IC

Table 191: MLD Filtering and Throttling Commands (Continued)

Command	Function	Mode
show ipv6 mld filter	Displays the MLD filtering status	PE
show ipv6 mld profile	Displays MLD profiles and settings	PE
show ipv6 mld query-drop	Shows if the interface is configured to drop MLD query packets	PE
show ipv6 mld throttle interface	Displays the MLD throttling setting for interfaces	PE

ipv6 mld filter (Global Configuration)

This command globally enables MLD filtering and throttling on the switch. Use the **no** form to disable the feature.

SYNTAX

[**no**] **ipv6 mld filter**

DEFAULT SETTING

Disabled

COMMAND MODE

Global Configuration

COMMAND USAGE

- MLD filtering enables you to assign a profile to a switch port that specifies multicast groups that are permitted or denied on the port. An MLD filter profile can contain one or more, or a range of multicast addresses; but only one profile can be assigned to a port. When enabled, MLD join reports received on the port are checked against the filter profile. If a requested multicast group is permitted, the MLD join report is forwarded as normal. If a requested multicast group is denied, the MLD join report is dropped.

- MLD filtering and throttling only applies to dynamically learned multicast groups, it does not apply to statically configured groups.

- The MLD filtering feature operates in the same manner when MVR6 is used to forward multicast traffic.

EXAMPLE

```
Console(config)#ipv6 mld filter
Console(config)#
```

RELATED COMMANDS

show ipv6 mld filter

ipv6 mld profile

This command creates an MLD filter profile number and enters MLD profile configuration mode. Use the **no** form to delete a profile number.

Syntax

[**no**] **ipv6 mld profile** *profile-number*

profile-number - An MLD filter profile number. (Range: 1-4294967295)

Default Setting

Disabled

Command Mode

Global Configuration

Command Usage

A profile defines the multicast groups that a subscriber is permitted or denied to join. The same profile can be applied to many interfaces, but only one profile can be assigned to one interface. Each profile has only one access mode; either permit or deny.

Example

```
Console(config)#ipv6 mld profile 19
Console(config-mld-profile)#
```

Related Commands

show ipv6 mld profile

permit, deny

This command sets the access mode for an MLD filter profile. Use the **no** form to delete a profile number.

Syntax

{**permit** | **deny**}

Default Setting

deny

Command Mode

MLD Profile Configuration

Command Usage

- Each profile has only one access mode; either permit or deny.

- When the access mode is set to permit, MLD join reports are processed when a multicast group falls within the controlled range. When the access mode is set to deny, MLD join reports are only processed when a multicast group is not in the controlled range.

EXAMPLE

```
Console(config)#ipv6 mld profile 19
Console(config-mld-profile)#permit
Console(config-mld-profile)#
```

range

This command specifies multicast group addresses for a profile. Use the **no** form to delete addresses from a profile.

SYNTAX

[**no**] **range** *low-ipv6-address* [*high-ipv6-address*]

low-ipv6-address - A valid IPv6 address (X:X:X:X::X) of a multicast group or start of a group range.

high-ipv6-address - A valid IPv6 address (X:X:X:X::X) for the end of a multicast group range.

DEFAULT SETTING

None

COMMAND MODE

MLD Profile Configuration

COMMAND USAGE

Enter this command multiple times to specify more than one multicast address or address range for a profile.

EXAMPLE

```
Console(config-mld-profile)#range ff01::0101 ff01::0202
Console(config-mld-profile)#
```

ipv6 mld filter (Interface Configuration)

This command assigns an MLD filtering profile to an interface on the switch. Use the **no** form to remove a profile from an interface.

SYNTAX

[**no**] **ipv6 mld filter** *profile-number*

profile-number - An MLD filter profile number. (Range: 1-4294967295)

DEFAULT SETTING

None

COMMAND MODE

Interface Configuration

COMMAND USAGE

- The MLD filtering profile must first be created with the ipv6 mld profile command before being able to assign it to an interface.

- Only one profile can be assigned to an interface.

- A profile can also be assigned to a trunk interface. When ports are configured as trunk members, the trunk uses the filtering profile assigned to the first port member in the trunk.

EXAMPLE

```
Console(config)#interface ethernet 1/1
Console(config-if)#ipv6 mld filter 19
Console(config-if)#
```

ipv6 mld max-groups

This command configures the maximum number of MLD groups that an interface can join. Use the **no** form to restore the default setting.

SYNTAX

ipv6 mld max-groups *number*

no ipv6 mld max-groups

number - The maximum number of multicast groups an interface can join at the same time. (Range: 1-1024)

DEFAULT SETTING

1024

COMMAND MODE

Interface Configuration (Ethernet)

COMMAND USAGE

- MLD throttling sets a maximum number of multicast groups that a port can join at the same time. When the maximum number of groups is reached on a port, the switch can take one of two actions; either "deny" or "replace." If the action is set to deny, any new MLD join reports will be dropped. If the action is set to replace, the switch randomly removes an existing group and replaces it with the new multicast group.

- MLD throttling can also be set on a trunk interface. When ports are configured as trunk members, the trunk uses the throttling settings of the first port member in the trunk.

- If the maximum number of MLD groups is set to the default value, the running status of MLD throttling will change to false. This means that any configuration for MLD throttling will have no effect until the maximum number of MLD groups is configured to another value.

EXAMPLE

```
Console(config)#interface ethernet 1/1
Console(config-if)#ipv6 mld max-groups 10
Console(config-if)#
```

ipv6 mld max-groups action

This command sets the MLD throttling action for an interface on the switch.

SYNTAX

ipv6 mld max-groups action {**deny** | **replace**}

deny - The new multicast group join report is dropped.

replace - The new multicast group replaces an existing group.

DEFAULT SETTING

Deny

COMMAND MODE

Interface Configuration (Ethernet)

COMMAND USAGE

When the maximum number of groups is reached on a port, the switch can take one of two actions; either “deny” or “replace.” If the action is set to deny, any new MLD join reports will be dropped. If the action is set to replace, the switch randomly removes an existing group and replaces it with the new multicast group.

EXAMPLE

```
Console(config)#interface ethernet 1/1
Console(config-if)#ipv6 mld max-groups action replace
Console(config-if)#
```

ipv6 mld query-drop

This command drops any received MLD query packets. Use the no form to restore the default setting.

SYNTAX

[**no**] **ipv6 mld query-drop**

DEFAULT SETTING

Disabled

COMMAND MODE

Interface Configuration (Ethernet)

COMMAND USAGE

This command can be used to drop any query packets received on the specified interface. If this switch is acting as a Querier, this prevents it from being affected by messages received from another Querier.

EXAMPLE

```
Console(config)#interface ethernet 1/1
Console(config-if)#ipv6 mld query-drop
Console(config-if)#
```

ipv6 multicast-data-drop

Use this command to enable multicast data guard mode on a port interface. Use the no form of the command to disable multicast data guard.

SYNTAX

[**no**] **ipv6 multicast-data-drop**

DEFAULT SETTING

Disabled

COMMAND MODE

Interface Configuration

EXAMPLE

```
Console(config)#interface ethernet 1/3
Console(config-if)#ipv6 multicast-data-drop
Console(config-if)#
```

show ipv6 mld filter

This command displays the global and interface settings for MLD filtering.

SYNTAX

show ipv6 mld filter [**interface** *interface*]

interface

ethernet *unit*/*port*

unit - Unit identifier. (Range: 1)

port - Port number. (Range: 1-28)

port-channel *channel-id* (Range: 1-8)

DEFAULT SETTING

None

COMMAND MODE

Privileged Exec

EXAMPLE

```
Console#show ipv6 mld filter
 MLD filter Enabled
Console#show ipv6 mld filter interface ethernet 1/3
Ethernet 1/3 information
---------------------------------
 MLD  Profile 19
 Deny
 Range  ff01::101         ff01::faa
Console#
```

show ipv6 mld profile

This command displays MLD filtering profiles created on the switch.

SYNTAX

show ipv6 mld profile [*profile-number*]

profile-number - An existing MLD filter profile number. (Range: 1-4294967295)

DEFAULT SETTING

None

COMMAND MODE

Privileged Exec

EXAMPLE

```
Console#show ipv6 mld profile
 MLD Profile 19
 MLD Profile 50
Console#show ipv6 mld profile 19
Console#show ipv6 mld profile 5
 MLD  Profile 19
 Deny
 Range  ff01::101         ff01::faa
```

show ipv6 mld query-drop

This command shows if the specified interface is configured to drop MLD query packets.

SYNTAX

show ipv6 mld throttle interface [*interface*]

interface

ethernet *unit/port*

unit - Stack unit. (Range: 1)

port - Port number. (Range: 1-28)

port-channel *channel-id* (Range: 1-16)

DEFAULT SETTING

None

COMMAND MODE

Privileged Exec

COMMAND USAGE

Using this command without specifying an interface displays all interfaces.

EXAMPLE

```
Console#show ipv6 mld query-drop interface ethernet 1/1
Ethernet 1/1: Enabled
Console#
```

show ipv6 mld throttle interface

This command displays the interface settings for MLD throttling.

SYNTAX

show ipv6 mld throttle interface [*interface*]

interface

ethernet *unit*/*port*

unit - Unit identifier. (Range: 1)

port - Port number. (Range: 1-28)

port-channel *channel-id* (Range: 1-16)

DEFAULT SETTING

None

COMMAND MODE

Privileged Exec

COMMAND USAGE

Using this command without specifying an interface displays information for all interfaces.

EXAMPLE

```
Console#show ipv6 mld throttle interface ethernet 1/3
Eth  1/3 Information
 Status                   : TRUE
 Action                   : Replace
 Max Multicast Groups     : 10
 Current Multicast Groups : 0

Console#
```

MVR FOR IPV4

This section describes commands used to configure Multicast VLAN Registration for IPv4 (MVR). A single network-wide VLAN can be used to transmit multicast traffic (such as television channels) across a service provider's network. Any multicast traffic entering an MVR VLAN is sent to all subscribers. This can significantly reduce to processing overhead required to dynamically monitor and establish the distribution tree for a normal multicast VLAN. Also note that MVR maintains the user isolation and data security provided by VLAN segregation by passing only multicast traffic into other VLANs to which the subscribers belong.

Table 192: Multicast VLAN Registration for IPv4 Commands

Command	Function	Mode
mvr	Globally enables MVR	GC
mvr associated-profile	Binds the MVR group addresses specified in a profile to an MVR domain	GC
mvr domain	Enables MVR for a specific domain	GC
mvr priority	Assigns a priority to all multicast traffic in the MVR VLAN	GC
mvr profile	Maps a range of MVR group addresses to a profile	GC
mvr proxy-query-interval	Configures the interval at which the receiver port sends out general queries.	GC
mvr proxy-switching	Enables MVR proxy switching, where the source port acts as a host, and the receiver port acts as an MVR router with querier service enabled	GC
mvr robustness-value	Configures the expected packet loss, and thereby the number of times to generate report and group-specific queries	GC
mvr source-port-mode dynamic	Configures the switch to only forward multicast streams which the source port has dynamically joined	GC
mvr upstream-source-ip	Configures the source IP address assigned to all control packets sent upstream	GC
mvr vlan	Specifies the VLAN through which MVR multicast data is received	GC
mvr immediate-leave	Enables immediate leave capability	IC
mvr type	Configures an interface as an MVR receiver or source port	IC
mvr vlan group	Configures an interface as a static member of an MVR group which is forwarded from the MVR VLAN to the specified interface within the receiver VLAN	IC
show mvr	Shows information about MVR domain settings, including MVR operational status, the multicast VLAN, the current number of group addresses, and the upstream source IP address	PE
show mvr associated-profile	Shows the profiles bound the specified domain	PE
show mvr interface	Shows MVR settings for interfaces attached to the MVR VLAN	PE

Table 192: Multicast VLAN Registration for IPv4 Commands (Continued)

Command	Function	Mode
show mvr members	Shows information about the current number of entries in the forwarding database, or detailed information about a specific multicast address	PE
show mvr profile	Shows all configured MVR profiles	PE
show mvr statistics	Shows MVR protocol statistics for the specified interface	PE

mvr

This command enables Multicast VLAN Registration (MVR) globally on the switch. Use the **no** form of this command to globally disable MVR.

Syntax

[**no**] **mvr**

Default Setting

Disabled

Command Mode

Global Configuration

Command Usage

Only IGMP version 2 or 3 hosts can issue multicast join or leave messages. If MVR must be configured for an IGMP version 1 host, the multicast groups must be statically assigned using the mvr vlan group command.

Example

The following example enables MVR globally.

```
Console(config)#mvr
Console(config)#
```

mvr associated-profile

This command binds the MVR group addresses specified in a profile to an MVR domain. Use the **no** form of this command to remove the binding.

Syntax

[**no**] **mvr domain** *domain-id* **associated-profile** *profile-name*

domain-id - An independent multicast domain. (Range: 1-5)

profile-name - The name of a profile containing one or more MVR group addresses. (Range: 1-21 characters)

Default Setting

Disabled

COMMAND MODE

Global Configuration

EXAMPLE

The following an MVR group address profile to domain 1:

```
Console(config)#mvr domain 1 associated-profile rd
Console(config)#
```

RELATED COMMANDS

mvr profile (1481)

mvr domain

This command enables Multicast VLAN Registration (MVR) for a specific domain. Use the **no** form of this command to disable MVR for a domain.

SYNTAX

[**no**] **mvr domain** *domain-id*

domain-id - An independent multicast domain. (Range: 1-5)

DEFAULT SETTING

Disabled

COMMAND MODE

Global Configuration

COMMAND USAGE

Only IGMP version 2 or 3 hosts can issue multicast join or leave messages. If MVR must be configured for an IGMP version 1 host, the multicast groups must be statically assigned using the mvr vlan group command.

EXAMPLE

The following example enables MVR for domain 1:

```
Console(config)#mvr domain 1
Console(config)#
```

mvr profile

This command maps a range of MVR group addresses to a profile. Use the **no** form of this command to remove the profile.

SYNTAX

mvr profile *profile-name start-ip-address end-ip-address*

profile-name - The name of a profile containing one or more MVR group addresses. (Range: 1-21 characters)

start-ip-address - Starting IPv4 address for an MVR multicast group. (Range: 224.0.1.0 - 239.255.255.255)

end-ip-address - Ending IPv4 address for an MVR multicast group. (Range: 224.0.1.0 - 239.255.255.255)

DEFAULT SETTING

No profiles are defined

COMMAND MODE

Global Configuration

COMMAND USAGE

- Use this command to statically configure all multicast group addresses that will join the MVR VLAN. Any multicast data associated an MVR group is sent from all source ports to all receiver ports that have registered to receive data from that multicast group.

- The IP address range from 224.0.0.0 to 239.255.255.255 is used for multicast streams. MVR group addresses cannot fall within the reserved IP multicast address range of 224.0.0.x.

- IGMP snooping and MVR share a maximum number of 1024 groups. Any multicast streams received in excess of this limitation will be flooded to all ports in the associated domain.

EXAMPLE

The following example maps a range of MVR group addresses to a profile:

```
Console(config)#mvr profile rd 228.1.23.1 228.1.23.10
Console(config)#
```

mvr proxy-query-interval

This command configures the interval at which the receiver port sends out general queries. Use the **no** form to restore the default setting.

SYNTAX

mvr proxy-query-interval *interval*

no mvr proxy-query-interval

interval - The interval at which the receiver port sends out general queries. (Range: 2-31744 seconds)

DEFAULT SETTING

125 seconds

COMMAND MODE

Global Configuration

COMMAND USAGE

This command sets the general query interval at which active receiver ports send out general queries. This interval is only effective when proxy switching is enabled with the mvr proxy-switching command.

EXAMPLE

This example sets the proxy query interval for MVR proxy switching.

```
Console(config)#mvr proxy-query-interval 250
Console(config)#
```

mvr priority

This command assigns a priority to all multicast traffic in the MVR VLAN. Use the **no** form of this command to restore the default setting.

SYNTAX

mvr priority *priority*

no mvr priority

priority - The CoS priority assigned to all multicast traffic forwarded into the MVR VLAN. (Range: 0-6, where 6 is the highest priority)

DEFAULT SETTING

Disabled

COMMAND MODE

Global Configuration

COMMAND USAGE

This command can be used to set a high priority for low-latency multicast traffic such as a video-conference, or to set a low priority for normal multicast traffic not sensitive to latency.

EXAMPLE

```
Console(config)#mvr priority 6
Console(config)#
```

RELATED COMMANDS

show mvr

mvr proxy-switching

This command enables MVR proxy switching, where the source port acts as a host, and the receiver port acts as an MVR router with querier service enabled. Use the **no** form to disable this function.

SYNTAX

[**no**] **mvr proxy-switching**

DEFAULT SETTING

Enabled

COMMAND MODE

Global Configuration

COMMAND USAGE

- When MVR proxy-switching is enabled, an MVR source port serves as the upstream or host interface. The source port performs only the host portion of MVR by sending summarized membership reports, and automatically disables MVR router functions.

- Receiver ports are known as downstream or router interfaces. These interfaces perform the standard MVR router functions by maintaining a database of all MVR subscriptions on the downstream interface. Receiver ports must therefore be configured on all downstream interfaces which require MVR proxy service.

- When the source port receives report and leave messages, it only forwards them to other source ports.

- When receiver ports receive any query messages, they are dropped.

- When changes occurring in the downstream MVR groups are learned by the receiver ports through report and leave messages, an MVR state change report is created and sent to the upstream source port, which in turn forwards this information upstream.

- When MVR proxy switching is disabled:
  - Any membership reports received from receiver/source ports are forwarded to all source ports.
  - When a source port receives a query message, it will be forwarded to all downstream receiver ports.
  - When a receiver port receives a query message, it will be dropped.

EXAMPLE

The following example enable MVR proxy switching.

```
Console(config)#mvr proxy-switching
Console(config)#
```

RELATED COMMANDS

mvr robustness-value (1484)

mvr robustness-value

This command configures the expected packet loss, and thereby the number of times to generate report and group-specific queries. Use the **no** form to restore the default setting.

SYNTAX

mvr robustness-value *value*

no mvr robustness-value

value - The robustness used for all interfaces. (Range: 1-255)

DEFAULT SETTING

1

COMMAND MODE

Global Configuration

COMMAND USAGE

- This command is used to set the number of times report messages are sent upstream when changes are learned about downstream groups, and the number of times group-specific queries are sent to downstream receiver ports.
- This command only takes effect when MVR proxy switching is enabled.

EXAMPLE

```
Console(config)#mvr robustness-value 5
Console(config)#
```

RELATED COMMANDS

mvr proxy-switching (1483)

mvr source-port-mode dynamic

This command configures the switch to only forward multicast streams which the source port has dynamically joined. Use the **no** form to restore the default setting.

SYNTAX

[**no**] **mvr source-port-mode dynamic**

DEFAULT SETTING

Forwards all multicast streams which have been specified in a profile and bound to a domain.

COMMAND MODE

Global Configuration

COMMAND USAGE

- By default, the switch forwards any multicast streams within the address range set by a profile, and bound to a domain. The multicast streams are sent to all source ports on the switch and to all receiver ports that have elected to receive data on that multicast address.
- When the **mvr source-port-mode dynamic** command is used, the switch only forwards multicast streams which the source port has dynamically joined. In other words, both the receiver port and source port must subscribe to a multicast group before a multicast stream is forwarded to any attached client. Note that the requested streams are still restricted to the address range which has been specified in a profile and bound to a domain.

EXAMPLE

```
Console(config)#mvr source-port-mode dynamic
Console(config)#
```

mvr upstream-source-ip

This command configures the source IP address assigned to all MVR control packets sent upstream on all domains or on a specified domain. Use the **no** form to restore the default setting.

SYNTAX

mvr [**domain** *domain-id*] **upstream-source-ip** *source-ip-address*

no mvr [**domain** *domain-id*] **upstream-source-ip**

domain-id - An independent multicast domain. (Range: 1-5)

source-ip-address – The source IPv4 address assigned to all MVR control packets sent upstream.

DEFAULT SETTING

All MVR reports sent upstream use a null source IP address

COMMAND MODE

Global Configuration

EXAMPLE

```
Console(config)#mvr domain 1 upstream-source-ip 192.168.0.3
Console(config)#
```

mvr vlan

This command specifies the VLAN through which MVR multicast data is received. Use the **no** form of this command to restore the default MVR VLAN.

Syntax

mvr domain *domain-id* **vlan** *vlan-id*

no mvr domain *domain-id* **vlan**

domain-id - An independent multicast domain. (Range: 1-5)

vlan-id - Specifies the VLAN through which MVR multicast data is received. This is also the VLAN to which all source ports must be assigned. (Range: 1-4094)

Default Setting

VLAN 1

Command Mode

Global Configuration

Command Usage

- This command specifies the VLAN through which MVR multicast data is received. This is the VLAN to which all source ports must be assigned.

- The VLAN specified by this command must be an existing VLAN configured with the vlan command.

- MVR source ports can be configured as members of the MVR VLAN using the switchport allowed vlan command and switchport native vlan command, but MVR receiver ports should not be statically configured as members of this VLAN.

Example

The following example sets the MVR VLAN to VLAN 2:

```
Console(config)#mvr
Console(config)#mvr domain 1 vlan 2
Console(config)#
```

mvr immediate-leave

This command causes the switch to immediately remove an interface from a multicast stream as soon as it receives a leave message for that group. Use the **no** form to restore the default settings.

Syntax

[**no**] **mvr** [**domain** *domain-id*] **immediate-leave**

domain-id - An independent multicast domain. (Range: 1-5)

Default Setting

Disabled

COMMAND MODE

Interface Configuration (Ethernet, Port Channel)

COMMAND USAGE

- Immediate leave applies only to receiver ports. When enabled, the receiver port is immediately removed from the multicast group identified in the leave message. When immediate leave is disabled, the switch follows the standard rules by sending a group-specific query to the receiver port and waiting for a response to determine if there are any remaining subscribers for that multicast group before removing the port from the group list.

- Using immediate leave can speed up leave latency, but should only be enabled on a port attached to only one multicast subscriber to avoid disrupting services to other group members attached to the same interface.

- Immediate leave does not apply to multicast groups which have been statically assigned to a port with the mvr vlan group command.

EXAMPLE

The following enables immediate leave on a receiver port.

```
Console(config)#interface ethernet 1/5
Console(config-if)#mvr domain 1 immediate-leave
Console(config-if)#
```

mvr type

This command configures an interface as an MVR receiver or source port. Use the **no** form to restore the default settings.

SYNTAX

[**no**] **mvr** [**domain** *domain-id*] **type** {**receiver** | **source**}

domain-id - An independent multicast domain. (Range: 1-5)

receiver - Configures the interface as a subscriber port that can receive multicast data.

source - Configures the interface as an uplink port that can send and receive multicast data for the configured multicast groups.

DEFAULT SETTING

The port type is not defined.

COMMAND MODE

Interface Configuration (Ethernet, Port Channel)

COMMAND USAGE

- A port which is not configured as an MVR receiver or source port can use IGMP snooping to join or leave multicast groups using the standard rules for multicast filtering.

- Receiver ports can belong to different VLANs, but should not normally be configured as a member of the MVR VLAN. IGMP snooping can also be used to allow a receiver port to dynamically join or leave multicast groups not sourced through the MVR VLAN.

- One or more interfaces may be configured as MVR source ports. A source port is able to both receive and send data for multicast groups which it has joined through the MVR protocol or which have been assigned through the mvr vlan group command.

- Only IGMP version 2 or 3 hosts can issue multicast join or leave messages. If MVR must be configured for an IGMP version 1 host, the multicast groups must be statically assigned using the mvr vlan group command.

EXAMPLE

The following configures one source port and several receiver ports on the switch.

```
Console(config)#interface ethernet 1/5
Console(config-if)#mvr domain 1 type source
Console(config-if)#exit
Console(config)#interface ethernet 1/6
Console(config-if)#mvr domain 1 type receiver
Console(config-if)#exit
Console(config)#interface ethernet 1/7
Console(config-if)#mvr domain 1 type receiver
Console(config-if)#
```

mvr vlan group

This command statically binds a multicast group to a port which will receive long-term multicast streams associated with a stable set of hosts. Use the **no** form to restore the default settings.

SYNTAX

[**no**] **mvr** [**domain** *domain-id*] **vlan** *vlan-id* **group** *ip-address*

domain-id - An independent multicast domain. (Range: 1-5)

vlan-id - Receiver VLAN to which the specified multicast traffic is flooded. (Range: 1-4094)

group - Defines a multicast service sent to the selected port.

ip-address - Statically configures an interface to receive multicast traffic from the IPv4 address specified for an MVR multicast group. (Range: 224.0.1.0 - 239.255.255.255)

DEFAULT SETTING

No receiver port is a member of any configured multicast group.

COMMAND MODE

Interface Configuration (Ethernet, Port Channel)

COMMAND USAGE

- Multicast groups can be statically assigned to a receiver port using this command.
- The IP address range from 224.0.0.0 to 239.255.255.255 is used for multicast streams. MVR group addresses cannot fall within the reserved IP multicast address range of 224.0.0.x.
- Only IGMP version 2 or 3 hosts can issue multicast join or leave messages. If MVR must be configured for an IGMP version 1 host, the multicast groups must be statically assigned using the **mvr vlan group** command.
- The MVR VLAN cannot be specified as the receiver VLAN for static bindings.

EXAMPLE

The following statically assigns a multicast group to a receiver port:

```
Console(config)#interface ethernet 1/7
Console(config-if)#mvr domain 1 type receiver
Console(config-if)#mvr domain 1 vlan 3 group 225.0.0.5
Console(config-if)#
```

show mvr

This command shows information about MVR domain settings, including MVR operational status, the multicast VLAN, the current number of group addresses, and the upstream source IP address.

SYNTAX

show mvr [**domain** *domain-id*]

domain-id - An independent multicast domain. (Range: 1-5)

DEFAULT SETTING

Displays configuration settings for all MVR domains.

COMMAND MODE

Privileged Exec

EXAMPLE

The following shows the MVR settings:

```
Console#show mvr
 MVR 802.1p Forwarding Priority : Disabled
 MVR Proxy Switching            : Enabled
 MVR Robustness Value           : 1
 MVR Proxy Query Interval       : 125(sec.)
 MVR Source Port Mode           : Always Forward

 MVR Domain                     : 1
 MVR Config Status              : Enabled
 MVR Running Status              : Active
 MVR Multicast VLAN              : 1
 MVR Current Learned Groups      : 10
 MVR Upstream Source IP          : 192.168.0.3
⋮
```

Table 193: **show mvr** - display description

Field	Description
MVR 802.1p Forwarding Priority	Priority assigned to multicast traffic forwarded into the MVR VLAN
MVR Proxy Switching	Shows if MVR proxy switching is enabled
MVR Robustness Value	Shows the number of reports or query messages sent when proxy switching is enabled
MVR Proxy Query Interval	Shows the interval at which the receiver port sends out general queries
MVR Source Port Mode	Shows if the switch forwards all multicast streams, or only those which the source port has dynamically joined
MVR Domain	An independent multicast domain.
MVR Config Status	Shows if MVR is globally enabled on the switch.
MVR Running Status	Indicates whether or not all necessary conditions in the MVR environment are satisfied. (Running status is true as long as MVR Status is enabled, and the specified MVR VLAN exists.)
MVR Multicast VLAN	Shows the VLAN used to transport all MVR multicast traffic.
MVR Current Learned Groups	The current number of MVR group addresses
MVR Upstream Source IP	The source IP address assigned to all upstream control packets.

show mvr associated-profile

This command shows the profiles bound the specified domain.

SYNTAX

show mvr [**domain** *domain-id*] **associated-profile**

domain-id - An independent multicast domain. (Range: 1-5)

DEFAULT SETTING

Displays profiles bound to all MVR domains.

COMMAND MODE

Privileged Exec

EXAMPLE

The following displays the profiles bound to domain 1:

```
Console#show mvr domain 1 associated-profile
Domain ID : 1
 MVR Profile Name     Start IP Addr.  End IP Addr.
 -------------------- --------------- ---------------
 rd                        228.1.23.1     228.1.23.10
 testing                   228.2.23.1     228.2.23.10
Console#
```

show mvr interface

This command shows MVR configuration settings for interfaces attached to the MVR VLAN.

SYNTAX

show mvr [**domain** *domain-id*] **interface**

domain-id - An independent multicast domain. (Range: 1-5)

DEFAULT SETTING

Displays configuration settings for all attached interfaces.

COMMAND MODE

Privileged Exec

EXAMPLE

The following displays information about the interfaces attached to the MVR VLAN in domain 1:

```
Console#show mvr domain 1 interface
MVR Domain : 1
 Port     Type     Status              Immediate  Static Group Address
 -------- -------- ------------------- ---------  -------------------------
 Eth 1/ 1 Source   Active/Forwarding
 Eth 1/ 2 Receiver Inactive/Discarding Disabled   234.5.6.8(VLAN2)
 Eth 1/ 3 Source   Inactive/Discarding
 Eth 1/ 1 Receiver Active/Forwarding   Disabled   225.0.0.1(VLAN1)
                                                  225.0.0.9(VLAN3)
 Eth 1/ 4 Receiver Active/Discarding   Disabled
Console#
```

Table 194: show mvr interface - display description

Field	Description
MVR Domain	An independent multicast domain.
Port	Shows interfaces attached to the MVR.
Type	Shows the MVR port type.
Status	Shows the MVR status and interface status. MVR status for source ports is “ACTIVE” if MVR is globally enabled on the switch. MVR status for receiver ports is “ACTIVE” only if there are subscribers receiving multicast traffic from one of the MVR groups, or a multicast group has been statically assigned to an interface. Also shows if MVR traffic is being forwarded or discarded.
Immediate	Shows if immediate leave is enabled or disabled.
Static Group Address	Shows any static MVR group assigned to an interface, and the receiver VLAN.

show mvr members

This command shows information about the current number of entries in the forwarding database, detailed information about a specific multicast address, the IP address of the hosts subscribing to all active multicast groups, or the multicast groups associated with each port.

SYNTAX

show mvr [**domain** *domain-id*] **members** [*ip-address* | **host-ip-address** [*interface*] | **sort-by-port** [*interface*]]]

domain-id - An independent multicast domain. (Range: 1-5)

ip-address - IPv4 address for an MVR multicast group. (Range: 224.0.1.0 - 239.255.255.255)

members - The multicast groups assigned to the MVR VLAN.

host-ip-address - The subscriber IP addresses.

sort-by-port - The multicast groups associated with an interface.

interface

ethernet *unit/port*

unit - Unit identifier. (Range: 1)

port - Port number. (Range: 1-28)

port-channel *channel-id* (Range: 1-8)

DEFAULT SETTING

Displays configuration settings for all domains and all forwarding entries.

COMMAND MODE

Privileged Exec

EXAMPLE

The following shows information about the number of multicast forwarding entries currently active in domain 1:

```
Console#show mvr domain 1 members
 MVR Domain : 1
 MVR Forwarding Entry Count :1
 Flag: S - Source port, R - Receiver port.
       H - Host counts (number of hosts joined to group on this port).
       P - Port counts (number of ports joined to group).
 Up time: Group elapsed time (d:h:m:s).
 Expire : Group remaining time (m:s).

 Group Address   VLAN Port        Up time     Expire Count
 --------------- ---- ----------- ----------- ------ --------
 234.5.6.7          1             00:00:09:17                2(P)
                    1 Eth 1/ 1(S)
                    2 Eth 1/ 2(R)

Console#
```

The following example shows detailed information about a specific multicast address:

```
Console#show mvr domain 1 members 234.5.6.7
 MVR Domain : 1
 MVR Forwarding Entry Count :1
 Flag: S - Source port, R - Receiver port.
       H - Host counts (number of hosts joined to group on this port).
       P - Port counts (number of ports joined to group).
 Up time: Group elapsed time (d:h:m:s).
 Expire : Group remaining time (m:s).

 Group Address   VLAN Port        Up time     Expire Count
 --------------- ---- ----------- ----------- ------ --------
 234.5.6.7          1                                    2(P)
                    1 Eth 1/ 1(S)
                    2 Eth 1/ 2(R)

Console#
```

Table 195: show mvr members - display description

Field	Description
Group Address	Multicast group address.
VLAN	VLAN to which this address is forwarded.
Port	Port to which this address is forwarded.
Uptime	Time that this multicast group has been known.
Expire	The time until this entry expires.
Count	The number of times this address has been learned by IGMP snooping.

show mvr profile

This command shows all configured MVR profiles.

COMMAND MODE

Privileged Exec

EXAMPLE

The following shows all configured MVR profiles:

```
Console#show mvr profile
 MVR Profile Name     Start IP Addr.  End IP Addr.
 -------------------- --------------- ---------------
 rd                        228.1.23.1     228.1.23.10
 testing                   228.2.23.1     228.2.23.10
Console#
```

show mvr statistics

This command shows MVR protocol-related statistics for the specified interface.

SYNTAX

show mvr statistics {**input** | **output**} [**interface** *interface*]

show mvr domain *domain-id* **statistics** {**input** [**interface** *interface*] | **output** [**interface** *interface*] | **query**}

domain-id - An independent multicast domain. (Range: 1-5)

interface

ethernet *unit*/*port*

unit - Unit identifier. (Range: 1)

port - Port number. (Range: 1-28)

port-channel *channel-id* (Range: 1-8)

vlan *vlan-id* - VLAN ID (Range: 1-4094)

query - Displays MVR query-related statistics.

DEFAULT SETTING

Displays statistics for all domains.

COMMAND MODE

Privileged Exec

EXAMPLE

The following shows MVR protocol-related statistics received:

```
Console#show mvr domain 1 statistics input
 MVR Domain : 1
 Input Statistics:
 Interface Report   Leave    G Query  G(-S)-S Query Drop     Join Succ Group
 --------- -------- -------- -------- ------------- -------- --------- ------
 Eth 1/ 1        23       11        4            10        5        20      9
 Eth 1/ 2        12       15        8            3         5        19      4
 VLAN    1        2        0        0             2        2        20      9
Console#
```

Table 196: show mvr statistics input - display description

Field	Description
Interface	Shows interfaces attached to the MVR.
Report	The number of IGMP membership reports received on this interface.
Leave	The number of leave messages received on this interface.
G Query	The number of general query messages received on this interface.
G(-S)-S Query	The number of group specific or group-and-source specific query messages received on this interface.

Table 196: show mvr statistics input - display description (Continued)

Field	Description
Drop	The number of times a report, leave or query was dropped. Packets may be dropped due to invalid format, rate limiting, packet content not allowed, or MVR group report received
Join Succ	The number of times a multicast group was successfully joined.
Group	The number of MVR groups active on this interface.

The following shows MVR protocol-related statistics sent:

```
Console#show mvr domain 1 statistics output
 MVR Domain : 1
 Output Statistics:
 Interface Report   Leave    G Query  G(-S)-S Query
 --------- -------- -------- -------- -------------
 Eth 1/ 1        12        0        1             0
 Eth 1/ 2         5        1        4             1
 VLAN    1        7        2        3             0
Console#
```

Table 197: show mvr statistics output - display description

Field	Description
Interface	Shows interfaces attached to the MVR.
Report	The number of IGMP membership reports sent from this interface.
Leave	The number of leave messages sent from this interface.
G Query	The number of general query messages sent from this interface.
G(-S)-S Query	The number of group specific or group-and-source specific query messages sent from this interface.

The following shows MVR query-related statistics:

```
Console#show mvr domain 1 statistics query
 Querier IP Address        : 192.168.1.1
 Querier Expire Time       : 00:00:30
 General Query Received    : 10
 General Query Sent        : 0
 Specific Query Received   : 2
 Specific Query Sent       : 0
 Number of Reports Sent    : 2
 Number of Leaves Sent     : 0
Console#
```

Table 198: show mvr statistics query - display description

Field	Description
Querier IP Address	The IP address of the querier on this interface.
Querier Expire Time	The time after which this querier is assumed to have expired.
General Query Received	The number of general queries received on this interface.

Table 198: show mvr statistics query - display description (Continued)

Field	Description
General Query Sent	The number of general queries sent from this interface.
Specific Query Received	The number of specific queries received on this interface.
Specific Query Sent	The number of specific queries sent from this interface.
Number of Reports Sent	The number of reports sent from this interface.
Number of Leaves Sent	The number of leaves sent from this interface.

MVR FOR IPV6

This section describes commands used to configure Multicast VLAN Registration for IPv6 (MVR6). A single network-wide VLAN can be used to transmit multicast traffic (such as television channels) across a service provider's network. Any multicast traffic entering an MVR VLAN is sent to all subscribers. This can significantly reduce to processing overhead required to dynamically monitor and establish the distribution tree for a normal multicast VLAN. Also note that MVR maintains the user isolation and data security provided by VLAN segregation by passing only multicast traffic into other VLANs to which the subscribers belong.

Table 199: Multicast VLAN Registration for IPv6 Commands

Command	Function	Mode
mvr6 associated-profile	Binds the MVR group addresses specified in a profile to an MVR domain	GC
mvr6 domain	Enables MVR for a specific domain	GC
mvr6 profile	Maps a range of MVR group addresses to a profile	GC
mvr6 proxy-query-interval	Configures the interval at which the receiver port sends out general queries.	GC
mvr6 proxy-switching	Enables MVR proxy switching, where the source port acts as a host, and the receiver port acts as an MVR router with querier service enabled	GC
mvr6 robustness-value	Configures the expected packet loss, and thereby the number of times to generate report and group-specific queries	GC
mvr6 source-port-mode dynamic	Configures the switch to only forward multicast streams which the source port has dynamically joined	GC
mvr6 upstream-source-ip	Configures the source IP address assigned to all control packets sent upstream	GC
mvr6 vlan	Specifies the VLAN through which MVR multicast data is received	GC
mvr6 immediate-leave	Enables immediate leave capability	IC
mvr6 type	Configures an interface as an MVR receiver or source port	IC
mvr6 vlan group	Statically binds a multicast group to a port	IC
clear mvr6 groups	Clears the multicast group dynamically learned entries.	PE

Table 199: Multicast VLAN Registration for IPv6 Commands (Continued)

Command	Function	Mode
clear mvr6 statistics	Clears the MVR statistics globally or on a per-interface basis.	PE
show mvr6	Shows information about MVR domain settings, including MVR operational status, the multicast VLAN, the current number of group addresses, and the upstream source IP address	PE
show mvr6 associated-profile	Shows the profiles bound the specified domain	PE
show mvr6 interface	Shows MVR settings for interfaces attached to the MVR VLAN	PE
show mvr6 members	Shows information about the current number of entries in the forwarding database, or detailed information about a specific multicast address	PE
show mvr6 profile	Shows all configured MVR profiles	PE
show mvr6 statistics	Shows MVR protocol statistics for the specified interface	PE

mvr6 associated-profile

This command binds the MVR group addresses specified in a profile to an MVR domain. Use the **no** form of this command to remove the binding.

SYNTAX

[**no**] **mvr6 domain** *domain-id* **associated-profile** *profile-name*

domain-id - An independent multicast domain. (Range: 1-5)

profile-name - The name of a profile containing one or more MVR group addresses. (Range: 1-21 characters)

DEFAULT SETTING

Disabled

COMMAND MODE

Global Configuration

COMMAND USAGE

MRV6 domains can be associated with more than one MVR6 profile. But since MVR6 domains cannot share the group range, an MRV6 profile can only be associated with one MVR6 domain.

EXAMPLE

The following an MVR group address profile to domain 1:

```
Console(config)#mvr6 domain 1 associated-profile rd
Console(config)#
```

mvr6 domain

This command enables Multicast VLAN Registration (MVR) for a specific domain. Use the **no** form of this command to disable MVR for a domain.

SYNTAX

[**no**] **mvr6 domain** *domain-id*

domain-id - An independent multicast domain. (Range: 1-5)

DEFAULT SETTING

Disabled

COMMAND MODE

Global Configuration

COMMAND USAGE

When MVR6 is enabled on a domain, any multicast data associated with an MVR6 group is sent from all designated source ports, to all receiver ports that have registered to receive data from that multicast group.

EXAMPLE

The following example enables MVR for domain 1:

```
Console(config)#mvr6 domain 1
Console(config)#
```

mvr6 profile

This command maps a range of MVR group addresses to a profile. Use the **no** form of this command to remove the profile.

SYNTAX

mvr6 profile *profile-name start-ip-address end-ip-address*

profile-name - The name of a profile containing one or more MVR group addresses. (Range: 1-21 characters)

start-ip-address - Starting IPv6 address for an MVR multicast group. This parameter must be a full IPv6 address including the network prefix and host address bits.

end-ip-address - Ending IPv6 address for an MVR multicast group. This parameter must be a full IPv6 address including the network prefix and host address bits.

DEFAULT SETTING

No profiles are defined

COMMAND MODE

Global Configuration

COMMAND USAGE

- Use this command to statically configure all multicast group addresses that will join the MVR VLAN. Any multicast data associated with an MVR group is sent from all source ports, and to all receiver ports that have registered to receive data from that multicast group.

- All IPv6 addresses must be according to RFC 2373 “IPv6 Addressing Architecture,” using 8 colon-separated 16-bit hexadecimal values. One double colon may be used in the address to indicate the appropriate number of zeros required to fill the undefined fields. (Note that the IP address ff02::X is reserved.)

- The MVR6 group address range assigned to a profile cannot overlap with the group address range of any other profile.

EXAMPLE

The following example maps a range of MVR group addresses to a profile:

```
Console(config)#mvr6 profile rd ff00::1 ff00::9
Console(config)#
```

mvr6 proxy-query-interval

This command configures the interval at which the receiver port sends out general queries. Use the **no** form to restore the default setting.

SYNTAX

mvr proxy-query-interval *interval*

no mvr proxy-query-interval

interval - The interval at which the receiver port sends out general queries. (Range: 2-31744 seconds)

DEFAULT SETTING

125 seconds

COMMAND MODE

Global Configuration

COMMAND USAGE

This command sets the general query interval at which active receiver ports send out general queries. This interval is only effective when proxy switching is enabled with the mvr6 proxy-switching command.

EXAMPLE

This example sets the proxy query interval for MVR proxy switching.

```
Console(config)#mvr profile rd 228.1.23.1 228.1.23.10
Console(config)#
```

mvr6 proxy-switching

This command enables MVR proxy switching, where the source port acts as a host, and the receiver port acts as an MVR router with querier service enabled. Use the **no** form to disable this function.

SYNTAX

[**no**] **mvr6 proxy-switching**

DEFAULT SETTING

Enabled

COMMAND MODE

Global Configuration

COMMAND USAGE

- When MVR proxy-switching is enabled, an MVR source port serves as the upstream or host interface, and the MVR receiver port serves as the querier. The source port performs only the host portion of MVR by sending summarized membership reports, and automatically disables MVR router functions.

- Receiver ports are known as downstream or router interfaces. These interfaces perform the standard MVR router functions by maintaining a database of all MVR subscriptions on the downstream interface. Receiver ports must therefore be configured on all downstream interfaces which require MVR proxy service.

- When the source port receives report and leave messages, it only forwards them to other source ports.

- When receiver ports receive any query messages, they are dropped.

- When changes occurring in the downstream MVR groups are learned by the receiver ports through report and leave messages, an MVR state change report is created and sent to the upstream source port, which in turn forwards this information upstream.

- When MVR proxy switching is disabled:

  - Any membership reports received from receiver/source ports are forwarded to all source ports.

  - When a source port receives a query message, it will be forwarded to all downstream receiver ports.

  - When a receiver port receives a query message, it will be dropped.

EXAMPLE

The following example enable MVR proxy switching.

```
Console(config)#mvr proxy-switching
Console(config)#
```

RELATED COMMANDS

mvr6 robustness-value (1501)

mvr6 robustness-value

This command configures the expected packet loss, and thereby the number of times to generate report and group-specific queries. Use the **no** form to restore the default setting.

SYNTAX

mvr6 robustness-value *value*

no mvr6 robustness-value

value - The robustness used for all interfaces. (Range: 1-10)

DEFAULT SETTING

1

COMMAND MODE

Global Configuration

COMMAND USAGE

- This command sets the number of times report messages are sent upstream when changes are learned about downstream groups, and the number of times group-specific queries are sent to downstream receiver ports.
- This command only takes effect when MVR6 proxy switching is enabled.

EXAMPLE

```
Console(config)#mvr6 robustness-value 5
Console(config)#
```

RELATED COMMANDS

mvr6 proxy-switching (1500)

mvr6 source-port-mode dynamic

This command configures the switch to only forward multicast streams which the source port has dynamically joined. Use the **no** form to restore the default setting.

SYNTAX

[**no**] **mvr6 source-port-mode dynamic**

DEFAULT SETTING

Forwards all multicast streams which have been specified in a profile and bound to a domain.

COMMAND MODE

Global Configuration

COMMAND USAGE

- By default, the switch forwards any multicast streams within the address range set by a profile, and bound to a domain. The multicast streams are sent to all source ports on the switch and to all receiver ports that have elected to receive data on that multicast address.

- When the **mvr6 source-port-mode dynamic** command is used, the switch only forwards multicast streams which the source port has dynamically joined. In other words, both the receiver port and source port must subscribe to a multicast group before a multicast stream is forwarded to any attached client. Note that the requested streams are still restricted to the address range which has been specified in a profile and bound to a domain.

EXAMPLE

```
Console(config)#mvr6 source-port-mode dynamic
Console(config)#
```

mvr6 upstream-source-ip

This command configures the source IPv6 address assigned to all MVR control packets sent upstream on the specified domain. Use the **no** form to restore the default setting.

SYNTAX

mvr6 domain *domain-id* **upstream-source-ip** *source-ip-address*

no mvr6 domain *domain-id* **upstream-source-ip**

domain-id - An independent multicast domain. (Range: 1-5)

source-ip-address – The source IPv6 address assigned to all MVR control packets sent upstream. This parameter must be a full IPv6 address including the network prefix and host address bits.

DEFAULT SETTING

All MVR reports sent upstream use a null source IP address

COMMAND MODE

Global Configuration

COMMAND USAGE

All IPv6 addresses must be according to RFC 2373 “IPv6 Addressing Architecture,” using 8 colon-separated 16-bit hexadecimal values. One double colon may be used in the address to indicate the appropriate number of zeros required to fill the undefined fields. (Note that the IP address ff02::X is reserved.)

EXAMPLE

```
Console(config)#mvr6 domain 1 upstream-source-ip 2001:DB8:2222:7223::72
Console(config)#
```

mvr6 vlan

This command specifies the VLAN through which MVR multicast data is received. Use the **no** form of this command to restore the default MVR VLAN.

SYNTAX

mvr6 domain *domain-id* **vlan** *vlan-id*

no mvr6 domain *domain-id* **vlan**

domain-id - An independent multicast domain. (Range: 1-5)

vlan-id - Specifies the VLAN through which MVR multicast data is received. This is also the VLAN to which all source ports must be assigned. (Range: 1-4094)

DEFAULT SETTING

VLAN 1

COMMAND MODE

Global Configuration

COMMAND USAGE

MVR source ports can be configured as members of the MVR VLAN using the switchport allowed vlan command and switchport native vlan command, but MVR receiver ports should not be statically configured as members of this VLAN.

EXAMPLE

The following example sets the MVR VLAN to VLAN 1:

```
Console(config)#mvr6 domain 1 vlan 1
Console(config)#
```

mvr6 immediate-leave

This command causes the switch to immediately remove an interface from a multicast stream as soon as it receives a leave message for that group. Use the **no** form to restore the default settings.

SYNTAX

[**no**] **mvr6 domain** *domain-id* **immediate-leave**

domain-id - An independent multicast domain. (Range: 1-5)

DEFAULT SETTING

Disabled

COMMAND MODE

Interface Configuration (Ethernet, Port Channel)

COMMAND USAGE

- Immediate leave applies only to receiver ports. When enabled, the receiver port is immediately removed from the multicast group identified in the leave message. When immediate leave is disabled, the switch follows the standard rules by sending a group-specific query to the receiver port and waiting for a response to determine if there are any remaining subscribers for that multicast group before removing the port from the group list.

- Using immediate leave can speed up leave latency, but should only be enabled on a port attached to only one multicast subscriber to avoid disrupting services to other group members attached to the same interface.

- Immediate leave does not apply to multicast groups which have been statically assigned to a port with the mvr6 vlan group command.

EXAMPLE

The following enables immediate leave on a receiver port.

```
Console(config)#interface ethernet 1/5
Console(config-if)#mvr6 domain 1 immediate-leave
Console(config-if)#
```

mvr6 type

This command configures an interface as an MVR receiver or source port. Use the **no** form to restore the default settings.

SYNTAX

[**no**] **mvr6 domain** *domain-id* **type** {**receiver** | **source**}

domain-id - An independent multicast domain. (Range: 1-5)

receiver - Configures the interface as a subscriber port that can receive multicast data.

source - Configures the interface as an uplink port that can send and receive multicast data for the configured multicast groups. Note that the source port must be manually configured as a member of the MVR6 VLAN using the switchport allowed vlan command.

DEFAULT SETTING

The port type is not defined.

COMMAND MODE

Interface Configuration (Ethernet, Port Channel)

COMMAND USAGE

- A port configured as an MVR6 receiver or source port can join or leave multicast groups configured under MVR6. A port which is not configured as an MVR receiver or source port can use MLD snooping to join or leave multicast groups using the standard rules for multicast filtering (see "MLD Snooping Commands" on page 1469).

- Receiver ports can belong to different VLANs, but should not be configured as a member of the MVR VLAN. Also, note that VLAN membership for MVR receiver ports cannot be set to access mode (see the switchport mode command).

- One or more interfaces may be configured as MVR source ports. A source port is able to both receive and send data for multicast groups which it has joined through the MVR6 protocol or which have been assigned through the mvr6 vlan group command.

  All source ports must belong to the MVR6 VLAN.

  Subscribers should not be directly connected to source ports.

- The same port cannot be configured as a source port in one MVR domain and as a receiver port in another domain.

EXAMPLE

The following configures one source port and several receiver ports on the switch.

```
Console(config)#interface ethernet 1/5
Console(config-if)#mvr6 domain 1 type source
Console(config-if)#exit
Console(config)#interface ethernet 1/6
Console(config-if)#mvr6 domain 1 type receiver
Console(config-if)#exit
Console(config)#interface ethernet 1/7
Console(config-if)#mvr6 domain 1 type receiver
Console(config-if)#
```

mvr6 vlan group

This command statically binds a multicast group to a port which will receive long-term multicast streams associated with a stable set of hosts. Use the **no** form to restore the default settings.

SYNTAX

[**no**] **mvr6 domain** *domain-id* **vlan** *vlan-id* **group** *ip-address*

domain-id - An independent multicast domain. (Range: 1-5)

vlan-id - Receiver VLAN to which the specified multicast traffic is flooded. (Range: 1-4094)

group - Defines a multicast service sent to the selected port.

ip-address - Statically configures an interface to receive multicast traffic from the IPv6 address specified for an MVR multicast group. This parameter must be a full IPv6 address including the network prefix and host address bits.

DEFAULT SETTING

No receiver port is a member of any configured multicast group.

COMMAND MODE

Interface Configuration (Ethernet, Port Channel)

COMMAND USAGE

- Multicast groups can be statically assigned to a receiver port using this command. The assigned address must fall within the range set by the mvr6 associated-profile command.

- All IPv6 addresses must be according to RFC 2373 “IPv6 Addressing Architecture,” using 8 colon-separated 16-bit hexadecimal values. One double colon may be used in the address to indicate the appropriate number of zeros required to fill the undefined fields. (Note that the IP address ff02::X is reserved.)

- The MVR VLAN cannot be specified as the receiver VLAN for static bindings.

EXAMPLE

The following statically assigns a multicast group to a receiver port:

```
Console(config)#interface ethernet 1/2
Console(config-if)#mvr6 domain 1 type receiver
Console(config-if)#mvr6 domain 1 vlan 2 group ff00::1
Console(config-if)#
```

clear mvr6 groups

This command clears multicast group information dynamically learned through MVR6.

SYNTAX

clear mvr6 groups dynamic [**domain** *domain-id*]

domain-id - An independent multicast domain. (Range: 1-5)

COMMAND MODE

Privileged Exec

COMMAND USAGE

This command only clears entries learned though MVR6. Statically configured multicast addresses are not cleared.

EXAMPLE

The following shows how to clear the MVR learned group entries:

```
Console#clear mvr6 groups dynamic
Console#
```

clear mvr6 statistics

Use this command to clear the MVR6 statistics.

SYNTAX

clear mvr6 statistics [**interface** {**ethernet** *unit/port* | **port-channel** *channel-id* | **vlan** *vlan-id*}]

ethernet *unit/port*

unit - Unit identifier. (Range: 1)

port - Port number. (Range: 1-28)

port-channel *channel-id* (Range: 1-8)

vlan vlan-id (Range: 1-4094)

COMMAND MODE

Privileged Exec

COMMAND USAGE

If the interface option is not used then all MVR6 statistics are cleared. Otherwise using the interface option will only clear MVR6 statistics for the specified interface.

EXAMPLE

The following shows how to clear all the MVR6 statistics:

```
Console#clear mvr6 statistics
Console#
```

show mvr6

This command shows information about MVR domain settings, including MVR operational status, the multicast VLAN, the current number of group addresses, and the upstream source IP address.

SYNTAX

show mvr6 [**domain** *domain-id*]

domain-id - An independent multicast domain. (Range: 1-5)

DEFAULT SETTING

Displays configuration settings for all MVR domains.

COMMAND MODE

Privileged Exec

EXAMPLE

The following shows the MVR settings:

```
Console#show mvr6
 MVR6 Proxy Switching            : Enabled
 MVR6 Robustness Value           : 1
```

```
MVR6 Proxy Query Interval      : 125(sec.)
MVR6 Source Port Mode          : Always Forward

MVR6 Domain                 : 1
MVR6 Config Status          : Enabled
MVR6 Running Status         : Active
MVR6 Multicast VLAN         : 1
MVR6 Current Learned Groups : 0
MVR6 Upstream Source IP     : FF05::25
:
```

Table 200: show mvr6 - display description

Field	Description
MVR Proxy Switching	Shows if MVR proxy switching is enabled
MVR6 Proxy Query Interval	The interval at which the receiver port sends out general queries
MVR6 Source Port Mode	Shows if the switch only forwards multicast streams which the source port has dynamically joined or always forwards multicast streams
MVR Robustness Value	Shows the number of reports or query messages sent when proxy switching is enabled
MVR6 Domain	An independent multicast domain.
MVR6 Config Status	Shows if MVR is globally enabled on the switch.
MVR6 Running Status	Indicates whether or not all necessary conditions in the MVR environment are satisfied. (Running status is true as long as MVR Status is enabled, and the specified MVR VLAN exists, and a source port with a valid link has been configured (using the mvr6 type command.)
MVR6 Multicast VLAN	Shows the VLAN used to transport all MVR multicast traffic.
MVR Current Learned Groups	The current number of MVR group addresses
MVR6 Upstream Source IP	The source IP address assigned to all upstream control packets.

show mvr6 associated-profile

This command shows the profiles bound the specified domain.

SYNTAX

show mvr6 [**domain** *domain-id*] **associated-profile**

domain-id - An independent multicast domain. (Range: 1-5)

DEFAULT SETTING

Displays profiles bound to all MVR domains.

COMMAND MODE

Privileged Exec

EXAMPLE

The following displays the profiles bound to domain 1:

```
Console#show mvr6 domain 1 associated-profile
Domain ID : 1
 MVR Profile Name     Start IPv6 Addr.          End IPv6 Addr.
 -------------------- ------------------------- -------------------------
 rd                                     FF00::1                   FF00::9
Console#
```

show mvr6 interface

This command shows MVR configuration settings for interfaces attached to the MVR VLAN.

SYNTAX

show mvr6 [**domain** *domain-id*] **interface**

domain-id - An independent multicast domain. (Range: 1-5)

DEFAULT SETTING

Displays configuration settings for all attached interfaces.

COMMAND MODE

Privileged Exec

EXAMPLE

The following displays information about the interfaces attached to the MVR VLAN in domain 1:

```
Console#show mvr6 domain 1 interface
 MVR6 Domain : 1
 Port     Type     Status        Immediate  Static Group Address
 -------- -------- ------------- ---------  -------------------------
 Eth1/ 1  Source   Active/Up
 Eth1/ 2  Receiver Active/Up     Disabled   FF00::1(VLAN2)
Console#
```

Table 201: show mvr6 interface - display description

Field	Description
Port	Shows interfaces attached to the MVR.
Type	Shows the MVR port type.
Status	Shows the MVR status and interface status. MVR status for source ports is “ACTIVE” if MVR is globally enabled on the switch. MVR status for receiver ports is “ACTIVE” only if there are subscribers receiving multicast traffic from one of the MVR groups, or a multicast group has been statically assigned to an interface.
Immediate	Shows if immediate leave is enabled or disabled.
Static Group Address	Shows any static MVR group assigned to an interface, and the receiver VLAN.

show mvr6 members

This command shows information about the current number of entries in the forwarding database, or detailed information about a specific multicast address.

SYNTAX

show mvr6 [**domain** *domain-id*] **members** [*ip-address*]

domain-id - An independent multicast domain. (Range: 1-5)

ip-address - IPv6 address for an MVR multicast group.

DEFAULT SETTING

Displays configuration settings for all domains and all forwarding entries.

COMMAND MODE

Privileged Exec

EXAMPLE

The following shows information about the number of multicast forwarding entries currently active in domain 1:

```
Console#show mvr6 domain 1 members
 MVR6 Domain : 1
 MVR6 Forwarding Entry Count :1
 Flag: S - Source port, R - Receiver port.
       H - Host counts (number of hosts join the group on this port).
       P - Port counts (number of ports join the group).
 Up time: Group elapsed time (d:h:m:s).
 Expire : Group remaining time (m:s).

 Group Address                  VLAN Port        Up time     Expire Count
 ------------------------------ ---- ----------- ----------- ------ --------
 FF00::1                           1                                    2(P)
                    1  Eth1/ 1(S)
                    2  Eth1/ 2(S)
Console#
```

The following example shows detailed information about a specific multicast address:

```
Console#show mvr6 domain 1 members ff00::1
 MVR6 Domain : 1
 MVR6 Forwarding Entry Count :1
 Flag: S - Source port, R - Receiver port.
       H - Host counts (number of hosts join the group on this port).
       P - Port counts (number of ports join the group).
 Up time: Group elapsed time (d:h:m:s).
 Expire : Group remaining time (m:s).

 Group Address                  VLAN Port        Up time     Expire Count
 ------------------------------ ---- ----------- ----------- ------ --------
 FF00::1                           1                                    2(P)
                    1  Eth1/ 1(S)
                    2  Eth1/ 2(S)
Console#
```

Table 202: show mvr6 members - display description

Field	Description
Group Address	Multicast group address.
VLAN	VLAN to which this address is forwarded.
Port	Port to which this address is forwarded.
Up time	Time that this multicast group has been known.
Expire	The time until this entry expires.
Count	The number of times this address has been learned by MVR (MLD snooping).

show mvr6 profile

This command shows all configured MVR profiles.

COMMAND MODE

Privileged Exec

EXAMPLE

The following shows all configured MVR profiles:

```
Console#show mvr6 profile
 MVR Profile Name     Start IPv6 Addr.          End IPv6 Addr.
 -------------------- ------------------------- -------------------------
 rd                                     FF00::1                   FF00::9
Console#
```

show mvr6 statistics

This command shows MVR protocol-related statistics for the specified interface.

SYNTAX

show mvr6 statistics {**input** | **output**} [**interface** *interface*]

show mvr6 domain *domain-id* **statistics** {**input** [**interface** *interface*] | **output** [**interface** *interface*] | **query**}

domain-id - An independent multicast domain. (Range: 1-5)

interface

ethernet *unit/port*

unit - Unit identifier. (Range: 1)

port - Port number. (Range: 1-28)

port-channel *channel-id* (Range: 1-8)

vlan *vlan-id* - VLAN ID (Range: 1-4094)

query - Displays MVR query-related statistics.

DEFAULT SETTING

Displays statistics for all domains.

COMMAND MODE

Privileged Exec

EXAMPLE

The following shows MVR protocol-related statistics received:

```
Console#show mvr6 domain 1 statistics input
 MVR Domain : 1
 Input Statistics:
 Interface Report   Leave    G Query  G(-S)-S Query Drop     Join Succ Group
 --------- -------- -------- -------- ------------- -------- --------- ------
 Eth 1/ 1        23       11        4            10        5        20      9
 Eth 1/ 2        12       15        8             3        5        19      4
 VLAN    1        2        0        0             2        2        20      9
Console#
```

Table 203: show mvr6 statistics input - display description

Field	Description
Interface	Shows interfaces attached to the MVR.
Report	The number of IGMP membership reports received on this interface.
Leave	The number of leave messages received on this interface.
G Query	The number of general query messages received on this interface.
G(-S)-S Query	The number of group specific or group-and-source specific query messages received on this interface.
Drop	The number of times a report, leave or query was dropped. Packets may be dropped due to invalid format, rate limiting, packet content not allowed, or MVR group report received
Join Succ	The number of times a multicast group was successfully joined.
Group	The number of MVR groups active on this interface.

The following shows MVR protocol-related statistics sent:

```
Console#show mvr6 domain 1 statistics output
 MVR Domain : 1
 Output Statistics:
 Interface Report   Leave    G Query  G(-S)-S Query
 --------- -------- -------- -------- -------------
 Eth 1/ 1        12        0        1             0
 Eth 1/ 2         5        1        4             1
 VLAN    1        7        2        3             0
Console#
```

Table 204: show mvr6 statistics output - display description

Field	Description
Interface	Shows interfaces attached to the MVR.
Report	The number of IGMP membership reports sent from this interface.
Leave	The number of leave messages sent from this interface.
G Query	The number of general query messages sent from this interface.
G(-S)-S Query	The number of group specific or group-and-source specific query messages sent from this interface.

The following shows MVR query-related statistics:

```
Console#show mvr6 domain 1 statistics query
 Querier IPv6 Address          : FE80::2E0:CFF:FE00:FB/64
 Querier Expire Time           : 00(h):00(m):30(s)
 General Query Received        : 10
 General Query Sent            : 0
 Specific Query Received       : 2
 Specific Query Sent           : 0
 Number of Reports Sent        : 2
 Number of Leaves Sent         : 0
Console#
```

IGMP (Layer 3)

This section describes commands used to configure Layer 3 Internet Group Management Protocol (IGMP) on the switch.

Table 205: IGMP Commands (Layer 3)

Command	Function	Mode
ip igmp	Enables IGMP for the specified interface	IC
ip igmp last-member-query-interval	Configures the frequency at which to send query messages in response to receiving a leave message	IC
ip igmp max-resp-interval	Configures the maximum host response time	IC
ip igmp query-interval	Configures frequency for sending host query messages	IC
ip igmp robustval	Configures the expected packet loss	IC
ip igmp static-group	Configures the router to be a static member of a multicast group on the specified VLAN interface	IC
ip igmp version	Configures IGMP version used on this interface	IC
clear ip igmp group	Deletes entries from the IGMP cache	PE
show ip igmp groups	Displays information for IGMP groups	PE
show ip igmp interface	Displays multicast information for the specified interface	PE

ip igmp

This command enables IGMP on a VLAN interface. Use the **no** form of this command to disable IGMP on the specified interface.

SYNTAX

[**no**] **ip igmp**

DEFAULT SETTING

Disabled

COMMAND MODE

Interface Configuration (VLAN)

COMMAND USAGE

- IGMP (including query functions) can be enabled for specific VLAN interfaces at Layer 3 through the **ip igmp** command.
- When a multicast routing protocol, such as PIM, is enabled, IGMP is also enabled.

EXAMPLE

```
Console(config)#interface vlan 1
Console(config-if)#ip igmp
Console(config-if)#end
Console#show ip igmp interface
  IGMP                                 : Enabled
  IGMP Version                         : 2
  IGMP Proxy                           : Disabled
  IGMP Unsolicited Report Interval : 400 sec
  Robustness Variable                  : 2
  Query Interval                       : 125 sec
  Query Max Response Time              : 100 (resolution in 0.1 sec)
  Last Member Query Interval           : 10  (resolution in 0.1 sec)
  Querier                              : 0.0.0.0
  Joined Groups :
  Static Groups :

Console#
```

RELATED COMMANDS

ip igmp snooping (1427)
show ip igmp snooping (1442)

ip igmp last-member-query-interval

This command configures the frequency at which to send IGMP group-specific or IGMPv3 group-source-specific query messages in response to receiving a group-specific or group-source-specific leave message. Use the **no** form to restore the default setting.

SYNTAX

ip igmp last-member-query-interval *seconds*

no ip igmp last-member-query-interval

seconds - The frequency at which the switch sends group-specific or group-source-specific queries upon receipt of a leave message. (Range: 1-255 tenths of a second)

DEFAULT SETTING

10 (1 second)

COMMAND MODE

Interface Configuration (VLAN)

COMMAND USAGE

When the switch receives an IGMPv2 or IGMPv3 leave message from a host that wants to leave a multicast group, source or channel, it sends a number of group-specific or group-source-specific query messages at intervals defined by this command. If no response is received after this period, the switch stops forwarding for the group, source or channel.

EXAMPLE

```
Console(config)#interface vlan 1
Console(config-if)#ip igmp last-member-query-interval 20
Console(config-if)#
```

ip igmp max-resp-interval

This command configures the maximum response time advertised in IGMP queries. Use the **no** form of this command to restore the default.

SYNTAX

ip igmp max-resp-interval *seconds*

no ip igmp max-resp-interval

seconds - The report delay advertised in IGMP queries. (Range: 0-255 tenths of a second)

DEFAULT SETTING

100 (10 seconds)

COMMAND MODE

Interface Configuration (VLAN)

COMMAND USAGE

- IGMPv1 does not support a configurable maximum response time for query messages. It is fixed at 10 seconds for IGMPv1.
- By varying the Maximum Response Interval, the burstiness of IGMP messages passed on the subnet can be tuned; where larger values make the traffic less bursty, as host responses are spread out over a larger interval.
- The number of seconds represented by the maximum response interval must be less than the Query Interval (page 1516).

EXAMPLE

The following shows how to configure the maximum response time to 20 seconds.

```
Console(config-if)#ip igmp query-max-response-time 200
Console(config-if)#
```

RELATED COMMANDS

ip igmp version (1519)
ip igmp query-interval (1516)

ip igmp query-interval

This command configures the frequency at which host query messages are sent. Use the **no** form to restore the default.

SYNTAX

ip igmp query-interval *seconds*

no ip igmp query-interval

seconds - The frequency at which the switch sends IGMP host-query messages. (Range: 1-255 seconds)

DEFAULT SETTING

125 seconds

COMMAND MODE

Interface Configuration (VLAN)

COMMAND USAGE

- Multicast routers send host query messages to determine the interfaces that are connected to downstream hosts requesting a specific multicast service. Only the designated multicast router for a subnet sends host query messages, which are addressed to the multicast address 224.0.0.1, and uses a time-to-live (TTL) value of 1.
- For IGMP Version 1, the designated router is elected according to the multicast routing protocol that runs on the LAN. But for IGMP Version 2

and 3, the designated querier is the lowest IP-addressed multicast router on the subnet.

EXAMPLE

The following shows how to configure the query interval to 100 seconds.

```
Console(config-if)#ip igmp query-interval 100
Console(config-if)#
```

RELATED COMMANDS

ip igmp max-resp-interval (1515)

ip igmp robustval

This command specifies the robustness (expected packet loss) for this interface. Use the **no** form of this command to restore the default value.

SYNTAX

ip igmp robustval *robust-value*

no ip igmp robustval

robust-value - The robustness of this interface. (Range: 1-255)

DEFAULT SETTING

2

COMMAND MODE

Interface Configuration (VLAN)

COMMAND USAGE

- The robustness value is used in calculating the appropriate range for other IGMP variables, such as the Group Membership Interval, as well as the Other Querier Present Interval, and the Startup Query Count (RFC 3376).

- Routers adopt the robustness value from the most recently received query. If the querier's robustness variable (QRV) is zero, indicating that the QRV field does not contain a declared robustness value, the switch will set the robustness variable to the value statically configured by this command. If the QRV exceeds 7, the maximum value of the QRV field, the robustness value is set to zero, meaning that this device will not advertise a QRV in any query messages it subsequently sends.

EXAMPLE

```
Console(config-if)#ip igmp robustness-variable 3
Console(config-if)#
```

ip igmp static-group

This command configures the router to be a static member of a multicast group on the specified VLAN interface. Use the **no** form to remove the static mapping.

SYNTAX

ip igmp static-group *group-address* [**source** *source-address*]

no ip igmp static-group

group-address - IP multicast group address. (The group addresses specified cannot be in the range of 224.0.0.1 - 239.255.255.255.)

source-address - Source address for a multicast server transmitting traffic to the corresponding multicast group address.

DEFAULT SETTING

None

COMMAND MODE

Interface Configuration (VLAN)

COMMAND USAGE

- Group addresses within the entire multicast group address range can be specified with this command. However, if any address within the source-specific multicast (SSM) address range (default 232/8) is specified, but no source address is included in the command, the request to join the multicast group will fail unless the next node up the reverse path tree has statically mapped this group to a specific source address. Also, if an address outside of the SSM address range is specified, and a specific source address is included in the command, the request to join the multicast group will also fail if the next node up the reverse path tree has enabled the PIM-SSM protocol.

- If a static group is configured for an any-source multicast (*,G), a source address cannot subsequently be defined for this group without first deleting the entry.

- If a static group is configured for one or more source-specific multicasts (S,G), an any-source multicast (*,G) cannot subsequently be defined for this group without first deleting all of the associated (S,G) entries.

- Using the **no** form of this command to delete a static group without specifying the source address will delete all any-source and source-specific multicast entries for the specified group.

- The switch supports a maximum of 16 static group entries.

EXAMPLE

The following example assigns VLAN 1 as a static member of the specified multicast group.

```
Console(config)#interface vlan1
Console(config-if)#ip igmp static-group 225.1.1.1
```

ip igmp version

This command configures the IGMP version used on an interface. Use the **no** form of this command to restore the default.

Syntax

ip igmp version {**1** | **2** | **3**}

no ip igmp version

1 - IGMP Version 1

2 - IGMP Version 2

3 - IGMP Version 3

Default Setting

IGMP Version 2

Command Mode

Interface Configuration (VLAN)

Command Usage

- All routers on the subnet must support the same version. However, the multicast hosts on the subnet may support any of the IGMP versions 1 - 3.
- If the switch receives an IGMP Version 1 Membership Report, it sets a timer to note that there are Version 1 hosts which are members of the group for which it heard the report.

  If there are Version 1 hosts present for a particular group, the switch will ignore any Leave Group messages that it receives for that group.

Example

```
Console(config-if)#ip igmp version 1
Console(config-if)#
```

clear ip igmp group

This command deletes entries from the IGMP cache.

Syntax

clear ip igmp group [*group-address* | **interface** *interface*]

group-address - IP address of the multicast group.

interface

vlan *vlan-id* - VLAN ID. (Range: 1-4094)

Default Setting

Deletes all entries in the cache if no options are selected.

Command Mode

Privileged Exec

COMMAND USAGE

Enter the address for a multicast group to delete all entries for the specified group. Enter the interface option to delete all multicast groups for the specified interface. Enter no options to clear all multicast groups from the cache.

EXAMPLE

The following example clears all multicast group entries for VLAN 1.

```
Console#clear ip igmp interface vlan1
Console#
```

show ip igmp groups

This command displays information on multicast groups active on the switch and learned through IGMP.

SYNTAX

show ip igmp groups [{*group-address* | *interface*} [**detail**] | **detail**]

group-address - IP multicast group address.

interface

vlan *vlan-id* - VLAN ID. (Range: 1-4094)

detail - Displays detailed information about the multicast process and source addresses when available.

COMMAND MODE

Privileged Exec

COMMAND USAGE

To display information about multicast groups, IGMP must first be enabled on the interface to which a group has been assigned using the ip igmp command, and multicast routing must be enabled globally on the system using the ip multicast-routing command.

EXAMPLE

The following shows options for displaying IGMP group information by interface, group address, and static listing.

```
Console#show ip igmp groups
Group Address   Interface VLAN  Last Reporter   Uptime   Expire   V1 Timer
--------------- --------------- --------------- -------- -------- --------
    224.0.17.17               1    192.168.1.10    0:0:1   0:4:19    0:0:0
Console#show ip igmp groups 234.5.6.8
Group Address   Interface VLAN  Last Reporter   Uptime   Expire   V1 Timer
--------------- --------------- --------------- -------- -------- --------
    224.0.17.17               1    192.168.1.10    0:0:1   0:4:19    0:0:0
Console#show ip igmp groups interface vlan 1
Group Address   Interface VLAN  Last Reporter   Uptime   Expire   V1 Timer
--------------- --------------- --------------- -------- -------- --------
```

```
    224.0.17.17                   1    192.168.1.10    0:0:1   0:4:19    0:0:0
Console#
```

Table 206: show ip igmp groups - display description

Field	Description
Group Address	IP multicast group address with subscribers directly attached or downstream from the switch.
Interface VLAN	The interface on the switch that has received traffic directed to the multicast group address.
Last Reporter	The IP address of the source of the last membership report received for this multicast group address on this interface.
Uptime	The time elapsed since this entry was created.
Expire	The time remaining before this entry will be aged out. (The default is 260 seconds.) This field displays “stopped” if the Group Mode is INCLUDE.
V1 Timer	The time remaining until the switch assumes that there are no longer any IGMP Version 1 members on the IP subnet attached to this interface. ◆ If the switch receives an IGMP Version 1 Membership Report, it sets a timer to note that there are Version 1 hosts present which are members of the group for which it heard the report. ◆ If there are Version 1 hosts present for a particular group, the switch will ignore any Leave Group messages that it receives for that group.

The following shows the information displayed in a detailed listing for a dynamically learned multicast group.

```
Console#show ip igmp groups detail
Interface        : VLAN 1
Group            : 224.1.2.3
Uptime           : 0h:0m:12s
Group mode       : Include
Last reporter    : 0.0.0.0
Group Source List:
Source Address  Uptime      v3 Exp      Fwd
--------------- ----------- ----------- ---
      192.1.2.3   0h:0m:12s    0h:0m:0s Yes
Console#
```

Table 207: show ip igmp groups detail - display description

Field	Description
Interface	The interface on the switch that has received traffic directed to the multicast group address.
Group	IP multicast group address with subscribers directly attached or downstream from the switch, or a static multicast group assigned to this interface.
Uptime	The time elapsed since this entry was created.

Table 207: show ip igmp groups detail - display description

Field	Description
`Group mode`	In INCLUDE mode, reception of packets sent to the specified multicast address is requested only from those IP source addresses listed in the source-list parameter. In EXCLUDE mode, reception of packets sent to the given multicast address is requested from all IP source addresses except for those listed in the source-list parameter, and where the source timer status has expired. Note that EXCLUDE mode does not apply to SSM addresses.
`Last Reporter`	The IP address of the source of the last membership report received for this multicast group address on this interface.
`Group Source List`	A list of zero or more IP unicast addresses from which multicast reception is desired or not desired, depending on the filter mode.
`Source Address`	The address of one of the multicast servers transmitting traffic to the specified group.
`Uptime`	The time elapsed since this entry was created.
`v3 Exp`	The time remaining before this entry will be aged out. The V3 label indicates that the expire time is only provided for sources learned through IGMP Version 3. (The default is 260 seconds.)
`Fwd`	Indicates whether or not traffic will be forwarded from the multicast source.

show ip igmp interface

This command shows multicast information for the specified interface.

SYNTAX

show ip igmp interface [*interface*]

interface

vlan *vlan-id* - VLAN ID. (Range: 1-4094)

DEFAULT SETTING

None

COMMAND MODE

Privileged Exec

EXAMPLE

The following example shows the IGMP configuration for VLAN 1, as well as the device currently serving as the IGMP querier for active multicast services on this interface.

```
switch#show ip igmp interface vlan 1
Vlan 1 : up
  IGMP                              : Disabled
  IGMP Version                      : 2
  IGMP Proxy                        : Enabled
  IGMP Unsolicited-report-interval : 400 sec
  Robustness variable               : 2
  Query Interval                    : 125 sec
  Query Max Response Time           : 100 (resolution in 0.1 sec)
  Last Member Query Interval        : 10  (resolution in 0.1 sec)
  Querier                           : 0.0.0.0
  Joined Groups :
  Static Groups :
switch#
```

IGMP PROXY ROUTING

This section describes commands used to configure IGMP Proxy Routing on the switch.

Table 208: IGMP Proxy Commands

Command	Function	Mode
ip igmp proxy	Enables IGMP proxy service for multicast routing	IC
ip igmp proxy unsolicited-report-interval	Specifies how often the upstream interface should transmit unsolicited IGMP reports	IC
show ip igmp interface	Displays multicast information for the specified interface	PE

To enable IGMP proxy service, follow these steps:

1. Use the ip multicast-routing command to enable IP multicasting globally on the router.

2. Use the ip igmp proxy command to enable IGMP proxy on the upstream interface that is attached to an upstream multicast router.

3. Use the ip igmp command to enable IGMP on the downstream interfaces from which to forward IGMP membership reports.

4. Optional – Use the ip igmp proxy unsolicited-report-interval command to indicate how often the system will send unsolicited reports to the upstream router.

ip igmp proxy

This command enables IGMP proxy service for multicast routing, forwarding IGMP membership information monitored on downstream interfaces onto the upstream interface in a summarized report. Use the **no** form to disable proxy service.

SYNTAX

[**no**] **ip igmp proxy**

DEFAULT SETTING

Disabled

COMMAND MODE

Interface Configuration (VLAN)

COMMAND USAGE

- When IGMP proxy is enabled on an interface, that interface is known as the upstream or host interface. This interface performs only the host portion of IGMP by sending IGMP membership reports, and automatically disables IGMP router functions.
- Interfaces with IGMP enabled, but not located in the direction of the multicast tree root are known as downstream or router interfaces. These interfaces perform the standard IGMP router functions by maintaining a database of all IGMP subscriptions on the downstream interface. IGMP must therefore be enabled on all downstream interfaces which require proxy multicast service.
- When changes occur in the downstream IGMP groups, a IGMP state change report is created and sent to the upstream router.
- If there is an IGMPv1 or IGMPv2 querier on the upstream network, then the proxy device will act as an IGMPv1 or IGMPv2 host on the upstream interface accordingly. Otherwise, it will act as an IGMPv3 host.
- Multicast routing protocols are not supported on interfaces where IGMP proxy service is enabled.
- Only one upstream interface is supported on the system.
- A maximum of 1024 multicast streams are supported.

EXAMPLE

The following example enables multicast routing globally on the switch, configures VLAN 2 as a downstream interface, and then VLAN 1 as the upstream interface.

```
Console(config)#ip multicast-routing
Console(config)#interface vlan2
Console(config-if)#ip igmp
Console(config-if)#exit
Console(config)#interface vlan1
Console(config-if)#ip igmp proxy
Console(config-if)#
```

ip igmp proxy unsolicited-report-interval

This command specifies how often the upstream interface should transmit unsolicited IGMP reports. Use the **no** form to restore the default value.

SYNTAX

ip igmp proxy unsolicited-report-interval *seconds*

no ip igmp proxy unsolicited-report-interval

seconds - The interval at which to issue unsolicited reports. (Range: 1-65535 seconds)

Default Setting

400 seconds

Command Mode

Interface Configuration (VLAN)

Example

The following example sets the interval for sending unsolicited IGMP reports to 5 seconds.

```
switch(config)#interface vlan
switch(config-if)#ip igmp proxy unsolicited-report-interval 5
switch(config)#
```

MLD (Layer 3)

This section describes commands used to configure Layer 3 Multicast Listener Discovery (MLD) on the switch.

Table 209: MLD Commands (Layer 3)

Command	Function	Mode
ipv6 mld	Enables MLD for the specified interface	IC
ipv6 mld last-member-query-response-interval	Configures the frequency at which to send query messages in response to receiving a leave message	IC
ipv6 mld max-resp-interval	Configures the maximum host response time	IC
ipv6 mld query-interval	Configures frequency for sending host query messages	IC
ipv6 mld robustval	Configures the expected packet loss	IC
ipv6 mld static-group	Statically binds multicast groups to a VLAN interface	IC
ipv6 mld version	Configures MLD version used on an interface	IC
clear ipv6 mld group	Deletes entries from the MLD cache	PE
show ipv6 mld groups	Displays information for MLD groups	PE
show ip igmp interface	Displays multicast information for an interface	PE

ipv6 mld

This command enables MLD on a VLAN interface. Use the **no** form of this command to disable MLD on the selected interface.

Syntax

[**no**] **ipv6 mld**

Default Setting

Disabled

COMMAND MODE

Interface Configuration (VLAN)

COMMAND USAGE

MLD (including query functions) can be enabled for specific VLAN interfaces at Layer 3 through the **ipv6 mld** command.

EXAMPLE

```
Console(config)#interface vlan 1
Console(config-if)#ipv6 mld
Console(config-if)#end
Console#show ipv6 mld interface
VLAN 1 : Up
  MLD                                : Enabled
  MLD Version                        : 2
  MLD Proxy                          : Disabled
  MLD Unsolicited Report Interval : 400 sec
  Robustness Variable                : 2
  Query Interval                     : 125 sec
  Query Max Response Time            : 10  sec
  Last Member Query Interval         : 1   sec
  Querier                            : ::
  Joined Groups :
  Static Groups :

Console#
```

ipv6 mld last-member-query-response-interval

This command configures the frequency at which to send MLD group-specific or MLDv2 group-source-specific query messages in response to receiving a group-specific or group-source-specific leave message from the last known active host on the subnet. Use the **no** form to restore the default setting.

SYNTAX

ipv6 mld last-member-query-response-interval *seconds*

no ipv6 mld last-member-query-response-interval

seconds - The frequency at which the switch sends group-specific or group-source-specific queries upon receipt of a leave message. (Range: 1-255 seconds)

DEFAULT SETTING

10 (1 second)

COMMAND MODE

Interface Configuration (VLAN)

COMMAND USAGE

When the switch receives an MLD or MLDv2 leave message from a host that wants to leave a multicast group, source or channel, it sends a number of group-specific or group-source-specific query messages at intervals defined by this command. If no response is received after this period, the switch stops forwarding for the group, source or channel.

EXAMPLE

```
Console(config)#interface vlan 1
Console(config-if)#ipv6 mld last-member-query-response-interval 20
Console(config-if)#
```

ipv6 mld max-resp-interval

This command configures the maximum response time advertised in MLD queries. Use the **no** form of this command to restore the default setting.

SYNTAX

ipv6 mld max-resp-interval *seconds*

no ipv6 mld max-resp-interval

seconds - The report delay advertised in MLD queries. (Range: 0-255 tenths of a second)

DEFAULT SETTING

100 (10 seconds)

COMMAND MODE

Interface Configuration (VLAN)

COMMAND USAGE

- By varying the Maximum Response Interval, the burstiness of MLD messages passed on the subnet can be tuned; where larger values make the traffic less bursty, as host responses are spread out over a larger interval.

- The number of seconds represented by the maximum response interval must be less than the Query Interval (page 1528).

EXAMPLE

The following shows how to configure the maximum response time to 20 seconds.

```
Console(config-if)#ipv6 mld max-resp-interval 200
Console(config-if)#
```

RELATED COMMANDS

ipv6 mld query-interval (1528)

ipv6 mld query-interval

This command configures the frequency at which host query messages are sent. Use the **no** form to restore the default.

SYNTAX

ipv6 mld query-interval *seconds*

no ipv6 mld query-interval

seconds - The frequency at which the switch sends MLD host-query messages. (Range: 1-255 seconds)

DEFAULT SETTING

125 seconds

COMMAND MODE

Interface Configuration (VLAN)

COMMAND USAGE

- Multicast routers send host query messages to determine the interfaces that are connected to downstream hosts requesting a specific multicast service. Only the designated multicast router for a subnet sends host query messages, which are addressed to the link-scope all-nodes multicast address FF02::1, and uses a time-to-live (TTL) value of 1.

- The designated querier is the lowest IP-addressed multicast router on the subnet.

EXAMPLE

The following shows how to configure the query interval to 100 seconds.

```
Console(config-if)#ipv6 mld query-interval 100
Console(config-if)#
```

RELATED COMMANDS

ipv6 mld max-resp-interval (1527)

ipv6 mld robustval

This command specifies the robustness (expected packet loss) for this interface. Use the **no** form of this command to restore the default value.

SYNTAX

ipv6 mld robustval *robust-value*

no ipv6 mld robustval

robust-value - The robustness of this interface. (Range: 1-255)

DEFAULT SETTING

2

COMMAND MODE

Interface Configuration (VLAN)

COMMAND USAGE

- The robustness value is used to compensate for expected packet lose on a link. It indicates the number of refresh packets related to the current MLD state which might be lost without having to terminate that state.
- Routers adopt the robustness value from the most recently received query. If the query's robustness variable (QRV) is zero, indicating that the QRV field does not contain a declared robustness value, the switch will set the robustness variable to the value statically configured by this command. If the QRV exceeds 7, the maximum value of the QRV field, the robustness value is set to zero, meaning that this device will not advertise a QRV in any query messages it subsequently sends.

EXAMPLE

```
Console(config-if)#ipv6 mld robustval 3
Console(config-if)#
```

ipv6 mld static-group

This command statically binds multicast groups to a VLAN interface. Use the **no** form to remove the static mapping.

SYNTAX

ipv6 mld static-group *group-address* [**source** *source-address*]

no ipv6 mld static-group [*group-address* [**source** *source-address*]]

group-address - IPv6 multicast group address. (Note that link-local scope addresses FF02:* are not allowed.)

source-address - IPv6 source address for a multicast server transmitting traffic to the corresponding multicast group address.

DEFAULT SETTING

None

COMMAND MODE

Interface Configuration (VLAN)

COMMAND USAGE

- If a static group is configured for an any-source multicast (*,G), a source address cannot subsequently be defined for this group without first deleting the entry.
- If a static group is configured for one or more source-specific multicasts (S,G), an any-source multicast (*,G) cannot subsequently be defined for this group without first deleting all of the associated (S,G) entries.

- Use the **no** form of this command without specifying a group address to delete all any-source and source-specific multicast entries.

- Use the **no** form of this command to delete a static group without specifying the source address to delete all any-source and source-specific multicast entries for the specified group.

- The switch supports a maximum of 64 static group entries.

EXAMPLE

The following example assigns VLAN 1 as a static member of the specified multicast group.

```
Console(config)#interface vlan 1
Console(config-if)#ipv6 mld static-group FFEE::0101
Console(config-if)#
```

ipv6 mld version

This command configures the MLD version used on an interface. Use the **no** form of this command to restore the default setting.

SYNTAX

ipv6 mld version {**1** | **2**}

no ipv6 mld version

1 - MLD Version 1

2 - MLD Version 2

DEFAULT SETTING

MLD Version 2

COMMAND MODE

Interface Configuration (VLAN)

COMMAND USAGE

- MLDv1 is derived from IGMPv2, and MLDv2 from IGMPv3. IGMP uses IP Protocol 2 message types, and MLD uses IP Protocol 58 message types, which is a subset of the ICMPv6 messages.

- MLDv2 adds the ability for a node to report interest in listening to packets with a particular multicast address only from specific source addresses as required to support Source-Specific Multicast (SSM), or from all sources except for specific source addresses.

- MLDv2 supports Source-Specific Multicast (SSM) which builds a reverse tree from a host requesting a service back up to the multicast server.

- Multicast hosts on the subnet may support either MLD versions 1 or 2.

EXAMPLE

```
Console(config-if)#ipv6 mld version 1
Console(config-if)#
```

clear ipv6 mld group

This command deletes entries from the MLD cache.

SYNTAX

clear ipv6 mld group [*group-address* | **interface** *interface*]

group-address - IPv6 address of the multicast group.

interface

vlan *vlan-id* - VLAN ID. (Range: 1-4094)

DEFAULT SETTING

Deletes all entries in the cache if no options are selected.

COMMAND MODE

Privileged Exec

COMMAND USAGE

Enter the address for a multicast group to delete all entries for the specified group. Enter the interface option to delete all multicast groups for the specified interface. Enter no options to clear all multicast groups from the cache.

EXAMPLE

The following example clears all multicast group entries for VLAN 1.

```
Console#clear ipv6 mld interface vlan 1
Console#
```

show ipv6 mld groups

This command displays information on multicast groups active on the switch and learned through MLD.

SYNTAX

show ipv6 mld groups [{*group-address* | *interface*} [**detail**] | **detail**]

group-address - IPv6 multicast group address. (Note that link-local scope addresses FF02:* are not allowed.)

interface

vlan *vlan-id* - VLAN ID. (Range: 1-4094)

detail - Displays detailed information about the multicast process and source addresses when available.

COMMAND MODE

Privileged Exec

COMMAND USAGE

To display information about multicast groups, MLD must first be enabled on the interface to which a group has been assigned using the ipv6 mld command, and multicast routing must be enabled globally on the system using the ip multicast-routing command.

EXAMPLE

The following shows options for displaying MLD group information.

```
Console#show ipv6 mld groups

Group Address                           Interface VLAN  Uptime   Expire
--------------------------------------- --------------- -------- --------
                              FFEE::101              1   0:1:59    Never
Console#show ipv6 mld groups detail
Interface        : VLAN 1
Group            : FFEE::101
Uptime           : 0h:2m:7s
Group Mode       : Include
Last Reporter    : FE80::0101
Group Source List:
Source Address                           Uptime     Expire      Fwd
--------------------------------------- ----------- ----------- ---
                             FFEE::0101 0h:0m:12s   0h:0m:0s    Yes
Console#
```

Table 210: show ipv6 mld groups - display description

Field	Description
Group Address	IP multicast group address with subscribers directly attached or downstream from the switch.
Interface VLAN	The interface on the switch that has received traffic directed to the multicast group address.
Uptime	The time elapsed since this entry was created.
Expire	The time remaining before this entry will be aged out. (The default is 260 seconds.) This field displays “stopped” if the Group Mode is INCLUDE.
Group Mode	In Include mode, reception of packets sent to the specified multicast address is requested only from those IP source addresses listed in the source-list parameter. In Exclude mode, reception of packets sent to the given multicast address is requested from all IP source addresses except for those listed in the source-list parameter, and where the source timer status has expired. Note that Exclude mode does not apply to SSM addresses.
Last Reporter	The IP address of the source of the last membership report received for this multicast group address on this interface.
Group Source List	A list of zero or more IP unicast addresses from which multicast reception is desired or not desired, depending on the filter mode.
Source Address	The address of one of the multicast servers transmitting traffic to the specified group.
Fwd	Indicates whether or not traffic will be forwarded from the multicast source.

show ipv6 mld interface

This command shows multicast information for the specified interface.

SYNTAX

show ipv6 mld interface [*interface*]

interface

vlan *vlan-id* - VLAN ID. (Range: 1-4094)

DEFAULT SETTING

None

COMMAND MODE

Privileged Exec

EXAMPLE

The following example shows the MLD configuration for VLAN 1, as well as the device currently serving as the MLD querier for active multicast services on this interface.

```
Console#show ipv6 mld interface vlan 1
VLAN 1 : Up
  MLD                                : Enabled
  MLD Version                        : 2
  MLD Proxy                          : Disabled
  MLD Unsolicited Report Interval : 400 sec
  Robustness Variable                : 2
  Query Interval                     : 125 sec
  Query Max Response Time            : 10
  Last Member Query Interval         : 1
  Querier                            : FE80::200:E8FF:FE93:82A0
  Joined Groups :
  Static Groups :
    FFEE::101
Console#
```

MLD PROXY ROUTING

This section describes commands used to configure MLD Proxy Routing on the switch.

Table 211: IGMP Proxy Commands

Command	Function	Mode
ipv6 mld proxy	Enables MLD proxy service for multicast routing	IC
ipv6 mld proxy unsolicited-report-interval	Specifies how often the upstream interface should transmit unsolicited IGMP reports	IC
show ipv6 mld interface	Displays multicast information for the specified interface	PE

To enable MLD proxy service, follow these steps:

1. Use the ipv6 multicast-routing command to enable IP multicasting globally on the router.

2. Use the ipv6 mld proxy command to enable MLD proxy on the upstream interface that is attached to an upstream multicast router.

3. Use the ipv6 mld command to enable MLD on the downstream interfaces from which to forward MLD membership reports.

4. Optional – Use the ipv6 mld proxy unsolicited-report-interval command to indicate how often the system will send unsolicited reports to the upstream router.

ipv6 mld proxy

This command enables MLD proxy service for multicast routing, forwarding MLD membership information monitored on downstream interfaces onto the upstream interface in a summarized report. Use the **no** form to disable proxy service.

SYNTAX

[**no**] **ipv6 mld proxy**

DEFAULT SETTING

Disabled

COMMAND MODE

Interface Configuration (VLAN)

COMMAND USAGE

- When MLD proxy is enabled on an interface, that interface is known as the upstream or host interface. This interface performs only the host portion of MLD by sending MLD membership reports, and automatically disables MLD router functions.

- Interfaces with MLD enabled, but not located in the direction of the multicast tree root are known as downstream or router interfaces. These interfaces perform the standard MLD router functions by maintaining a database of all MLD subscriptions on the downstream interface. MLD must therefore be enabled on all downstream interfaces which require proxy multicast service.

- When changes occur in the downstream MLD groups, an MLD state change report is created and sent to the upstream router.

- If there is an MLDv1 querier on the upstream network, then the proxy device will act as an MLDv1 host on the upstream interface accordingly. Otherwise, it will act as an MLDv2 host.

- Multicast routing protocols are not supported on interfaces where MLD proxy service is enabled.

- Only one upstream interface is supported on the system.

- MLD and MLD proxy cannot be enabled on the same interface.

- A maximum of 1024 multicast streams are supported.

EXAMPLE

The following example enables multicast routing globally on the switch, configures VLAN 2 as a downstream interface, and then VLAN 1 as the upstream interface.

```
Console(config)#ip multicast-routing
Console(config)#interface vlan2
Console(config-if)#ipv6 mld
Console(config-if)#exit
Console(config)#interface vlan1
Console(config-if)#ipv6 mld proxy
Console(config-if)#
```

ipv6 mld proxy unsolicited-report-interval

This command specifies how often the upstream interface should transmit unsolicited MLD reports. Use the **no** form to restore the default value.

SYNTAX

ipv6 mld proxy unsolicited-report-interval *seconds*

no ipv6 mld proxy unsolicited-report-interval

seconds - The interval at which to issue unsolicited reports. (Range: 1-65535 seconds)

DEFAULT SETTING

400 seconds

COMMAND MODE

Interface Configuration (VLAN)

COMMAND USAGE

- The unsolicited report interval only applies to the interface where MLD proxy has been enabled.

- MLD and MLD proxy cannot be enabled on the same interface.

EXAMPLE

The following example sets the interval for sending unsolicited MLD reports to 5 seconds.

```
Console(config)#interface vlan
Console(config-if)#ip igmp proxy unsolicited-report-interval 5
Console(config)#
```

44 LLDP Commands

Link Layer Discovery Protocol (LLDP) is used to discover basic information about neighboring devices on the local broadcast domain. LLDP is a Layer 2 protocol that uses periodic broadcasts to advertise information about the sending device. Advertised information is represented in Type Length Value (TLV) format according to the IEEE 802.1ab standard, and can include details such as device identification, capabilities and configuration settings. LLDP also defines how to store and maintain information gathered about the neighboring network nodes it discovers.

Link Layer Discovery Protocol - Media Endpoint Discovery (LLDP-MED) is an extension of LLDP intended for managing endpoint devices such as Voice over IP phones and network switches. The LLDP-MED TLVs advertise information such as network policy, power, inventory, and device location details. LLDP and LLDP-MED information can be used by SNMP applications to simplify troubleshooting, enhance network management, and maintain an accurate network topology.

Table 212: LLDP Commands

Command	Function	Mode
lldp	Enables LLDP globally on the switch	GC
lldp holdtime-multiplier	Configures the time-to-live (TTL) value sent in LLDP advertisements	GC
lldp med-fast-start-count	Configures how many medFastStart packets are transmitted	GC
lldp notification-interval	Configures the allowed interval for sending SNMP notifications about LLDP changes	GC
lldp refresh-interval	Configures the periodic transmit interval for LLDP advertisements	GC
lldp reinit-delay	Configures the delay before attempting to re-initialize after LLDP ports are disabled or the link goes down	GC
lldp tx-delay	Configures a delay between the successive transmission of advertisements initiated by a change in local LLDP MIB variables	GC
lldp admin-status	Enables LLDP transmit, receive, or transmit and receive mode on the specified port	IC
lldp basic-tlv management-ip-address	Configures an LLDP-enabled port to advertise the management address for this device	IC
lldp basic-tlv port-description	Configures an LLDP-enabled port to advertise its port description	IC
lldp basic-tlv system-capabilities	Configures an LLDP-enabled port to advertise its system capabilities	IC
lldp basic-tlv system-description	Configures an LLDP-enabled port to advertise the system description	IC

Table 212: LLDP Commands (Continued)

Command	Function	Mode
lldp basic-tlv system-name	Configures an LLDP-enabled port to advertise its system name	IC
lldp dot1-tlv proto-ident*	Configures an LLDP-enabled port to advertise the supported protocols	IC
lldp dot1-tlv proto-vid*	Configures an LLDP-enabled port to advertise port-based protocol related VLAN information	IC
lldp dot1-tlv pvid*	Configures an LLDP-enabled port to advertise its default VLAN ID	IC
lldp dot1-tlv vlan-name*	Configures an LLDP-enabled port to advertise its VLAN name	IC
lldp dot3-tlv link-agg	Configures an LLDP-enabled port to advertise its link aggregation capabilities	IC
lldp dot3-tlv mac-phy	Configures an LLDP-enabled port to advertise its MAC and physical layer specifications	IC
lldp dot3-tlv max-frame	Configures an LLDP-enabled port to advertise its maximum frame size	IC
lldp med-location civic-addr	Configures an LLDP-MED-enabled port to advertise its location identification details	IC
lldp med-notification	Enables the transmission of SNMP trap notifications about LLDP-MED changes	IC
lldp med-tlv inventory	Configures an LLDP-MED-enabled port to advertise its inventory identification details	IC
lldp med-tlv location	Configures an LLDP-MED-enabled port to advertise its location identification details	IC
lldp med-tlv med-cap	Configures an LLDP-MED-enabled port to advertise its Media Endpoint Device capabilities	IC
lldp med-tlv network-policy	Configures an LLDP-MED-enabled port to advertise its network policy configuration	IC
lldp notification	Enables the transmission of SNMP trap notifications about LLDP changes	IC
show lldp config	Shows LLDP configuration settings for all ports	PE
show lldp info local-device	Shows LLDP global and interface-specific configuration settings for this device	PE
show lldp info remote-device	Shows LLDP global and interface-specific configuration settings for remote devices	PE
show lldp info statistics	Shows statistical counters for all LLDP-enabled interfaces	PE

* Vendor-specific options may or may not be advertised by neighboring devices.

lldp

This command enables LLDP globally on the switch. Use the **no** form to disable LLDP.

SYNTAX

[**no**] **lldp**

DEFAULT SETTING

Enabled

COMMAND MODE

Global Configuration

EXAMPLE

```
Console(config)#lldp
Console(config)#
```

lldp holdtime-multiplier

This command configures the time-to-live (TTL) value sent in LLDP advertisements. Use the **no** form to restore the default setting.

SYNTAX

lldp holdtime-multiplier *value*

no lldp holdtime-multiplier

value - Calculates the TTL in seconds based on the following rule: minimum of ((Transmission Interval * Holdtime Multiplier), or 65536)

(Range: 2 - 10)

DEFAULT SETTING

Holdtime multiplier: 4
TTL: 4*30 = 120 seconds

COMMAND MODE

Global Configuration

COMMAND USAGE

The time-to-live tells the receiving LLDP agent how long to retain all information pertaining to the sending LLDP agent if it does not transmit updates in a timely manner.

EXAMPLE

```
Console(config)#lldp holdtime-multiplier 10
Console(config)#
```

lldp med-fast-start-count

This command specifies the amount of MED Fast Start LLDPDUs to transmit during the activation process of the LLDP-MED Fast Start mechanism. Use the **no** form to restore the default setting.

SYNTAX

lldp med-fast-start-count *packets*

no lldp med-fast-start-count

seconds - Amount of packets. (Range: 1-10 packets; Default: 4 packets)

DEFAULT SETTING

4 packets

COMMAND MODE

Global Configuration

COMMAND USAGE

This parameter is part of the timer which ensures that the LLDP-MED Fast Start mechanism is active for the port. LLDP-MED Fast Start is critical to the timely startup of LLDP, and therefore integral to the rapid availability of Emergency Call Service.

EXAMPLE

```
Console(config)#lldp med-fast-start-count 6
Console(config)#
```

lldp notification-interval

This command configures the allowed interval for sending SNMP notifications about LLDP MIB changes. Use the **no** form to restore the default setting.

SYNTAX

lldp notification-interval *seconds*

no lldp notification-interval

seconds - Specifies the periodic interval at which SNMP notifications are sent. (Range: 5 - 3600 seconds)

DEFAULT SETTING

5 seconds

COMMAND MODE

Global Configuration

COMMAND USAGE

- This parameter only applies to SNMP applications which use data stored in the LLDP MIB for network monitoring or management.

- Information about changes in LLDP neighbors that occur between SNMP notifications is not transmitted. Only state changes that exist at the time of a notification are included in the transmission. An SNMP agent should therefore periodically check the value of lldpStatsRemTableLastChangeTime to detect any lldpRemTablesChange notification-events missed due to throttling or transmission loss.

EXAMPLE

```
Console(config)#lldp notification-interval 30
Console(config)#
```

lldp refresh-interval

This command configures the periodic transmit interval for LLDP advertisements. Use the **no** form to restore the default setting.

SYNTAX

lldp refresh-interval *seconds*

no lldp refresh-delay

seconds - Specifies the periodic interval at which LLDP advertisements are sent. (Range: 5 - 32768 seconds)

DEFAULT SETTING

30 seconds

COMMAND MODE

Global Configuration

EXAMPLE

```
Console(config)#lldp refresh-interval 60
Console(config)#
```

lldp reinit-delay

This command configures the delay before attempting to re-initialize after LLDP ports are disabled or the link goes down. Use the **no** form to restore the default setting.

SYNTAX

lldp reinit-delay *seconds*

no lldp reinit-delay

seconds - Specifies the delay before attempting to re-initialize LLDP. (Range: 1 - 10 seconds)

DEFAULT SETTING

2 seconds

COMMAND MODE
Global Configuration

COMMAND USAGE
When LLDP is re-initialized on a port, all information in the remote systems LLDP MIB associated with this port is deleted.

EXAMPLE

```
Console(config)#lldp reinit-delay 10
Console(config)#
```

lldp tx-delay

This command configures a delay between the successive transmission of advertisements initiated by a change in local LLDP MIB variables. Use the **no** form to restore the default setting.

SYNTAX

lldp tx-delay *seconds*

no lldp tx-delay

seconds - Specifies the transmit delay. (Range: 1 - 8192 seconds)

DEFAULT SETTING
2 seconds

COMMAND MODE
Global Configuration

COMMAND USAGE
- The transmit delay is used to prevent a series of successive LLDP transmissions during a short period of rapid changes in local LLDP MIB objects, and to increase the probability that multiple, rather than single changes, are reported in each transmission.
- This attribute must comply with the following rule:
  (4 * tx-delay) ≤ refresh-interval

EXAMPLE

```
Console(config)#lldp tx-delay 10
Console(config)#
```

lldp admin-status

This command enables LLDP transmit, receive, or transmit and receive mode on the specified port. Use the **no** form to disable this feature.

SYNTAX

lldp admin-status {**rx-only** | **tx-only** | **tx-rx**}

no lldp admin-status

rx-only - Only receive LLDP PDUs.

tx-only - Only transmit LLDP PDUs.

tx-rx - Both transmit and receive LLDP Protocol Data Units (PDUs).

DEFAULT SETTING

tx-rx

COMMAND MODE

Interface Configuration (Ethernet, Port Channel)

EXAMPLE

```
Console(config)#interface ethernet 1/1
Console(config-if)#lldp admin-status rx-only
Console(config-if)#
```

lldp basic-tlv management-ip-address

This command configures an LLDP-enabled port to advertise the management address for this device. Use the **no** form to disable this feature.

SYNTAX

[**no**] **lldp basic-tlv management-ip-address**

DEFAULT SETTING

Enabled

COMMAND MODE

Interface Configuration (Ethernet, Port Channel)

COMMAND USAGE

- The management address protocol packet includes the IPv4 address of the switch. If no management address is available, the address should be the MAC address for the CPU or for the port sending this advertisement.

- The management address TLV may also include information about the specific interface associated with this address, and an object identifier indicating the type of hardware component or protocol entity associated with this address. The interface number and OID are included to assist SNMP applications to perform network discovery by indicating enterprise specific or other starting points for the search, such as the Interface or Entity MIB.

- Since there are typically a number of different addresses associated with a Layer 3 device, an individual LLDP PDU may contain more than one management address TLV.

- Every management address TLV that reports an address that is accessible on a port and protocol VLAN through the particular port should be accompanied by a port and protocol VLAN TLV that indicates the VLAN identifier (VID) associated with the management address reported by this TLV.

EXAMPLE

```
Console(config)#interface ethernet 1/1
Console(config-if)#lldp basic-tlv management-ip-address
Console(config-if)#
```

lldp basic-tlv port-description

This command configures an LLDP-enabled port to advertise its port description. Use the **no** form to disable this feature.

SYNTAX

[**no**] **lldp basic-tlv port-description**

DEFAULT SETTING

Enabled

COMMAND MODE

Interface Configuration (Ethernet, Port Channel)

COMMAND USAGE

The port description is taken from the ifDescr object in RFC 2863, which includes information about the manufacturer, the product name, and the version of the interface hardware/software.

EXAMPLE

```
Console(config)#interface ethernet 1/1
Console(config-if)#lldp basic-tlv port-description
Console(config-if)#
```

lldp basic-tlv system-capabilities

This command configures an LLDP-enabled port to advertise its system capabilities. Use the **no** form to disable this feature.

SYNTAX

[**no**] **lldp basic-tlv system-capabilities**

DEFAULT SETTING

Enabled

COMMAND MODE

Interface Configuration (Ethernet, Port Channel)

COMMAND USAGE

The system capabilities identifies the primary function(s) of the system and whether or not these primary functions are enabled. The information advertised by this TLV is described in IEEE 802.1AB.

EXAMPLE

```
Console(config)#interface ethernet 1/1
Console(config-if)#lldp basic-tlv system-capabilities
Console(config-if)#
```

lldp basic-tlv system-description

This command configures an LLDP-enabled port to advertise the system description. Use the **no** form to disable this feature.

SYNTAX

[**no**] **lldp basic-tlv system-description**

DEFAULT SETTING

Enabled

COMMAND MODE

Interface Configuration (Ethernet, Port Channel)

COMMAND USAGE

The system description is taken from the sysDescr object in RFC 3418, which includes the full name and version identification of the system's hardware type, software operating system, and networking software.

EXAMPLE

```
Console(config)#interface ethernet 1/1
Console(config-if)#lldp basic-tlv system-description
Console(config-if)#
```

lldp basic-tlv system-name

This command configures an LLDP-enabled port to advertise the system name. Use the **no** form to disable this feature.

SYNTAX

[**no**] **lldp basic-tlv system-name**

DEFAULT SETTING

Enabled

COMMAND MODE

Interface Configuration (Ethernet, Port Channel)

COMMAND USAGE

The system name is taken from the sysName object in RFC 3418, which contains the system's administratively assigned name, and is in turn based on the hostname command.

EXAMPLE

```
Console(config)#interface ethernet 1/1
Console(config-if)#lldp basic-tlv system-name
Console(config-if)#
```

lldp dot1-tlv proto-ident

This command configures an LLDP-enabled port to advertise the supported protocols. Use the **no** form to disable this feature.

SYNTAX

[**no**] **lldp dot1-tlv proto-ident**

DEFAULT SETTING

Enabled

COMMAND MODE

Interface Configuration (Ethernet, Port Channel)

COMMAND USAGE

This option advertises the protocols that are accessible through this interface.

EXAMPLE

```
Console(config)#interface ethernet 1/1
Console(config-if)#no lldp dot1-tlv proto-ident
Console(config-if)#
```

lldp dot1-tlv proto-vid

This command configures an LLDP-enabled port to advertise port-based protocol VLAN information. Use the **no** form to disable this feature.

SYNTAX

[**no**] **lldp dot1-tlv proto-vid**

DEFAULT SETTING

Enabled

COMMAND MODE

Interface Configuration (Ethernet, Port Channel)

COMMAND USAGE

This option advertises the port-based protocol VLANs configured on this interface (see "Configuring Protocol-based VLANs" on page 1371).

EXAMPLE

```
Console(config)#interface ethernet 1/1
Console(config-if)#no lldp dot1-tlv proto-vid
Console(config-if)#
```

lldp dot1-tlv pvid

This command configures an LLDP-enabled port to advertise its default VLAN ID. Use the **no** form to disable this feature.

SYNTAX

[**no**] **lldp dot1-tlv pvid**

DEFAULT SETTING

Enabled

COMMAND MODE

Interface Configuration (Ethernet, Port Channel)

COMMAND USAGE

The port's default VLAN identifier (PVID) indicates the VLAN with which untagged or priority-tagged frames are associated (see the switchport native vlan command).

EXAMPLE

```
Console(config)#interface ethernet 1/1
Console(config-if)#no lldp dot1-tlv pvid
Console(config-if)#
```

lldp dot1-tlv vlan-name

This command configures an LLDP-enabled port to advertise its VLAN name. Use the **no** form to disable this feature.

SYNTAX

[**no**] **lldp dot1-tlv vlan-name**

DEFAULT SETTING

Enabled

COMMAND MODE

Interface Configuration (Ethernet, Port Channel)

COMMAND USAGE

This option advertises the name of all VLANs to which this interface has been assigned. See "switchport allowed vlan" on page 1347 and "protocol-vlan protocol-group (Configuring Interfaces)" on page 1373.

EXAMPLE

```
Console(config)#interface ethernet 1/1
Console(config-if)#no lldp dot1-tlv vlan-name
Console(config-if)#
```

lldp dot3-tlv link-agg

This command configures an LLDP-enabled port to advertise link aggregation capabilities. Use the **no** form to disable this feature.

SYNTAX

[**no**] **lldp dot3-tlv link-agg**

DEFAULT SETTING

Enabled

COMMAND MODE

Interface Configuration (Ethernet, Port Channel)

COMMAND USAGE

This option advertises link aggregation capabilities, aggregation status of the link, and the 802.3 aggregated port identifier if this interface is currently a link aggregation member.

EXAMPLE

```
Console(config)#interface ethernet 1/1
Console(config-if)#no lldp dot3-tlv link-agg
Console(config-if)#
```

lldp dot3-tlv mac-phy

This command configures an LLDP-enabled port to advertise its MAC and physical layer capabilities. Use the **no** form to disable this feature.

SYNTAX

[**no**] **lldp dot3-tlv mac-phy**

DEFAULT SETTING

Enabled

COMMAND MODE

Interface Configuration (Ethernet, Port Channel)

COMMAND USAGE

This option advertises MAC/PHY configuration/status which includes information about auto-negotiation support/capabilities, and operational Multistation Access Unit (MAU) type.

EXAMPLE

```
Console(config)#interface ethernet 1/1
Console(config-if)#no lldp dot3-tlv mac-phy
Console(config-if)#
```

lldp dot3-tlv max-frame

This command configures an LLDP-enabled port to advertise its maximum frame size. Use the **no** form to disable this feature.

SYNTAX

[**no**] **lldp dot3-tlv max-frame**

DEFAULT SETTING

Disabled

COMMAND MODE

Interface Configuration (Ethernet, Port Channel)

COMMAND USAGE

Refer to "Frame Size" on page 910 for information on configuring the maximum frame size for this switch.

EXAMPLE

```
Console(config)#interface ethernet 1/1
Console(config-if)#lldp dot3-tlv max-frame
Console(config-if)#
```

lldp med-location civic-addr

This command configures an LLDP-MED-enabled port to advertise its location identification details. Use the **no** form to restore the default settings.

SYNTAX

lldp med-location civic-addr [[**country** *country-code*] | [**what** *device-type*] | [*ca-type ca-value*]]

no lldp med-location civic-addr [[**country**] | [**what**] | [*ca-type*]]

country-code – The two-letter ISO 3166 country code in capital ASCII letters. (Example: DK, DE or US)

device-type – The type of device to which the location applies.

0 – Location of DHCP server.

1 – Location of network element closest to client.

2 – Location of client.

ca-type – A one-octet descriptor of the data civic address value. (Range: 0-255)

ca-value – Description of a location. (Range: 1-32 characters)

DEFAULT SETTING

Not advertised
No description

COMMAND MODE

Interface Configuration (Ethernet, Port Channel)

COMMAND USAGE

- Use this command without any keywords to advertise location identification details.
- Use the *ca-type* to advertise the physical location of the device, that is the city, street number, building and room information. The address location is specified as a type and value pair, with the civic address (CA) type being defined in RFC 4776. The following table describes some of the CA type numbers and provides examples.

Table 213: LLDP MED Location CA Types

CA Type	Description	CA Value Example
1	National subdivisions (state, canton, province)	California
2	County, parish	Orange
3	City, township	Irvine
4	City division, borough, city district	West Irvine
5	Neighborhood, block	Riverside
6	Group of streets below the neighborhood level	Exchange

Table 213: LLDP MED Location CA Types (Continued)

CA Type	Description	CA Value Example
18	Street suffix or type	Avenue
19	House number	320
20	House number suffix	A
21	Landmark or vanity address	Tech Center
26	Unit (apartment, suite)	Apt 519
27	Floor	5
28	Room	509B

Any number of CA type and value pairs can be specified for the civic address location, as long as the total does not exceed 250 characters.

- For the location options defined for *device-type*, normally option **2** is used to specify the location of the client device. In situations where the client device location is not known, **0** and **1** can be used, providing the client device is physically close to the DHCP server or network element.

Example

The following example enables advertising location identification details.

```
Console(config)#interface ethernet 1/1
Console(config-if)#lldp med-location civic-addr
Console(config-if)#lldp med-location civic-addr 1 California
Console(config-if)#lldp med-location civic-addr 2 Orange
Console(config-if)#lldp med-location civic-addr 3 Irvine
Console(config-if)#lldp med-location civic-addr 4 West Irvine
Console(config-if)#lldp med-location civic-addr 6 Exchange
Console(config-if)#lldp med-location civic-addr 18 Avenue
Console(config-if)#lldp med-location civic-addr 19 320
Console(config-if)#lldp med-location civic-addr 27 5
Console(config-if)#lldp med-location civic-addr 28 509B
Console(config-if)#lldp med-location civic-addr country US
Console(config-if)#lldp med-location civic-addr what 2
Console(config-if)#
```

lldp med-notification

This command enables the transmission of SNMP trap notifications about LLDP-MED changes. Use the **no** form to disable LLDP-MED notifications.

Syntax

[**no**] **lldp med-notification**

Default Setting

Disabled

Command Mode

Interface Configuration (Ethernet, Port Channel)

COMMAND USAGE

- This option sends out SNMP trap notifications to designated target stations at the interval specified by the lldp notification-interval command. Trap notifications include information about state changes in the LLDP MIB (IEEE 802.1AB), the LLDP-MED MIB (ANSI/TIA 1057), or organization-specific LLDP-EXT-DOT1 and LLDP-EXT-DOT3 MIBs.

- SNMP trap destinations are defined using the snmp-server host command.

- Information about additional changes in LLDP neighbors that occur between SNMP notifications is not transmitted. Only state changes that exist at the time of a trap notification are included in the transmission. An SNMP agent should therefore periodically check the value of lldpStatsRemTableLastChangeTime to detect any lldpRemTablesChange notification-events missed due to throttling or transmission loss.

EXAMPLE

```
Console(config)#interface ethernet 1/1
Console(config-if)#lldp med-notification
Console(config-if)#
```

lldp med-tlv inventory

This command configures an LLDP-MED-enabled port to advertise its inventory identification details. Use the **no** form to disable this feature.

SYNTAX

[**no**] **lldp med-tlv inventory**

DEFAULT SETTING

Enabled

COMMAND MODE

Interface Configuration (Ethernet, Port Channel)

COMMAND USAGE

This option advertises device details useful for inventory management, such as manufacturer, model, software version and other pertinent information.

EXAMPLE

```
Console(config)#interface ethernet 1/1
Console(config-if)#no lldp med-tlv inventory
Console(config-if)#
```

lldp med-tlv location

This command configures an LLDP-MED-enabled port to advertise its location identification details. Use the **no** form to disable this feature.

SYNTAX

[**no**] **lldp med-tlv location**

DEFAULT SETTING

Enabled

COMMAND MODE

Interface Configuration (Ethernet, Port Channel)

COMMAND USAGE

This option advertises location identification details.

EXAMPLE

```
Console(config)#interface ethernet 1/1
Console(config-if)#lldp med-tlv location
Console(config-if)#
```

lldp med-tlv med-cap

This command configures an LLDP-MED-enabled port to advertise its Media Endpoint Device capabilities. Use the **no** form to disable this feature.

SYNTAX

[**no**] **lldp med-tlv med-cap**

DEFAULT SETTING

Enabled

COMMAND MODE

Interface Configuration (Ethernet, Port Channel)

COMMAND USAGE

This option advertises LLDP-MED TLV capabilities, allowing Media Endpoint and Connectivity Devices to efficiently discover which LLDP-MED related TLVs are supported on the switch.

EXAMPLE

```
Console(config)#interface ethernet 1/1
Console(config-if)#lldp med-tlv med-cap
Console(config-if)#
```

lldp med-tlv network-policy

This command configures an LLDP-MED-enabled port to advertise its network policy configuration. Use the **no** form to disable this feature.

SYNTAX

[**no**] **lldp med-tlv network-policy**

DEFAULT SETTING

Enabled

COMMAND MODE

Interface Configuration (Ethernet, Port Channel)

COMMAND USAGE

This option advertises network policy configuration information, aiding in the discovery and diagnosis of VLAN configuration mismatches on a port. Improper network policy configurations frequently result in voice quality degradation or complete service disruption.

EXAMPLE

```
Console(config)#interface ethernet 1/1
Console(config-if)#lldp med-tlv network-policy
Console(config-if)#
```

lldp notification

This command enables the transmission of SNMP trap notifications about LLDP changes. Use the **no** form to disable LLDP notifications.

SYNTAX

[**no**] **lldp notification**

DEFAULT SETTING

Disabled

COMMAND MODE

Interface Configuration (Ethernet, Port Channel)

COMMAND USAGE

- This option sends out SNMP trap notifications to designated target stations at the interval specified by the lldp notification-interval command. Trap notifications include information about state changes in the LLDP MIB (IEEE 802.1AB), or organization-specific LLDP-EXT-DOT1 and LLDP-EXT-DOT3 MIBs.

- SNMP trap destinations are defined using the snmp-server host command.

- Information about additional changes in LLDP neighbors that occur between SNMP notifications is not transmitted. Only state changes that exist at the time of a trap notification are included in the transmission.

An SNMP agent should therefore periodically check the value of lldpStatsRemTableLastChangeTime to detect any lldpRemTablesChange notification-events missed due to throttling or transmission loss.

EXAMPLE

```
Console(config)#interface ethernet 1/1
Console(config-if)#lldp notification
Console(config-if)#
```

show lldp config

This command shows LLDP configuration settings for all ports.

SYNTAX

show lldp config [**detail** *interface*]

detail - Shows configuration summary.

interface

ethernet *unit*/*port*

unit - Unit identifier. (Range: 1)

port - Port number. (Range: 1-28)

port-channel *channel-id* (Range: 1-8)

COMMAND MODE

Privileged Exec

EXAMPLE

```
Console#show lldp config

LLDP Global Configuation

 LLDP Enabled                 : Yes
 LLDP Transmit Interval       : 30 sec.
 LLDP Hold Time Multiplier    : 4
 LLDP Delay Interval          : 2 sec.
 LLDP Re-initialization Delay : 2 sec.
 LLDP Notification Interval   : 5 sec.
 LLDP MED Fast Start Count    : 4

LLDP Port Configuration
 Port     Admin Status Notification Enabled
 -------- ------------ --------------------
 Eth 1/1  Tx-Rx        True
 Eth 1/2  Tx-Rx        True
 Eth 1/3  Tx-Rx        True
 Eth 1/4  Tx-Rx        True
 Eth 1/5  Tx-Rx        True
.
.
.
```

```
Console#show lldp config detail ethernet 1/1

LLDP Port Configuration Detail

 Port : Eth 1/1
 Admin Status : Tx-Rx
 Notification Enabled : True
 Basic TLVs Advertised:
   port-description
   system-name
   system-description
   system-capabilities
   management-ip-address
 802.1 specific TLVs Advertised:
  *port-vid
  *vlan-name
  *proto-vlan
  *proto-ident
 802.3 specific TLVs Advertised:
  *mac-phy
  *link-agg
  *max-frame
 MED Configuration:
 MED Notification Status : Enabled
 MED Enabled TLVs Advertised:
  *med-cap
  *network-policy
  *location
  *inventory
 MED Location Identification:
  Location Data Format : Civic Address LCI
  Civic Address Status : Enabled
  Country Name         : US
  What                 : 2
  CA-Type              : 1
  CA-Value             : Alabama
  CA-Type              : 2
  CA-Value             : Tuscaloosa

Console#
```

show lldp info local-device

This command shows LLDP global and interface-specific configuration settings for this device.

SYNTAX

show lldp info local-device [**detail** *interface*]

detail - Shows configuration summary.

interface

ethernet *unit*/*port*

unit - Unit identifier. (Range: 1)

port - Port number. (Range: 1-28)

port-channel *channel-id* (Range: 1-8)

COMMAND MODE

Privileged Exec

EXAMPLE

```
Console#show lldp info local-device

 LLDP Local System Information
  Chassis Type : MAC Address
  Chassis ID   : 00-01-02-03-04-05
  System Name  :
  System Description : ECS4600-28F
 System Capabilities Support : Bridge, Router
 System Capabilities Enabled : Bridge, Router
  Management Address : 192.168.0.101 (IPv4)

 LLDP Port Information
  Port    PortID Type      PortID            Port Description
 -------- ---------------- ----------------- --------------------------------
 Eth 1/1  MAC Address      00-12-CF-DA-FC-E9 Ethernet Port on unit 0, port 1
 Eth 1/2  MAC Address      00-12-CF-DA-FC-EA Ethernet Port on unit 0, port 2
 Eth 1/3  MAC Address      00-12-CF-DA-FC-EB Ethernet Port on unit 0, port 3
 Eth 1/4  MAC Address      00-12-CF-DA-FC-EC Ethernet Port on unit 0, port 4
.
.
.
Console#show lldp info local-device detail ethernet 1/1

LLDP Port Information Details

 Port             : Eth 1/1
 Port Type        : MAC Address
 Port ID          : 00-E0-0C-00-00-AE
 Port Description : Ethernet Port on unit 0, port 1
 MED Capability   : LLDP-MED Capabilities
                    Network Policy
                    Location Identification
                    Inventory

Console#
```

show lldp info remote-device

This command shows LLDP global and interface-specific configuration settings for remote devices attached to an LLDP-enabled port.

SYNTAX

show lldp info remote-device [**detail** *interface*]

detail - Shows configuration summary.

interface

ethernet *unit*/*port*

unit - Unit identifier. (Range: 1)

port - Port number. (Range: 1-28)

port-channel *channel-id* (Range: 1-8)

COMMAND MODE

Privileged Exec

EXAMPLE

Note that an IP phone or other end-node device which advertises LLDP-MED capabilities must be connected to the switch for information to be displayed in the “LLDP-MED Capability” and other related fields.

```
Console#show lldp info remote-device

 LLDP Remote Devices Information

  Interface Chassis ID        Port ID           System Name
  --------- ----------------- ----------------- ---------------------
  Eth 1/1   00-E0-0C-00-00-FD 00-E0-0C-00-01-02
  Eth 1/2   00-E0-0C-9C-CA-10 00-E0-0C-9C-CA-11

Console#show lldp info remote-device detail ethernet 1/1
---------------------------------------------------------------
  Local Port Name    : Eth 1/1
  Chassis Type       : MAC Address
  Chassis ID         : 00-01-02-03-04-05
  Port ID Type       : Network Address
  Port ID            : 00-01-02-03-04-06
  System Name        :
  System Description :
  System Description : ECS5110-12M
  SystemCapSupported : Bridge
  SystemCapEnabled   : Bridge
  Remote Management Address :
    192.168.1.2 (IPv4)
  Remote Port VID : 1
  Remote VLAN Name :
    VLAN-1 : DefaultVlan
  Remote Port-Protocol VLAN :
    VLAN-3 : supported, enabled
  Remote Protocol Identity (Hex) :
    88-CC
  Remote MAC/PHY Configuration Status :
    Remote port auto-neg supported : Yes
    Remote port auto-neg enabled : Yes
    Remote port auto-neg advertised cap (Hex) : 0000
    Remote port MAU type : 6
  Remote Power via MDI :
    Remote power class : PSE
    Remote power MDI supported : Yes
    Remote power MDI enabled : Yes
    Remote power pair controllable : No
    Remote power pairs : Spare
    Remote power classification : Class1
  Remote Link Aggregation :
    Remote link aggregation capable : Yes
    Remote link aggregation enable : No
    Remote link aggregation port ID : 0
  Remote Max Frame Size : 1518
  LLDP-MED Capability :
    Device Class                   : Network Connectivity
    Supported Capabilities         : LLDP-MED Capabilities
                                     Network Policy
                                     Location Identification
                                     Extended Power via MDI - PSE
                                     Inventory
    Current Capabilities           : LLDP-MED Capabilities
                                     Location Identification
                                     Extended Power via MDI - PSE
                                     Inventory
  Location Identification :
    Location Data Format           : Civic Address LCI
    Country Name                   : TW
    What                           : 2
  Extended Power via MDI :
    Power Type                     : PSE
    Power Source                   : Unknown
    Power Priority                 : Unknown
    Power Value                    : 0 Watts
  Inventory          :
    Hardware Revision              : R01
    Firmware Revision              : 1.2.2.1
    Software Revision              : 1.2.2.1
    Serial Number                  :
    Manufacture Name               :
    Model Name                     :
    Asset ID                       :

Console#
```

The following example shows information which is displayed for end-node device which advertises LLDP-MED TLVs.

```
...
  LLDP-MED Capability :
    Device Class                   : Network Connectivity
    Supported Capabilities         : LLDP-MED Capabilities
                                     Network Policy
                                     Location Identification
                                     Extended Power via MDI - PSE
                                     Inventory
    Current Capabilities           : LLDP-MED Capabilities
                                     Location Identification
                                     Extended Power via MDI - PSE
                                     Inventory
  Location Identification :
    Location Data Format           : Civic Address LCI
    Country Name                   : TW
    What                           : 2
  Extended Power via MDI :
    Power Type                     : PSE
    Power Source                   : Unknown
    Power Priority                 : Unknown
    Power Value                    : 0 Watts
  Inventory          :
    Hardware Revision              : R0A
    Firmware Revision              : 1.2.6.0
    Software Revision              : 1.2.6.0
    Serial Number                  : S123456
    Manufacture Name               : Prye
    Model Name                     : VP101
    Asset ID                       : 340937

Console#
```

show lldp info statistics

This command shows statistics based on traffic received through all attached LLDP-enabled interfaces.

SYNTAX

show lldp info statistics [**detail** *interface*]

detail - Shows configuration summary.

interface

ethernet *unit/port*

unit - Unit identifier. (Range: 1)

port - Port number. (Range: 1-28)

port-channel *channel-id* (Range: 1-8)

COMMAND MODE

Privileged Exec

EXAMPLE

```
Console#show lldp info statistics

 LLDP Device Statistics

  Neighbor Entries List Last Updated : 2450279 seconds
  New Neighbor Entries Count         : 1
  Neighbor Entries Deleted Count     : 0
  Neighbor Entries Dropped Count     : 0
  Neighbor Entries Ageout Count      : 0

  Port     NumFramesRecvd NumFramesSent NumFramesDiscarded
  -------- -------------- ------------- ------------------
  Eth 1/1               0            83                  0
  Eth 1/2              11            12                  0
  Eth 1/3               0             0                  0
  Eth 1/4               0             0                  0
  Eth 1/5               0             0                  0
⋮
Console#show lldp info statistics detail ethernet 1/1

 LLDP Port Statistics Detail

  PortName           : Eth 1/1
  Frames Discarded   : 0
  Frames Invalid     : 0
  Frames Received    : 12
  Frames Sent        : 13
  TLVs Unrecognized  : 0
  TLVs Discarded     : 0
  Neighbor Ageouts   : 0

Console#
```

45 CFM COMMANDS

Connectivity Fault Management (CFM) is an OAM protocol that includes proactive connectivity monitoring using continuity check messages, fault verification through loop back messages, and fault isolation by examining end-to-end connections between Provider Edge devices or between Customer Edge devices.

CFM is implemented as a service level protocol based on service instances which encompass only that portion of the metropolitan area network supporting a specific customer. CFM can also provide controlled management access to a hierarchy of maintenance domains (such as the customer, service provider, and equipment operator).

The following list of commands support functions for defining the CFM structure, including domains, maintenance associations, and maintenance access points. It also provides commands for fault detection through continuity check messages for all known maintenance points, and cross-check messages for statically configured maintenance points located on other devices. Fault verification is supported through loop back messages, and fault isolation through link trace messages. Fault notification is also provided by SNMP alarms which are automatically generated by maintenance points when connectivity faults or configuration errors are detected in the local maintenance domain.

Table 214: CFM Commands

Command	Function	Mode
Defining CFM Structures		
ethernet cfm ais level	Configures the maintenance level at which Alarm Indication Signal information will be sent	GC
ethernet cfm ais ma	Enables the MEPs within the specified MA to send frames with AIS information	GC
ethernet cfm ais period	Configures the interval at which AIS information is sent	GC
ethernet cfm ais suppress alarm	Suppresses AIS messages following the detection of defect conditions	GC
ethernet cfm domain	Defines a CFM maintenance domain, sets the authorized maintenance level, and enters CFM configuration mode; also specifies the MIP creation method for MAs within this domain	GC
ethernet cfm enable	Enables CFM processing globally on the switch	GC
ma index name	Creates a maintenance association within the current maintenance domain, maps it to a customer service instance, and sets the manner in which MIPs are created for this service instance	CFM
ma index name-format	Specifies the name format for the maintenance association as IEEE 802.1ag character based, or ITU-T SG13/SG15 Y.1731 defined ICC-based format	CFM

Table 214: CFM Commands (Continued)

Command	Function	Mode
ethernet cfm mep	Sets an interface as a domain boundary, defines it as a maintenance end point (MEP), and sets direction of the MEP in regard to sending and receiving CFM messages	IC
ethernet cfm port-enable	Enables CFM processing on an interface	IC
clear ethernet cfm ais mpid	Clears AIS defect information for the specified MEP	PE
show ethernet cfm configuration	Displays CFM configuration settings, including global settings, SNMP traps, and interface settings	PE
show ethernet cfm md	Displays configured maintenance domains	PE
show ethernet cfm ma	Displays configured maintenance associations	PE
show ethernet cfm maintenance-points local	Displays maintenance points configured on this device	PE
show ethernet cfm maintenance-points local detail mep	Displays detailed CFM information about a specified local MEP in the continuity check database	PE
show ethernet cfm maintenance-points remote detail	Displays detailed CFM information about a specified remote MEP in the continuity check database	PE
Continuity Check Operations		
ethernet cfm cc ma interval	Sets the transmission delay between continuity check messages	GC
ethernet cfm cc enable	Enables transmission of continuity check messages within a specified maintenance association	GC
snmp-server enable traps ethernet cfm cc	Enables SNMP traps for CFM continuity check events	GC
mep archive-hold-time	Sets the time that data from a missing MEP is kept in the continuity check database before being purged	CFM
clear ethernet cfm maintenance-points remote	Clears the contents of the continuity check database	PE
clear ethernet cfm errors	Clears continuity check errors logged for the specified maintenance domain and maintenance level	PE
show ethernet cfm errors	Displays CFM continuity check errors logged on this device	PE
Cross Check Operations		
ethernet cfm mep crosscheck start-delay	Sets the maximum delay that a device waits for remote MEPs to come up before starting the cross-check operation	GC
snmp-server enable traps ethernet cfm crosscheck	Enables SNMP traps for CFM continuity check events, in relation to the cross-check operations between statically configured MEPs and those learned via continuity check messages	GC
mep crosscheck mpid	Statically defines a remote MEP in a maintenance association	CFM
ethernet cfm mep crosscheck	Enables cross-checking between the list of configured remote MEPs within a maintenance association and MEPs learned through continuity check messages	PE
show ethernet cfm maintenance-points remote crosscheck	Displays information about remote maintenance points configured statically in a cross-check list	PE

Table 214: CFM Commands (Continued)

Command	Function	Mode
Link Trace Operations		
ethernet cfm linktrace cache	Enables caching of CFM data learned through link trace messages	GC
ethernet cfm linktrace cache hold-time	Sets the hold time for CFM link trace cache entries	GC
ethernet cfm linktrace cache size	Sets the maximum size for the link trace cache	GC
ethernet cfm linktrace	Sends CFM link trace messages to the MAC address for a MEP	PE
clear ethernet cfm linktrace-cache	Clears link trace messages logged on this device	PE
show ethernet cfm linktrace-cache	Displays the contents of the link trace cache	PE
Loopback Operations		
ethernet cfm loopback	Sends CFM loopback messages to a MAC address for a MEP or MIP	PE
Fault Generator Operations		
mep fault-notify alarm-time	Sets the time a defect must exist before a fault alarm is issued	CFM
mep fault-notify lowest-priority	Sets the lowest priority defect that is allowed to generate a fault alarm	CFM
mep fault-notify reset-time	Configures the time after a fault alarm has been issued, and no defect exists, before another fault alarm can be issued	CFM
show ethernet cfm fault-notify-generator	Displays configuration settings for the fault notification generator	PE
Delay Measure Operations		
ethernet cfm delay-measure two-way	Sends periodic delay-measure requests to a specified MEP within a maintenance association	PE

Basic Configuration Steps for CFM

1. Configure the maintenance domains with the ethernet cfm domain command.

2. Configure the maintenance associations with the ma index name command.

3. Configure the local maintenance end points (MEPs) which will serve as the domain service access points for the specified maintenance association using the ethernet cfm mep command.

4. Enter a static list of MEPs assigned to other devices within the same maintenance association using the mep crosscheck mpid command. This allows CFM to automatically verify the functionality of these remote end points by cross-checking the static list configured on this device against information learned through continuity check messages.

5. Enable CFM globally on the switch with the ethernet cfm enable command.

6. Enable CFM on the local MEPs with the ethernet cfm port-enable command.

7. Enable continuity check operations with the ethernet cfm cc enable command.

8. Enable cross-check operations with the ethernet cfm mep crosscheck command.

Other configuration changes may be required for your particular environment, such as adjusting the interval at which continuity check messages are sent (page 1581), or setting the start-up delay for the cross-check operation (page 1586). You can also enable SNMP traps for events discovered by continuity check messages (page 1583) or cross-check messages (page 1587).

Defining CFM Structures

ethernet cfm ais level

This command configures the maintenance level at which Alarm Indication Signal (AIS) information will be sent within the specified MA. Use the **no** form restore the default setting.

SYNTAX

ethernet cfm ais level *level-id* **md** *domain-name* **ma** *ma-name*

no ethernet cfm ais level md *domain-name* **ma** *ma-name*

level-id – Maintenance level at which AIS information will be sent. (Range: 0-7)

domain-name – Domain name. (Range: 1-43 alphanumeric characters)

ma-name – Maintenance association name. (Range: 1-44 alphanumeric characters)

DEFAULT SETTING

Level 0

COMMAND MODE

Global Configuration

COMMAND USAGE

The configured AIS level must be higher than the maintenance level of the domain containing the specified MA.

EXAMPLE

This example sets the maintenance level for sending AIS messages within the specified MA.

```
Console(config)#ethernet cfm ais level 4 md voip ma rd
Console(config)#
```

ethernet cfm ais ma

This command enables the MEPs within the specified MA to send frames with AIS information following detection of defect conditions. Use the **no** form to disable this feature.

SYNTAX

[**no**] **ethernet cfm ais md** *domain-name* **ma** *ma-name*

domain-name – Domain name. (Range: 1-43 alphanumeric characters)

ma-name – Maintenance association name. (Range: 1-44 alphanumeric characters)

DEFAULT SETTING

Disabled

COMMAND MODE

Global Configuration

COMMAND USAGE

- Each MA name must be unique within the CFM domain.
- Frames with AIS information can be issued at the client's maintenance level by a MEP upon detecting defect conditions. For example, defect conditions may include:
  - Signal failure conditions if continuity checks are enabled.
  - AIS condition or LCK condition if continuity checks are disabled.
- A MEP continues to transmit periodic frames with AIS information until the defect condition is removed.

EXAMPLE

This example enables the MEPs within the specified MA to send frames with AIS information.

```
Console(config)#ethernet cfm ais md voip ma rd
Console(config)#
```

ethernet cfm ais period

This command configures the interval at which AIS information is sent. Use the **no** form to restore the default setting.

SYNTAX

ethernet cfm ais period *period* **md** *domain-name* **ma** *ma-name*

no ethernet cfm ais period md *domain-name* **ma** *ma-name*

period – The interval at which AIS information is sent. (Options: 1 second, 60 seconds)

domain-name – Domain name. (Range: 1-43 alphanumeric characters)

ma-name – Maintenance association name. (Range: 1-44 alphanumeric characters)

DEFAULT SETTING

1 second

COMMAND MODE

Global Configuration

EXAMPLE

This example sets the interval for sending frames with AIS information at 60 seconds.

```
Console(config)#ethernet cfm ais period 60 md voip ma rd
Console(config)#
```

ethernet cfm ais suppress alarm

This command suppresses sending frames containing AIS information following the detection of defect conditions. Use the **no** form to restore the default setting.

SYNTAX

[**no**] **ethernet cfm ais suppress alarm md** *domain-name* **ma** *ma-name*

domain-name – Domain name. (Range: 1-43 alphanumeric characters)

ma-name – Maintenance association name. (Range: 1-44 alphanumeric characters)

DEFAULT SETTING

Suppression is disabled

COMMAND MODE

Global Configuration

Command Usage

- For multipoint connectivity, a MEP cannot determine the specific maintenance level entity that has encountered defect conditions upon receiving a frame with AIS information. More importantly, it cannot determine the associated subset of its peer MEPs for which it should suppress alarms since the received AIS information does not contain that information. Therefore, upon reception of a frame with AIS information, the MEP will suppress alarms for all peer MEPs whether there is still connectivity or not.

- However, for a point-to-point connection, a MEP has only a single peer MEP for which to suppress alarms when it receives frames with AIS information.

- If suppression is enabled by this command, upon receiving a frame with AIS information, a MEP detects an AIS condition and suppresses loss of continuity alarms associated with all its peer MEPs. A MEP resumes loss of continuity alarm generation upon detecting loss of continuity defect conditions in the absence of AIS messages.

Example

This example suppresses sending frames with AIS information.

```
Console(config)#ethernet cfm ais suppress alarm md voip ma rd
Console(config)#
```

ethernet cfm domain

This command defines a CFM maintenance domain, sets the authorized maintenance level, and enters CFM configuration mode. Use the **no** form to delete a CFM maintenance domain.

Syntax

ethernet cfm domain index *index* **name** *domain-name* **level** *level-id* [**mip-creation** *type*]

no ethernet cfm domain index *index*

index – Domain index. (Range: 1-65535)

domain-name – Domain name. (Range: 1-43 alphanumeric characters)

level-id – Authorized maintenance level for this domain. (Range: 0-7)

type – Specifies the CFM protocol's creation method for maintenance intermediate points (MIPs) in this domain:

default – MIPs can be created for any maintenance association (MA) configured in this domain on any bridge port through which the MA's VID can pass.

explicit – MIPs can be created for any MA configured in this domain only on bridge ports through which the MA's VID can pass, and only if a maintenance end point (MEP) is created at some lower MA Level.

none – No MIP can be created for any MA configured in this domain.

DEFAULT SETTING

No maintenance domains are configured.
No MIPs are created for any MA in the specified domain.

COMMAND MODE

Global Configuration

COMMAND USAGE

- A domain can only be configured with one name.

- Where domains are nested, an upper-level hierarchical domain must have a higher maintenance level than the ones it encompasses. The higher to lower level domain types commonly include entities such as customer, service provider, and operator.

- More than one domain can be configured at the same maintenance level, but a single domain can only be configured with one maintenance level.

- If MEPs or MAs are configured for a domain using the ethernet cfm mep command or ma index name command, they must first be removed before you can remove the domain.

- Maintenance domains are designed to provide a transparent method of verifying and resolving connectivity problems for end-to-end connections. By default, these connections run between the domain service access points (DSAPs) within each MA defined for a domain, and are manually configured using the ethernet cfm mep command.

  In contrast, MIPs are interconnection points that make up all possible paths between the DSAPs within an MA. MIPs are automatically generated by the CFM protocol when the *mip-creation* option in this command is set to "default" or "explicit," and the MIP creation state machine is invoked (as defined in IEEE 802.1ag). The default option allows MIPs to be created for all interconnection points within an MA, regardless of the domain's level in the maintenance hierarchy (e.g., customer, provider, or operator). While the explicit option only generates MIPs within an MA if its associated domain is not at the bottom of the maintenance hierarchy. This option is used to hide the structure of network at the lowest domain level.

  The diagnostic functions provided by CFM can be used to detect connectivity failures between any pair of MEPs in an MA. Using MIPs allows these failures to be isolated to smaller segments of the network.

  Allowing the CFM to generate MIPs exposes more of the network structure to users at higher domain levels, but can speed up the process of fault detection and recovery. This trade-off should be carefully considered when designing a CFM maintenance structure.

Also note that while MEPs are active agents which can initiate consistency check messages (CCMs), transmit loop back or link trace messages, and maintain the local CCM database. MIPs, on the other hand are passive agents which can only validate received CFM messages, and respond to loop back and link trace messages.

The MIP creation method defined by the ma index name command takes precedence over the method defined by this command.

EXAMPLE

This example creates a maintenance domain set to maintenance level 3, and enters CFM configuration mode for this domain.

```
Console(config)#ethernet cfm domain index 1 name voip level 3 mip-creation
  explicit
Console(config-ether-cfm)#
```

RELATED COMMANDS

ma index name (1570)

ethernet cfm enable

This command enables CFM processing globally on the switch. Use the **no** form to disable CFM processing globally.

SYNTAX

[**no**] **ethernet cfm enable**

DEFAULT SETTING

Disabled

COMMAND MODE

Global Configuration

COMMAND USAGE

- To avoid generating an excessive number of traps, the complete CFM maintenance structure and process parameters should be configured prior to globally enabling CFM processing with this command. Specifically, the maintenance domains, maintenance associations, and MEPs should be configured on each participating bridge.
- When CFM is enabled, hardware resources are allocated for CFM processing.

EXAMPLE

This example enables CFM globally on the switch.

```
Console(config)#ethernet cfm enable
Console(config)#
```

ma index name

This command creates a maintenance association (MA) within the current maintenance domain, maps it to a customer service instance (S-VLAN), and sets the manner in which MIPs are created for this service instance. Use the **no** form with the **vlan** keyword to remove the S-VLAN from the specified MA. Or use the **no** form with only the **index** keyword to remove the MA from the current domain.

SYNTAX

ma index *index* **name** *ma-name* [**vlan** *vlan-id* [**mip-creation** *type*]]

no ma index *index* [**vlan** *vlan-id*]

index – MA identifier. (Range: 1-2147483647)

ma-name – MA name. (Range: 1-44 alphanumeric characters)

vlan-id - Service VLAN ID. (Range: 1-4094)

type – Specifies the CFM protocol's creation method for maintenance intermediate points (MIPs) in this MA:

default – MIPs can be created for this MA on any bridge port through which the MA's VID can pass.

explicit – MIPs can be created this MA only on bridge ports through which the MA's VID can pass, and only if a maintenance end point (MEP) is created at some lower MA Level.

none – No MIP can be created for this MA.

DEFAULT SETTING

10 seconds

COMMAND MODE

CFM Domain Configuration

COMMAND USAGE

- The maintenance domain used to enter CFM domain configuration mode, the MA name and VLAN identifier specified by this command, and the DSAPs configured with the mep crosscheck mpid command create a unique service instance for each customer.

- If only the MA index and name are entered for this command, the MA will be recorded in the domain database, but will not function. No MEPs can be created until the MA is associated with a service VLAN.

- Note that multiple domains at the same maintenance level (see the ethernet cfm domain command) cannot have an MA on the same VLAN. Also, each MA name must be unique within the CFM-managed network.

- Before removing an MA, first remove all the MEPs configured for it (see the mep crosscheck mpid command).

- If the MIP creation method is not defined by this command, the creation method defined by the ethernet cfm domain command is applied to this MA. For a detailed description of the MIP types, refer to the Command Usage section under the ethernet cfm domain command.

EXAMPLE

This example creates a maintenance association, binds it to VLAN 1, and allows MIPs to be created within this MA using the default method.

```
Console(config)#ethernet cfm domain index 1 name voip level 3
Console(config-ether-cfm)#ma index 1 name rd vlan 1 mip-creation default
Console(config-ether-cfm)#
```

ma index name-format

This command specifies the name format for the maintenance association as IEEE 802.1ag character based, or ITU-T SG13/SG15 Y.1731 defined ICC-based format. Use the **no** form to restore the default setting.

SYNTAX

ma index *index* **name-format** {**character-string** | **icc-based**}

no ma index *index* **name-format**

index – MA identifier. (Range: 1-2147483647)

character-string – IEEE 802.1ag defined character string format. This is an IETF RFC 2579 DisplayString.

icc-based – ITU-T SG13/SG15 Y.1731 defined ICC based format.

DEFAULT SETTING

character-string

COMMAND MODE

CFM Domain Configuration

EXAMPLE

This example specifies the name format as character string.

```
Console(config)#ethernet cfm domain index 1 name voip level 3
Console(config-ether-cfm)#ma index 1 name-format character-string
Console(config-ether-cfm)#
```

ethernet cfm mep

This command sets an interface as a domain boundary, defines it as a maintenance end point (MEP), and sets direction of the MEP in regard to sending and receiving CFM messages. Use the **no** form to delete a MEP.

SYNTAX

ethernet cfm mep mpid *mpid* **md** *domain-name* **ma** *ma-name* [**up**]

no ethernet cfm mep mpid *mpid* **ma** *ma-name*

mpid – Maintenance end point identifier. (Range: 1-8191)

domain-name – Domain name. (Range: 1-43 alphanumeric characters) *ma-name* – Maintenance association name. (Range: 1-44 alphanumeric characters)

up – Indicates that the MEP faces inward toward the switch cross-connect matrix, and transmits CFM messages towards, and receives them from, the direction of the internal bridge relay mechanism. If the **up** keyword is not included in this command, then the MEP is facing away from the switch, and transmits CFM messages towards, and receives them from, the direction of the physical medium.

DEFAULT SETTING

No MEPs are configured.
The MEP faces outward (down).

COMMAND MODE

Interface Configuration (Ethernet, Port Channel)

COMMAND USAGE

- CFM elements must be configured in the following order: (1) maintenance domain at the same level as the MEP to be configured (using the ethernet cfm domain command), (2) maintenance association within the domain (using the ma index name command), and (3) finally the MEP using this command.
- An interface may belong to more than one domain. This command can be used to configure an interface as a MEP for different MAs in different domains.
- To change the MEP's MA or the direction it faces, first delete the MEP, and then create a new one.

EXAMPLE

This example sets port 1 as a DSAP for the specified maintenance association.

```
Console(config)#interface ethernet 1/1
Console(config-if)#ethernet cfm mep mpid 1 md voip ma rd
Console(config-if)#
```

ethernet cfm port-enable

This command enables CFM processing on an interface. Use the **no** form to disable CFM processing on an interface.

SYNTAX

[**no**] **ethernet cfm port-enable**

DEFAULT SETTING

Enabled

COMMAND MODE

Interface Configuration (Ethernet, Port Channel)

COMMAND USAGE

- An interface must be enabled before a MEP can be created with the ethernet cfm mep command.
- If a MEP has been configured on an interface with the ethernet cfm mep command, it must first be deleted before CFM can be disabled on that interface.
- When CFM is disabled, hardware resources previously used for CFM processing on that interface are released, and all CFM frames entering that interface are forwarded as normal data traffic.

EXAMPLE

This example enables CFM on port 1.

```
Console(config)#interface ethernet 1/1
Console(config-if)#ethernet cfm port-enable
Console(config-if)#
```

clear ethernet cfm ais mpid

This command clears AIS defect information for the specified MEP.

SYNTAX

clear ethernet cfm ais mpid *mpid* **md** *domain-name* **ma** *ma-name*

mpid – Maintenance end point identifier. (Range: 1-8191)

domain-name – Domain name. (Range: 1-43 alphanumeric characters)

ma-name – Maintenance association name. (Range: 1-44 alphanumeric characters)

DEFAULT SETTING

None

COMMAND MODE

Privileged Exec

COMMAND USAGE

This command can be used to clear AIS defect entries if a MEP does not exit the AIS state when all errors are resolved.

EXAMPLE

This example clears AIS defect entries on port 1.

```
Console#clear ethernet cfm ais mpid 1 md voip ma rd
Console(config)#
```

show ethernet cfm configuration

This command displays CFM configuration settings, including global settings, SNMP traps, and interface settings.

SYNTAX

show ethernet cfm configuration {**global** | **traps** | **interface** *interface*}

global – Displays global settings including CFM global status, cross-check start delay, and link trace parameters.

traps – Displays the status of all continuity check and cross-check traps.

interface – Displays CFM status for the specified interface.

ethernet *unit*/*port*

unit - Unit identifier. (Range: 1)

port - Port number. (Range: 1-28)

port-channel *channel-id* (Range: 1-8)

DEFAULT SETTING

None

COMMAND MODE

Privileged Exec

EXAMPLE

This example shows the global settings for CFM.

```
Console#show ethernet cfm configuration global
CFM Global Status          : Enabled
Crosscheck Start Delay     : 10 seconds
Linktrace Cache Status     : Enabled
Linktrace Cache Hold Time  : 100 minutes
Linktrace Cache Size       : 100 entries
Console#
```

This example shows the configuration status for continuity check and cross-check traps.

```
Console#show ethernet cfm configuration traps
CC MEP Up Trap                :Disabled
CC MEP Down Trap              :Disabled
CC Configure Trap             :Disabled
CC Loop Trap                  :Disabled
Cross Check MEP Unknown Trap :Disabled
Cross Check MEP Missing Trap :Disabled
Cross Check MA Up             :Disabled
Console#
```

Table 215: show ethernet cfm configuration traps - display description

Field	Description
CC MEP Up Trap	Sends a trap if a remote MEP is discovered and added to the local database, the port state of a previously discovered remote MEP changes, or a CCM is received from a remote MEP which as an expired entry in the archived database.
CC Mep Down Trap	Sends a trap if this device loses connectivity with a remote MEP, or connectivity has been restored to a remote MEP which has recovered from an error condition.
CC Configure Trap	Sends a trap if this device receives a CCM with the same MPID as its own but with a different source MAC address, indicating that a CFM configuration error exists.
CC Loop Trap	Sends a trap if this device receives a CCM with the same source MAC address and MPID as its own, indicating that a forwarding loop exists.
Cross Check MEP Unknown Trap	A CCM is received from a MEP that has not been configured as a DSAP (see the ethernet cfm mep command), manually configured as a remote MEP (see the mep crosscheck mpid command), nor learned through previous CCM messages.
Cross Check MEP Missing Trap	This device failed to receive three consecutive CCMs from another MEP in the same MA.
Cross Check MA Up	Generates a trap when all remote MEPs belonging to an MA come up.

This example shows the CFM status for port 1.

```
Console#show ethernet cfm configuration interface ethernet 1/1
Ethernet 1/1 CFM Status:Enabled
Console#
```

show ethernet cfm md

This command displays the configured maintenance domains.

SYNTAX

show ethernet cfm md [**level** *level*]

level – Maintenance level. (Range: 0-7)

DEFAULT SETTING

None

COMMAND MODE

Privileged Exec

EXAMPLE

This example shows all configured maintenance domains.

```
Console#show ethernet cfm md
MD Index  MD Name               Level  MIP Creation  Archive Hold Time (m.)
--------  --------------------  -----  ------------  ----------------------
       1  rd                        0  default                          100
Console#
```

show ethernet cfm ma

This command displays the configured maintenance associations.

SYNTAX

show ethernet cfm ma [**level** *level*]

level – Maintenance level. (Range: 0-7)

DEFAULT SETTING

None

COMMAND MODE

Privileged Exec

COMMAND USAGE

For a description of the values displayed in the CC Interval field, refer to the ethernet cfm cc ma interval command.

EXAMPLE

This example shows all configured maintenance associations.

```
Console#show ethernet cfm ma
MD Name         MA Index MA Name         Primary VID  CC Interval MIP Creation
--------------- -------- --------------- ----------- ----------- ------------
steve                  1 voip                      1           4 Default

Console#
```

show ethernet cfm maintenance-points local

This command displays the maintenance points configured on this device.

SYNTAX

show ethernet cfm maintenance-points local
{**mep** [**domain** *domain-name* | **interface** *interface* |
level *level-id*] | **mip** [**domain** *domain-name* | **level** *level-id*]}

mep – Displays only local maintenance end points.

mip – Displays only local maintenance intermediate points.

domain-name – Domain name. (Range: 1-43 alphanumeric characters)

interface – Displays CFM status for the specified interface.

ethernet *unit/port*

unit - Unit identifier. (Range: 1)

port - Port number. (Range: 1-28)

port-channel *channel-id* (Range: 1-8)

level-id – Maintenance level for this domain. (Range: 0-7)

DEFAULT SETTING

None

COMMAND MODE

Privileged Exec

COMMAND USAGE

- Use the **mep** keyword with this command to display the MEPs configured on this device as DSAPs through the ethernet cfm mep command.
- Using the **mip** keyword with this command to display the MIPs generated on this device by the CFM protocol when the mip-creation method is set to either "default" or "explicit" by the ethernet cfm domain command or the ma index name command.

EXAMPLE

This example shows all MEPs configured on this device for maintenance domain rd.

```
Console#show ethernet cfm maintenance-points local mep
MPID MD Name           Level Direct VLAN Port     CC Status MAC Address
---- ---------------- ----- ------ ---- -------- --------- -----------------
   1 rd                   0 UP        1 Eth 1/ 1 Enabled   00-12-CF-3A-A8-C0
Console#
```

show ethernet cfm maintenance-points local detail mep

This command displays detailed CFM information about a local MEP in the continuity check database.

SYNTAX

show ethernet cfm maintenance-points local detail mep [**domain** *domain-name* | **interface** *interface* | **level** *level-id*]

domain-name – Domain name. (Range: 1-43 alphanumeric characters)

interface – Displays CFM status for the specified interface.

ethernet *unit/port*

unit - Unit identifier. (Range: 1)

port - Port number. (Range: 1-28)

port-channel *channel-id* (Range: 1-8)

level-id – Maintenance level for this domain. (Range: 0-7)

DEFAULT SETTING

None

COMMAND MODE

Privileged Exec

EXAMPLE

This example shows detailed information about the local MEP on port 1.

```
Console#show ethernet cfm maintenance-points local detail mep
  interface ethernet 1/1
MEP Settings:
-------------
MPID                : 1
MD Name             : voip
MA Name             : rd
MA Name Format      : Character String
Level               : 0
Direction           : Up
Interface           : Eth 1/ 1
CC Status           : Enabled
MAC Address         : 00-E0-0C-00-00-FD
Defect Condition    : No Defect
Received RDI        : False
AIS Status          : Enabled
AIS Period          : 1 seconds
AIS Transmit Level  : Default
Suppress Alarm      : Disabled
Suppressing Alarms  : Disabled

Console#
```

Table 216: show ethernet cfm maintenance-points local detail mep - display

Field	Description
MPID	MEP identifier
MD Name	The maintenance domain for this entry.
MA Name	Maintenance association to which this remote MEP belongs
MA Name Format	The format of the Maintenance Association name, including primary VID, character string, unsigned Integer 16, or RFC 2865 VPN ID
Level	Maintenance level of the local maintenance point
Direction	The direction in which the MEP faces on the Bridge port (up or down).
Interface	The port to which this MEP is attached.
CC Status	Shows if the MEP will generate CCM messages.
MAC Address	MAC address of the local maintenance point. (If a CCM for the specified remote MEP has never been received or the local MEP record times out, the address will be set to the initial value of all Fs.)
Defect Condition	Shows the defect detected on the MEP.
Received RDI	Receive status of remote defect indication (RDI) messages on the MEP.
AIS Status	Shows if MEPs within the specified MA are enabled to send frames with AIS information following detection of defect conditions.
AIS Period	The interval at which AIS information is sent.
AIS Transmit Level	The maintenance level at which AIS information will be sent for the specified MEP.

Table 216: show ethernet cfm maintenance-points local detail mep - display

Field	Description
Suppress Alarm	Shows if the specified MEP is configured to suppress sending frames containing AIS information following the detection of defect conditions.
Suppressing Alarms	Shows if the specified MEP is currently suppressing sending frames containing AIS information following the detection of defect conditions.

show ethernet cfm maintenance-points remote detail

This command displays detailed CFM information about a remote MEP in the continuity check database.

SYNTAX

show ethernet cfm maintenance-points remote detail
{**mac** *mac-address* | **mpid** *mpid*}
[**domain** *domain-name* | **level** *level-id* | **ma** *ma-name*]

mac-address – MAC address of a remote maintenance point. This address can be entered in either of the following formats: xx-xx-xx-xx-xx-xx or xxxxxxxxxxxx

mpid – Maintenance end point identifier. (Range: 1-8191)

domain-name – Domain name. (Range: 1-43 alphanumeric characters)

level-id – Authorized maintenance level for this domain. (Range: 0-7)

ma-name – Maintenance association name. (Range: 1-44 alphanumeric characters)

DEFAULT SETTING

None

COMMAND MODE

Privileged Exec

COMMAND USAGE

Use the **mpid** keyword with this command to display information about a specific maintenance point, or use the **mac** keyword to display information about all maintenance points that have the specified MAC address.

EXAMPLE

This example shows detailed information about the remote MEP designated by MPID 2.

```
Console#show ethernet cfm maintenance-points remote detail mpid 2
MAC Address             : 00-0D-54-FC-A2-73
Domain/Level            : voip / 3
MA Name                 : rd
Primary VLAN            : 1
MPID                    : 2
Incoming Port           : Eth 1/ 2
```

```
CC Lifetime             : 645 seconds
Age of Last CC Message : 2 seconds
Frame Loss              : 137
CC Packet Statistics    : 647/1
Port State              : Up
Interface State         : Up
Crosscheck Status       : Enabled

Console#
```

Table 217: show ethernet cfm maintenance-points remote detail - display

Field	Description
MAC Address	MAC address of the remote maintenance point. (If a CCM for the specified remote MEP has never been received or the remote MEP record times out, the address will be set to the initial value of all Fs.)
Domain/Level	Maintenance domain and level of the remote maintenance point
MA Name	Maintenance association to which this remote MEP belongs
Primary VLAN	VLAN to which this MEP belongs
MPID	MEP identifier
Incoming Port	Port to which this remote MEP is attached.
CC Lifetime	Length of time to hold messages about this MEP in the CCM database
Age of Last CC Message	Length of time the last CCM message about this MEP has been in the CCM database
Frame Loss	Percentage of transmitted frames lost
CC Packet Statistics (received/error)	The number of CCM packets received successfully and those with errors
Port State	Port states include: Up – The port is functioning normally. Blocked – The port has been blocked by the Spanning Tree Protocol. No port state – Either no CCM has been received, or nor port status TLV was received in the last CCM.
Interface State	Interface states include: No Status – Either no CCM has been received, or no interface status TLV was received in the last CCM. Up – The interface is ready to pass packets. Down – The interface cannot pass packets. Testing – The interface is in some test mode. Unknown – The interface status cannot be determined for some reason. Dormant – The interface is not in a state to pass packets but is in a pending state, waiting for some external event. Not Present – Some component of the interface is missing. isLowerLayerDown – The interface is down due to state of the lower layer interfaces.
Crosscheck Status	Shows if crosscheck function has been enabled.

Continuity Check Operations

ethernet cfm cc ma interval

This command sets the transmission delay between continuity check messages (CCMs). Use the **no** form to restore the default settings.

SYNTAX

ethernet cfm cc md *domain-name* **ma** *ma-name*
interval *interval-level*

no ethernet cfm cc ma *ma-name* **interval**

domain-name – Domain name. (Range: 1-43 alphanumeric characters)

ma-name – Maintenance association name. (Range: 1-44 alphanumeric characters)

interval-level – The transmission delay between connectivity check messages. The setting for this parameter is expressed as levels 4 through 7, which in turn map to specific intervals of time. (CCM lifetime field options: 4 - 1 second, 5 - 10 seconds, 6 - 1 minute, 7 - 10 minutes).

DEFAULT SETTING

4 (1 second)

COMMAND MODE

Global Configuration

COMMAND USAGE

- CCMs provide a means to discover other MEPs and to detect connectivity failures in an MA. If any MEP fails to receive three consecutive CCMs from any other MEPs in its MA, a connectivity failure is registered. The interval at which CCMs are issued should therefore be configured to detect connectivity problems in a timely manner, as dictated by the nature and size of the MA.

- The maintenance of a MIP CCM database by a MIP presents some difficulty for bridges carrying a large number of Service Instances, and for whose MEPs are issuing CCMs at a high frequency. For this reason, slower CCM transmission rates may have to be used.

EXAMPLE

This example sets the transmission delay for continuity check messages to level 7 (60 seconds).

```
Console(config)#ethernet cfm cc md voip ma rd interval 7
Console(config)#
```

RELATED COMMANDS

ethernet cfm cc enable (1582)

ethernet cfm cc enable

This command enables the transmission of continuity check messages (CCMs) within a specified maintenance association. Use the **no** form to disable the transmission of these messages.

SYNTAX

[**no**] **ethernet cfm cc enable md** *domain-name* **ma** *ma-name*

domain-name – Domain name. (Range: 1-43 alphanumeric characters)

ma-name – Maintenance association name. (Range: 1-44 alphanumeric characters)

DEFAULT SETTING

Disabled

COMMAND MODE

Global Configuration

COMMAND USAGE

- CCMs are multicast periodically by a MEP in order to discover other MEPs in the same MA, and to assure connectivity to all other MEPs/MIPs in the MA.

- Each CCM received is checked to verify that the MEP identifier field sent in the message does not match its own MEPID, which would indicate a duplicate MEP or network loop. If these error types are not found, the CCM is stored in the MEP’s local database until aged out.

- If a maintenance point fails to receive three consecutive CCMs from any other MEP in the same MA, a connectivity failure is registered.

- If a maintenance point receives a CCM with an invalid MEPID or MA level or an MA level lower than its own, a failure is registered which indicates a configuration error or cross-connect error (i.e., overlapping MAs).

EXAMPLE

This example enables continuity check messages for the specified maintenance association.

```
Console(config)#ethernet cfm cc enable md voip ma rd
Console(config)#
```

snmp-server enable traps ethernet cfm cc

This command enables SNMP traps for CFM continuity check events. Use the **no** form to disable these traps.

SYNTAX

[**no**] **snmp-server enable traps ethernet cfm cc** [**config** | **loop** | **mep-down** | **mep-up**]

config – Sends a trap if this device receives a CCM with the same MPID as its own but with a different source MAC address, indicating that a CFM configuration error exists.

loop – Sends a trap if this device receives a CCM with the same source MAC address and MPID as its own, indicating that a forwarding loop exists.

mep-down – Sends a trap if this device loses connectivity with a remote MEP, or connectivity has been restored to a remote MEP which has recovered from an error condition.

mep-up – Sends a trap if a remote MEP is discovered and added to the local database, the port state of a previously discovered remote MEP changes, or a CCM is received from a remote MEP which as an expired entry in the archived database.

DEFAULT SETTING

All continuity checks are enabled.

COMMAND MODE

Global Configuration

COMMAND USAGE

All mep-up traps are suppressed when cross-checking of MEPs is enabled because cross-check traps include more detailed status information.

EXAMPLE

This example enables SNMP traps for mep-up events.

```
Console(config)#snmp-server enable traps ethernet cfm cc mep-up
Console(config)#
```

RELATED COMMANDS

ethernet cfm mep crosscheck (1589)

mep archive-hold-time

This command sets the time that data from a missing MEP is retained in the continuity check message (CCM) database before being purged. Use the **no** form to restore the default setting.

SYNTAX

mep archive-hold-time *hold-time*

hold-time – The time to retain data for a missing MEP. (Range: 1-65535 minutes)

DEFAULT SETTING

100 minutes

COMMAND MODE

CFM Domain Configuration

COMMAND USAGE

A change to the hold time only applies to entries stored in the database after this command is entered.

EXAMPLE

This example sets the aging time for missing MEPs in the CCM database to 30 minutes.

```
Console(config)#ethernet cfm domain index 1 name voip level 3
Console(config-ether-cfm)#mep archive-hold-time 30
Console(config-ether-cfm)#
```

clear ethernet cfm maintenance-points remote

This command clears the contents of the continuity check database.

SYNTAX

clear ethernet cfm maintenance-points remote
[**domain** *domain-name* | **level** *level-id*]

domain-name – Domain name. (Range: 1-43 alphanumeric characters)

level-id – Maintenance level. (Range: 0-7)

DEFAULT SETTING

None

COMMAND MODE

Privileged Exec

COMMAND USAGE

Use this command without any keywords to clear all entries in the CCM database. Use the **domain** keyword to clear the CCM database for a specific domain, or the **level** keyword to clear it for a specific maintenance level.

EXAMPLE

```
Console#clear ethernet cfm maintenance-points remote domain voip
Console#
```

clear ethernet cfm errors

This command clears continuity check errors logged for the specified maintenance domain or maintenance level.

SYNTAX

clear ethernet cfm errors [**domain** *domain-name* | **level** *level-id*]

domain-name – Domain name. (Range: 1-43 alphanumeric characters)

level-id – Maintenance level. (Range: 0-7)

DEFAULT SETTING

None

COMMAND MODE

Privileged Exec

COMMAND USAGE

Use this command without any keywords to clear all entries in the error database. Use the **domain** keyword to clear the error database for a specific domain, or the **level** keyword to clear it for a specific maintenance level.

EXAMPLE

```
Console#clear ethernet cfm errors domain voip
Console#
```

show ethernet cfm errors

This command displays the CFM continuity check errors logged on this device.

SYNTAX

show ethernet cfm errors [**domain** *domain-name* | **level** *level-id*]

domain-name – Domain name. (Range: 1-43 alphanumeric characters)

level-id – Authorized maintenance level for this domain. (Range: 0-7)

DEFAULT SETTING

None

COMMAND MODE

Privileged Exec

EXAMPLE

```
Console#show ethernet cfm errors
Level VLAN MPID Interface Remote MAC        Reason           MA Name
----- ---- ---- --------- ----------------- ---------------- ----------------
5       2    40 Eth 1/1   ab.2f.9c.00.05.01 LEAK             provider_1_2
Console#
```

Table 218: show ethernet cfm errors - display description

Field	Description
Level	Maintenance level associated with this entry.
VLAN	VLAN in which this error occurred.
MPID	Identifier of remote MEP.
Interface	Port at which the error was recorded
Remote MAC	MAC address of remote MEP.
Reason	Error types include: LEAK – MA *x* is associated with a specific VID list*, one or more of the VIDs in this MA can pass through the bridge port, no MEP is configured facing outward (down) on any bridge port for this MA, and some other MA *y*, at a higher maintenance level, and associated with at least one of the VID(s) also in MA *x*, does have a MEP configured on the bridge port. VIDS – MA *x* is associated with a specific VID list* on this MA on the bridge port, and some other MA *y*, associated with at least one of the VID(s) also in MA *x*, also has an Up MEP configured facing inward (up) on some bridge port. EXCESS_LEV – The number of different MD levels at which MIPs are to be created on this port exceeds the bridge's capabilities. OVERLAP_LEV – A MEP is created for one VID at one maintenance level, but a MEP is configured on another VID at an equivalent or higher level, exceeding the bridge's capabilities.
MA	The maintenance association for this entry.

* This definition is based on the IEEE 802.1ag standard. Current software for this switch only supports a single VLAN per MA. However, since it may interact with other devices which support multiple VLAN assignments per MA, this error message may be reported.

Cross Check Operations

ethernet cfm mep crosscheck start-delay

This command sets the maximum delay that a device waits for remote MEPs to come up before starting the cross-check operation. Use the **no** form to restore the default setting.

SYNTAX

ethernet cfm mep crosscheck start-delay *delay*

delay – The time a device waits for remote MEPs to come up before the cross-check is started. (Range: 1-65535 seconds)

DEFAULT SETTING

30 seconds

Command Mode

Global Configuration

Command Usage

- This command sets the delay that a device waits for a remote MEP to come up, and it starts cross-checking the list of statically configure remote MEPs in the local maintenance domain against the MEPs learned through CCMs.
- The cross-check start delay should be configured to a value greater than or equal to the continuity check message interval to avoid generating unnecessary traps.

Example

This example sets the maximum delay before starting the cross-check process.

```
Console(config)#ethernet cfm mep crosscheck start-delay 60
Console(config)#
```

snmp-server enable traps ethernet cfm crosscheck

This command enables SNMP traps for CFM continuity check events, in relation to the cross-check operations between statically configured MEPs and those learned via continuity check messages (CCMs). Use the **no** form to restore disable these traps.

Syntax

[**no**] **snmp-server enable traps ethernet cfm crosscheck** [**ma-up** | **mep-missing** | **mep-unknown**]

ma-up – Sends a trap when all remote MEPs in an MA come up.

mep-missing – Sends a trap if the cross-check timer expires and no CCMs have been received from a remote MEP configured in the static list.

mep-unknown – Sends a trap if an unconfigured MEP comes up.

Default Setting

All continuity checks are enabled.

Command Mode

Global Configuration

Command Usage

- For this trap type to function, cross-checking must be enabled on the required maintenance associations using the ethernet cfm mep crosscheck command.
- A mep-missing trap is sent if cross-checking is enabled (with the ethernet cfm mep crosscheck command), and no CCM is received for a

remote MEP configured in the static list (with the mep crosscheck mpid command).

- A mep-unknown trap is sent if cross-checking is enabled, and a CCM is received from a remote MEP that is not configured in the static list.

- A ma-up trap is sent if cross-checking is enabled, and a CCM is received from all remote MEPs configured in the static list for this maintenance association.

EXAMPLE

This example enables SNMP traps for mep-unknown events detected in cross-check operations.

```
Console(config)#snmp-server enable traps ethernet cfm crosscheck mep-unknown
Console(config)#
```

mep crosscheck mpid

This command statically defines a remote MEP in a maintenance association. Use the **no** form to remove a remote MEP.

SYNTAX

[**no**] **mep crosscheck mpid** *mpid* **ma** *ma-name*

mpid – Identifier for a maintenance end point which exists on another CFM-enabled device within the same MA. (Range: 1-8191)

ma-name – Maintenance association name. (Range: 1-44 alphanumeric characters)

DEFAULT SETTING

No remote MEPs are configured.

COMMAND MODE

CFM Domain Configuration

COMMAND USAGE

- Use this command to statically configure remote MEPs that exist inside the maintenance association. These remote MEPs are used in the cross-check operation to verify that all endpoints in the specified MA are operational.

- Remote MEPs can only be configured with this command if domain service access points (DSAPs) have already been created with the ethernet cfm mep command at the same maintenance level and in the same MA. DSAPs are MEPs that exist on the edge of the domain, and act as primary service access points for end-to-end cross-check, loop-back, and link-trace functions.

EXAMPLE

This example defines a static MEP for the specified maintenance association.

```
Console(config)#ethernet cfm domain index 1 name voip level 3
Console(config-ether-cfm)#ma index 1 name rd vlan 1
Console(config-ether-cfm)#mep crosscheck mpid 2 ma rd
Console(config-ether-cfm)#
```

ethernet cfm mep crosscheck

This command enables cross-checking between the static list of MEPs assigned to other devices within the same maintenance association and the MEPs learned through continuity check messages (CCMs). Use the **disable** keyword to stop the cross-check process.

SYNTAX

ethernet cfm mep crosscheck {**enable** | **disable**}
md *domain-name* **ma** *ma-name*

enable – Starts the cross-check process.

disable – Stops the cross-check process.

domain-name – Domain name. (Range: 1-43 alphanumeric characters)

ma-name – MA name. (Range: 1-44 alphanumeric characters)

DEFAULT SETTING

Disabled

COMMAND MODE

Privileged Exec

COMMAND USAGE

- Before using this command to start the cross-check process, first configure the remote MEPs that exist on other devices inside the maintenance association using the mep crosscheck mpid command. These remote MEPs are used in the cross-check operation to verify that all endpoints in the specified MA are operational.
- The cross-check process is disabled by default, and must be manually started using this command with the **enable** keyword.

EXAMPLE

This example enables cross-checking within the specified maintenance association.

```
Console#ethernet cfm mep crosscheck enable md voip ma rd
Console#
```

show ethernet cfm maintenance-points remote crosscheck

This command displays information about remote MEPs statically configured in a cross-check list.

SYNTAX

show ethernet cfm maintenance-points remote crosscheck [**domain** *domain-name* | **mpid** *mpid*]

domain-name – Domain name. (Range: 1-43 alphanumeric characters)

mpid – Maintenance end point identifier. (Range: 1-8191)

DEFAULT SETTING

None

COMMAND MODE

Privileged Exec

EXAMPLE

This example shows all remote MEPs statically configured on this device.

```
Console#show ethernet cfm maintenance-points remote crosscheck
MPID  MA Name               Level  VLAN  MEP Up  Remote MAC
----  --------------------  -----  ----  ------  ------------------
   2  downtown                  4     2  Yes     00-0D-54-FC-A2-73
Console#
```

Link Trace Operations

ethernet cfm linktrace cache

This command enables caching of CFM data learned through link trace messages. Use the **no** form to disable caching.

SYNTAX

[**no**] **ethernet cfm linktrace cache**

DEFAULT SETTING

Enabled

COMMAND MODE

Global Configuration

COMMAND USAGE

- A link trace message is a multicast CFM frame initiated by a MEP, and forwarded from MIP to MIP, with each MIP generating a link trace reply, up to the point at which the link trace message reaches its destination or can no longer be forwarded.

- Use this command to enable the link trace cache to store the results of link trace operations initiated on this device. Use the ethernet cfm linktrace command to transmit a link trace message.

- Link trace responses are returned from each MIP along the path and from the target MEP. Information stored in the cache includes the maintenance domain name, MA name, MEPID, sequence number, and TTL value.

Example

This example enables link trace caching.

```
Console(config)#ethernet cfm linktrace cache
Console(config)#
```

ethernet cfm linktrace cache hold-time

This command sets the hold time for CFM link trace cache entries. Use the **no** form to restore the default setting.

Syntax

ethernet cfm linktrace cache hold-time *minutes*

minutes – The aging time for entries stored in the link trace cache. (Range: 1-65535 minutes)

Default Setting

100 minutes

Command Mode

Global Configuration

Command Usage

Before setting the aging time for cache entries, the cache must first be enabled with the ethernet cfm linktrace cache command.

Example

This example sets the aging time for entries in the link trace cache to 60 minutes.

```
Console(config)#ethernet cfm linktrace cache hold-time 60
Console(config)#
```

ethernet cfm linktrace cache size

This command sets the maximum size for the link trace cache. Use the **no** form to restore the default setting.

Syntax

ethernet cfm linktrace cache size *entries*

entries – The number of link trace responses stored in the link trace cache. (Range: 1-4095 entries)

DEFAULT SETTING

100 entries

COMMAND MODE

Global Configuration

COMMAND USAGE

- Before setting the cache size, the cache must first be enabled with the ethernet cfm linktrace cache command.
- If the cache reaches the maximum number of specified entries, or the size is set to a value less than the current number of stored entries, no new entries are added. To add additional entries, the cache size must first be increased with this command, or purged with the clear ethernet cfm linktrace-cache command.

EXAMPLE

This example limits the maximum size of the link trace cache to 500 entries.

```
Console(config)#ethernet cfm linktrace cache size 500
Console(config)#
```

ethernet cfm linktrace

This command sends CFM link trace messages to the MAC address of a remote MEP.

SYNTAX

ethernet cfm linktrace {**dest-mep** *destination-mpid* | **src-mep** *source-mpid* {**dest-mep** *destination-mpid* | *mac-address*} | *mac-address*} **md** *domain-name* **ma** *ma-name* [**ttl** *number*]

destination-mpid – The identifier of a remote MEP that is the target of the link trace message. (Range: 1-8191)

source-mpid – The identifier of a source MEP that will send the link trace message. (Range: 1-8191)

mac-address – MAC address of a remote MEP that is the target of the link trace message. This address can be entered in either of the following formats: xx-xx-xx-xx-xx-xx or xxxxxxxxxxxx

domain-name – Domain name. (Range: 1-43 alphanumeric characters)

ma-name – Maintenance association name. (Range: 1-44 alphanumeric characters)

number – The time to live of the linktrace message. (Range: 0-255 hops)

DEFAULT SETTING

None

Command Mode

Privileged Exec

Command Usage

- Link trace messages can be targeted to MEPs, not MIPs. Before sending a link trace message, be sure you have configured the target MEP for the specified MA.
- If the MAC address of target MEP has not been learned by any local MEP, then the linktrace may fail. Use the show ethernet cfm maintenance-points remote crosscheck command to verify that a MAC address has been learned for the target MEP.
- Link trace messages (LTMs) are sent as multicast CFM frames, and forwarded from MIP to MIP, with each MIP generating a link trace reply, up to the point at which the LTM reaches its destination or can no longer be forwarded.
- Link trace messages are used to isolate faults. However, this task can be difficult in an Ethernet environment, since each node is connected through multipoint links. Fault isolation is even more challenging since the MAC address of the target node can age out in several minutes. This can cause the traced path to vary over time, or connectivity lost if faults cause the target MEP to be isolated from other MEPs in an MA.
- When using the command line or web interface, the source MEP used by to send a link trace message is chosen by the CFM protocol. However, when using SNMP, the source MEP can be specified by the user.

Example

This example sends a link trace message to the specified MEP with a maximum hop count of 25.

```
Console#linktrace ethernet dest-mep 2 md voip ma rd ttl 25
Console#
```

clear ethernet cfm linktrace-cache

This command clears link trace messages logged on this device.

Command Mode

Privileged Exec

Example

```
Console#clear ethernet cfm linktrace-cache
Console#
```

show ethernet cfm linktrace-cache

This command displays the contents of the link trace cache.

COMMAND MODE

Privileged Exec

EXAMPLE

```
Console#show ethernet cfm linktrace-cache
Hops MA             IP / Alias              Ingress MAC       Ing. Action Relay
                    Forwarded               Egress MAC        Egr. Action
---- -------------- ----------------------- ----------------- ----------- -----
   2 rd             192.168.0.6             00-12-CF-12-12-2D ingOk       Hit
                    Not Forwarded
Console#
```

Table 219: show ethernet cfm linktrace-cache - display description

Field	Description
Hops	The number hops taken to reach the target MEP.
MA	Name of the MA to which this device belongs.
IP/Alias	IP address or alias of the target device’s CPU.
Forwarded	Shows whether or not this link trace message was forwarded. A message is not forwarded if received by the target MEP.
Ingress MAC	MAC address of the ingress port on the target device.
Egress MAC	MAC address of the egress port on the target device.
Ing. Action	Action taken on the ingress port: IngOk – The target data frame passed through to the MAC Relay Entity. IngDown – The bridge port’s MAC_Operational parameter is false. This value could be returned, for example, by an operationally Down MEP that has another Down MEP at a higher MD level on the same bridge port that is causing the bridge port’s MAC_Operational parameter to be false. IngBlocked – The ingress port can be identified, but the target data frame was not forwarded when received on this port due to active topology management, i.e., the bridge port is not in the forwarding state. IngVid – The ingress port is not in the member set of the LTM’s VIDs, and ingress filtering is enabled, so the target data frame was filtered by ingress filtering.
Egr. Action	Action taken on the egress port: EgrOk – The targeted data frame was forwarded. EgrDown – The Egress Port can be identified, but that bridge port’s MAC_Operational parameter is false. EgrBlocked – The egress port can be identified, but the data frame was not passed through the egress port due to active topology management, i.e., the bridge port is not in the forwarding state. EgrVid – The Egress Port can be identified, but the bridge port is not in the LTM’s VID member set, and was therefore filtered by egress filtering.
Relay	Relay action: FDB – Target address found in forwarding database. MPDB – Target address found in the maintenance point database. HIT – Target located on this device.

Loopback Operations

ethernet cfm loopback

This command sends CFM loopback messages to a MAC address for a MEP or MIP.

SYNTAX

ethernet cfm loopback {**dest-mep** *destination-mpid* | **src-mep** *source-mpid* {**dest-mep** *destination-mpid* | *mac-address*} | *mac-address*} **md** *domain-name* **ma** *ma-name* [**count** *transmit-count*] [**size** *packet-size*]

destination-mpid – The identifier of a MEP that is the target of the loopback message. (Range: 1-8191)

source-mpid – The identifier of a source MEP that will send the loopback message. (Range: 1-8191)

mac-address – MAC address of the remote maintenance point that is the target of the loopback message. This address can be entered in either of the following formats: xx-xx-xx-xx-xx-xx or xxxxxxxxxxxx

domain-name – Domain name. (Range: 1-43 alphanumeric characters)

ma-name – Maintenance association name. (Range: 1-44 alphanumeric characters)

transmit-count – The number of times the loopback message is sent. (Range: 1-1024)

packet-size – The size of the loopback message. (Range: 64-1518 bytes)

DEFAULT SETTING

Loop back count: One loopback message is sent.
Loop back size: 64 bytes

COMMAND MODE

Privileged Exec

COMMAND USAGE

- Use this command to test the connectivity between maintenance points. If the continuity check database does not have an entry for the specified maintenance point, an error message will be displayed.
- The point from which the loopback message is transmitted (i.e., the DSAP) and the target maintenance point specified in this command must be within the same MA.
- Loop back messages can be used for fault verification and isolation after automatic detection of a fault or receipt of some other error report. Loopback messages can also used to confirm the successful restoration or initiation of connectivity. The receiving maintenance point should respond to the loop back message with a loopback reply.

- When using the command line or web interface, the source MEP used by to send a loopback message is chosen by the CFM protocol. However, when using SNMP, the source MEP can be specified by the user.

EXAMPLE

This example sends a loopback message to the specified remote MEP.

```
Console#ethernet cfm loopback dest-mep 1 md voip ma rd
Console#
```

Fault Generator Operations

mep fault-notify alarm-time

This command sets the time a defect must exist before a fault alarm is issued. Use the **no** form to restore the default setting.

SYNTAX

mep fault-notify alarm-time *alarm-time*

no fault-notify alarm-time

alarm-time – The time that one or more defects must be present before a fault alarm is generated. (Range: 3-10 seconds)

DEFAULT SETTING

3 seconds

COMMAND MODE

CFM Domain Configuration

COMMAND USAGE

A fault alarm is issued when the MEP fault notification generator state machine detects that a time period configured by this command has passed with one or more defects indicated, and fault alarms are enabled at or above the priority level set by the mep fault-notify lowest-priority command.

EXAMPLE

This example set the delay time before generating a fault alarm.

```
Console(config)#ethernet cfm domain index 1 name voip level 3
Console(config-ether-cfm)#mep fault-notify alarm-time 10
Console(config-ether-cfm)#
```

mep fault-notify lowest-priority

This command sets the lowest priority defect that is allowed to generate a fault alarm. Use the **no** form to restore the default setting.

SYNTAX

mep fault-notify lowest-priority *priority*

no fault-notify lowest-priority

priority – Lowest priority default allowed to generate a fault alarm. (Range: 1-6)

DEFAULT SETTING

Priority level 2

COMMAND MODE

CFM Domain Configuration

COMMAND USAGE

- A fault alarm can generate an SNMP notification. It is issued when the MEP fault notification generator state machine detects that a configured time period (see the mep fault-notify alarm-time command) has passed with one or more defects indicated, and fault alarms are enabled at or above the priority level set by this command. The state machine transmits no further fault alarms until it is reset by the passage of a configured time period (see the mep fault-notify reset-time command) without a defect indication. The normal procedure upon receiving a fault alarm is to inspect the reporting MEP's managed objects using an appropriate SNMP software tool, diagnose the fault, correct it, re-examine the MEP's managed objects to see whether the MEP fault notification generator state machine has been reset, and repeat those steps until the fault is resolved.

- Only the highest priority defect currently detected is reported in the fault alarm.

- Priority defects include the following items:

Table 220: Remote MEP Priority Levels

Priority Level	Level Name	Description
1	allDef	All defects.
2	macRemErrXcon	DefMACstatus, DefRemoteCCM, DefErrorCCM, or DefXconCCM.
3	remErrXcon	DefErrorCCM, DefXconCCM or DefRemoteCCM.
4	errXcon	DefErrorCCM or DefXconCCM.
5	xcon	DefXconCCM
6	noXcon	No defects DefXconCCM or lower are to be reported.

Table 221: MEP Defect Descriptions

Field	Description
DefMACstatus	Either some remote MEP is reporting its Interface Status TLV as not isUp, or all remote MEPs are reporting a Port Status TLV that contains some value other than psUp.
DefRemoteCCM	The MEP is not receiving valid CCMs from at least one of the remote MEPs.
DefErrorCCM	The MEP has received at least one invalid CCM whose CCM Interval has not yet timed out.
DefXconCCM	The MEP has received at least one CCM from either another MAID or a lower MD Level whose CCM Interval has not yet timed out.

EXAMPLE

This example sets the lowest priority defect that will generate a fault alarm.

```
Console(config)#ethernet cfm domain index 1 name voip level 3
Console(config-ether-cfm)#mep fault-notify lowest-priority 1
Console(config-ether-cfm)#
```

mep fault-notify reset-time

This command configures the time after a fault alarm has been issued, and no defect exists, before another fault alarm can be issued. Use the **no** form to restore the default setting.

SYNTAX

mep fault-notify reset-time *reset-time*

no fault-notify reset-time

reset-time – The time that must pass without any further defects indicated before another fault alarm can be generated. (Range: 3-10 seconds)

DEFAULT SETTING

10 seconds

COMMAND MODE

CFM Domain Configuration

EXAMPLE

This example sets the reset time after which another fault alarm can be generated.

```
Console(config)#ethernet cfm domain index 1 name voip level 3
Console(config-ether-cfm)#mep fault-notify reset-time 7
Console(config-ether-cfm)#
```

show ethernet cfm fault-notify-generator

This command displays configuration settings for the fault notification generator.

SYNTAX

show ethernet cfm fault-notify-generator mep *mpid*

mpid – Maintenance end point identifier. (Range: 1-8191)

DEFAULT SETTING

None

COMMAND MODE

Privileged Exec

EXAMPLE

This example shows the fault notification settings configured for one MEP.

```
Console#show ethernet cfm fault-notify-generator mep 1
MD Name      MA Name      Highest Defect Lowest Alarm  Alarm Time Reset Time
------------ ------------ -------------- ------------- ---------- ----------
        voip           rd none           macRemErrXcon      3sec.     10sec.
Console#
```

Table 222: show fault-notify-generator - display description

Field	Description
MD Name	The maintenance domain for this entry.
MA Name	The maintenance association for this entry.
Hihest Defect	The highest defect that will generate a fault alarm. (This is disabled by default.)
Lowest Alarm	The lowest defect that will generate a fault alarm (see the mep fault-notify lowest-priority command).
Alarm Time	The time a defect must exist before a fault alarm is issued (see the mep fault-notify alarm-time, command).
Reset Time	The time after a fault alarm has been issued, and no defect exists, before another fault alarm can be issued (see the mep fault-notify reset-time command).

Delay Measure Operations

ethernet cfm delay-measure two-way

This command sends periodic delay-measure requests to a specified MEP within a maintenance association.

SYNTAX

ethernet cfm delay-measure two-way [**src-mep** *source-mpid*]
{**dest-mep** *destination-mpid* | *mac-address*} **md** *domain-name*
ma *ma-name* [**count** *transmit-count*] [**interval** *interval*]
[**size** *packet-size*] [**timeout** *timeout*]

source-mpid – The identifier of a source MEP that will send the delay-measure message. (Range: 1-8191)

destination-mpid – The identifier of a remote MEP that is the target of the delay-measure message. (Range: 1-8191)

mac-address – MAC address of a remote MEP that is the target of the delay-measure message. This address can be entered in either of the following formats: xx-xx-xx-xx-xx-xx or xxxxxxxxxxxx

domain-name – Domain name. (Range: 1-43 alphanumeric characters)

ma-name – Maintenance association name. (Range: 1-44 alphanumeric characters)

count – The number of times to retry sending the message if no response is received before the specified timeout. (Range: 1-5)

interval – The transmission delay between delay-measure messages. (Range: 1-5 seconds)

packet-size – The size of the delay-measure message. (Range: 64-1518 bytes)

timeout - The timeout to wait for a response. (Range: 1-5 seconds)

DEFAULT SETTING

Count: 5
Interval: 1 second
Size: 64 bytes
Timeout: 5 seconds

COMMAND MODE

Privileged Exec

COMMAND USAGE

- Delay measurement can be used to measure frame delay and frame delay variation between MEPs.

- A local MEP must be configured for the same MA before you can use this command.

- If a MEP is enabled to generate frames with delay measurement (DM) information, it periodically sends DM frames to its peer MEP in the same MA., and expects to receive DM frames back from it.

- Frame delay measurement can be made only for two-way measurements, where the MEP transmits a frame with DM request information with the TxTimeStampf (Timestamp at the time of sending a frame with DM request information), and the receiving MEP responds with a frame with DM reply information with TxTimeStampf copied from the DM request information, RxTimeStampf (Timestamp at the time of receiving a frame with DM request information), and TxTimeStampb (Timestamp at the time of transmitting a frame with DM reply information):

  Frame Delay = (RxTimeStampb-TxTimeStampf)-(TxTimeStampb-RxTimeStampf)

- The MEP can also make two-way frame delay variation measurements based on its ability to calculate the difference between two subsequent two-way frame delay measurements.

EXAMPLE

This example sends periodic delay-measure requests to a remote MEP.

```
Console#ethernet cfm delay-measure two-way dest-mep 1 md voip ma rd
Type ESC to abort.
Sending 5 Ethernet CFM delay measurement message, timeout is 5 sec.
Sequence  Delay Time (ms.)  Delay Variation (ms.)
--------  ----------------  ---------------------
       1              < 10                      0
       2              < 10                      0
       3              < 10                      0
       4                40                     40
       5              < 10                     40
Success rate is 100% (5/5), delay time min/avg/max=0/8/40 ms.
Average frame delay variation is 16 ms.
Console#
```

46 OAM Commands

The switch provides OAM (Operation, Administration, and Maintenance) remote management tools required to monitor and maintain the links to subscriber CPEs (Customer Premise Equipment). This section describes functions including enabling OAM for selected ports, loop back testing, and displaying device information.

Table 223: OAM Commands

Command	Function	Mode
efm oam	Enables OAM services	IC
efm oam critical-link-event	Enables reporting of critical event or dying gasp	IC
efm oam link-monitor frame	Enables reporting of errored frame link events	IC
efm oam link-monitor frame threshold	Sets the threshold for errored frame link events	IC
efm oam link-monitor frame window	Sets the monitor period for errored frame link events	IC
efm oam mode	Sets the OAM operational mode to active or passive	IC
clear efm oam counters	Clears statistical counters for various OAMPDU message types	PE
clear efm oam event-log	Clears all entries from the OAM event log for the specified port	PE
efm oam remote-loopback	Initiates or terminates remote loopback test	PE
efm oam remote-loopback test	Performs remote loopback test, sending a specified number of packets	PE
show efm oam counters interface	Displays counters for various OAM PDU message types	NE,PE
show efm oam event-log interface	Displays OAM event log	NE,PE
show efm oam remote-loopback interface	Displays results of OAM remote loopback test	NE,PE
show efm oam status interface	Displays OAM configuration settings and event counters	NE,PE
show efm oam status remote interface	Displays information about attached OAM-enabled devices	NE,PE

efm oam

This command enables OAM functions on the specified port. Use the **no** form to disable this function.

SYNTAX

[**no**] **efm oam**

DEFAULT SETTING

Disabled

COMMAND MODE

Interface Configuration

COMMAND USAGE

- If the remote device also supports OAM, both exchange Information OAMPDUs to establish an OAM link.
- Not all CPEs support OAM functions, and OAM is therefore disabled by default. If the CPE attached to a port supports OAM, then this functionality must first be enabled by the **efm oam** command to gain access to other remote configuration functions.

EXAMPLE

```
Console(config)#interface ethernet 1/1
Console(config-if)#efm oam
Console(config-if)#
```

efm oam critical-link-event

This command enables reporting of critical event or dying gasp. Use the **no** form to disable this function.

SYNTAX

[**no**] **efm oam critical-link-event** {**critical-event** | **dying-gasp**}

critical-event - If a critical event occurs, the local OAM entity (this switch) indicates this to its peer by setting the appropriate flag in the next OAMPDU to be sent and stores this information in its OAM event log.

dying-gasp - If an unrecoverable condition occurs, the local OAM entity indicates this by immediately sending a trap message.

DEFAULT SETTING

Enabled

COMMAND MODE

Interface Configuration

COMMAND USAGE

- Critical events are vendor-specific and may include various failures, such as abnormal voltage fluctuations, out-of-range temperature detected, fan failure, CRC error in flash memory, insufficient memory, or other hardware faults.

- Dying gasp events are caused by an unrecoverable failure, such as a power failure or device reset.

NOTE: When system power fails, the switch will always send a dying gasp trap message prior to power down.

EXAMPLE

```
Console(config)#interface ethernet 1/1
Console(config-if)#efm oam critical-link-event dying-gasp
Console(config-if)#
```

efm oam link-monitor frame

This command enables reporting of errored frame link events. Use the **no** form to disable this function.

SYNTAX

[**no**] **efm oam link-monitor frame**

DEFAULT SETTING

Enabled

COMMAND MODE

Interface Configuration

COMMAND USAGE

- An errored frame is a frame in which one or more bits are errored.
- If this feature is enabled and an errored frame link event occurs, the local OAM entity (this switch) sends an Event Notification OAMPDU.

EXAMPLE

```
Console(config)#interface ethernet 1/1
Console(config-if)#efm oam link-monitor frame
Console(config-if)#
```

efm oam link-monitor frame threshold

This command sets the threshold for errored frame link events. Use the **no** form to restore the default setting.

SYNTAX

[**no**] **efm oam link-monitor frame threshold** *count*

count - The threshold for errored frame link events. (Range: 1-65535)

DEFAULT SETTING

1

COMMAND MODE

Interface Configuration

COMMAND USAGE

If this feature is enabled, an event notification message is sent if the threshold is reached or exceeded within the period specified by the efm oam link-monitor frame window command. The Errored Frame Event TLV includes the number of errored frames detected during the specified period.

EXAMPLE

```
Console(config)#interface ethernet 1/1
Console(config-if)#efm oam link-monitor frame threshold 5
Console(config-if)#
```

efm oam link-monitor frame window

This command sets the monitor period for errored frame link events. Use the **no** form to restore the default setting.

SYNTAX

[**no**] **efm oam link-monitor frame window** *size*

size - The period of time in which to check the reporting threshold for errored frame link events. (Range: 10-65535 units of 10 milliseconds)

DEFAULT SETTING

10 (units of 100 milliseconds) = 1 second

COMMAND MODE

Interface Configuration

COMMAND USAGE

If this feature is enabled, an event notification message is sent if the threshold specified by the efm oam link-monitor frame threshold command is reached or exceeded within the period specified by this command. The Errored Frame Event TLV includes the number of errored frames detected during the specified period.

EXAMPLE

This example set the window size to 5 seconds.

```
Console(config)#interface ethernet 1/1
Console(config-if)#efm oam link-monitor frame window 50
Console(config-if)#
```

efm oam mode

This command sets the OAM mode on the specified port. Use the **no** form to restore the default setting.

SYNTAX

efm oam mode {**active** | **passive**}

no efm oam mode

active - All OAM functions are enabled.

passive - All OAM functions are enabled, except for OAM discovery, and sending loopback control OAMPDUs.

DEFAULT SETTING

Active

COMMAND MODE

Interface Configuration

COMMAND USAGE

When set to active mode, the selected interface will initiate the OAM discovery process. When in passive mode, it can only respond to discovery messages.

EXAMPLE

```
Console(config)#interface ethernet 1/1
Console(config-if)#efm oam mode active
Console(config-if)#
```

clear efm oam counters

This command clears statistical counters for various OAMPDU message types.

SYNTAX

clear efm oam counters [*interface-list*]

interface-list - *unit/port*

unit - Unit identifier. (Range: 1)

port - Port number or list of ports. To enter a list, separate nonconsecutive port identifiers with a comma and no spaces; use a hyphen to designate a range of ports. (Range: 1-28)

COMMAND MODE

Privileged Exec

EXAMPLE

```
Console#clear efm oam counters
Console#
```

RELATED COMMANDS

show efm oam counters interface (1610)

clear efm oam event-log

This command clears all entries from the OAM event log for the specified port.

SYNTAX

clear efm oam event-log [*interface-list*]

unit - Unit identifier. (Range: 1)

port - Port number or list of ports. To enter a list, separate nonconsecutive port identifiers with a comma and no spaces; use a hyphen to designate a range of ports. (Range: 1-28)

COMMAND MODE

Privileged Exec

EXAMPLE

```
Console#clear efm oam event-log
Console#
```

efm oam remote-loopback

This command starts or stops OAM loopback test mode to the attached CPE.

SYNTAX

efm oam remote-loopback {**start** | **stop**} *interface*

start - Starts remote loopback test mode.

stop - Stops remote loopback test mode.

interface - *unit/port*

unit - Unit identifier. (Range: 1)

port - Port number. (Range: 1-28)

DEFAULT SETTING

None

COMMAND MODE

Privileged Exec

COMMAND USAGE

- OAM remote loop back can be used for fault localization and link performance testing. Statistics from both the local and remote DTE can be queried and compared at any time during loop back testing.

- Use the **efm oam remote-loopback start** command to start OAM remote loop back test mode on the specified port. Afterwards, use the efm oam remote-loopback test command to start sending test packets. Then use the **efm oam remote loopback stop** command to terminate testing (if test packets are still being sent) and to terminate loop back test mode.

- The port that you specify to run this test must be connected to a peer OAM device capable of entering into OAM remote loopback mode. During a remote loopback test, the remote OAM entity loops back every frame except for OAMPDUs and pause frames.

- During loopback testing, both the switch and remote device are permitted to send OAMPDUs to the peer device and to process any OAMPDUs received from the peer.

EXAMPLE

```
Console#efm oam remote-loopback start 1/1
Loopback operation is processing, please wait.
Enter loopback mode succeeded.
Console#
```

efm oam remote-loopback test

This command performs a remote loopback test, sending a specified number of packets.

SYNTAX

efm oam remote-loopback test *interface* [*number-of-packets* [*packet-size*]]

interface - *unit*/*port*

unit - Unit identifier. (Range: 1)

port - Port number. (Range: 1-28)

number-of-packets - Number of packets to send. (Range: 1-99999999)

packet-size - Size of packets to send. (Range: 64-1518 bytes)

DEFAULT SETTING

Number of packets: 10,000

Packet size: 64 bytes

COMMAND MODE

Privileged Exec

COMMAND USAGE

- You can use this command to perform an OAM remote loopback test on the specified port. The port that you specify to run this test must be connected to a peer OAM device capable of entering into OAM remote loopback mode. During a remote loopback test, the remote OAM entity loops back every frame except for OAMPDUs and pause frames.

- OAM remote loopback can be used for fault localization and link performance testing. Statistics from both the local and remote DTE can be queried and compared at any time during loopback testing.

- A summary of the test is displayed after it is finished.

EXAMPLE

```
Console#efm oam remote-loopback test 1/1
Loopback test is processing, press ESC to suspend.
...
Port OAM loopback Tx OAM loopback Rx Loss Rate
---- --------------- --------------- ---------
1/2             1990            1016   48.94 %
Console#
```

show efm oam counters interface

This command displays counters for various OAM PDU message types.

SYNTAX

show efm oam counters interface [*interface-list*]

interface-list - *unit/port*

unit - Unit identifier. (Range: 1)

port - Port number or list of ports. To enter a list, separate nonconsecutive port identifiers with a comma and no spaces; use a hyphen to designate a range of ports. (Range: 1-28)

COMMAND MODE

Normal Exec, Privileged Exec

EXAMPLE

```
Console#show efm oam counters interface 1/1
Port OAMPDU Type           TX         RX
---- --------------------- ---------- ----------
1/1  Information           1121       1444
1/1  Event Notification    0          0
1/1  Loopback Control      1          0
1/1  Organization Specific 76         0
Console#
```

show efm oam event-log interface

This command displays the OAM event log for the specified port(s) or for all ports that have logs.

show efm oam event-log interface [*interface-list*]

interface-list - *unit*/*port*

unit - Unit identifier. (Range: 1)

port - Port number or list of ports. To enter a list, separate nonconsecutive port identifiers with a comma and no spaces; use a hyphen to designate a range of ports. (Range: 1-28)

COMMAND MODE

Normal Exec, Privileged Exec

COMMAND USAGE

- When a link event occurs, no matter whether the location is local or remote, this information is entered in the OAM event log.
- When the log system becomes full, older events are automatically deleted to make room for new entries.

EXAMPLE

```
Console#show efm oam event-log interface 1/1
OAM event log of Eth 1/1:
 00:24:07 2001/01/01
 "Unit 1, Port 1: Dying Gasp at Remote"
Console#
```

This command can show OAM link status changes for link partner as shown in this example.

```
Console#show efm oam event-log interface 1/1
OAM event log of Eth 1/1:
 10:22:55 2013/09/13
 "Unit 1, Port 1: Connection to remote device is up at Local"
 10:22:44 2013/09/13
 "Unit 1, Port 1: Connection to remote device is down at Local"
    <--- When the link is down,this event will be written to OAM event-log
 10:20:02 2013/09/13
 "Unit 1, Port 1: Connection to remote device is up at Local"
    <--- When the link is up,this event will be written to OAM event-log,
Console#clear efm oam event-log
    <--- Use he "clear efm oam event-log” command to clear the event-log.
Console#show efm oam event-log interface 1/1
Console#
```

This command can show OAM dying gasp changes for link partner as shown in this example.

```
Console#show efm oam event-log interface 1/1
   <--- When dying gasp happens and the switch get these packets, it will log
        this event in OAM event-log.
OAM event log of Eth 1/1:
 10:27:21 2013/09/13
 "Unit 1, Port 1: Connection to remote device is down at Local"
 10:27:20 2013/09/13
 "Unit 1, Port 1: Dying Gasp occurred at Remote"
Console#show efm oam event-log interface 1/1
OAM event log of Eth 1/1:
 10:28:31 2013/09/13
 "Unit 1, Port 1: Connection to remote device is up at Local"
 10:28:28 2013/09/13
 "Unit 1, Port 1: Dying Gasp clear occurred at Remote"
   <--- When the remote device comes up, the switch will get OAM packets
        without the dying gasp bit and display "dying gasp event clear".
Console#
```

show efm oam remote-loopback interface

This command displays the results of an OAM remote loopback test.

SYNTAX

show efm oam remote-loopback interface [*interface-list*]

interface-list - *unit*/*port*

unit - Unit identifier. (Range: 1)

port - Port number or list of ports. To enter a list, separate nonconsecutive port identifiers with a comma and no spaces; use a hyphen to designate a range of ports. (Range: 1-28)

COMMAND MODE

Normal Exec, Privileged Exec

EXAMPLE

```
Console#show efm oam remote-loopback interface 1/1
Port OAM loopback Tx OAM loopback Rx Loss Rate
---- --------------- --------------- ---------
1/1            10000           9999    0.01 %
Console#
```

show efm oam status interface

This command displays OAM configuration settings and event counters.

SYNTAX

show efm oam status interface [*interface-list*] [**brief**]

interface - *unit*/*port*

unit - Unit identifier. (Range: 1)

port - Port number or list of ports. To enter a list, separate nonconsecutive port identifiers with a comma and no spaces; use a hyphen to designate a range of ports. (Range: 1-28)

brief - Displays a brief list of OAM configuration states.

COMMAND MODE

Normal Exec, Privileged Exec

EXAMPLE

```
Console#show efm oam status interface 1/1
OAM information of Eth 1/1:
 Basic Information:
  Admin State                     : Enabled
  Operation State                 : Operational
  Mode                            : Active
  Remote Loopback                 : Disabled
  Remote Loopback Status          : No loopback
  Dying Gasp                      : Enabled
  Critical Event                  : Enabled
  Link Monitor (Errored Frame)    : Enabled
 Link Monitor:
  Errored Frame Window (100msec) : 10
  Errored Frame Threshold        : 1
Console#show efm oam status interface 1/1 brief
$ = local OAM in loopback
* = remote OAM in loopback

Port Admin   Mode    Remote   Dying   Critical Errored
     State           Loopback Gasp    Event    Frame
---- ------- ------- -------- ------- -------- -------
1/1  Enabled Active  Disabled Enabled Enabled  Enabled
Console#
```

show efm oam status remote interface

This command displays information about attached OAM-enabled devices.

SYNTAX

show efm oam status remote interface [*interface-list*]

interface-list - *unit*/*port*

unit - Unit identifier. (Range: 1)

port - Port number or list of ports. To enter a list, separate nonconsecutive port identifiers with a comma and no spaces; use a hyphen to designate a range of ports. (Range: 1-28)

COMMAND MODE

Normal Exec, Privileged Exec

EXAMPLE

```
Console#show efm oam status remote interface 1/1
Port MAC Address       OUI    Remote   Unidirectional Link    MIB Variable
                              Loopback                Monitor Retrieval
---- ----------------- ------ -------- -------------- ------- ------------
1/1  00-12-CF-6A-07-F6 000084 Enabled  Disabled       Enabled Disabled
Console#
```

47 DOMAIN NAME SERVICE COMMANDS

These commands are used to configure Domain Naming System (DNS) services. Entries can be manually configured in the DNS domain name to IP address mapping table, default domain names configured, or one or more name servers specified to use for domain name to address translation.

Note that domain name services will not be enabled until at least one name server is specified with the ip name-server command and domain lookup is enabled with the ip domain-lookup command.

Table 224: Address Table Commands

Command	Function	Mode
ip domain-list	Defines a list of default domain names for incomplete host names	GC
ip domain-lookup	Enables DNS-based host name-to-address translation	GC
ip domain-name	Defines a default domain name for incomplete host names	GC
ip host	Creates a static IPv4 host name-to-address mapping	GC
ip name-server	Specifies the address of one or more name servers to use for host name-to-address translation	GC
ipv6 host	Creates a static IPv6 host name-to-address mapping	GC
clear dns cache	Clears all entries from the DNS cache	PE
clear host	Deletes entries from the host name-to-address table	PE
show dns	Displays the configuration for DNS services	PE
show dns cache	Displays entries in the DNS cache	PE
show hosts	Displays the static host name-to-address mapping table	PE

ip domain-list

This command defines a list of 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). Use the **no** form to remove a name from this list.

SYNTAX

[**no**] **ip domain-list** *name*

name - Name of the host. Do not include the initial dot that separates the host name from the domain name. (Range: 1-127 characters)

DEFAULT SETTING

None

Command Mode

Global Configuration

Command Usage

- Domain names are added to the end of the list one at a time.
- When an incomplete host name is received by the DNS service on this switch, it will work through the domain list, appending each domain name in the list to the host name, and checking with the specified name servers for a match.
- If there is no domain list, the domain name specified with the ip domain-name command is used. If there is a domain list, the default domain name is not used.

Example

This example adds two domain names to the current list and then displays the list.

```
Console(config)#ip domain-list sample.com.jp
Console(config)#ip domain-list sample.com.uk
Console(config)#end
Console#show dns
Domain Lookup Status:
    DNS Disabled
Default Domain Name:
    sample.com
Domain Name List:
    sample.com.jp
    sample.com.uk
Name Server List:
Console#
```

Related Commands

ip domain-name (1617)

ip domain-lookup

This command enables DNS host name-to-address translation. Use the **no** form to disable DNS.

Syntax

[**no**] **ip domain-lookup**

Default Setting

Disabled

Command Mode

Global Configuration

Command Usage

- At least one name server must be specified before DNS can be enabled.

- If all name servers are deleted, DNS will automatically be disabled.

EXAMPLE

This example enables DNS and then displays the configuration.

```
Console(config)#ip domain-lookup
Console(config)#end
Console#show dns
Domain Lookup Status:
    DNS Enabled
Default Domain Name:
    sample.com
Domain Name List:
    sample.com.jp
    sample.com.uk
Name Server List:
    192.168.1.55
    10.1.0.55
Console#
```

RELATED COMMANDS

ip domain-name (1617)
ip name-server (1619)

ip domain-name

This command defines the default domain name appended to incomplete host names (i.e., host names passed from a client that are not formatted with dotted notation). Use the **no** form to remove the current domain name.

SYNTAX

ip domain-name *name*

no ip domain-name

name - Name of the host. Do not include the initial dot that separates the host name from the domain name.
(Range: 1-127 characters)

DEFAULT SETTING

None

COMMAND MODE

Global Configuration

EXAMPLE

```
Console(config)#ip domain-name sample.com
Console(config)#end
Console#show dns
Domain Lookup Status:
    DNS Disabled
Default Domain Name:
    sample.com
```

```
Domain Name List:
Name Server List:
Console#
```

RELATED COMMANDS

ip domain-list (1615)
ip name-server (1619)
ip domain-lookup (1616)

ip host

This command creates a static entry in the DNS table that maps a host name to an IPv4 address. Use the **no** form to remove an entry.

SYNTAX

[**no**] **ip host** *name address*

name - Name of an IPv4 host. (Range: 1-100 characters)

address - Corresponding IPv4 address.

DEFAULT SETTING

No static entries

COMMAND MODE

Global Configuration

COMMAND USAGE

Use the **no ip host** command to clear static entries, or the clear host command to clear dynamic entries.

EXAMPLE

This example maps an IPv4 address to a host name.

```
Console(config)#ip host rd5 192.168.1.55
Console(config)#end
Console#show hosts
No.  Flag Type    IP Address           TTL   Domain
---- ---- ------- -------------------- ----- ------------------------------
   0    2 Address 192.168.1.55               rd5
Console#
```

ip name-server

This command specifies the address of one or more domain name servers to use for name-to-address resolution. Use the **no** form to remove a name server from this list.

SYNTAX

[**no**] **ip name-server** *server-address1* [*server-address2* … *server-address6*]

server-address1 - IPv4 or IPv6 address of domain-name server.

server-address2 … *server-address6* - IPv4 or IPv6 address of additional domain-name servers.

DEFAULT SETTING

None

COMMAND MODE

Global Configuration

COMMAND USAGE

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.

EXAMPLE

This example adds two domain-name servers to the list and then displays the list.

```
Console(config)#ip name-server 192.168.1.55 10.1.0.55
Console(config)#end
Console#show dns
Domain Lookup Status:
    DNS disabled
Default Domain Name:
    sample.com
Domain Name List:
    sample.com.jp
    sample.com.uk
Name Server List:
    192.168.1.55
    10.1.0.55
Console#
```

RELATED COMMANDS

ip domain-name (1617)
ip domain-lookup (1616)

ipv6 host

This command creates a static entry in the DNS table that maps a host name to an IPv6 address. Use the **no** form to remove an entry.

SYNTAX

[**no**] **ipv6 host** *name ipv6-address*

name - Name of an IPv6 host. (Range: 1-100 characters)

ipv6-address - Corresponding IPv6 address. This address must be entered according to RFC 2373 “IPv6 Addressing Architecture,” using 8 colon-separated 16-bit hexadecimal values. One double colon may be used in the address to indicate the appropriate number of zeros required to fill the undefined fields.

DEFAULT SETTING

No static entries

COMMAND MODE

Global Configuration

EXAMPLE

This example maps an IPv6 address to a host name.

```
Console(config)#ipv6 host rd6 2001:0db8:1::12
Console(config)#end
Console#show hosts
No.  Flag Type    IP Address           TTL   Domain
---- ---- ------- -------------------- ----- -------------------------------
   0    2 Address 192.168.1.55               rd5
   1    2 Address 2001:DB8:1::12             rd6
Console#
```

clear dns cache

This command clears all entries in the DNS cache.

COMMAND MODE

Privileged Exec

EXAMPLE

```
Console#clear dns cache
Console#show dns cache
No.     Flag    Type    IP Address      TTL     Domain
------- ------- ------- --------------- ------- --------
Console#
```

clear host

This command deletes dynamic entries from the DNS table.

Syntax

clear host {*name* | *}

name - Name of the host. (Range: 1-100 characters)

* - Removes all entries.

Default Setting

None

Command Mode

Privileged Exec

Command Usage

Use the **clear host** command to clear dynamic entries, or the no ip host command to clear static entries.

Example

This example clears all dynamic entries from the DNS table.

```
Console(config)#clear host *
Console(config)#
```

show dns

This command displays the configuration of the DNS service.

Command Mode

Privileged Exec

Example

```
Console#show dns
Domain Lookup Status:
    DNS enabled
Default Domain Name:
    sample.com
Domain Name List:
    sample.com.jp
    sample.com.uk
Name Server List:
    192.168.1.55
    10.1.0.55
Console#
```

show dns cache

This command displays entries in the DNS cache.

COMMAND MODE

Privileged Exec

EXAMPLE

```
Console#show dns cache
No.     Flag    Type    IP Address      TTL     Host
------- ------- ------- --------------- ------- --------
      3       4 Host    209.131.36.158      115 www-real.wa1.b.yahoo.com
      4       4 CNAME   POINTER TO:3        115 www.yahoo.com
      5       4 CNAME   POINTER TO:3        115 www.wa1.b.yahoo.com
Console#
```

Table 225: show dns cache - display description

Field	Description
No.	The entry number for each resource record.
Flag	The flag is always "4" indicating a cache entry and therefore unreliable.
Type	This field includes "Host" which specifies the primary name for the owner, and "CNAME" which specifies multiple domain names (or aliases) which are mapped to the same IP address as an existing entry.
IP Address	The IP address associated with this record.
TTL	The time to live reported by the name server.
Host	The host name associated with this record.

show hosts

This command displays the static host name-to-address mapping table.

COMMAND MODE

Privileged Exec

EXAMPLE

Note that a host name will be displayed as an alias if it is mapped to the same address(es) as a previously configured entry.

```
Console#show hosts
No.  Flag Type    IP Address           TTL   Domain
---- ---- ------- -------------------- ----- -------------------------------
   0    2 Address 192.168.1.55               rd5
   1    2 Address 2001:DB8:1::12             rd6
   3    4 Address 209.131.36.158          65 www-real.wa1.b.yahoo.com
   4    4 CNAME   POINTER TO:3            65 www.yahoo.com
   5    4 CNAME   POINTER TO:3            65 www.wa1.b.yahoo.com
Console#
```

Table 226: show hosts - display description

Field	Description
No.	The entry number for each resource record.
Flag	The field displays “2” for a static entry, or “4” for a dynamic entry stored in the cache.
Type	This field includes “Address” which specifies the primary name for the owner, and “CNAME” which specifies multiple domain names (or aliases) which are mapped to the same IP address as an existing entry.
IP Address	The IP address associated with this record.
TTL	The time to live reported by the name server. This field is always blank for static entries.
Domain	The domain name associated with this record.

48 DHCP COMMANDS

These commands are used to configure Dynamic Host Configuration Protocol (DHCP) client, relay, and server functions. Any VLAN interface on this switch can be configured to automatically obtain an IPv4 address through DHCP. This switch can also be configured to relay DHCP client configuration requests to a DHCP server on another network, or it can be configured to provide DHCP service directly to any client.

Table 227: DHCP Commands

Command Group	Function
DHCP Client	Allows interfaces to dynamically acquire IPv4 address information
DHCP Relay	Relays DHCP requests from local hosts to a remote DHCP server
DHCP Server	Configures DHCP service using address pools or static bindings

DHCP CLIENT

Use the commands in this section to allow the switch's VLAN interfaces to dynamically acquire IP address information.

Table 228: DHCP Client Commands

Command	Function	Mode
DHCP for IPv4		
ip dhcp client class-id	Specifies the DHCP client identifier for an interface	IC
ip dhcp restart client	Submits a BOOTP or DHCP client request	PE
DHCP for IPv6		
ipv6 dhcp client rapid-commit vlan	Specifies the Rapid Commit option for DHCPv6 message exchange	GC

DHCP for IPv4

ip dhcp client class-id

This command specifies the DCHP client vendor class identifier for the current interface. Use the **no** form to remove the class identifier option from the DHCP packet.

SYNTAX

ip dhcp client class-id [**text** *text* | **hex** *hex*]

no ip dhcp client class-id

text - A text string. (Range: 1-32 characters) *hex* - A hexadecimal value. (Range: 1-64 characters)

DEFAULT SETTING

Class identifier option enabled, with the name ECS4660-28F

COMMAND MODE

Interface Configuration (VLAN)

COMMAND USAGE

- Use this command without any keyword to restore the default setting.
- This command is used to identify the vendor class and configuration of the switch to the DHCP server, which then uses this information to decide on how to service the client or the type of information to return.
- The general framework for this DHCP option is set out in RFC 2132 (Option 60). This information is used to convey configuration settings or other identification information about a client, but the specific string to use should be supplied by your service provider or network administrator. Options 60, 66 and 67 statements can be added to the server daemon's configuration file.

Table 229: Options 60, 66 and 67 Statements

Option	Statement	
	Keyword	Parameter
60	vendor-class-identifier	a string indicating the vendor class identifier
66	tftp-server-name	a string indicating the tftp server name
67	bootfile-name	a string indicating the bootfile name

- By default, DHCP option 66/67 parameters are not carried in a DHCP server reply. To ask for a DHCP reply with option 66/67 information, the DHCP client request sent by this switch includes a "parameter request list" asking for this information. Besides, the client request also includes a "vendor class identifier" set by the **ip dhcp client class-id** command that allows the DHCP server to identify the device, and select the appropriate configuration file for download. This information is included in Option 55 and 124.

Table 230: Options 55 and 124 Statements

Option	Statement	
	Keyword	Parameter
55	dhcp-parameter-request-list	a list of parameters, separated by ','
124	vendor-class-identifier	a string indicating the vendor class identifier

- The server should reply with the TFTP server name and boot file name.

- Note that the vendor class identifier can be formatted in either text or hexadecimal using the **ip dhcp client class-id** command, but the format used by both the client and server must be the same.

EXAMPLE

```
Console(config)#interface vlan 2
Console(config-if)#ip dhcp client class-id hex 0000e8666572
Console(config-if)#
```

RELATED COMMANDS

ip dhcp restart client (1627)

ip dhcp restart client

This command submits a BOOTP or DHCP client request.

DEFAULT SETTING

None

COMMAND MODE

Privileged Exec

COMMAND USAGE

- This command issues a BOOTP or DHCP client request for any IP interface that has been set to BOOTP or DHCP mode through 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.

EXAMPLE

In the following example, the device is reassigned the same address.

```
Console(config)#interface vlan 1
Console(config-if)#ip address dhcp
Console(config-if)#exit
Console#ip dhcp restart client
Console#show ip interface
VLAN 1 is Administrative Up - Link Up
  Address is 12-34-12-34-12-34
  Index: 1001, MTU: 1500
  Address Mode is DHCP
  IP Address: 192.168.0.9 Mask: 255.255.255.0
  Proxy ARP is disabled
Console#
```

RELATED COMMANDS

ip address (1648)

DHCP for IPv6

ipv6 dhcp client rapid-commit vlan

This command specifies the Rapid Commit option for DHCPv6 message exchange for all DHCPv6 client requests submitted from the specified interface. Use the **no** form to disable this option.

SYNTAX

[**no**] **ipv6 dhcp client rapid-commit vlan** *vlan-id*

vlan-id - VLAN ID, specified as a single number, a range of consecutive numbers separated by a hyphen, or multiple numbers separated by commas. (Range: 1-4094; Maximum command length: 300 characters)

DEFAULT SETTING

Disabled

COMMAND MODE

Global Configuration

COMMAND USAGE

- DHCPv6 clients can obtain configuration parameters from a server through a normal four-message exchange (solicit, advertise, request, reply), or through a rapid two-message exchange (solicit, reply). The rapid-commit option must be enabled on both client and server for the two-message exchange to be used.

- This command allows two-message exchange method for prefix delegation. When enabled, DCHPv6 client requests submitted from the specified interface will include the rapid commit option in all solicit messages.

- If the rapid commit option has been enabled on the switch with this command, and on the DHCPv6 server, message exchange can be reduced from the normal four step process to a two-step exchange of only solicit and reply messages.

EXAMPLE

```
Console(config)#ipv6 dhcp client rapid-commit vlan 2
Console(config)#
```

DHCP RELAY

This section describes commands used to configure DHCP relay functions for host devices attached to the switch.

Table 231: DHCP Relay Commands

Command	Function	Mode
DHCP Relay for IPv4		
ip dhcp relay server	Specifies DHCP server addresses for relay	IC
ip dhcp restart relay	Enables DHCP relay agent	PE
DHCP Relay for IPv6		
ipv6 dhcp relay destination	Specifies destination address or VLAN to which client messages are forwarded for relay service	IC
show ipv6 dhcp relay destination	Shows destination addresses or VLAN to which client messages are forwarded for relay service	PE

DHCP Relay for IPv4

ip dhcp relay server

This command specifies the DHCP server or relay server addresses to be used by the switch's DHCP relay agent. Use the **no** form to clear all addresses.

SYNTAX

ip dhcp relay server *address1* [*address2* [*address3* ...]]

no ip dhcp relay server

address - IP address of DHCP server. (Range: 1-5 addresses)

DEFAULT SETTING

None

COMMAND MODE

Interface Configuration (VLAN)

USAGE GUIDELINES

- DHCP relay service applies to DHCP client requests received on the specified VLAN.

- This command is used to configure DHCP relay for host devices attached to the switch. If DHCP relay service is enabled, and this switch sees a DHCP client request, it inserts its own IP address into the request so that the DHCP server will know the subnet where the client is located. Then, the switch forwards the packet to a DHCP server on another network. When the server receives the DHCP request, it allocates a free IP address for the DHCP client from its defined scope for the DHCP client's subnet, and sends a DHCP response back to the DHCP relay agent (i.e., this switch). This switch then passes the DHCP response received from the server to the client.

- You must specify the IP address for at least one active DHCP server. Otherwise, the switch's DHCP relay agent will not be able to forward client requests to a DHCP server. Up to five DHCP servers can be specified in order of preference.

- If any of the specified DHCP server addresses are not located in the same network segment with this switch, use the ip default-gateway or ipv6 default-gateway command to specify the default router through which this switch can reach other IP subnetworks.

- To start DHCP relay service, enter the ip dhcp restart relay command.

EXAMPLE

```
Console(config)#interface vlan 1
Console(config-if)#ip dhcp relay server 10.1.0.99
Console(config-if)#
```

ip dhcp restart relay

This command enables DHCP relay for the specified VLAN. Use the **no** form to disable it.

DEFAULT SETTING

Disabled

COMMAND MODE

Privileged Exec

COMMAND USAGE

This command is used to configure DHCP relay functions for host devices attached to the switch. If DHCP relay service is enabled, and this switch sees a DHCP request broadcast, it inserts its own IP address into the request so the DHCP server will know the subnet where the client is located. Then, the switch forwards the packet to the DHCP server on another network. When the server receives the DHCP request, it allocates a free IP address for the DHCP client from its defined scope for the DHCP client's subnet, and sends a DHCP response back to the DHCP relay agent (i.e., this switch). This switch then broadcasts the DHCP response received from the server to the client.

EXAMPLE

In the following example, the device is reassigned the same address.

```
Console#ip dhcp restart relay
Console#show ip interface
VLAN 1 is Administrative Up - Link Up
  Address is 00-00-0C-00-00-FD
  Index: 1001, MTU: 1500
  Address Mode is DHCP
  IP Address: 192.168.0.3 Mask: 255.255.255.0
  Proxy ARP is disabled
Console#
```

RELATED COMMANDS

ip dhcp relay server (1629)

DHCP Relay for IPv6

ipv6 dhcp relay destination

This command specifies the destination address or VLAN to which client messages are forwarded for DHCP service. Use the **no** form to remove an entry.

SYNTAX

[**no**] **ipv6 dhcp relay destination** {*ipv6-address* | **multicast** {**all** | **vlan** *vlan-id*}}

ipv6-address - A full IPv6 address including the network prefix and host address bits. This address may designate another relay server or a DHCPv6 server.

multicast - All DHCP server multicast address (FF:05::1:3).

all - All configured VLANs.

vlan-id - ID of configured VLAN. (Range: 1-4094)

DEFAULT SETTING

None

COMMAND MODE

Interface Configuration (VLAN)

USAGE GUIDELINES

- This command is used to configure DHCPv6 relay functions for host devices attached to the switch. If DHCPv6 relay service is enabled, and this switch sees a DHCPv6 request broadcast, it inserts its own IP address into the request so the DHCPv6 server will know the subnet where the client is located. Then, the switch forwards the packet to the next relay agent or DHCPv6 server on another network. When the server receives the DHCPv6 request, it allocates a free IP address for the DHCPv6 client from its defined scope for the DHCPv6 client’s subnet, and sends a DHCPv6 response back to the DHCPv6 relay agent (i.e., this switch). This switch then broadcasts the DHCPv6 response received from the server to the client.

- When the multicast option is used, the switch multicasts the modified client request to all configured VLANs or to a specified VLAN, and enables DHCPv6 relay service for those VLANs.

- Up to five relay destinations may be configured by repeating this command.

- When issuing the **no ipv6 dhcp relay destination** command without any arguments, the switch will delete all configured destination addresses and disable DHCP for IPv6 relay for all VLANs.

EXAMPLE

```
Console(config)#interface vlan 1
Console(config-if)#ipv6 dhcp relay destination 2001:0DB8:3000:3000::42
Console(config-if)#
```

show ipv6 dhcp relay destination

This command shows the destination addresses or VLAN to which client messages are forwarded for DHCP relay service.

SYNTAX

show ipv6 dhcp relay destination interface [**vlan** *vlan-id*]

vlan-id - ID of configured VLAN. (Range: 1-4094, no leading zeroes)

COMMAND MODE

Privileged Exec

EXAMPLE

```
Console#show ipv6 dhcp relay destination interface vlan 1
DHCP relay destination :
VLAN 1 :
  Unicast    : 2001:DB8:3000:3000::42
Console#
```

DHCP SERVER

This section describes commands used to configure client address pools for the DHCP service.

Table 232: DHCP Server Commands

Command	Function	Mode
ip dhcp excluded-address	Specifies IP addresses that a DHCP server should not assign to DHCP clients	GC
ip dhcp pool	Configures a DHCP address pool on a DHCP Server	GC
service dhcp	Enables the DHCP server feature on this switch	GC
bootfile	Specifies a default boot image for a DHCP client	DC
client-identifier*	Specifies a client identifier for a DHCP client	DC
default-router	Specifies the default router list for a DHCP client	DC
dns-server	Specifies the Domain Name Server (DNS) servers available to a DHCP client	DC
domain-name	Specifies the domain name for a DHCP client	DC
hardware-address*	Specifies the hardware address of a DHCP client	DC
host*	Specifies the IP address and network mask to manually bind to a DHCP client	DC

Table 232: DHCP Server Commands (Continued)

Command	Function	Mode
lease	Sets the duration an IP address is assigned to a DHCP client	DC
netbios-name-server	Configures NetBIOS Windows Internet Naming Service (WINS) name servers available to Microsoft DHCP clients	DC
netbios-node-type	Configures NetBIOS node type for Microsoft DHCP clients	DC
network	Configures the subnet number and mask for a DHCP address pool	DC
next-server	Configures the next server in the boot process of a DHCP client	DC
clear ip dhcp binding	Deletes an automatic address binding from the DHCP server database	PE
show ip dhcp	Displays brief list of DHCP address pools	PE
show ip dhcp binding	Displays address bindings on the DHCP server	PE
show ip dhcp pool	Displays configuration settings for DHCP address pools	PE

* These commands are used for manually binding an address to a client.

ip dhcp excluded-address

This command specifies IP addresses that the DHCP server should not assign to DHCP clients. Use the **no** form to remove the excluded IP addresses.

SYNTAX

[**no**] **ip dhcp excluded-address** *low-address* [*high-address*]

low-address - An excluded IP address, or the first IP address in an excluded address range.

high-address - The last IP address in an excluded address range.

DEFAULT SETTING

All IP pool addresses may be assigned.

COMMAND MODE

Global Configuration

EXAMPLE

```
Console(config)#ip dhcp excluded-address 10.1.0.19
Console(config)#
```

ip dhcp pool

This command configures a DHCP address pool and enter DHCP Pool Configuration mode. Use the **no** form to remove the address pool.

SYNTAX

[**no**] **ip dhcp pool** *name*

name - A string or integer. (Range: 1-8 characters)

DEFAULT SETTING

DHCP address pools are not configured.

COMMAND MODE

Global Configuration

USAGE GUIDELINES

- After executing this command, the switch changes to DHCP Pool Configuration mode, identified by the (config-dhcp)# prompt.
- From this mode, first configure address pools for the network interfaces (using the network command). You can also manually bind an address to a specific client (with the host command) if required. You can configure up to 8 network address pools, and up to 32 manually bound host address pools (i.e., listing one host address per pool). However, note that any address specified in a host command must fall within the range of a configured network address pool.

EXAMPLE

```
Console(config)#ip dhcp pool R&D
Console(config-dhcp)#
```

RELATED COMMANDS

network (1641)
host (1638)

service dhcp

This command enables the DHCP server on this switch. Use the **no** form to disable the DHCP server.

SYNTAX

[**no**] **service dhcp**

DEFAULT SETTING

Enabled

COMMAND MODE

Global Configuration

COMMAND USAGE

If the DHCP server is running, you must restart it to implement any configuration changes.

EXAMPLE

```
Console(config)#service dhcp
Console(config)#
```

bootfile

This command specifies the name of the default boot image for a DHCP client. This file should placed on the Trivial File Transfer Protocol (TFTP) server specified with the next-server command. Use the **no** form to delete the boot image name.

SYNTAX

bootfile *filename*

no bootfile

filename - Name of the file that is used as a default boot image.

DEFAULT SETTING

None

COMMAND MODE

DHCP Pool Configuration

EXAMPLE

```
Console(config-dhcp)#bootfile wme.bat
Console(config-dhcp)#
```

RELATED COMMANDS

next-server (1642)

client-identifier

This command specifies the client identifier of a DHCP client. Use the **no** form to remove the client identifier.

SYNTAX

client-identifier {**text** *text* | **hex** *hex*}

no client-identifier

text - A text string. (Range: 1-15 characters)

hex - The hexadecimal value.

DEFAULT SETTING

None

COMMAND MODE

DHCP Pool Configuration

COMMAND USAGE

- This command identifies a DHCP client to bind to an address specified in the host command. If both a client identifier and hardware address are configured for a host address, the client identifier takes precedence over the hardware address in the search procedure.
- BOOTP clients cannot transmit a client identifier. To bind an address to a BOOTP client, you must associate a hardware address with the host entry.

EXAMPLE

```
Console(config-dhcp)#client-identifier text steve
Console(config-dhcp)#
```

RELATED COMMANDS

host (1638)

default-router

This command specifies default routers for a DHCP pool. Use the **no** form to remove the default routers.

SYNTAX

default-router *address1* [*address2*]

no default-router

address1 - Specifies the IP address of the primary router.

address2 - Specifies the IP address of an alternate router.

DEFAULT SETTING

None

COMMAND MODE

DHCP Pool Configuration

USAGE GUIDELINES

The IP address of the router should be on the same subnet as the client. You can specify up to two routers. Routers are listed in order of preference (starting with *address1* as the most preferred router).

EXAMPLE

```
Console(config-dhcp)#default-router 10.1.0.54 10.1.0.64
Console(config-dhcp)#
```

dns-server

This command specifies the Domain Name System (DNS) IP servers available to a DHCP client. Use the **no** form to remove the DNS server list.

SYNTAX

dns-server *address1* [*address2*]

no dns-server

address1 - Specifies the IP address of the primary DNS server.

address2 - Specifies the IP address of the alternate DNS server.

DEFAULT SETTING

None

COMMAND MODE

DHCP Pool Configuration

USAGE GUIDELINES

- If DNS IP servers are not configured for a DHCP client, the client cannot correlate host names to IP addresses.

- Servers are listed in order of preference (starting with *address1* as the most preferred server).

EXAMPLE

```
Console(config-dhcp)#dns-server 10.1.1.253 192.168.3.19
Console(config-dhcp)#
```

domain-name

This command specifies the domain name for a DHCP client. Use the **no** form to remove the domain name.

SYNTAX

domain-name *domain*

no domain-name

domain - Specifies the domain name of the client.
(Range: 1-32 characters)

DEFAULT SETTING

None

COMMAND MODE

DHCP Pool Configuration

EXAMPLE

```
Console(config-dhcp)#domain-name sample.com
Console(config-dhcp)#
```

hardware-address

This command specifies the hardware address of a DHCP client. This command is valid for manual bindings only. Use the **no** form to remove the hardware address.

SYNTAX

hardware-address *hardware-address type*

no hardware-address

hardware-address - Specifies the MAC address of the client device.

type - Indicates the following protocol used on the client device:

- ethernet
- ieee802
- fddi

DEFAULT SETTING

If no type is specified, the default protocol is Ethernet.

COMMAND MODE

DHCP Pool Configuration

COMMAND USAGE

This command identifies a DHCP or BOOTP client to bind to an address specified in the host command. BOOTP clients cannot transmit a client identifier. To bind an address to a BOOTP client, you must associate a hardware address with the host entry.

EXAMPLE

```
Console(config-dhcp)#hardware-address 00-e0-29-94-34-28 ethernet
Console(config-dhcp)#
```

RELATED COMMANDS

host (1638)

host

Use this command to specify the IP address and network mask to manually bind to a DHCP client. Use the **no** form to remove the IP address for the client.

SYNTAX

host *address* [*mask*]

no host

address - Specifies the IP address of a client.

mask - Specifies the network mask of the client.

DEFAULT SETTING

None

COMMAND MODE

DHCP Pool Configuration

USAGE GUIDELINES

- Host addresses must fall within the range specified for an existing network pool.
- When a client request is received, the switch first checks for a network address pool matching the gateway where the request originated (i.e., if the request was forwarded by a relay server). If there is no gateway in the client request (i.e., the request was not forwarded by a relay server), the switch searches for a network pool matching the interface through which the client request was received. It then searches for a manually configured host address that falls within the matching network pool.
- When searching for a manual binding, the switch compares the client identifier for DHCP clients, and then compares the hardware address for DHCP or BOOTP clients.
- If no manual binding has been specified for a host entry with the client-identifier or hardware-address commands, then the switch will assign an address from the matching network pool.
- If the mask is unspecified, DHCP examines its address pools. If no mask is found in the pool database, the Class A, B, or C natural mask is used (see page 1641). This command is valid for manual bindings only.
- The **no host** command only clears the address from the DHCP server database. It does not cancel the IP address currently in use by the host.

EXAMPLE

```
Console(config-dhcp)#host 10.1.0.21 255.255.255.0
Console(config-dhcp)#
```

RELATED COMMANDS

client-identifier (1635)
hardware-address (1638)

lease

This command configures the duration that an IP address is assigned to a DHCP client. Use the **no** form to restore the default value.

SYNTAX

lease {*days* [*hours*] [*minutes*] | **infinite**}

no lease

days - Specifies the duration of the lease in numbers of days. (Range: 0-364) *hours* - Specifies the number of hours in the lease. A *days* value must be supplied before you can configure *hours*. (Range: 0-23)

minutes - Specifies the number of minutes in the lease. A *days* and *hours* value must be supplied before you can configure *minutes*. (Range: 0-59)

infinite - Specifies that the lease time is unlimited. This option is normally used for addresses manually bound to a BOOTP client via the **host** command.

DEFAULT SETTING

One day

COMMAND MODES

DHCP Pool Configuration

EXAMPLE

The following example leases an address to clients using this pool for 7 days.

```
Console(config-dhcp)#lease 7
Console(config-dhcp)#
```

netbios-name-server

This command configures NetBIOS Windows Internet Naming Service (WINS) name servers that are available to Microsoft DHCP clients. Use the **no** form to remove the NetBIOS name server list.

SYNTAX

netbios-name-server *address1* [*address2*]

no netbios-name-server

address1 - Specifies IP address of primary NetBIOS WINS name server.

address2 - Specifies IP address of alternate NetBIOS WINS name server.

DEFAULT SETTING

None

COMMAND MODE

DHCP Pool Configuration

USAGE GUIDELINES

Servers are listed in order of preference (starting with *address1* as the most preferred server).

EXAMPLE

```
Console(config-dhcp)#netbios-name-server 10.1.0.33 10.1.0.34
Console(config-dhcp)#
```

RELATED COMMANDS

netbios-node-type (1641)

netbios-node-type

This command configures the NetBIOS node type for Microsoft DHCP clients. Use the **no** form to remove the NetBIOS node type.

SYNTAX

netbios-node-type *type*

no netbios-node-type

type - Specifies the NetBIOS node type:

broadcast

hybrid (recommended)

mixed

peer-to-peer

DEFAULT SETTING

None

COMMAND MODE

DHCP Pool Configuration

EXAMPLE

```
Console(config-dhcp)#netbios-node-type hybrid
Console(config-dhcp)#
```

RELATED COMMANDS

netbios-name-server (1640)

network

This command configures the subnet number and mask for a DHCP address pool. Use the **no** form to remove the subnet number and mask.

SYNTAX

network *network-number* [*mask*]

no network

network-number - The IP address of the DHCP address pool.

mask - The bit combination that identifies the network (or subnet) and the host portion of the DHCP address pool.

COMMAND MODE

DHCP Pool Configuration

USAGE GUIDELINES

- When a client request is received, the switch first checks for a network address pool matching the gateway where the request originated (i.e., if the request was forwarded by a relay server). If there is no gateway in the client request (i.e., the request was not forwarded by a relay server), the switch searches for a network pool matching the interface through which the client request was received. It then searches for a manually configured host address that falls within the matching network pool. If no manually configured host address is found, it assigns an address from the matching network address pool. However, if no matching address pool is found the request is ignored.

- This command is valid for DHCP network address pools only. If the mask is not specified, the class A, B, or C natural mask is used. Subnet addresses are interpreted as class A, B or C, based on the first field in the specified address. In other words, if a subnet address nnn.xxx.xxx.xxx is entered, the first field (nnn) determines the class:

  0 - 127 is class A, only uses the first field in the network address.
  128 - 191 is class B, uses the first two fields in the network address.
  192 - 223 is class C, uses the first three fields in the network address.

- The DHCP server assumes that all host addresses are available. You can exclude subsets of the address space by using the ip dhcp excluded-address command.

EXAMPLE

```
Console(config-dhcp)#network 10.1.0.0 255.255.255.0
Console(config-dhcp)#
```

next-server

This command configures the next server in the boot process of a DHCP client. Use the **no** form to remove the boot server list.

SYNTAX

[**no**] **next-server** *address*

address - Specifies the IP address of the next server in the boot process, which is typically a Trivial File Transfer Protocol (TFTP) server.

DEFAULT SETTING

None

COMMAND MODE

DHCP Pool Configuration

EXAMPLE

```
Console(config-dhcp)#next-server 10.1.0.21
Console(config-dhcp)#
```

RELATED COMMANDS

bootfile (1635)

clear ip dhcp binding

This command deletes an automatic address binding from the DHCP server database.

SYNTAX

clear ip dhcp binding {*address* | *****}

address - The address of the binding to clear.

***** - Clears all automatic bindings.

DEFAULT SETTING

None

COMMAND MODE

Privileged Exec

USAGE GUIDELINES

- An *address* specifies the client’s IP address. If an asterisk (*) is used as the address parameter, the DHCP server clears all automatic bindings.
- Use the no host command to delete a manual binding.
- This command is normally used after modifying the address pool, or after moving DHCP service to another device.

EXAMPLE.

```
Console#clear ip dhcp binding *
Console#
```

RELATED COMMANDS

show ip dhcp binding (1644)

show ip dhcp

This command displays a brief list of DHCP address pools configured on the switch.

COMMAND MODE

Privileged Exec

EXAMPLE

```
Console#show ip dhcp

  Name   Type   IP Address         Mask                Active Pool
-------- ---- --------------- --------------- -------------------------------
tps      Net  192.168.1.0     255.255.255.0   192.168.1.1     - 192.168.1.254

Total entry : 1
Console#
```

show ip dhcp binding

This command displays address bindings on the DHCP server.

SYNTAX

show ip dhcp binding [*address*]

address - Specifies the IP address of the DHCP client for which bindings will be displayed.

DEFAULT SETTING

None

COMMAND MODE

Privileged Exec

EXAMPLE

```
Console#show ip dhcp binding

     IP                MAC           Lease Time        Start
                                    (dd/hh/mm/ss)
--------------- ----------------- ------------------ -----------
     192.1.3.21 00-00-e8-98-73-21              86400 Dec 25 08:01:57 2002
Console#
```

show ip dhcp pool

This command displays configuration settings for DHCP address pools.

SYNTAX

show ip dhcp pool [**host** | **network**]

host - Shows detailed settings for host device pools.

network - Shows detailed settings for network pools.

DEFAULT SETTING

None

COMMAND MODE

Privileged Exec

EXAMPLE

```
Console#show ip dhcp pool
Pool name : R&D
Pool type : Network
    Network address        : 192.168.0.1


    Subnet mask            : 255.255.255.0

    Boot file              :
    Client identifier mode : Hex
    Client identifier      :
    Default router         : 0.0.0.0
                             0.0.0.0
    DNS server             : 0.0.0.0
                             0.0.0.0
    Domain name            :
    Hardware type          : None
    Hardware address       : 00-00-00-00-00-00
    Lease time             : infinite
    Netbios name server    : 0.0.0.0
                             0.0.0.0
    Netbios node type      : Hybrid
    Next server            : 0.0.0.0

Console#
```

49 IP Interface Commands

An IP Version 4 and Version 6 address may be used for management access to the switch over the network. Both IPv4 or IPv6 addresses can be used simultaneously to access the switch. You can manually configure a specific IPv4 or IPv6 address or direct the switch to obtain an IPv4 address from a BOOTP or DHCP server when it is powered on. An IPv6 address can either be manually configured or dynamically generated.

An IPv4 address for this switch is obtained via DHCP by default for VLAN 1. You may also need to a establish an IPv4 or IPv6 default gateway between this device and management stations that exist on another network segment.

Table 233: IP Interface Commands

Command Group	Function
IPv4 Interface	Configures an IPv4 address for the switch
IPv6 Interface	Configures an IPv6 address for the switch
IPv6 to IPv4 Tunnels	Configures IPv6 over IPv4 tunnels
ND Snooping	Maintains IPv6 prefix table and user address binding table which can be used for stateless address auto-configuration or for address filtering by IPv6 Source Guard

IPv4 Interface

There are no IP addresses assigned to this switch by default. You must manually configure a new address to manage the switch over your network or to connect the switch to existing IP subnets. You may also need to a establish a default gateway between this device and management stations or other devices that exist on another network segment. (if routing is not enabled).

This section includes commands for configuring IP interfaces, the Address Resolution Protocol (ARP) and Proxy ARP.

Table 234: IPv4 Interface Commands

Command Group	Function
Basic IPv4 Configuration	Configures the IP address for interfaces and the gateway router
ARP Configuration	Configures static, dynamic and proxy ARP service
UDP Helper Configuration	Forwards UDP broadcast packets to a specified server

BASIC IPV4 CONFIGURATION

This section describes commands used to configure IP addresses for VLAN interfaces on the switch.

Table 235: Basic IP Configuration Commands

Command	Function	Mode
ip address	Sets the IP address for the current interface	IC
ip default-gateway	Defines the default gateway through which this switch can reach other subnetworks	GC
show ip interface	Displays the IP settings for this device	PE
show ip route	Displays specified entries in the routing table	PE
show ip traffic	Displays statistics for IP, ICMP, UDP, TCP and ARP protocols	PE
traceroute	Shows the route packets take to the specified host	PE
ping	Sends ICMP echo request packets to another node on the network	NE, PE

ip address

This command sets the IPv4 address for the currently selected VLAN interface. Use the **no** form to restore the default IP address.

SYNTAX

[**no**] **ip address** {*ip-address netmask* [**secondary**] | **bootp** | **dhcp**}

ip-address - IP address

netmask - Network mask for the associated IP subnet. This mask identifies the host address bits used for routing to specific subnets. The network mask use either the traditional format xxx.xxx.xxx.xxx or classless format within the range /5 to /32. For example the subnet 255.255.224.0 would be /19.

secondary - Specifies a secondary IP address.

bootp - Obtains IP address from BOOTP.

dhcp - Obtains IP address from DHCP.

DEFAULT SETTING

DHCP

COMMAND MODE

Interface Configuration (VLAN)

COMMAND USAGE

- If this router is directly connected to end node devices (or connected to end nodes via shared media) that will be assigned to a specific subnet, then you must create a router interface for each VLAN that will support routing. The router interface consists of an IP address and subnet mask. This interface address defines both the network number to which the router interface is attached and the router's host number on that network. In other words, a router interface address defines the network and subnetwork numbers of the segment that is connected to that interface, and allows you to send IP packets to or from the router.

- Before any network interfaces are configured on the router, first create a VLAN for each unique user group, or for each network application and its associated users. Then assign the ports associated with each of these VLANs.

- An IP address must be assigned to this device to gain management access over the network or to connect the router to existing IP subnets. A specific IP address can be manually configured, or the router can be directed to obtain an address from a BOOTP or DHCP server. Valid IP addresses consist of four numbers, 0 to 255, separated by periods. Anything other than this format is not be accepted by the configuration program.

- An interface can have only one primary IP address, but can have many secondary IP addresses. In other words, secondary addresses need to be specified if more than one IP subnet can be accessed through this interface. Note that a secondary address cannot be configured prior to setting the primary IP address, and the primary address cannot be removed if a secondary address is still present. Also, if any router/switch in a network segment uses a secondary address, all other routers/switches in that segment must also use a secondary address from the same network or subnet address space.

- If **bootp** or **dhcp** options are selected, the system will immediately start broadcasting service requests for all VLANs configured to obtain address assignments through BOOTP or DHCP. IP is enabled but will not function until a BOOTP or DHCP reply has been received. Requests are broadcast periodically by the router in an effort to learn its IP address. (BOOTP and DHCP values can include the IP address, default gateway, and subnet mask). If the DHCP/BOOTP server is slow to respond, you may need to use the ip dhcp restart client command to re-start broadcasting service requests, or reboot the router.

NOTE: Each VLAN group can be assigned its own IP interface address. You can manage the router via any of these IP addresses.

EXAMPLE

In the following example, the device is assigned an address in VLAN 1.

```
Console(config)#interface vlan 1
Console(config-if)#ip address 192.168.1.5 255.255.255.0
Console(config-if)#
```

This example assigns an IP address to VLAN 2 using a classless network mask.

```
Console(config)#interface vlan 2
Console(config-if)#ip address ip address 10.2.2.1/24
Console(config-if)#
```

RELATED COMMANDS

ip dhcp restart client (1627)
ip default-gateway (1650)
ipv6 address (1665)

ip default-gateway

This command specifies the default gateway for destinations not found in the local routing tables. Use the **no** form to remove a default gateway.

SYNTAX

ip default-gateway *gateway*

no ip default-gateway

gateway - IP address of the default gateway

DEFAULT SETTING

No default gateway is established.

COMMAND MODE

Global Configuration

COMMAND USAGE

- The default gateway can also be defined using the following Global configuration command: **ip route 0.0.0.0 0.0.0.0** *gateway-address*.

- Static routes can also be defined using the ip route command to ensure that traffic to the designated address or subnet passes through a preferred gateway.

- A default gateway can only be successfully set when a network interface that directly connects to the gateway has been configured on the router.

- The same link-local address may be used by different interfaces/nodes in different zones (RFC 4007). Therefore, when specifying a link-local address for a default gateway, include zone-id information indicating the VLAN identifier after the % delimiter. For example, FE80::7272%1 identifies VLAN 1 as the interface from which the ping is sent.

EXAMPLE

The following example defines a default gateway for this device:

```
Console(config)#ip default-gateway 10.1.1.254
Console(config)#end
Console#show ip route
Codes: C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
      i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default

S*      0.0.0.0/0 [1/0] via 10.1.1.254, VLAN1
C       127.0.0.0/8 is directly connected, lo0
C       192.168.2.0/24 is directly connected, VLAN1

Console#
```

RELATED COMMANDS

ip address (1648)
ip route (1724)
ipv6 default-gateway (1664)

show ip interface

This command displays the settings of an IPv4 interface.

COMMAND MODE

Privileged Exec

EXAMPLE

```
Console#show ip interface
VLAN 1 is Administrative Up - Link Up
  Address is 00-00-0C-00-00-FD
  Index: 1001, MTU: 1500
  Address Mode is DHCP
  IP Address: 192.168.0.3 Mask: 255.255.255.0
  Proxy ARP is disabled
Console#
```

RELATED COMMANDS

ip address (1648)
show ipv6 interface (1672)

show ip traffic

This command displays statistics for IP, ICMP, UDP, TCP and ARP protocols.

COMMAND MODE

Privileged Exec

EXAMPLE

```
Console#show ip traffic
IP Statistics:
IP received
                   3 total received
                     header errors
                     unknown protocols
                     address errors
                     discards
                   3 delivers
                     reassembly request datagrams
                     reassembly succeeded
                     reassembly failed
IP sent
                     forwards datagrams
                   2 requests
                     discards
                     no routes
                     generated fragments
                     fragment succeeded
                     fragment failed
ICMP Statistics:
ICMP received
                     input
                     errors
                     destination unreachable messages
                     time exceeded messages
                     parameter problem message
                     echo request messages
                     echo reply messages
                     redirect messages
                     timestamp request messages
                     timestamp reply messages
                     source quench messages
                     address mask request messages
                     address mask reply messages
ICMP sent
                     output
                     errors
                     destination unreachable messages
                     time exceeded messages
                     parameter problem message
                     echo request messages
                     echo reply messages
                     redirect messages
                     timestamp request messages
                     timestamp reply messages
                     source quench messages
                     address mask request messages
                     address mask reply messages
UDP Statistics:
                     input
                     no port errors
                     other errors
                     output
TCP Statistics:
                   4 input
```

```
                     input errors
                   4 output

Console#
```

traceroute

This command shows the route packets take to the specified destination.

Syntax

traceroute *host*

host - IP address or alias of the host.

Default Setting

None

Command Mode

Privileged Exec

Command Usage

- Use the **traceroute** command to determine the path taken to reach a specified destination.
- A trace terminates when the destination responds, when the maximum timeout (TTL) is exceeded, or the maximum number of hops is exceeded.
- The traceroute command first sends probe datagrams with the TTL value set at one. This causes the first router to discard the datagram and return an error message. The trace function then sends several probe messages at each subsequent TTL level and displays the round-trip time for each message. Not all devices respond correctly to probes by returning an "ICMP port unreachable" message. If the timer goes off before a response is returned, the trace function prints a series of asterisks and the "Request Timed Out" message. A long sequence of these messages, terminating only when the maximum timeout has been reached, may indicate this problem with the target device.
- If the target device does not respond or other errors are detected, the switch will indicate this by one of the following messages:
  - * - No Response
  - H - Host Unreachable
  - N - Network Unreachable
  - P - Protocol Unreachable
  - O -Other

EXAMPLE

```
Console#traceroute 192.168.0.1
Press "ESC" to abort.
Traceroute to 192.168.0.1, 30 hops max, timeout is 3 seconds
Hop Packet 1 Packet 2 Packet 3 IP Address
--- -------- -------- -------- ---------------
  1    10 ms   <10 ms   <10 ms 192.168.0.1

Trace completed.
Console#
```

ping

This command sends (IPv4) ICMP echo request packets to another node on the network.

SYNTAX

ping *host* [**count** *count*] [**size** *size*]

host - IP address or IP alias of the host.

count - Number of packets to send. (Range: 1-16)

size - Number of bytes in a packet. (Range: 32-512)
The actual packet size will be eight bytes larger than the size specified because the router adds header information.

DEFAULT SETTING

count: 5
size: 32 bytes

COMMAND MODE

Normal Exec, Privileged Exec

COMMAND USAGE

- Use the ping command to see if another site on the network can be reached.

- The following are some results of the **ping** command:

  - *Normal response* - The normal response occurs in one to ten seconds, depending on network traffic.

  - *Destination does not respond* - If the host does not respond, a “timeout” appears in ten seconds.

  - *Destination unreachable* - The gateway for this destination indicates that the destination is unreachable.

  - *Network or host unreachable* - The gateway found no corresponding entry in the route table.

- When pinging a host name, be sure the DNS server has been defined (see page 1616) and host name-to-address translation enabled (see page 1616). If necessary, local devices can also be specified in the DNS static host table (see page 1618).

EXAMPLE

```
Console#ping 10.1.0.9
Type ESC to abort.
PING to 10.1.0.9, by 5 32-byte payload ICMP packets, timeout is 5 seconds
response time: 10 ms
response time: 10 ms
response time: 10 ms
response time: 10 ms
response time: 0 ms
Ping statistics for 10.1.0.9:
 5 packets transmitted, 5 packets received (100%), 0 packets lost (0%)
Approximate round trip times:
 Minimum = 0 ms, Maximum = 10 ms, Average = 8 ms
Console#
```

RELATED COMMANDS

interface (1188)

ARP CONFIGURATION

This section describes commands used to configure the Address Resolution Protocol (ARP) on the switch.

Table 236: Address Resolution Protocol Commands

Command	Function	Mode
arp	Adds a static entry in the ARP cache	GC
arp timeout	Sets the time a dynamic entry remains in the ARP cache	GC
ip proxy-arp	Enables proxy ARP service	IC
clear arp-cache	Deletes all dynamic entries from the ARP cache	PE
show arp	Displays entries in the ARP cache	NE, PE

arp

This command adds a static entry in the Address Resolution Protocol (ARP) cache. Use the **no** form to remove an entry from the cache.

SYNTAX

arp *ip-address hardware-address*

no arp *ip-address*

ip-address - IP address to map to a specified hardware address.

hardware-address - Hardware address to map to a specified IP address. (The format for this address is xx-xx-xx-xx-xx-xx.)

DEFAULT SETTING

No default entries

COMMAND MODE

Global Configuration

COMMAND USAGE

- The ARP cache is used to map 32-bit IP addresses into 48-bit hardware (i.e., Media Access Control) addresses. This cache includes entries for hosts and other routers on local network interfaces defined on this router.
- The maximum number of static entries allowed in the ARP cache is 128.
- You may need to enter a static entry in the cache if there is no response to an ARP broadcast message. For example, some applications may not respond to ARP requests or the response arrives too late, causing network operations to time out.
- Static entries will not be aged out nor deleted when power is reset. A static entry can only be removed through the configuration interface.

EXAMPLE

```
Console(config)#arp 10.1.0.19 01-02-03-04-05-06
Console(config)#
```

RELATED COMMANDS

clear arp-cache (1658)
show arp (1658)

arp timeout

This command sets the aging time for dynamic entries in the Address Resolution Protocol (ARP) cache. Use the **no** form to restore the default timeout.

SYNTAX

arp timeout *seconds*

no arp timeout

seconds - The time a dynamic entry remains in the ARP cache. (Range: 300-86400; 86400 seconds is one day)

DEFAULT SETTING

1200 seconds (20 minutes)

COMMAND MODE

Global Configuration

COMMAND USAGE

- When a ARP entry expires, it is deleted from the cache and an ARP request packet is sent to re-establish the MAC address.

- The aging time determines how long dynamic entries remain in the cache. If the timeout is too short, the router may tie up resources by repeating ARP requests for addresses recently flushed from the table.

EXAMPLE

This example sets the ARP cache timeout for 15 minutes (i.e., 900 seconds).

```
Console(config)#arp timeout 900
Console(config)#
```

ip proxy-arp

This command enables proxy Address Resolution Protocol (ARP). Use the **no** form to disable proxy ARP.

SYNTAX

[**no**] **ip proxy-arp**

DEFAULT SETTING

Disabled

COMMAND MODE

Interface Configuration (VLAN)

COMMAND USAGE

- Proxy ARP allows a non-routing device to determine the MAC address of a host on another subnet or network.
- End stations that require Proxy ARP must view the entire network as a single network. These nodes must therefore use a smaller subnet mask than that used by the router or other relevant network devices.
- Extensive use of Proxy ARP can degrade router performance because it may lead to increased ARP traffic and increased search time for larger ARP address tables.

EXAMPLE

```
Console(config)#interface vlan 3
Console(config-if)#ip proxy-arp
Console(config-if)#
```

clear arp-cache

This command deletes all dynamic entries from the Address Resolution Protocol (ARP) cache.

COMMAND MODE

Privileged Exec

EXAMPLE

This example clears all dynamic entries in the ARP cache.

```
Console#clear arp-cache
This operation will delete all the dynamic entries in ARP Cache.
Are you sure to continue this operation (y/n)?y
Console#
```

show arp

This command displays entries in the Address Resolution Protocol (ARP) cache.

COMMAND MODE

Normal Exec, Privileged Exec

COMMAND USAGE

- This command displays information about the ARP cache. The first line shows the cache timeout. It also shows each cache entry, including the IP address, MAC address, type (static, dynamic, other), and VLAN interface. Note that entry type "other" indicates local addresses for this router.
- You can define up to 128 static entries in the ARP cache.
- A static entry may need to be used if there is no response to an ARP broadcast message. For example, some applications may not respond to ARP requests or the response arrives too late, causing network operations to time out.
- Static entries will not be aged out or deleted when power is reset. You can only remove a static entry via the configuration interface.
- Static entries are only displayed for VLANs that are up. In other words, static entries are only displayed when configured for the IP subnet of a existing VLAN, and that VLAN is linked up.

EXAMPLE

This example displays all entries in the ARP cache.

```
Console#show arp
ARP Cache Timeout: 1200 (seconds)

IP Address      MAC Address       Type      Interface
--------------- ----------------- --------- -----------
10.1.0.0        FF-FF-FF-FF-FF-FF other     VLAN1
10.1.0.254      00-00-AB-CD-00-00 other     VLAN1
```

```
10.1.0.255       FF-FF-FF-FF-FF-FF other     VLAN1
145.30.20.23     09-50-40-30-20-10 dynamic   VLAN3

Total entry : 5
Console#
```

UDP Helper Configuration

User Datagram Protocol (UDP) Helper allows host applications to forward UDP broadcast packets from this switch to another part of the network. This section describes the commands used to configure UDP Helper.

Table 237: UDP Helper Commands

Command	Function	Mode
ip forward-protocol udp	Specifies the UDP destination ports for which broadcast traffic will be forwarded	GC
ip helper	Enables UDP helper globally on the switch	GC
ip helper-address	Specifies the servers to which designated UDP protocol packets are forwarded	IC
show ip helper	Displays configuration settings for UDP helper	PE

ip forward-protocol udp

This command specifies the UDP destination ports for which broadcast traffic will be forwarded when the UDP helper is enabled. Use the **no** form to remove a UDP port from the forwarding list.

Syntax

[**no**] **ip forward-protocol udp** *destination-port*

destination-port - UDP application port for which UDP service requests are forwarded. (Range: 1-65535)

Default Setting

The following UDP ports are included in the forwarding list when UDP helper is enabled with the ip helper command and a remote server address is configured with the ip helper-address command:

BOOTP client	port 67
BOOTP server	port 68
Domain Name Service	port 53
IEN-116 Name Service	port 42
NetBIOS Datagram Server	port 138
NetBIOS Name Server	port 137
NTP	port 37
TACACS service	port 49
TFTP	port 69

Command Mode

Global Configuration

COMMAND USAGE

Up to 100 UDP ports can be specified with this command for forwarding to one or more remote servers.

EXAMPLE

This example enables forwarding for DHCPv6 UDP packets.

```
Console(config)#ip forward-protocol udp 547
Console(config)#
```

ip helper

This command enables UDP helper globally on the switch. Use the **no** form to disable this feature.

SYNTAX

[**no**] **ip helper**

DEFAULT SETTING

Disabled

COMMAND MODE

Global Configuration

COMMAND USAGE

- Network hosts occasionally use UDP broadcasts to determine information such as address configuration, and domain name mapping. These broadcasts are confined to the local subnet, either as an all hosts broadcast (all ones broadcast - 255.255.255.255), or a directed subnet broadcast (such as 10.10.10.255). To reduce the number of application servers deployed in a multi-segment network, UDP helper can be used to forward broadcast packets for specified UDP application ports to remote servers located in another network segment.

- To configure UDP helper, it must be enabled globally with the **ip helper** command. The UDP destination ports for which broadcast traffic will be forwarded must be specified with the ip forward-protocol udp command. And the remote servers which are configured to service UDP clients on another network segment specified with the ip helper-address command.

EXAMPLE

This example enables UDP helper globally on the switch.

```
Console(config)#ip helper
Console(config)#
```

ip helper-address

This command specifies the application server or subnet (indicated by a directed broadcast address) to which designated UDP broadcast packets are forwarded. Use the **no** form to remove a UDP helper address.

SYNTAX

[**no**] **ip helper-address** *ip-address*

ip-address - Host address or directed broadcast address to which UDP broadcast packets are forwarded. (Range: 1-65535)

DEFAULT SETTING

None

COMMAND MODE

Interface Configuration (VLAN)

COMMAND USAGE

- Up to 20 helper addresses can be specified with this command.

- To forward UDP packets with the UDP helper, the clients must be connected to the selected interface, and the interface configured with an IP address.

- The UDP packets to be forwarded must be specified by the ip forward-protocol udp command, and the packets meet the following criteria:

  - The MAC address of the received frame must be all-ones broadcast address (ffff.ffff.ffff).

  - The IP destination address must be one of the following:

    - all-ones broadcast (255.255.255.255)
    - subnet broadcast for the receiving interface

  - The IP time-to-live (TTL) value must be at least 2.

  - The IP protocol must be UDP (17).

  - The UDP destination port must be TFTP, Domain Name System (DNS), Time, NetBIOS, BOOTP or DHCP packet, or a UDP port specified by the ip forward-protocol udp command.

- If a helper address is specified with this command, but no UDP ports have been specified with the ip forward-protocol udp command, broadcast traffic for several UDP protocol types will be forwarded by default as described under the ip forward-protocol udp command.

EXAMPLE

This example indicates that designated UDP broadcast packets are to be forwarded to the directed broadcast address of 192.168.2.255.

```
Console(config)#interface vlan 1
Console(config-if)#ip helper-address 192.168.2.255
Console(config-if)#
```

show ip helper

This command displays configuration settings for UDP helper.

COMMAND MODE

Privileged Exec

COMMAND USAGE

This command displays all configuration settings for UDP helper, including its functional status, the UDP ports for which broadcast traffic will be forwarded, and the remote servers or subnets to which the traffic will be forwarded.

EXAMPLE

```
Console#show ip helper
Helper mechanism is enabled
Forward port list(maximum count: 100)
  547
Total port number now is: 1
Helper address list(maximum count: 1024)
Interface VLAN 1:
  192.168.2.255
Total helper number now is: 1
Console#
```

IPv6 Interface

This switch supports the following IPv6 interface commands.

Table 238: IPv6 Configuration Commands

Command	Function	Mode
Interface Address Configuration and Utilities		
ipv6 default-gateway	Sets an IPv6 default gateway for traffic with no known next hop	GC
ipv6 address	Configures an IPv6 global unicast address, and enables IPv6 on an interface	IC
ipv6 address eui-64	Configures an IPv6 global unicast address for an interface using an EUI-64 interface ID in the low order 64 bits, and enables IPv6 on the interface	IC
ipv6 address link-local	Configures an IPv6 link-local address for an interface and enables IPv6 on the interface	IC
ipv6 enable	Enables IPv6 on an interface that has not been configured with an explicit IPv6 address	IC
ipv6 mtu	Sets the size of the maximum transmission unit (MTU) for IPv6 packets sent on an interface	IC
show ipv6 interface	Displays the usability and configured settings for IPv6 interfaces	NE, PE
show ipv6 mtu	Displays maximum transmission unit (MTU) information for IPv6 interfaces	NE, PE
show ipv6 traffic	Displays statistics about IPv6 traffic	NE, PE
clear ipv6 traffic	Resets IPv6 traffic counters	PE
ping6	Sends IPv6 ICMP echo request packets to another node on the network	PE
traceroute6	Shows the route packets take to the specified host	PE
Neighbor Discovery		
ipv6 hop-limit	Configures the maximum number of hops used in all IPv6 packets originated by this router	GC
ipv6 neighbor	Configures a static entry in the IPv6 neighbor discovery cache	GC
ipv6 nd dad attempts	Configures the number of consecutive neighbor solicitation messages sent on an interface during duplicate address detection	IC
ipv6 nd managed-config-flag	Configures router advertisements to indicate that attached hosts can use stateful autoconfiguration to obtain addresses	IC
ipv6 nd other-config-flag	Configures router advertisements to indicate that attached hosts can obtain autoconfiguration information other than addresses	IC
ipv6 nd ns-interval	Configures the interval between IPv6 neighbor solicitation retransmissions on an interface	IC
ipv6 nd raguard	Blocks incoming Router Advertisement and Router Redirect packets	IC
ipv6 nd reachable-time	Configures the amount of time that a remote IPv6 node is considered reachable after some reachability confirmation event has occurred	IC

Table 238: IPv6 Configuration Commands (Continued)

Command	Function	Mode
ipv6 nd prefix	Configures the IPv6 prefixes to include in router advertisements	IC
ipv6 nd ra interval	Configures the interval between the transmission of router advertisements on an interface	IC
ipv6 nd ra lifetime	Configures the router lifetime value used in router advertisements sent from an interface	IC
ipv6 nd ra router-preference	Configures the default router preference for the router on an interface	IC
ipv6 nd ra suppress	Suppresses router advertisement transmissions on an interface	IC
clear ipv6 neighbors	Deletes all dynamic entries in the IPv6 neighbor discovery cache	PE
show ipv6 nd raguard	Displays the configuration setting for RA Guard	PE
show ipv6 neighbors	Displays information in the IPv6 neighbor discovery cache	PE

Interface Address Configuration and Utilities

ipv6 default-gateway

This command sets an IPv6 default gateway to use for destinations with no known next hop. Use the **no** form to remove a previously configured default gateway.

SYNTAX

ipv6 default-gateway *ipv6-address*

no ipv6 address

ipv6-address - The IPv6 address of the default next hop router to use when the target device is located in a different network segment.

DEFAULT SETTING

No default gateway is defined

COMMAND MODE

Global Configuration

COMMAND USAGE

- All IPv6 addresses must be according to RFC 2373 “IPv6 Addressing Architecture,” using 8 colon-separated 16-bit hexadecimal values. One double colon may be used in the address to indicate the appropriate number of zeros required to fill the undefined fields.

- The same link-local address may be used by different interfaces/nodes in different zones (RFC 4007). Therefore, when specifying a link-local address, include zone-id information indicating the VLAN identifier after the % delimiter. For example, FE80::7272%1 identifies VLAN 1 as the interface from which the ping is sent.

- An IPv6 default gateway should be defined if the destination has been assigned an IPv6 address that is located in a different IP segment.

- An IPv6 default gateway can only be successfully set when a network interface that directly connects to the gateway has been configured on the router.

EXAMPLE

The following example defines a default gateway for this device:

```
Console(config)#ipv6 default-gateway FE80::269:3EF9:FE19:6780%1
Console(config)#
```

RELATED COMMANDS

show ipv6 route (1731)
ip default-gateway (1650)

ipv6 address

This command configures an IPv6 global unicast address and enables IPv6 on an interface. Use the **no** form without any arguments to remove all IPv6 addresses from the interface, or use the **no** form with a specific IPv6 address to remove that address from the interface.

SYNTAX

[**no**] **ipv6 address** *ipv6-address*[/*prefix-length*]

ipv6-address - A full IPv6 address including the network prefix and host address bits.

prefix-length - A decimal value indicating how many contiguous bits (from the left) of the address comprise the prefix (i.e., the network portion of the address).

DEFAULT SETTING

No IPv6 addresses are defined

COMMAND MODE

Interface Configuration (VLAN, IPv6/v4 Tunnel)

COMMAND USAGE

- All IPv6 addresses must be according to RFC 2373 “IPv6 Addressing Architecture,” using 8 colon-separated 16-bit hexadecimal values. One double colon may be used in the address to indicate the appropriate number of zeros required to fill the undefined fields.

- To connect to a larger network with multiple subnets, you must configure a global unicast address. This address can be manually configured with this command.

- If a link-local address has not yet been assigned to this interface, this command will assign the specified static global unicast address and also dynamically generate a link-local unicast address for the interface. (The link-local address is made with an address prefix of FE80 and a host portion based the switch's MAC address in modified EUI-64 format.)

- When configuring a global IPv6 address for a static tunnel, the link-local address generated by this command is the 32-bit IPv4 address of the underlying source interface, with the bytes in the same order in which they would appear in the header of an IPv4 packet, padded at the left with zeros to a total of 64 bits. Note that the "Universal/Local" bit is zero, indicating that the interface identifier is not globally unique. When the host has more than one IPv4 address in use on the physical interface concerned, the primary address for that interface is used. The IPv6 link-local address for an IPv4 virtual interface is formed by appending the interface identifier, as defined above, to the prefix FE80::/64.

- If a duplicate address is detected, a warning message is sent to the console.

EXAMPLE

This example specifies a full IPv6 address and prefix length.

```
Console(config)#interface vlan 1
Console(config-if)#ipv6 address 2001:DB8:2222:7272::72/96
Console(config-if)#end
Console#show ipv6 interface
VLAN 1 is up
IPv6 is enabled.
Link-local address:
  FE80::2E0:CFF:FE00:FD/64
Global unicast address(es):
  2001:DB8:2222:7272::72/96, subnet is 2001:DB8:2222:7272::/96
Joined group address(es):
FF02::1:FF00:72
FF02::1:FF00:FD
FF02::1
IPv6 link MTU is 1500 bytes
ND DAD is enabled, number of DAD attempts: 3.
ND retransmit interval is 1000 milliseconds
ND advertised retransmit interval is 0 milliseconds
ND reachable time is 30000 milliseconds
ND advertised reachable time is 0 milliseconds

Console#
```

RELATED COMMANDS

ipv6 address eui-64 (1667)
show ipv6 interface (1672)
ip address (1648)

ipv6 address eui-64

This command configures an IPv6 address for an interface using an EUI-64 interface ID in the low order 64 bits and enables IPv6 on the interface. Use the **no** form without any arguments to remove all manually configured IPv6 addresses from the interface. Use the **no** form with a specific address to remove it from the interface.

SYNTAX

ipv6 address *ipv6-prefix*/*prefix-length* **eui-64**

no ipv6 address [*ipv6-prefix*/*prefix-length* **eui-64**]

ipv6-prefix - The IPv6 network portion of the address assigned to the interface.

prefix-length - A decimal value indicating how many contiguous bits (from the left) of the address comprise the prefix (i.e., the network portion of the address).

DEFAULT SETTING

No IPv6 addresses are defined

COMMAND MODE

Interface Configuration (VLAN)

COMMAND USAGE

- The prefix must be formatted according to RFC 2373 "IPv6 Addressing Architecture," using 8 colon-separated 16-bit hexadecimal values. One double colon may be used in the address to indicate the appropriate number of zeros required to fill the undefined fields.

- If a link local address has not yet been assigned to this interface, this command will dynamically generate a global unicast address and a link-local address for this interface. (The link-local address is made with an address prefix of FE80 and a host portion based the switch's MAC address in modified EUI-64 format.)

- Note that the value specified in the ipv6-prefix may include some of the high-order host bits if the specified prefix length is less than 64 bits. If the specified prefix length exceeds 64 bits, then the network portion of the address will take precedence over the interface identifier.

- If a duplicate address is detected, a warning message is sent to the console.

- IPv6 addresses are 16 bytes long, of which the bottom 8 bytes typically form a unique host identifier based on the device's MAC address. The EUI-64 specification is designed for devices that use an extended 8-byte MAC address. For devices that still use a 6-byte MAC address (also known as EUI-48 format), it must be converted into EUI-64 format by inverting the universal/local bit in the address and inserting the hexadecimal number FFFE between the upper and lower three bytes of the MAC address.

- For example, if a device had an EUI-48 address of 28-9F-18-1C-82-35, the global/local bit must first be inverted to meet EUI-64 requirements (i.e., 1 for globally defined addresses and 0 for locally defined addresses), changing 28 to 2A. Then the two bytes FFFE are inserted between the OUI (i.e., company id) and the rest of the address, resulting in a modified EUI-64 interface identifier of 2A-9F-18-FF-FE-1C-82-35.

- This host addressing method allows the same interface identifier to be used on multiple IP interfaces of a single device, as long as those interfaces are attached to different subnets.

- When configuring an global IPv6 address for a static tunnel, the link-local address generated by this command is the 32-bit IPv4 address of the underlying source interface, with the bytes in the same order in which they would appear in the header of an IPv4 packet, padded at the left with zeros to a total of 64 bits. Note that the "Universal/Local" bit is zero, indicating that the interface identifier is not globally unique. When the host has more than one IPv4 address in use on the physical interface concerned, the primary address for that interface is used. The IPv6 link-local address for an IPv4 virtual interface is formed by appending the interface identifier, as defined above, to the prefix FE80::/64.

EXAMPLE

This example uses the network prefix of 2001:0DB8:0:1::/64, and specifies that the EUI-64 interface identifier be used in the lower 64 bits of the address.

```
Console(config)#interface vlan 1
Console(config-if)#ipv6 address 2001:0DB8:0:1::/64 eui-64
Console(config-if)#end
Console#show ipv6 interface
VLAN 1 is up
IPv6 is enable.
Link-local address:
  FE80::2E0:CFF:FE00:FD/64
Global unicast address(es):
  2001:DB8::1:2E0:CFF:FE00:FD/64, subnet is 2001:DB8::1:0:0:0:0/64[EUI]
  2001:DB8:2222:7272::72/96, subnet is 2001:DB8:2222:7272::/96[EUI]
Joined group address(es):
FF02::1:FF00:72
FF02::1:FF00:FD
FF02::1
IPv6 link MTU is 1500 bytes
ND DAD is enabled, number of DAD attempts: 3.
ND retransmit interval is 1000 milliseconds
ND advertised retransmit interval is 0 milliseconds
ND reachable time is 30000 milliseconds
ND advertised reachable time is 0 milliseconds

Console#
```

RELATED COMMANDS

show ipv6 interface (1672)

ipv6 address link-local

This command configures an IPv6 link-local address for an interface and enables IPv6 on the interface. Use the **no** form without any arguments to remove all manually configured IPv6 addresses from the interface. Use the **no** form with a specific address to remove it from the interface.

SYNTAX

ipv6 address *ipv6-address* **link-local**

no ipv6 address [*ipv6-address* **link-local**]

ipv6-address - The IPv6 address assigned to the interface.

DEFAULT SETTING

No IPv6 addresses are defined

COMMAND MODE

Interface Configuration (VLAN)

COMMAND USAGE

- The specified address must be formatted according to RFC 2373 “IPv6 Addressing Architecture,” using 8 colon-separated 16-bit hexadecimal values. One double colon may be used in the address to indicate the appropriate number of zeros required to fill the undefined fields. And the address prefix must be in the range of FE80~FEBF.
- The address specified with this command replaces a link-local address that was automatically generated for the interface.
- You can configure multiple IPv6 global unicast addresses per interface, but only one link-local address per interface.
- If a duplicate address is detected, a warning message is sent to the console.

EXAMPLE

This example assigns a link-local address of FE80::269:3EF9:FE19:6779 to VLAN 1. Note that a prefix in the range of FE80~FEBF is required for link-local addresses, and the first 16-bit group in the host address is padded with a zero in the form 0269.

```
Console(config)#interface vlan 1
Console(config-if)#ipv6 address FE80::269:3EF9:FE19:6779 link-local
Console(config-if)#end
Console#show ipv6 interface
VLAN 1 is up
IPv6 is enabled.
Link-local address:
  FE80::269:3EF9:FE19:6779/64
Global unicast address(es):
  2001:DB8::1:2E0:CFF:FE00:FD/64, subnet is 2001:DB8::1:0:0:0:0/64[EUI]
  2001:DB8:2222:7272::72/96, subnet is 2001:DB8:2222:7272::/96[EUI]
Joined group address(es):
FF02::1:FF19:6779
FF02::1:FF00:72
FF02::1:FF00:FD
```

```
FF02::1
IPv6 link MTU is 1500 bytes
ND DAD is enabled, number of DAD attempts: 3.
ND retransmit interval is 1000 milliseconds
ND advertised retransmit interval is 0 milliseconds
ND reachable time is 30000 milliseconds
ND advertised reachable time is 0 milliseconds

Console#
```

RELATED COMMANDS

ipv6 enable (1670)
show ipv6 interface (1672)

ipv6 enable

This command enables IPv6 on an interface that has not been configured with an explicit IPv6 address. Use the **no** form to disable IPv6 on an interface that has not been configured with an explicit IPv6 address.

SYNTAX

[**no**] **ipv6 enable**

DEFAULT SETTING

IPv6 is disabled

COMMAND MODE

Interface Configuration (VLAN)

COMMAND USAGE

- This command enables IPv6 on the current VLAN interface and automatically generates a link-local unicast address. The address prefix uses FE80, and the host portion of the address is generated by converting the switch’s MAC address to modified EUI-64 format (see page 1667). This address type makes the switch accessible over IPv6 for all devices attached to the same local subnet.

- If a duplicate address is detected on the local segment, this interface will be disabled and a warning message displayed on the console.

- The **no ipv6 enable** command does not disable IPv6 for an interface that has been explicitly configured with an IPv6 address.

EXAMPLE

In this example, IPv6 is enabled on VLAN 1, and the link-local address FE80::2E0:CFF:FE00:FD/64 is automatically generated by the switch.

```
Console(config)#interface vlan 1
Console(config-if)#ipv6 enable
Console(config-if)#end
Console#show ipv6 interface
VLAN 1 is up
IPv6 is enabled.
```

```
Link-local address:
  FE80::2E0:CFF:FE00:FD/64
Global unicast address(es):
  2001:DB8:2222:7273::72/96, subnet is 2001:DB8:2222:7273::/96
Joined group address(es):
FF02::1:FF00:72
FF02::1:FF00:FD
FF02::1
IPv6 link MTU is 1280 bytes
ND DAD is enabled, number of DAD attempts: 3.
ND retransmit interval is 1000 milliseconds
ND advertised retransmit interval is 0 milliseconds
ND reachable time is 30000 milliseconds
ND advertised reachable time is 0 milliseconds

Console#
```

RELATED COMMANDS

ipv6 address link-local (1669)
show ipv6 interface (1672)

ipv6 mtu

This command sets the size of the maximum transmission unit (MTU) for IPv6 packets sent on an interface. Use the **no** form to restore the default setting.

SYNTAX

ipv6 mtu *size*

no ipv6 mtu

size - Specifies the MTU size. (Range: 1280-65535 bytes)

DEFAULT SETTING

1500 bytes

COMMAND MODE

Interface Configuration (VLAN)

COMMAND USAGE

- If a non-default value is configured, an MTU option is included in the router advertisements sent from this device.
- The maximum value set by this command cannot exceed the MTU of the physical interface, which is currently fixed at 1500 bytes.
- IPv6 routers do not fragment IPv6 packets forwarded from other routers. However, traffic originating from an end-station connected to an IPv6 router may be fragmented.
- All devices on the same physical medium must use the same MTU in order to operate correctly.
- IPv6 must be enabled on an interface before the MTU can be set.

EXAMPLE

The following example sets the MTU for VLAN 1 to 1280 bytes:

```
Console(config)#interface vlan 1
Console(config-if)#ipv6 mtu 1280
Console(config-if)#
```

RELATED COMMANDS

show ipv6 mtu (1674)
jumbo frame (911)

show ipv6 interface

This command displays the usability and configured settings for IPv6 interfaces.

SYNTAX

show ipv6 interface [**brief** [**vlan** *vlan-id* [*ipv6-prefix*/*prefix-length*]]]

brief - Displays a brief summary of IPv6 operational status and the addresses configured for each interface.

vlan-id - VLAN ID (Range: 1-4094)

ipv6-prefix - The IPv6 network portion of the address assigned to the interface. The prefix must be formatted according to RFC 2373 "IPv6 Addressing Architecture," using 8 colon-separated 16-bit hexadecimal values. One double colon may be used in the address to indicate the appropriate number of zeros required to fill the undefined fields.

prefix-length - A decimal value indicating how many of the contiguous bits (from the left) of the address comprise the prefix (i.e., the network portion of the address).

COMMAND MODE

Normal Exec, Privileged Exec

EXAMPLE

This example displays all the IPv6 addresses configured for the switch.

```
Console#show ipv6 interface
VLAN 1 is up
IPv6 is enabled.
Link-local address:
  FE80::2E0:CFF:FE00:FD/64
Global unicast address(es):
  2001:DB8:2222:7273::72/96, subnet is 2001:DB8:2222:7273::/96
Joined group address(es):
FF02::1:FF00:72
FF02::1:FF00:FD
FF02::1
IPv6 link MTU is 1280 bytes
ND DAD is enabled, number of DAD attempts: 3.
ND retransmit interval is 1000 milliseconds
ND advertised retransmit interval is 0 milliseconds
ND reachable time is 30000 milliseconds
ND advertised reachable time is 0 milliseconds

Console#
```

Table 239: show ipv6 interface - display description

Field	Description
VLAN	A VLAN is marked "up" if the switch can send and receive packets on this interface, "down" if a line signal is not present, or "administratively down" if the interface has been disabled by the administrator.
IPv6	IPv6 is marked "enable" if the switch can send and receive IP traffic on this interface, "disable" if the switch cannot send and receive IP traffic on this interface, or "stalled" if a duplicate link-local address is detected on the interface.
Link-local address	Shows the link-local address assigned to this interface
Global unicast address(es)	Shows the global unicast address(es) assigned to this interface
Joined group address(es)	In addition to the unicast addresses assigned to an interface, a node is required to join the all-nodes multicast addresses FF01::1 and FF02::1 for all IPv6 nodes within scope 1 (interface-local) and scope 2 (link-local), respectively. FF01::1/16 is the transient interface-local multicast address for all attached IPv6 nodes, and FF02::1/16 is the link-local multicast address for all attached IPv6 nodes. The interface-local multicast address is only used for loopback transmission of multicast traffic. Link-local multicast addresses cover the same types as used by link-local unicast addresses, including all nodes (FF02::1), all routers (FF02::2), and solicited nodes (FF02::1:FFXX:XXXX) as described below. A node is also required to compute and join the associated solicited-node multicast addresses for every unicast and anycast address it is assigned. IPv6 addresses that differ only in the high-order bits, e.g. due to multiple high-order prefixes associated with different aggregations, will map to the same solicited-node address, thereby reducing the number of multicast addresses a node must join. In this example, FF02::1:FF90:0/104 is the solicited-node multicast address which is formed by taking the low-order 24 bits of the address and appending those bits to the prefix.
MTU	Maximum transmission unit for this interface.
ND DAD	Indicates whether (neighbor discovery) duplicate address detection is enabled.
number of DAD attempts	The number of consecutive neighbor solicitation messages sent on the interface during duplicate address detection.
ND retransmit interval	The interval between IPv6 neighbor solicitation retransmissions sent on an interface during duplicate address detection.
ND advertised retransmit interval	The retransmit interval is included in all router advertisements sent out of an interface so that nodes on the same link use the same time value.
ND reachable time	The amount of time a remote IPv6 node is considered reachable after a reachability confirmation event has occurred
ND advertised reachable time	The reachable time is included in all router advertisements sent out of an interface so that nodes on the same link use the same time value.

This example displays a brief summary of IPv6 addresses configured on the switch.

```
Console#show ipv6 interface brief
Interface       VLAN       IPv6       IPv6 Address
--------------- ---------- ---------- ------------------------------------
VLAN 1          Up         Up         2001:DB8:2222:7273::72/96
VLAN 1          Up         Up         FE80::2E0:CFF:FE00:FD%1/64
Console#
```

RELATED COMMANDS

show ip interface (1651)

show ipv6 mtu

This command displays the maximum transmission unit (MTU) cache for destinations that have returned an ICMP packet-too-big message along with an acceptable MTU to this switch.

COMMAND MODE

Normal Exec, Privileged Exec

EXAMPLE

The following example shows the MTU cache for this device:

```
Console#show ipv6 mtu
MTU     Since    Destination Address
1400    00:04:21  5000:1::3
1280    00:04:50  FE80::203:A0FF:FED6:141D
Console#
```

Table 240: show ipv6 mtu - display description*

Field	Description
MTU	Adjusted MTU contained in the ICMP packet-too-big message returned from this destination, and now used for all traffic sent along this path.
Since	Time since an ICMP packet-too-big message was received from this destination.
Destination Address	Address which sent an ICMP packet-too-big message.

* No information is displayed if an IPv6 address has not been assigned to the switch.

show ipv6 traffic

This command displays statistics about IPv6 traffic passing through this switch.

COMMAND MODE

Normal Exec, Privileged Exec

EXAMPLE

The following example shows statistics for all IPv6 unicast and multicast traffic, as well as ICMP, UDP and TCP statistics:

```
Console#show ipv6 traffic
IPv6 Statistics:
IPv6 received
                     total received
                     header errors
                     too big errors
                     no routes
                     address errors
                     unknown protocols
                     truncated packets
                     discards
                     delivers
                     reassembly request datagrams
                     reassembly succeeded
                     reassembly failed
IPv6 sent
                     forwards datagrams
                  15 requests
                     discards
                     no routes
                     generated fragments
                     fragment succeeded
                     fragment failed
ICMPv6 Statistics:
ICMPv6 received
                     input
                     errors
                     destination unreachable messages
                     packet too big messages
                     time exceeded messages
                     parameter problem message
                     echo request messages
                     echo reply messages
                     router solicit messages
                     router advertisement messages
                     neighbor solicit messages
                     neighbor advertisement messages
                     redirect messages
                     group membership query messages
                     group membership response messages
                     group membership reduction messages
                     multicast listener discovery version 2 reports
ICMPv6 sent
                   4 output
                     destination unreachable messages
                     packet too big messages
                     time exceeded messages
                     parameter problem message
                     echo request messages
                     echo reply messages
                   3 router solicit messages
                     router advertisement messages
                   1 neighbor solicit messages
                     neighbor advertisement messages
                     redirect messages
                     group membership query messages
                     group membership response messages
                     group membership reduction messages
                     multicast listener discovery version 2 reports
UDP Statistics:
                     input
                     no port errors
                     other errors
                     output
Console#
```

Table 241: show ipv6 traffic - display description

Field	Description
IPv6 Statistics	
IPv6 received	
total received	The total number of input datagrams received by the interface, including those received in error.
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, IPv6 options, etc.
too big errors	The number of input datagrams that could not be forwarded because their size exceeded the link MTU of outgoing interface.
no routes	The number of input datagrams discarded because no route could be found to transmit them to their destination.
address errors	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.
unknown protocols	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.
truncated packets	The number of input datagrams discarded because datagram frame didn't carry enough data.
discards	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.
delivers	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.
reassembly request datagrams	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.

Table 241: show ipv6 traffic - display description (Continued)

Field	Description
reassembly succeeded	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.
reassembly failed	The number of failures detected by the IPv6 re-assembly 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.
IPv6 sent	
forwards datagrams	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.
requests	The 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.
discards	The 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.
no routes	The number of input datagrams discarded because no route could be found to transmit them to their destination.
generated fragments	The number of output datagram fragments that have been generated as a result of fragmentation at this output interface.
fragment succeeded	The number of IPv6 datagrams that have been successfully fragmented at this output interface.
fragment failed	The number of IPv6 datagrams that have been discarded because they needed to be fragmented at this output interface but could not be.
ICMPv6 Statistics	
ICMPv6 received	
input	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.
errors	The number of ICMP messages which the interface received but determined as having ICMP-specific errors (bad ICMP checksums, bad length, etc.).
destination unreachable messages	The number of ICMP Destination Unreachable messages received by the interface.
packet too big messages	The number of ICMP Packet Too Big messages received by the interface.
time exceeded messages	The number of ICMP Time Exceeded messages received by the interface.
parameter problem message	The number of ICMP Parameter Problem messages received by the interface.

Table 241: show ipv6 traffic - display description (Continued)

Field	Description
echo request messages	The number of ICMP Echo (request) messages received by the interface.
echo reply messages	The number of ICMP Echo Reply messages received by the interface.
router solicit messages	The number of ICMP Router Solicit messages received by the interface.
router advertisement messages	The number of ICMP Router Advertisement messages received by the interface.
neighbor solicit messages	The number of ICMP Neighbor Solicit messages received by the interface.
neighbor advertisement messages	The number of ICMP Neighbor Advertisement messages received by the interface.
redirect messages	The number of Redirect messages received by the interface.
group membership query messages	The number of ICMPv6 Group Membership Query messages received by the interface.
group membership response messages	The number of ICMPv6 Group Membership Response messages received by the interface.
group membership reduction messages	The number of ICMPv6 Group Membership Reduction messages received by the interface.
multicast listener discovery version 2 reports	The number of MLDv2 reports received by the interface.
ICMPv6 sent	
output	The total number of ICMP messages which this interface attempted to send. Note that this counter includes all those counted by icmpOutErrors.
destination unreachable messages	The number of ICMP Destination Unreachable messages sent by the interface.
packet too big messages	The number of ICMP Packet Too Big messages sent by the interface.
time exceeded messages	The number of ICMP Time Exceeded messages sent by the interface.
parameter problem message	The number of ICMP Parameter Problem messages sent by the interface.
echo request messages	The number of ICMP Echo (request) messages sent by the interface.
echo reply messages	The number of ICMP Echo Reply messages sent by the interface.
router solicit messages	The number of ICMP Router Solicitation messages sent by the interface.
router advertisement messages	The number of ICMP Router Advertisement messages sent by the interface.
neighbor solicit messages	The number of ICMP Neighbor Solicit messages sent by the interface.
neighbor advertisement messages	The number of ICMP Router Advertisement messages sent by the interface.
redirect messages	The number of Redirect messages sent. For a host, this object will always be zero, since hosts do not send redirects.
group membership query messages	The number of ICMPv6 Group Membership Query messages sent by the interface.

Table 241: show ipv6 traffic - display description (Continued)

Field	Description
group membership response messages	The number of ICMPv6 Group Membership Response messages sent.
group membership reduction messages	The number of ICMPv6 Group Membership Reduction messages sent.
multicast listener discovery version 2 reports	The number of MLDv2 reports sent by the interface.
UDP Statistics	
input	The total number of UDP datagrams delivered to UDP users.
no port errors	The total number of received UDP datagrams for which there was no application at the destination port.
other errors	The number of received UDP datagrams that could not be delivered for reasons other than the lack of an application at the destination port.
output	The total number of UDP datagrams sent from this entity.

clear ipv6 traffic

This command resets IPv6 traffic counters.

COMMAND MODE

Privileged Exec

COMMAND USAGE

This command resets all of the counters displayed by the show ipv6 traffic command.

EXAMPLE

```
Console#clear ipv6 traffic
Console#
```

ping6

This command sends (IPv6) ICMP echo request packets to another node on the network.

SYNTAX

ping6 {*ipv6-address* | *host-name*} [**count** *count*] [**size** *size*]

ipv6-address - The IPv6 address of a neighbor device. You can specify either a link-local or global unicast address formatted according to RFC 2373 "IPv6 Addressing Architecture," using 8 colon-separated 16-bit hexadecimal values. One double colon may be used in the address to indicate the appropriate number of zeros required to fill the undefined fields.

host-name - A host name string which can be resolved into an IPv6 address through a domain name server.

count - Number of packets to send. (Range: 1-16) *size* - Number of bytes in a packet. (Range: 48-18024 bytes) The actual packet size will be eight bytes larger than the size specified because the router adds header information.

DEFAULT SETTING

count: 5
size: 100 bytes

COMMAND MODE

Privileged Exec

COMMAND USAGE

- Use the **ping6** command to see if another site on the network can be reached, or to evaluate delays over the path.

- The same link-local address may be used by different interfaces/nodes in different zones (RFC 4007). Therefore, when specifying a link-local address, include zone-id information indicating the VLAN identifier after the % delimiter. For example, FE80::7272%1 identifies VLAN 1 as the interface from which the ping is sent.

- When pinging a host name, be sure the DNS server has been enabled (see page 1616). If necessary, local devices can also be specified in the DNS static host table (see page 1618).

- When using ping6 with a host name, the router first attempts to resolve the alias into an IPv6 address before trying to resolve it into an IPv4 address.

EXAMPLE

```
Console#ping6 FE80::2E0:CFF:FE00:FC%1/64
Type ESC to abort.
PING to FE80::2E0:CFF:FE00:FC%1/64, by 5 32-byte payload ICMP packets,
  timeout is 3 seconds
response time: 20 ms    [FE80::2E0:CFF:FE00:FC] seq_no: 1
response time: 0 ms     [FE80::2E0:CFF:FE00:FC] seq_no: 2
response time: 0 ms     [FE80::2E0:CFF:FE00:FC] seq_no: 3
response time: 0 ms     [FE80::2E0:CFF:FE00:FC] seq_no: 4
response time: 0 ms     [FE80::2E0:CFF:FE00:FC] seq_no: 5
Ping statistics for FE80::2E0:CFF:FE00:FC%1/64:
 5 packets transmitted, 5 packets received (100%), 0 packets lost (0%)
Approximate round trip times:
 Minimum = 0 ms, Maximum = 20 ms, Average = 4 ms
Console#
```

traceroute6

This command shows the route packets take to the specified destination.

SYNTAX

traceroute6 {*ipv6-address* | *host-name*}
[**max-failures** *failure-count*]

ipv6-address - The IPv6 address of a neighbor device. You can specify either a link-local or global unicast address formatted according to RFC 2373 "IPv6 Addressing Architecture," using 8 colon-separated 16-bit hexadecimal values. One double colon may be used in the address to indicate the appropriate number of zeros required to fill the undefined fields.

host-name - A host name string which can be resolved into an IPv6 address through a domain name server.

failure-count – The maximum number of failures before which the trace route is terminated. (Range: 1-255)

DEFAULT SETTING

Maximum failures: 5

COMMAND MODE

Privileged Exec

COMMAND USAGE

- Use the **traceroute6** command to determine the path taken to reach a specified destination.

- The same link-local address may be used by different interfaces/nodes in different zones (RFC 4007). Therefore, when specifying a link-local address, include zone-id information indicating the VLAN identifier after the % delimiter. For example, FE80::7272%1 identifies VLAN 1 as the interface from which the ping is sent.

- A trace terminates when the destination responds, when the maximum timeout (TTL) is exceeded, or the maximum number of hops is exceeded.

- The traceroute command first sends probe datagrams with the TTL value set at one. This causes the first router to discard the datagram and return an error message. The trace function then sends several probe messages at each subsequent TTL level and displays the round-trip time for each message. Not all devices respond correctly to probes by returning an "ICMP port unreachable" message. If the timer goes off before a response is returned, the trace function prints a series of asterisks and the "Request Timed Out" message. A long sequence of these messages, terminating only when the maximum timeout has been reached, may indicate this problem with the target device.

EXAMPLE

```
Console#traceroute6 FE80::2E0:CFF:FE9C:CA10%1/64
Press "ESC" to abort.

Traceroute to FE80::2E0:CFF:FE9C:CA10%1/64, 30 hops max, timeout is 3
  seconds, 5 max failure(s) before termination.

Hop Packet 1 Packet 2 Packet 3 IPv6 Address
--- -------- -------- -------- ---------------------------------------------
  1   <10 ms   <10 ms   <10 ms FE80::2E0:CFF:FE9C:CA10%1/64

Trace completed.
Console#
```

Neighbor Discovery

ipv6 hop-limit

This command configures the maximum number of hops used in router advertisements that are originated by this router. Use the **no** form to restore the default setting.

SYNTAX

ipv6 hop-limit *hops*

no ipv6 hop-limit

hops - The maximum number of hops in router advertisements and all IPv6 packets. (Range: 1-255)

DEFAULT SETTING

1

COMMAND MODE

Global Configuration

EXAMPLE

The following sets the hop limit for router advertisements to 64:

```
Console(config)#ipv6 hop-limit 64
Console(config)#
```

ipv6 neighbor

This command configures a static entry in the IPv6 neighbor discovery cache. Use the **no** form to remove a static entry from the cache.

SYNTAX

ipv6 neighbor *ipv6-address* **vlan** *vlan-id hardware-address*

no ipv6 mtu

ipv6-address - The IPv6 address of a neighbor device that can be reached through one of the network interfaces configured on this switch. You can specify either a link-local or global unicast address formatted according to RFC 2373 “IPv6 Addressing Architecture,” using 8 colon-separated 16-bit hexadecimal values. One double colon may be used in the address to indicate the appropriate number of zeros required to fill the undefined fields.

vlan-id - VLAN ID (Range: 1-4094)

hardware-address - The 48-bit MAC layer address for the neighbor device. This address must be formatted as six hexadecimal pairs separated by hyphens.

DEFAULT SETTING

None

COMMAND MODE

Global Configuration

COMMAND USAGE

- Address Resolution Protocol (ARP) has been replaced in IPv6 with the Neighbor Discovery Protocol (NDP). The **ipv6 neighbor** command is similar to the mac-address-table static command that is implemented using ARP.

- Static entries can only be configured on an IPv6-enabled interface.

- The switch does not determine whether a static entry is reachable before placing it in the IPv6 neighbor discovery cache.

- If the specified entry was dynamically learned through the IPv6 neighbor discovery process, and already exists in the neighbor discovery cache, it is converted to a static entry. Static entries in the IPv6 neighbor discovery cache are not modified if subsequently detected by the neighbor discovery process.

- Disabling IPv6 on an interface with the no ipv6 enable command (see page 1670) deletes all dynamically learned entries in the IPv6 neighbor discovery cache for that interface, but does not delete static entries.

EXAMPLE

The following maps a static entry for global unicast address to a MAC address:

```
Console(config)#ipv6 neighbor 2009:DB9:2229::81 vlan 1 30-65-14-01-11-86
Console(config)#end
Console#show ipv6 neighbors
State: I1 - Incomplete, I2 - Invalid, R - Reachable, S - Stale, D - Delay,
       P1 - Probe, P2 - Permanent, U - Unknown
IPv6 Address                Age          Link-layer Addr    State       VLAN
2009:DB9:2229::80           956          12-34-11-11-43-21      R          1
2009:DB9:2229::81           Permanent    30-65-14-01-11-86      R          1
FE80::1034:11FF:FE11:4321   961          12-34-11-11-43-21      R          1
Console#
```

RELATED COMMANDS

show ipv6 neighbors (1694)

ipv6 nd dad attempts

This command configures the number of consecutive neighbor solicitation messages sent on an interface during duplicate address detection. Use the **no** form to restore the default setting.

SYNTAX

ipv6 nd dad attempts *count*

no ipv6 nd dad attempts

count - The number of neighbor solicitation messages sent to determine whether or not a duplicate address exists on this interface. (Range: 0-600)

DEFAULT SETTING

1

COMMAND MODE

Interface Configuration (VLAN)

COMMAND USAGE

- Configuring a value of 0 disables duplicate address detection.

- Duplicate address detection determines if a new unicast IPv6 address already exists on the network before it is assigned to an interface.

- Duplicate address detection is stopped on any interface that has been suspended (see the vlan command). While an interface is suspended, all unicast IPv6 addresses assigned to that interface are placed in a “pending” state. Duplicate address detection is automatically restarted when the interface is administratively re-activated.

- An interface that is re-activated restarts duplicate address detection for all unicast IPv6 addresses on the interface. While duplicate address detection is performed on the interface’s link-local address, the other

IPv6 addresses remain in a "tentative" state. If no duplicate link-local address is found, duplicate address detection is started for the remaining IPv6 addresses.

- If a duplicate address is detected, it is set to "duplicate" state, and a warning message is sent to the console. If a duplicate link-local address is detected, IPv6 processes are disabled on the interface. If a duplicate global unicast address is detected, it is not used. All configuration commands associated with a duplicate address remain configured while the address is in "duplicate" state.
- If the link-local address for an interface is changed, duplicate address detection is performed on the new link-local address, but not for any of the IPv6 global unicast addresses already associated with the interface.

EXAMPLE

The following configures five neighbor solicitation attempts for addresses configured on VLAN 1. The show ipv6 interface command indicates that the duplicate address detection process is still on-going.

```
Console(config)#interface vlan 1
Console(config-if)#ipv6 nd dad attempts 5
Console(config-if)#end
Console#show ipv6 interface
VLAN 1 is up
IPv6 is enabled.
Link-local address:
  FE80::200:E8FF:FE90:0/64
Global unicast address(es):
  2009:DB9:2229::79, subnet is 2009:DB9:2229:0::/64
Joined group address(es):
  FF01::1/16
  FF02::1/16
  FF02::1:FF00:79/104
  FF02::1:FF90:0/104
IPv6 link MTU is 1500 bytes
ND DAD is enabled, number of DAD attempts: 5.
ND retransmit interval is 1000 milliseconds
ND advertised retransmit interval is 0 milliseconds
ND reachable time is 30000 milliseconds
ND advertised reachable time is 0 milliseconds
Console#
```

RELATED COMMANDS

ipv6 nd ns-interval (1687)
show ipv6 neighbors (1694)

ipv6 nd managed-config-flag

This command configures IPv6 router advertisements to indicate to attached hosts that they can use stateful autoconfiguration to obtain addresses. Use the **no** form to clear this flag from router advertisements.

SYNTAX

[**no**] **ipv6 nd managed-config-flag**

DEFAULT SETTING

Disabled

COMMAND MODE

Interface Configuration (VLAN)

COMMAND USAGE

- The “managed-address configuration” flag tells hosts that they should use stateful autoconfiguration to obtain addresses from a DHCPv6 server.

- The ipv6 nd other-config-flag command is used to tell hosts that they should use stateless address autoconfiguration to get IPv6 address (based on the IPv6 prefixes found in router advertisements) and stateful autoconfiguration to get other non-address parameters (such as DNS server addresses) from DHCPv6 servers.

- The absence of the “managed-address configuration” flag tells hosts to use only stateless address autoconfiguration (based on IPv6 prefixes found in router advertisements).

- The “managed address configuration” flag is only a suggestion to attached hosts. They may still use stateful and/or stateless address autoconfiguration. If hosts must be forced to use DHCPv6 for security reasons, ensure that no route prefixes are sent in router adverstiments.

EXAMPLE

The following tells hosts to use stateful autoconfiguration to obtain addresses:

```
Console(config)#interface vlan 1
Console(config)#ipv6 nd managed-config-flag
Console(config)#
```

ipv6 nd other-config-flag

This command configures IPv6 router advertisements to indicate to attached hosts that they can obtain stateful autoconfiguration information other than addresses. Use the **no** form to clear this flag from router advertisements.

SYNTAX

[**no**] **ipv6 nd other-config-flag**

DEFAULT SETTING

Disabled

COMMAND MODE

Interface Configuration (VLAN)

COMMAND USAGE

- The “other-stateful-configuration” flag tells hosts that they should use stateful autoconfiguration to obtain information other than addresses from a DHCPv6 server.

- Some hosts interpret the “other stateful configuration” flag to indicate that they should use stateless address autoconfiguration to get IPv6 address (based on the IPv6 prefixes found in router advertisements) and stateful autoconfiguration to get other non-address parameters from DHCPv6 servers. In this case, the absence of both the “managed address configuration” flag and the “other stateful configuration” flag is interpreted to mean that they should use only stateless autoconfiguration to obtain addresses.

EXAMPLE

The following tells hosts to use stateful autoconfiguration to obtain other non-address information from a DHCPv6 server:

```
Console(config)#interface vlan 1
Console(config)#ipv6 nd other-config-flag
Console(config)#
```

ipv6 nd ns-interval

This command configures the interval between transmitting IPv6 neighbor solicitation messages on an interface. Use the **no** form to restore the default value.

SYNTAX

ipv6 nd ns-interval *milliseconds*

no ipv6 nd ns-interval

milliseconds - The interval between transmitting IPv6 neighbor solicitation messages. (Range: 1000-3600000)

DEFAULT SETTING

1000 milliseconds is used for neighbor discovery operations
0 milliseconds is advertised in router advertisements

COMMAND MODE

Interface Configuration (VLAN)

COMMAND USAGE

- When a non-default value is configured, the specified interval is used both for router advertisements and by the router itself.

- This command specifies the interval between transmitting neighbor solicitation messages when resolving an address, or when probing the reachability of a neighbor. Therefore, avoid using very short intervals for normal IPv6 operations.

- Setting the neighbor solicitation interval to 0 means that the configured time is unspecified by this router.

EXAMPLE

The following sets the interval between sending neighbor solicitation messages to 30000 milliseconds:

```
Console(config)#interface vlan 1
Console(config)#pv6 nd ns-interval 30000
Console(config)#end
Console#show ipv6 interface
VLAN 1 is up
IPv6 is enabled.
Link-local address:
  FE80::200:E8FF:FE90:0/64
Global unicast address(es):
  2009:DB9:2229::79, subnet is 2009:DB9:2229:0::/64
Joined group address(es):
  FF01::1/16
  FF02::1/16
  FF02::1:FF00:79/104
  FF02::1:FF90:0/104
IPv6 link MTU is 1500 bytes
ND DAD is enabled, number of DAD attempts: 1.
ND retransmit interval is 1000 milliseconds
ND advertised retransmit interval is 0 milliseconds
ND reachable time is 30000 milliseconds
ND advertised reachable time is 0 milliseconds
ND advertised router lifetime is 1800 seconds
Console#
```

RELATED COMMANDS

show running-config (904)

ipv6 nd raguard

This command blocks incoming Router Advertisement and Router Redirect packets. Use the no form to disable this feature.

SYNTAX

[**no**] **ipv6 nd raguard**

DEFAULT SETTING

Disabled

COMMAND MODE

Interface Configuration (Ethernet, Port Channel)

COMMAND USAGE

- IPv6 Router Advertisements (RA) convey information that enables nodes to auto-configure on the network. This information may include the default router address taken from the observed source address of the RA message, as well as on-link prefix information. However, unintended misconfigurations, or possibly malicious attacks on the network, may lead to bogus RAs being sent, which in turn can cause operational problems for hosts on the network.

- This command can be used to block RAs and Router Redirect (RR) messages on the specified interface. Determine which interfaces are connected to known routers, and enable RA Guard on all other untrusted interfaces.

EXAMPLE

```
Console(config)#interface ethernet 1/1
Console(config-if)#pv6 nd raguard
Console(config-if)#
```

ipv6 nd reachable-time

This command configures the amount of time that a remote IPv6 node is considered reachable after some reachability confirmation event has occurred. Use the **no** form to restore the default setting.

SYNTAX

ipv6 nd reachable-time *milliseconds*

no ipv6 nd reachable-time

milliseconds - The time that a node can be considered reachable after receiving confirmation of reachability. (Range: 0-3600000)

DEFAULT SETTING

30000 milliseconds is used for neighbor discovery operations
0 milliseconds is advertised in router advertisements

COMMAND MODE

Interface Configuration (VLAN)

COMMAND USAGE

- The time limit configured by this command allows the router to detect unavailable neighbors.

- This time limit is included in all router advertisements sent out through an interface, ensuring that nodes on the same link use the same time value.

- Setting the time limit to 0 means that the configured time is unspecified by this router.

EXAMPLE

The following sets the reachable time for a remote node to 1000 milliseconds:

```
Console(config)#interface vlan 1
Console(config)#pv6 nd reachable-time 1000
Console(config)#
```

ipv6 nd prefix

This command configures the IPv6 prefixes to include in router advertisements. Use the **no** form to remove a prefix.

SYNTAX

ipv6 nd prefix *ipv6-address/prefix-length* {**default** | [*valid-lifetime preferred-lifetime* [**no-autoconfig** | **off-link**]]}

no ipv6 nd prefix *ipv6-address***/***prefix-length*

ipv6-address - An IPv6 address including the network prefix and host address bits.

prefix-length - A decimal value indicating how many contiguous bits (from the left) of the address comprise the prefix (i.e., the network portion of the address).

default - Uses default values for remaining parameters.

valid-lifetime - The amount of time that the specified IPv6 prefix is advertised as being valid. (Range: 0-4294967295 seconds)

preferred-lifetime - The amount of time that the specified IPv6 prefix is advertised as being preferred. The preferred lifetime is counted down in real time. (Range: 0-4294967295 seconds)

no-autoconfig - Indicates to hosts on the local link that the specified prefix cannot be used for IPv6 autoconfiguration.

off-link - Indicates that the specified prefix is assigned to the link. Nodes sending traffic to addresses that contain the prefix consider the destination to be locally reachable on the link.

DEFAULT SETTING

valid-lifetime	2592000 seconds
preferred-lifetime	2592000 seconds
no-autoconfig	Disabled
off-link	Disabled

COMMAND MODE

Interface Configuration (VLAN)

COMMAND USAGE

- Prefixes configured as addresses on an interface using the ipv6 address command are advertised in router advertisements. If prefixes are configured for advertisement using the **ipv6 nd prefix** command, then only these prefixes are advertised.

- The preferred lifetime and valid lifetime are counted down in real time. After the preferred lifetime expires, no new connections are made using this prefix. When the valid lifetime expires, this prefix will no longer be advertised.

- All prefixes are inserted in the routing table as Connected (i.e., online), unless specified with the off-link option. If the off-link option is specified, and the prefix is already present in the routing table as a Connected prefix, it will be removed.

- Do not include the link-local prefix in the list of advertised prefixes.

EXAMPLE

The following configures a network prefix with a valid lifetime of 1000 seconds, and a preferred lifetime of 900 seconds:

```
Console(config)#interface vlan 1
Console(config)#ipv6 nd prefix 2011:0DBF::/35 1000 900
Console(config)#
```

ipv6 nd ra interval

This command configures the interval between the transmission of IPv6 router advertisements on an interface. Use the **no** form to restore the default interval.

SYNTAX

ipv6 nd ra interval *interval*

no ipv6 nd ra interval

interval - The interval between IPv6 router advertisements. (Range: 3-1800 seconds)

COMMAND MODE

Interface Configuration (VLAN)

DEFAULT SETTING

600 seconds

COMMAND USAGE

- The interval between transmissions should be less than or equal to the IPv6 router advertisement lifetime if you configure a route as a default router by using the ipv6 nd ra lifetime command.

- To prevent synchronization with other IPv6 nodes, the actual interval used is randomly selected from a value between the minimum value set by the system (33% of the maximum RA interval) and the maximum value set by the **ipv6 nd ra interval** command.

EXAMPLE

The following sets the maximum RA interval to 1800 seconds:

```
Console(config)#interface vlan 1
Console(config)#ipv6 nd ra interval 1800
Console(config)#
```

ipv6 nd ra lifetime

This command configures the router lifetime value used in IPv6 router advertisements sent from an interface. Use the **no** form to restore the default setting.

Syntax

ipv6 nd ra lifetime *lifetime*

no ipv6 nd ra lifetime

lifetime - Router lifetime. (Range: 0-90000 seconds)

Command Mode

Interface Configuration (VLAN)

Default Setting

1800 seconds

Command Usage

- This command can be used to indicate the usefulness of this router as a default router on this interface.
- Set the router lifetime to 0 to indicate that this router should not be considered a default router. Set the lifetime to a non-zero value to indicate that it should be considered a default router. When a non-zero value is used, the lifetime should not be less than the router advertisement interval.

Example

The following sets the router lifetime to 8000 seconds:

```
Console(config)#interface vlan 1
Console(config)#ipv6 nd ra lifetime 8000
Console(config)#
```

ipv6 nd ra router-preference

This command configures the default router preference for the router on an interface. Use the **no** form to restore the default setting.

Syntax

ipv6 nd ra router-preference {**high** | **medium** | **low**}

no ipv6 nd ra router-preference

high - Preference for the router is high.

medium - Preference for the router is medium.

low - Preference for the router is low.

Command Mode

Interface Configuration (VLAN)

Default Setting

medium

Command Usage

Default router preference may be used to prioritize routers which provide equivalent, but not equal-cost, routing, and policy dictates that hosts should prefer one of the routers.

Example

The following sets the default router preference to high:

```
Console(config)#interface vlan 1
Console(config)#ipv6 nd ra router-preference high
Console(config)#
```

ipv6 nd ra suppress

This command suppresses router advertisement transmissions on an interface. Use the **no** form to re-enable router advertisements.

Syntax

[**no**] **ipv6 nd ra suppress**

Command Mode

Interface Configuration (VLAN, IPv6/v4 Tunnel)

Default Setting

Not suppressed

Command Usage

This command suppresses periodic unsolicited router advertisements. It does not suppress advertisements sent in response to a router solicitation.

Example

The following suppresses router advertisements on the current interface:

```
Console(config)#interface vlan 1
Console(config)#ipv6 nd ra suppress
Console(config)#
```

clear ipv6 neighbors

This command deletes all dynamic entries in the IPv6 neighbor discovery cache.

Command Mode

Privileged Exec

Example

The following deletes all dynamic entries in the IPv6 neighbor cache:

```
Console#clear ipv6 neighbors
Console#
```

show ipv6 nd raguard

This command displays the configuration setting for RA Guard.

Syntax

show ipv6 nd raguard [*interface*]

interface

ethernet *unit/port*

unit - Unit identifier. (Range: 1)

port - Port number. (Range: 1-28)

port-channel *channel-id* (Range: 1-8)

Command Mode

Privileged Exec

Example

```
Console#show ipv6 nd raguard interface ethernet 1/1
Interface RA Guard
--------- --------
Eth 1/ 1  Yes
Console#
```

show ipv6 neighbors

This command displays information in the IPv6 neighbor discovery cache.

Syntax

show ipv6 neighbors [**vlan** *vlan-id* | *ipv6-address*]

vlan-id - VLAN ID (Range: 1-4094)

ipv6-address - The IPv6 address of a neighbor device. You can specify either a link-local or global unicast address formatted according to RFC 2373 “IPv6 Addressing Architecture,” using 8 colon-separated 16-bit hexadecimal values. One double colon may be used in the address to indicate the appropriate number of zeros required to fill the undefined fields.

DEFAULT SETTING

All IPv6 neighbor discovery cache entries are displayed.

COMMAND MODE

Privileged Exec

EXAMPLE

The following shows all known IPv6 neighbors for this switch:

```
Console#show ipv6 neighbors
State: I1 - Incomplete, I2 - Invalid, R - Reachable, S - Stale, D - Delay,
       P1 - Probe, P2 - Permanent, U - Unknown
IPv6 Address                            Age       Link-layer Addr   State VLAN
FE80::2E0:CFF:FE9C:CA10                 4         00-E0-0C-9C-CA-10     R    1
Console#
```

Table 242: show ipv6 neighbors - display description

Field	Description
IPv6 Address	IPv6 address of neighbor
Age	The time since the address was verified as reachable (in seconds). A static entry is indicated by the value "Permanent."
Link-layer Addr	Physical layer MAC address.
State	The following states are used for dynamic entries: I1 (Incomplete) - Address resolution is being carried out on the entry. A neighbor solicitation message has been sent to the multicast address of the target, but it has not yet returned a neighbor advertisement message. I2 (Invalid) - An invalidated mapping. Setting the state to invalid dis-associates the interface identified with this entry from the indicated mapping (RFC 4293). R (Reachable) - Positive confirmation was received within the last ReachableTime interval that the forward path to the neighbor was functioning. While in REACH state, the device takes no special action when sending packets. S (Stale) - More than the ReachableTime interval has elapsed since the last positive confirmation was received that the forward path was functioning. While in STALE state, the device takes no action until a packet is sent. D (Delay) - More than the ReachableTime interval has elapsed since the last positive confirmation was received that the forward path was functioning. A packet was sent within the last DELAY_FIRST_PROBE_TIME interval. If no reachability confirmation is received within this interval after entering the DELAY state, the switch will send a neighbor solicitation message and change the state to PROBE. P1 (Probe) - A reachability confirmation is actively sought by resending neighbor solicitation messages every RetransTimer interval until confirmation of reachability is received. U (Unknown) - Unknown state. The following states are used for static entries: I1 (Incomplete)-The interface for this entry is down. R (Reachable) - The interface for this entry is up. Reachability detection is not applied to static entries in the IPv6 neighbor discovery cache. P2 (Permanent) - Indicates a static entry.
VLAN	VLAN interface from which the address was reached.

RELATED COMMANDS

show mac-address-table (1273)

IPV6 TO IPV4 TUNNELS

This switch supports connection between isolated IPv6 nodes over IPv4 networks using manually configured tunnels (RFC 2893), as well as the connection of isolated IPv6 domains over IPv4 clouds without explicit tunnel configuration (RFC 3056).

Table 243: IPv6 to IPv4 Tunnelling Commands

Command	Function	Mode
interface tunnel	Configures a tunnel interface and enters tunnel configuration mode	GC
ipv6 address	Configures an IPv6 global unicast address, and enables IPv6 on an interface	IC (tunnel)
ipv6 address link-local	Configures an IPv6 link-local address for an interface and enables IPv6 on the interface	IC (tunnel)
ipv6 address eui-64	Configures an IPv6 global unicast address for an interface using an EUI-64 interface ID in the low order 64 bits, and enables IPv6 on the interface	IC (tunnel)
tunnel destination*	Configures the IPv4 address of a tunnel destination	IC (tunnel)
tunnel mode ipv6ip	Configures the tunnel mode to manual configuration or 6-to-4 automatic tunneling	IC (tunnel)
tunnel source vlan	Sets the VLAN to which a tunnel source is assigned	IC (tunnel)
tunnel ttl	Configures the TTL value in the IPv4 header of a packet used for tunneling IPv6 traffic	IC (tunnel)
show ipv6 tunnel	Displays the status and configuration settings for all IPv6 over IPv4 tunnels	PE

* The tunnel destination only applies to manually configured tunneling (RFC 2893).

COMMAND USAGE

To create a manually configured or automatically configured tunnel, follow these steps:

1. Configure a VLAN with the vlan command.

2. Assign the ports which will use this VLAN for local services, and those which will form the entry point for the IPv6 over IPv4 tunnel (using the switchport allowed vlan command.

3. Assign an IPv4 address to the VLAN to serve as the source (or local end point) of the tunnel using the ip address command.

4. Create an IPv6 over IPv4 tunnel using the interface tunnel command.

5. Set the tunnel mode to “configured” for host-to-router or router-to-router connections, or “6to4” for router-to-host or host-to-host connections using the tunnel mode ipv6ip command.

6. For "configured" tunnel mode, specify the IPv4 address of the far end of the tunnel using the tunnel destination command.

7. Bind the tunnel to a VLAN with the tunnel source vlan command.

8. Assign an IPv6 global unicast address to the tunnel using the ipv6 address command.

9. Then check your configuration settings using the show ipv6 tunnel command, and the interface status of the tunnel using the show ipv6 interface or show ipv6 interface brief command.

interface tunnel

This command configures an IPv6 to IPv4 tunnel interface and enters tunnel configuration mode. Use the **no** form with a tunnel number to remove a tunnel, or without a tunnel number to remove all tunnels.

SYNTAX

interface tunnel *tunnel-number*

no interface tunnel [*tunnel-number*]

tunnel-number - Tunnel interface identifier. (Range: 1-16)

DEFAULT SETTING

None

COMMAND MODE

Global Configuration

COMMAND USAGE

- Although this command is labeled with the name "tunnel," it allows configuration of either a manually configured IPv6 over IPv4 transport network based on RFC 2893, or of an automatic method of transporting IPv6 traffic over IPv4 clouds without explicit tunnels using RFC 3056.

- Configured IPv6 over IPv4 tunneling uses point-to-point tunnels by encapsulating IPv6 packets within IPv4 headers to carry them over IPv4 routing infrastructures.

- Transporting IPv6 over IPv4 clouds (based on RFC 3056) defines a method for assigning a unique IPv6 address prefix to any site that currently has at least one globally unique IPv4 address, and specifies an encapsulation mechanism for transmitting IPv6 packets using such a prefix over the global IPv4 network.

EXAMPLE

```
Console(config)#interface tunnel 1
Console(config-if)#
```

tunnel destination

This command sets the IPv4 address of a tunnel destination (or far end-point of a tunnel). Use the **no** form to remove the assigned IPv4 address.

SYNTAX

tunnel destination *ip-address*

no tunnel destination

ip-address - IPv4 address of the device at the far end of the tunnel.

DEFAULT SETTING

None

COMMAND MODE

Interface Configuration (IPv6/v4 Tunnel)

COMMAND USAGE

- This command is only applicable to the "configured" tunnel mode (see the tunnel mode ipv6ip command).

- When an IPv6 packet is transmitted over a tunnel, the tunnel end-point address configured by this command is used as the destination address for the encapsulating IPv4 header.

- The determination of which packets to tunnel is based on information in the routing table, which directs packets based on their destination address using the prefix mask and match technique.

- IPv6/IPv4 hosts that are connected to data links with no IPv6 routers may use a configured tunnel to reach an IPv6 router. This tunnel allows the host to communicate with the rest of the IPv6 Internet (i.e., nodes with IPv6-native addresses). If the IPv4 address of an IPv6/IPv4 router bordering the IPv6 backbone is known, this can be used as the tunnel end-point address. This tunnel can be configured into the routing table as an IPv6 "default route." That is, all IPv6 destination addresses will match the route and could potentially traverse the tunnel. Since the "mask length" of such a default route is zero, it will be used only if there are no other routes with a longer mask that match the destination. Note that the default configured tunnel can also be used in conjunction with 6to4 automatic tunneling.

- The tunnel end-point address of a default tunnel could be the IPv4 address of one IPv6/IPv4 router at the border of the IPv6 backbone. Alternatively, the tunnel end point could be an IPv4 "anycast address." Using this approach, multiple IPv6/IPv4 routers at the border advertise IPv4 reachability to the same IPv4 address. All of these routers accept packets to this address as their own, and will decapsulate IPv6 packets tunneled to this address. When an IPv6/IPv4 node sends an encapsulated packet to this address, it will be delivered to only one of the border routers, usually the closest one.

- Care must be taken when using a default tunnel to prevent different IPv4 fragments from arriving at different routers for reassembly. This can be prevented by either avoiding fragmentation of the encapsulated packets (by ensuring an IPv4 MTU of at least 1300 bytes is used) or by preventing frequent changes to IPv4 routing.

- Packets delivered to transport protocols on the decapsulating node should not be subject to ingress filtering. For bidirectionally configured tunnels this is done by verifying that the source address is the IPv4 address of the other end of the tunnel. For unidirectionally configured tunnels, the decapsulating node must be configured with a list of source IPv4 address prefixes that are acceptable. Such a list must default to not having any entries, i.e. the node has to be explicitly configured to forward decapsulated packets received over unidirectionally configured tunnels.

EXAMPLE

```
Console(config)#interface tunnel 2
Console(config-if)#tunnel destination 192.168.1.5
Console(config-if)#
```

tunnel mode ipv6ip

This command sets the tunnel mode to manual configuration or 6-to-4 automatic tunneling. Use the **no** form to restore the default setting.

SYNTAX

tunnel mode ipv6ip {**configured** | **6to4**}

no tunnel mode ipv6ip

configured - Configured IPv6 over IPv4 tunneling using point-to-point tunnels by encapsulating IPv6 packets within IPv4 headers to carry them over IPv4 routing infrastructures (based on RFC 2893).

6to4 - Transports IPv6 over IPv4 clouds by assigning a unique IPv6 address prefix to any site that currently has at least one globally unique IPv4 address, and specifying an encapsulation mechanism for transmitting IPv6 packets using such a prefix over the global IPv4 network. (This method is based on RFC 3056.)

DEFAULT SETTING

configured

COMMAND MODE

Interface Configuration (IPv6/v4 Tunnel)

COMMAND USAGE

- Configured tunneling of IPv6 over IPv4 based on RFC 2893 uses point-to-point tunnels made by encapsulating IPv6 packets within IPv4 headers to carry them over IPv4 routing infrastructures. These tunnels can be either unidirectional or bidirectional. Bidirectionally configured tunnels behave as virtual point-to-point links. When using configured tunnels, the IPv4 tunnel end-point address must be manually configured on the encapsulating node with the tunnel destination command.

The 6to4 mechanism is typically implemented almost entirely in routers bordering between IPv4 and IPv6 domains.

The tunnel end-point address of a 6to4 tunnel is dynamically determined by the tunnel source (local end-point node) via the IPv6 6to4 address of the packet sent from IPv6 6to4 hosts. The 6to4 end-point address is constructed using "2002:*Public IPv4 Address*::/48" as the IPv6 address prefix. This prefix can be used exactly like any other valid IPv6 prefix, e.g., for "Neighbor Discovery for IP Version 6 (IPv6)" defined in RFC 2461.

- IPv6/IPv4 hosts and routers can tunnel IPv6 datagrams over regions of IPv4 routing topology by encapsulating them within IPv4 packets. Tunneling can be used in a variety of ways, including the following:
  - Router-to-Router: IPv6/IPv4 routers interconnected by an IPv4 infrastructure can tunnel IPv6 packets between themselves. In this case, the tunnel spans one segment of the end-to-end path that the IPv6 packet takes.
  - Host-to-Router: IPv6/IPv4 hosts can tunnel IPv6 packets to an intermediate IPv6/IPv4 router that is reachable via an IPv4 infrastructure. This type of tunnel spans the first segment of the packet's end-to-end path.
  - Host-to-Host: IPv6/IPv4 hosts that are interconnected by an IPv4 infrastructure can tunnel IPv6 packets between themselves. In this case, the tunnel spans the entire end-to-end path that the packet takes; and a host can be either a 6to4 node or native IPv6 host.
  - Router-to-Host: IPv6/IPv4 routers can tunnel IPv6 packets to their final destination IPv6/IPv4 host. This tunnel spans only the last segment of the end-to-end path.

Tunneling techniques are classified according to the mechanism by which the encapsulating node determines the address of the node at the end of the tunnel. In the first two tunneling methods listed above – router-to-router and host-to-router – the IPv6 packet is being tunneled to a router. The end point of this type of tunnel is an intermediate router which must decapsulate the IPv6 packet and forward it on to its final destination. When tunneling to a router, the end point of the tunnel is different from the destination of the packet being tunneled. So the addresses in the IPv6 packet being tunneled can not provide the IPv4 address of the tunnel end point. Instead, the tunnel end-point address must be determined from information configured on the encapsulating node. In other words, "configured tunneling" must be used to explicitly identify the end point.

In the last two tunneling methods – host-to-host and router-to-host – the IPv6 packet is tunneled all the way to its final destination. In this case, the destination address of both the IPv6 packet and the encapsulating IPv4 header identify the same node. This fact can be exploited by encoding information in the IPv6 destination address that will allow the encapsulating node to determine the tunnel end point IPv4 address automatically. "6to4 automatic tunneling" employs this technique, using an special IPv6 address format with an embedded IPv4 address to allow tunneling nodes to automatically derive the tunnel end-point IPv4 address. This eliminates the need to explicitly configure the tunnel end-point address.

- The two tunneling techniques – configured and automatic – differ primarily in how they determine the tunnel end-point address. Most of the underlying mechanisms are the same:
  - The entry node of the tunnel (the encapsulating node) creates an encapsulating IPv4 header and transmits the encapsulated packet.
  - The exit node of the tunnel (the decapsulating node) receives the encapsulated packet, reassembles the packet if needed, removes the IPv4 header, updates the IPv6 header, and processes the received IPv6 packet.

EXAMPLE

```
Console(config)#interface tunnel 2
Console(config-if)#tunnel mode ipv6ip configured
Console(config-if)#
```

tunnel source vlan

This command sets the VLAN to which a tunnel source (or local end-point of a tunnel) is assigned. Use the **no** form to detach the tunnel from the assigned VLAN.

SYNTAX

tunnel source vlan *vlan-id*

no tunnel source vlan

vlan-id - VLAN ID (Range: 1-4094)

DEFAULT SETTING

None

COMMAND MODE

Interface Configuration (IPv6/v4 Tunnel)

COMMAND USAGE

The VLAN assigned to a tunnel must be a L3 VLAN with an IPv4 address. Otherwise, an error message will be displayed on the console.

EXAMPLE

```
Console(config)#interface tunnel 2
Console(config-if)#tunnel source vlan 2
Console(config-if)#
```

tunnel ttl

This command configures the TTL (Time to Live) value stored in the IPv4 header of a packet used for tunneling IPv6 traffic. Use the **no** form to restore the default value.

SYNTAX

tunnel ttl *ttl-value*

no tunnel ttl

ttl-value - The TTL value of the IPv4 encapsulating packet. (Range: 0-255, where zero means that the TTL value is taken from the Hop Limit set in the IP header of the encapsulated IPv6 packet)

DEFAULT SETTING

0

COMMAND MODE

Interface Configuration (IPv6/v4 Tunnel)

COMMAND USAGE

The command sets the hop limit for the IPv4 encapsulating packet. However, note that IPv6 over IPv4 tunnels are modeled as a “single-hop.” That is, the IPv6 hop limit is decremented by only one when an IPv6 packet traverses the tunnel. The single-hop model serves to hide the existence of a tunnel. The tunnel is opaque to users of the network, and is not detectable by network diagnostic tools such as traceroute.

EXAMPLE

```
Console(config)#interface tunnel 2
Console(config-if)#tunnel ttl 5
Console(config-if)#
```

show ipv6 tunnel

This command displays the status and configuration settings for all IPv6 over IPv4 tunnels.

COMMAND MODE

Privileged Exec

EXAMPLE

```
Console#show ipv6 tunnel

Tunnel:1
 Tunnel Current State                         : Up
 Tunnel Source Address                        : [VLAN1]192.168.0.3
 Tunnel Destination Address                   : 192.168.0.2
 Time to Live                                 : 255
 Tunnel Mode (Configured / 6-to-4 / ISATAP)  : Configured

Console#
```

The following example shows the interface status of the configured tunnels.

```
Console#show ipv6 interface
VLAN 1 is up
IPv6 is stale.
Link-local address:
(None)
Global unicast address(es):
(None)
Joined group address(es):
FF02::1:2
FF02::1
IPv6 link MTU is 1500 bytes
ND DAD is enabled, number of DAD attempts: 2.
ND retransmit interval is 1000 milliseconds
ND reachable time is 30000 milliseconds
ND advertised reachable time is 0 milliseconds

Tunnel 1 is up
IPv6 is stale.
Link-local address:
  FE80::C0A8:3/64
Global unicast address(es):
  2002:DB9:2222:7272::72/48, subnet is 2002:DB9:2222::/48
Joined group address(es):
FF02::1
IPv6 link MTU is 0 bytes
ND DAD is enabled, number of DAD attempts: 2.
ND retransmit interval is 1000 milliseconds
ND advertised retransmit interval is 0 milliseconds
ND reachable time is 30000 milliseconds
ND advertised reachable time is 0 milliseconds

Console#show ipv6 interface brief
Interface       VLAN       IPv6       IPv6 Address
--------------- ---------- ---------- ---------------------------------------
VLAN 1          Up         Down       Unassigned
TUNNEL 1        Up         Down       2002:DB9:2222:7272::72/48
TUNNEL 1        Up         Down       FE80::C0A8:3

Console#
```

ND SNOOPING

Neighbor Discover (ND) Snooping maintains an IPv6 prefix table and user address binding table. These tables can be used for stateless address auto-configuration or for address filtering by IPv6 Source Guard.

ND snooping maintains a binding table in the process of neighbor discovery. When it receives an Neighbor Solicitation (NS) packet from a host, it creates a new binding. If it subsequently receives a Neighbor Advertisement (NA) packet, this means that the address is already being used by another host, and the binding is therefore deleted. If it does not receive an NA packet after a timeout period, the binding will be bound to the original host. ND snooping can also maintain a prefix table used for stateless address auto-configuration by monitoring Router Advertisement (RA) packets sent from neighboring routers.

ND snooping can also detect if an IPv6 address binding is no longer valid. When a binding has been timed out, it checks to see if the host still exists by sending an NS packet to the target host. If it receives an NA packet in response, it knows that the target still exists and updates the lifetime of the binding; otherwise, it deletes the binding.

This section describes commands used to configure ND Snooping.

Table 244: ND Snooping Commands

Command	Function	Mode
ipv6 nd snooping	Enables ND snooping globally or on a specified VLAN or range of VLANs	GC
ipv6 nd snooping auto-detect	Enables automatic validation of binding table entries by periodically sending NS messages and awaiting NA replies	GC
ipv6 nd snooping auto-detect retransmit count	Sets the number of times to send an NS message to determine if a binding is still valid	GC
ipv6 nd snooping auto-detect retransmit interval	Sets the interval between sending NS messages to determine if a binding is still valid	GC
ipv6 nd snooping prefix timeout	Sets the time to wait for an RA message before deleting an entry in the prefix table	GC
ipv6 nd snooping max-binding	Sets the maximum number of address entries which can be bound to a port	IC
ipv6 nd snooping trust	Configures a port as a trusted interface from which prefix information in RA messages can be added to the prefix table, or NS messages can be forwarded without validation	IC
clear ipv6 nd snooping binding	Clears all entries in the address binding table	PE
clear ipv6 nd snooping prefix	Clears all entries in the prefix table	PE
show ipv6 nd snooping	Shows configuration settings for ND snooping	PE
show ipv6 nd snooping binding	Shows entries in the binding table	PE
show ipv6 nd snooping prefix	Show entries in the prefix table	PE

ipv6 nd snooping

This command enables ND snooping globally or on a specified VLAN or range of VLANs. Use the **no** form to disable this feature.

SYNTAX

[**no**] **ipv6 nd snooping** [**vlan** {*vlan-id* | *vlan-range*}]

vlan-id - VLAN ID. (Range: 1-4094)

vlan-range - A consecutive range of VLANs indicated by the use a hyphen, or a random group of VLANs with each entry separated by a comma.

DEFAULT SETTING

Disabled

COMMAND MODE

Global Configuration

COMMAND USAGE

- Use this command without any keywords to enable ND snooping globally on the switch. Use the VLAN keyword to enable ND snooping on a specific VLAN or a range of VLANs.

- Once ND snooping is enabled both globally and on the required VLANs, the switch will start monitoring RA messages to build an address prefix table as described below:

  - If an RA message is received on an untrusted interface, it is dropped. If received on a trusted interface, the switch adds an entry in the prefix table according to the Prefix Information option in the RA message. The prefix table records prefix, prefix length, valid lifetime, as well as the VLAN and port interface which received the message.

  - If an RA message is not received updating a table entry with the same prefix for a specified timeout period, the entry is deleted.

- Once ND snooping is enabled both globally and on the required VLANs, the switch will start monitoring NS messages to build a dynamic user binding table for use in Duplicate Address Detection (DAD) or for use by other security filtering protocols (e.g., IPv6 Source Guard) as described below:

  - If an NS message is received on an trusted interface, it is forwarded without further processing.

  - If an NS message is received on an untrusted interface, and the address prefix does not match any entry in the prefix table, it drops the packet.

    If the message does match an entry in the prefix table, it adds an entry to the dynamic user binding table after a fixed delay, and forwards the packet. Each entry in the dynamic binding table includes the link-layer address, IPv6 address, lifetime, as well as the VLAN and port interface which received the message.

- If an RA message is received in response to the original NS message (indicating a duplicate address) before the dynamic binding timeout period expires, the entry is deleted. Otherwise, when the timeout expires, the entry is dropped if the auto-detection process is not enabled.

- If the auto-detection process is enabled, the switch periodically sends an NS message to determine is the client still exists. If it does not receive an RA message in response after the configured timeout, the entry is dropped. If the switch receives an RA message before the timeout expires, it resets the lifetime for the dynamic binding, and the auto-detection process resumes.

EXAMPLE

This example enables ND snooping globally and on VLAN 1.

```
Console(config)#ipv6 nd snooping
Console(config)#ipv6 nd snooping vlan 1
Console(config)#ipv6 nd snooping vlan ?
  <1-4094>  VLAN ID
Console(config)#
```

ipv6 nd snooping auto-detect

This command enables automatic validation of dynamic user binding table entries by periodically sending NS messages and awaiting NA replies. Use the **no** form to disable this feature.

SYNTAX

[**no**] **ipv6 nd snooping auto-detect**

DEFAULT SETTING

Disabled

COMMAND MODE

Global Configuration

COMMAND USAGE

If auto-detection is enabled, the switch periodically sends an NS message to determine is a client listed in the dynamic binding table still exists. If it does not receive an RA message in response after the configured timeout, the entry is dropped. If the switch receives an RA message before the timeout expires, it resets the lifetime for the dynamic binding, and the auto-detection process resumes.

EXAMPLE

```
Console(config)#ipv6 nd snooping auto-detect
Console(config)#
```

ipv6 nd snooping auto-detect retransmit count

This command sets the number of times the auto-detection process sends an NS message to determine if a dynamic user binding is still valid. Use the **no** form to restore the default setting.

SYNTAX

ipv6 nd snooping auto-detect retransmit count *retransmit-times*

no ipv6 nd snooping auto-detect retransmit count

retransmit-times – The number of times to send an NS message to determine if a client still exists. (Range: 1-5)

DEFAULT SETTING

3

COMMAND MODE

Global Configuration

COMMAND USAGE

The timeout after which the switch will delete a dynamic user binding if no RA message is received is set to the retransmit count x the retransmit interval (see the ipv6 nd snooping auto-detect retransmit interval command). Based on the default settings, this is 3 seconds.

EXAMPLE

```
Console(config)#ipv6 nd snooping auto-detect retransmit count 5
Console(config)#
```

ipv6 nd snooping auto-detect retransmit interval

This command sets the interval between which the auto-detection process sends NS messages to determine if a dynamic user binding is still valid. Use the **no** form to restore the default setting.

SYNTAX

ipv6 nd snooping auto-detect retransmit interval *retransmit-interval*

no ipv6 nd snooping auto-detect retransmit interval

retransmit-interval – The interval between which the switch sends an NS message to determine if a client still exists. (Range: 1-10 seconds)

DEFAULT SETTING

1 second

COMMAND MODE

Global Configuration

COMMAND USAGE

The timeout after which the switch will delete a dynamic user binding if no RA message is received is set to the retransmit count (see the ipv6 nd snooping auto-detect retransmit count command) x the retransmit interval. Based on the default settings, this is 3 seconds.

EXAMPLE

```
Console(config)#ipv6 nd snooping auto-detect retransmit interval 5
Console(config)#ipv6 nd snooping auto-detect retransmit interval ?
  <1-10>  Retransmit interval (seconds)
Console(config)#
```

ipv6 nd snooping prefix timeout

This command sets the time to wait for an RA message before deleting an entry in the prefix table. Use the **no** form to restore the default setting.

SYNTAX

ipv6 nd snooping prefix timeout *timeout*

no ipv6 nd snooping prefix timeout

timeout – The time to wait for an RA message to confirm that a prefix entry is still valid. (Range: 3-1800 seconds)

DEFAULT SETTING

Set to the valid lifetime field in received RA packet

COMMAND MODE

Global Configuration

COMMAND USAGE

If ND snooping is enabled and an RA message is received on a trusted interface, the switch will add an entry in the prefix table based upon the Prefix Information contained in the message. If an RA message is not received for a table entry with the same prefix for the specified timeout period, the entry is deleted.

EXAMPLE

```
Console(config)#ipv6 nd snooping prefix timeout 200
Console(config)#
```

ipv6 nd snooping max-binding

This command sets the maximum number of address entries in the dynamic user binding table which can be bound to a port. Use the **no** form to restore the default setting.

SYNTAX

ipv6 nd snooping max-binding *max-bindings*

no ipv6 nd snooping max-binding

max-bindings – The maximum number of address entries in the dynamic user binding table which can be bound to a port. (Range: 1-5)

DEFAULT SETTING

5

COMMAND MODE

Interface Configuration (Ethernet, Port Channel)

EXAMPLE

```
Console(config)#ipv6 nd snooping prefix timeout 200
Console(config)#
```

ipv6 nd snooping trust

This command configures a port as a trusted interface from which prefix information in RA messages can be added to the prefix table, or NS messages can be forwarded without validation. Use the **no** form to restore the default setting.

SYNTAX

[**no**] **ipv6 nd snooping trust**

DEFAULT SETTING

Not trusted

COMMAND MODE

Interface Configuration (Ethernet, Port Channel)

COMMAND USAGE

- In general, interfaces facing toward to the network core, or toward routers supporting the Network Discovery protocol, are configured as trusted interfaces.
- RA messages received from a trusted interface are added to the prefix table and forwarded toward their destination.
- NS messages received from a trusted interface are forwarded toward their destination. Nothing is added to the dynamic user binding table.

EXAMPLE

```
Console(config)#interface ethernet 1/1
Console(config-if)#ipv6 nd snooping trust
Console(config-if)#
```

clear ipv6 nd snooping binding

This command clears all entries in the dynamic user address binding table.

SYNTAX

clear ipv6 nd snooping binding

COMMAND MODE

Privileged Exec

EXAMPLE

```
Console#clear ipv6 nd snooping binding
Console#show ipv6 nd snooping binding
MAC Address    IPv6 Address                                 Lifetime    VLAN Interface
-------------- ------------------------------------- ---------- ---- ---------

Console#
```

clear ipv6 nd snooping prefix

This command clears all entries in the address prefix table.

SYNTAX

clear ipv6 nd snooping prefix [**interface vlan** *vlan_id*]

vlan-id - VLAN ID. (Range: 1-4094)

COMMAND MODE

Privileged Exec

EXAMPLE

```
Console#clear ipv6 nd snooping prefix
Console#show ipv6 nd snooping prefix
Prefix entry timeout: (seconds)
Prefix                                Len Valid-Time Expire     VLAN Interface
------------------------------------- --- ---------- ---------- ---- ---------

Console#
```

show ipv6 nd snooping

This command shows the configuration settings for ND snooping.

SYNTAX

show ipv6 nd snooping

COMMAND MODE

Privileged Exec

EXAMPLE

```
Console#show ipv6 nd snooping
Global ND Snooping status: enabled
ND Snooping auto-detection: disabled
ND Snooping auto-detection retransmit count: 3
ND Snooping auto-detection retransmit interval: 1 (second)
ND Snooping is configured on the following VLANs:
VLAN   1,
Interface           Trusted       Max-binding
---------           ---------     -----------
Eth 1/1             Yes                     1
Eth 1/2             No                      5
Eth 1/3             No                      5
Eth 1/4             No                      5
Eth 1/5             No                      5
:
```

show ipv6 nd snooping binding

This command shows all entries in the dynamic user binding table.

SYNTAX

show ipv6 nd snooping binding

COMMAND MODE

Privileged Exec

EXAMPLE

```
Console#show ipv6 nd snooping binding
MAC Address    IPv6 Address                           Lifetime   VLAN Interface
-------------- -------------------------------------- ---------- ---- ---------
0013-49aa-3926 2001:b001::211:95ff:fe84:cb9e                 100    1 Eth 1/1
0012-cf01-0203 2001::1                                      3400    2 Eth 1/2
Console#
```

show ipv6 nd snooping prefix

This command shows all entries in the address prefix table.

SYNTAX

show ipv6 nd snooping prefix [**interface vlan** *vlan_id*]

vlan-id - VLAN ID. (Range: 1-4094)

COMMAND MODE

Privileged Exec

EXAMPLE

```
Console#show ipv6 nd snooping prefix
Prefix entry timeout: 100 (second)
Prefix                                 Len Valid-Time Expire     VLAN Interface
-------------------------------------- --- ---------- ---------- ---- ---------
2001:b000::                             64    2592000        100    1 Eth 1/1
2001::                                  64        600         34    2 Eth 1/2
Console#
```

50 VRRP Commands

Virtual Router Redundancy Protocol (VRRP) use a virtual IP address to support a primary router and multiple backup routers. The backup routers can be configured to take over the workload if the master router fails, or can also be configured to share the traffic load. The primary goal of router redundancy is to allow a host device which has been configured with a fixed gateway to maintain network connectivity in case the primary gateway goes down.

To configure VRRP, select an interface on each router in the group that will participate in the protocol as the master router or a backup router. To select a specific device as the master router, set the address of this interface as the virtual router address for the group. Now set the same virtual address and a priority on the backup routers, and configure an authentication string. You can also enable the preempt feature which allows a router to take over as the master router when it comes on line if it has a higher priority than the currently active master router.

Table 245: VRRP Commands

Command	Function	Mode
vrrp authentication	Configures a key used to authenticate VRRP packets received from other routers	IC
vrrp ip	Enables VRRP and sets the IP address of the virtual router	IC
vrrp preempt	Configures the router to take over as master virtual router for a VRRP group if it has a higher priority than the current master virtual router	IC
vrrp priority	Sets the priority of this router in the VRRP group	IC
vrrp timers advertise	Sets the interval between successive advertisements by the master virtual router	IC
clear vrrp interface counters	Clears VRRP interface statistics	PE
clear vrrp router counters	Clears VRRP router statistics	PE
show vrrp	Displays VRRP status information	PE
show vrrp interface	Displays VRRP status information for the specified interface	PE
show vrrp interface counters	Displays VRRP statistics for the specified interface	PE
show vrrp router counters	Displays VRRP statistics	PE

vrrp authentication

This command specifies the key used to authenticate VRRP packets received from other routers. Use the **no** form to prevent authentication.

SYNTAX

vrrp *group* **authentication** *key*

no vrrp *group* **authentication**

group - Identifies the virtual router group. (Range: 1-255)

key - Authentication string. (Range: 1-8 alphanumeric characters)

DEFAULT SETTING

No key is defined.

COMMAND MODE

Interface (VLAN)

COMMAND USAGE

- All routers in the same VRRP group must be configured with the same authentication key.
- When a VRRP packet is received from another router in the group, its authentication key is compared to the string configured on this router. If the keys match, the message is accepted. Otherwise, the packet is discarded.
- Plain text authentication does not provide any real security. It is supported only to prevent a misconfigured router from participating in VRRP.

EXAMPLE

```
Console(config-if)#vrrp 1 authentication bluebird
Console(config-if)#
```

vrrp ip

This command enables the Virtual Router Redundancy Protocol (VRRP) on an interface and specifies the IP address of the virtual router. Use the **no** form to disable VRRP on an interface and remove the IP address from the virtual router.

SYNTAX

[**no**] **vrrp** *group* **ip** *ip-address*

group - Identifies the virtual router group. (Range: 1-255)

ip-address - The IP address of the virtual router. This is the IP address that end-hosts set as their default gateway.

DEFAULT SETTING

No virtual router groups are configured.

Command Mode

Interface (VLAN)

Command Usage

- The interfaces of all routers participating in a virtual router group must be within the same IP subnet.
- If the IP address assigned to the virtual router with this command is already configured as the primary address on this interface, this router is considered the Owner, and will assume the role of the Master virtual router in the group.
- This interface is used for two purposes - to send/receive advertisement messages and to forward on behalf of the virtual router when operating as the Master VRRP router.
- VRRP is enabled as soon as this command is entered. If you need to customize any of the other parameters for VRRP such as authentication, priority, or advertisement interval, then first configure these parameters before enabling VRRP.

Example

This example creates VRRP group 1 using the primary interface for VLAN 1 as the VRRP group Owner.

```
Console(config)#interface vlan 1
Console(config-if)#vrrp 1 ip 192.168.1.6
Console(config-if)#
```

vrrp preempt

This command configures the router to take over as the master virtual router for a VRRP group if it has a higher priority than the current acting master router. Use the **no** form to disable preemption.

Syntax

vrrp *group* **preempt** [**delay** *seconds*]

no vrrp *group* **preempt**

group - Identifies the VRRP group. (Range: 1-255)

seconds - The time to wait before issuing a claim to become the master. (Range: 0-120 seconds)

Default Setting

Preempt: Enabled
Delay: 0 seconds

Command Mode

Interface (VLAN)

COMMAND USAGE

- If preempt is enabled, and this backup router has a priority higher than the current acting master, it will take over as the new master. However, note that if the original master (i.e., the owner of the VRRP IP address) comes back on line, it will always resume control as the master.
- The delay can give additional time to receive an advertisement message from the current master before taking control. If the router attempting to become the master has just come on line, this delay also gives it time to gather information for its routing table before actually preempting the currently active router.

EXAMPLE

```
Console(config-if)#vrrp 1 preempt delay 10
Console(config-if)#
```

RELATED COMMANDS

vrrp priority (1716)

vrrp priority

This command sets the priority of this router in a VRRP group. Use the **no** form to restore the default setting.

SYNTAX

vrrp *group* **priority** *level*

no vrrp *group* **priority**

group - Identifies the VRRP group. (Range: 1-255)

level - Priority of this router in the VRRP group. (Range: 1-254)

DEFAULT SETTING

Master: 255
Backup: 100

COMMAND MODE

Interface (VLAN)

COMMAND USAGE

- A router that has a physical interface with the same IP address as that used for the virtual router (that is, the owner of the VRRP IP address) will become the master virtual router. The backup router with the highest priority will become the master router if the current master fails. When the original master router recovers, it will take over as the active master router again.
- If two or more routers are configured with the same VRRP priority, the router with the highest IP address is elected as the new master router if the current master fails.

- If the backup preempt function is enabled with the vrrp preempt command, and a backup router with a priority higher than the current acting master comes on line, this backup router will take over as the new acting master. However, note that if the original master (i.e., the owner of the VRRP IP address) comes back on line, it will always resume control as the master.

- If the virtual IP address for the VRRP group is the same as that of the configured device, the priority will automatically be set to 255 prior to using this command.

EXAMPLE

```
Console(config-if)#vrrp 1 priority 1
Console(config-if)#
```

RELATED COMMANDS

vrrp preempt (1715)

vrrp timers advertise

This command sets the interval at which the master virtual router sends advertisements communicating its state as the master. Use the **no** form to restore the default interval.

SYNTAX

vrrp *group* **timers advertise** *interval*

no vrrp *group* **timers advertise**

group - Identifies the VRRP group. (Range: 1-255)

interval - Advertisement interval for the master virtual router. (Range: 1-255 seconds)

DEFAULT SETTING

1 second

COMMAND MODE

Interface (VLAN)

COMMAND USAGE

- VRRP advertisements from the current master virtual router include information about its priority and current state as the master.

- VRRP advertisements are sent to the multicast address 224.0.0.18. Using a multicast address reduces the amount of traffic that has to processed by network devices that are not part of the designated VRRP group.

- If the master router stops sending advertisements, backup routers will bid to become the master router based on priority. The dead interval before attempting to take over as the master is three times the hello interval plus half a second

EXAMPLE

```
Console(config-if)#vrrp 1 timers advertise 5
Console(config-if)#
```

clear vrrp interface counters

This command clears VRRP system statistics for the specified group and interface.

clear vrrp *group* **interface** *interface* **counters**

group - Identifies a VRRP group. (Range: 1-255)

interface - Identifier of configured VLAN interface. (Range: 1-4094)

DEFAULTS

None

COMMAND MODE

Privileged Exec

EXAMPLE

```
Console#clear vrrp 1 interface 1 counters
Console#
```

clear vrrp router counters

This command clears VRRP system statistics.

COMMAND MODE

Privileged Exec

EXAMPLE

```
Console#clear vrrp router counters
Console#
```

show vrrp

This command displays status information for VRRP.

SYNTAX

show vrrp [**brief** | *group*]

brief - Displays summary information for all VRRP groups on this router.

group - Identifies a VRRP group. (Range: 1-255)

DEFAULTS

None

COMMAND MODE

Privileged Exec

COMMAND USAGE

- Use this command without any keywords to display the full listing of status information for all VRRP groups configured on this router.
- Use this command with the **brief** keyword to display a summary of status information for all VRRP groups configured on this router.
- Specify a group number to display status information for a specific group

EXAMPLE

This example displays the full listing of status information for all groups.

```
Console#show vrrp
 VLAN 1 - Group 1,
 State                             Master
 Virtual IP Address                192.168.1.6
 Virtual MAC Address               00-00-5E-00-01-01
 Advertisement Interval            5 sec
 Preemption                        Enabled
 Min Delay                         10 sec
 Priority                          255
 Authentication                    SimpleText
 Authentication Key                bluebird
 Master Router                     192.168.1.6
 Master Priority                   255
 Master Advertisement Interval     5 sec
 Master Down Interval              15
Console#
```

Table 246: show vrrp - display description

Field	Description
State	VRRP role of this interface (master or backup)
Virtual IP address	Virtual address that identifies this VRRP group
Virtual MAC address	Virtual MAC address derived from the owner of the virtual IP address
Advertisement interval	Interval at which the master virtual router advertises its role as the master
Preemption	Shows whether or not a higher priority router can preempt the current acting master
Min delay	Delay before a router with a higher priority can preempt the current acting master
Priority	Priority of this router
Authentication	Authentication mode used to verify VRRP packets
Authentication key	Key used to authenticate VRRP packets received from other routers
Master Router	IP address of the router currently acting as the VRRP group master
Master priority	The priority of the router currently acting as the VRRP group master

Table 246: show vrrp - display description (Continued)

Field	**Description**
Master Advertisement interval	The advertisement interval configured on the VRRP master.
Master down interval	The down interval configured on the VRRP master (This interval is used by all the routers in the group regardless of their local settings)

This example displays the brief listing of status information for all groups.

```
Console#show vrrp brief
Interface   Grp    State    Virtual Addr     Interval   Preempt  Priority
---------- ----- -------- ---------------- ----------- --------- --------
VLAN 1         1  Master       192.168.0.3           1  E            255
Console#
```

Table 247: show vrrp brief - display description

Field	**Description**
Interface	VLAN interface
Grp	VRRP group
State	VRRP role of this interface (master or backup)
Virtual Addr	Virtual address that identifies this VRRP group
Interval	Interval at which the master virtual router advertises its role as the master
Preempt	Shows whether or not a higher priority router can preempt the current acting master
Priority	Priority of this router

show vrrp interface

This command displays status information for the specified VRRP interface.

SYNTAX

show vrrp interface vlan *vlan-id* [**brief**]

vlan-id - Identifier of configured VLAN interface. (Range: 1-4094)

brief - Displays summary information for all VRRP groups on this router.

DEFAULTS

None

COMMAND MODE

Privileged Exec

EXAMPLE

This example displays the full listing of status information for VLAN 1.

```
Console#show vrrp interface vlan 1
 Vlan 1 - Group 1,
 State                            Master
 Virtual IP Address               192.168.1.6
 Virtual MAC Address              00-00-5E-00-01-01
 Advertisement Interval           5 sec
 Preemption                       Enabled
 Min Delay                        10 sec
 Priority                         1
 Authentication                   SimpleText
 Authentication Key               bluebird
 Master Router                    192.168.1.6
 Master Priority                  1
 Master Advertisement Interval    5 sec
 Master Down Interval             15
Console#
```

* Refer to the show vrrp command for a description of the display items.

show vrrp interface counters

This command displays counters for VRRP protocol events and errors that have occurred for the specified group and interface.

show vrrp *group* **interface vlan** *interface* **counters**

group - Identifies a VRRP group. (Range: 1-255)

interface - Identifier of configured VLAN interface. (Range: 1-4094)

DEFAULTS

None

COMMAND MODE

Privileged Exec

EXAMPLE

```
Console#show vrrp 1 interface vlan 1 counters
 Total Number of Times Transitioned to MASTER                       : 6
 Total Number of Received Advertisements Packets                    : 0
 Total Number of Received Error Advertisement Interval Packets      : 0
 Total Number of Received Authentication Failures Packets           : 0
 Total Number of Received Error IP TTL VRRP Packets                 : 0
 Total Number of Received Priority 0 VRRP Packets                   : 0
 Total Number of Sent Priority 0 VRRP Packets                       : 5
 Total Number of Received Invalid Type VRRP Packets                 : 0
 Total Number of Received Error Address List VRRP Packets           : 0
 Total Number of Received Invalid Authentication Type VRRP Packets  : 0
 Total Number of Received Mismatch Authentication Type VRRP Packets : 0
 Total Number of Received Error Packet Length VRRP Packets          : 0
Console#
```

* Refer to "Displaying VRRP Group Statistics" on page 767 for a description of the display items.

show vrrp router counters

This command displays counters for errors found in VRRP protocol packets.

COMMAND MODE

Privileged Exec

EXAMPLE

Note that unknown errors indicate VRRP packets received with an unknown or unsupported version number.

```
Console#show vrrp router counters
 Total Number of VRRP Packets with Invalid Checksum : 0
 Total Number of VRRP Packets with Unknown Error    : 0
 Total Number of VRRP Packets with Invalid VRID     : 0
Console#
```

51 IP Routing Commands

After network interfaces are configured for the switch, the paths used to send traffic between different interfaces must be set. If routing is enabled on the switch, traffic will automatically be forwarded between all of the local subnetworks. However, to forward traffic to devices on other subnetworks, either configure fixed paths with static routing commands, or enable a dynamic routing protocol that exchanges information with other routers on the network to automatically determine the best path to any subnetwork.

This section includes commands for both static and dynamic routing. These commands are used to connect between different local subnetworks or to connect the router to the enterprise network.

Table 248: IP Routing Commands

Command Group	Function
Global Routing Configuration	Configures global parameters for static and dynamic routing, displays the routing table and statistics for protocols used to exchange routing information
Routing Information Protocol (RIP)	Configures global and interface specific parameters for RIP
Open Shortest Path First (OSPFv2)	Configures global and interface specific parameters for OSPFv2
Open Shortest Path First (OSPFv3)	Configures global and interface specific parameters for OSPFv3
Border Gateway Protocol (BGPv4)	Configures general and neighbor specific parameters for BGPv4
Policy-based Routing for BGP	Configures next-hop routing policies based on criteria defined in various routing parameters

Global Routing Configuration

Table 249: Global Routing Configuration Commands

Command	Function	Mode
IPv4 Commands		
ip route	Configures static routes	GC
maximum-paths	Sets the maximum number of paths allowed	GC
show ip host-route	Displays the interface associated with known routes	PE
show ip route	Displays specified entries in the routing table	PE
show ip route database	Displays static or dynamically learned entries in the routing table	PE

Table 249: Global Routing Configuration Commands (Continued)

Command	Function	Mode
show ip route summary	Displays summary information for the routing table	PE
show ip traffic	Displays statistics for IP, ICMP, UDP, TCP and ARP protocols	PE
IPv6 Commands		
ipv6 route	Configures static routes	GC
show ipv6 route	Displays specified entries in the routing table	PE

IPv4 Commands

ip route

This command configures static routes. Use the **no** form to remove static routes.

SYNTAX

ip route *destination-ip netmask next-hop* [*distance*]

no ip route {*destination-ip netmask next-hop* | *****}

destination-ip – IP address of the destination network, subnetwork, or host.

netmask - Network mask for the associated IP subnet. This mask identifies the host address bits used for routing to specific subnets.

next-hop – IP address of the next hop router used for this route.

distance – An administrative distance indicating that this route can be overridden by dynamic routing information if the distance of the dynamic route is less than that configured for the static route. Note that the default administrative distances used by the dynamic unicast routing protocols is 110 for OSPF, 120 for RIP, 20 for eBGP, and 200 for iBGP. (Range: 1-255, Default: 1)

***** – Removes all static routing table entries.

DEFAULT SETTING

No static routes are configured.

COMMAND MODE

Global Configuration

COMMAND USAGE

- Up to 512 static routes can be configured.
- Up to eight equal-cost multipaths (ECMP) can be configured for static routing using the maximum-paths command.
- If an administrative distance is defined for a static route, and the same destination can be reached through a dynamic route at a lower administration distance, then the dynamic route will be used.

- If both static and dynamic paths have the same lowest cost, the first route stored in the routing table, either statically configured or dynamically learned via a routing protocol, will be used.

- Static routes are included in RIP, OSPF or BGP updates periodically sent by the router if this feature is enabled by the RIP, OSPF or BGP **redistribute** command (see page 1739, page 1760, page 1849 respectively).

EXAMPLE

This example forwards all traffic for subnet 192.168.1.0 to the gateway router 192.168.5.254, using the default metric of 1.

```
Console(config)#ip route 192.168.1.0 255.255.255.0 192.168.5.254
Console(config)#
```

maximum-paths

This command sets the maximum number of paths allowed. Use the **no** form to restore the default settings.

SYNTAX

maximum-paths *path-count*

no maximum-paths

path-count - The maximum number of equal-cost paths to the same destination that can be installed in the routing table. (Range: 1-8)

DEFAULT SETTING

Enabled, 4 paths

COMMAND MODE

Global Configuration

EXAMPLE

```
switch(config)#maximum-paths 8
switch(config)#
```

show ip host-route

This command displays the interface associated with known routes.

COMMAND MODE

Privileged Exec

EXAMPLE

```
Console#show ip host-route
 IP Address      MAC Address       VLAN Port
 --------------- ----------------- ---- -------
 192.168.0.99    00-E0-29-94-34-64    1 1/1
 192.168.1.250   00-00-30-01-01-01    3 1/ 1
 10.2.48.2       00-00-30-01-01-02    1 1/ 1
 10.2.5.6        00-00-30-01-01-03    1 1/ 2
 10.3.9.1        00-00-30-01-01-04    2 1/ 3
Console#
```

Table 250: show ip host-route - display description

Field	Description
IP Address	IP address of the destination network, subnetwork, or host.
MAC Address	The physical layer address associated with the IP address.
VLAN	The VLAN that connects to this IP address.
Port	The port that connects to this IP address.

show ip route

This command displays information in the Forwarding Information Base (FIB).

SYNTAX

show ip route [**bgp** | **connected** | **database** | **ospf** | **rip** | **static** | **summary**]

bgp – Displays external routes imported from the Border Gateway Protocol (BGP) into this routing domain.

connected – Displays all currently connected entries.

database – All known routes, including inactive routes.

ospf – Displays external routes imported from the Open Shortest Path First (OSPF) protocol into this routing domain.

rip – Displays all entries learned through the Routing Information Protocol (RIP).

static – Displays all static entries.

summary – Displays a brief list of summary information about entries in the routing table, including the maximum number of entries supported, the number of connected routes, the total number of routes currently stored in the routing table, and the number of entries in the FIB.

COMMAND MODE

Privileged Exec

COMMAND USAGE

- The FIB contains information required to forward IP traffic. It contains the interface identifier and next hop information for each reachable destination network prefix based on the IP routing table. When routing or topology changes occur in the network, the routing table is updated, and those changes are immediately reflected in the FIB.

  The FIB is distinct from the routing table (or, Routing Information Base), which holds all routing information received from routing peers. The forwarding information base contains unique paths only. It does not contain any secondary paths. A FIB entry consists of the minimum amount of information necessary to make a forwarding decision on a particular packet. The typical components within a forwarding information base entry are a network prefix, a router port identifier, and next hop information.

- This command only displays routes which are currently accessible for forwarding. The router must be able to directly reach the next hop, so the VLAN interface associated with any dynamic or static route entry must be up. Note that routes currently not accessible for forwarding, may still be displayed by using the show ip route database command.

EXAMPLE

In the following example, note that the entry for RIP displays both the distance and metric for this route.

```
Console#show ip route
Codes: C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
      i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default

R        10.1.1.0/24 [120/2] via 192.168.1.10, VLAN1, 00:00:14
C        127.0.0.0/8 is directly connected, lo
C        192.168.1.0/24 is directly connected, VLAN1
Console#
```

show ip route database

This command displays entries in the Routing Information Base (RIB).

COMMAND MODE

Privileged Exec

COMMAND USAGE

The RIB contains all available routes learned through dynamic routing protocols, directly attached networks, and any additionally configured routes such as static routes. The RIB contains the set of all available routes from which optimal entries are selected for use by the Forwarding

Information Base (see Command Usage under the show ip route command).

EXAMPLE

```
Console#show ip route database
Codes: C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
      i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       > - selected route, * - FIB route, p - stale info

C     *> 127.0.0.0/8 is directly connected, lo0
C     *> 192.168.1.0/24 is directly connected, VLAN1

Console#
```

show ip route summary

This command displays summary information for the routing table.

COMMAND MODE

Privileged Exec

EXAMPLE

In the following example the numeric identifier following the routing table name (0) indicates the Forwarding Information Base identifier.

```
Console#show ip route summary
IP routing table name is Default-IP-Routing-Table(0)
IP routing table maximum-paths is 8
Connected       2
Total           2
Console#
```

show ip traffic

This command displays statistics for IP, ICMP, UDP, TCP and ARP protocols.

COMMAND MODE

Privileged Exec

EXAMPLE

```
Console#show ip traffic
IP Statistics:
IP received
                4877 total received
                     header errors
                     unknown protocols
                     address errors
                     discards
                4763 delivers
                     reassembly request datagrams
                     reassembled succeeded
                     reassembled failed
```

```
IP sent
                     forwards datagrams
                5927 requests
                     discards
                     no routes
                     generated fragments
                     fragment succeeded
                     fragment failed
ICMP Statistics:
ICMP received
                     input
                     errors
                     destination unreachable messages
                     time exceeded messages
                     parameter problem message
                     echo request messages
                     echo reply messages
                     redirect messages
                     timestamp request messages
                     timestamp reply messages
                     source quench messages
                     address mask request messages
                     address mask reply messages
ICMP sent
                     output
                     errors
                     destination unreachable messages
                     time exceeded messages
                     parameter problem message
                     echo request messages
                     echo reply messages
                     redirect messages
                     timestamp request messages
                     timestamp reply messages
                     source quench messages
                     address mask request messages
                     address mask reply messages
UDP Statistics:
                   2 input
                     no port errors
                     other errors
                     output
TCP Statistics:
                4698 input
                     input errors
                5867 output

Console#
```

IPv6 Commands

ipv6 route

This command configures static IPv6 routes. Use the **no** form to remove static routes.

SYNTAX

[**no**] **ipv6 route** *destination-ipv6-address*/*prefix-length*
{*gateway-address* [*distance*] |
*link-local-address***%***zone-id* [*distance*] |
tunnel *interface-number*}

destination-ipv6-address – The IPv6 address of a destination network, subnetwork, or host. This must be a full IPv6 address including the network prefix and host address bits.

prefix-length - A decimal value indicating how many contiguous bits (from the left) of the address comprise the prefix (i.e., the network portion of the address).

gateway-address – IP address of the next hop router used for this route.

*link-local-address***%***zone-id* – a link-local address, including a zone-id indicating the VLAN identifier after the % delimiter.

distance – An administrative distance indicating that this route can be overridden by dynamic routing information if the distance of the dynamic route is less than that configured for the static route. Note that the default administrative distances used by the dynamic unicast routing protocols is 110 for OSPF, 120 for RIP, 20 for eBGP, and 200 for iBGP. (Range: 1-255, Default: 1)

interface-number – The number of the outgoing tunnel interface used to reach the destination IPv6 address. (Range: 1-16)
See the interface tunnel command for more information.

DEFAULT SETTING

No static routes are configured.

COMMAND MODE

Global Configuration

COMMAND USAGE

- Up to 1K static routes can be configured.
- Up to eight equal-cost multipaths (ECMP) can be configured for static routing using the maximum-paths command.
- If an administrative distance is defined for a static route, and the same destination can be reached through a dynamic route at a lower administration distance, then the dynamic route will be used.
- The default distance of 1 will take precedence over any other type of route, except for local routes.

- If both static and dynamic paths have the same lowest cost, the first route stored in the routing table, either statically configured or dynamically learned via a routing protocol, will be used.

- Static routes are included in RIP, OSPF and BGP updates periodically sent by the router if this feature is enabled by the RIP, OSPF or BGP **redistribute** command (see page 1739, page 1760, page 1849 respectively.

EXAMPLE

This example forwards all traffic for subnet 2001::/64 to the next hop router 2001:DB8:2222:7272::254, using the default metric of 1.

```
Console(config)#ipv6 route 2001::/64 2001:DB8:2222:7272::254
Console(config)#
```

RELATED COMMANDS

show ip route summary (1728)

show ipv6 route

This command displays information in the Forwarding Information Base (FIB).

SYNTAX

show ipv6 route [*ipv6-address*[/*prefix-length*] | **bgp** | **database** | **interface** [**tunnel** *tunnel-number* | **vlan** *vlan-id*] | **local** | **ospf** | **rip** | **static**]

ipv6-address - A full IPv6 address including the network prefix and host address bits.

prefix-length - A decimal value indicating how many contiguous bits (from the left) of the address comprise the prefix (i.e., the network portion of the address).

bgp – Displays external routes imported from the Border Gateway Protocol (BGP) into this routing domain.

database – All known routes, including inactive routes.

interface – Displays all routes that be accessed through this interface.

local – Displays all entries for destinations attached directly to this router.

ospf – Displays external routes imported from the Open Shortest Path First (OSPF) protocol into this routing domain.

rip – Displays all entries learned through the Routing Information Protocol (RIP).

static – Displays all static entries.

tunnel-number - Tunnel interface identifier. (Range: 1-16)

vlan-id - VLAN ID. (Range: 1-4094)

COMMAND MODE

Privileged Exec

COMMAND USAGE

- The FIB contains information required to forward IP traffic. It contains the interface identifier and next hop information for each reachable destination network prefix based on the IP routing table. When routing or topology changes occur in the network, the routing table is updated, and those changes are immediately reflected in the FIB.

  The FIB is distinct from the routing table (or, Routing Information Base), which holds all routing information received from routing peers. The forwarding information base contains unique paths only. It does not contain any secondary paths. A FIB entry consists of the minimum amount of information necessary to make a forwarding decision on a particular packet. The typical components within a forwarding information base entry are a network prefix, a router port identifier, and next hop information.

- This command only displays routes which are currently accessible for forwarding. The router must be able to directly reach the next hop, so the VLAN interface associated with any dynamic or static route entry must be up.

EXAMPLE

In the following example, note that the last entry displays both the distance and metric for this route.

```
Console#show ipv6 route
Codes: C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
      i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
C    ::1/128, lo0
?    FE80::/64, VLAN1 inactive
C    FE80::/64, VLAN1
?    FF00::/8, VLAN1 inactive
O IA 3FFF:1::/32 [110/3]
      via FE80::204:FF:FE05:6, VLAN1

Console#
```

ROUTING INFORMATION PROTOCOL (RIP)

Table 251: Routing Information Protocol Commands

Command	Function	Mode
router rip	Enables the RIP routing protocol	GC
default-information originate	Generates a default external route into an autonomous system	RC
default-metric	Sets the default metric assigned to external routes imported from other protocols	RC
distance	Defines an administrative distance for external routes learned from other routing protocols	RC
maximum-prefix	Sets the maximum number of RIP routes allowed	RC
neighbor	Defines a neighboring router with which to exchange information	RC
network	Specifies the network interfaces that are to use RIP routing	RC
passive-interface	Stops RIP from sending routing updates on the specified interface	RC
redistribute	Redistribute routes from one routing domain to another	RC
timers basic	Sets basic timers, including update, timeout, garbage collection	RC
version	Specifies the RIP version to use on all network interfaces (if not already specified with a receive version or send version command)	RC
ip rip authentication mode	Specifies the type of authentication used for RIP2 packets	IC
ip rip authentication string	Enables authentication for RIP2 packets and specifies keys	IC
ip rip receive version	Sets the RIP receive version to use on a network interface	IC
ip rip receive-packet	Configures the interface to receive of RIP packets	IC
ip rip send version	Sets the RIP send version to use on a network interface	IC
ip rip send-packet	Configures the interface to send RIP packets	IC
ip rip split-horizon	Enables split-horizon or poison-reverse loop prevention	IC
clear ip rip route	Clears specified data from the RIP routing table	PE
show ip protocols rip	Displays RIP process parameters	PE
show ip rip	Displays information about RIP routes and configuration settings	PE

router rip

This command enables Routing Information Protocol (RIP) routing for all IP interfaces on the router. Use the **no** form to disable it.

Syntax

[**no**] **router rip**

Command Mode

Global Configuration

Default Setting

Disabled

Command Usage

- RIP is used to specify how routers exchange routing table information.
- This command is also used to enter router configuration mode.

Example

```
Console(config)#router rip
Console(config-router)#
```

Related Commands

network (1738)

default-information originate

This command generates a default external route into the local RIP autonomous system. Use the **no** form to disable this feature.

Syntax

[**no**] **default-information originate**

Default Setting

Disabled

Command Mode

Router Configuration

Command Usage

This command sets a default route for every Layer 3 interface where RIP is enabled. The response packet to external queries marks each active RIP interface as a default router with the IP address 0.0.0.0.

Example

```
Console(config-router)#default-information originate
Console(config-router)#
```

RELATED COMMANDS

ip route (1724)
redistribute (1739)

default-metric

This command sets the default metric assigned to external routes imported from other protocols. Use the **no** form to restore the default value.

SYNTAX

default-metric *metric-value*

no default-metric

metric-value – Metric assigned to external routes. (Range: 1-15)

DEFAULT SETTING

1

COMMAND MODE

Router Configuration

COMMAND USAGE

- This command does not override the metric value set by the redistribute command. When a metric value has not been configured by the redistribute command, the **default-metric** command sets the metric value to be used for all imported external routes.

- The default metric must be used to resolve the problem of redistributing external routes with incompatible metrics.

- It is advisable to use a low metric when redistributing routes from another protocol into RIP. Using a high metric limits the usefulness of external routes redistributed into RIP. For example, if a metric of 10 is defined for redistributed routes, these routes can only be advertised to routers up to 5 hops away, at which point the metric exceeds the maximum hop count of 15. By defining a low metric of 1, traffic can follow a imported route the maximum number of hops allowed within a RIP domain. However, note that using a low metric can increase the possibility of routing loops For example, this can occur if there are multiple redistribution points and the router learns about the same external network with a better metric from a redistribution point other than that derived from the original source.

EXAMPLE

This example sets the default metric to 5.

```
Console(config-router)#default-metric 5
Console(config-router)#
```

RELATED COMMANDS

redistribute (1739)

distance

This command defines an administrative distance for external routes learned from other routing protocols. Use the **no** form to restore the default setting.

SYNTAX

[**no**] **distance** *distance network-address netmask*

distance - Administrative distance for external routes. External routes are routes for which the best path is learned from a neighbor external to the local RIP autonomous system. Routes with a distance of 255 are not installed in the routing table.
(Range: 1-255)

network-address - IP address of a route entry.

netmask - Network mask for the route. This mask identifies the network address bits used for the associated routing entries.

DEFAULT SETTING

None

COMMAND MODE

Router Configuration

COMMAND USAGE

- Administrative distance is used by the routers to select the preferred path when there are two or more different routes to the same destination from two different routing protocols. A smaller administrative distance indicates a more reliable protocol.

- The administrative distance is applied to all routes learned for the specified network.

EXAMPLE

```
Console(config-router)#distance 2 192.168.3.0 255.255.255.0
Console(config-router)#
```

maximum-prefix

This command sets the maximum number of RIP routes allowed by the system. Use the **no** form to restore the default setting.

SYNTAX

maximum-prefix *maximum-routes*

no maximum-prefix

maximum-routes - The maximum number of RIP routes which can be installed in the routing table. (Range: 1-7168)

DEFAULT SETTING

1024

Command Mode

Router Configuration

Command Usage

All the learned RIP routes may not be copied to the hardware tables in ASIC for fast data forwarding because of hardware resource limitations.

Example

```
Console(config-router)#maximum-prefix 1024
Console(config-router)#
```

neighbor

This command defines a neighboring router with which this router will exchange routing information. Use the **no** form to remove an entry.

Syntax

[**no**] **neighbor** *ip-address*

ip-address - IP address of a neighboring router.

Default Setting

No neighbors are defined.

Command Mode

Router Configuration

Command Usage

- This command can be used to configure a static neighbor (specifically for point-to-point links) with which this router will exchange routing information, rather than relying on broadcast or multicast messages generated by the RIP protocol.
- Use this command in conjunction with the passive-interface command to control the routing updates sent to specific neighbors.

Example

```
Console(config-router)#neighbor 10.2.0.254
Console(config-router)#
```

Related Commands

passive-interface (1738)

network

This command specifies the network interfaces that will be included in the RIP routing process. Use the **no** form to remove an entry.

SYNTAX

[**no**] **network** {*ip-address netmask* | **vlan** *vlan-id*}

ip-address – IP address of a network directly connected to this router.

netmask - Network mask for the route. This mask identifies the network address bits used for the associated routing entries.

vlan-id - VLAN ID. (Range: 1-4094)

DEFAULT SETTING

No networks are specified.

COMMAND MODE

Router Configuration

COMMAND USAGE

RIP only sends and receives updates on interfaces specified by this command. If a network is not specified, the interfaces in that network will not be advertised in any RIP updates.

EXAMPLE

This example includes network interface 10.1.0.0 in the RIP routing process.

```
Console(config-router)#network 10.1.0.0
Console(config-router)#
```

RELATED COMMANDS

router rip (1734)

passive-interface

This command stops RIP from sending routing updates on the specified interface. Use the **no** form to disable this feature.

SYNTAX

[**no**] **passive-interface vlan** *vlan-id*

vlan-id - VLAN ID. (Range: 1-4094)

DEFAULT SETTING

Disabled

COMMAND MODE

Router Configuration

Command Usage

- If this command is used to stop sending routing updates on an interface, the attached subnet will still continue to be advertised to other interfaces, and updates from other routers on that interface will continue to be received and processed.

- Use this command in conjunction with the neighbor command to control the routing updates sent to specific neighbors.

Example

```
Console(config-router)#passive-interface vlan1
Console(config-router)#
```

Related Commands

neighbor (1737)

redistribute

This command imports external routing information from other routing domains (that is, directly connected routes, protocols, or static routes) into the autonomous system. Use the **no** form to disable this feature.

Syntax

[**no**] **redistribute** (**bgp** | **connected** | **ospf** | **static**}
[**metric** *metric-value*]

bgp – Displays external routes imported from the Border Gateway Protocol (BGP) into this routing domain.

connected - Imports routes that are established automatically just by enabling IP on an interface.

ospf - External routes will be imported from the Open Shortest Path First (OSPF) protocol into this routing domain.

static - Static routes will be imported into this routing domain.

metric-value - Metric value assigned to all external routes for the specified protocol. (Range: 1-16)

Default Setting

redistribution - none
metric-value - set by the default-metric command

Command Mode

Router Configuration

Command Usage

- When a metric value has not been configured by the **redistribute** command, the default-metric command sets the metric value to be used for all imported external routes.

- A route metric must be used to resolve the problem of redistributing external routes with incompatible metrics.

- It is advisable to use a low metric when redistributing routes from another protocol into RIP. Using a high metric limits the usefulness of external routes redistributed into RIP. For example, if a metric of 10 is defined for redistributed routes, these routes can only be advertised to routers up to 5 hops away, at which point the metric exceeds the maximum hop count of 15. By defining a low metric of 1, traffic can follow a imported route the maximum number of hops allowed within a RIP domain. However, using a low metric can increase the possibility of routing loops For example, this can occur if there are multiple redistribution points and the router learns about the same external network with a better metric from a redistribution point other than that derived from the original source.

EXAMPLE

This example redistributes routes learned from OSPF and sets the metric for all external routes imported from OSPF to a value of 3.

```
Console(config-router)#redistribute ospf metric 3
Console(config-router)#
```

This example redistributes static routes and sets the metric for all of these routes to a value of 3.

```
Console(config-router)#redistribute static metric 3
Console(config-router)#
```

RELATED COMMANDS

default-metric (1735)

timers basic

This command configures the RIP update timer, timeout timer, and garbage- collection timer. Use the **no** form to restore the defaults.

SYNTAX

timers basic *update timeout garbage*

no timers basic

update – Sets the update timer to the specified value. (Range: 5-2147483647 seconds)

timeout – Sets the timeout timer to the specified value. (Range: 90-360 seconds)

garbage – Sets the garbage collection timer to the specified value. (Range: 60-240 seconds)

DEFAULT SETTING

Update: 30 seconds
Timeout: 180 seconds
Garbage collection: 120 seconds

COMMAND MODE

Router Configuration

COMMAND USAGE

- The *update* timer sets the rate at which updates are sent. This is the fundamental timer used to control all basic RIP processes.
- The *timeout* timer is the time after which there have been no update messages that a route is declared dead. The route is marked inaccessible (i.e., the metric set to infinite) and advertised as unreachable. However, packets are still forwarded on this route.
- After the *timeout* interval expires, the router waits for an interval specified by the *garbage-collection* timer before removing this entry from the routing table. This timer allows neighbors to become aware of an invalid route prior to it being purged by this device.
- Setting the update timer to a short interval can cause the router to spend an excessive amount of time processing updates.
- These timers must be set to the same values for all routers in the network.

EXAMPLE

This example sets the update timer to 40 seconds. The timeout timer is subsequently set to 240 seconds, and the garbage-collection timer to 160 seconds.

```
Console(config-router)#timers basic 15
Console(config-router)#
```

version

This command specifies a RIP version used globally by the router. Use the **no** form to restore the default value.

SYNTAX

version {**1** | **2**}

no version

1 - RIP Version 1

2 - RIP Version 2

DEFAULT SETTING

Receive: Accepts RIPv1 or RIPv2 packets
Send: Route information is broadcast to other routers with RIPv2.

COMMAND MODE

Router Configuration

COMMAND USAGE

- When this command is used to specify a global RIP version, any VLAN interface not previously set by the ip rip receive version or ip rip send version command will use the global RIP version setting.

- When the **no** form of this command is used to restore the default value, any VLAN interface not previously set by the ip rip receive version or ip rip send version command will be set to the default send or receive version.

- Any configured interface settings take precedence over the global settings.

EXAMPLE

This example sets the global version for RIP to send and receive version 2 packets.

```
Console(config-router)#version 2
Console(config-router)#
```

RELATED COMMANDS

ip rip receive version (1744)
ip rip send version (1745)

ip rip authentication mode

This command specifies the type of authentication that can be used for RIPv2 packets. Use the **no** form to restore the default value.

SYNTAX

ip rip authentication mode {**md5** | **text**}

no ip rip authentication mode

md5 - Message Digest 5 (MD5) authentication

text - Indicates that a simple password will be used.

DEFAULT SETTING

Text authentication

COMMAND MODE

Interface Configuration (VLAN)

COMMAND USAGE

- The password to be used for authentication is specified in the ip rip authentication string command.

- This command requires the interface to exchange routing information with other routers based on an authorized password. (Note that this command only applies to RIPv2.)

- For authentication to function properly, both the sending and receiving interface must be configured with the same password or authentication key.

- MD5 is a one-way hash algorithm is that takes the authentication key and produces a 128 bit message digest or "fingerprint." This makes it computationally infeasible to produce two messages having the same message digest, or to produce any message having a given pre-specified target message digest.

EXAMPLE

This example sets the authentication mode to plain text.

```
Console(config)#interface vlan 1
Console(config-if)#ip rip authentication mode text
Console(config-if)#
```

RELATED COMMANDS

ip rip authentication string (1743)

ip rip authentication string

This command specifies an authentication key for RIPv2 packets. Use the **no** form to delete the authentication key.

SYNTAX

ip rip authentication string *key-string*

no ip rip authentication string

key-string - A password used for authentication. (Range: 1-16 characters, case sensitive)

DEFAULT SETTING

No authentication key

COMMAND MODE

Interface Configuration (VLAN)

COMMAND USAGE

- This command can be used to restrict the interfaces that can exchange RIPv2 routing information. (Note that this command does not apply to RIPv1.)

- For authentication to function properly, both the sending and receiving interface must be configured with the same password, and authentication enabled by the ip rip authentication mode command.

EXAMPLE

This example sets an authentication password of “small” to verify incoming routing messages and to tag outgoing routing messages.

```
Console(config)#interface vlan 1
Console(config-if)#ip rip authentication string small
Console(config-if)#
```

RELATED COMMANDS

ip rip authentication mode (1742)

ip rip receive version

This command specifies a RIP version to receive on an interface. Use the **no** form to restore the default value.

SYNTAX

ip rip receive version {**1** | **2**}

no ip rip receive version

1 - Accepts only RIPv1 packets.

2 - Accepts only RIPv2 packets.

DEFAULT SETTING

RIPv1 and RIPv2 packets

COMMAND MODE

Interface Configuration (VLAN)

COMMAND USAGE

- Use this command to override the global setting specified by the RIP version command.
- You can specify the receive version based on these options:
  - Use version 1 or version 2 if all routers in the local network are based on RIPv1 or RIPv2, respectively.
  - Use the default of version 1 or 2 if some routers in the local network are using RIPv2, but there are still some older routers using RIPv1.

EXAMPLE

This example sets the interface version for VLAN 1 to receive RIPv1 packets.

```
Console(config)#interface vlan 1
Console(config-if)#ip rip receive version 1
Console(config-if)#
```

RELATED COMMANDS

version (1741)

ip rip receive-packet

This command configures the interface to receive RIP packets. Use the **no** form to disable this feature.

SYNTAX

[**no**] **ip rip receive-packet**

DEFAULT SETTING

Enabled

COMMAND MODE

Interface Configuration (VLAN)

DEFAULT SETTING

Enabled

COMMAND USAGE

Use the **no** form of this command if it is not required to add any dynamic entries to the routing table for an interface. For example, when only static routes are to be allowed for a specific interface.

EXAMPLE

```
Console(config)#interface vlan 1
Console(config-if)#ip rip receive-packet
Console(config-if)#
```

RELATED COMMANDS

ip rip send-packet (1746)

ip rip send version

This command specifies a RIP version to send on an interface. Use the **no** form to restore the default value.

SYNTAX

ip rip send version {**1** | **2** | **1-compatible**}

no ip rip send version

1 - Sends only RIPv1 packets.

2 - Sends only RIPv2 packets.

1-compatible - Route information is broadcast to other routers with RIPv2.

DEFAULT SETTING

1-compatible (Route information is broadcast to other routers with RIPv2)

COMMAND MODE

Interface Configuration (VLAN)

COMMAND USAGE

- Use this command to override the global setting specified by the RIP version command.
- You can specify the send version based on these options:
  - Use version 1 or version 2 if all routers in the local network are based on RIPv1 or RIPv2, respectively.
  - Use “1-compatible” to propagate route information by broadcasting to other routers on the network using RIPv2, instead of multicasting as normally required by RIPv2. (Using this mode allows older RIPv2 routers which only receive RIP broadcast messages to receive all of the information provided by RIPv2, including subnet mask, next hop and authentication information.)

EXAMPLE

This example sets the interface version for VLAN 1 to send RIPv1 packets.

```
Console(config)#interface vlan 1
Console(config-if)#ip rip send version 1
Console(config-if)#
```

RELATED COMMANDS

version (1741)

ip rip send-packet

This command configures the interface to send RIP packets. Use the **no** form to disable this feature.

[**no**] **ip rip send-packet**

DEFAULT SETTING

Enabled

COMMAND MODE

Interface Configuration (VLAN)

DEFAULT SETTING

Enabled

COMMAND USAGE

The **no** form of this command allows the router to passively monitor route information advertised by other routers attached to the network, without transmitting any RIP updates.

Example

```
Console(config)#interface vlan 1
Console(config-if)#ip rip send-packet
Console(config-if)#
```

Related Commands

ip rip receive-packet (1745)

ip rip split-horizon

This command enables split-horizon or poison-reverse (a variation) on an interface. Use the **no** form to disable this function.

Syntax

ip rip split-horizon [**poisoned**]

no rip ip split-horizon

poisoned - Enables poison-reverse on the current interface.

Command Mode

Interface Configuration (VLAN)

Default Setting

split-horizon poisoned

Command Usage

- Split horizon never propagates routes back to an interface from which they have been acquired.

- Poison reverse propagates routes back to an interface port from which they have been acquired, but sets the distance-vector metrics to infinity. (This provides faster convergence.)

- If split-horizon is disabled with the **no rip ip split-horizon** command, and a loop occurs, the hop count for a route may be gradually incremented to infinity (that is, 16) before the route is deemed unreachable.

Example

This example propagates routes back to the source using poison-reverse.

```
Console(config)#interface vlan 1
Console(config-if)#ip split-horizon poison-reverse
Console(config-if)#
```

clear ip rip route

This command clears specified data from the RIP routing table.

SYNTAX

clear ip rip route {*ip-address netmask* | **all** | **connected** | **ospf** | **rip** | **static**}

ip-address - IP address of a route entry.

netmask - Network mask for the route. This mask identifies the network address bits used for the associated routing entries.

all - Deletes all entries from the routing table.

connected - Deletes all currently connected entries.

ospf - Deletes all entries learned through the Open Shortest Path First routing protocol.

rip - Deletes all entries learned through the Routing Information Protocol.

static - Deletes all static entries.

DEFAULT SETTING

None

COMMAND MODE

Privileged Exec

COMMAND USAGE

Using this command with the “all” parameter clears the RIP table of all routes. To avoid deleting the entire RIP network, use the redistribute connected command to make the RIP network a connected route. To delete the RIP routes learned from neighbors and also keep the RIP network intact, use the “rip” parameter with this command (**clear ip rip route rip**).

EXAMPLE

This example clears one specific route.

```
Console#clear ip rip route 192.168.1.0 255.255.255.0
Console#
```

show ip protocols rip

This command displays RIP process parameters.

COMMAND MODE

Privileged Exec

EXAMPLE

```
Console#show ip protocols rip
Routing Protocol is "rip"
  Sending updates every 30 seconds with +/-5 seconds
  Timeout after 180 seconds, garbage collect after 120 seconds
  Outgoing update filter list for all interface is not set
  Incoming update filter list for all interface is not set
  Default redistribution metric is 1
  Redistributing:
  Default version control: send version by interface set,receive version by
  interface set
    Interface  Send         Recv
    VLAN1      1-compatible 1 2
  Routing for Networks:
    10.0.0.0/24
  Routing Information Sources:
    Gateway         Distance  Last Update  Bad Packets  Bad Routes
    10.0.0.2            120    00:00:13         0           0
  The maximum number of RIP routes allowed: 7872
  Distance: Default is 120
Console#
```

show ip rip

This command displays information about RIP routes and configuration settings. Use this command without any keywords to display all RIP routes.

SYNTAX

show ip rip [**interface** [**vlan** *vlan-id*]]

interface - Shows RIP configuration settings for all interfaces or for a specified interface.

vlan-id - VLAN ID. (Range: 1-4094)

COMMAND MODE

Privileged Exec

EXAMPLE

```
Console#show ip rip

Codes: R - RIP, Rc - RIP connected, Rs - RIP static,
       C - Connected, S - Static, O - OSPF

   Network            Next Hop        Metric From             Interface Time
Rc 192.168.0.0/24                     1                       VLAN1     01:57
Console#show ip rip interface vlan 1
Interface: vlan1
  Routing Protocol: RIP
    Receive RIPv1 and RIPv2 packets
    Send RIPv1 Compatible
    Passive interface: Disabled
    Authentication mode: (None)
    Authentication string: (None)
    Split horizon: Enabled with Poisoned Reverse
    IP interface address: 192.168.0.2/24
Console#
```

OPEN SHORTEST PATH FIRST (OSPFV2)

Table 252: Open Shortest Path First Commands

Command	Function	Mode
General Configuration		
router ospf	Enables or disables OSPFv2	GC
compatible rfc1583	Calculates summary route costs using RFC 1583 (early OSPFv2)	RC
default-information originate	Generates a default external route into an autonomous system	RC
router-id	Sets the router ID for this device	RC
timers spf	Configures the delay after a topology change and the hold time between consecutive SPF calculations	RC
clear ip ospf process	Clears and restarts the OSPF routing process	PE
Route Metrics and Summaries		
area default-cost	Sets the cost for a default summary route sent into a stub or NSSA	RC
area range	Summarizes routes advertised by an ABR	RC
auto-cost reference-bandwidth	Calculates default metrics for an interface based on bandwidth	RC
default-metric	Sets the default metric for external routes imported from other protocols	RC
redistribute	Redistribute routes from one routing domain to another	RC
summary-address	Summarizes routes advertised by an ASBR	RC
Area Configuration		
area nssa	Defines a not-so-stubby that can import external routes	RC
area stub	Defines a stubby area that cannot send or receive LSAs	RC
area virtual-link	Defines a virtual link from an area border routers to the backbone	RC
network area	Assigns specified interface to an area	RC
Interface Configuration		
ip ospf authentication	Specifies the authentication type for an interface	IC
ip ospf authentication-key	Assigns a simple password to be used by neighboring routers	IC
ip ospf cost	Specifies the cost of sending a packet on an interface	IC
ip ospf dead-interval	Sets the interval at which hello packets are not seen before neighbors declare the router down	IC
ip ospf hello-interval	Specifies the interval between sending hello packets	IC
ip ospf message-digest-key	Enables MD5 authentication and sets the key for an interface	IC
ip ospf priority	Sets the router priority used to determine the designated router	IC

Table 252: Open Shortest Path First Commands (Continued)

Command	Function	Mode
ip ospf retransmit-interval	Specifies the time between resending a link-state advertisement	IC
ip ospf transmit-delay	Estimates time to send a link-state update packet over an interface	IC
passive-interface	Suppresses OSPF routing traffic on the specified interface	RC
Display Information		
show ip ospf	Displays general information about the routing processes	PE
show ip ospf border-routers	Displays routing table entries for Area Border Routers (ABR) and Autonomous System Boundary Routers (ASBR)	PE
show ip ospf database	Shows information about different LSAs in the database	PE
show ip ospf interface	Displays interface information	PE
show ip ospf neighbor	Displays neighbor information	PE
show ip ospf route	Displays the OSPF routing table	PE
show ip ospf virtual-links	Displays parameters and the adjacency state of virtual links	PE
show ip protocols ospf	Displays OSPF process parameters	PE

General Configuration

router ospf

This command enables Open Shortest Path First (OSPFv2) routing for all IP interfaces on the router and enters router configuration mode. Use the **no** form to disable OSPF for all processes or for a specified process.

SYNTAX

[**no**] **router ospf** [*process-id*]

process-id - Process ID must be entered when configuring multiple routing instances. (Range: 1-65535; Default: 1)

COMMAND MODE

Global Configuration

DEFAULT SETTING

No routing process is defined.

COMMAND USAGE

- OSPF is used to specify how routers exchange routing table information.
- This command is also used to enter router configuration mode.
- If the process ID is not defined, the default is instance 1.

EXAMPLE

```
Console(config)#router ospf
Console(config-router)#
```

RELATED COMMANDS

network area (1768)

compatible rfc1583

This command calculates summary route costs using RFC 1583 (early OSPFv2). Use the **no** form to calculate costs using RFC 2328 (OSPFv2).

SYNTAX

[**no**] **compatible rfc1583**

COMMAND MODE

Router Configuration

DEFAULT SETTING

RFC 1583 compatible

COMMAND USAGE

- When RFC 1583 compatibility is enabled, only cost is used when choosing among multiple AS-external LSAs advertising the same destination. When disabled, preference is based on type of path (where type 1 external paths are preferred over type 2 external paths, using cost only to break ties (RFC 2328).

- All routers in an OSPF routing domain should use the same RFC for calculating summary routes.

- If there are any OSPF routers in an area exchanging summary information (specifically, ABRs) which have not been upgraded to OSPFv2, this command should be used on the newly upgraded OSPFv2 routers to ensure compatibility with routers still running older OSPFv2 code. Once all systems have been upgraded to newer OSPFv2 code, use the no form of this command to restore compatibility for all systems with RFC 2328.

EXAMPLE

```
Console(config-router)#compatible rfc1583
Console(config-router)#
```

default-information originate

This command generates a default external route into an autonomous system. Use the **no** form to disable this feature.

SYNTAX

default-information originate [**always**] [**metric** *interface-metric*] [**metric-type** *metric-type*]

no default-information originate [**always** | **metric** | **metric-type**]

always - Always advertise itself as a default external route for the local AS regardless of whether the router has a default route. (See "ip route" on page 1724.)

interface-metric - Metric assigned to the default route. (Range: 0-16777214)

metric-type - External link type used to advertise the default route. (Options: Type 1, Type 2)

COMMAND MODE

Router Configuration

DEFAULT SETTING

Disabled
Metric: 20
Metric Type: 2

COMMAND USAGE

- If the **always** parameter is not selected, the router can only advertise a default external route into the AS if it has been configured to import external routes through other routing protocols or static routing, and such a route is known. (See the redistribute command.)

- The metric for the default external route is used to calculate the path cost for traffic passed from other routers within the AS out through the ASBR.

- When you use this command to redistribute routes into a routing domain (i.e., an Autonomous System, this router automatically becomes an Autonomous System Boundary Router (ASBR). However, an ASBR does not, by default, generate a default route into the routing domain.

  - If you use the **always** keyword, the router will advertise itself as a default external route into the AS, even if a default external route does not actually exist. To define a default route, use the ip route command.

  - If you do *not* use the **always** keyword, the router can only advertise a default external route into the AS if the redistribute command is used to import external routes via RIP or static routing, and such a route is known.

- Type 1 route advertisements add the internal cost to the external route metric. Type 2 routes do not add the internal cost metric. When comparing Type 2 routes, the internal cost is only used as a tie-breaker if several Type 2 routes have the same cost.

- This command should not be used to generate a default route for a stub or NSSA. To generate a default route for these area types, use the area stub or area nssa commands.

EXAMPLE

This example assigns a metric of 20 to the default external route advertised into an autonomous system, sending it as a Type 2 external metric.

```
Console(config-router)#default-information originate metric 20 metric-type 2
Console(config-router)#
```

RELATED COMMANDS

ip route (1724)
redistribute (1799)

router-id

This command assigns a unique router ID for this device within the autonomous system for the current OSPF process. Use the **no** form to use the default router identification method (i.e., the highest interface address).

SYNTAX

router-id *ip-address*

no router-id

ip-address - Router ID formatted as an IPv4 address.

COMMAND MODE

Router Configuration

DEFAULT SETTING

Highest interface address

COMMAND USAGE

- This command sets the router ID for the OSPF process specified in the router ospf command.

- The router ID must be unique for every router in the autonomous system. Using the default setting based on the highest interface address ensures that each router ID is unique. (Note that the router ID cannot be set to 255.255.255.255.)

- If this router already has registered neighbors, the new router ID will be used when the router is rebooted, or manually restarted by entering the **no router ospf** followed by the **router ospf** command.

- If the priority values of the routers bidding to be the designated router or backup designated router for an area are equal, the router with the highest ID is elected.

EXAMPLE

```
Console(config-router)#router-id 10.1.1.1
Console(config-router)#
```

RELATED COMMANDS

router ospf (1751)

timers spf

This command configures the delay after receiving a topology change and starting the shortest path first (SPF) calculation, and the hold time between making two consecutive SPF calculations. Use the **no** form to restore the default values.

SYNTAX

timers spf *spf-delay spf-holdtime*

no timers spf

spf-delay - The delay after receiving a topology change notification and starting the SPF calculation. (Range: 0-2147483647 seconds)

spf-holdtime - Minimum time between two consecutive SPF calculations. (Range: 0-2147483647 seconds)

COMMAND MODE

Router Configuration

DEFAULT SETTING

SPF delay: 5 seconds
SPF holdtime: 10 seconds

COMMAND USAGE

- Setting the SPF holdtime to 0 means that there is no delay between consecutive calculations.
- Using a low value allows the router to switch to a new path faster, but uses more CPU processing time.

EXAMPLE

```
Console(config-router)#timers spf 20
Console(config-router)#
```

clear ip ospf process

This command clears and restarts the OSPF routing process. Specify the process ID to clear a particular OSPF process. When no process ID is specified, this command clears all running OSPF processes.

SYNTAX

clear ip ospf [*process-id*] **process**

process-id - Specifies the routing process ID. (Range: 1-65535)

DEFAULT SETTING

Clears all routing processes.

COMMAND MODE

Privileged Exec

EXAMPLE

```
Console#clear ip ospf process
Console#
```

Route Metrics and Summaries

area default-cost

This command specifies a cost for the default summary route sent into a stub or NSSA from an Area Border Router (ABR). Use the **no** form to remove the assigned default cost.

SYNTAX

area *area-id* **default-cost** *cost*

no area *area-id* **default-cost**

area-id - Identifies the stub or NSSA. (The area ID can be in the form of an IPv4 address or as a four octet unsigned integer ranging from 0-4294967295.)

cost - Cost for the default summary route sent to a stub or NSSA. (Range: 0-16777215)

COMMAND MODE

Router Configuration

DEFAULT SETTING

Default cost: 1

COMMAND USAGE

- If the default cost is set to "0," the router will not advertise a default route into the attached stub or NSSA.

Example

```
Console(config-router)#area 10.3.9.0 default-cost 10
Console(config-router)#
```

Related Commands

area stub (1764)
area nssa (1762)

area range

This command summarizes the routes advertised by an Area Border Router (ABR). Use the **no** form to disable this function.

Syntax

[**no**] **area** *area-id* **range** *ip-address* **netmask** [**advertise** | **not-advertise**]

area-id - Identifies an area for which the routes are summarized. The area ID can be in the form of an IPv4 address or as a four octet unsigned integer ranging from 0-4294967295.

ip-address - Base address for the routes to summarize.

netmask - Network mask for the summary route.

advertise - Advertises the specified address range.

not-advertise - The summary is not sent, and the routes remain hidden from the rest of the network.

Command Mode

Router Configuration

Default Setting

Disabled

Command Usage

- This command can be used to summarize intra-area routes and advertise this information to other areas through Area Border Routers (ABRs).

- If the network addresses within an area are assigned in a contiguous manner, the ABRs can advertise a summary route that covers all of the individual networks within the area that fall into the specified range using a single **area range** command.

- If routes are set to be advertised by this command, the router will issue a Type 3 summary LSA for each address range specified by this command.

- This router supports up 64 summary routes for area ranges.

EXAMPLE

This example creates a summary address for all area routes in the range of 10.2.x.x.

```
Console(config-router)#area 10.2.0.0 range 10.2.0.0 255.255.0.0 advertise
Console(config-router)#
```

auto-cost reference-bandwidth

Use this command to calculate the default metrics for an interface based on bandwidth. Use the **no** form to automatically assign costs based on interface type.

SYNTAX

auto-cost reference-bandwidth *reference-value*

no auto-cost reference-bandwidth

reference-value - Bandwidth of interface. (Range: 1-4294967 Mbps)

COMMAND MODE

Router Configuration

DEFAULT SETTING

1 Mbps

COMMAND USAGE

- The system calculates the cost for an interface by dividing the reference bandwidth by the interface bandwidth. By default, the cost is 1 Mbps for all port types (including 100 Mbps ports, 1 Gigabit ports, and 10 Gigabit ports).

- A higher reference bandwidth can be used for aggregate links to indicate preferred use as a lower cost interface.

- The ip ospf cost command overrides the cost calculated by the **auto-cost reference-bandwidth** command.

EXAMPLE

This example sets the reference value to 10000, which generates a cost of 100 for 100 Mbps ports, 10 for 1 Gbps ports and 1 for 10 Gbps ports.

```
Console(config-router)#auto-cost reference-bandwidth 10000
Console(config-router)#
```

RELATED COMMANDS

ip ospf cost (1771)

default-metric

This command sets the default metric for external routes imported from other protocols. Use the **no** form to remove the default metric for the supported protocol types.

SYNTAX

default-metric *metric-value*

no default-metric

metric-value – Metric assigned to all external routes imported from other protocols. (Range: 0-16777214)

COMMAND MODE

Router Configuration

DEFAULT SETTING

20

COMMAND USAGE

- The default metric must be used to resolve the problem of redistributing external routes from other protocols that use incompatible metrics.

- This command does not override the metric value set by the redistribute command. When a metric value has not been configured by the redistribute command, the **default-metric** command sets the metric value to be used for all imported external routes.

EXAMPLE

```
Console(config-router)#default-metric 100
Console(config-router)#
```

RELATED COMMANDS

redistribute (1760)

redistribute

This command redistributes external routing information from other routing protocols and static routes into an autonomous system. Use the **no** form to disable this feature or to restore the default settings.

SYNTAX

redistribute {**bgp** | **connected** | **rip** | **static**} [**metric** *metric-value*] [**metric-type** *type-value*] [**tag** *tag-value*]

no redistribute {**connected** | **rip** | **static**} [**metric**] [**metric-type**] [**tag**]

bgp – Displays external routes imported from the Border Gateway Protocol (BGP) into this routing domain.

connected - Imports all currently connected entries.

rip - Imports entries learned through the Routing Information Protocol.

static - Static routes will be imported into this Autonomous System.

metric-value - Metric assigned to all external routes for the specified protocol. (Range: 0-16777214: Default: 10)

type-value

1 - Type 1 external route

2 - Type 2 external route (default) - Routers do not add internal route metric to external route metric.

tag-value - A tag placed in the AS-external LSA to identify a specific external routing domain, or to pass additional information between routers. (Range: 0-4294967295)

COMMAND MODE

Router Configuration

DEFAULT SETTING

redistribution - none
metric-value - 10
type-metric - 2

COMMAND USAGE

- This command is used to import routes learned from other routing protocols into the OSPF domain, and to generate AS-external-LSAs.

- When you redistribute external routes into an OSPF autonomous system (AS), the router automatically becomes an autonomous system boundary router (ASBR). If the **redistribute** command is used in conjunction with the default-information originate command to generate a “default” external route into the AS, the metric value specified in this command supersedes the metric specified in the default-information originate command.

- Metric type specifies the way to advertise routes to destinations outside the AS through External LSAs. When a Type 1 LSA is received by a router, it adds the internal cost to the external route metric. In other words, the cost of the route from any router within the AS is equal to the cost associated with reaching the advertising ASBR, plus the cost of the external route. When a Type 2 LSA is received by a router, it only uses the external route metric to determine route cost.

- A tag can be used to distinguish between routes learned from different external autonomous systems (other routing protocols). For example, if there are two ASBRs in a routing domain: A and B. ASBR A can be configured to redistribute routes learned from RIP domain 1 (identified by tag 1) and ASBR B can redistribute routes learned from RIP domain 2 (identified by tag 2).

EXAMPLE

This example redistributes routes learned from RIP as Type 1 external routes.

```
Console(config-router)#redistribute rip metric-type 1
Console(config-router)#
```

RELATED COMMANDS

default-information originate (1753)

summary-address

This command aggregates routes learned from other protocols. Use the **no** form to remove a summary address.

SYNTAX

[**no**] **summary-address** *summary-address netmask*

summary-address - Summary address covering a range of addresses.

netmask - Network mask for the summary route.

COMMAND MODE

Router Configuration

DEFAULT SETTING

Disabled

COMMAND USAGE

Redistributing routes from other protocols into OSPF normally requires the router to advertise each route individually in an external LSA. An Autonomous System Boundary Router (ASBR) can be configured to redistribute routes learned from other protocols by advertising an aggregate route into all attached autonomous systems. This helps both to decrease the number of external LSAs and the size of the OSPF link state database.

Example

This example creates a summary address for all routes contained in 192.168.x.x.

```
Console(config-router)#summary-address 192.168.0.0 255.255.0.0
Console(config-router)#
```

Related Commands

area range (1798)
redistribute (1799)

Area Configuration

area nssa

This command defines a not-so-stubby area (NSSA). To remove an NSSA, use the **no** form without any optional keywords. To remove an optional attribute, use the **no** form without the relevant keyword.

Syntax

[**no**] **area** *area-id* **nssa**
[**translator-role** [**candidate** | **never** | **always**]] | [**no-redistribution**] | [**no-summary**] | [**default-information-originate** [**metric** *metric-value* | **metric-type** *type-value*]]

area-id - Identifies the NSSA. The area ID can be in the form of an IPv4 address or as a four octet unsigned integer ranging from 0-4294967295.

translator-role - Indicates NSSA-ABR translator role for Type 5 external LSAs.

candidate - Router translates NSSA LSAs to Type-5 external LSAs if elected.

never - Router never translates NSSA LSAs to Type-5 external LSAs.

always - Router always translates NSSA LSAs to Type-5 external LSAs.

no-redistribution - Use this keyword when the router is an NSSA Area Border Router (ABR) and you want the redistribute command to import routes only into normal areas, and not into the NSSA. In other words, this keyword prevents the NSSA ABR from advertising external routing information (learned via routers in other areas) into the NSSA.

no-summary - Allows an area to retain standard NSSA features, but does not inject inter-area routes into this area.

default-information-originate - When the router is an NSSA Area Border Router (ABR) or an NSSA Autonomous System Boundary Router (ASBR), this parameter causes it to generate Type-7 default LSA into the NSSA. This default provides a route to other areas within the AS for an NSSA ABR, or to areas outside the AS for an NSSA ASBR.

metric-value - Metric assigned to Type-7 default LSAs. (Range: 0-16777214: Default: 1)

type-value

1 - Type 1 external route

2 - Type 2 external route (default) - Routers do not add internal cost to the external route metric.

COMMAND MODE

Router Configuration

DEFAULT SETTING

No NSSA is configured.

COMMAND USAGE

- All routers in a NSSA must be configured with the same area ID.
- An NSSA is similar to a stub, because when the router is an ABR, it can send a default route for other areas in the AS into the NSSA using the **default- information-originate** keyword. However, an NSSA is different from a stub, because when the router is an ASBR, it can import a default external AS route (for routing protocol domains adjacent to the NSSA but not within the OSPF AS) into the NSSA using the **default-information-originate** keyword.
- External routes advertised into an NSSA can include network destinations outside the AS learned via OSPF, the default route, static routes, routes imported from other routing protocols such as RIP, and networks directly connected to the router that are not running OSPF.
- NSSA external LSAs (Type 7) are converted by any ABR adjacent to the NSSA into external LSAs (Type-5), and propagated into other areas within the AS.
- Also, note that unlike stub areas, all Type-3 summary LSAs are always imported into NSSAs to ensure that internal routes are always chosen over Type-7 NSSA external routes.
- This router supports up to 16 total areas (either normal transit areas, stubs, or NSSAs).

EXAMPLE

This example creates a stub area 10.3.0.0, and assigns all interfaces with class B addresses 10.3.x.x to the NSSA. It also instructs the router to generate external LSAs into the NSSA when it is an NSSA ABR or NSSA ASBR.

```
Console(config-router)#area 10.3.0.0 nssa default-information-originate
Console(config-router)#network 10.3.0.0 255.255.0.0 area 10.2.0.0
Console(config-router)#
```

area stub

This command defines a stub area. To remove a stub, use the **no** form without the optional keyword. To remove the summary attribute, use the **no** form with the summary keyword.

SYNTAX

[**no**] **area** *area-id* **stub** [**no-summary**]

area-id - Identifies the stub area. The area ID can be in the form of an IPv4 address or as a four octet unsigned integer ranging from 0-4294967295.

no-summary - Stops an Area Border Router (ABR) from sending summary link advertisements into the stub area.

COMMAND MODE

Router Configuration

DEFAULT SETTING

No stub is configured.

Summary advertisement are sent into the stub.

COMMAND USAGE

- All routers in a stub must be configured with the same area ID.

- Routing table space is saved in a stub by blocking Type-4 AS summary LSAs and Type 5 external LSAs. The default setting for this command completely isolates the stub by blocking Type-3 summary LSAs that advertise the default route for destinations external to the local area or the autonomous system.

- Use the **no-summary** parameter of this command on the ABR attached to the stub to define a totally stubby area. Define an area as a totally stubby area only if routers in the area do not require summary LSAs from other areas.

- Use the area default-cost command to specify the cost of a default summary route sent into a stub by an ABR attached to the stub area.

EXAMPLE

This example creates a stub area 10.2.0.0, and assigns all interfaces with class B addresses 10.2.x.x to the stub.

```
Console(config-router)#area 10.2.0.0 stub
Console(config-router)#network 10.2.0.0 0.255.255.255 area 10.2.0.0
Console(config-router)#
```

RELATED COMMANDS

area default-cost (1756)

area virtual-link

This command defines a virtual link. To remove a virtual link, use the **no** form with no optional keywords. To restore the default value for an attribute, use the **no** form with the required keyword.

SYNTAX

area *area-id* **virtual-link** *router-id*
[**authentication**] [**dead-interval** *seconds*] [**hello-interval** *seconds*] [**retransmit-interval** *seconds*]
[**transmit-delay** *seconds*]

no area area-id virtual-link *router-id*
[**authentication** | **dead-interval** | **hello-interval** | **retransmit-interval** | **transmit-delay**]

area *area-id* **virtual-link** *router-id*
authentication [**message-digest** | **null**]
[**authentication-key** *key* | **message-digest-key** *key-id* **md5** *key*]

no area *area-id* **virtual-link** *router-id*
authentication [**authentication-key** | **message-digest-key** *key-id*]

area *area-id* **virtual-link** *router-id*
[**authentication-key** *key* | **message-digest-key** *key-id* **md5** *key*]

no area *area-id* **virtual-link** *router-id*
[**authentication-key** | **message-digest-key** *key-id*]

area-id - Identifies the transit area for the virtual link.The area ID can be in the form of an IPv4 address or as a four octet unsigned integer ranging from 0-4294967295.

router-id - Router ID of the virtual link neighbor. This specifies the Area Border Router (ABR) at the other end of the virtual link. To create a virtual link, enter this command for an ABR at both ends of the link. One of the ABRs must be next to the isolated area and the transit area at one end of the link, while the other ABR must be next to the transit area and backbone at the other end of the link.

dead-interval *seconds* - Specifies the time that neighbor routers will wait for a hello packet before they declare the router down. This value must be the same for all routers attached to an autonomous system. (Range: 1-65535 seconds; Default: 4 x hello interval, or 40 seconds)

hello-interval *seconds* - Specifies the transmit delay between sending hello packets. Setting the hello interval to a smaller value can reduce the delay in detecting topological changes, but will increase the routing traffic. This value must be the same for all routers attached to an autonomous system. (Range: 1-65535 seconds; Default: 10 seconds)

retransmit-interval *seconds* - Specifies the interval at which the ABR retransmits link-state advertisements (LSA) over the virtual link. The retransmit interval should be set to a conservative value that provides an adequate flow of routing information, but does not produce unnecessary protocol traffic. However, note that this value should be larger for virtual links. (Range: 1-3600 seconds; Default: 5 seconds)

transmit-delay *seconds* - Estimates the time required to send a link-state update packet over the virtual link, considering the transmission and propagation delays. LSAs have their age incremented by this amount before transmission. This value must be the same for all routers attached to an autonomous system. (Range: 1-65535 seconds; Default: 1 second)

authentication - Specifies the authentication mode. If no optional parameters follow this keyword, then plain text authentication is used along with the password specified by the **authentication-key**. If **message-digest** authentication is specified, then the **message-digest-key** and **md5** parameters must also be specified. If the **null** option is specified, then no authentication is performed on any OSPF routing protocol messages.

> **message-digest** - Specifies message-digest (MD5) authentication.
>
> **null** - Indicates that no authentication is used.

authentication-key *key* - Sets a plain text password (up to 8 characters) that is used by neighboring routers on a virtual link to generate or verify the authentication field in protocol message headers. A separate password can be assigned to each network interface. However, this key must be the same for all neighboring routers on the same network (i.e., autonomous system). This key is only used when authentication is enabled for the backbone.

message-digest-key *key-id* **md5** *key* - Sets the key identifier and password to be used to authenticate protocol messages passed between neighboring routers and this router when using message digest (MD5) authentication. The *key-id* is an integer from 0-255, and the *key* is an alphanumeric string up to 16 characters long. If MD5 authentication is used on a virtual link, then it must be enabled on all routers within an autonomous system; and the key identifier and key must also be the same for all routers.

COMMAND MODE

Router Configuration

DEFAULT SETTING

area-id: None
router-id: None
hello-interval: 10 seconds
retransmit-interval: 5 seconds
transmit-delay: 1 second
dead-interval: 40 seconds
authentication-key: None
message-digest-key: None

COMMAND USAGE

- All areas must be connected to a backbone area (0.0.0.0) to maintain routing connectivity throughout the autonomous system. If it not possible to physically connect an area to the backbone, you can use a virtual link. A virtual link can provide a logical path to the backbone for an isolated area, or can be configured as a backup connection that can take over if the normal connection to the backbone fails.

- A virtual link can be configured between any two backbone routers that have an interface to a common non-backbone area. The two routers joined by a virtual link are treated as if they were connected by an unnumbered point-to-point network.

- Any area disconnected from the backbone must include the transit area ID and the router ID for a virtual link neighbor that is adjacent to the backbone.

EXAMPLE

This example creates a virtual link using the defaults for all optional parameters.

```
Console(config-router)#network 10.4.0.0 0.255.255.0.0 area 10.4.0.0
Console(config-router)#area 10.4.0.0 virtual-link 10.4.3.254
Console(config-router)#
```

This example creates a virtual link using MD5 authentication.

```
Console(config-router)#network 10.4.0.0 0.255.255.0.0 area 10.4.0.0
Console(config-router)#area 10.4.0.0 virtual-link 10.4.3.254 message-digest-
  key 5 md5 ld83jdpq
Console(config-router)#
```

RELATED COMMANDS

show ip protocols ospf (1790)

network area

This command defines an OSPF area and the interfaces that operate within this area. Use the **no** form to disable OSPF for a specified interface.

SYNTAX

[**no**] **network** *ip-address netmask* **area** *area-id*

ip-address - Address of the interfaces to add to the area.

netmask - Network mask of the address range to add to the area.

area-id - Area to which the specified address or range is assigned. An OSPF area identifies a group of routers that share common routing information. The area ID can be in the form of an IPv4 address or as a four octet unsigned integer ranging from 0-4294967295.

COMMAND MODE

Router Configuration

DEFAULT SETTING

Disabled

COMMAND USAGE

- An area ID uniquely defines an OSPF broadcast area. The area ID 0.0.0.0 indicates the OSPF backbone for an autonomous system. Each router must be connected to the backbone via a direct connection or a virtual link.
- Set the area ID to the same value for all routers on a network segment using the network mask to add one or more interfaces to an area.
- If an address range is overlapped in subsequent network area commands, the router will use the network area with the address range that most closely matches the interface address. Also, note that if a more specific address range is removed from an area, the interface belonging to that range may still remain active if a less specific address range covering that area has been specified.

EXAMPLE

This example creates the backbone 0.0.0.0 covering class B addresses 10.1.x.x, and a normal transit area 10.2.9.0 covering the class C addresses 10.2.9.x.

```
Console(config-router)#network 10.1.0.0 255.255.0.0 area 0.0.0.0
Console(config-router)#network 10.2.9.0 255.255.255.0 area 10.1.0.0
Console(config-router)#
```

Interface Configuration

ip ospf authentication

This command specifies the authentication type used for an interface. Enter this command without any optional parameters to specify plain text (or simple password) authentication. Use the **no** form to restore the default of no authentication.

SYNTAX

ip ospf [*ip-address*] **authentication** [**message-digest** | **null**]

no ip ospf [*ip-address*] **authentication**

ip-address - IP address of the interface. Enter this parameter to specify a unique authentication type for a primary or secondary IP address associated with the current VLAN. If not specified, the command applies to all networks connected to the current interface.

message-digest - Specifies message-digest (MD5) authentication.

null - Indicates that no authentication is used.

COMMAND MODE

Interface Configuration (VLAN)

DEFAULT SETTING

No authentication

COMMAND USAGE

- Use authentication to prevent routers from inadvertently joining an unauthorized area. Configure routers in the same area with the same password or key. All neighboring routers on the same network with the same password will exchange routing data.

- This command creates a password (key) that is inserted into the OSPF header when routing protocol packets are originated by this device. Assign a separate password to each network for different interfaces.

- When using simple password authentication, a password is included in the packet. If it does not match the password configured on the receiving router, the packet is discarded. This method provides very little security as it is possible to learn the authentication key by snooping on routing protocol packets.

- When using Message-Digest 5 (MD5) authentication, the router uses the MD5 algorithm to verify data integrity by creating a 128-bit message digest from the authentication key. Without the proper key and key-id, it is nearly impossible to produce any message that matches the pre-specified target message digest.

- Before specifying plain-text password authentication for an interface, configure a password with the ip ospf authentication-key command. Before specifying MD5 authentication for an interface, configure the message-digest key-id and key with the ip ospf message-digest-key command.

- The plain-text authentication-key, or the MD5 *key-id* and *key*, must be used consistently throughout the autonomous system.

EXAMPLE

This example enables message-digest authentication for the specified interface.

```
Console(config)#interface vlan 1
Console(config-if)#ip ospf authentication message-digest
Console(config-if)#
```

RELATED COMMANDS

ip ospf authentication-key (1770)
ip ospf message-digest-key (1773)

ip ospf authentication-key

This command assigns a simple password to be used by neighboring routers to verify the authenticity of routing protocol messages. Use the **no** form to remove the password.

SYNTAX

ip ospf [*ip-address*] **authentication-key** *key*

no ip ospf [*ip-address*] **authentication-key**

ip-address - This parameter can be used to indicate a specific IP address connected to the current interface. If not specified, the command applies to all networks connected to the current interface.

key - Sets a plain text password. (Range: 1-8 characters)

COMMAND MODE

Interface Configuration (VLAN)

DEFAULT SETTING

No password

COMMAND USAGE

- Before specifying plain-text password authentication for an interface with the ip ospf authentication command, configure a password with this command.

- This command creates a password (key) that is inserted into the OSPF header when routing protocol packets are originated by this device. Assign a separate password to each network for different interfaces. All neighboring routers on the same network with the same password will exchange routing data.

- A different password can be assigned to each network interface, but the password must be used consistently on all neighboring routers throughout a network (i.e., autonomous system).

EXAMPLE

This example sets a password for the specified interface.

```
Console(config)#interface vlan 1
Console(config-if)#ip ospf authentication-key badboy
Console(config-if)#
```

RELATED COMMANDS

ip ospf authentication (1769)

ip ospf cost

This command explicitly sets the cost of sending a protocol packet on an interface, where higher values indicate slower ports. Use the **no** form to restore the default value.

SYNTAX

ip ospf [*ip-address*] **cost** *cost*

no ip ospf [*ip-address*] **cost**

ip-address - This parameter can be used to indicate a specific IP address connected to the current interface. If not specified, the command applies to all networks connected to the current interface.

cost - Link metric for this interface. Use higher values to indicate slower ports. (Range: 1-65535)

COMMAND MODE

Interface Configuration (VLAN)

DEFAULT SETTING

1

COMMAND USAGE

- The interface cost indicates the overhead required to send packets across a certain interface. This is advertised as the link cost in router link state advertisements.

- Routes are assigned a metric equal to the sum of all metrics for each interface link in the route.

- This router uses a default cost of 1 for all port types. Therefore, if any VLAN contains 10 Gbps ports, you may want to reset the cost for other VLANs which do not contain 10 Gbps ports to a value greater than 1.

EXAMPLE

```
Console(config)#interface vlan 1
Console(config-if)#ip ospf cost 10
Console(config-if)#
```

ip ospf dead-interval

This command sets the interval at which hello packets are not seen before neighbors declare the router down. Use the **no** form to restore the default value.

SYNTAX

ip ospf [*ip-address*] **dead-interval** *seconds*

no ip ospf [*ip-address*] **dead-interval**

ip-address - This parameter can be used to indicate a specific IP address connected to the current interface. If not specified, the command applies to all networks connected to the current interface.

seconds - The maximum time that neighbor routers can wait for a hello packet before declaring the transmitting router down. This interval must be set to the same value for all routers on the network. (Range: 1-65535)

COMMAND MODE

Interface Configuration (VLAN)

DEFAULT SETTING

40, or four times the interval specified by the ip ospf hello-interval command.

COMMAND USAGE

The dead-interval is advertised in the router's hello packets. It must be a multiple of the hello-interval and be the same for all routers on a specific network.

EXAMPLE

```
Console(config)#interface vlan 1
Console(config-if)#ip ospf dead-interval 50
Console(config-if)#
```

RELATED COMMANDS

ip ospf hello-interval (1772)

ip ospf hello-interval

This command specifies the interval between sending hello packets on an interface. Use the **no** form to restore the default value.

SYNTAX

ip ospf [ip-address] **hello-interval** *seconds*

no ip ospf [*ip-address*] **hello-interval**

ip-address - This parameter can be used to indicate a specific IP address connected to the current interface. If not specified, the command applies to all networks connected to the current interface.

seconds - Interval at which hello packets are sent from an interface. This interval must be set to the same value for all routers on the network. (Range: 1-65535)

COMMAND MODE

Interface Configuration (VLAN)

DEFAULT SETTING

10 seconds

COMMAND USAGE

Hello packets are used to inform other routers that the sending router is still active. Setting the hello interval to a smaller value can reduce the delay in detecting topological changes, but will increase routing traffic.

EXAMPLE

```
Console(config)#interface vlan 1
Console(config-if)#ip ospf hello-interval 5
Console(config-if)#
```

ip ospf message-digest-key

This command enables message-digest (MD5) authentication on the specified interface and to assign a key-id and key to be used by neighboring routers. Use the **no** form to remove an existing key.

SYNTAX

ip ospf [*ip-address*] **message-digest-key** *key-id* **md5** *key*

no ip ospf [*ip-address*] **message-digest-key** *key-id*

ip-address - This parameter can be used to indicate a specific IP address connected to the current interface. If not specified, the command applies to all networks connected to the current interface.

key-id - Index number of an MD5 key. (Range: 0-255)

key - Alphanumeric password used to generate a 128 bit message digest or "fingerprint." (Range: 1-16 characters)

COMMAND MODE

Interface Configuration (VLAN)

DEFAULT SETTING

MD5 authentication is disabled.

COMMAND USAGE

- Before specifying MD5 authentication for an interface with the ip ospf authentication command, configure the message-digest key-id and key with this command.

- Normally, only one key is used per interface to generate authentication information for outbound packets and to authenticate incoming packets. Neighbor routers must use the same key identifier and key value.

- When changing to a new key, the router will send multiple copies of all protocol messages, one with the old key and another with the new key. Once all the neighboring routers start sending protocol messages back to this router with the new key, the router will stop using the old key. This rollover process gives the network administrator time to update all the routers on the network without affecting the network connectivity. Once all the network routers have been updated with the new key, the old key should be removed for security reasons.

Example

This example sets a message-digest key identifier and password.

```
Console(config)#interface vlan 1
Console(config-if)#ip ospf message-digest-key 1 md5 aiebel
Console(config-if)#
```

Related Commands

ip ospf authentication (1769)

ip ospf priority

This command sets the router priority used when determining the designated router (DR) and backup designated router (BDR) for an area. Use the **no** form to restore the default value.

Syntax

ip ospf [*ip-address*] **priority** *priority*

no ip ospf [*ip-address*] **priority**

ip-address - This parameter can be used to indicate a specific IP address connected to the current interface. If not specified, the command applies to all networks connected to the current interface.

priority - Sets the interface priority for this router. (Range: 0-255)

Command Mode

Interface Configuration (VLAN)

Default Setting

1

Command Usage

- A designated router (DR) and backup designated router (BDR) are elected for each OSPF network segment based on Router Priority. The DR forms an active adjacency to all other routers in the network segment to exchange routing topology information. If for any reason the DR fails, the BDR takes over this role.

- Set the priority to zero to prevent a router from being elected as a DR or BDR. If set to any value other than zero, the router with the highest priority will become the DR and the router with the next highest priority becomes the BDR. If two or more routers are tied with the same highest priority, the router with the higher ID will be elected.

- If a DR already exists for a network segment when this interface comes up, the new router will accept the current DR regardless of its own priority. The DR will not change until the next time the election process is initiated.

- Configure router priority for multi-access networks only and not for point-to-point networks.

EXAMPLE

```
Console(config)#interface vlan 1
Console(config-if)#ip ospf priority 5
Console(config-if)#
```

ip ospf retransmit-interval

This command specifies the time between resending link-state advertisements (LSAs). Use the **no** form to restore the default value.

SYNTAX

ip ospf [*ip-address*] **retransmit-interval** *seconds*

no ip ospf [*ip-address*] **retransmit-interval**

ip-address - This parameter can be used to indicate a specific IP address connected to the current interface. If not specified, the command applies to all networks connected to the current interface.

seconds - Sets the interval at which LSAs are retransmitted from this interface. (Range: 1-65535)

COMMAND MODE

Interface Configuration (VLAN)

DEFAULT SETTING

5 seconds

COMMAND USAGE

- A router will resend an LSA to a neighbor if it receives no acknowledgment after the specified retransmit interval. The retransmit interval should be set to a conservative value that provides an adequate flow of routing information, but does not produce unnecessary protocol traffic. Note that this value should be larger for virtual links.

- Set this interval to a value that is greater than the round-trip delay between any two routers on the attached network to avoid unnecessary retransmissions.

EXAMPLE

```
Console(config)#interface vlan 1
Console(config-if)#ip ospf retransmit-interval 7
Console(config-if)#
```

ip ospf transmit-delay

This command sets the estimated time to send a link-state update packet over an interface. Use the **no** form to restore the default value.

SYNTAX

ip ospf [*ip-address*] **transmit-delay** *seconds*

no ip ospf [*ip-address*] **transmit-delay**

ip-address - This parameter can be used to indicate a specific IP address connected to the current interface. If not specified, the command applies to all networks connected to the current interface.

seconds - Sets the estimated time required to send a link-state update. (Range: 1-65535)

COMMAND MODE

Interface Configuration (VLAN)

DEFAULT SETTING

1 second

COMMAND USAGE

- LSAs have their age incremented by this delay before transmission. When estimating the transmit delay, consider both the transmission and propagation delays for an interface. Set the transmit delay according to link speed, using larger values for lower-speed links.

- If this delay is not added, the time required to transmit an LSA over the link is not taken into consideration by the routing process. On slow links, the router may send packets more quickly than devices can receive them. To avoid this problem, use the transmit delay to force the router to wait a specified interval between transmissions.

EXAMPLE

```
Console(config)#interface vlan 1
Console(config-if)#ip ospf transmit-delay 6
Console(config-if)#
```

passive-interface

This command suppresses OSPF routing traffic on the specified interface. Use the **no** form to allow routing traffic to be sent and received on the specified interface.

SYNTAX

[**no**] **passive-interface vlan** *vlan-id* [*ip-address*]

vlan-id - VLAN ID. (Range: 1-4094)

ip-address - An IPv4 address configured on this interface.

COMMAND MODE

Router Configuration

DEFAULT SETTING

None

COMMAND USAGE

You can configure an OSPF interface as passive to prevent OSPF routing traffic from exiting or entering that interface. No OSPF adjacency can be formed if one of the interfaces involved is set to passive mode. The specified interface will appear as a stub in the OSPF domain. Also, if you configure an OSPF interface as passive where an adjacency already exists, the adjacency will drop almost immediately.

EXAMPLE

```
Console(config-router)#passive-interface vlan 1
Console(config-router)#
```

Display Information

show ip ospf

This command shows basic information about the routing configuration.

SYNTAX

show ip ospf [*process-id*]

process-id - The ID of the router process for which information will be displayed. (Range: 1-65535)

COMMAND MODE

Privileged Exec

EXAMPLE

```
Console#show ip ospf
 Routing Process "ospf 1" with ID 192.168.1.3
 Process uptime is 20 minutes
 Conforms to RFC2328, and RFC1583Compatibility flag is disabled
 Supports only single TOS(TOS0) routes
 SPF schedule delay 5 secs, Hold time between two SPFs 10 secs
 Refresh timer 10 secs
 Number of incoming current DD exchange neighbors 0/5
 Number of outgoing current DD exchange neighbors 0/5
 Number of external LSA 0. Checksum 0x000000
 Number of opaque AS LSA 0. Checksum 0x000000
 LSDB database overflow limit is 20480
 Number of LSA originated 1
 Number of LSA received 0
 Number of areas attached to this router: 1

    Area 192.168.1.3
        Number of interfaces in this area is 1(1)
        Number of fully adjacent neighbors in this area is 0
        Area has no authentication
        SPF algorithm last executed 00:00:08.739 ago
        SPF algorithm executed 1 times
        Number of LSA 1. Checksum 0x007f09
Console#
```

Table 253: show ip ospf - display description

Field	Description
Routing Process with ID	OSPF process ID and router ID. The router ID uniquely identifies the router in the autonomous system. By convention, this is normally set to one of the router's IP interface addresses.
Process uptime	The time this process has been running
Conforms to RFC2328	Shows that this router is compliant with OSPF Version 2.
RFC1583 Compatibility flag	Shows whether or not compatibility with the RFC 1583 (an earlier version of OSPFv2) is enabled.
Supports only single TOS (TOS0) routes	Optional Type of Service (ToS) specified in OSPF Version 2, Appendix F.1.2 is not supported, so only one cost per interface can be assigned.
SPF schedule delay	Delay between receiving a change to SPF calculation.
Hold time	Sets the hold time between two consecutive SPF calculations.
Refresh timer	The time between refreshing the LSA database.
Number of current DD exchange neighbors	Number of neighbors currently exchanging database descriptor packets.
Number of external LSA	The number of external link-state advertisements (Type 5 LSAs) in the link-state database. These LSAs advertise information about routes outside of the autonomous system.
Checksum	The sum of the LS checksums of the external link-state advertisements contained in the link-state database.
Number of opaque AS LSA	Number of opaque link-state advertisements (Type 9, 10 and 11 LSAs) in the link-state database. These LSAs advertise information about external applications, and are only used by OSPF for the graceful restart process.
Checksum	The sum of the LS checksums of opaque link-state advertisements contained in the link-state database.
LSDB database overflow limit	The maximum number of LSAs allowed in the external database.
Number of LSA originated	The number of new link-state advertisements that have been originated.
Number of LSA received	The number of link-state advertisements that have been received.

Table 253: show ip ospf - display description (Continued)

Field	Description
Number of areas attached to this router	The number of configured areas attached to this router.
Number of interfaces in this area is	The number of interfaces attached to this area
Number of fully adjacent neighbors in this area is	The number of neighbors for which the exchange of recognition protocol messages has been completed and are now fully adjacent
Area has (no) authentication	Shows whether or not the authentication has been enabled
SPF algorithm last executed	The last time the shortest path first algorithm was executed
SPF algorithm executed x times	The number of times the shortest path first algorithm has been executed for this area
Number of LSA	The number of new link-state advertisements that have been originated.
Checksum	The sum of the link-state advertisements' LS checksums contained in this area's link-state database.

show ip ospf border-routers

This command shows entries in the routing table that lead to an Area Border Router (ABR) or Autonomous System Boundary Router (ASBR).

SYNTAX

show ip ospf [*process-id*] **border-routers**

process-id - The ID of the router process for which information will be displayed. (Range: 1-65535)

COMMAND MODE

Privileged Exec

EXAMPLE

```
Console#show ip ospf border-routers
OSPF process 1 internal Routing Table

Codes: i - Intra-area route, I - Inter-area route

i 192.168.0.3 [1] via 192.168.0.3, vlan1, ABR, ASBR, Area 0.0.0.0
Console#
```

show ip ospf database

This command shows information about different OSPF Link State Advertisements (LSAs) stored in this router’s database.

SYNTAX

show ip ospf [*process-id*] **database** [**asbr-summary** | **external** | **network** | **nssa-external** | **router** | **summary**] [**adv-router** *ip-address* | *link-state-id* | **self-originate**]

process-id - The ID of the router process for which information will be displayed. (Range: 1-65535)

adv-router - IP address of the advertising router. If not entered, information about all advertising routers is displayed.

ip-address - IP address of the specified router. If no address is entered, information about the local router is displayed.

link-state-id - The network portion described by an LSA. The *link-state-id* entered should be:

- An IP network number for Type 3 Summary and External LSAs
- A Router ID for Router, Network, and Type 4 AS Summary LSAs

Also, note that when an Type 5 ASBR External LSA is describing a default route, its *link-state-id* is set to the default destination (0.0.0.0).

self-originate - Shows LSAs originated by this router.

asbr-summary - Shows information about Autonomous System Boundary Router summary LSAs.

external - Shows information about external LSAs.

network - Shows information about network LSAs.

nssa-external - Shows information about NSSA external LSAs.

router - Shows information about router LSAs.

summary - Shows information about summary LSAs.

COMMAND MODE

Privileged Exec

EXAMPLES

The following shows output for the **show ip ospf database** command.

```
Console#show ip ospf database

            OSPF Router with ID (192.168.0.2) (Process ID 1)

                Router Link States (Area 0.0.0.0)

Link ID         ADV Router      Age  Seq#       CkSum  Link count
192.168.0.2     192.168.0.2      225 0x80000004 0xdac5 1
192.168.0.3     192.168.0.3      220 0x80000004 0xd8c4 1
```

```
                Net Link States (Area 0.0.0.0)

Link ID         ADV Router      Age  Seq#       CkSum
192.168.0.2     192.168.0.2      225 0x80000001 0x9c0f

                AS External Link States

Link ID         ADV Router      Age  Seq#       CkSum  Route              Tag
0.0.0.0         192.168.0.2      487 0x80000001 0xd491 E2 0.0.0.0/0 0
0.0.0.0         192.168.0.3      222 0x80000001 0xce96 E2 0.0.0.0/0 0

Console#
```

Table 254: show ip ospf database - display description

Field	Description
OSPF Router Process with ID	OSPF process ID and router ID. The router ID uniquely identifies the router in the autonomous system. By convention, this is normally set to one of the router's IP interface addresses.
Link ID	Either a Router ID or an IP Address; it identifies the piece of the routing domain that is being described by the advertisement
ADV Router	Advertising router ID
Age	Age of LSA (in seconds)
Seq#	Sequence number of LSA (used to detect older duplicate LSAs)
CkSum	Checksum of the complete contents of the LSA
Link count	Number of interfaces attached to the router
Route	Type 1 or Type 2 external metric (see the redistribute command) and route
Tag	Optional tag if defined (see the redistribute command)

The following shows output when using the **asbr-summary** keyword.

```
Console#show ip ospf database asbr-summary

            OSPF Router with ID (0.0.0.0) (Process ID 1)

                ASBR-Summary Link States (Area 0.0.0.1)

  LS Age: 0
  Options: 0x2 (*|-|-|-|-|-|E|-)
  LS Type: ASBR-summary-LSA
  Link State ID: 2.1.0.0 (AS Boundary Router address)
  Advertising Router: 192.168.2.1
  LS Seq Number: 80000001
  Checksum: 0x7b67
  Length: 28
  Network Mask: /0
        TOS: 0  Metric: 10

Console#
```

Table 255: show ip ospf database summary - display description

Field	Description
OSPF Router ID	Router ID
LS Age	Age of LSA (in seconds)
Options	Optional capabilities associated with the LSA
LS Type	Summary Links - LSA describes routes to AS boundary routers
Link State ID	Interface address of the autonomous system boundary router
Advertising Router	Advertising router ID
LS Sequence Number	Sequence number of LSA (used to detect older duplicate LSAs)
Checksum	Checksum of the complete contents of the LSA
Length	The length of the LSA in bytes
Network Mask	Address mask for the network
TOS	Type of Service – This router only supports TOS 0 (or normal service)
Metric	Cost of the link

The following shows output when using the **external** keyword.

```
Console#show ip ospf database external
OSPF Router process 100 with ID (10.10.11.50)
AS External Link States LS age: 298
Options: 0x2 (*|-|-|-|-|-|E|-)
LS Type: AS-external-LSA
Link State ID: 10.10.100.0 (External Network Number)
Advertising Router: 10.10.11.50
LS Seq Number: 80000001
Checksum: 0x7033
Length: 36
Network Mask: /24
Metric Type: 2 (Larger than any link state path)
TOS: 0
Metric: 20
Forward Address: 10.10.11.50
External Route Tag: 0


            OSPF Router with ID (0.0.0.0) (Process ID 1)

                AS External Link States

  LS Age: 0
  Options: 0x2 (*|-|-|-|-|-|E|-)
  LS Type: AS-external-LSA
  Link State ID: 0.0.0.0 (External Network Number)
  Advertising Router: 192.168.0.2
  LS Seq Number: 80000005
  Checksum: 0xcc95
  Length: 36
  Network Mask: /0
        Metric Type: 2 (Larger than any link state path)
        TOS: 0
        Metric: 1
        Forward Address: 0.0.0.0
        External Route Tag: 0

Console#
```

Table 256: show ip ospf database external - display description

Field	Description
OSPF Router ID	Router ID
LS Age	Age of LSA (in seconds)
Options	Optional capabilities associated with the LSA
LS Type	AS External Links - LSA describes routes to destinations outside the AS (including default external routes for the AS)
Link State ID	IP network number (External Network Number)
Advertising Router	Advertising router ID
LS Sequence Number	Sequence number of LSA (used to detect older duplicate LSAs)
Checksum	Checksum of the complete contents of the LSA
Length	The length of the LSA in bytes
Network Mask	Address mask for the network
Metric Type	Type 1 or Type 2 external metric (see the redistribute command)
TOS	Type of Service – This router only supports TOS 0 (or normal service)
Metric	Cost of the link
Forward Address	Next hop address. If this field is set to 0.0.0.0, data is forwarded to the originator of the advertisement.
External Route Tag	Optional tag if defined (see the redistribute command)

The following shows output when using the **network** keyword.

```
Console#show ip ospf database network

            OSPF Router with ID (0.0.0.0) (Process ID 1)

                Net Link States (Area 0.0.0.0)

  LS Age: 0
  Options: 0x2 (*|-|-|-|-|-|E|-)
  LS Type: network-LSA
  Link State ID: 192.168.0.2 (address of Designated Router)
  Advertising Router: 192.168.0.2
  LS Seq Number: 80000005
  Checksum: 0x9413
  Length: 32
  Network Mask: /24
        Attached Router: 192.168.0.2
        Attached Router: 192.168.0.3
.
.
.
```

Table 257: show ip ospf database network - display description

Field	Description
OSPF Router ID	Router ID
LS Age	Age of LSA (in seconds)
Options	Optional capabilities associated with the LSA
LS Type	Network Link - LSA describes the routers attached to the network
Link State ID	Interface address of the designated router
Advertising Router	Advertising router ID
LS Sequence Number	Sequence number of LSA (used to detect older duplicate LSAs)
Checksum	Checksum of the complete contents of the LSA
Length	The length of the LSA in bytes
Network Mask	Address mask for the network
Attached Router	List of routers attached to the network; i.e., fully adjacent to the designated router, including the designated router itself

The following shows output when using the **router** keyword.

```
Console#show ip ospf database router

            OSPF Router with ID (0.0.0.0) (Process ID 1)

                Router Link States (Area 0.0.0.0)

  LS Age: 0
  Options: 0x2 (*|-|-|-|-|-|E|-)
  Flags: 0x2 : ASBR
  LS Type: router-LSA
  Link State ID: 192.168.0.2
  Advertising Router: 192.168.0.2
  LS Seq Number: 80000008
  Checksum: 0xd2c9
  Length: 36
    Link connected to: a Transit Network
     (Link ID) Designated Router address: 192.168.0.2
     (Link Data) Router Interface address: 192.168.0.2
      Number of TOS metrics: 0
      TOS 0 Metric: 1
⋮
```

Table 258: show ip ospf database router - display description

Field	Description
OSPF Router ID	Router ID
LS Age	Age of LSA (in seconds)
Options	Optional capabilities associated with the LSA
Flags	Indicate if this router is a virtual link endpoint, an ASBR, or an ABR
LS Type	Router Link - LSA describes the router's interfaces.

Table 258: show ip ospf database router - display description (Continued)

Field	Description
Link State ID	Router ID of the router that originated the LSA
Advertising Router	Advertising router ID
LS Sequence Number	Sequence number of LSA (used to detect older duplicate LSAs)
Checksum	Checksum of the complete contents of the LSA
Length	The length of the LSA in bytes
Link connected to	Link-state type, including transit network, stub network, or virtual link
Link ID	Link type and corresponding Router ID or network address
Link Data	◆ Router ID for transit network ◆ Network's IP address mask for stub network ◆ Neighbor Router ID for virtual link
Number of TOS metrics	Type of Service metric – This router only supports TOS 0 (or normal service)
TOS	Type of Service – This router only supports TOS 0 (or normal service)
Metric	Cost of the link

The following shows output when using the **summary** keyword.

```
Console#show ip ospf database summary

            OSPF Router with ID (0.0.0.0) (Process ID 1)

                Summary Link States (Area 0.0.0.0)

  LS Age: 1
  Options: 0x0 (*|-|-|-|-|-|-|-)
  LS Type: summary-LSA
  Link State ID: 192.168.10.0 (summary Network Number)
  Advertising Router: 2.1.0.0
  LS Seq Number: 80000005
  Checksum: 0x479d
  Length: 28
  Network Mask: /24
        TOS: 0  Metric: 0
⋮
```

Table 259: show ip ospf database summary - display description

Field	Description
OSPF Router ID	Router ID
LS Age	Age of LSA (in seconds)
Options	Optional capabilities associated with the LSA
LS Type	Summary Links - LSA describes routes to networks
Link State ID	Router ID of the router that originated the LSA

Table 259: show ip ospf database summary - display description (Continued)

Field	Description
Advertising Router	Advertising router ID
LS Sequence Number	Sequence number of LSA (used to detect older duplicate LSAs)
Checksum	Checksum of the complete contents of the LSA
Length	The length of the LSA in bytes
Network Mask	Destination network's IP address mask
Metrics	Cost of the link

show ip ospf interface

This command displays summary information for OSPF interfaces.

SYNTAX

show ip ospf interface [**vlan** *vlan-id*]

vlan-id - VLAN ID (Range: 1-4094)

COMMAND MODE

Privileged Exec

EXAMPLE

```
Console#show ip ospf interface vlan 1
VLAN1 is up, line protocol is up
  Internet Address 192.168.0.2/24, Area 0.0.0.0, MTU 1500
  Process ID 1, Router ID 192.168.0.2, Network Type BROADCAST, Cost: 1
  Transmit Delay is 1 sec, State DR, Priority 1
  Designated Router (ID) 192.168.0.2, Interface Address 192.168.0.2
  Backup Designated Router (ID) 192.168.0.3, Interface Address 192.168.0.3
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
  Hello due in 00:00:10
  Neighbor Count is 1, Adjacent neighbor count is 1
  Hello received 920 sent 975, DD received 5 sent 4
  LS-Req received 1 sent 1, LS-Upd received 14 sent 18
  LS-Ack received 17 sent 13, Discarded 0
Console#
```

Table 260: show ip ospf interface - display description

Field	Description
VLAN	VLAN ID and Status of physical link
Internet Address	IP address of OSPF interface
Area	OSPF area to which this interface belongs
MTU	Maximum transfer unit
Process ID	OSPF process ID
Router ID	Router ID

Table 260: show ip ospf interface - display description (Continued)

Field	Description
Network Type	Includes broadcast, non-broadcast, or point-to-point networks
Cost	Interface transmit cost
Transmit Delay	Interface transmit delay (in seconds)
State	◆ Disabled – OSPF not enabled on this interface ◆ Down – OSPF is enabled on this interface, but interface is down ◆ Loopback – This is a loopback interface ◆ Waiting – Router is trying to find the DR and BDR ◆ DR – Designated Router ◆ BDR – Backup Designated Router ◆ DRother – Interface is on a multiaccess network, but is not the DR or BDR
Priority	Router priority
Designated Router	Designated router ID and respective interface address
Backup Designated Router	Backup designated router ID and respective interface address
Timer intervals	Configuration settings for timer intervals, including Hello, Dead and Retransmit
Neighbor Count	Count of network neighbors and adjacent neighbors
Adjacent neighbor count	Count of adjacent neighbors
Hello	Number of Hello LSAs received and sent
DD	Number of Database Descriptor packets received and sent.
LS-Req	Number of LSA requests
LS-Upd	Number of LSA updates
LS-Ack	Number of LSA acknowledgements
Discarded	Number of LSAs discarded

show ip ospf neighbor

This command displays information about neighboring routers on each interface within an OSPF area.

SYNTAX

show ip ospf [*process-id*] **neighbor**

process-id - The ID of the router process for which information will be displayed. (Range: 1-65535)

COMMAND MODE

Privileged Exec

EXAMPLE

```
Console#show ip ospf neighbor

      ID          Pri        State          Address       Interface
--------------- ------ ---------------- --------------- --------------
    192.168.0.3      1         FULL/BDR     192.168.0.3           VLAN1
Console#
```

Table 261: show ip ospf neighbor - display description

Field	Description
Neighbor ID	Neighbor's router ID
Pri	Neighbor's router priority
State	OSPF state and identification flag States include: Down – Connection down Attempt – Connection down, but attempting contact (for non-broadcast networks) Init – Have received Hello packet, but communications not yet established Two-way – Bidirectional communications established ExStart – Initializing adjacency between neighbors Exchange – Database descriptions being exchanged Loading – LSA databases being exchanged Full – Neighboring routers now fully adjacent Identification flags include: D – Dynamic neighbor S – Static neighbor DR – Designated router BDR – Backup designated router
Address	IP address of this interface
Interface	The interface to which this neighbor is attached

show ip ospf route

This command displays the OSPF routing table.

SYNTAX

show ip ospf [*process-id*] **route**

process-id - The ID of the router process for which information will be displayed. (Range: 1-65535)

COMMAND MODE

Privileged Exec

EXAMPLE

```
Console#show ip ospf route
OSPF process 1:
Codes: C - connected, D - Discard, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
O  10.10.0.0/24 [10] is directly connected, fe1/1, Area 0.0.0.0
O  10.10.11.0/24 [10] is directly connected, fe1/2, Area 0.0.0.0
O  10.10.11.100/32 [10] is directly connected, lo, Area 0.0.0.0
E2 10.15.0.0/24 [10/50] via 10.10.0.1, VLAN1
```

```
IA 172.16.10.0/24 [30] via 10.10.11.50, VLAN2, Area 0.0.0.0
E2 192.168.0.0/16 [10/20] via 10.10.11.50, VLAN2

Console#
```

show ip ospf virtual-links

This command displays detailed information about virtual links.

SYNTAX

show ip ospf virtual-links

COMMAND MODE

Privileged Exec

EXAMPLE

```
Console#show ip ospf virtual-links
Virtual Link VLINK1 to router 192.168.0.2 is up
  Transit area 0.0.0.1 via interface VLAN1
  Local address 192.168.0.3
  Remote address 192.168.0.2
  Transmit Delay is 1 sec, State Point-To-Point,
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:08
    Adjacency state Down
Console#
```

Table 262: show ip ospf virtual-links - display description

Field	Description
Virtual Link to router	OSPF neighbor and link state (up or down)
Transit area	Common area the virtual link crosses to reach the target router
Local address	The IP address of ABR that serves as an endpoint connecting the isolated area to the common transit area.
Remote address	The IP address this virtual neighbor is using. The neighbor must be an ABR at the other endpoint connecting the common transit area to the backbone itself.
Transmit Delay	Estimated transmit delay (in seconds) on the virtual link
Timer intervals	Configuration settings for timer intervals, including Hello, Dead and Retransmit

RELATED COMMANDS

area virtual-link (1765)

show ip protocols ospf

This command displays OSPF process parameters.

SYNTAX

show ip protocols ospf

COMMAND MODE

Privileged Exec

EXAMPLE

```
Console#show ip protocols ospf
Routing Protocol is "ospf 200"
Redistributing: rip
Routing for Networks:
192.30.30.0/24
192.40.40.0/24
  Routing for Summary Address:
    192.168.1.0/24
    192.168.3.0/24
Distance: (default is 110)
Console#
```

Table 263: show ip protocols ospf - display description

Field	Description
Routing Protocol	Name and autonomous system number of this OSPF process.
Redistributing	Shows if route redistribution has been enabled with the redistribute command.
Routing for Networks	Networks for which the OSPF is currently registering routing information.
Routing for Summary Address	Shows the networks for which route summarization is in effect
Distance	The administrative distance used for external routes learned by OSPF (see the ip route command).

OPEN SHORTEST PATH FIRST (OSPFV3)

Table 264: Open Shortest Path First Commands (Version 3)

Command	Function	Mode
General Configuration		
router ipv6 ospf	Enables or disables OSPFv3 routing process	GC
abr-type	Sets the criteria used to determine if this router can declare itself an ABR and issue Type 3 and Type 4 summary LSAs	RC
max-current-dd	Sets the maximum number of neighbors with which the switch can concurrently exchange database descriptor packets	RC
router-id	Sets the router ID for this device	RC

Table 264: Open Shortest Path First Commands (Version 3) (Continued)

Command	Function	Mode
timers spf	Configures the delay after a topology change and the hold time between consecutive SPF calculations	RC
Route Metrics and Summaries		
area default-cost	Sets the cost for a default summary route sent into a stub	RC
area range	Summarizes routes advertised by an ABR	RC
default-metric	Sets the default metric for external routes imported from other protocols	RC
redistribute	Redistribute routes from one routing domain to another	RC
Area Configuration		
area stub	Defines a stubby area that cannot send or receive LSAs	RC
area virtual-link	Defines a virtual link from an area border routers to the backbone	RC
ipv6 router ospf area	Binds an area to the selected interface	IC
ipv6 router ospf tag area	Binds an area to the selected interface and process	IC
Interface Configuration		
ipv6 ospf cost	Specifies the cost of sending a packet on an interface	IC
ipv6 ospf dead-interval	Sets the interval at which hello packets are not seen before neighbors declare the router down	IC
ipv6 ospf hello-interval	Specifies the interval between sending hello packets	IC
ipv6 ospf priority	Sets the router priority used to determine the designated router	IC
ipv6 ospf retransmit-interval	Specifies the time between resending a link-state advertisement	IC
ipv6 ospf transmit-delay	Estimates time to send a link-state update packet over an interface	IC
passive-interface	Suppresses OSPF routing traffic on the specified interface	RC
Display Information		
show ipv6 ospf	Displays general information about the routing processes	PE
show ipv6 ospf database	Shows information about different LSAs in the database	PE
show ipv6 ospf interface	Displays interface information	PE
show ipv6 ospf neighbor	Displays neighbor information	PE
show ipv6 ospf route	Displays the OSPF routing table	PE
show ipv6 ospf virtual-links	Displays parameters and the adjacency state of virtual links	PE

General Guidelines

Follow these basic steps to configure OSPFv3:

1. Assign an IPv6 link-local address to each VLAN interface that will participate in an OSPF routing process. You can automatically generate a link-local address using the ipv6 enable command, or manually assign an address to an interface using the ipv6 address link-local command.

2. Use the router ipv6 ospf command to create a local OSPF router process and enter router configuration mode.

3. Use the router-id command to assign a unique identifier to the router. Note that the default router ID of "0.0.0.0" cannot be used with the current software version.

4. Use the ipv6 router ospf area command or the ipv6 router ospf tag area command to assign an area to each interface that will participate in the specified OSPF process.

General Configuration

router ipv6 ospf

This command creates an Open Shortest Path First (OSPFv3) routing process and enters router configuration mode. Use the **no** form to disable OSPF for all processes or for a specified process.

SYNTAX

[**no**] **router ipv6 ospf** [**tag** *process-name*]

process-name - A process name must be entered when configuring multiple routing instances. (Range: Alphanumeric string up to 16 characters)

COMMAND MODE

Global Configuration

DEFAULT SETTING

Disabled

COMMAND USAGE

- This command is used to enable an OSPFv3 routing process, and to enter router configuration mode.

- The *process-name* is only used on the local router to distinguish between different routing processes. It should not be confused with the *instance-id* configured with the ipv6 router ospf area command which is used to distinguish between different routing processes running on the same link-local network segment.

Example

```
Console(config)#router ipv6 ospf tag 0
Console(config-router)#end
Console#show ipv6 ospf
 Routing Process "ospf r&d" with ID 192.168.0.2
 Process uptime is 1 hour 34 minutes
 Supports only single TOS(TOS0) routes
 SPF schedule delay 5 secs, Hold time between two SPFs 10 secs
 Number of incoming concurrent DD exchange neighbors 0/5
 Number of outgoing concurrent DD exchange neighbors 0/5
 Number of external LSA 0. Checksum 0x000000
 Number of opaque AS LSA 0. Checksum 0x000000
 Number of LSA received 0
 Number of areas attached to this router: 1

    Area 0.0.0.0 (BACKBONE)
        SPF algorithm executed 1 times
        Number of LSA 2. Checksum 0x00ab4f

Console#
```

Related Commands

ipv6 router ospf area (1804)

abr-type

This command sets the criteria used to determine if this router can declare itself an ABR and issue Type 3 and Type 4 summary LSAs. Use the **no** form to restore the default setting.

Syntax

abr-type {**cisco** | **ibm** | **standard**}

no abr-type

cisco - ABR criteria and functional behavior is based on RFC 3509.

ibm - ABR criteria and functional behavior is briefly described in RFC 3509, and fully documented in IBM Nways Multiprotocol Routing Services (MRS) 3.3.

standard - ABR criteria and functional behavior is based on RFC 2328.

Command Mode

Router Configuration

Default Setting

cisco

Command Usage

- The basic criteria for a router to serve as an ABR is shown below:

  - Cisco Systems Interpretation: A router is considered to be an ABR if it has more than one area actively attached and one of them is the backbone area.

- IBM Interpretation: A router is considered to be an ABR if it has more than one actively attached area and the backbone area is configured.

- Standard Interpretation: A router is considered to be an ABR if it is attached to two or more areas. It does not have to be attached to the backbone area.

- To successfully route traffic to inter-area and AS external destinations, an ABR must be connected to the backbone. If an ABR has no backbone connection, all traffic destined for areas not connected to it or outside the AS will be dropped. This situation is normally resolved, by configuring a virtual link from the ABR to the backbone area.

- In both the Cisco and IBM interpretation, a router connected to more than one area cannot issue a Type 1 router LSA declaring itself as an ABR unless it meets the other criteria listed above.

  Routing table calculations are changed to allow the router to consider summary-LSAs from all attached areas if it is not an ABR, but has more than one attached area, or it does not have an active backbone connection.

  In other words, inter-area routes are calculated by examining summary-LSAs. If the router is an ABR and has an active backbone connection, only backbone summary-LSAs are examined. Otherwise (when either the router is not an ABR or it has no active backbone connection), the router should consider summary-LSAs from all actively attached areas.

  This ensures that the summary-LSAs originated by area border routers advertise only intra-area routes into the backbone if the router has an active backbone connection, and advertises both intra-area and inter-area routes into the other areas. Otherwise, the router only advertises intra-area routes into non-backbone areas.

EXAMPLE

```
Console(config-router)#abr-type ibm
Console(config-router)#
```

max-current-dd

This command sets the maximum number of neighbors with which the switch can concurrently exchange database descriptor (DD) packets. Use the **no** form to restore the default setting.

SYNTAX

max-current-dd *max-packets*

no max-current-dd

max-packets - The maximum number of neighbors with which the switch can concurrently send or receive DD packets.
(Range: 1-65535)

COMMAND MODE

Router Configuration

DEFAULT SETTING

5

COMMAND USAGE

- This limit applies separately to the number of neighbors to which DD packets can be concurrently sent, and to the number of neighbors from which DD packets can be concurrently received.

EXAMPLE

```
Console(config-router)#maximum-current-dd 10
Console(config-router)#
```

RELATED COMMANDS

show ipv6 ospf (1812)

router-id

This command assigns a unique router ID for this device within the autonomous system for the current OSPFv3 process. Use the **no** form to restore the default setting.

SYNTAX

router-id *ip-address*

no router-id

ip-address - Router ID formatted as an IPv4 address.

COMMAND MODE

Router Configuration

DEFAULT SETTING

None

COMMAND USAGE

- This command sets the router ID for the OSPF process specified in the router ipv6 ospf command.

- The router ID must be unique for every router in the autonomous system. (Note that the router ID can also be set to 0.0.0.0 or 255.255.255.255).

- If this router already has registered neighbors, the new router ID will be used when the router is rebooted, or manually restarted by entering the no router ipv6 ospf followed by the router ipv6 ospf command.

- If the priority values of the routers bidding to be the designated router or backup designated router for an area are equal, the router with the highest ID is elected.

- The current routing process will not be enabled until a Router ID is configured with this command.

EXAMPLE

```
Console(config-router)#router-id 10.1.1.1
Console(config-router)#
```

RELATED COMMANDS

router ipv6 ospf (1792)

timers spf

This command configures the delay after receiving a topology change and starting the shortest path first (SPF) calculation, and the hold time between making two consecutive SPF calculations. Use the **no** form to restore the default values.

SYNTAX

timers spf *spf-delay spf-holdtime*

no timers spf

spf-delay - The delay after receiving a topology change notification and starting the SPF calculation. (Range: 0-2147483647 seconds)

spf-holdtime - The minimum time between two consecutive SPF calculations. (Range: 0-2147483647 seconds)

COMMAND MODE

Router Configuration

DEFAULT SETTING

SPF delay: 5 seconds
SPF holdtime: 10 seconds

COMMAND USAGE

- Setting the SPF holdtime to 0 means that there is no delay between consecutive calculations.

- Using a low value for the holdtime allows the router to switch to a new path faster, but uses more CPU processing time.

EXAMPLE

```
Console(config-router)#timers spf 20
Console(config-router)#
```

Route Metrics and Summaries

area default-cost

This command specifies a cost for the default summary route sent into a stub from an Area Border Router (ABR). Use the **no** form to remove the assigned default cost.

SYNTAX

area *area-id* **default-cost** *cost*

no area *area-id* **default-cost**

area-id - Identifies the stub. (The area ID can be in the form of an IPv4 address or as a four octet unsigned integer ranging from 0-4294967295.)

cost - Cost for the default summary route sent to a stub. (Range: 0-16777215)

COMMAND MODE

Router Configuration

DEFAULT SETTING

Default cost: 1

COMMAND USAGE

If the default cost is set to “0,” the router will not advertise a default route into the attached stub.

EXAMPLE

```
Console(config)#router ipv6 ospf tag 1
Console(config-router)#area 1 default-cost 1
Console(config-router)#
```

RELATED COMMANDS

area stub (1764)

area range

This command summarizes the routes advertised by an Area Border Router (ABR). Use the **no** form to disable this function.

SYNTAX

[**no**] **area** *area-id* **range** *ipv6-prefix/prefix-length* {**advertise** | **not-advertise**}

area-id - Identifies an area for which the routes are summarized. The area ID can be in the form of an IPv4 address or as a four octet unsigned integer ranging from 0-4294967295.

ipv6-prefix - A full IPv6 address including the network prefix and host address bits.

prefix-length - A decimal value indicating how many contiguous bits (from the left) of the address comprise the prefix (i.e., the portion of the address to summarize).

advertise - Advertises the specified address range.

not-advertise - The summary is not sent, and the routes remain hidden from the rest of the network.

COMMAND MODE

Router Configuration

DEFAULT SETTING

Disabled

COMMAND USAGE

- This command can be used to summarize intra-area routes and advertise this information to other areas through Area Border Routers (ABRs).
- If the network addresses within an area are assigned in a contiguous manner, the ABRs can advertise a summary route that covers all of the individual networks within the area that fall into the specified range using a single **area range** command.
- If routes are set to be advertised by this command, the router will issue a Type 3 summary LSA for each address range specified by this command.
- This router supports up 64 summary routes for area ranges.

EXAMPLE

This example creates a summary address for all area routes in the range of 73::/8, or all IPv6 address that start with the first byte 73 (hexadecimal).

```
Console(config-router)#area 1 range 73::/8 advertise
Console(config-router)#
```

default-metric

This command sets the default metric for external routes imported from other protocols. Use the **no** form to remove the default metric for the supported protocol types.

Syntax

default-metric *metric-value*

no default-metric

metric-value – Metric assigned to all external routes imported from other protocols. (Range: 0-16777214)

Command Mode

Router Configuration

Default Setting

20

Command Usage

- The default metric must be used to resolve the problem of redistributing external routes from other protocols that use incompatible metrics.

- This command does not override the metric value set by the redistribute command. When a metric value has not been configured by the redistribute command, the **default-metric** command sets the metric value to be used for all imported external routes.

Example

```
Console(config-router)#default-metric 100
Console(config-router)#
```

Related Commands

redistribute (1799)

redistribute

This command redistributes external routing information from other routing protocols and static routes into an autonomous system. Use the **no** form to disable this feature or to restore the default settings.

Syntax

[**no**] **redistribute** {**connected** | **static**} [**metric** *metric-value*] [**metric-type** *type-value*]

connected - Imports all currently connected entries.

static - IPv6 static routes will be imported into this Autonomous System.

metric-value - Metric assigned to all external routes for the specified protocol. (Range: 0-16777214: Default: 20) *type-value*

1 - Type 1 external route

2 - Type 2 external route (default) - Routers do not add internal route metric to external route metric.

Command Mode

Router Configuration

Default Setting

redistribution - none
metric-value - 20
type-metric - 2

Command Usage

- This command is used to import routes learned from other routing protocols into the OSPF domain, and to generate AS-external-LSAs.
- When you redistribute external routes into an OSPF autonomous system (AS), the router automatically becomes an autonomous system boundary router (ASBR).
- Metric type specifies the way to advertise routes to destinations outside the AS through External LSAs. When a Type 1 LSA is received by a router, it adds the internal cost to the external route metric. In other words, the cost of the route from any router within the AS is equal to the cost associated with reaching the advertising ASBR, plus the cost of the external route. When a Type 2 LSA is received by a router, it only uses the external route metric to determine route cost.

Example

This example redistributes automatically connected routes as Type 1 external routes.

```
Console(config-router)#redistribute connected metric-type 1
Console(config-router)#
```

Area Configuration

area stub

This command defines a stub area. To remove a stub, use the **no** form without the optional keyword. To remove the summary attribute, use the **no** form with the summary keyword.

Syntax

[**no**] **area** *area-id* **stub** [**no-summary**]

area-id - Identifies the stub area. The area ID can be in the form of an IPv4 address or as a four octet unsigned integer ranging from 0-4294967295.

no-summary - Stops an Area Border Router (ABR) from sending summary link advertisements into the stub area.

Command Mode

Router Configuration

Default Setting

No stub is configured.
Summary advertisement are sent into the stub.

Command Usage

- All routers in a stub must be configured with the same area ID.
- Routing table space is saved by stopping an ABR from flooding Type-4 Inter-Area Router and Type 5 AS-External LSAs into the stub. Since no information on external routes is known inside the stub, an ABR will advertise the default route 0::0/0 using a Type 3 Inter-Area Prefix LSA.
- The default setting for this command blocks Type-4 Inter-Area Router and Type 5 AS-External LSAs. Therefore, any destinations that cannot be matched to an inter-area or intra-area route will have to use the default route.
- Use the **no-summary** parameter of this command on an ABR attached to the stub to define a totally stubby area, blocking all Type 3 network summary LSAs. Define an area as a totally stubby area only if routers in the area do not require summary LSAs from other areas.
- Use the area default-cost command to specify the cost of a default summary route sent into a stub by an ABR attached to the stub area.

Example

This example creates a stub area 2, and makes it totally stubby by blocking all Type 3 summary LSAs.

```
Console(config-router)#area 2 stub no-summary
Console(config-router)#
```

RELATED COMMANDS

area default-cost (1797)

area virtual-link

This command defines a virtual link. To remove a virtual link, use the **no** form with no optional keywords. To restore the default value for an attribute, use the **no** form with the required keyword.vvvv

SYNTAX

area *area-id* **virtual-link** *router-id*
[**dead-interval** *seconds*] [**hello-interval** *seconds*]
[**retransmit-interval** *seconds*] [**transmit-delay** *seconds*]

no area area-id virtual-link *router-id*
[**dead-interval** | **hello-interval** | **retransmit-interval** | **transmit-delay**]

area-id - Identifies the transit area for the virtual link.The area ID can be in the form of an IPv4 address or as a four octet unsigned integer ranging from 0-4294967295.

router-id - Router ID of the virtual link neighbor. This specifies the Area Border Router (ABR) at the other end of the virtual link. To create a virtual link, enter this command for an ABR at both ends of the link. One of the ABRs must be next to the isolated area and the transit area at one end of the link, while the other ABR must be next to the transit area and backbone at the other end of the link.

dead-interval *seconds* - Specifies the time that neighbor routers will wait for a hello packet before they declare the router down. This value must be the same for all routers attached to an autonomous system. (Range: 1-65535 seconds; Default: 4 x hello interval, or 40 seconds)

hello-interval *seconds* - Specifies the transmit delay between sending hello packets. Setting the hello interval to a smaller value can reduce the delay in detecting topological changes, but will increase the routing traffic. This value must be the same for all routers attached to an autonomous system. (Range: 1-65535 seconds; Default: 10 seconds)

retransmit-interval *seconds* - Specifies the interval at which the ABR retransmits link-state advertisements (LSA) over the virtual link. The retransmit interval should be set to a conservative value that provides an adequate flow of routing information, but does not produce unnecessary protocol traffic. However, note that this value should be larger for virtual links. (Range: 1-65535 seconds; Default: 5 seconds)

transmit-delay *seconds* - Estimates the time required to send a link-state update packet over the virtual link, considering the transmission and propagation delays. LSAs have their age incremented by this amount before transmission. This value must be the same for all routers attached to an autonomous system. (Range: 1-65535 seconds; Default: 1 second)

COMMAND MODE

Router Configuration

DEFAULT SETTING

area-id: None
router-id: None
hello-interval: 10 seconds
retransmit-interval: 5 seconds
transmit-delay: 1 second
dead-interval: 40 seconds

COMMAND USAGE

- All areas must be connected to a backbone area (0.0.0.0) to maintain routing connectivity throughout the autonomous system. If it not possible to physically connect an area to the backbone, you can use a virtual link. A virtual link can provide a logical path to the backbone for an isolated area, or can be configured as a backup connection that can take over if the normal connection to the backbone fails.

- A virtual link can be configured between any two backbone routers that have an interface to a common non-backbone area. The two routers joined by a virtual link are treated as if they were connected by an unnumbered point-to-point network.

- Any area disconnected from the backbone must include the transit area ID and the router ID for a virtual link neighbor that is adjacent to the backbone.

EXAMPLE

This example creates a virtual link using the defaults for all optional parameters.

```
Console(config-router)#area 3 virtual-link 192.168.0.9
Console(config-router)#
```

ipv6 router ospf area

This command binds an OSPF area to the selected interface. Use the **no** form to remove an OSPF area, disable an OSPF process, or remove an instance identifier from an interface.

SYNTAX

[**no**] **ipv6 router ospf area** *area-id* [**tag** *process-name* | **instance-id** *instance-id*]

area-id - Area to bind to the current Layer 3 interface. An OSPF area identifies a group of routers that share common routing information. The area ID can be in the form of an IPv4 address or as a four octet unsigned integer ranging from 0-4294967295.

process-name - A process name must be entered when configuring multiple routing instances. (Range: Alphanumeric string up to 16 characters)

instance-id - Identifies a specific OSPFv3 routing process on the link-local network segment attached to this interface.
(Range: 0-255)

COMMAND MODE

Interface Configuration

DEFAULT SETTING

None

COMMAND USAGE

- An area ID uniquely defines an OSPF broadcast area. The area ID 0.0.0.0 indicates the OSPF backbone for an autonomous system. Each router must be connected to the backbone via a direct connection or a virtual link.

- Set the area ID to the same value for all routers on a network segment.

- The *process-name* is only used on the local router to distinguish between different routing processes (and must be configured with the router ipv6 ospf command before using it in the **ipv6 router ospf area** command).

- The *instance-id* is used on the link-local network segment to distinguish between different routing processes running on the same link, and allows routers participating in a common routing process to form adjacencies and exchange routing information.

- The backbone (area 0.0.0.0) must be created before any other area.

EXAMPLE

This example creates the backbone 0.0.0.0.

```
Console(config)#router ipv6 ospf tag 0
Console(config-router)#router-id 192.168.0.2
Console(config-router)#exit
Console(config)#interface vlan 1
Console(config-if)#ipv6 router ospf area 0 tag 0 instance-id 0
Console(config-if)#
```

Related Commands

router ipv6 ospf (1792)
router-id (1795)
ipv6 router ospf tag area (1805)

ipv6 router ospf tag area

This command binds an OSPF area to the selected interface and process. Use the **no** form to remove the specified area from an interface.

[**no**] **ipv6 router ospf tag** *process-name* **area** *area-id* [**instance-id** *instance-id*]

area-id - Area to bind to the current Layer 3 interface. An OSPF area identifies a group of routers that share common routing information. The area ID can be in the form of an IPv4 address or as a four octet unsigned integer ranging from 0-4294967295.

process-name - A process name used to distinguish between multiple routing instances configured on the local router. (Range: Alphanumeric string up to 16 characters)

instance-id - Identifies a specific OSPFv3 routing process on the link-local network segment attached to this interface. (Range: 0-255)

Command Mode

Interface Configuration (VLAN)

Default Setting

No areas are defined.

Command Usage

- An area ID uniquely defines an OSPF broadcast area. The area ID 0.0.0.0 indicates the OSPF backbone for an autonomous system. Each router must be connected to the backbone via a direct connection or a virtual link.
- Set the area ID to the same value for all routers on a network segment.
- The *process-name* is only used on the local router to distinguish between different routing processes (and must be configured with the router ipv6 ospf command before using it in this command.
- The *instance-id* is used on the link-local network segment to distinguish between different routing processes running on the same link, and allows routers participating in a common routing process to form adjacencies and exchange routing information.
- The backbone (area 0.0.0.0) must be created before any other area.

EXAMPLE

This example assigns area 0.0.0.1 to the currently selected interface under routing process "1."

```
Console(config)#interface vlan 1
Console(config-if)#ipv6 router ospf tag 1 area 0.0.0.1
Console(config-if)#
```

RELATED COMMANDS

router ipv6 ospf (1792)
router-id (1795)
ipv6 router ospf area (1804)

Interface Configuration

ipv6 ospf cost

This command explicitly sets the cost of sending a protocol packet on an interface, where higher values indicate slower ports. Use the **no** form to restore the default value.

SYNTAX

ipv6 ospf cost *cost* [**instance-id** *instance-id*]

no ipv6 ospf cost [**instance-id** *instance-id*]

cost - Link metric for this interface. Use higher values to indicate slower ports. (Range: 1-65535)

instance-id - Identifies a specific OSPFv3 routing process on the link-local network segment attached to this interface.
(Range: 0-255)

COMMAND MODE

Interface Configuration (VLAN)

DEFAULT SETTING

1

COMMAND USAGE

- The interface cost indicates the overhead required to send packets across a certain interface. This is advertised as the link cost in router link state advertisements.

- Routes are assigned a metric equal to the sum of all metrics for each interface link in the route.

- This router uses a default cost of 1 for all interfaces. Therefore, if you install a 10 Gigabit module, you may need to reset the cost for all other VLAN interfaces with only 1 Gbps ports to a value greater than 1 to reflect the actual interface bandwidth.

EXAMPLE

```
Console(config)#interface vlan 1
Console(config-if)#ipv6 ospf cost 10
Console(config-if)#
```

ipv6 ospf dead-interval

This command sets the interval at which hello packets are not seen before neighbors declare the router down. Use the **no** form to restore the default value.

SYNTAX

ipv6 ospf dead-interval *seconds* [**instance-id** *instance-id*]

no ipv6 ospf dead-interval [**instance-id** *instance-id*]

seconds - The maximum time that neighbor routers can wait for a hello packet before declaring the transmitting router down. This interval must be set to the same value for all routers on the network. (Range: 1-65535)

instance-id - Identifies a specific OSPFv3 routing process on the link-local network segment attached to this interface.
(Range: 0-255)

COMMAND MODE

Interface Configuration (VLAN)

DEFAULT SETTING

40 seconds, or four times the interval specified by the ipv6 ospf hello-interval command.

COMMAND USAGE

The dead-interval is advertised in the router's hello packets. It must be a multiple of the hello-interval and be the same for all routers on a specific network.

EXAMPLE

```
Console(config)#interface vlan 1
Console(config-if)#ipv6 ospf dead-interval 50
Console(config-if)#
```

RELATED COMMANDS

ipv6 ospf hello-interval (1808)

ipv6 ospf hello-interval

This command specifies the interval between sending hello packets on an interface. Use the **no** form to restore the default value.

SYNTAX

ipv6 ospf hello-interval *seconds* [**instance-id** *instance-id*]

no ipv6 ospf hello-interval [**instance-id** *instance-id*]

seconds - Interval at which hello packets are sent from an interface. This interval must be set to the same value for all routers on the network. (Range: 1-65535)

instance-id - Identifies a specific OSPFv3 routing process on the link-local network segment attached to this interface. (Range: 0-255)

COMMAND MODE

Interface Configuration (VLAN)

DEFAULT SETTING

10 seconds

COMMAND USAGE

Hello packets are used to inform other routers that the sending router is still active. Setting the hello interval to a smaller value can reduce the delay in detecting topological changes, but will increase routing traffic.

EXAMPLE

```
Console(config)#interface vlan 1
Console(config-if)#ipv6 ospf hello-interval 5
Console(config-if)#
```

RELATED COMMANDS

ipv6 ospf dead-interval (1807)

ipv6 ospf priority

This command sets the router priority used when determining the designated router (DR) and backup designated router (BDR) for an area. Use the **no** form to restore the default value.

SYNTAX

ipv6 ospf priority *priority* [**instance-id** *instance-id*]

no ipv6 ospf priority [**instance-id** *instance-id*]

priority - Sets the interface priority for this router. (Range: 0-255)

instance-id - Identifies a specific OSPFv3 routing process on the link-local network segment attached to this interface. (Range: 0-255)

COMMAND MODE

Interface Configuration (VLAN)

DEFAULT SETTING

1

COMMAND USAGE

- A designated router (DR) and backup designated router (BDR) are elected for each OSPF area based on Router Priority. The DR forms an active adjacency to all other routers in the area to exchange routing topology information. If for any reason the DR fails, the BDR takes over this role.
- Set the priority to zero to prevent a router from being elected as a DR or BDR. If set to any value other than zero, the router with the highest priority will become the DR and the router with the next highest priority becomes the BDR. If two or more routers are tied with the same highest priority, the router with the higher ID will be elected.
- If a DR already exists for a network segment when this interface comes up, the new router will accept the current DR regardless of its own priority. The DR will not change until the next time the election process is initiated.
- Configure router priority for multi-access networks only and not for point-to-point networks.

EXAMPLE

```
Console(config)#interface vlan 1
Console(config-if)#ipv6 ospf priority 5
Console(config-if)#
```

ipv6 ospf retransmit-interval

This command specifies the time between resending link-state advertisements (LSAs). Use the **no** form to restore the default value.

SYNTAX

ipv6 ospf retransmit-interval *seconds* [**instance-id** *instance-id*]

no ipv6 ospf retransmit-interval [**instance-id** *instance-id*]

seconds - Sets the interval at which LSAs are retransmitted from this interface. (Range: 1-65535)

instance-id - Identifies a specific OSPFv3 routing process on the link-local network segment attached to this interface. (Range: 0-255)

COMMAND MODE

Interface Configuration (VLAN)

DEFAULT SETTING

5 seconds

COMMAND USAGE

- A router will resend an LSA to a neighbor if it receives no acknowledgment after the specified retransmit interval. The retransmit interval should be set to a conservative value that provides an adequate flow of routing information, but does not produce unnecessary protocol traffic. Note that this value should be larger for virtual links.
- Set this interval to a value that is greater than the round-trip delay between any two routers on the attached network to avoid unnecessary retransmissions.

EXAMPLE

```
Console(config)#interface vlan 1
Console(config-if)#ipv6 ospf retransmit-interval 7
Console(config-if)#
```

ipv6 ospf transmit-delay

This command sets the estimated time to send a link-state update packet over an interface. Use the **no** form to restore the default value.

SYNTAX

ipv6 ospf transmit-delay *seconds* [**instance-id** *instance-id*]

no ipv6 ospf transmit-delay [**instance-id** *instance-id*]

seconds - Sets the estimated time required to send a link-state update. (Range: 1-65535)

instance-id - Identifies a specific OSPFv3 routing process on the link-local network segment attached to this interface. (Range: 0-255)

COMMAND MODE

Interface Configuration (VLAN)

DEFAULT SETTING

1 second

COMMAND USAGE

- LSAs have their age incremented by this delay before transmission. When estimating the transmit delay, consider both the transmission and propagation delays for an interface. Set the transmit delay according to link speed, using larger values for lower-speed links.
- If this delay is not added, the time required to transmit an LSA over the link is not taken into consideration by the routing process. On slow links, the router may send packets more quickly than devices can

receive them. To avoid this problem, use the transmit delay to force the router to wait a specified interval between transmissions.

EXAMPLE

```
Console(config)#interface vlan 1
Console(config-if)#ipv6 ospf transmit-delay 6
Console(config-if)#
```

passive-interface

This command suppresses OSPF routing traffic on the specified interface. Use the **no** form to allow routing traffic to be sent and received on the specified interface.

SYNTAX

[**no**] **passive-interface vlan** *vlan-id* [*ipv6-address*]

vlan-id - VLAN ID. (Range: 1-4094)

ipv6-address - A full IPv6 address including the network prefix and host address bits.

COMMAND MODE

Router Configuration

DEFAULT SETTING

None

COMMAND USAGE

You can configure an OSPF interface as passive to prevent OSPF routing traffic from exiting or entering that interface. No OSPF adjacency can be formed if one of the interfaces involved is set to passive mode. The specified interface will appear as a stub in the OSPF domain. Also, if you configure an OSPF interface as passive where an adjacency already exists, the adjacency will drop almost immediately.

EXAMPLE

```
Console(config-router)#passive-interface vlan 1 73::9
Console(config-router)#
```

Display Information

show ipv6 ospf

This command shows basic information about the routing configuration.

COMMAND MODE

Privileged Exec

EXAMPLE

```
Console#show ipv6 ospf
  Routing Process "ospf 1" with ID 192.168.0.2
 Process uptime is 24 minutes
 Supports only single TOS(TOS0) routes
 SPF schedule delay 5 secs, Hold time between two SPFs 10 secs
 Number of incoming concurrent DD exchange neighbors 0/5
 Number of outgoing concurrent DD exchange neighbors 0/5
 Number of external LSA 0. Checksum 0x000000
 Number of opaque AS LSA 0. Checksum 0x000000
 Number of LSA received 0
 Number of areas attached to this router: 2

    Area 0.0.0.0 (BACKBONE)
        SPF algorithm executed 2 times
        Number of LSA 1. Checksum 0x001aa9
    Area 0.0.0.1
        SPF algorithm executed 2 times
        Number of LSA 1. Checksum 0x001aa9

Console#
```

Table 265: show ip ospf - display description

Field	Description
Routing Process	
Routing Process	OSPF process name and router ID. The router ID uniquely identifies the router in the autonomous system. By convention, this is normally set to one of the router's IP interface addresses.
Process uptime	The time this process has been running
Supports only single TOS (TOS0) routes	Optional Type of Service (ToS) specified in OSPF Version 2, Appendix F.1.2 is not supported, so only one cost per interface can be assigned.
SPF schedule delay	The delay after receiving a topology change notification and starting the SPF calculation.
Hold time	Sets the hold time between two consecutive SPF calculations.
Number of concurrent DD exchange neighbors	Number of neighbors currently exchanging database descriptor packets.
Number of external LSA	The number of external link-state advertisements (Type 5 LSAs) in the link-state database. These LSAs advertise information about routes outside of the autonomous system.
Checksum	The sum of the LS checksums of the external link-state advertisements contained in the link-state database.
Number of opaque AS LSA	Number of opaque link-state advertisements (Type 9, 10 and 11 LSAs) in the link-state database. These LSAs advertise information about external applications, and are only used by OSPF for the graceful restart process.

Table 265: show ip ospf - display description (Continued)

Field	Description
Checksum	The sum of the LS checksums of opaque link-state advertisements contained in the link-state database.
Number of LSA received	The number of link-state advertisements that have been received.
Number of areas attached to this router	The number of configured areas attached to this router.
Area Information	
Area	The area identifier. Note that "(Inactive)" will be displayed if no IPv6 address has been configured on the interface.
SPF algorithm executed x times	The number of times the shortest path first algorithm has been executed for this area
Number of LSA	The total number of link-state advertisements in this area's link-state database, excluding AS External LSA's.
Checksum	The sum of the LS checksums of link-state advertisements for this network (area) contained in the link-state database.

show ipv6 ospf database

This command shows information about different OSPF Link State Advertisements (LSAs) stored in this router's database.

SYNTAX

show ipv6 ospf [**tag** *process-id*] **database**

process-id - The ID of the router process for which information will be displayed. (Range: 1-10)

COMMAND MODE

Privileged Exec

EXAMPLES

The following shows output for the **show ip ospf database** command.

```
Console#show ipv6 ospf database

            OSPF Router with ID (192.168.0.2) (TAG: 1)

                Link-LSA
Link State ID   ADV Router      Age  Seq#       CkSum    Link
1001            192.168.0.2       71 0x80000001 0x06b7     0

                Router-LSA (Area 0)
Link State ID   ADV Router      Age  Seq#       CkSum
0               192.168.0.2       31 0x80000002 0x14b1

                AS-external-LSA
Link State ID   ADV Router      Age  Seq#       CkSum
Console#
```

Table 266: show ip ospf database - display description

Field	Description
OSPF Router Process with ID	OSPF router ID and process ID. The router ID uniquely identifies the router in the autonomous system. By convention, this is normally set to one of the router's IP interface addresses.
Link State ID	This field identifies the piece of the routing domain that is being described by the advertisement.
ADV Router	Advertising router ID
Age	Age of LSA (in seconds)
Seq#	Sequence number of LSA (used to detect older duplicate LSAs)
CkSum	Checksum of the complete contents of the LSA
Link	Number of interfaces attached to the router

show ipv6 ospf interface

This command displays summary information for OSPF interfaces.

SYNTAX

show ipv6 ospf interface [**vlan** *vlan-id*]

vlan-id - VLAN ID (Range: 1-4094)

COMMAND MODE

Privileged Exec

EXAMPLE

```
Console#show ipv6 ospf interface vlan 1
 VLAN 1 is up, line protocol is up
 Link local Address FE80::200:E8FF:FE93:82A0/64, Area 0.0.0.0
 Tag 1, Router ID 192.168.0.2, Network Type BROADCAST, Cost: 1
 Transmit Delay is 1 sec, State DR, Priority 1
 Designated Router (ID) 192.168.0.2, Interface Address
  FE80::200:E8FF:FE93:82A0
 No backup designated router on this network
 Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
 Neighbor Count is 0, Adjacent neighbor count is 0
 Hello received 0 sent 92, DD received 0 sent 0
 LS-Req received 0 sent 0, LS-Upd received 0 sent 0
 LS-Ack received 0 sent 0, Discarded 0
Console
```

Table 267: show ip ospf interface - display description

Field	Description
VLAN	VLAN ID and Status of physical link
Link local Address	Link local address of OSPF interface
Area	OSPF area to which this interface belongs
Tag	OSPF process identifier string
Router ID	Identifier for this router

Table 267: show ip ospf interface - display description (Continued)

Field	Description
Network Type	Includes broadcast, non-broadcast, or point-to-point networks
Cost	Interface transmit cost
Transmit Delay	Interface transmit delay (in seconds)
State	◆ Backup – Backup Designated Router ◆ Down – OSPF is enabled on this interface, but interface is down ◆ DR – Designated Router ◆ DROther – Interface is on a multiaccess network, but is not the DR or BDR ◆ Loopback – This is a loopback interface ◆ PointToPoint – A direct link between two routers. ◆ Waiting – Router is trying to find the DR and BDR
Priority	Router priority
Designated Router	Designated router ID and respective interface address
Backup Designated Router	Backup designated router ID and respective interface address
Timer intervals	Configuration settings for timer intervals, including Hello, Dead and Retransmit
Neighbor Count	Count of network neighbors and adjacent neighbors
Hello	Number of Hello LSAs received and sent
DD	Number of Database Descriptor packets received and sent
LS-Req	Number of LSA requests
LS-Upd	Number of LSA updates
LS-Ack	Number of LSA acknowledgements
Discarded	Number of LSAs discarded

show ipv6 ospf neighbor

This command displays information about neighboring routers on each interface within an OSPF area.

SYNTAX

show ipv6 ospf [**tag** *process-id*] **neighbor**

process-id - The ID of the router process for which information will be displayed. (Range: 1-10)

COMMAND MODE

Privileged Exec

Example

```
Console#show ipv6 ospf neighbor

       ID          Pri         State        Interface ID     Interface
--------------- ------ ---------------- --------------- --------------
    192.168.0.2      1          FULL/DR            1001     vlan1
Console#
```

Table 268: show ipv6 ospf neighbor - display description

Field	Description
ID	Neighbor's router ID
Pri	Neighbor's router priority
State	OSPF state and identification flag States include: Down – Connection down Attempt – Connection down, but attempting contact (for non-broadcast networks) Init – Have received Hello packet, but communications not yet established Two-way – Bidirectional communications established ExStart – Initializing adjacency between neighbors Exchange – Database descriptions being exchanged Loading – LSA databases being exchanged Full – Neighboring routers now fully adjacent Identification flags include: D – Dynamic neighbor S – Static neighbor DR – Designated router BDR – Backup designated router
Interface ID	
Interface	The interface to which this neighbor is attached

show ipv6 ospf route

This command displays the OSPF routing table.

Syntax

show ipv6 ospf [**tag** *process-id*] **route**

process-id - The ID of the router process for which information will be displayed. (Range: 1-10)

Command Mode

Privileged Exec

Example

```
Console#show ipv6 ospf route
Codes: C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
C    ::1/128, lo0
O    2001:DB8:2222:7272::/64, VLAN1
```

```
C     2001:DB8:2222:7272::/64, VLAN1
?     FE80::/64, VLAN1 inactive
C     FE80::/64, VLAN1
?     FF00::/8, VLAN1 inactive

Console#
```

show ipv6 ospf virtual-links

This command displays detailed information about virtual links.

SYNTAX

show ipv6 ospf [**tag** *process-id*] **virtual-links**

process-id - The ID of the router process for which information will be displayed. (Range: 1-10)

COMMAND MODE

Privileged Exec

EXAMPLE

```
Console#show ipv6 ospf virtual-links
Virtual Link VLINK1 to router 192.168.0.2 is up
  Transit area 0.0.0.1 via interface VLAN1
  Local address 192.168.0.3
  Remote address 192.168.0.2
  Transmit Delay is 1 sec, State Point-To-Point,
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:02
    Adjacency state Full
Console#
```

Table 269: show ipv6 ospf virtual-links - display description

Field	Description
Virtual Link to router	OSPF neighbor and link state (up or down)
Transit area	Common area the virtual link crosses to reach the target router
Local address	The IP address of ABR that serves as an endpoint connecting the isolated area to the common transit area.
Remote address	The IP address this virtual neighbor is using. The neighbor must be an ABR at the other endpoint connecting the common transit area to the backbone itself.
Transmit Delay	Estimated transmit delay (in seconds) on the virtual link
Timer intervals	Configuration settings for timer intervals, including Hello, Dead and Retransmit

Table 269: show ipv6 ospf virtual-links - display description

Field	Description
Hello due	The timeout for the next hello message from the neighbor
Adjacency state	The adjacency state between these neighbors: Down – Connection down Attempt – Connection down, but attempting contact (for non-broadcast networks) Init – Have received Hello packet, but communications not yet established Two-way – Bidirectional communications established ExStart – Initializing adjacency between neighbors Exchange – Database descriptions being exchanged Loading – LSA databases being exchanged Full – Neighboring routers now fully adjacent

RELATED COMMANDS

area virtual-link (1802)

BORDER GATEWAY PROTOCOL (BGPV4)

BGP OVERVIEW

An autonomous system (AS) functions as a separate routing domain under one administrative authority, which implements its own routing policies. An AS exchanges routing information within its boundaries using Interior Gateway Protocols (IGPs) such as RIP or OSPF, and connects to external organizations or to the Internet using an Exterior Gateway Protocol (EGP). BGP version 4 is the primary EGP deployed on the Internet today.

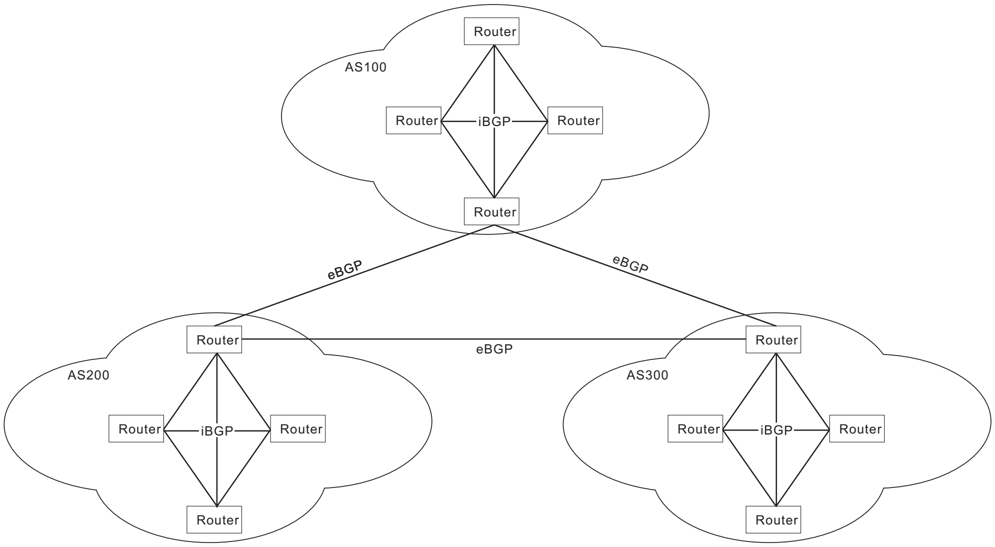
A communication session must be maintained between bordering ASs to support the periodic exchange of routing information. One of the major design choices for BGP is the use of a TCP connection to exchange routing information between peers. Exchanging connectivity information over a reliable transport mechanism effectively delegates all error control functions to TCP.

The other major innovation for BGP is the use of path vectors which carry the full list of transit networks, or ASs, traversed between the source and destination. Loops are prevented simply by checking the path vector to see if same AS is listed twice. This approach solves many of the scalability problems encountered when applying distance-vector or link-state methods to make routing decisions in complex topologies.

EXTERNAL AND INTERNAL BGP

When connecting to the Internet, external BGP (eBGP) is used. Although BGP is widely used as an exterior gateway protocol (EGP), it is also used in many organizations with complex internal networks. Internal networks can be simplified by exchanging routing information among BGP peers within the same organization through internal BGP (iBGP) peering sessions.

Figure 555: Connections for Internal and External BGP



External BGP – eBGP interconnects different ASs through border routers, or eBGP peers. These peering routers are commonly connected over a WAN link using a single physical path. Alternatively, multiple eBGP peer connections may be used to provide redundancy or load balancing. Distinct BGP sessions are used between redundancy peers to ensure that if one session fails, another will take over.

BGP uses the AS path attribute to record the ASs that must be followed to reach the prefix for a network aggregate. When a prefix is announced to an eBGP peer, the local AS number is prepended to the AS path. This prevents routing loops by rejecting any prefix announcements that include the local AS number in the AS path. These announcements are also used by eBGP in the best path selection process.

eBGP speakers, can communicate with other external peers or with iBGP peers. A BGP speaker can determine if it communicating with an external or internal peer by comparing the AS number sent in OPEN messages by a peer with that of its own internal value. If it matches, then this neighbor is an iBGP speaker, and if it does not, then it is an eBGP speaker. An eBGP speaker can advertise prefixes it has learned from another eBGP speaker to a neighboring iBGP speaker; and it can also advertise prefixes it has learned from an iBGP speaker to an eBGP speaker.

Internal BGP – In contrast to eBGP peers which have different AS numbers, iBGP peers are configured with the same AS number. All iBGP peers within the same AS should be connected to one another in a full-mesh connection (except when using route reflection). When a prefix is announced from one iBGP peer to another, the AS path is not changed. Since all iBGP peers are fully meshed, they will have the same information in their BGP table, unless routing policies have been modified for some of the peers.

When a iBGP peer receives a prefix announcement, it uses the best path selection algorithm to see if the received announcement is the best path for that prefix. If it is, the peer inserts this route into its routing table, and announces it to all of its peers, both iBGP and eBGP. If it is not the best available path, the peer keeps a copy of it in its routing table so that if path information for that prefix changes (such as if the current best available path is withdrawn), it can be used to calculate a new best available path.

BGP cannot detect routes and provide reachability information. To ensure that each iBGP peer knows how to reach other, each peer must run some sort of Interior Gateway Protocol (such as static routes, direct routes, RIP or OSPF) which provides neighbor IP addresses. In order to avoid routing loops, an iBGP speaker cannot advertise prefixes it has learned from one iGBP peer to another neighboring iBGP peer.

BGP ROUTING BASICS

Both RIP and OSPF attach a metric, or cost, to each path. These protocols rely on every router attaching the same meaning to each metric, allowing consistent calculation of routes. However, after routing policies are put in place, routers may value some metrics differently, invalidating the basic assumptions up which RIP and OSPF are based. This makes it unrealistic to run a distance-vector AS-level protocol

BGP uses a path vector routing approach, which is roughly based on a distance-vector approach, where the cost between two adjacent ASes is implicitly assumed to be a single hop. The shortest path from an AS to a remote AS is therefore the path with the shortest number or AS hops. Just note that each AS may be comprised of multiple routers or networks that a packet traverses as it crosses the associated route to the destination, so the AS hop count does not equal to the number of routers along that path.

PATH ATTRIBUTES

The key information passed along with the path vector in routing messages include the following attributes:

- ORIGIN – This attribute indicates how the network of BGP routers first learned of a route, and is set by the first BGP router to introduce the routes to its peers. There are three methods for injected a prefix into an update message: IGP, EGP and Incomplete.
- AS_PATH – This attribute lists the autonomous systems that make up the path to the routes' destination. Each entry contains a series of path segments. Each path segment begins with a 1 for SETS or a 2 for SEQUENCES, where a SET indicates that it is an aggregate prefix which was derived from multiple ASes.
- NEXT_HOP – This attribute indicates the IP address of the router that should be used as the next hop to reach the router' destination. This address is normally that of the router sending the BGP message, but a BGP router may advertise a route on behalf of another router.
- MULTI_EXIT_DISC (MED) – The multi-exit discriminator attribute lets an autonomous system set a preference for different routes when there are multiple external links to a neighboring AS. Selection is normally based on the exit point with the lowest metric.
- WEIGHT – This attribute is used locally by a router to select a path when multiple paths are available for a prefix.

- LOCAL_PREF – This local preference attribute is similar to that of the MED, but within an AS. It sets a metric which is used between BGP speakers within an AS. It can help in selecting an outgoing BGP when an AS has connectivity to multiple ASes or multiple BGP routes even with the same next hop AS.
- ATOMIC_AGGREGATE – This attribute indicates that the routes were created by aggregating more specific routes. More specific routes may exist for some the these longer prefixes, but the router chose not to send them, so as to reduce the size for the AS path parameters.
- AGGRATOR – This is an optional attribute that identifies the AS and router that originally aggregated the routes.
- COMMUNITY – This attribute associates routing information with a community of users. These communities share a common property, and tagging routes with a community makes it easier for routers to identify that property and enforce appropriate routing policies.
- ORIGINATOR_ID – This attribute is included when a route reflector reflects a route. Then if the reflector later receives a route with its own originator ID, a potential routing loop can be broken.
- CLUSTER_LIST – This attribute is of a list of the clusters through which a route has been reflected. Every route reflector adds its own cluster ID to the list. If the reflector receives a route with its own cluster ID, a potential routing loop can be broken.
- MP_REACH_NLRI – This attribute describes routes for network protocols other than IPv4. The attribute identifies the protocol with an address family identifier (AFI) and a subsequent address family identifier (SAFI). It contains the address of the next hop router for the destinations, as well as the link level (e.g., Ethernet) addresses for that next hop. It concludes with the destinations expressed as prefixes.
- MP_UNREACH_NLRI – This attribute withdraws non-IPv4 routes. It includes the route’s AFI, SAFI, and network address prefixes.
- EXTENDED-COMMUNITIES – This attribute provides a mechanism for labeling various information carried in route advertisements. It provides an extended type field to ensure that communities can be assigned for a broad range of uses, without fear of overlap.

PATH SELECTION

When there are multiple paths to the same prefix (with the same prefix length), the information included in route advertisement is used to select the best path to a destination following the rules shown below.

1. Choose the path with the highest WEIGHT. If the value of this attribute is the same for more than one candidate, go to the next step.

2. Choose the path with the highest LOCAL-PREF. If the value of this attribute is the same for more than one candidate, go to the next step.

3. Choose the path that was generated by the local router with the network or aggregate-address command. If the value of this criteria is the same for more than one candidate, go to the next step.

4. Choose the path with the shortest AS_PATH. If the value of this attribute is the same for more than one candidate, go to the next step. Note that this attribute may be disabled in the selection process using the bgp bestpath as-path ignore command.

5. Choose the path with the lowest ORIGIN (IGP < EGP < Incomplete). If the value of this criteria is the same for more than one candidate, go to the next step.

6. Choose the path with the lowest MED. By default, the MED attribute is considered only when a prefix is received from neighbors in the same AS. If the value of this criteria is the same for more than one candidate, go to the next step.

7. Choose an eBGP path over an outer confederation, and an outer confederation over an iBGP path. If the value of this criteria is the same for more than one candidate, go to the next step.

8. Choose the path with the lowest IGP metric to the next hop. If the value of this criteria is the same for more than one candidate, go to the next step.

9. Choose the path originated by the BGP router with the lowest router ID.

MESSAGE TYPES

Four message types are used by BGP. The OPEN message is used by BGP peers to identify their capabilities, the UPDATE message is used to advertise/withdraw prefixes, the NOTIFICATION message is used to send errors or close the session, and the KEEPALIVE messages is used to keep the BGP session up. These message types are described below.

- OPEN – BGP routers normally wait for BGP connections on TCP port 179. A router that wants to establish an association will first open a TCP connection leading to that port on the peer router. Once the connection has been set, each side sends an OPEN message to negotiate the association’s parameters based on the capabilities advertised in these messages. Open messages include information about the BGP version number in use, the peer’s AS number, the hold time, the BGP identifier (i.e., loopback address or the highest value of all the BGP speaker’s interfaces), and optional parameter length.

- UPDATE – These messages are used to announce or withdraw IP prefixes, and include the following components: withdrawn route length, withdrawn routes, total path attributes length, path attributes, and network layer reachability information.

- NOTIFICATION – These messages are used to indicate error conditions. The underlying TCP session is closed after a notification message is sent.

- KEEPALIVE – These messages are sent at a set interval and are used to verify that the BGP session is active. The hold timer is reset upon receipt of a KEEPALIVE or UPDATE message. If the hold time is set to zero by both peers, a BGP session can be kept open without generating KEEPALIVE messages.

ROUTE AGGREGATION AND DISSEMINATION

In the Internet, the number of destinations is larger than most routing protocols can manage. It is not possible for routers to track every possible destination in their routing tables. To overcome this problem BGP relies on route aggregation, whereby multiple destinations are combined in a single advertisement. Routers receiving this information, treat the combined destinations as a single destination, thus reducing the number of individual routes that must be remembered. This also reduces the network overhead required to transmit update packets and maintain routing tables.

In BGP, route aggregation combines the address blocks for networks from two or more ASes into a supernet, and transmits this information to a downstream AS. This supernetted address block is less specific, and only lists the AS number of the AS where the supernetting was done. The Atomic_Aggregate attribute indicates that attributes for more specific paths are not included in the aggregated route, and the Aggregator attribute indicates the AS and router where the aggregation was done. The aggregator node will now serve as a proxy, using the more specific routes it still maintains in its own routing table.

After inbound routes have been aggregated, the BGP speaker can propagates this information based on export policies for individual neighbors or for defined router groups, using route maps or other more precise routing criteria.

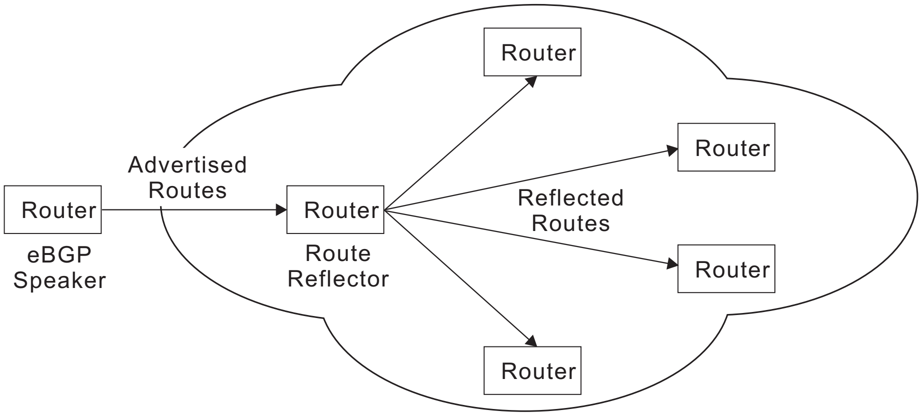
INTERNAL BGP SCALABILITY

An iBGP speaker cannot advertise IP prefixes it has learned from one iBGP speaker to another neighboring iBGP speaker. iBGP therefore requires full-mesh connectivity among all iBGP speakers. For local networks containing a large number of speakers, this requirement may be difficult to meet. There are several commonly used approaches to resolving this problem, including route reflectors, confederations, and route servers.

ROUTE REFLECTORS

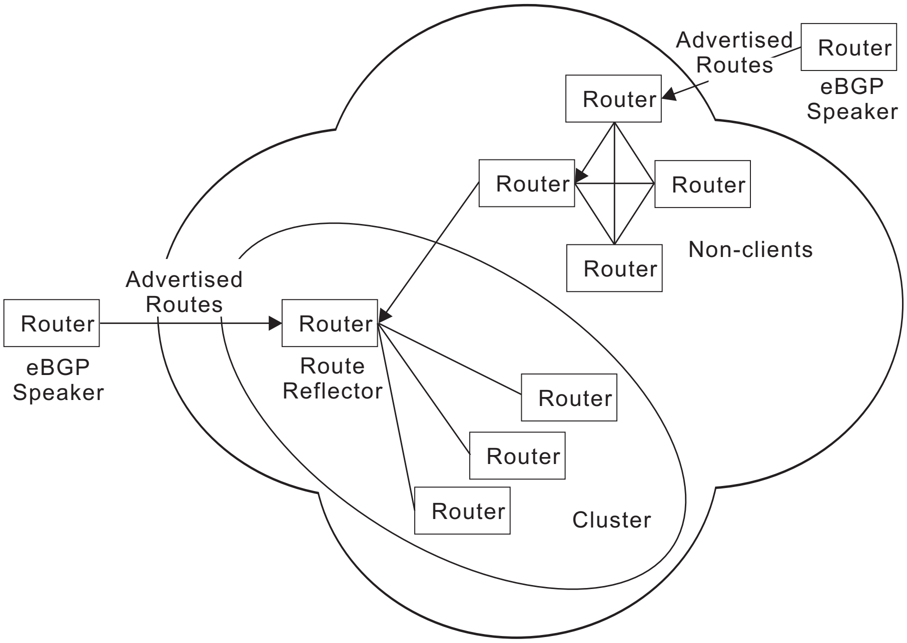
Route reflection designates one or more iBGP speakers as router concentrators or route reflectors, which are allowed to re-advertise routing information within the same autonomous system. It also clusters a subset of iBGP speakers with each route reflector (also known as route reflector clients), and adds several new attributes to help detect routing loops. Using the cluster hierarchy, connections are only required between the route reflector and its clients, overcoming the normal requirement for full-mesh connectivity among all iBGP speakers.

Figure 556: Connections for Single Route Reflector



Route reflector clients are not aware that they are connected to a route reflector, and function as though fully meshed within the autonomous system. For redundancy, a cluster many contain more than one route reflector. Each cluster is identified a Cluster-ID. When there is only one route reflector in a cluster, the Cluster-ID is the BGP identifier of the route reflector. If there is more than one route reflector in a cluster, a common identifier can be defined for use by all route reflectors in the cluster.

Figure 557: Connections for Multiple Route Reflectors



If there is only one route reflector in a cluster, that router would still have to process the same number of routing messages that would be required if it were in a fully meshed network. It is therefore preferable to use more than one route reflector in a cluster to reduce the overall number of iBGP sessions a single reflector has to handle.

If multiple route reflectors are configured in the same cluster, they must be fully meshed with each other. However, the route reflector clients only need to be connected to its designated route reflector. Once all iBGP routing sessions are established, routing advertisements must follow these rules:

- Announcements received by a route reflector from another reflector are passed to its clients.

- Announcements received by a route reflector from a reflector client are passed to other route reflectors in the cluster.

- Announcements received by a route reflector from an eBGP speaker are passed to all route reflectors in the cluster and to its own clients.

It can now be seen that routing information learned from an iBGP speaker can be passed to another iBGP speaker. This breaks the normal rules for a fully meshed iBGP autonomous system, and other steps are now required to avoid routing loops. These include the addition of the following new attributes:

- Originator-ID – When a route reflector learns about a route from one of its clients, it adds this attribute to the announcement before reflecting it to other speakers. If a route reflector receives an announcement about a route with an Originator-ID that matches its own router ID, it should drop it.

- Cluster-List – This is a list of the clusters through which a route announcement has passed. When a route reflector passes on an announcement, it must prepend the local Cluster-ID to this list. The Cluster-List thereby serves a similar function to the AS-Path attribute in detecting routing loops.

Configuration Guidelines

1. Route reflection from this router is enabled by default. If it has been disabled, use the bgp client-to-client reflection command to restore route reflection via this router.

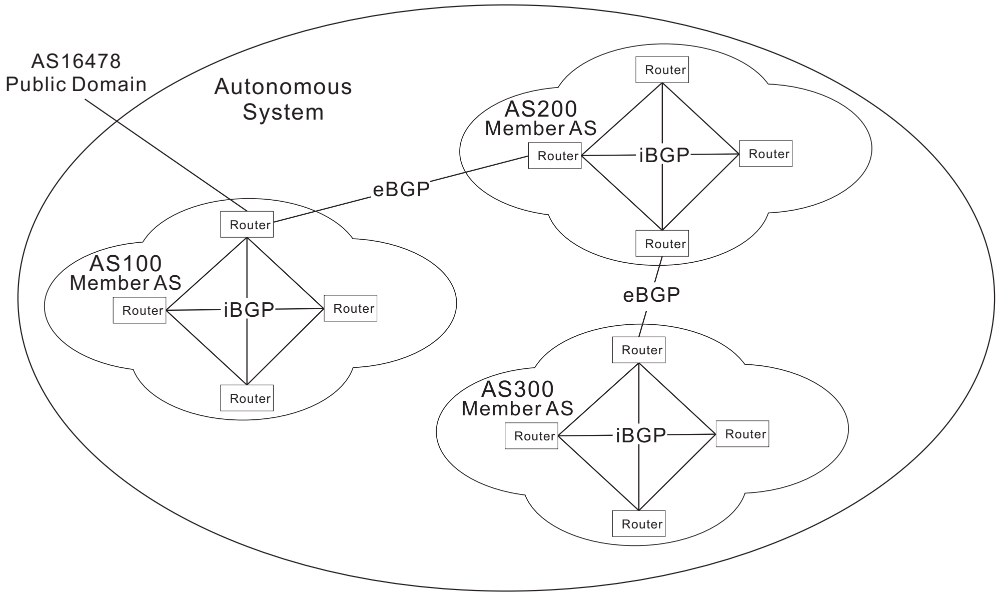
2. If more than one route reflector is used, use the bgp cluster-id command to configure the cluster identifier.

3. Use the neighbor route-reflector-client command configure a neighboring router as a client.

CONFEDERATIONS

Confederations simply divides an autonomous system into smaller groups. It splits up an AS into multiple sub-ASes, where full mesh connections are maintained only within each sub-As, and sub-ASes are connected by eBGP. The overall AS is known as a confederation, while the sub-ASes may also be referred to as member ASes. The entire confederation has a unique AS number, while the member ASes may have AS numbers obtained from public AS number space, or use AS number from private AS number space.

Figure 558: Connections for BGP Confederation



To prevent looping within the confederation, the AS-Confed-Set and AS-Confed-Sequence path attributes are added. These attributes function in the same manner as AS-Set and AS-Sequence. The following additional requirements are applied for route advertisements passed between member ASes:

- The Local-Pref for a route may be passed from one member AS to another member AS. This exception to normal practice is allowed within the confederation since this attribute is meant for use by the entire AS.
- The Next-Hop for a route set by the first BGP speaker in the confederation may be passed from one member AS to another member.
- When a route advertisement is passed from one member AS to another, the AS-Confed-Sequence must be inserted into the AS-Path along with the AS number of the member AS to help prevent looping.

Border routers that also peer with outside ASes have to modify routing information that leaves the confederation so that the internal structure of the confederation remains hidden to exterior peers, primarily because this information is of no use to another external AS. The information stripped from route advertisements and update messages sent outside of the confederation include AS-Confed-Sequence and AS-Confed-Set. Neither are AS numbers of member ASes advertised to exterior peers.

Configuration Guidelines

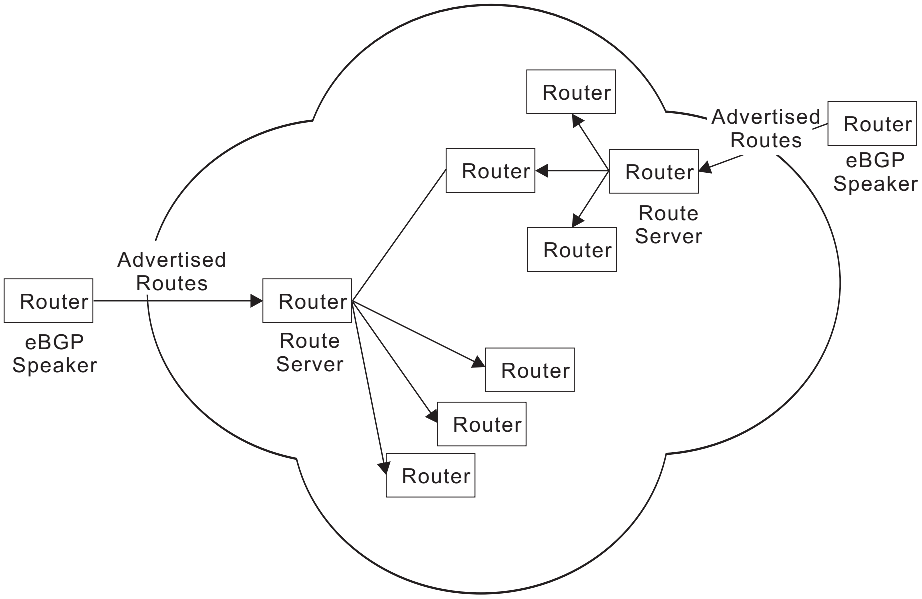
1. Use the bgp confederation identifier command to configures the identifier for a confederation containing smaller multiple internal autonomous systems.

2. Use the bgp confederation peer command to add an internal peer autonomous system to a confederation.

ROUTE SERVERS

Route Servers are used to relay routes received from remote ASes to client routers, as well as to relay routes between client routers. Clients maintain BGP sessions only with the assigned route servers. Sessions with more than one server can be used to provide redundancy and load sharing. All routes received from a client router are propagated to other clients through the Route Server. Since all external routes and their attributes are relayed unmodified between client routers, they acquire the same routing information as they would via direct peering in a full mesh configuration.

Figure 559: Connections for Route Server



Configuration Guidelines

Use the neighbor route-server-client command to configure this router as a route server and the specified neighbor as its client.

ROUTE FLAP DAMPENING

An update message is sent from a BGP speaker to a neighboring speaker whenever any change to a route occurs. A speaker announcing such a route is also responsible for any changes, including withdrawal, change in AS-Path or Next-Hop, to the same neighbor, irrespective of where the change was learned. In practice this may cause a BGP speaker to announce a new route, and then almost immediately withdraw or update the route a few seconds later, repeatedly. Since routing information is propagated to other downstream speakers, there is a ripple effect that creates a cascading storm of updates through the ASes. This causes instability in the routing tables, as well as the computational overhead required to compute the best path, and an increase in convergence time.

Route damping provides a relief mechanism to minimize the effects of route flapping. It can reduce the propagation of updates for flapping routes without impacting the route convergence time for stable routes. When enabled, a route is assigned a penalty each time it flaps (i.e., announced and then quickly withdrawn). If the penalty exceeds 2000 (the suppress limit) the route is suppressed. After the route remains stable for a specified interval (half-life), the penalty is reduced by half. Subsequently, the penalty is reduced every 15 minutes. When the penalty falls below a specified value (reuse limit), the route is unsuppressed.

The penalty never exceeds the maximum penalty, which is computed from specified attributes as shown below:

Maximum penalty = reuse-limit * 2^(max-suppress-time/half-life)

When a route is being “damped,” any updates or withdrawals for this route received from a peer are ignored. This limits the effects of route flapping to a single peering connection. Since most ASes are connected by high-speed links, it is not always necessary to use route dampening. However, when invoked, it may be necessary to fine tune the penalty attributes to ensure fair treatment to unstable routes.

Configuration Guidelines

1. Use the bgp dampening command to enable route dampening.

2. Use the bgp dampening command to adjust the penalty attributes of *half-life*, *reuse-limit*, *suppress-limit*, and *max-suppress-time*.

3. Use the clear ip bgp dampening command to clears route dampening information and unsuppresses any suppressed routes.

BGP COMMAND LIST

Table 270: Border Gateway Protocol Commands – Version 4

Command	Function	Mode
General Configuration		
router bgp	Enables BGPv4 routing process and enters router configuration mode	GC
ip as-path access-list	Configures an autonomous system path access list	GC
ip community-list	Configures a community list	GC
ip extcommunity-list	Configures an extended community list	GC
ip prefix-list	Configures an address prefix list	GC
aggregate-address	Configures an aggregate address in the routing table	RC

Table 270: Border Gateway Protocol Commands – Version 4 (Continued)

Command	Function	Mode
bgp client-to-client reflection	Configures route reflection between clients via route reflector	RC
bgp cluster-id	Configures cluster identifier for multiple route reflectors in the same cluster	RC
bgp confederation identifier	Configures the identifier for a confederation containing smaller multiple internal autonomous systems	RC
bgp confederation peer	Adds an internal peer autonomous system to a confederation	RC
bgp dampening	Configures route dampening to reduce the propagation of unstable routes	RC
bgp enforce-first-as	Denies an update received from an external peer that does not list its own autonomous system number at the beginning of the AS path attribute	RC
bgp fast-external-failover	Resets sessions for any directly connected external peers if the link goes down	RC
bgp log-neighbor-changes	Enables logging of neighbor resets (that is, up or down status changes)	RC
bgp network import-check	Checks the existence of the next-hop and its accessibility to IGP	RC
bgp router-id	Sets the router ID for this device	RC
bgp scan-time	Sets the interval at which to validate next hop information for BGP routes	RC
network	Specifies a network to advertise	RC
redistribute	Redistribute routes from one routing domain to another	RC
timers bgp	Sets the Keep Alive time used for maintaining connectivity, and the Hold time to wait for Keep Alive messages before declaring a neighbor down	RC
clear ip bgp	Clears connections using hard or soft re-configuration	PE
clear ip bgp dampening	Clears route dampening information and unsuppresses any suppressed routes	PE
Route Metrics and Selection		
bgp always-compare-med	Allows comparison of the Multi Exit Discriminator (MED) for paths advertised from neighbors in different autonomous systems	RC
bgp bestpath as-path ignore	Ignores AS path length in the selection of a path	RC
bgp bestpath compare-confed-aspath	Compare confederation AS path length in addition to external AS path length in the selection of a path	RC
bgp bestpath compare-routerid	Compare similar routes from external peers, and give preference to a route with the lowest router identifier	RC
bgp bestpath med	Enables comparison of MED attribute for paths learned from confederation peers, and the treatment of a route when the MED is missing	RC
bgp default local-preference	Sets the default local preference used for best path selection among local iBGP peers	RC
bgp deterministic-med	Enforces deterministic comparison of the MED attribute between all paths received from the same AS, ensuring that selection of the best path will always be the same, regardless of the order in which the paths are received by the local router	RC

Table 270: Border Gateway Protocol Commands – Version 4 (Continued)

Command	Function	Mode
distance	Sets the administrative distance for a specified external BGP (eBGP) route	RC
distance bgp	Sets the administrative distance for BGP external, internal, and local routes	RC
Neighbor Configuration		
neighbor activate	Enables exchange of routing information with a neighboring router or peer group	RC
neighbor advertisement-interval	Configures the interval between sending update messages to a neighbor	RC
neighbor allowas-in	Configures the number of times the AS path for a received route can contain the same AS number	RC
neighbor attribute-unchanged	Configures certain attributes to be kept unchanged for transparent transmission to the specified neighbor	RC
neighbor capability dynamic	Configures dynamic negotiation of capabilities between neighboring routers	RC
neighbor capability orf prefix-list	Configures negotiation of outbound route filter capabilities with neighboring router	RC
neighbor default-originate	Allows the local router to send a default route to a neighbor	RC
neighbor description	Configures the description of a neighbor or peer group	RC
neighbor distribute-list	Filters route updates to/from a neighbor or peer group	RC
neighbor dont-capability-negotiate	Disables capability negotiation when creating connections	RC
neighbor ebgp-multihop	Allows eBGP neighbors to exist in different segments, and configures the maximum hop count (TTL)	RC
neighbor enforce-multihop	Enforces the requirement for all neighbors to form multi-hop connections	RC
neighbor filter-list	Filters route updates sent to or received from a neighbor based on an AS path access-list	RC
neighbor interface	Specifies the interface to a neighbor	RC
neighbor maximum-prefix	Sets the maximum number or route prefixes that can be received from a neighbor	RC
neighbor next-hop-self	Configures the local router as the next hop for a neighbor	RC
neighbor override-capability	Overrides the result of capability negotiations, allowing a session to be formed with a peer that does not support capability negotiation	RC
neighbor passive	Passively forms a connection with the specified neighbor, not sending a TCP connection request, but waiting a request from the specified neighbor	RC
neighbor peer-group (Creating)	Configures a router peer group which can be easily configured with the same attributes	RC
neighbor peer-group (Group Members)	Assigns routers to a peer group	RC
neighbor port	Specifies the TCP port number of the partner through which communications are carried	RC
neighbor prefix-list	Configures prefix restrictions applied in inbound/ outbound route updates to/from specified neighbors	RC

Table 270: Border Gateway Protocol Commands – Version 4 (Continued)

Command	Function	Mode
neighbor remote-as	Configures a neighbor and its AS number, identifying the neighbor as a local AS member	RC
neighbor remove-private-as	Removes private autonomous system numbers from outbound routing updates to an external neighbor	RC
neighbor route-map	Specifies the route mapping policy for inbound/ outbound routing updates for specified neighbors	RC
neighbor route-reflector-client	Configures this router as a route reflector and the specified neighbor as its client	RC
neighbor route-server-client	Configures this router as a route server and the specified neighbor as its client	RC
neighbor send-community	Configures the router to send community attributes to a neighbor in peering messages	RC
neighbor shutdown	Closes a neighbor connection without canceling the neighbor configuration	RC
neighbor soft-reconfiguration inbound	Configures the switch to store updates in the inbound message buffer, and perform soft re-configuration from this buffer for specified neighbors when required	RC
neighbor strict-capability-match	Forces strict capability matching when establishing connections	RC
neighbor timers	Sets the Keep Alive time and Hold time used for specified neighbors	RC
neighbor timers connect	Sets the time to wait before attempting to reconnect to a neighbor whose TCP connection has failed	RC
neighbor unsuppress-map	Allows specified suppressed routes to be advertised	RC
neighbor update-source	Specifies the interface to use for a connection, instead of using the nearest interface	RC
neighbor weight	Assigns a weight to a neighbor connection	RC
Display Information		
show ip bgp	Shows entries in the routing table	PE
show ip bgp attribute-info	Shows internal attribute information	PE
show ip bgp cidr-ony	Shows routes which use classless inter-domain routing network masks	
show ip bgp community	Shows routes that belong to specified BGP communities	PE
show ip bgp community-info	Shows permitted community messages	PE
show ip bgp community-list	Shows the routes matching a community-list	PE
show ip bgp dampening	Shows dampened routes	PE
show ip bgp filter-list	Shows routes matching the specified filter list	PE
show ip bgp neighbors	Shows connection information for neighbor sessions	PE
show ip bgp paths	Shows all paths in the database	PE
show ip bgp prefix-list	Shows routes matching the specified prefix-list	PE
show ip bgp regexp	Shows routes matching the AS path regular expression	PE
show ip bgp route-map	Shows routes matching the specified route map	PE

Table 270: Border Gateway Protocol Commands – Version 4 (Continued)

Command	Function	Mode
show ip bgp scan	Shows BGP scan status	PE
show ip bgp summary	Shows summary information for all connections	PE
show ip community-list	Shows routes permitted by a community list	PE
show ip extcommunity-list	Shows routes permitted by an extended community list	PE
show ip prefix-list	Shows the specified prefix list	PE
show ip prefix-list detail	Shows detailed information for the specified prefix list	PE
show ip prefix-list summary	Shows summary information for the specified prefix list	PE

General Configuration

router bgp

This command enables the Border Gateway Protocol (BGPv4) routing process and enters router configuration mode. Use the **no** form to disable it.

SYNTAX

[**no**] **router bgp** *as-number*

as-number – Autonomous system number which identifies this router as a member of the specified domain, and tags routing messages passed to other BGP routers with this number. (Range: 1-4294967295)

COMMAND MODE

Global Configuration

DEFAULT SETTING

No routing process is defined.

COMMAND USAGE

- To enable BGP routing, you must use this command to establish a BGP routing process. After entering this command, the switch enters router configuration mode.

- AS numbers in the range 64512-65535 are normally used for private routing domains, and can be removed from the AS path attribute in outbound routing messages using the neighbor remove-private-as command. Note that AS number 23456 is reserved for the AS-Transitive attribute which is required when setting up a new BGP speaker.

- Use this command to specify all of the routers within an autonomous system used to exchange interior or exterior BGP routing messages. Repeat this process for any other autonomous system under your administrative control to create a distributed routing core for the exchange of routing information between autonomous systems.

EXAMPLE

```
Console(config)#router bgp 100
Console(config-router)#
```

RELATED COMMANDS

network (1848)

ip as-path access-list

This command configures an autonomous system path access list. Use the **no** form with only the access list name to disable its use, or with all parameters to remove a path attribute from the access list.

SYNTAX

ip as-path access-list *access-list-name* {**deny** | **permit**} *regular-expression*

no ip as-path access-list *access-list-name* [{**deny** | **permit**} *regular-expression*]

access-list-name – Name of the access list. (Maximum length: 16 characters, no spaces or other special characters)

deny – Permits access for messages with matching path attribute.

permit – Denies access to messages with matching path attribute.

regular-expression – Autonomous system in the access list expressed as a regular expression[29].

COMMAND MODE

Global Configuration

DEFAULT SETTING

No AS path access lists are defined.

COMMAND USAGE

- If the regular expression in an AS path list is matched, then the deny/permit condition is applied to the routing message.
- Use this command in conjunction with the neighbor filter-list command to filter route updates sent to or received from a neighbor, or with the match as-path route map command to implement a more comprehensive filter for policy-based routing.

[29] Syntax complies with the IEEE POSIX Basic Regular Expressions (BRE) standard.

EXAMPLE

The regular expression in this example uses symbols which instruct the filter to match the character or null string at the beginning and end of an input string.

```
Console(config-router)#ip as-path access-list RD deny ^100$
Console(config-router)#
```

RELATED COMMANDS

neighbor filter-list (1867)
match as-path (1902)

ip community-list

This command configures a community access list. Use the **no** form with only the access list name to disable its use, or with all parameters to remove a community attribute from the access list.

SYNTAX

[**no**] **ip community-list**
{1-99 | **standard** *community-list-name* {**deny** | **permit**}
[*AA*:*NN*] [**internet**] [**local-as**] [**no-advertise**] [**no-export**]} |
{100-500 | **expanded** *community-list-name* {**deny** | **permit**}
regular-expression}

1-99 – Standard community list number that identifies one or more groups of communities.

standard *community-list-name* – Name of standard access list. A maximum of 16 communities can be configured in a standard community list (Maximum length: 32 characters, no spaces or other special characters)

deny – Denies access to messages with matching community attribute.

permit – Permits access for messages with matching community attribute.

AA:*NN* – Standard community-number to deny or permit. The 4-byte community number is composed of a 2-byte autonomous system number and a 2-byte network number, separated by one colon. Each 2-byte number can range from 0 to 65535. One or more communities can be entered, separated by a space. Up to 16 community numbers are supported.

internet – Specifies the entire Internet. Routes with this community attribute are advertised to all internal and external peers.

local-as – Specifies the local autonomous system. Routes with this community attribute are advertised only to peers that are part of the local autonomous system or to peers within a sub-autonomous system of a confederation. These routes are not advertised to external peers or to other sub-autonomous systems within a confederation.

no-advertise – Routes with this community attribute are not advertised to any internal or external peer.

no-export – Routes with this community attribute are advertised only to peers in the same autonomous system or to other sub-autonomous systems within a confederation. These routes are not advertised to external peers.

100-500 – Expanded community list number that identifies one or more groups of communities.

expanded *community-list-name* – Name of expanded access list. (Maximum length: 32 characters, no spaces or other special characters)

regular-expression – Regular expression indicating the community list number or name[29].

COMMAND MODE

Global Configuration

DEFAULT SETTING

No community lists are defined.

COMMAND USAGE

- Standard community lists are used to configure well-known communities or community numbers. Expanded community lists are used to filter communities using a regular expression.

- When multiple values are entered in the same community list, they form a logical AND condition. When multiple values are configured in separate community lists, the form a logical OR condition, where the first list that matches a condition is processed.

- If the criteria specified for a community list is matched, then the deny/permit condition is applied to the routing message.

- If a permit value is applied to a community list, the filter will implicitly deny other community values.

- By default, the internet community is set with a route if no other communities are defined.

- Use this command in conjunction with the neighbor send-community to filter route updates sent to or received from a neighbor, or with the match community route map command to implement a more comprehensive filter for policy-based routing.

EXAMPLE

This example configures a named standard community list LN that permits routes with community value 100:10, denoting that they come from autonomous system 100 and network 10.

```
Console(config)#ip community-list standard LN permit 100:10
Console(config)#
```

RELATED COMMANDS

neighbor send-community (1878)
match community (1902)

ip extcommunity-list

This command configures an extended community access list. Use the **no** form with only the access list name to disable its use, or with the relevant parameters to remove a community attribute from the access list.

SYNTAX

[**no**] **ip extcommunity-list**
{1-99 | **standard** *community-list-name* {**deny** | **permit**}
[{**rt** | **soo**} *extended-community-value*]} |
{100-500 | **expanded** *community-list-name* {**deny** | **permit**}
regular-expression}

1-99 – Standard community list number that identifies one or more groups of communities.

standard *community-list-name* – Name of standard access list. A maximum of 16 extended communities can be configured in a standard community list. (Maximum length: 32 characters, no spaces or other special characters)

deny – Denies access to messages with matching extended community attribute.

permit – Permits access for messages with matching extended community attribute.

rt – The route target extended community attribute.

soo – The site of origin extended community attribute.

extended-community-value – The route target or site of origin in one of the following formats:

AAAA:*NN* or *AA*:*NNNN* – Community-number to deny or permit. The community number can either be formatted as a 4-byte autonomous system number and a 2-byte network number, or as a 2-byte autonomous system number and a 4-byte network number, separated by one colon. Each 2-byte number can range from 0 to 65535, and 4-byte numbers from 0 to 4294967295.

IP:*NN* – Community to deny or permit. The community number is composed of a 4-byte IP address (representing the autonomous system number) and a 2-byte network number, separated by one colon. The 2-byte network number can range from 0 to 65535.

One or more community numbers can be entered, separated by a space. Up to 3 community numbers are supported.

100-500 – Expanded community list number that identifies one or more groups of communities.

expanded *community-list-name* – Name of expanded access list. (Maximum length: 32 characters, no spaces or other special characters)

regular-expression – Regular expression indicating the community list number or name. Syntax complies with the IEEE POSIX Basic Regular Expressions (BRE) standard.

COMMAND MODE

Global Configuration

DEFAULT SETTING

No extended community lists are defined.

COMMAND USAGE

- Standard community lists are used to configure well-known communities or community numbers. Expanded community lists are used to filter communities using a regular expression.

- When multiple values are entered in the same community list, they form a logical AND condition. When multiple values are configured in separate community lists, the form a logical OR condition, where the first list that matches a condition is processed.

- If the criteria specified for a community list is matched, then the deny/permit condition is applied to the routing message.

- If a permit value is applied to a community list, the filter will implicitly deny other community values.

- The route target (RT) attribute is used to identify sites that may receive routes tagged with a specific route target. Using this attribute allows that route to be placed in per-site forwarding tables used for routing traffic received from the corresponding sites.

- The site of origin (SOO) attribute is used to identify the site from which the provider edge (PE) router learned the route. All routes learned from a particular site are assigned the same site of origin attribute, no matter if a site is connected to a single PE router or multiple PE routers. Filtering based on this extended community attribute can prevent routing loops from occurring when a site is multi-homed.

- Use this command in conjunction with the neighbor filter-list to filter route updates sent to or received from a neighbor, or with the match extcommunity route map command to implement a more comprehensive filter for policy-based routing.

EXAMPLE

This example configures a named standard community list LR that permits routes with the route target 100:20, denoting that they destined for the autonomous system 100 and network 20.

```
Console(config)#ip extcommunity-list standard LP permit soo 100:20
Console(config)#
```

RELATED COMMANDS

neighbor filter-list (1867)
match extcommunity (1903)

ip prefix-list

This command configures an IP address prefix list. Use the **no** form with only the prefix list name to disable its use, or with the relevant parameters to remove an attribute from the prefix list.

SYNTAX

[**no**] **ip prefix-list** *prefix-list-name* [**seq** *sequence-number*]
{**deny** | **permit**} **any**

[**no**] **ip prefix-list** *prefix-list-name* [**seq** *sequence-number*]
{**deny** | **permit**} {*ip-address netmask* | **any**}
[**ge** *min-prefix-length*] [**le** *max-prefix-length*]

prefix-list-name – Name of prefix list. (Maximum length: 128 characters, no spaces or other special characters)

sequence-number – Applies a sequence number to the entry. If not specified, the entry is added to the bottom of the list, using a default numbering interval of 5. (Range: 1-429496725)

deny – Denies access to messages matching specified criteria.

permit – Permits access for messages matching specified criteria.

any – Any matching criteria.

ip-address – An IPv4 address expressed in dotted decimal notation.

netmask – Network mask for the route. This mask identifies the network address bits used for the associated routing entries.

ge – The minimum prefix length to match.

le – The maximum prefix length to match.

COMMAND MODE

Global Configuration

DEFAULT SETTING

No prefix lists are defined.

COMMAND USAGE

- Prefix filtering can be performed on an IP address expressed as a classful network, a subnet, or a single host route.

- Prefix lists are checked starting from the lowest sequence number and continues through the list until a match is found. Once an entry is found that covers a network, the permit or deny statement is applied to that network, and the search process stops.

- At least one "permit" statement should be included when more than one entry is defined. Commonly used "Deny" statements can be included at the top of the list to quickly remove unsuitable routing messages. If a list includes all "Deny" statements, then an entry of "permit 0.0.0.0 255.255.255.255 ge 0 le 32" can be included at the bottom of the list to grant passage for all other routing messages.

- A prefix list can be applied to inbound or outbound updates for a specific peer by entering the neighbor prefix-list command, or with the match ip address prefix-list route map command to implement a more comprehensive filter for policy-based routing.

EXAMPLE

This example denies access to routing messages for the specified address.

```
Console(config)#ip prefix-list LS deny 10.0.0.0 255.0.0.0 ge 14 le 22
Console(config)#
```

RELATED COMMANDS

neighbor prefix-list (1873)
match ip address (1904)

aggregate-address

This command configures an aggregate address in the routing table. Use the **no** form to delete an aggregate address.

SYNTAX

[**no**] **aggregate-address** *ip-address netmask* [**as-set**]
[**summary-only**]

ip-address – An IPv4 address expressed in dotted decimal notation.

netmask – Network mask for the route. This mask identifies the network address bits used for the associated routing entries.

as-set – Generates autonomous system set information for the AS path attribute, indicating that a route originated in multiple autonomous systems.

summary-only – Sends the summary routes only, ignoring more specific routes.

COMMAND MODE

Router Configuration

DEFAULT SETTING

No aggregate routes are defined.

COMMAND USAGE

- Using this command without any keywords will create an aggregate entry in the routing table if any more specific routes are available in the specified range. The aggregate route does not include any individual route attributes (e.g., AS-Path or Community). It is advertised as coming from this autonomous system and has the atomic aggregate attribute set to indicate that some information may be missing.

- Using the **as-set** keyword creates an aggregate route where the advertised path is an AS-Set that consists of all elements contained in all of paths being summarized. AS-Set information can be used to avoid routing loops because it records where the route has been. If a router notes its own AS number in the AS-Set of the aggregate update, it will drop the aggregate to prevents loop. However, when aggregating tens or hundreds of routes, avoid advertising routing information in this manner, since this route may be frequently withdrawn and updated as AS path reachability information for the summarized routes changes.

- Using the **summary-only** keyword creates the aggregate route, while at the same time suppressing advertisements of more specific routes to all neighbors.

EXAMPLE

```
Console(config-router)#aggregate-address 100.1.0.0 255.255.0.0 summary-only
Console(config-router)#aggregate-address 100.2.0.0 255.255.0.0 summary-only
  as-set
Console(config-router)#aggregate-address 100.3.0.0 255.255.0.0 as-set
Console(config-router)#end
Console#show ip bgp
BGP table version is 0, local router ID is 192.168.0.4
Status codes: s suppressed, d damped, h history, * valid, > best, i -
  internal,
              r RIB-failure, S Stale, R Removed
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric LocPrf Weight Path
*>i192.168.0.0/24   0.0.0.0                  0         32768 i
```

bgp client-to-client reflection

This command restores route reflection via this router. Use the **no** form to disable route reflection.

SYNTAX

[**no**] **bgp client-to-client reflection**

COMMAND MODE

Router Configuration

DEFAULT SETTING

Enabled

COMMAND USAGE

- Route reflection from this device is enabled by default, but is only functional if a client has been configured with the neighbor route-reflector-client command.

- Route reflection is not required if all of the routers in an AS are fully meshed as normally required by interior BGP. However, to make interior BGP more scalable, route reflection or confederations can be used. Route reflection uses one or more route reflectors to reflect routes between specified clients within a cluster. Clients within a reflector cluster therefore need not be fully meshed, and the exchange of routing information is thereby reduced since the clients need not communicate with any routers outside of the cluster.

- Routing information from an external BGP router is advertised to all cluster clients and non-client peers. Information from a non-client peer is advertised to all clients. And information from cluster members is reflected to all routing peers, both inside and outside of the cluster. using this model, the local AS can be divided into many clusters.

- Use the bgp cluster-id command to designate route reflectors within the same cluster so that route reflectors can recognize updates from other route reflectors in the same cluster.

EXAMPLE

```
Console(config-router)#bgp client-to-client reflection
Console(config-router)#
```

RELATED COMMANDS

neighbor route-reflector-client (1876)
bgp cluster-id (1841)

bgp cluster-id

This command configures the cluster identifier for multiple route reflectors in the same cluster. Use the **no** form to remove the cluster identifier.

SYNTAX

bgp cluster-id *cluster-identifier*

no bgp cluster-id

cluster-identifier – The cluster identifier of this router when acting as a route reflector. This identifier can be expressed in the form an IPv4 address or an integer in the range of 1-4294967295.

COMMAND MODE

Router Configuration

DEFAULT SETTING

The router identifier of a lone route reflector in a cluster.

COMMAND USAGE

- A cluster of clients will usually have a single route reflector (RR). In that case, the cluster can be identified by the BGP Identifier of the RR. However, this represents a single point of failure. This command is used to designate multiple route reflectors used within the same cluster so that they can recognize updates from other peer route reflectors and discard them to prevent loopbacks.

- All the route reflectors in the same cluster should be fully meshed and all of them configured with identical sets of client and non-client peers.

- A route reflector uses the non-transitive cluster-list attribute to avoid routing loops. A cluster-list is a sequence of cluster IDs the route has passed through. When a RR reflects a route from its clients to non-client peers, and vice versa, it appends this ID to the cluster list. Using this attribute, an RR can determine if routing information has looped back to the same cluster due to mis-configuration. If the local cluster ID is found in the cluster list, the advertisement is ignored.

EXAMPLE

```
Console(config-router)#bgp cluster-id 192.168.0.0
Console(config-router)#
```

RELATED COMMANDS

bgp client-to-client reflection (1840)

bgp confederation identifier

This command configures the identifier for a confederation containing smaller multiple internal autonomous systems, and declares this router as a member of the confederation. Use the **no** form to remove the confederation identifier.

SYNTAX

bgp confederation identifier *as-number*

no bgp confederation identifier

as-number – Autonomous system number which identifies this router as a member of the specified domain, and tags routing messages passed to other BGP routers with this number. (Range: 1-4294967295)

COMMAND MODE

Router Configuration

DEFAULT SETTING

No confederation identifier is configured.

COMMAND USAGE

- BGP confederations are used to reduce the requirement for fully meshed connections between iBGP peers in the same AS. It works by dividing up a large AS into several smaller ASes, where only the peers in the same smaller AS are fully meshed, thus reducing the number of required connections and routing traffic.

- Even though different local confederation peers may have external BGP (eBGP) sessions, they exchange routing information among themselves as if they were iBGP peers. Next hop, Multi Exit Discriminator (MED), and local preference information is preserved. By preserving this information, a single Interior Gateway Protocol (IGP) can be used among the local confederations. When viewed from the outside by external peers, the larger AS is still identified as a single entity or autonomous system.

- Use the bgp confederation peer command to specify the autonomous systems within a confederation.

EXAMPLE

```
Console(config-router)#bgp confederation identifier 600
Console(config-router)#
```

RELATED COMMANDS

bgp confederation peer (1843)

bgp confederation peer

This command adds an internal peer autonomous system to a confederation. Use the **no** form to remove an autonomous system from a confederation.

SYNTAX

bgp confederation peer *as-number*

no bgp confederation identifier

as-number – Autonomous system number which identifies this router as a member of the specified domain, and tags routing messages passed to other BGP routers with this number. (Range: 1-4294967295)

COMMAND MODE

Router Configuration

DEFAULT SETTING

No confederation peer is configured.

COMMAND USAGE

- This command is used to add multiple ASes to a confederation. Each AS is fully meshed within itself, and the AS members are visible internally within the confederation.

- Use the bgp confederation identifier command to create a confederation.

EXAMPLE

This example divides AS 600 into four smaller ASes 101-104, and assigns a neighboring router as a member of the sub-AS 101.

```
Console(config-router)#bgp confederation identifier 600
Console(config-router)#bgp confederation peer 101
Console(config-router)#bgp confederation peer 102
Console(config-router)#bgp confederation peer 103
Console(config-router)#bgp confederation peer 104
Console(config-router)#neighbor 192.168.0.9 remote-as 101
Console(config-router)#
```

RELATED COMMANDS

bgp confederation identifier (1842)

bgp dampening

This command configures route dampening to reduce the propagation of unstable routes. Use the **no** form to restore the default settings.

SYNTAX

bgp dampening [*half-life* [*reuse-limit* [*suppress-limit max-suppress-time*]]]

no dampening

half-life – The time after which a penalty is reduced. The penalty value is reduced to half of the previous value after the half-life time expires. (Range: 1-45 minutes)

reuse-limit – The point at which the penalty for a flapping route must fall before a route is unsuppressed. (Range: 1-2000)

suppress-limit – The point at which to start suppressing a route. (Range: 1-2000)

max-suppress-time – The maximum time a route can be suppressed. (Range: 1-255 minutes)

COMMAND MODE

Router Configuration

DEFAULT SETTING

half-life: 15 minutes
reuse-limit: 750
suppress-limit: 2000
max-suppress-time: 60 minutes (4 x half-life)

COMMAND USAGE

- Route dampening is used to reduce the frequency of routing updates due to unstable routes. Dampened routes are not used in the BGP decision process nor installed in the routing table.

- Each time a route flaps, the router assigns the route a penalty of 1000. If BGP receives an attribute change, BGP increases the penalty by 500.

Penalties are cumulative, and the penalty for the route is stored in the BGP routing table until it exceeds the suppress limit. At that point, the route state changes to damped.

- Note that route dampening only applies to external BGP routes.

EXAMPLE

```
Console(config-router)#bgp dampening 20 1200 20000 220
Console(config-router)#
```

bgp enforce-first-as

This command denies an update received from an external peer that does not list its own autonomous system number at the beginning of the AS path attribute. Use the **no** form to disable this feature.

SYNTAX

[**no**] **bgp enforce-first-as**

COMMAND MODE

Router Configuration

DEFAULT SETTING

Disabled

COMMAND USAGE

This command can be used to prevent a peer from misdirecting traffic by advertising a route as if sourced from another autonomous system.

EXAMPLE

```
Console(config-router)#bgp enforce-first-as
Console(config-router)#
```

bgp fast-external-failover

This command resets sessions for any directly connected external peers if the link goes down. Use the **no** form to disable this feature.

SYNTAX

[**no**] **bgp fast-external-failover**

COMMAND MODE

Router Configuration

DEFAULT SETTING

Enabled

COMMAND USAGE

- This command immediately resets the connection for directly adjacent external peers if the interface goes down for any reason other than TCP timeout.
- If fast external failover is disabled, the routing process waits until the default hold timer expires to reset the session.

EXAMPLE

```
Console(config-router)#bgp fast-external-failover
Console(config-router)#
```

bgp log-neighbor-changes

This command enables logging of neighbor resets (that is, up or down status changes). Use the **no** form to disable this feature.

COMMAND MODE

Router Configuration

DEFAULT SETTING

Disabled

COMMAND USAGE

- This command helps detect network problems by indicating if a neighbor connection is flapping. A high number of neighbor resets might indicate unacceptable error rates or high packet loss in the network.
- Log messages for neighbor resets are recorded as level 6 messages in the system log file which can viewed using the show log ram command.

EXAMPLE

```
Console(config-router)#bgp log-neighbor-changes
Console(config-router)#
```

bgp network import-check

This command checks for the existence of the next-hop and its accessibility to an Interior Gateway Protocol. Use the no form to disable this feature.

SYNTAX

[**no**] **bgp network import-check**

COMMAND MODE

Router Configuration

DEFAULT SETTING

Disabled

COMMAND USAGE

By default, BGP will advertise a route regardless of the Interior Gateway Protocol (IGP) in use. This command forces the router to verify the existence of the next hop for an advertised route, and to ensure that the route is accessible to an IGP.

EXAMPLE

```
Console(config-router)#bgp network import-check
Console(config-router)#
```

bgp router-id

This command sets the router ID for this device. Use the no form to remove this ID.

SYNTAX

bgp router-id *router-id*

no bgp router-id

router-id – Router ID formatted as an IPv4 address.

COMMAND MODE

Router Configuration

DEFAULT SETTING

The highest IP address configured for an interface.

COMMAND USAGE

- By default, the router ID is automatically set to the highest IP address configured for a Layer 3 interface. This command can be used manually set the router ID to a fixed value.
- The router ID must be unique for every router in the autonomous system. Using the default setting based on the highest interface address ensures that each router ID is unique.
- All neighbor sessions will be reset if the router ID is changed.

EXAMPLE

```
Console(config-router)#bgp router-id 192.168.0.254
Console(config-router)#
```

bgp scan-time

This command sets the interval at which to validate next hop information for BGP routes. Use the **no** form to restore the default setting.

Syntax

bgp scan-time *scan-time*

no bgp scan-time

scan-time – Next hop validation interval. (Range: 5-60 seconds)

Command Mode

Router Configuration

Default Setting

60 seconds

Command Usage

This command sets the interval at which to check the validity of the next hop for all routes in the routing information database. During the interval between scan cycles, IGP instability or other network problems may cause black holes or routing loops to form.

Example

```
Console(config-router)#bgp scan-time 30
Console(config-router)#
```

network

This command specifies a network to advertise. Use the **no** form to stop advertising a network.

Syntax

network *ip-address* [*netmask*] [**route-map** *map-name* | [**backdoor**] **pathlimit** *ttl*]

no network *ip-address* [*netmask*]

ip-address – IP address of a to advertise.

netmask – Network mask for the route. This mask identifies the network address bits used for the associated routing entries.

map-name – Name of the route map. The route map can be used to filter the networks to advertise. (Range: 1-80 characters)

backdoor – Specifies a backdoor route to a BGP border router that provides better information about the network.

pathlimit *ttl* – Maximum number of hops allowed in an AS path. (Range: 0-255)

Command Mode

Router Configuration

DEFAULT SETTING

No networks are configured.

COMMAND USAGE

- Use this command to specify the networks to advertise to BGP neighbors. BGP networks can be learned from directly connected routes, dynamic routing, or static route sources.

- BGP only sends and receives updates on interfaces specified by this command. If a network is not specified, the interfaces in that network will not be advertised in any BGP updates.

- A backdoor network has an administrative distance of 200, making routes learned through interior gateway protocols (RIP, OSPF, iBGP) preferred. A backdoor network is treated as a local network, except that it not advertised by the local router. A backdoor route should not be sourced at the local router, but should be one that has been learned from external neighbors. However, since these routes are treated as a local network, they are given priority over routes learned through eBGP, even if the distance of the external route is shorter.

EXAMPLE

```
Console(config-router)#network 172.16.0.0 255.255.0.0
Console(config-router)#
```

redistribute

This command redistributes routes from one routing domain to another. Use the **no** form to stop redistributing an previously configured entry.

SYNTAX

redistribute {**connected** | **ospf** | **rip** | **static**} [**metric** *metric-value*] [**route-map** *map-name*]

no redistribute {**connected** | **ospf** | **rip** | **static**} [**metric** *metric-value*] [**route-map** *map-name*]

connected - Imports routes that are established automatically just by enabling IP on an interface.

ospf - External routes will be imported from the Open Shortest Path First (OSPF) protocol into this routing domain.

rip - External routes will be imported from the Routing Information Protocol (RIP) into this routing domain.

static - Static routes will be imported into this routing domain.

metric-value - Metric value assigned to all external routes for the specified protocol. (Range: 1-16)

map-name – Name of the route map. The route map can be used to filter the networks to advertise, and to modify their weight or other attributes. (Range: 1-80 characters)

COMMAND MODE

Router Configuration

DEFAULT SETTING

No redistribution is configured.

COMMAND USAGE

- Use this command to advertise routes that are learned by some other means, such as from another routing protocol or static routing entries. Since all internal routes are maintained by interior gateway protocols such as RIP and OSPF, careful filtering should be used to ensure that only routes that need to be advertised reach the Internet.

- A route metric must be used to resolve the problem of redistributing external routes with incompatible metrics.

EXAMPLE

```
Console(config-router)#redistribute static metric 10
Console(config-router)#
```

timers bgp

This command sets the Keep Alive time used for maintaining connectivity, and the Hold time to wait for Keep Alive or Update messages before declaring a neighbor down. Use the **no** form to restore the default settings.

SYNTAX

timers bgp *keepalive-time hold-time*

no timers bgp

keepalive-time – The frequency at which the local router sends keep-alive messages to its neighbors. (Range: 0-65535 seconds)

hold-time – The maximum interval after which a neighbor is declared dead if a keep-alive or update message has not been received. (Range: 0-65535 seconds)

COMMAND MODE

Router Configuration

DEFAULT SETTING

Keep Alive time: 60 seconds
Hold time: 180 seconds

COMMAND USAGE

- Use this command to set global BGP timers used for monitoring connectivity to neighboring routers. These timers will be applied to all neighbors unless the neighbor timers command has been used to explicitly configure other timer settings for a neighbor.

- When the minimum acceptable hold-time is configured with this command, a remote peer session can be established only if the neighboring router is advertising a hold-time equal to, or greater than, that configured on this device.

EXAMPLE

```
Console(config-router)#timers bgp 60 200
Console(config-router)#
```

clear ip bgp

This command clears connections using hard or soft re-configuration.

SYNTAX

clear ip bgp {* | *as-number* | **external** | **peer-group** *group-name* | *neighbor-address*} [**in** [**prefix-list**] | **out** | **soft** [**in** | **out**]]

* – All BGP peering sessions.

as-number – All peering sessions within this autonomous system number. (Range: 1-4294967295)

external – All eBGP peering sessions.

peer-group *group-name* – A BGP peer group containing a list of neighboring routers configured with the neighbor peer-group command.

neighbor-address – IPv4 address of a neighbor.

in – Inbound sessions.

prefix-list – The outbound route filter (ORF) prefix list. This option triggers a new route refresh or soft re-configuration, which updates the ORF prefix list. This option is ignored unless ORF capabilities have been enabled using the neighbor capability orf prefix-list command or ORF capability information has been received from a sending peer. If ignored, a normal inbound soft reset is performed.

out – Outbound sessions.

soft – Uses soft re-configuration for the reset, which does not tear down the session.

COMMAND MODE

Privileged Exec

DEFAULT SETTING

None

COMMAND USAGE

- Use this command to initiate a hard reset or soft re-configuration. A hard reset clears and rebuilds specified peering sessions and routing tables. Soft re-configuration uses stored information to reconfigure and activate routing tables without clearing existing sessions. It uses stored update information to allow you to apply a new BGP policy without disrupting the network.

- To generate new inbound updates from stored information without resetting peer sessions, you must preconfigure the local router using the neighbor capability orf prefix-list command, which causes the router to store all received updates. Note that storing updates is memory intensive and should only be applied to critical links.

  Outbound soft configuration requires no memory or preconfiguration. Outbound re-configuration can be used on the other side of a peering session to make initiate a new inbound policy on the local side.

- Use this command to clear peering sessions when changes are made to any BGP access lists, weights, or route-maps.

- Route refresh (RFC 2918) allows a router to reset inbound routing tables dynamically by exchanging route refresh requests with peers. Route refresh relies on the dynamic exchange of information with supporting peers. It is advertised through BGP capability negotiation, and all BGP routers must support this capability.

EXAMPLE

This example assumes that soft re-configuration has been set on the neighboring router.

```
Console(config-router)#clear ip bgp 192.168.0.254 soft in
Console(config-router)#
```

clear ip bgp dampening

This command clears route dampening information and unsuppresses any currently suppressed routes.

SYNTAX

clear ip bgp dampening [*ip-address* [*netmask*]]

ip-address – IP address of network or peer router.

netmask – Network mask that identifies the network address bits.

COMMAND MODE

Privileged Exec

DEFAULT SETTING

None

EXAMPLE

If no keywords are entered as in this example, route dampening information is cleared for the entire routing table.

```
Console(config-router)#clear ip bgp dampening
Console(config-router)#
```

Route Metrics and Selection

bgp always-compare-med

This command allows comparison of the Multi Exit Discriminator (MED) for paths advertised from neighbors in different autonomous systems. Use the **no** form to disable this feature.

SYNTAX

[**no**] **bgp always-compare-med**

COMMAND MODE

Router Configuration

DEFAULT SETTING

Disabled

COMMAND USAGE

- The MED is an optional non-transitive[30] attribute used to discriminate among multiple exit points to a neighboring autonomous system. A path with a lower MED is preferred over a path with a higher MED.
- By default, during best-path selection, the MED is compared only among paths from the same autonomous system. This command allows the comparison of MEDs among different paths regardless of the autonomous system from which the paths are received.
- The bgp deterministic-med command can be used to enforce comparison of the MED value between all paths received from within the same autonomous system.

EXAMPLE

This example assumes that a peer router is advertising the same route prefix through the two ASes (100 and 300) to the same AS (200), each of which carries a different MED.

```
Console(config-router)#bgp always-compare-med
Console(config-router)#
```

bgp bestpath as-path ignore

This command ignores the AS path length in the selection of a path. Use the **no** form to disable this feature.

SYNTAX

[**no**] **bgp bestpath as-path ignore**

COMMAND MODE

Router Configuration

[30] If a router does not understand an optional non-transitive attribute, it will be removed.

DEFAULT SETTING

Disabled

EXAMPLE

```
Console(config-router)#bgp bestpath as-path ignore
Console(config-router)#
```

bgp bestpath compare-confed-aspath

This command compare confederation AS path length in addition to external AS path length in the selection of a path. Use the no form to disable this feature.

SYNTAX

[**no**] **bgp bestpath compare-confed-aspath**

COMMAND MODE

Router Configuration

DEFAULT SETTING

Disabled

EXAMPLE

```
Console(config-router)#bgp bestpath compare-confed-aspath
Console(config-router)#
```

bgp bestpath compare-routerid

This command compares similar routes from external peers, and gives preference to a route with the lowest router identifier. Use the **no** form to restore the default setting.

SYNTAX

[**no**] **bgp bestpath compare-routerid**

COMMAND MODE

Router Configuration

DEFAULT SETTING

When making the best-path selection, the router does not compare identical routes received from different external peers.

COMMAND USAGE

Normally, the first route arriving from different external peers (with other conditions equal) will be chosen as the best route. By using this command, the route with lowest router ID will be selected.

EXAMPLE

```
Console(config-router)#bgp bestpath compare-routerid
Console(config-router)#
```

bgp bestpath med

This command enables comparison of the Multi Exit Discriminator (MED) attribute for paths learned from confederation peers, and the treatment of a route when the MED is missing. Use the **no** form to disable this feature.

SYNTAX

[**no**] **bgp bestpath med** {[**confed**] [**missing-as-worst**]}

confed – Compare MED in confederation path.

missing-as-worst – Consider as maximum MED value when missing.

COMMAND MODE

Router Configuration

DEFAULT SETTING

When making the best-path selection, the router does not consider the MED.

COMMAND USAGE

- The MED for paths learned from confederation peers is compared only if no external autonomous systems (AS) appear in the path. If an external AS is within the path, then the external MED is passed transparently through the confederation, and it is not compared.

- If the missing-as-worst option is disabled, the missing MED is assigned a value of 0, making a path missing the MED attribute the best path.

EXAMPLE

```
Console(config-router)#bgp bestpath med config missing-as-worst
Console(config-router)#
```

bgp default local-preference

This command sets the default local preference used for best path selection among local iBGP peers. Use the **no** form to restore the default setting.

SYNTAX

bgp default local-preference *preference*

preference – Degree of preference iBGP peers give local routes during BGP best path selection. The higher the value, the more the route is to be preferred. (Range: 0-4294967295)

COMMAND MODE

Router Configuration

Default Setting

100

Command Usage

Local preference is a discretionary attribute applied to a route during the BGP best path selection process. It is exchanged only between iBGP peers, and used to determine local policy.

Example

```
Console(config-router)#bgp default local-preference 100
Console(config-router)#
```

bgp deterministic-med

This command enforces deterministic comparison of the MED attribute between all paths received from the same AS, ensuring that selection of the best path will always be the same, regardless of the order in which the paths are received by the local router. Use the **no** form to disable this feature.

Syntax

[**no**] **bgp deterministic-med**

Command Mode

Router Configuration

Default Setting

Disabled

Command Usage

- The MED is compared after BGP attributes weight, local preference, AS-path and origin have been compared and are equal. When deterministic comparison of the MED is enabled, all paths for the same route prefix (received from peers within the same AS) are grouped together and arranged according to their MED value. Based on this comparison, the best path is then chosen.

- The router immediately groups and sorts all local paths when this command is entered. For correct results, deterministic comparison of the MED must be configured in the same manner (enabled or disabled) on all routers in the local AS.

- If deterministic comparison of the MED is not enabled, route selection can be affected by the order in which routes are received.

- This command compares the MED when choosing routes advertised by different peers in the same AS. To compare the MED when choosing routes from neighbors in different ASs, use the bgp always-compare-med command.

EXAMPLE

```
Console(config-router)#bgp deterministic-med
Console(config-router)#
```

distance

This command sets the administrative distance for a specified external BGP (eBGP) routes. Use the **no** form to restore the default setting.

SYNTAX

distance *distance ip-address netmask* [*access-list-name*]

no distance *ip-address netmask*

distance – Administrative distance for an eBGP route. (Range: 1-255)

ip-address – IP address of a route entry.

netmask – Network mask for the route. This mask identifies the network address bits used for the associated routing entries.

access-list-name – Name of standard or extended access list. (Maximum length: 16 characters, no spaces or other special characters)

COMMAND MODE

Router Configuration

DEFAULT SETTING

None

COMMAND USAGE

- The route distance indicates the trustworthiness of a router. The higher the distance the lower the trust rating. A distance of 255 means that the routing source cannot be trusted and should be ignored.
- This distance set by this command only applies to external BGP paths routes learned from a neighbor outside of the AS. Use the distance bgp command to configure the global setting for the distance of eBGP, iBGP, and local routes.
- If an access-list is specified, it will be applied to received routes. If the received routes are not matched in the access-list or the specified list does not exist, the original distance value will be used.

EXAMPLE

```
Console(config-router)#distance 90 10.1.1.64 255.255.255.255
Console(config-router)#
```

RELATED COMMANDS

distance bgp (1858)

distance bgp

This command sets the administrative distance for external BGP, internal BGP, and local routes. Use the **no** form to restore the default settings.

SYNTAX

distance bgp *ebgp-distance ibgp-distance local-distance*

no distance bgp

ebgp-distance – Administrative distance for eBGP routes. (Range: 1-255)

ibgp-distance – Administrative distance for iBGP routes. (Range: 1-255)

local-distance – Administrative distance for local routes. (Range: 1-255)

COMMAND MODE

Router Configuration

DEFAULT SETTING

eBGP: 20
iBGP: 200
local: 200

COMMAND USAGE

- External routes are learned from an external autonomous system, and internal routes from a peer within the local autonomous system. Local routes are those configured with the network command as a back door for the router or for the networks being redistributed from another routing process.
- The route distance indicates the trustworthiness of a router. The higher the distance the lower the trust rating. A distance of 255 means that the routing source cannot be trusted and should be ignored.
- This command can be used to indicate that another protocol can provide a better route to a node than that learned via eBGP, or to indicate that some internal routes should be preferred by BGP.
- Changing the administrative distance of iBGP routes is not recommended. It may cause an accumulation of routing table inconsistencies which can break routing to many parts of the network.

EXAMPLE

```
Console(config-router)#distance bgp 20 200 20
Console(config-router)#
```

RELATED COMMANDS

distance (1857)

Neighbor Configuration

neighbor activate

This command enables the exchange of routing information with a neighboring router or peer group. Use the **no** form to disable the exchange of routing information.

SYNTAX

[**no**] **neighbor** {*ip-address* | *group-name*} **activate**

ip-address – IP address of a neighbor.

group-name – A BGP peer group containing a list of neighboring routers configured with the neighbor peer-group command.

COMMAND MODE

Router Configuration

DEFAULT SETTING

Enabled

COMMAND USAGE

- After a connection is opened with a neighboring router, this command is used to enable the exchange of information with the neighbor.
- The exchange of information is enabled by default for each routing session configured with the neighbor remote-as command.

EXAMPLE

```
Console(config-router)#neighbor 10.1.1.64 activate
Console(config-router)#
```

neighbor advertisement-interval

This command configures the interval between sending update messages to a neighbor. Use the **no** form to restore the default setting.

SYNTAX

neighbor *ip-address* **advertisement-interval** *interval*

no neighbor *ip-address* **advertisement-interval**

ip-address – IP address of a neighbor.

interval – The minimum interval between sending routing updates to the specified neighbor. (Range: 0-600 seconds)

COMMAND MODE

Router Configuration

DEFAULT SETTING

iBGP: 5 seconds
eBGP: 30 seconds

COMMAND USAGE

This command can be used to reduce route flapping. However, the bgp dampening command can provide more precise control of route flapping.

EXAMPLE

```
Console(config-router)#neighbor 10.1.1.64 advertisement-interval 20
Console(config-router)#
```

neighbor allowas-in

This command configures the number of times the AS path for a received route can contain the same AS number. Use the **no** form to restore the default setting.

SYNTAX

neighbor {*ip-address* | *group-name*} **allowas-in** [*count*]

no neighbor {*ip-address* | *group-name*} **allowas-in**

ip-address – IP address of a neighbor.

group-name – A BGP peer group containing a list of neighboring routers configured with the neighbor peer-group command.

count – Maximum number of times the same AS number can appear in the AS path of a received route. (Range: 1-10, or 3 if the count is not undefined)

COMMAND MODE

Router Configuration

DEFAULT SETTING

No repeats allowed

COMMAND USAGE

Under standard routing practices, BGP will not accept a route sent from a neighbor if the same AS number appears in the AS path more than once. This could indicate a routing loop, and the route message would therefore be dropped. However, for purposes of traffic engineering (such as degrading the preference for a certain path), this command can be used to configure the number of times the same AS is allowed re-appear in the AS path of a route received from a neighbor.

EXAMPLE

```
Console(config-router)#neighbor 10.1.1.64 allowas-in 5
Console(config-router)#
```

neighbor attribute-unchanged

This command configures certain route attributes to be kept unchanged for transparent transmission to the specified neighbor. Use the **no** form to disable this feature.

SYNTAX

[**no**] **neighbor** {*ip-address* | *group-name*} **attribute-unchanged** [**as-path**] [**med**] [**next-hop**]

ip-address – IP address of a neighbor.

group-name – A BGP peer group containing a list of neighboring routers configured with the neighbor peer-group command.

as-path – AS path attribute

med – Mult-Exit Discriminator (MED) attribute

next-hop – Next hop attribute

COMMAND MODE

Router Configuration

DEFAULT SETTING

Disabled

COMMAND USAGE

If this command is entered without specifying any route attributes, then all three optional attributes are used.

EXAMPLE

```
Console(config-router)#neighbor 10.1.1.64 attribute-unchanged
Console(config-router)#
```

neighbor capability dynamic

This command configures dynamic negotiation of capabilities between neighboring routers. Use the **no** form to disable this feature.

SYNTAX

[**no**] **neighbor** {*ip-address* | *group-name*} **capability dynamic**

ip-address – IP address of a neighbor.

group-name – A BGP peer group containing a list of neighboring routers configured with the neighbor peer-group command.

COMMAND MODE

Router Configuration

DEFAULT SETTING

Disabled

COMMAND USAGE

- BGP normally requires a router to terminate a peering session if it receives an OPEN message with an unrecognized optional parameter. This command allows new capabilities to be introduced gracefully, without requiring a peering session to be terminated if a negotiated capability is unknown.
- With dynamic negotiation of capabilities is enabled, the capabilities by both sides are negotiated in OPEN messages, with the partner responding if a capability is supported or sending a NOTIFICATION if not.

EXAMPLE

```
Console(config-router)#neighbor 10.1.1.64 capability dynamic
Console(config-router)#
```

neighbor capability orf prefix-list

This command configures the negotiation of outbound route filter (ORF) capabilities with a neighboring router. Use the **no** form to disable negotiation.

SYNTAX

[**no**] **neighbor** {*ip-address* | *group-name*} **orf prefix-list** {**both** | **receive** | **send**}

ip-address – IP address of a neighbor.

group-name – A BGP peer group containing a list of neighboring routers configured with the neighbor peer-group command.

both – Capability to send and receive the ORF to/from this neighbor.

receive – Capability to receive the ORF from this neighbor.

send – Capability to send the ORF to this neighbor.

COMMAND MODE

Router Configuration

DEFAULT SETTING

Disabled

COMMAND USAGE

When this command is entered, the side configured with inbound prefix-list filter rules will transmit its own rules to the peer, and the peer will then use these rules as its own outbound rules, thereby avoiding sending routes which will be denied by its partner.

EXAMPLE

```
Console(config-router)#neighbor 10.1.1.64 orf prefix-list both
Console(config-router)#
```

neighbor default-originate

This command allows the local router to send a default route to a neighbor. Use the **no** form to disable this feature.

SYNTAX

neighbor {*ip-address* | *group-name*} **default-originate** [**route-map** *map-name*]

no neighbor {*ip-address* | *group-name*} **default-originate**

ip-address – IP address of a neighbor.

group-name – A BGP peer group containing a list of neighboring routers configured with the neighbor peer-group command.

map-name – Name of the route map. The route map can be used to filter the criteria used for sending the default route to a neighbor. (Range: 1-80 characters)

COMMAND MODE

Router Configuration

DEFAULT SETTING

Disabled

COMMAND USAGE

- This command is used to advertise the local router's default route (0.0.0.0) to a neighbor. This route can be used by the neighbor to reach the local router if no other routes are available.
- If several neighbors supply a default route to the same partner, the best one will be elected according to the standard path selection process.
- If a route map is specified, the default route 0.0.0.0 is advertised if the route map contains a match ip address clause and there is a route that matches an entry in the ip prefix-list.

EXAMPLE

```
Console(config-router)#neighbor 10.1.1.64 default-originate
Console(config-router)#
```

neighbor description

This command configures the description of a neighbor or peer group. Use the **no** form to remove a description.

SYNTAX

neighbor {*ip-address* | *group-name*} **description** *description*

no neighbor {*ip-address* | *group-name*} **description**

ip-address – IP address of a neighbor.

group-name – A BGP peer group containing a list of neighboring routers configured with the neighbor peer-group command.

description – Descriptive string. (Range: 1-80 characters)

COMMAND MODE

Router Configuration

DEFAULT SETTING

No description specified

EXAMPLE

```
Console(config-router)#neighbor 10.1.1.64 description bill’s router
Console(config-router)#
```

neighbor distribute-list

This command filters route updates to/from a neighbor or peer group. Use the **no** form to remove this list.

SYNTAX

neighbor {*ip-address* | *group-name*} **distribute-list** *access-list-name* {**in** | **out**}

no neighbor {*ip-address* | *group-name*} **distribute-list** {**in** | **out**}

ip-address – IP address of a neighbor.

group-name – A BGP peer group containing a list of neighboring routers configured with the neighbor peer-group command.

access-list-name – Name of standard or extended access list. (Maximum length: 32 characters, no spaces or other special characters)

in – Filters inbound routing messages.

out – Filters outbound routing messages.

COMMAND MODE

Router Configuration

DEFAULT SETTING

None

COMMAND USAGE

- If the specified access list for input or output mode does not exist, all input or output route updates will be filtered.
- The neighbor prefix-list and the neighbor distribute-list commands are mutually exclusive for a BGP peer. That is, only one of these commands may be applied in the inbound or outbound direction.

EXAMPLE

```
Console(config-router)#neighbor 10.1.1.64 distribute-list RD in
Console(config-router)#
```

neighbor dont-capability-negotiate

This command disables capability negotiation when creating connections. Use the **no** form to restore the default setting.

SYNTAX

[**no**] **neighbor** {*ip-address* | *group-name*} **dont-capability-negotiate**

ip-address – IP address of a neighbor.

group-name – A BGP peer group containing a list of neighboring routers configured with the neighbor peer-group command.

COMMAND MODE

Router Configuration

DEFAULT SETTING

Capability negotiation is enabled

COMMAND USAGE

Earlier versions of BGPv4 require that when a BGP speaker receives an Open message with one or more unrecognized Optional Parameters, the speaker must terminate BGP peering. This command can be used when connecting to a partner known to use an older BGP version which does not support capabilities negotiation (RFC 2842), thereby allowing the peering session to continue.

EXAMPLE

```
Console(config-router)#neighbor 10.1.1.64 dont-capability-negotiate
Console(config-router)#
```

neighbor ebgp-multihop

This command allows eBGP neighbors to exist in different segments, and configures the maximum hop count (TTL). Use the **no** form to restore the default setting.

Syntax

neighbor {*ip-address* | *group-name*} **ebgp-multihop** [*count*]

no neighbor {*ip-address* | *group-name*} **ebgp-multihop**

ip-address – IP address of a neighbor.

group-name – A BGP peer group containing a list of neighboring routers configured with the neighbor peer-group command.

count – Maximum hop count. (Range: 1-255)

Command Mode

Router Configuration

Default Setting

eBGP neighbors must be located in the same segment.

Command Usage

- This command can be used to allow routers in different network segments to create a BGP neighbor relationship.
- If this command is entered without specifying a count, the hop limit is set at 255.
- To avoid creating loops through oscillating routes, a multi-hop session will not be established if the only route to a multi-hop peer is the default route.

Example

```
Console(config-router)#neighbor 10.1.1.64 ebgp-multihop 2
Console(config-router)#
```

neighbor enforce-multihop

This command enforces the requirement for all neighbors to form multi-hop connections. Use the **no** form to disable this requirement.

Syntax

[**no**] **neighbor** {*ip-address* | *group-name*} **enforce-multihop**

ip-address – IP address of a neighbor.

group-name – A BGP peer group containing a list of neighboring routers configured with the neighbor peer-group command.

Command Mode

Router Configuration

DEFAULT SETTING

Not enforced

COMMAND USAGE

By default, the multi-hop check is only performed on iBGP and eBGP non-direct routes. This command can be used to force the router to perform the multi-hop check on directly connected routes as well. In other words, the router will not perform the next-hop direct-connect check the specified neighbor.

EXAMPLE

```
Console(config-router)#neighbor 10.1.1.64 enforce-multihop
Console(config-router)#
```

neighbor filter-list

This command filters route updates sent to or received from a neighbor based on an AS path access-list. Use the **no** form to disable route filtering.

SYNTAX

neighbor {*ip-address* | *group-name*} **filter-list** *access-list* {**in** | **out**}

no neighbor {*ip-address* | *group-name*} **filter-list** {**in** | **out**}

ip-address – IP address of a neighbor.

group-name – A BGP peer group containing a list of neighboring routers configured with the neighbor peer-group command.

access-list – Name of an AS-Path access list configured with the ip as-path access-list command.

in – Filter inbound routing updates.

out – Filter outbound routing updates.

COMMAND MODE

Router Configuration

DEFAULT SETTING

Disabled

COMMAND USAGE

Use this command in conjunction with the ip as-path access-list command to filter route updates sent to or received from a neighbor.

EXAMPLE

In this example, the AS path access list "ASPF" is first configured to deny access to any route passing through AS 100. It then enables route filtering by assigning this list to a peer.

```
Console(config)#ip as-path access-list ASPF deny 100
Console(config)#router bgp 100
Console(config-router)#redistribute static
Console(config-router)#neighbor 10.1.1.66 filter-list ASPF out
Console(config-router)#
```

neighbor interface

This command specifies the interface to a neighbor. Use the **no** form to remove this configuration setting.

Syntax

neighbor *ip-address* **interface vlan** *vlan-id*

no neighbor *ip-address* **interface**

ip-address – IP address of a neighbor.

vlan-id - VLAN ID. (Range: 1-4094)

Command Mode

Router Configuration

Default Setting

None

Example

```
Console(config-router)#neighbor 10.1.1.64 interface vlan 1
Console(config-router)#
```

neighbor maximum-prefix

This command sets the maximum number or route prefixes that can be received from a neighbor. Use the **no** form to restore the default setting.

Syntax

neighbor {*ip-address* | *group-name*} **maximum-prefix** *max-count* [*threshold* [**restart** *interval* | **warning**]]

no neighbor {*ip-address* | *group-name*} **maximum-prefix**

ip-address – IP address of a neighbor.

group-name – A BGP peer group containing a list of neighboring routers configured with the neighbor peer-group command.

max-count – The maximum number of route prefixes that will be accepted from a neighbor. (Range: 1-4294967295)

threshold – The percentage of the maximum number of allowed prefixes at which the router will initiate the specified response.

restart – Restarts BGP connection after the threshold is exceeded.

interval – Time to wait after a BGP connection has been terminated, before reestablishing the session. (Range: 1-65535 minutes)

warning – Sends a log message if the threshold is exceeded.

COMMAND MODE

Router Configuration

DEFAULT SETTING

No limit is set

DEFAULT USAGE

- This command is used to control the maximum number of route prefixes that can be sent by a neighbor. It provides a method to reserve resources for other processes, or to prevent malicious attacks.

- If the threshold is specified, but neither the **restart** nor **warning** keywords are used), the connection will be closed until the records are cleared with the clear ip bgp command.

EXAMPLE

In this example, the router warns when the number of route prefixes reaches 6, and the connection will be closed when the prefixes hit 13.

```
Console(config-router)#neighbor 10.1.1.64 maximum-prefix 12 50
Console(config-router)#
```

neighbor next-hop-self

This command configures the local router as the next hop for a neighbor in all routing messages it sends. Use the **no** form to disable this feature.

SYNTAX

[**no**] **neighbor** {*ip-address* | *group-name*} **next-hop-self**

ip-address – IP address of a neighbor.

group-name – A BGP peer group containing a list of neighboring routers configured with the neighbor peer-group command.

COMMAND MODE

Router Configuration

DEFAULT SETTING

Disabled

DEFAULT USAGE

- iBGP routers only connected to other iBGP routers in same segment will not be able to talk with iBGP routers outside of the segment if they are not directly connected with each other. This command can be used in these kinds of networks (i.e., un-meshed or non-broadcast) where iBGP neighbors may not have direct access to all other neighbors on the same IP subnet.

- Even when a successful BGP relationship seems to have been established within the local AS, you may not able to see some routes in the routing table. iBGP routers only connected with other iBGP routers in same AS will not be able to talk with routers outside of the AS if they are not directly connected with each other. The **neighbor next-hop-self** command can be used to configure an iBGP router which is directly connected with an eBGP neighbor so that other iBGP routers in the same AS can talk with eBGP routers outside the AS.

EXAMPLE

```
Console(config-router)#neighbor 10.1.1.64 next-hop-self
Console(config-router)#
```

neighbor override-capability

This command overrides the result of capability negotiations, allowing a session to be formed with a peer that does not support capability negotiation. Use the **no** form to disable this feature.

SYNTAX

[**no**] **neighbor** {*ip-address* | *group-name*}
neighbor override-capability

ip-address – IP address of a neighbor.

group-name – A BGP peer group containing a list of neighboring routers configured with the neighbor peer-group command.

COMMAND MODE

Router Configuration

DEFAULT SETTING

Disabled

EXAMPLE

```
Console(config-router)#neighbor 10.1.1.64 override-capability
Console(config-router)#
```

neighbor passive

This command passively forms a connection with the specified neighbor, not sending a TCP connection request, but waiting a connection request from the specified neighbor. Use the **no** form to disable this feature.

SYNTAX

[**no**] **neighbor** {*ip-address* | *group-name*} **passive**

ip-address – IP address of a neighbor.

group-name – A BGP peer group containing a list of neighboring routers configured with the neighbor peer-group command.

COMMAND MODE

Router Configuration

DEFAULT SETTING

Disabled

COMMAND USAGE

This command configures the local router so that it remains in Active state, waiting for an inbound connection request from a neighbor, and not initiating any outbound connections with the neighbor via an Open message.

EXAMPLE

```
Console(config-router)#neighbor 10.1.1.64 passive
Console(config-router)#
```

neighbor peer-group (Creating)

This command configures a router peer group which can be easily configured with the same attributes. Use the **no** form to remove a peer group.

SYNTAX

[**no**] **neighbor** *group-name* **peer-group**

group-name – A BGP peer group. (Range: 1-256 characters)

COMMAND MODE

Router Configuration

DEFAULT SETTING

No peer groups are defined.

COMMAND USAGE

- Neighbors with the same BGP attributes can grouped into peer groups. This simplifies the application of various policies, such as filter lists. Other configuration settings can be applied to a peer-group using any of the neighbor commands. Any changes made to the peer group affect all members.Use this command to create a peer-group.

- To assign members to a peer group, use the neighbor *ip-address* peer-group *group-name* command.

EXAMPLE

```
Console(config-router)#neighbor RD peer-group
Console(config-router)#
```

neighbor peer-group (Group Members)

This command assigns routers to a peer group. Use the **no** form to remove a group member.

SYNTAX

[**no**] **neighbor** *ip-address* **peer-group** *group-name*

ip-address – IP address of a neighbor.

group-name – A BGP peer group.

COMMAND MODE

Router Configuration

DEFAULT SETTING

No group members are defined.

COMMAND USAGE

To create a peer group, use the neighbor *group-name* peer-group command.

EXAMPLE

```
Console(config-router)#neighbor 10.1.1.64 peer-group RD
Console(config-router)#
```

neighbor port

This command specifies the TCP port number of the partner through which communications are carried. Use the **no** form to restore the default setting.

SYNTAX

neighbor *ip-address* **port** *port-number*

no neighbor *ip-address* **port**

ip-address – IP address of a neighbor.

port-number – TCP port number to use for BGP communications. (Range: 0-65535)

COMMAND MODE

Router Configuration

DEFAULT SETTING

179

EXAMPLE

```
Console(config-router)#neighbor 10.1.1.64 port 1023
Console(config-router)#
```

neighbor prefix-list

This command configures prefix restrictions applied in inbound/outbound route updates to/from specified neighbors. Use the **no** form to remove the neighbor binding for a prefix list.

SYNTAX

neighbor {*ip-address* | *group-name*} **prefix-list** *list-name* {**in** | **out**}

no neighbor {*ip-address* | *group-name*} **prefix-list** {**in** | **out**}

ip-address – IP address of a neighbor.

group-name – A BGP peer group containing a list of neighboring routers configured with the neighbor peer-group command.

list-name – Name of a prefix-list. The prefix list can be used to filter the networks to import or export. (Range: 1-80 characters)

in – Filter inbound routing updates.

out – Filter outbound routing updates.

COMMAND MODE

Router Configuration

DEFAULT SETTING

No prefix list restrictions are configured.

COMMAND USAGE

- First, configure a prefix list with the ip prefix-list command, and then use this command to specify the neighbors to which it applies, and whether it applies to inbound or outbound messages.

- Filtering routes based on a prefix list searches for entries matching the router specified by this command. If a match is found and the entry is configured to permit the route, the route will be imported or exported as defined by this command. An empty prefix list permits all prefixes. If a prefix does not match any entries in a list, the route is denied. When multiple entries in the list match a prefix, the entry with the smallest sequence number is used.

- The search starts at the top of the prefix list. Once an entry matches, the router stops searching. To reduce the load on system resources, the most commonly used entries should be placed at the top of the list.

EXAMPLE

```
Console(config)#ip prefix-list RD permit 100.1.0.0 255.255.0.0 ge 17 le 18
Console(config)#router bgp 200
Console(config-router)#redistribute static
Console(config-router)#neighbor 10.1.1.66 prefix-list RD out
Console(config-router)#
```

neighbor remote-as

This command configures a neighbor and its AS number, identifying the neighbor as an iBGP or eBGP peer. Use the **no** form to remove a neighbor.

SYNTAX

neighbor {*ip-address* | *group-name*} **remote-as** *as-number*

no neighbor {*ip-address* | *group-name*} **remote-as**

ip-address – IP address of a neighbor.

group-name – A BGP peer group containing a list of neighboring routers configured with the neighbor peer-group command.

as-number – Autonomous system number which identifies this router as a member of the specified domain, and tags routing messages passed to other BGP routers with this number. (Range: 1-4294967295)

COMMAND MODE

Router Configuration

DEFAULT SETTING

No neighbors are configured.

COMMAND USAGE

- BGP neighbors must be manually configured. A neighbor relationship can only be established if partners are configured on both sides a connection.
- If the neighbor's AS number is the same as that of the local router, the neighbor is an iBGP peer. If it is different, the neighbor is an eBGP peer.

EXAMPLE

```
Console(config-router)#neighbor 10.1.1.64 remote-as 100
Console(config-router)#
```

neighbor remove-private-as

This command removes private autonomous system numbers from outbound routing updates to an external neighbor. Use the **no** form to disable this feature.

SYNTAX

neighbor {*ip-address* | *group-name*} **remove-private-as**

ip-address – IP address of a neighbor.

group-name – A BGP peer group containing a list of neighboring routers configured with the neighbor peer-group command.

COMMAND MODE

Router Configuration

DEFAULT SETTING

Disabled

COMMAND USAGE

- This command only applies to eBGP neighbors. It is used to avoid passing an internal AS number to an external AS. Internal AS numbers range from 64512-65535, and should not be sent to the Internet since they are not valid external AS numbers.
- This configuration only takes effect when the AS Path attribute of a route contains only internal AS numbers. If the AS Path attribute for a route contains both internal and external AS numbers, the route will not be processed.
- This command may be used in BGP confederations provided that the private AS numbers appear after the confederation portion of the AS path.

EXAMPLE

```
Console(config-router)#neighbor 10.1.1.64 remove-private-as
Console(config-router)#
```

neighbor route-map

This command specifies the route mapping policy for inbound/outbound routing updates for specified neighbors. Use the **no** form to remove this policy binding.

SYNTAX

neighbor {*ip-address* | *group-name*} **route-map** *map-name* {**in** | **out**}

no neighbor {*ip-address* | *group-name*} **route-map** {**in** | **out**}

ip-address – IP address of a neighbor.

group-name – A BGP peer group containing a list of neighboring routers configured with the neighbor peer-group command.

map-name – Name of the route map. The route map can be used to filter the networks to advertise or receive based on various attributes. (Range: 1-128 characters)

in – Filter inbound routing updates.

out – Filter outbound routing updates.

COMMAND MODE

Router Configuration

DEFAULT SETTING

No route maps are configured nor bound to any neighbor.

COMMAND USAGE

- First, use route-map command to create a route map, and the **match** and **set** commands to configure the route attributes to act upon. Then use this command to specify neighbors to which the route map is applied.

- If the specified route map does not exist, all input/output route updates will be filtered.

EXAMPLE

```
Console(config-router)#neighbor 10.1.1.64 route-map RD in
Console(config-router)#
```

neighbor route-reflector-client

This command configures this router as a route reflector and the specified neighbor as its client. Use the **no** form to disable route reflection for the specified neighbor.

SYNTAX

[**no**] **neighbor** {*ip-address* | *group-name*} **route-reflector-client**

ip-address – IP address of a neighbor.

group-name – A BGP peer group containing a list of neighboring routers configured with the neighbor peer-group command.

COMMAND MODE

Router Configuration

DEFAULT SETTING

Disabled

COMMAND USAGE

- Route reflection from this device is enabled by default, but is only functional if a client has been configured with this command.

- Under standard configuration rules, all BGP speakers within the same AS must be fully meshed. Route reflection can used to reduce the number of connections required between peers. Reflector clients exchange messages only with the route reflector, while the reflector handles message exchanges among each client and other iBGP, eBGP, and non-client routers. For more information on configuring route reflection, refer to the Command Usage section under the bgp client-to-client reflection command.

EXAMPLE

```
Console(config-router)#neighbor 10.1.1.64 route-reflector-client
Console(config-router)#
```

neighbor route-server-client

This command configures this router as a route server and the specified neighbor as its client. Use the **no** form to disable the route server for the specified neighbor.

SYNTAX

[**no**] **neighbor** {*ip-address* | *group-name*} **route-server-client**

ip-address – IP address of a neighbor.

group-name – A BGP peer group containing a list of neighboring routers configured with the neighbor peer-group command.

COMMAND MODE

Router Configuration

DEFAULT SETTING

None

COMMAND USAGE

- A route server is used as a replacement for full mesh eBGP routing in internet exchange points in a manner similar to the way route reflectors are used in iBGP. Instead of maintaining direct eBGP peering sessions with every other service provider, providers can acquire the same routing information through a single connection to a route server at the Internet exchange.

- Using a route server reduces the configuration complexity required for an eBGP full mesh, limits CPU and memory requirements for the exchange of peering messages, and avoids the need for negotiating a large number of individual peering agreements.

EXAMPLE

In the following example, the router 10.1.1.64 (AS100) is configured as the route server for neighbors 10.1.1.66 (AS200) and 10.1.1.68 (AS300).

```
Console(config)#router bgp 100
Console(config-router)#neighbor 10.1.1.66 remote-as 200
Console(config-router)#neighbor 10.1.1.66 route-server-client
Console(config-router)#neighbor 10.1.1.68 remote-as 300
Console(config-router)#neighbor 10.1.1.68 route-server-client
Console(config-router)#
```

neighbor send-community

This command configures the router to send community attributes to a neighbor in peering messages. Use the **no** form to stop sending this attribute to a neighbor.

SYNTAX

[**no**] **neighbor** {*ip-address* | *group-name*} **send-community** [**both** | **extended** | **standard**]

ip-address – IP address of a neighbor.

group-name – A BGP peer group containing a list of neighboring routers configured with the neighbor peer-group command.

both – Sends both extended and standard community attributes.

extended – Sends extended community attributes.

standard – Standard community attributes.

COMMAND MODE

Router Configuration

DEFAULT SETTING

No community attributes are sent. If community type is not specified, then only standard community attributes are sent.

COMMAND USAGE

Community attributes are used to group destinations into a certain community, and apply routing decisions to the overall community.

EXAMPLE

```
Console(config-router)#neighbor 10.1.1.66 send-community extended
Console(config-router)#
```

RELATED COMMANDS

set community (1911)

neighbor shutdown

This command closes a neighbor connection without canceling the neighbor configuration. Use the **no** form to restore the connection.

SYNTAX

[**no**] **neighbor** {*ip-address* | *group-name*} **shutdown**

ip-address – IP address of a neighbor.

group-name – A BGP peer group containing a list of neighboring routers configured with the neighbor peer-group command.

COMMAND MODE

Router Configuration

DEFAULT SETTING

None

COMMAND USAGE

- This command terminates any active sessions for the specified neighbor, and removes any associated routing information.

- Use the show ip bgp summary command display the neighbors which have been administratively shut down. Entries with in an Idle (Admin) state have been disabled by the **neighbor shutdown** command.

EXAMPLE

```
Console(config-router)#neighbor 10.1.1.66 shutdown
Console(config-router)#
```

neighbor soft-reconfiguration inbound

This command configures the switch to store updates in the inbound message buffer, and perform soft re-configuration from this buffer for specified neighbors when required. Use the **no** form to disable this feature.

SYNTAX

[**no**] **neighbor** {*ip-address* | *group-name*} **soft-reconfiguration inbound**

ip-address – IP address of a neighbor.

group-name – A BGP peer group containing a list of neighboring routers configured with the neighbor peer-group command.

COMMAND MODE

Router Configuration

DEFAULT SETTING

Disabled

COMMAND USAGE

- Use this command to employ soft reconfiguration for a neighbor. A hard reset clears and rebuilds specified peering sessions and routing tables. Soft reconfiguration uses stored information to reconfigure and activate routing tables without clearing existing sessions. It uses stored update information to allow you to restore a connection or to apply a new BGP policy without disrupting the network. Note that outbound soft reconfiguration does not require inbound soft reconfiguration to be enabled.

- The command is only available when route refresh capability is not enabled. Route refresh (RFC 2918) allows a router to reset inbound routing tables dynamically by exchanging route refresh requests with peers. Route refresh relies on the dynamic exchange of information with supporting peers. It is advertised through BGP capability negotiation, and all BGP routers must support this capability.

- To use soft reconfiguration, without preconfiguration, both BGP neighbors must support the soft route refresh capability advertised in open messages sent when a BGP session is established. To see if a BGP router supports this capability, use the show ip bgp neighbors command.

EXAMPLE

```
Console(config-router)#neighbor 11.1.1.120 soft-reconfiguration inbound
Console(config-router)#
```

neighbor strict-capability-match

This command forces strict capability matching when establishing connections. Use the **no** form to disable this requirement.

SYNTAX

[**no**] **neighbor** {*ip-address* | *group-name*} **strict-capability-match**

ip-address – IP address of a neighbor.

group-name – A BGP peer group containing a list of neighboring routers configured with the neighbor peer-group command.

COMMAND MODE

Router Configuration

DEFAULT SETTING

Disabled

COMMAND USAGE

This command specifies that a connection can only be established when the both sides have perfectly matching capabilities.

EXAMPLE

```
Console(config-router)#neighbor 10.1.1.66 strict-capability-match
Console(config-router)#
```

neighbor timers

This command sets the Keep Alive time and Hold time used for specified neighbors. Use the **no** form to restore the default settings.

SYNTAX

[**no**] **neighbor** {*ip-address* | *group-name*} **timers** *keepalive-time hold-time*

ip-address – IP address of a neighbor.

group-name – A BGP peer group containing a list of neighboring routers configured with the neighbor peer-group command.

keepalive-time – The frequency at which the local router sends keep-alive messages to its neighbors. (Range: 0-65535 seconds) *hold-time* – The maximum interval after which a neighbor is declared dead if a keep-alive or update message has not been received. (Range: 0, 3-65535 seconds)

COMMAND MODE

Router Configuration

DEFAULT SETTING

Keep Alive time: 60 seconds
Hold time: 180 seconds

COMMAND USAGE

- This command sets the Keep Alive time used for maintaining connectivity, and the Hold time to wait for Keep Alive or Update messages before declaring a neighbor down.

- This command sets timers for monitoring connectivity to specific neighboring routers, which supercede those applied to all neighbors with the global timers bgp command.

EXAMPLE

```
Console(config-router)#neighbor 10.1.1.66 timers 50 200
Console(config-router)#
```

neighbor timers connect

This command sets the time to wait before attempting to reconnect to a neighbor whose TCP connection has failed. Use the **no** form to restore the default setting.

SYNTAX

[**no**] **neighbor** *ip-address* **timers connect** *retry-interval*

ip-address – IP address of a neighbor.

group-name – A BGP peer group containing a list of neighboring routers configured with the neighbor peer-group command.

retry-interval – The amount of time the system waits for the transport protocol connection to complete. If this timer expires, the state remains in Connect state, the timer is reset, and the system tries to initiate a new transport connection. (Range: 0-65535 seconds)

COMMAND MODE

Router Configuration

DEFAULT SETTING

120 seconds

COMMAND USAGE

This command sets the time to wait before attempting to reconnect to a BGP neighbor after having failed to connect. During the idle time specified by the Connect Retry timer, the remote BGP peer can actively establish a BGP session with the local router.

EXAMPLE

```
Console(config-router)#neighbor 10.1.1.66 timers connect 100
Console(config-router)#
```

neighbor unsuppress-map

This command allows routes suppressed by the aggregate-address (summary-only option) to be advertised to specified neighbors. Use the **no** form to remove this configuration entry.

SYNTAX

[**no**] **neighbor** {*ip-address* | *group-name*} **unsuppress-map** *map-name*

ip-address – IP address of a neighbor.

group-name – A BGP peer group containing a list of neighboring routers configured with the neighbor peer-group command.

map-name – Name of the route map. The route map can be used to filter the networks to advertise. (Range: 1-80 characters)

COMMAND MODE

Router Configuration

DEFAULT SETTING

No exceptions

COMMAND USAGE

This command is used to leak routes suppressed by the aggregate-address command (with summary-only option) to specified neighbors. Other routes that meet the route map conditions, but have not been suppressed, will still be sent.

EXAMPLE

```
Console(config-router)#neighbor 10.1.1.66 unsuppress-map rmp
Console(config-router)#
```

neighbor update-source

This command specifies the interface to use for a TCP connection, instead of using the nearest interface. Use the **no** form to use the default interface.

SYNTAX

[**no**] **neighbor** {*ip-address* | *group-name*} **update-source interface vlan** *vlan-id*

ip-address – IP address of a neighbor.

group-name – A BGP peer group containing a list of neighboring routers configured with the neighbor peer-group command.

vlan-id - VLAN ID. (Range: 1-4094)

COMMAND MODE

Router Configuration

DEFAULT SETTING

The nearest (best/closest) interface is used.

COMMAND USAGE

By default the nearest interface to the neighbor is used for BGP connections. This command can be used to specify any available interface for a TCP connection.

EXAMPLE

```
Console(config-router)#neighbor 10.1.1.66 update-source interface vlan 1
Console(config-router)#
```

neighbor weight

This command assigns a weight to routes sent from a neighbor. Use the **no** form to restore the default weight.

SYNTAX

neighbor {*ip-address* | *group-name*} **weight** *weight*

no neighbor {*ip-address* | *group-name*} **weight**

ip-address – IP address of a neighbor.

group-name – A BGP peer group containing a list of neighboring routers configured with the neighbor peer-group command.

weight – The weight to be assigned to routes received from this neighbor. (Range: 0-65535)

COMMAND MODE

Router Configuration

DEFAULT SETTING

Routes learned from a neighbor: 0
Static routes sourced by the local router: 32768

COMMAND USAGE

- Use this command to specify a weight for all the routes learned from a neighbor. The route with the highest weight gets preference over other routes to the same network.
- Weights assigned using the set weight command override those assigned by this command.

EXAMPLE

```
Console(config-router)#neighbor 10.1.1.66 weight 500
Console(config-router)#
```

Display Information

show ip bgp

This command shows entries in the routing table.

SYNTAX

show ip bgp *ip-address* [*netmask* [**longer-prefixes**]]

ip-address – IP address of a route entry.

netmask – Network mask for the route. This mask identifies the network address bits used for the associated routing entries.

longer-prefixes – Specified route and all more specific routes.

COMMAND MODE

Privileged Exec

EXAMPLE

```
Console#show ip bgp
BGP table version is 0, local router ID is 192.168.0.2
Status codes: s suppressed, d damped, h history, * valid, > best, i internal,
              r RIB-failure, S Stale, R Removed
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop             Metric LocPrf Weight Path
*>12.0.0.0          10.1.1.121                0         32768 ?
*>100.1.1.0/24      10.1.1.200                0         32768 ?
*>100.1.2.0/24      10.1.1.200                0         32768 ?
*i192.168.0.0/24    0.0.0.0                   0         32768 i

Total number of prefixes 4
Console#
```

Table 271: show ip bgp - display description

Field	Description
BGP table version	Internal version number of routing table, incremented per table change.
local router ID	IP address of router.

Table 271: show ip bgp - display description (Continued)

Field	Description
Status codes	Status of table entry includes these values: ◆ s – Entry is suppressed. ◆ d – Entry is dampened. ◆ h – Entry history ◆ * – Entry is valid ◆ > – Best entry for that network ◆ i – Entry learned via internal BGP (iBGP). ◆ r – Entry is Routing Information Base (RIB) failure ◆ S – Entry is stale. ◆ R – Entry removed.
Origin codes	Origin of table entry includes these values: ◆ i – Entry originated from an Interior Gateway Protocol (IGP) and was advertised using a **network** router configuration command. ◆ e – Entry originated from an Exterior Gateway Protocol (EGP). ◆ ? – Origin of the path undetermined. This normally indicates a route which has been redistributed into BGP from an IGP.
Network	IP address of network entry.
Next Hop	IP address of the next router used to reach destination network.
Metric	Value of inter-autonomous system metric.
LocPrf	Local preference value defined by the set local-preference route-map configuration command.
Weight	Weight of the route determined by autonomous system filters.
Path	Autonomous system paths used to reach the destination network.
Total number of prefixes	Total number of unique route prefixes in the table.

show ip bgp attribute-info

This command shows internal attribute hash information.

SYNTAX

show ip bgp attribute-info

COMMAND MODE

Privileged Exec

EXAMPLE

In the following example, Refcnt refers to the number of routes using the indicated next hop.

```
Console#show ip bgp attribute-info
Refcnt  Nexthop
      1 0.0.0.0
      1 10.1.1.64
      3 10.1.1.64
      1 10.1.1.121
      2 10.1.1.200
Console#
```

show ip bgp cidr-ony

This command shows routes which use classless interdomain routing network masks.

SYNTAX

show ip bgp cidr-only

COMMAND MODE

Privileged Exec

EXAMPLE

This example shows routes that do not match the natural A, B, C or D network masks defined for the earliest IP networks.

```
Console#show ip bgp cidr-only
BGP table version is 0, local router ID is 192.168.0.2
Status codes: s suppressed, d damped, h history, * valid, > best, i internal,
              r RIB-failure, S Stale, R Removed
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric LocPrf Weight Path
*>3.3.3.0/24       10.10.10.10                              0 11 i
*>6.6.6.0/24       0.0.0.0                              32768 i
Console#
```

show ip bgp community

This command shows routes that belong to specified BGP communities.

SYNTAX

show ip bgp community [{[*AA*:*NN*] [**internet**] [**local-as**] [**no-advertise**] [**no-export**]} [**exact-match**]]

AA:*NN* – Standard community-number to match. The 4-byte community number is composed of a 2-byte autonomous system number and a 2-byte network number, separated by one colon. Each 2-byte number can range from 0 from 65535. One or more communities can be entered, separated by a space. Up to 16 community numbers are supported.

internet – Specifies the entire Internet. Routes with this community attribute are advertised to all internal and external peers.

local-as – Specifies the local autonomous system. Routes with this community attribute are advertised only to peers that are part of the local autonomous system or to peers within a sub-autonomous system of a confederation. These routes are not advertised to external peers or to other sub-autonomous systems within a confederation.

no-advertise – Routes with this community attribute are not advertised to any internal or external peer.

no-export – Routes with this community attribute are advertised only to peers in the same autonomous system or to other sub-autonomous systems within a confederation. These routes are not advertised to external peers.

exact-match – Displays only routes that match the specified communities exactly.

COMMAND MODE

Privileged Exec

EXAMPLE

```
Console#show ip bgp community
BGP table version is 0, local router ID is 192.168.0.2
Status codes: s suppressed, d damped, h history, * valid, > best, i internal,
              r RIB-failure, S Stale, R Removed
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric LocPrf Weight Path
*  100.1.1.0/24     0.0.0.0                           32768 700 800 i
*> 172.0.0.0/8      0.0.0.0                           32768 700 800 i

Total number of prefixes 2
Console#
```

show ip bgp community-info

This command shows community messages permitted by BGP.

SYNTAX

show ip bgp community-info

COMMAND MODE

Privileged Exec

EXAMPLE

```
Console#show ip bgp community-info
Address    Refcnt  Community
[0x3312558](3)     100:50
Console#
```

Table 272: show ip bgp community-info - display description

Field	Description
Address	Internal address in memory where the entry is stored.
Refcnt	The number of routes which refer to this community.
Community	4-byte community number composed of a 2-byte autonomous system number and a 2-byte network number, separated by one colon

show ip bgp community-list

This command shows the routes matching a community-list.

SYNTAX

show ip bgp community-list {1-99 | 100-500 | *community-list-name*} [**exact-match**]

1-99 – Standard community list number that identifies one or more groups of communities.

100-500 – Expanded community list number that identifies one or more groups of communities.

community-list-name – Name of standard or expanded access list. (Maximum length: 32 characters, no spaces or other special characters)

exact-match – Displays only routes that match the specified communities exactly.

COMMAND MODE

Privileged Exec

EXAMPLE

```
Console#show ip bgp community-list rd
BGP table version is 0, local router ID is 192.168.0.2
Status codes: s suppressed, d damped, h history, * valid, > best, i internal,
              r RIB-failure, S Stale, R Removed
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric LocPrf Weight Path
*  100.1.1.0/24     0.0.0.0                              32768 700 800 i
*> 172.0.0.0/8      0.0.0.0                              32768 700 800 i
Console#
```

show ip bgp dampening

This command shows dampened routes.

SYNTAX

show ip bgp dampening {**dampened-paths** | **flap-statistics** | **parameters**}

dampened-paths – Routes suppressed due to dampening.

flap-statistics – Statistics for flapping route prefixes.

parameters – Route dampening parameters.

COMMAND MODE

Privileged Exec

EXAMPLE

In the following example, "From" indicates the peer that advertised this path, while "Reuse" is the time after which the path will be made available.

```
Console#show ip bgp dampening dampened-paths
BGP table version is 0, local router ID is 192.168.0.2
Status codes: s suppressed, d damped, h history, * valid, > best, i internal,
              r RIB-failure, S Stale, R Removed
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          From             Reuse    Path
*d 100.1.3.0/24     10.1.1.64        00:27:40 100 ?

Total number of prefixes 1
Console#
```

In this example, "Duration" indicates the time since the first flap occurred.

```
Console#show ip bgp dampening flap-statistics
BGP table version is 0, local router ID is 192.168.0.2
Status codes: s suppressed, d damped, h history, * valid, > best, i internal,
              r RIB-failure, S Stale, R Removed
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          From            Flaps Duration Reuse    Path
*d 100.1.3.0/24     10.1.1.64       3     00:06:05 00:27:00 100 ?

Total number of prefixes 1
Console#
```

This example shows the dampening parameters configured on this router.

```
Console#show ip bgp dampening parameters
 Dampening 15 750 2000 60
  Reachability half-life time    :15 min
  Reuse penalty                  :750
  Suppress penalty               :2000
  Max suppress time              :60 min
Console#
```

Table 273: show ip bgp dampening parameters- display description

Field	Description
Reachability half-life time	The time after which a penalty is reduced. The penalty value is reduced to half of the previous value after the half-life time expires.
Reuse penalty	The point to which the penalty for a flapping route must fall before a route is unsuppressed.
Suppress penalty	The point at which to start suppressing a route.
Max suppress time	The maximum time a route can be suppressed.

show ip bgp filter-list

This command shows routes matching the specified filter list.

SYNTAX

show ip bgp filter-list *access-list-name*

access-list-name – Name of a list of autonomous system paths as defined by the ip as-path access-list command. (Maximum length: 16 characters, no spaces or other special characters)

COMMAND MODE

Privileged Exec

EXAMPLE

```
Console#show ip bgp filter-list rd
BGP table version is 0, local router ID is 192.168.0.2
Status codes: s suppressed, d damped, h history, * valid, > best, i internal,
              r RIB-failure, S Stale, R Removed
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric LocPrf Weight Path
*> 100.1.1.0/24     10.1.1.64                0              0 100 ?
Total number of prefixes 1
Console#
```

show ip bgp neighbors

This command chows connection information for neighbor sessions.

SYNTAX

show ip bgp neighbors [*ip-address* [**advertised-routes** | **received prefix-filter** | **received-routes** | **routes**]]

ip-address – IP address of the neighbor.

advertised-routes – Shows the routes advertised to a neighbor.

received prefix-filter – Shows the prefix-list (outbound route filter) sent from a neighbor.

received-routes – Shows all routes, both accepted and rejected, which have been received from a neighbor. To display all received routes from a neighbor, first enable soft reconfiguration with the neighbor soft-reconfiguration inbound command.

routes – Displays all accepted routes learned from a neighbor.

COMMAND MODE

Privileged Exec

```
Console#show ip bgp neighbors 192.168.0.3
BGP neighbor is 192.168.0.3, remote AS 200, local AS 100, external link
 Member of peer-group  for session parameters
  BGP version 4, remote router ID 192.168.0.3
  BGP state = Established, up for 00:00:58
  Last read 16:40:37, hold time is 180, keepalive interval is 60 seconds
  Neighbor capabilities:
    4 Byte AS: advertised and received
    Route refresh: advertised and received(old & new)
    Address family IPv4 Unicast: advertised and received
  Message statistics:
    Inq depth is 0
    Outq depth is 0
                         Sent       Rcvd
    Opens:                  1          0
    Notifications:          0          0
    Updates:                1          1
    Keepalives:             2          1
    Route Refresh:          0          0
    Capability:             0          0
    Total:                  4          2
  Minimum time between advertisement runs is 30 seconds

 For address family: IPv4 Unicast
  Community attribute sent to this neighbor(both)
  Inbound path policy configured
  1 accepted prefixes

  Connections established 1; dropped 0
  Last reset never
Local host: 192.168.0.2, Local port: 179
Foreign host: 192.168.0.3, Foreign port: 3987
Nexthop:
Read thread: on  Write thread: off

Console#
```

Table 274: **show ip bgp** - display description

Field	Description
BGP neighbor	IP address of neighbor.
remote AS	Autonomous system number of the neighbor.
local AS	Local autonomous system number.
external link	“external link” is displayed for external BGP neighbors. “internal link” is displayed for iBGP neighbors.
BGP version	BGP version used to communicate with remote router.
remote router ID	IP address of the neighbor.
BGP state	Stage of session negotiation.
Last read	Time since a message was last received from this neighbor.
hold time	Time to maintain the session with this neighbor without receiving a message.
keepalive interval	Interval at which keepalive messages are transmitted to this neighbor.
Neighbor capabilities	BGP capabilities advertised and received from this neighbor.
Message statistics	Statistics organized by message type.
Minimum time between advertisement runs	Time between transmission of advertisements.
For address family	Address family to which the following information refers.
Local host/port	IP address and TCP port of the local BGP speaker.

Table 274: show ip bgp - display description (Continued)

Field	Description
Foreign host/port	IP address and TCP port of the neighbor BGP speaker.
Nexthop	IP address of next system via which packets are forwarded to the destination network.
Read thread	The read status for the socket connection with this neighbor.
Write thread	The write status for the socket connection with this neighbor.

show ip bgp paths

This command shows all paths in the database.

SYNTAX

show ip bgp paths

COMMAND MODE

Privileged Exec

EXAMPLE

```
Console#show ip bgp paths
Address     RefCnt  ASpath
0x331dad0:0      1
0x331d850:93     1  600
0x331d8d8:249    2  200 300
Console#
```

Table 275: show ip bgp paths - display description

Field	Description
Address	Internal address in memory where the path is stored.
Refcnt	The number of routes using this path.
ASpath	The autonomous system path for this route.

show ip bgp prefix-list

This command shows routes matching the specified prefix-list.

SYNTAX

show ip bgp prefix-list *list-name*

list-name – Name of a prefix-list. The prefix list can be used to filter the networks to import or export as defined by the match ip address prefix-list command. (Range: 1-80 characters)

COMMAND MODE

Privileged Exec

EXAMPLE

```
Console#show ip bgp prefix-list rd
BGP table version is 0, local router ID is 192.168.0.2
Status codes: s suppressed, d damped, h history, * valid, > best, i internal,
              r RIB-failure, S Stale, R Removed
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric LocPrf Weight Path
*  100.1.1.0/24     10.1.1.66                              0 200 300 ?
*>                  10.1.1.100               0         32768 ?
Console#
```

show ip bgp regexp

This command shows routes matching the AS path regular expression.

SYNTAX

show ip bgp regexp *regular-expression*

regular-expression – Regular expression indicating the path attributes to match. Syntax complies with the IEEE POSIX Basic Regular Expressions (BRE) standard.

COMMAND MODE

Privileged Exec

EXAMPLE

```
Console#show ip bgp regexp 100
BGP table version is 0, local router ID is 192.168.0.2
Status codes: s suppressed, d damped, h history, * valid, > best, i internal,
              r RIB-failure, S Stale, R Removed
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric LocPrf Weight Path
*  100.1.1.0/24     10.1.1.64                0             0 500 100 600 ?
Console#
```

show ip bgp route-map

This command shows routes matching the specified route map.

SYNTAX

show ip bgp route-map *map-name*

map-name – Name of the route map as defined by the route-map command. The route map can be used to filter the networks to advertise. (Range: 1-80 characters)

COMMAND MODE

Privileged Exec

EXAMPLE

```
Console#show ip bgp route-map rd
BGP table version is 0, local router ID is 192.168.0.2
Status codes: s suppressed, d damped, h history, * valid, > best, i internal,
              r RIB-failure, S Stale, R Removed
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop           Metric LocPrf Weight Path
*  100.1.1.0/24     10.1.1.64               0             0 500 100 600 ?
*>                  10.1.1.68               0             0 300 ?
Console#
```

show ip bgp scan

This command shows BGP scan status.

SYNTAX

show ip bgp scan

COMMAND MODE

Privileged Exec

EXAMPLE

```
Console#show ip bgp scan
BGP scan is running
BGP scan interval is 60
Current BGP nexthop cache:
 10.10.10.64 valid [IGP metric 0]
BGP connected route:
 10.10.10.0/24
 10.10.11.0/24
Console#
```

show ip bgp summary

This command shows summary information for all connections.

SYNTAX

show ip bgp summary

COMMAND MODE

Privileged Exec

EXAMPLE

In the following example, “Up/Down” refers to the length of time the session has been in the Established state, or the current status if not in Established state.

```
Console#show ip bgp summary
BGP router identifier 192.168.0.2, local AS number 100
RIB entries 0
Peers 1
Peer groups 0
```

```
Neighbor      V   AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
192.168.0.3   4  200     166     168        0    0    0 02:45:00        1

Total number of neighbors 1

Console#
```

show ip community-list

This command shows routes permitted by a community list.

Syntax

show ip community-list [1-99 | 100-500 | *community-list-name*]

1-99 – Standard community list number that identifies one or more groups of communities.

100-500 – Expanded community list number that identifies one or more groups of communities.

community-list-name – Name of standard or expanded access list. (Maximum length: 32 characters, no spaces or other special characters)

Command Mode

Privileged Exec

Example

```
Console#show ip community-list rd
Named Community standard list rd
    permit 100:10
Console#
```

show ip extcommunity-list

This command shows routes permitted by an extended community list.

Syntax

show ip extcommmunity-list [1-99 | 100-500 | *community-list-name*]

1-99 – Standard community list number that identifies one or more groups of communities.

100-500 – Expanded community list number that identifies one or more groups of communities.

community-list-name – Name of standard or expanded access list. (Maximum length: 32 characters, no spaces or other special characters)

Command Mode

Privileged Exec

EXAMPLE

```
Console#show ip extcommunity-list rd
Named extended community standard list rd
    permit RT:192.168.0.0:10
Console#
```

show ip prefix-list

This command shows the specified prefix list.

SYNTAX

show ip prefix-list [*prefix-list-name* [*ip-address netmask* [**first-match** | **longer**] | **seq** *sequence-number*]]

prefix-list-name – Name of prefix list. (Maximum length: 128 characters, no spaces or other special characters)

ip-address – An IPv4 address expressed in dotted decimal notation.

netmask – Network mask for the route. This mask identifies the network address bits used for the associated routing entries.

first-match – First matched prefix.

longer – All entries more specific than the specified network/mask.

sequence-number – The sequence number of an entry. (Range: 1-429496725)

COMMAND MODE

Privileged Exec

EXAMPLE

```
Console#show ip prefix-list rd
ip prefix-list rd: 1 entries
   seq 5 deny 10.0.0.0/8 ge 14 le 22
Console#
```

show ip prefix-list detail

This command shows detailed information for the specified prefix list.

SYNTAX

show ip prefix-list detail [*prefix-list-name*]

prefix-list-name – Name of prefix list. (Maximum length: 128 characters, no spaces or other special characters)

COMMAND MODE

Privileged Exec

EXAMPLE

```
Console#show ip prefix-list detail rd
ip prefix-list rd:
   count: 1, range entries: 0, sequences: 5 - 5
   seq 5 deny 10.0.0.0/8 ge 14 le 22 (hit count: 0, refcount: 0)
Console#
```

show ip prefix-list summary

This command shows summary information for the specified prefix list.

SYNTAX

show ip prefix-list summary [*prefix-list-name*]

prefix-list-name – Name of prefix list. (Maximum length: 128 characters, no spaces or other special characters)

COMMAND MODE

Privileged Exec

EXAMPLE

```
Console#show ip prefix-list summary rd
ip prefix-list rd:
   count: 1, range entries: 0, sequences: 5 - 5
Console#
```

POLICY-BASED ROUTING FOR BGP

This section describes commands used to configure policy-based routing (PBR) maps for Border Gateway Protocol (BGP).

Policy-based routing is performed before regular routing. PBR inspects traffic on the interface where the policy is applied and then, based on the policy, makes some decision. First, the traffic is "matched" according to the policy. Second, for each match, there is something "set." What is set could be that the traffic matches must exit out a different interface, or the traffic could be given a higher priority, or it could choose to just drop that traffic.

Matching of the traffic is usually done with an ACL (access-control list) that is referenced by a route-map. In the route-map, if there is a "match" for the traffic defined in that ACL, then a "set" defines what the administrator wants to happen to that traffic (prioritize it, route it differently, drop it, or other actions). Policies can be based on IP address, port numbers, protocols, or size of packets.

If matching criteria is found and the specified action is to permit the packet, then it will be forwarded to the next hop based on policy-based routing. If the action is to deny the packet, normal unicast routing is used to determine the packet's next hop, instead of using policy-based routing. If no matching criteria are found in the route map, normal unicast routing is used to determine the packet's next hop. Although route redistribution is protocol-independent, some of the route-map match and set commands defined in this section are specific to BGP.

Like matches in the same route map subblock are filtered with "or" semantics. If any one match clause is matched in the entire route map subblock, this match is treated as a successful match. Dissimilar match clauses are filtered with "and" semantics. If the first set of conditions is not met, the second match clause is filtered. This process continues until a match occurs or there are no more match clauses.

A route map can have several sequences. A route that does not match at least one match command defined in a route-map will be ignored; that is, the route will not be advertised for outbound route maps nor accepted for inbound route maps.

Table 276: Policy-based Routing Configuration Commands

Command	Function	Mode
route-map	Enters route-map configuration mode, allowing route maps to be created or modified	GC
call	Jumps to another route map after match and set commands are executed	RM
continue	Goes to a route-map entry with a higher sequence number after a successful match occurs	RM
description	Creates a description of an entry in the route map	RM
match as-path	Sets an AS path access list to match	RM
match community	Sets a BGP community access list to match	RM
match extcommunity	Sets a BGP extended community access list to match	RM
match ip address	Specifies destination addresses to match in a standard access list, extended access list, or prefix list	RM
match ip next-hop	Specifies next hop addresses to match in a standard access list, extended access list, or prefix list	RM
match ip route-source	Specifies the source of routing messages to match in a standard access list, extended access list, or prefix list	RM
match metric	Sets the metric value to match in routing messages	RM
match origin	Sets the originating protocol to match in routing messages	RM
match pathlimit as	Sets the maximum AS path length for propagation of more specific prefixes to match in routing messages	RM
match peer	Sets the peer address to match in routing messages	RM
on-match	Sets the next entry to go to when this entry matches	RM
set aggregator as	Assigns an AS number and IP address to the aggregator attribute of a route	RM
set as-path	Modifies the AS path by prepending or excluding an AS number	RM
set atomic-aggregate	Indicates the loss of some information in the route aggregation process	RM
set comm-list delete	Removes communities from the community attribute of inbound or outbound routing messages	RM

Table 276: Policy-based Routing Configuration Commands (Continued)

Command	Function	Mode
set community	Sets the community attributes of routing messages	RM
set extcommunity	Sets the extended community attributes of routing messages	RM
set ip next-hop	Sets the next-hop for a routing message	RM
set local-preference	Sets the priority within the local AS for a routing message	RM
set metric	Sets the metric value of a route to external neighbors	RM
set origin	Sets the origin code for the routing protocol which generated this message	RM
set originator-id	Sets the IP address of the routing message's originator	RM
set pathlimit ttl	Sets the maximum AS path length for propagation of more specific prefixes in routing messages	RM
set weight	Sets the weight for routing messages	RM
show route-map	Shows the configuration setting for a route map	PE

route-map

This command enters route-map configuration mode, allowing route maps to be created or modified. Use the **no** form to remove a route map.

SYNTAX

[**no**] **route-map** *map-name* {**deny** | **permit**} *sequence-number*

map-name – Name for the route map. (Range: 1-128 case-sensitive alphanumeric characters)

deny – Route-map denies set operations.

permit – Route-map permits set operations.

sequence-number – Sequence to insert to or delete from existing route-map entry. (Range: 1-65535)

COMMAND MODE

Global Configuration

DEFAULT SETTING

Disabled

COMMAND USAGE

- This command enters the route map configuration mode. In this mode, a new route map can be created, or an existing route map modified.
- The match commands specify the conditions under which policy routing occurs, and the set commands specify the routing actions to perform if the criteria enforced by the match commands are met.
- If the match criteria are met for a route map, and the permit keyword specified, the packet is policy routed based on defined set commands.

- If the match criteria are not met, and the permit keyword specified, the next route map with the same map-name is tested. If a route passes none of the match criteria for the set of route maps sharing the same name, it is not policy routed by that set.

- If the match criteria are met for the route map and the deny keyword specified, the packet is not policy routed, and no further route maps sharing the same map-name are examined. If the packet is not policy routed, the normal forwarding process is used.

- Processing for exceptions include the following results:
  - For a deny route-map, if it does not have a match clause, any routing message is matched, and therefore all routes are denied.
  - For a deny route-map which includes a match clause for an access-list, if the access-list does not exist, no routing message will be matched, and therefore all routes are skipped.
  - For a permit route-map, if it does not have a match clause, any routing message is matched, and therefore all routes are permitted.
  - For a permit route-map which includes a match clause for an access-list, if the access-list does not exist, no routing messages are matched, and therefore all routes are skipped.

EXAMPLE

```
Console(config)#route-map r1 permit 1
Console(config-route-map)#match as-path 60
Console(config-route-map)#set weight 30
Console(config-route-map)#
```

call

This command jumps to another route map after match and set commands are executed. Use the **no** form to remove an entry from a route map.

SYNTAX

call *map-name*

no call

map-name – Name for the route map. (Range: 1-128 case-sensitive alphanumeric characters)

COMMAND MODE

Route Map

COMMAND USAGE

Only one call clause is permitted per route map. The call clause executed only after all match and set commands are executed.

EXAMPLE

```
Console(config)#route-map r1 permit 1
Console(config-route-map)#match as-path 60
Console(config-route-map)#set weight 30
Console(config-route-map)#call FD
Console(config-route-map)#
```

continue

This command goes to a route-map entry with a higher sequence number after a successful match occurs. Use the **no** form to remove this entry from a route map.

SYNTAX

continue [*sequence-number*]

no continue

sequence-number – Sequence number at which to continue processing. (Range: 1-65535)

COMMAND MODE

Route Map

COMMAND USAGE

If no match statements precede the call entry, the call is automatically executed. If no sequence number is specified by the call entry, the next entry is executed.

EXAMPLE

```
Console(config)#route-map RD permit 1
Console(config-route-map)#match as-path 60
Console(config-route-map)#set weight 30
Console(config-route-map)#continue 3
Console(config-route-map)#
```

description

This command creates a description of an entry in the route map. Use the **no** form to remove the description.

SYNTAX

description *text*

no description

text – Comment describing this route-map rule. (Maximum length: 128 characters, no spaces or other special characters)

COMMAND MODE

Route Map

EXAMPLE

```
Console(config)#route-map RD permit 1
Console(config-route-map)#description AS-Path rule
Console(config-route-map)#match as-path 60
Console(config-route-map)#set weight 30
Console(config-route-map)#
```

match as-path

This command sets a BGP autonomous system path access list to match. Use the **no** form to remove this entry from a route map.

SYNTAX

[**no**] **match as-path** *access-list-name*

access-list-name – Name of the access list. (Maximum length: 16 characters, no spaces or other special characters)

COMMAND MODE

Route Map

COMMAND USAGE

The weights assigned by the **match as-path** and set weight route-map commands command override the weight assigned using the BGP neighbor weight command.

EXAMPLE

```
Console(config)#route-map RD permit 1
Console(config-route-map)#match as-path 60
Console(config-route-map)#set weight 30
Console(config-route-map)#
```

RELATED COMMANDS

ip as-path access-list (1833)

match community

This command sets a BGP community access list to match. Use the **no** form to remove this entry from a route map.

SYNTAX

match community {1-99 | 100-500 | *community-list-name*} [**exact-match**]

no match community

1-99 – Standard community list number that identifies one or more groups of communities.

100-500 – Expanded community list number that identifies one or more groups of communities.

community-list-name – Name of standard or expanded community list. (Maximum length: 32 characters, no spaces or other special characters)

exact-match – Must exactly match the specified community list. All and only those communities specified must be present.

COMMAND MODE

Route Map

COMMAND USAGE

This command matches the community attributes of the BGP routing message following the rules specified with the ip community-list command.

EXAMPLE

```
Console(config)#route-map RD permit 2
Console(config-route-map)#match community 60
Console(config-route-map)#set weight 30
Console(config-route-map)#
```

match extcommunity

This command sets a BGP extended community access list to match. Use the **no** form to remove this entry from a route map.

SYNTAX

match extcommunity {1-99 | 100-500} [**exact-match**]

no match extcommunity

1-99 – Standard community list number that identifies one or more groups of communities.

100-500 – Expanded community list number that identifies one or more groups of communities.

COMMAND MODE

Route Map

COMMAND USAGE

This command matches the extended community attributes of the BGP routing message following the rules specified with the ip extcommunity-list command.

EXAMPLE

```
Console(config)#route-map RD permit 3
Console(config-route-map)#match extcommunity 160
Console(config-route-map)#set weight 30
Console(config-route-map)#
```

match ip address

This command specifies the destination addresses to be matched in a standard access list, an extended access list, or a prefix list. Use the **no** form to remove this entry from a route map.

SYNTAX

match ip address {*access-list-name* | **prefix-list** *prefix-list-name*}

no match ip address

access-list-name – Name of standard or extended access list. (Maximum length: 32 characters, no spaces or other special characters)

prefix-list-name – Name of a specific prefix list.

COMMAND MODE

Route Map

EXAMPLE

```
Console(config)#route-map RD permit 4
Console(config-route-map)#match ip address rd-addresses
Console(config-route-map)#set weight 30
Console(config-route-map)#
```

RELATED COMMANDS

ip prefix-list (1838)
Access Control Lists (1163)

match ip next-hop

This command specifies the next-hop addresses to be matched in a standard access list, an extended access list, or a prefix list. Use the **no** form to remove this entry from a route map.

SYNTAX

match ip next-hop {*access-list-name* | **prefix-list** *prefix-list-name*}

no match ip next-hop

access-list-name – Name of standard or extended access list. (Maximum length: 32 characters, no spaces or other special characters)

prefix-list-name – Name of a specific prefix list.

COMMAND MODE

Route Map

COMMAND USAGE

When inbound update messages are received from a neighbor, next-hop information contained in Network Layer Reachability Information (NLRI) entries is checked against the specified access-list or prefix-list before any routes are learned.

EXAMPLE

```
Console(config)#route-map RD permit 5
Console(config-route-map)#match ip next-hop rd-next-hops
Console(config-route-map)#set weight 30
Console(config-route-map)#
```

match ip route-source

This command specifies the source of routing messages advertised by routers and access servers to be matched in a standard access list, an extended access list, or a prefix list. Use the **no** form to remove this entry from a route map.

SYNTAX

match ip route-source {*access-list-name* | **prefix-list** *prefix-list-name*}

no match ip route-source [*access-list-name* | **prefix-list**]

access-list-name – Name of standard or extended access list. (Maximum length: 32 characters, no spaces or other special characters)

prefix-list-name – Name of a specific prefix list.

COMMAND MODE

Route Map

COMMAND USAGE

Note that there may be situations in which the next hop and source router address of the route are not the same.

EXAMPLE

```
Console(config)#route-map RD permit 6
Console(config-route-map)#match ip route-source rd-sources
Console(config-route-map)#set weight 30
Console(config-route-map)#
```

match metric

This command sets the metric value to match in routing messages. Use the **no** form to remove this entry from a route map.

SYNTAX

match metric *metric-value*

no match metric

metric-value – The metric value in the routing messages. (Range: 0-4294967295)

COMMAND MODE

Route Map

EXAMPLE

```
Console(config)#route-map RD permit 7
Console(config-route-map)#match metric 60
Console(config-route-map)#set weight 30
Console(config-route-map)#
```

match origin

This command sets the originating protocol to match in routing messages. Use the **no** form to remove this entry from a route map.

SYNTAX

match origin {**egp** | **igp** | **incomplete**}

no match origin

egp – Routes learned from exterior gateway protocols.

igp – Routes learned from internal gateway protocols.

incomplete – Routes of uncertain origin.

COMMAND MODE

Route Map

EXAMPLE

```
Console(config)#route-map RD permit 8
Console(config-route-map)#match origin igp
Console(config-route-map)#set weight 30
Console(config-route-map)#
```

match pathlimit as

This command sets the maximum AS path length allowed for propagation of more specific prefixes to match in routing messages. Use the **no** form to remove this entry from a route map.

SYNTAX

match pathlimit as *as-limit*

no match pathlimit as

as-limit – Maximum AS path length. (Range: 1-4294967295)

COMMAND MODE

Route Map

COMMAND USAGE

- To perform inter-domain traffic engineering, a multi-homed site can advertise its prefix to all of its neighbors via an aggregate address, and also advertise more specific prefixes to a subset of its neighbors. The longest match lookup algorithm then causes traffic for the more specific prefixes to be forwarded to the subset of neighbors with the more specific prefix.

These longer prefixes may be advertised in addition to an aggregate, even when the aggregate advertisement is sufficient for basic reachability. This type of inter-domain traffic engineering is a widely used phenomenon that is contributing to growth in the size of the global routing table.

Traffic engineering via longer prefixes is only effective when the longer prefixes have a different next hop from the less specific prefix. Thus, past the point where the next hops become identical, the longer prefixes provide no value whatsoever. This command can be used to limit the radius of propagation of more specific prefixes by adding a count of the ASes that may be traversed by the more specific prefix.

- Private AS numbers [RFC1930] and confederation AS members [RFC3065] found in the AS_PATH are not counted. AS numbers found within an AS_SET are not counted and an entire AS_SET is counted as a single AS. Each instance of an AS number that appears multiple times in an AS_PATH is counted.

  If the AS_PATHLIMIT attribute is attached to a prefix by a private AS, then when the prefix is advertised outside of the parent AS, the AS number contained in the AS_PATHLIMIT attribute should be replaced by the AS number of the parent AS.

  Similarly, if the AS_PATHLIMIT attribute is attached to a prefix by a member of a confederation, then when the prefix is advertised outside of the confederation boundary, then the AS number of the confederation member inside of the AS_PATHLIMIT attribute should be replaced by the confederation's AS number.

EXAMPLE

```
Console(config)#route-map RD permit 8
Console(config-route-map)#match pathlimit as 5
Console(config-route-map)#on match goto 20
Console(config-route-map)#
```

match peer

This command sets the peer address to match in routing messages. Use the **no** form to remove this entry from a route map.

SYNTAX

match peer {*peer-address* | **local**}

no match peer [*peer-address* | **local**]

peer-address – IP address of neighboring router sending routing messages.

local – Static or redistributed routes.

COMMAND MODE

Route Map

EXAMPLE

```
Console(config)#route-map RD permit 9
Console(config-route-map)#match peer 192.168.0.99
Console(config-route-map)#set weight 30
Console(config-route-map)#
```

on-match

This command sets the next entry to go to when this entry matches. Use the **no** form to remove this entry from a route map.

SYNTAX

on-match peer {**goto** *sequence-number* | **next**}

no on-match peer {**goto** | **next**}

goto – On match, go to specified entry.

sequence-number – Route-map entry. (Range: 1-65535)

next – Go to next entry.

COMMAND MODE

Route Map

COMMAND USAGE

Use this command when no set action is for a match clause.

EXAMPLE

```
Console(config)#route-map RD permit 8
Console(config-route-map)#match pathlimit as 5
Console(config-route-map)#on match goto 20
Console(config-route-map)#
```

set aggregator as

This command assigns an AS number and IP address to the aggregator attribute of a route. Use the **no** form to remove this entry from a route map.

SYNTAX

set aggregator as *as-number ip-address*

no set aggregator as [*as-number ip-address*]

as-number – Autonomous system number. (Range: 1-4294967295)

ip-address – IP address of aggregator.

COMMAND MODE

Route Map

Command Usage

Aggregate routes advertised to a neighbor contain an aggregator attribute. This attribute contains an AS number and IP address. The AS number is the creator's AS number (or confed ID in a confederation) and an IP address which is the creator’s router-id. The **set aggregator as** command can be used to overwrite the aggregator attribute in routes created locally with the aggregate-address command, or in routes learned from a neighbor which already carry an aggregator attribute, or to add a new aggregator attribute to a route which has no aggregator attribute.

Example

```
Console(config)#route-map RD permit 8
Console(config-route-map)#match pathlimit as 5
Console(config-route-map)#set aggregator 1 192.168.0.0
Console(config-route-map)#
```

set as-path

This command modifies the AS path by prepending or excluding an AS number. Use the **no** form to remove this entry from a route map.

Syntax

set as-path {**exclude** | **prepend**} *as-number*...

no set as-path {**exclude** | **prepend**}

exclude – Removes one or more autonomous system numbers from the AS path of the route that is matched.

prepend – Appends one or more autonomous system numbers to the AS path of the route that is matched.

as-number – Autonomous system number. (Range: 1-4294967295)

Command Mode

Route Map

Command Usage

Note that best path selection may be influenced with this command by varying the length of the autonomous system path.

Example

```
Console(config)#route-map RD permit 8
Console(config-route-map)#match peer 192.168.0.99
Console(config-route-map)#set as-path prepend 2
Console(config-route-map)#
```

set atomic-aggregate

This command indicates the loss of some information in the route aggregation process. Use the **no** form to remove this entry from a route map.

SYNTAX

[**no**] **set atomic-aggregate**

COMMAND MODE

Route Map

COMMAND USAGE

The purpose of the atomic-aggregate attribute is to alert BGP speakers along the path that some information have been lost due to the route aggregation process and that the aggregate path might not be the best path to the destination. This attribute should be set when the BGP speaker advertises ONLY the less-specific prefix and suppresses more specific ones.

EXAMPLE

```
Console(config)#route-map RD permit 9
Console(config-route-map)#match peer 192.168.0.99
Console(config-route-map)#set atomic-aggregate
Console(config-route-map)#
```

set comm-list delete

This command removes communities from the community attribute of inbound or outbound routing messages. Use the **no** form to remove this entry from a route map.

SYNTAX

[**no**] **set comm-list** {1-99 | 100-500 | *community-list-name*} [delete]

1-99 – Standard community list number that identifies one or more groups of communities.

100-500 – Expanded community list number that identifies one or more groups of communities.

community-list-name – Name of standard or expanded community list. (Maximum length: 32 characters, no spaces or other special characters)

COMMAND MODE

Route Map

COMMAND USAGE

When using the ip community-list command to configure a community access list, each entry of a standard community list should list only one community. Otherwise, the **set comm-list delete** command will not succeed. For example, in order to be able to delete communities 100 and 200, you must create two separate entries with the ip community-list command.

EXAMPLE

```
Console(config)#route-map RD permit 10
Console(config-route-map)#match peer 192.168.0.77
Console(config-route-map)#set comm-list 10:01 delete
Console(config-route-map)#exit
Console(config)#route-map RD permit 11
Console(config-route-map)#match peer 192.168.0.99
Console(config-route-map)#set comm-list 20:01 delete
Console(config-route-map)#
```

set community

This command sets the community attributes of routing messages. Use the **no** form to remove this entry from a route map.

SYNTAX

set community
[*AA*:*NN...*]
[**additive** {[*AA*:*NN...*] [**internet**] [**local-as**] [**no-advertise**] [**no-export**]}
[**internet** [[*AA*:*NN...*] [**local-as**] [**no-advertise**] [**no-export**]]
[**local-as** [[*AA*:*NN...*] [**no-advertise**] [**no-export**]]
[**no-advertise** [*AA*:*NN...*] [**no-export**]]
[**no-export** [*AA*:*NN...*]]
[**none**]

no set community

AA:*NN* – Standard community-number. The 4-byte community number is composed of a 2-byte autonomous system number and a 2-byte network number, separated by one colon. Each 2-byte number can range from 0 from 65535. One or more communities can be entered, separated by a space. Up to 16 community numbers are supported.

additive – Adds community attributes to already existing community attributes.

internet – Specifies the entire Internet. Routes with this community attribute are advertised to all internal and external peers.

local-as – Specifies the local autonomous system. Routes with this community attribute are advertised only to peers that are part of the local autonomous system or to peers within a sub-autonomous system of a confederation. These routes are not advertised to external peers or to other sub-autonomous systems within a confederation.

no-advertise – Routes with this community attribute are not advertised to any internal or external peer.

no-export – Routes with this community attribute are advertised only to peers in the same autonomous system or to other sub-autonomous systems within a confederation. These routes are not advertised to external peers.

none – Delete the community attributes from the prefix of this route.

COMMAND MODE

Route Map

EXAMPLE

```
Console(config)#route-map RD permit 11
Console(config-route-map)#match peer 192.168.0.99
Console(config-route-map)#set community 10:01
Console(config-route-map)#exit
Console(config)#route-map RD permit 12
Console(config-route-map)#match peer 192.168.0.99
Console(config-route-map)#set community 20:01
Console(config-route-map)#
```

RELATED COMMANDS

set comm-list delete

set extcommunity

This command sets the extended community attributes of routing messages. Use the **no** form to remove this entry from a route map.

SYNTAX

set extcommunity {**rt** *extended-community-value* |
  soo *extended-community-value*}

no set extcommunity [**rt** | **soo**]

rt – The route target extended community attribute.

soo – The site of origin extended community attribute.

extended-community-value – The route target or site of origin in one of the following formats:

AAAA:*NN* or *AA*:*NNNN* – Community-number to deny or permit. The community number can either be formatted as a 4-byte autonomous system number and a 2-byte network number, or as a 2-byte autonomous system number and a 4-byte network number, separated by one colon. Each 2-byte number can range from 0 to 65535, and 4-byte numbers from 0 to 4294967295.

IP:*NN* – Community to deny or permit. The community number is composed of a 4-byte IP address (representing the autonomous system number) and a 2-byte network number, separated by one colon. The 2-byte network number can range from 0 to 65535.

One or more community numbers can be entered, separated by a space. Up to 3 community numbers are supported.

COMMAND MODE

Route Map

COMMAND USAGE

- Using the **rt** keyword to specify new route targets replaces existing route targets.

- The route target (RT) attribute is used to identify sites that may receive routes tagged with a specific route target. Using this attribute allows that route to be placed in per-site forwarding tables used for routing traffic received from the corresponding sites.

- The site of origin (SOO) attribute is used to identify the site from which the provider edge (PE) router learned the route. All routes learned from a particular site are assigned the same site of origin attribute, no matter if a site is connected to a single PE router or multiple PE routers. Filtering based on this extended community attribute can prevent routing loops from occurring when a site is multi-homed.

EXAMPLE

```
Console(config)#route-map RD permit 13
Console(config-route-map)#match peer 192.168.0.99
Console(config-route-map)#set extcommunity 100:0 192.168.1.1:1
Console(config-route-map)#
```

set ip next-hop

This command sets the next-hop for a routing message. Use the **no** form to remove this entry from a route map.

SYNTAX

set ip next-hop {*ip-address* | **peer-address**}

no set ip next-hop [*ip-address*]

ip-address – An IPv4 address of the next hop, expressed in dotted decimal notation.

peer-address – Sets the next hop as the BGP peering address.

COMMAND MODE

Route Map

COMMAND USAGE

- The IP address specified as the next hop need not be an adjacent router.

- When this command is used with the **peer-address** keyword in an inbound route map received from a BGP peer, the next hop of the received matching routes are set to be the neighbor peer address, overriding any other next hops.

- When this command is used with the **peer-address** keyword in an outbound route map for a BGP peer, the next hop of the advertised matching routes will be set to be the peering address of the local router, thus disabling next hop calculation. This command therefore has finer granularity than the neighbor next-hop-self command, because it can set the next hop for some routes, but not others. While the neighbor next-hop-self command sets the next hop for all routes sent to the specified neighbor(s).

EXAMPLE

```
Console(config)#route-map RD permit 14
Console(config-route-map)#match peer 192.168.0.99
Console(config-route-map)#set ip next-hop 192.168.0.254
Console(config-route-map)#
```

set local-preference

This command sets the priority within the local AS for a routing message. Use the **no** form to remove this entry from a route map.

SYNTAX

set local-preference *preference*

no set local-preference

preference – Degree of preference iBGP peers give local routes during BGP best path selection. The higher the value, the more the route is to be preferred. (Range: 1-4294967295)

COMMAND MODE

Route Map

COMMAND USAGE

- The preference is sent only to routers in the local autonomous system. To specify the metric for inter-autonomous systems, use the set metric command.
- A route with a higher local priority level when compared with other routes to the same destination will be preferred over other routes.

EXAMPLE

```
Console(config)#route-map RD permit 15
Console(config-route-map)#match peer 192.168.0.99
Console(config-route-map)#set local-preference 2
Console(config-route-map)#
```

set metric

This command sets the metric value of a route to external neighbors. Use the **no** form to restore the default value.

SYNTAX

set metric [**+** | **-**]*metric-value*

no set metric

metric-value – Metric value assigned to all external routes for the specified protocol. (Range: 0-4294967295)

DEFAULT SETTING

The dynamically learned metric value.

COMMAND MODE

Route Map

COMMAND USAGE

- Lower metric values indicate a higher priority.
- This command can modify the current metric for a route using the "+" or "-" keywords.
- The metric applies to external routers in the inter-autonomous system. To specify the metric for the local AS, use the set local-preference command.
- This path metric is normally only compared with neighbors in the local AS. To extend the comparison to paths advertised from neighbors in different autonomous systems, use the bgp always-compare-med command.

EXAMPLE

```
Console(config)#route-map RD permit 16
Console(config-route-map)#match peer 192.168.0.99
Console(config-route-map)#set metric +1
Console(config-route-map)#
```

set origin

This command sets the BGP origin code for the routing protocol which generated this message. Use the **no** form to remove this entry from a route map.

SYNTAX

set origin {**egp** | **igp** | **incomplete**}

no set origin

egp – Exterior gateway protocols.

igp – Interior gateway protocols.

incomplete – Route origin unknown.

DEFAULT SETTING

As indicated in main IP routing table

COMMAND MODE

Route Map

COMMAND USAGE

EGP is an inter-domain routing protocol which has been superceded by BGP. IGP indicates any intra-domain routing protocol such as RIP or OSPF.

EXAMPLE

```
Console(config)#route-map RD permit 16
Console(config-route-map)#match peer 192.168.0.99
Console(config-route-map)#set origin egp
Console(config-route-map)#
```

set originator-id

This command sets the IP address of the routing message's originator. Use the **no** form to remove this entry from a route map.

SYNTAX

set originator-id *ip-address*

no set originator-id

ip-address – An IPv4 address of the route source, expressed in dotted decimal notation.

COMMAND MODE

Route Map

COMMAND USAGE

This attribute is commonly used for loop prevention by rejecting updates that contain the receiving router's own router-ID in the originator-ID attribute.

EXAMPLE

```
Console(config)#route-map RD permit 17
Console(config-route-map)#match peer 192.168.0.99
Console(config-route-map)#set originator-id 192.168.0.254
Console(config-route-map)#
```

set pathlimit ttl

This command sets the maximum AS path length for propagation of more specific prefixes in routing messages. Use the **no** form to remove this entry from a route map.

SYNTAX

set pathlimit ttl *ttl-value*

no set pathlimit ttl

ttl-value – Maximum number of router hops allowed in an AS path. (Range: 1-255)

COMMAND MODE

Route Map

COMMAND USAGE

Due to the dynamic changes in connections for network paths, it is not advisable to restrict the number of router hops for any path. However, if the connections to the destination network are relatively stable, the hop count can be restricted to force traffic to follow an alternate path. This method may be used to avoid less heavily congested paths or to route traffic through a preferred provider.

EXAMPLE

```
Console(config)#route-map RD permit 18
Console(config-route-map)#match peer 192.168.0.99
Console(config-route-map)#set pathlimit ttl 255
Console(config-route-map)#
```

set weight

This command sets the weight for routing messages. Use the **no** form to remove this entry from a route map.

SYNTAX

set weight *weight*

no set weight

weight – The weight assigned to this route. (Range: 0-4294967295)

COMMAND MODE

Route Map

COMMAND USAGE

- Weights are used to determine the best path available to the local switch. The route with the highest weight gets preference over other routes to the same network.

- Weights assigned using this command override those assigned by the neighbor weight command.

EXAMPLE

```
Console(config)#route-map RD permit 19
Console(config-route-map)#match peer 192.168.0.99
Console(config-route-map)#set weight 255
Console(config-route-map)#
```

show route-map

This command shows the configuration setting for a route map.

SYNTAX

show route-map [*map-name*]

map-name – Name for the route map. (Range: 1-128 case-sensitive alphanumeric characters)

COMMAND MODE

Privileged Exec

EXAMPLE

```
Console#show route-map RD
route-map RD, permit, sequence 1
  Match clauses:
    peer 102.168.0.99
  Set clauses:
    comm-list 100 delete
  Call clause:
  Action:
    Exit routemap
Console#
```

52 Multicast Routing Commands

Multicast routers can use various kinds of multicast routing protocols to deliver IP multicast packets across different subnetworks. This router supports Protocol Independent Multicasting (PIM). (Note that IGMP will be enabled for any interface that is using multicast routing.)

Table 277: Multicast Routing Commands

Command Group	Function
General Multicast Routing	Enables IP multicast routing globally; also displays the IP multicast routing table created from static and dynamic routing information
Static Multicast Routing	Configures static multicast router ports
PIM Multicast Routing	Configures global and interface settings for PIM-DM and PIM-SM

General Multicast Routing

This section describes commands used to configure multicast routing globally on the switch.

Table 278: General Multicast Routing Commands

Command	Function	Mode
IPv4 Commands		
ip multicast-routing	Enables IPv4 multicast routing	GC
show ip mroute	Shows the IPv4 multicast routing table	PE
IPv6 Commands		
ipv6 multicast-routing	Enables IPv6 multicast routing	GC
show ipv6 mroute	Shows the IPv6 multicast routing table	PE

IPv4 Commands

ip multicast-routing

This command enables IPv4 multicast routing. Use the **no** form to disable IP multicast routing.

Syntax

[**no**] **ip multicast-routing**

Default Setting

Disabled

COMMAND MODE

Global Configuration

COMMAND USAGE

- This command is used to enable IPv4 multicast routing globally for the router. A specific multicast routing protocol also needs to be enabled on the interfaces that will support multicast routing using the router pim command, and then specify the interfaces that will support multicast routing using the ip pim dense-mode or ip pim sparse-mode commands.

- To use multicast routing, IGMP proxy can not enabled on any interface of the device (see ip igmp proxy on page 1523).

EXAMPLE

```
Console(config)#ip multicast-routing
Console(config)#
```

show ip mroute

This command displays the IPv4 multicast routing table.

SYNTAX

show ip mroute [*group-address source*] [**summary**]

group-address - An IPv4 multicast group address with subscribers directly attached or downstream from this router.

source - The IPv4 subnetwork at the root of the multicast delivery tree. This subnetwork contains a known multicast source.

summary - Displays summary information for each entry in the IP multicast routing table.

COMMAND MODE

Privileged Exec

COMMAND USAGE

This command displays information for multicast routing. If no optional parameters are selected, detailed information for each entry in the multicast address table is displayed. If you select a multicast group and source pair, detailed information is displayed only for the specified entry. If the **summary** option is selected, an abbreviated list of information for each entry is displayed on a single line.

EXAMPLE

This example shows detailed multicast information for a specified group/ source pair

```
Console#show ip mroute 224.0.255.3 192.111.46.8

IP Multicast Forwarding is enabled.

IP Multicast Routing Table
Flags: D - Dense, S - Sparse, s - SSM Channel, C - Connected, P - Pruned,
       F - Register flag, R - RPT-bit set, T - SPT-bit set, J - Join SPT
Interface state: F - Forwarding, P - Pruned, L - Local

(192.168.2.1, 224.0.17.17), uptime 00:00:05
Owner: PIM-DM, Flags: D
Incoming Interface: VLAN2, RPF neighbor: 192.168.2.1
Outgoing Interface List:
VLAN1(F)

Console#
```

Table 279: show ip mroute - display description

Field	Description
`Flags`	The flags associated with this entry: ◆ D (Dense) - PIM Dense mode in use. ◆ S (Sparse) - PIM Sparse mode in use. ◆ s (SSM) - A multicast group with the range of IP addresses used for PIM-SSM. ◆ C (Connected) - A member of the multicast group is present on this interface. ◆ P (Pruned) - This route has been terminated. ◆ F (Register flag) - This device is registering for a multicast source. ◆ R (RP-bit set) - The (S,G) entry is pointing to the Rendezvous Point (RP), which normally indicates a pruned state along the shared tree for a particular source. ◆ T (SPT-bit set) - Multicast packets have been received from a source on the shortest path tree. ◆ J (Join SPT) - The rate of traffic arriving over the shared tree has exceeded the SPT-threshold for this group. If the SPT flag is set for (*,G) entries, the next (S,G) packet received will cause the router to join the shortest path tree. If the SPT flag is set for (S,G), the router immediately joins the shortest path tree.
`Interface state`	The multicast state for the displayed interface.
`group address`	IP multicast group address for a requested service.
`source`	Subnetwork containing the IP multicast source.
`uptime`	The time elapsed since this entry was created.
`Owner`	The associated multicast protocol (PIM).
`Incoming Interface`	Interface leading to the upstream neighbor. PIM creates a multicast routing tree based on the unicast routing table. If the related unicast routing table does not exist, PIM will still create a multicast routing entry, but displays “Null” for the upstream interface to indicate that the unicast routing table is not valid. This field may also display “Register” to indicate that a pseudo interface is being used to send or receive PIM-SM register packets.

Table 279: show ip mroute - display description (Continued)

Field	Description
`RPF neighbor`	IP address of the multicast router immediately upstream for this group.
`Outgoing interface list and flags`	The interface(s) on which multicast subscribers have been recorded. The flags associated with each interface indicate: ◆ F (Register flag) - This device is registering for a multicast source. ◆ P (Pruned) - This route has been terminated. ◆ L (Local) - Downstream interface has received IGMP report message from host in this subnet.

This example lists all entries in the multicast table in summary form:

```
Console#show ip mroute summary

IP Multicast Forwarding is enabled

IP Multicast Routing Table (Summary)
Flags: F - Forwarding,  P - Pruned
     Group          Source        Source Mask    Interface  Owner   Flags
--------------- --------------- --------------- ---------- ------- ------
    224.0.17.17     192.168.2.1 255.255.255.255 VLAN2      PIM-DM  F
 Total Entry is 1

Console#
```

IPv6 Commands

ipv6 multicast-routing

This command enables IPv6 multicast routing. Use the **no** form to disable IP multicast routing.

SYNTAX

[**no**] **iv6p multicast-routing**

DEFAULT SETTING

Disabled

COMMAND MODE

Global Configuration

COMMAND USAGE

- This command is used to enable IPv6 multicast routing globally for the router. A multicast routing protocol also needs to be enabled on the interfaces that will support multicast routing using the router pim6 command, and then specify the interfaces that will support multicast routing using the ipv6 pim command.

- To use multicast routing, MLD proxy can not enabled on any interface of the device (see ipv6 mld proxy on page 1534).

EXAMPLE

```
Console(config)#ipv6 multicast-routing
Console(config)#
```

show ipv6 mroute

This command displays the IPv6 multicast routing table.

SYNTAX

show ipv6 mroute [*group-address source*] [**summary**]

group-address - An IPv6 multicast group address with subscribers directly attached or downstream from this router.

source - The IPv6 subnetwork at the root of the multicast delivery tree. This subnetwork contains a known multicast source.

summary - Displays summary information for each entry in the IP multicast routing table.

COMMAND MODE

Privileged Exec

COMMAND USAGE

This command displays information for multicast routing. If no optional parameters are selected, detailed information for each entry in the multicast address table is displayed. If you select a multicast group and source pair, detailed information is displayed only for the specified entry. If the **summary** option is selected, an abbreviated list of information for each entry is displayed on a single line.

EXAMPLE

This example shows detailed multicast information for a specified group/ source pair

```
Console#show ipv6 mroute FF02::0101 FE80::0202

IP Multicast Forwarding is enabled.

IP Multicast Routing Table
Flags: D - Dense, S - Sparse, s - SSM Channel, C - Connected, P - Pruned,
       F - Register flag, R - RPT-bit set, T - SPT-bit set, J - Join SPT
Interface state: F - Forwarding, P - Pruned, L - Local

(FF02::0101, FE80::0202), uptime 00:00:05
Owner: PIM-DM, Flags: D
Incoming Interface: VLAN2, RPF neighbor: FE80::0303
Outgoing Interface List:
VLAN1(F)
Console#
```

Table 280: show ip mroute - display description

Field	Description
Flags	The flags associated with this entry: ◆ D (Dense) - PIM Dense mode in use. ◆ S (Sparse) - PIM Sparse mode in use. ◆ s (SSM) - A multicast group with the range of IP addresses used for PIM-SSM. ◆ C (Connected) - A member of the multicast group is present on this interface. ◆ P (Pruned) - This route has been terminated. ◆ F (Register flag) - This device is registering for a multicast source. ◆ R (RP-bit set) - The (S,G) entry is pointing to the Rendezvous Point (RP), which normally indicates a pruned state along the shared tree for a particular source. ◆ T (SPT-bit set) - Multicast packets have been received from a source on the shortest path tree. ◆ J (Join SPT) - The rate of traffic arriving over the shared tree has exceeded the SPT-threshold for this group. If the SPT flag is set for (*,G) entries, the next (S,G) packet received will cause the router to join the shortest path tree. If the SPT flag is set for (S,G), the router immediately joins the shortest path tree.
Interface state	The multicast state for the displayed interface.
group address	IP multicast group address for a requested service.
source	Subnetwork containing the IP multicast source.
Uptime	The time elapsed since this entry was created.
Owner	The associated multicast protocol (PIM).
Incoming Interface	Interface leading to the upstream neighbor. PIM creates a multicast routing tree based on the unicast routing table. If the related unicast routing table does not exist, PIM will still create a multicast routing entry, but displays “Null” for the upstream interface to indicate that the unicast routing table is not valid. This field may also display “Register” to indicate that a pseudo interface is being used to send or receive PIM-SM register packets.
RPF neighbor	IP address of the multicast router immediately upstream for this group.
Outgoing interface list and flags	The interface(s) on which multicast subscribers have been recorded. The flags associated with each interface indicate: ◆ F (Register flag) - This device is registering for a multicast source. ◆ P (Pruned) - This route has been terminated. ◆ L (Local) - Downstream interface has received IGMP report message from host in this subnet.

This example lists all entries in the multicast table in summary form:

```
Console#show ipv6 mroute summary

IP Multicast Forwarding is disabled

IP Multicast Routing Table (Summary)
Flags:  F - Forwarding, P - Pruned, D - PIM-DM, S - PIM-SM, V - DVMRP,
        M - MLD
Group                          Source                         Interface  Flag
------------------------------ ------------------------------ ---------- ----
                     FF02::0101                     FE80::0101 VLAN 4096   DF
Total Entry is 1
Console#
```

STATIC MULTICAST ROUTING

This section describes commands used to configure static multicast routes on the switch.

Table 281: Static Multicast Routing Commands

Command	Function	Mode
ip igmp snooping vlan mrouter	Adds a multicast router port	GC
show ip igmp snooping mrouter	Shows multicast router ports	PE

ip igmp snooping vlan mrouter

This command statically configures a multicast router port. Use the **no** form to remove the configuration.

SYNTAX

ip igmp snooping vlan *vlan-id* **mrouter** *interface*

no ip igmp snooping vlan *vlan-id* **mrouter** *interface*

vlan-id - VLAN ID (Range: 1-4094)

interface

ethernet *unit/port*

unit - Unit identifier. (Range: 1)

port - Port number. (Range: 1-28)

port-channel *channel-id* (Range: 1-8)

DEFAULT SETTING

No static multicast router ports are configured.

COMMAND MODE

Global Configuration

COMMAND USAGE

Depending on your network connections, IGMP snooping may not always be able to locate the IGMP querier. Therefore, if the IGMP querier is a known multicast router/switch connected over the network to an interface (port or trunk) on your router, you can manually configure that interface to join all the current multicast groups.

EXAMPLE

The following shows how to configure port 11 as a multicast router port within VLAN 1:

```
Console(config)#ip igmp snooping vlan 1 mrouter ethernet 1/11
Console(config)#
```

show ip igmp snooping mrouter

This command displays information on statically configured and dynamically learned multicast router ports.

SYNTAX

show ip igmp snooping mrouter [**vlan** *vlan-id*]

vlan-id - VLAN ID (Range: 1-4094)

DEFAULT SETTING

Displays multicast router ports for all configured VLANs.

COMMAND MODE

Privileged Exec

COMMAND USAGE

Multicast router port types displayed include Static or Dynamic.

EXAMPLE

The following shows that port 11 in VLAN 1 is attached to a multicast router:

```
Console#show ip igmp snooping mrouter vlan 1
 VLAN M'cast Router Ports Type
 ---- ------------------- -------
    1            Eth 1/11  Static
    2            Eth 1/12  Dynamic
Console#
```

PIM MULTICAST ROUTING

This section describes the PIM commands used for IPv4 and IPv6. Note that PIM can run on an IPv4 network and PIM6 on an IPv6 network simultaneously. Also note that Internet Group Management Protocol (IGMP) is used for IPv4 networks and Multicast Listener Discovery (MLD) for IPv6 networks.

Table 282: IPv4 and IPv6 PIM Commands

Command Group	Function
IPv4 PIM Commands	Configures multicast routing for IPv4 PIM.
IPv6 PIM Commands	Co figures multicast routing for IPv6 PIM.

IPV4 PIM COMMANDS

This section describes commands used to configure IPv4 PIM-DM and PIM-SM dynamic multicast routing on the switch.

Table 283: PIM-DM and PIM-SM Multicast Routing Commands

Command	Function	Mode
Shared Mode Commands		
router pim	Enables IPv4 PIM globally for the router	GC
ip pim	Enables PIM-DM or PIM-SM on the specified interface	IC
ip pim hello-holdtime	Sets the time to wait for hello messages from a neighboring PIM router before declaring it dead	IC
ip pim hello-interval	Sets the interval between sending PIM hello messages	IC
ip pim join-prune-holdtime	Configures the hold time for the prune state	IC
ip pim lan-prune-delay	Informs downstream routers of the delay before it prunes a flow after receiving a prune request	IC
ip pim override-interval	Specifies the time it takes a downstream router to respond to a lan-prune-delay message	IC
ip pim propagation-delay	Configures the propagation delay required for a LAN prune delay message to reach downstream routers	IC
ip pim trigger-hello-delay	Configures the trigger hello delay	IC
show ip pim interface	Displays information about interfaces configured for PIM	NE, PE
show ip pim neighbor	Displays information about PIM neighbors	NE, PE
PIM-DM Commands		
ip pim graft-retry-interval	Configures the time to wait for a Graft acknowledgement before resending a Graft message	IC
ip pim max-graft-retries	Configures the maximum number of times to resend a Graft message if it has not been acknowledged	IC
ip pim state-refresh origination-interval	Sets the interval between PIM-DM state refresh control messages	IC

Table 283: PIM-DM and PIM-SM Multicast Routing Commands (Continued)

Command	Function	Mode
PIM-SM Commands		
ip pim bsr-candidate	Configures the switch as a Bootstrap Router (BSR) candidate	GC
ip pim register-rate-limit	Configures the rate at which register messages are sent by the Designated Router (DR)	GC
ip pim register-source	Configure the IP source address of a register message to an address other than the outgoing interface address of the designated router (DR) leading toward the rendezvous point (RP)	GC
ip pim rp-address	Sets a static address for the rendezvous point	GC
ip pim rp-candidate	Configures the switch rendezvous point (RP) candidate	GC
ip pim spt-threshold	Prevents the last-hop PIM router from switching to Shortest Path Source Tree (SPT) mode	GC
ip pim dr-priority	Sets the priority value for a DR candidate	IC
ip pim join-prune-interval	Sets the join/prune timer	IC
clear ip pim bsr rp-set	Clears RP entries learned through the BSR	PE
show ip pim bsr-router	Displays information about the BSR	PE
show ip pim rp mapping	Displays active RPs and associated multicast routing entries	PE
show ip pim rp-hash	Displays the RP used for the specified multicast group	PE

PIM Shared Mode Commands

router pim

This command enables IPv4 Protocol-Independent Multicast routing globally on the router. Use the **no** form to disable PIM multicast routing.

SYNTAX

[**no**] **router pim**

DEFAULT SETTING

Disabled

COMMAND MODE

Global Configuration

COMMAND USAGE

- This command enables PIM-DM and PIM-SM globally for the router. You also need to enable PIM-DM or PIM-SM for each interface that will support multicast routing using the ip pim dense-mode or ip pim sparse mode command, and make any changes necessary to the multicast protocol parameters.

- To use multicast routing, IGMP proxy cannot be enabled on any interface of the device (see the ip igmp proxy command).

EXAMPLE

```
Console(config)#router pim
Console(config)#exit
Console#show ip pim interface
PIM is enabled.
VLAN 1 is up.
 PIM Mode                 :      Dense Mode
 IP Address               :     192.168.0.2
 Hello Interval           :          30 sec
 Hello HoldTime           :         105 sec
 Triggered Hello Delay    :           5 sec
 Join/Prune Holdtime      :         210 sec
 Lan Prune Delay          :        Disabled
 Propagation Delay        :         500  ms
 Override Interval        :        2500  ms
 Graft Retry Interval     :           3 sec
 Max Graft Retries        :           3
 State Refresh Ori Int    :          60 sec

Console#
```

ip pim

This command enables PIM-DM or PIM-SM on the specified interface. Use the **no** form to disable PIM-DM or PIM-SM on this interface.

SYNTAX

[**no**] **ip pim** {**dense-mode** | **sparse-mode**}

dense-mode - Enables PIM Dense Mode.

sparse-mode - Enables PIM Sparse Mode.

DEFAULT SETTING

Disabled

COMMAND MODE

Interface Configuration (VLAN)

COMMAND USAGE

- To fully enable PIM, you need to enable multicast routing globally for the router with the ip multicast-routing command, enable PIM globally for the router with the router pim command, and also enable PIM-DM or PIM-SM for each interface that will participate in multicast routing with this command.

- If you enable PIM on an interface, you should also enable IGMP on that interface. PIM mode selection determines how the switch populates the multicast routing table, and how it forwards packets received from directly connected LAN interfaces. Dense mode interfaces are always added to the multicast routing table. Sparse mode interfaces are added only when periodic join messages are received from downstream routers, or a group member is directly connected to the interface.

- Dense-mode interfaces are subject to multicast flooding by default, and are only removed from the multicast routing table when the router determines that there are no group members or downstream routers, or when a prune message is received from a downstream router.

- Sparse-mode interfaces forward multicast traffic only if a join message is received from a downstream router or if group members are directly connected to the interface. When routers want to receive a multicast flow, they periodically send join messages to the Rendezvous Point (RP), and are subsequently added to the shared path for the specified flow back up to the RP. If routers want to join the source path up through the Shortest Path Source Tree (SPT), they periodically send join messages toward the source. They also send prune messages toward the RP to prune the shared path if they have already connected to the source through the SPT, or if there are no longer any group members connected to the interface.

EXAMPLE

```
Console(config)#interface vlan 1
Console(config-if)#ip pim dense-mode
Console(config-if)#end
Console#show ip pim interface
PIM is enabled.
VLAN 1 is up.
 PIM Mode                :      Dense Mode
 IP Address              :     192.168.0.2
 Hello Interval          :          30 sec
 Hello HoldTime          :         105 sec
 Triggered Hello Delay   :           5 sec
 Join/Prune Holdtime     :         210 sec
 Lan Prune Delay         :        Disabled
 Propagation Delay       :         500  ms
 Override Interval       :        2500  ms
 Graft Retry Interval    :           3 sec
 Max Graft Retries       :           3
 State Refresh Ori Int   :          60 sec

Console#
```

ip pim hello-holdtime

This command configures the interval to wait for hello messages from a neighboring PIM router before declaring it dead. Use the **no** form to restore the default value.

SYNTAX

ip pim hello-holdtime *seconds*

no ip pim hello-interval

seconds - The hold time for PIM hello messages. (Range: 1-65535)

DEFAULT SETTING

105 seconds

COMMAND MODE

Interface Configuration (VLAN)

COMMAND USAGE

The **ip pim hello-holdtime** should be greater than the value of ip pim hello-interval (1931).

EXAMPLE

```
Console(config-if)#ip pim hello-holdtime 210
Console(config-if)#
```

ip pim hello-interval

This command configures the frequency at which PIM hello messages are transmitted. Use the **no** form to restore the default value.

SYNTAX

ip pim hello-interval *seconds*

no pim hello-interval

seconds - Interval between sending PIM hello messages. (Range: 1-65535)

DEFAULT SETTING

30 seconds

COMMAND MODE

Interface Configuration (VLAN)

COMMAND USAGE

Hello messages are sent to neighboring PIM routers from which this device has received probes, and are used to verify whether or not these neighbors are still active members of the multicast tree.

EXAMPLE

```
Console(config-if)#ip pim hello-interval 60
Console(config-if)#
```

ip pim join-prune-holdtime

This command configures the hold time for the prune state. Use the **no** form to restore the default value.

SYNTAX

ip pim join-prune-holdtime *seconds*

no ip pim join-prune-holdtime

seconds - The hold time for the prune state. (Range: 0-65535)

DEFAULT SETTING

210 seconds

COMMAND MODE

Interface Configuration (VLAN)

COMMAND USAGE

The multicast interface that first receives a multicast stream from a particular source forwards this traffic to all other PIM interfaces on the router. If there are no requesting groups on that interface, the leaf node sends a prune message upstream and enters a prune state for this multicast stream. The prune state is maintained until the join-prune-holdtime timer expires or a graft message is received for the forwarding entry.

EXAMPLE

```
Console(config-if)#ip pim join-prune-holdtime 60
Console(config-if)#
```

ip pim lan-prune-delay

This command causes this device to inform downstream routers of how long it will wait before pruning a flow after receiving a prune request. Use the **no** form to disable this feature.

SYNTAX

[**no**] **ip pim lan-prune-delay**

DEFAULT SETTING

Disabled

COMMAND MODE

Interface Configuration (VLAN)

COMMAND USAGE

- When other downstream routers on the same VLAN are notified that this upstream router has received a prune request, they must send a Join to override the prune before the prune delay expires if they want to continue receiving the flow. The message generated by this command effectively prompts any downstream neighbors with hosts receiving the flow to reply with a Join message. If no join messages are received after the prune delay expires, this router will prune the flow.

- Prune delay is the sum of the effective propagation-delay and effective override-interval, where effective propagation-delay is the largest propagation-delay from those advertised by each neighbor (including this switch), and effective override-interval is the largest override-interval from those advertised by each neighbor (including this switch).

EXAMPLE

```
Console(config-if)#ip pim lan-prune-delay
Console(config-if)#
```

RELATED COMMANDS

ip pim override-interval (1933)
ip pim propagation-delay (1934)

ip pim override-interval

This command configures the override interval, or the time it takes a downstream router to respond to a lan-prune-delay message. Use the **no** form to restore the default setting.

SYNTAX

ip pim override-interval *milliseconds*

no ip pim override-interval

milliseconds - The time required for a downstream router to respond to a lan-prune-delay message by sending back a Join message if it wants to continue receiving the flow referenced in the message. (Range: 500-6000 milliseconds)

DEFAULT SETTING

2500 milliseconds

COMMAND MODE

Interface Configuration (VLAN)

COMMAND USAGE

The override interval configured by this command and the propagation delay configured by the ip pim propagation-delay command are used to calculate the LAN prune delay. If a downstream router has group members which want to continue receiving the flow referenced in a LAN prune delay message, then the override interval represents the time required for the downstream router to process the message and then respond by sending a Join message back to the upstream router to ensure that the flow is not terminated.

EXAMPLE

```
Console(config-if)#ip pim override-interval 3500
Console(config-if)#
```

RELATED COMMANDS

ip pim propagation-delay (1934)
ip pim lan-prune-delay (1932)

ip pim propagation-delay

This command configures the propagation delay required for a LAN prune delay message to reach downstream routers. Use the **no** form to restore the default setting.

ip pim propagation-delay *milliseconds*

no ip pim propagation-delay

milliseconds - The time required for a lan-prune-delay message to reach downstream routers attached to the same VLAN interface. (Range: 100-5000 milliseconds)

DEFAULT SETTING

500 milliseconds

COMMAND MODE

Interface Configuration (VLAN)

COMMAND USAGE

The override interval configured by the ip pim override-interval command and the propagation delay configured by this command are used to calculate the LAN prune delay. If a downstream router has group members which want to continue receiving the flow referenced in a LAN prune delay message, then the propagation delay represents the time required for the lan-prune-delay message to be propagated down from the upstream router to all downstream routers attached to the same VLAN interface.

EXAMPLE

```
Console(config-if)#ip pim propagation-delay 600
Console(config-if)#
```

RELATED COMMANDS

ip pim override-interval (1933)
ip pim lan-prune-delay (1932)

ip pim trigger-hello-delay

This command configures the maximum time before transmitting a triggered PIM Hello message after the router is rebooted or PIM is enabled on an interface. Use the **no** form to restore the default value.

SYNTAX

ip pim trigger-hello-delay *seconds*

no ip pim trigger-hello-delay

seconds - The maximum time before sending a triggered PIM Hello message. (Range: 0-5 seconds)

DEFAULT SETTING

5 seconds

COMMAND MODE

Interface Configuration (VLAN)

COMMAND USAGE

- When a router first starts or PIM is enabled on an interface, the hello delay is set to random value between 0 and the trigger-hello-delay. This prevents synchronization of Hello messages on multi-access links if multiple routers are powered on simultaneously.

- Also, if a Hello message is received from a new neighbor, the receiving router will send its own Hello message after a random delay between 0 and the trigger-hello-delay.

EXAMPLE

```
Console(config-if)#ip pim trigger-hello-delay 3
Console(config-if)#
```

show ip pim interface

This command displays information about interfaces configured for PIM.

SYNTAX

show ip pim interface [**vlan** *vlan-id*]

vlan-id - VLAN ID (Range: 1-4094)

COMMAND MODE

Normal Exec, Privileged Exec

COMMAND USAGE

This command displays the PIM settings for the specified interface as described in the preceding pages. It also shows the address of the designated PIM router and the number of neighboring PIM routers.

EXAMPLE

```
Console#show ip pim interface vlan 1
PIM is enabled.
VLAN 1 is up.
 PIM Mode                 :      Dense Mode
 IP Address               :     192.168.0.2
 Hello Interval           :          30 sec
 Hello HoldTime           :         105 sec
 Triggered Hello Delay    :           5 sec
 Join/Prune Holdtime      :         210 sec
 Lan Prune Delay          :        Disabled
 Propagation Delay        :         500  ms
 Override Interval        :        2500  ms
 Graft Retry Interval     :           3 sec
 Max Graft Retries        :           3
 State Refresh Ori Int    :          60 sec

Console#
```

show ip pim neighbor

This command displays information about PIM neighbors.

SYNTAX

show ip pim neighbor [**interface vlan** *vlan-id*]

vlan-id - VLAN ID (Range: 1-4094)

DEFAULT SETTING

Displays information for all known PIM neighbors.

COMMAND MODE

Normal Exec, Privileged Exec

EXAMPLE

```
Console#show ip pim neighbor
Neighbor Address VLAN Interface Uptime (sec.) Expiration Time (sec)
---------------- -------------- ------------- ---------------------
192.168.0.3/32   1              00:00:21      00:01:30
Console#
```

Table 284: show ip pim neighbor - display description

Field	Description
`Neighbor Address`	IP address of the next-hop router.
`VLAN Interface`	Interface number that is attached to this neighbor.
`Uptime`	The duration this entry has been active.
`Expiration Time`	The time before this entry will be removed.

PIM-DM Commands

ip pim graft-retry-interval

This command configures the time to wait for a Graft acknowledgement before resending a Graft. Use the **no** form to restore the default value.

SYNTAX

ip pim graft-retry-interval *seconds*

no ip pim graft-retry-interval

seconds - The time before resending a Graft.
(Range: 1-10 seconds)

DEFAULT SETTING

3 seconds

COMMAND MODE

Interface Configuration (VLAN)

COMMAND USAGE

A graft message is sent by a router to cancel a prune state. When a router receives a graft message, it must respond with an graft acknowledgement message. If this acknowledgement message is lost, the router that sent the graft message will resend it a number of times (as defined by the ip pim max-graft-retries command).

EXAMPLE

```
Console(config-if)#ip pim graft-retry-interval 9
Console(config-if)#
```

ip pim max-graft-retries

This command configures the maximum number of times to resend a Graft message if it has not been acknowledged. Use the **no** form to restore the default value.

SYNTAX

ip pim max-graft-retries *retries*

no ip pim max-graft-retries

retries - The maximum number of times to resend a Graft. (Range: 1-10)

DEFAULT SETTING

3

COMMAND MODE

Interface Configuration (VLAN)

EXAMPLE

```
Console(config-if)#ip pim max-graft-retries 5
Console(config-if)#
```

ip pim state-refresh origination-interval

This command sets the interval between sending PIM-DM state refresh control messages. Use the **no** form to restore the default value.

SYNTAX

ip pim state-refresh origination-interval *seconds*

no ip pim max-graft-retries

seconds - The interval between sending PIM-DM state refresh control messages. (Range: 1-100 seconds)

DEFAULT SETTING

60 seconds

COMMAND MODE

Interface Configuration (VLAN)

COMMAND USAGE

- The pruned state times out approximately every three minutes and the entire PIM-DM network is reflooded with multicast packets and prune messages. The state refresh feature keeps the pruned state from timing out by periodically forwarding a control message down the distribution tree, refreshing the prune state on the outgoing interfaces of each router in the tree. This also enables PIM routers to recognize topology changes (sources joining or leaving a multicast group) before the default three-minute state timeout expires.

- This command is only effectively for interfaces of first hop, PIM-DM routers that are directly connected to the sources of multicast groups.

EXAMPLE

```
Console(config-if)#ip pim state-refresh origination-interval 30
Console(config-if)#
```

PIM-SM Commands

ip pim bsr-candidate

This command configures the switch as a Bootstrap Router (BSR) candidate. Use the **no** form to restore the default value.

SYNTAX

ip pim bsr-candidate interface vlan *vlan-id*
[**hash** *hash-mask-length*] [**priority** *priority*]

no ip pim bsr-candidate

vlan-id - VLAN ID (Range: 1-4094)

hash-mask-length - Hash mask length (in bits) used for RP selection (see ip pim rp-candidate and ip pim rp-address). The portion of the hash specified by the mask length is ANDed with the group address. Therefore, when the hash function is executed on any BSR, all groups with the same seed hash will be mapped to the same RP. If the mask length is less than 32, then only the first portion of the hash is used, and a single RP will be defined for multiple groups. (Range: 0-32 bits)

priority - Priority used by the candidate bootstrap router in the election process. The BSR candidate with the largest priority is preferred. If the priority values are the same, the candidate with the larger IP address is elected to be the BSR. Setting the priority to zero means that this router is not eligible to server as the BSR. At least one router in the PIM-SM domain must be set to a value greater than zero. (Range: 0-255)

DEFAULT SETTING

Hash Mask Length: 10
Priority: 0

COMMAND MODE

Global Configuration

COMMAND USAGE

- When the **ip pim bsr-candidate** command is entered, the router starts sending bootstrap messages to all of its PIM-SM neighbors. The IP address of the designated VLAN is sent as the candidate's BSR address. Each neighbor receiving the bootstrap message compares the BSR address with the address from previous messages. If the current address is the same or a higher address, it accepts the bootstrap message and forwards it. Otherwise, it drops the message.

- This router will continue to be the BSR until it receives a bootstrap message from another candidate with a higher priority (or a higher IP address if the priorities are the same).

- To improve failover recovery, it is advisable to select at least two core routers in diverse locations, each to serve as both a candidate BSR and candidate RP. It is also preferable to set up one of these routers as both the primary BSR and RP.

EXAMPLE

The following example configures the router to start sending bootstrap messages out of the interface for VLAN 1 to all of its PIM-SM neighbors.

```
Console(config)#ip pim bsr-candidate interface vlan 1 hash 20 priority 200
Console(config)#exit
Console#show ip pim bsr-router
PIMv2 Bootstrap information
BSR Address      : 192.168.0.2/32
Uptime           : 00:00:08
BSR Priority     : 200
Hash Mask Length : 20
Expire           : 00:00:57
Role             : Candidate BSR
State            : Elected BSR
Console#
```

ip pim register-rate-limit

This command configures the rate at which register messages are sent by the Designated Router (DR) for each (source, group) entry. Use the **no** form to restore the default value.

SYNTAX

ip pim register-rate-limit *rate*

no ip pim register-rate-limit

rate - The maximum number of register packets per second. (Range: 1-65535: Default: 0, which means no limit)

DEFAULT SETTING

0

COMMAND MODE

Global Configuration

COMMAND USAGE

This command can be used to relieve the load on the Designated Router (DR) and RP. However, because register messages exceeding the limit are dropped, some receivers may experience data packet loss within the first few seconds in which register messages are sent from bursty sources.

EXAMPLE

This example sets the register rate limit to 500 pps.

```
Console(config)#ip pim register-rate-limit 500
Console(config)#
```

ip pim register-source

This command configures the IP source address of a register message to an address other than the outgoing interface address of the designated router (DR) that leads back toward the rendezvous point (RP). Use the **no** form to restore the default setting.

SYNTAX

ip pim register-source interface vlan *vlan-id*

no ip pim register-source

vlan-id - VLAN ID (Range: 1-4094)

DEFAULT SETTING

The IP address of the DR's outgoing interface that leads back to the RP

COMMAND MODE

Global Configuration

COMMAND USAGE

When the source address of a register message is filtered by intermediate network devices, or is not a uniquely routed address to which the RP can send packets, the replies sent from the RP to the source address will fail to reach the DR, resulting in PIM-SM protocol failures. This command can be used to overcome this type of problem by manually configuring the source address of register messages to an interface that leads back to the RP.

EXAMPLE

This example sets the register rate limit to 500 pps.

```
Console(config)#ip pim register-source interface vlan 1
Console(config)#
```

ip pim rp-address

This command sets a static address for the Rendezvous Point (RP) for a particular multicast group. Use the **no** form to remove an RP address or an RP address for a specific group.

SYNTAX

[**no**] **ip pim rp-address** *rp-address* [**group-prefix** *group-address mask*]

rp-address - Static IP address of the router that will be an RP for the specified multicast group(s).

group-address - An IP multicast group address. If a group address is not specified, the RP is used for all multicast groups.

mask - Subnet mask that is used for the group address.

DEFAULT SETTING

None

COMMAND MODE

Global Configuration

COMMAND USAGE

- The router specified by this command will act as an RP for all multicast groups in the local PIM-SM domain if no groups are specified. A static RP can either be configured for the whole multicast group range 224.0.0.0/4, or for specific group ranges.

- Using this command to configure multiple static RPs with the same RP address is not allowed. If an IP address is specified that was previously used for an RP, then the older entry is replaced.

- Multiple RPs can be defined for different groups or group ranges. If a group is matched by more than one entry, the router will use the RP associated with the longer group prefix length. If the prefix lengths are the same, then the static RP with the highest IP address is chosen.

- Static definitions for RP addresses may be used together with RP addresses dynamically learned through the bootstrap router (BSR). If an RP address learned by the BSR and one statically configured using this command are both available for a group range, the RP address learned by the BSR is chosen over the one statically configured with this command.

- All routers within the same PIM-SM domain must be configured with the same RP(s). Selecting an RP through the dynamic election process is therefore preferable for most situations. Using the dynamic RP election process also allows a backup RP to automatically take over if the active RP router becomes unavailable.

- If the **no** form of this command is used without specifying a multicast group, the default 224.0.0.0 (with the mask 240.0.0.0) is removed. In other words, all multicast groups are removed.

EXAMPLE

In the following example, the first PIM-SM command just specifies the RP address 192.168.1.1 to indicate that it will be used to service all multicast groups. The second PIM-SM command includes the multicast groups to be serviced by the RP.

```
Console(config)#ip pim rp-address 192.168.1.1
Console(config)#ip pim rp-address 192.168.2.1 group-prefix 224.9.0.0
  255.255.0.0
Console(config)#end
Console#show ip pim rp mapping
PIM Group-to-RP Mappings
Groups            : 224.0.0.0/4
RP address        : 192.168.1.1/32
Info source       : static
Uptime            : 00:00:33
Expire            : Never
Groups            : 224.9.0.0/16
RP address        : 192.168.2.1/32
Info source       : static
Uptime            : 00:00:21
Expire            : Never
Console#
```

ip pim rp-candidate

This command configures the router to advertise itself as a Rendezvous Point (RP) candidate to the bootstrap router (BSR). Use the **no** form to remove this router as an RP candidate.

SYNTAX

ip pim rp-candidate interface vlan *vlan-id*
[**group-prefix** *group-address mask*]
[**interval** *seconds*] [**priority** *value*]

no ip pim rp-candidate interface vlan *vlan-id*

vlan-id - VLAN ID (Range: 1-4094)

group-address - An IP multicast group address. If a group address is not specified, the RP is advertised for all multicast groups.

mask - Subnet mask that is used for the group address.

seconds - The interval at which this device advertises itself as an RP candidate. (Range: 60-16383 seconds)

value - Priority used by the candidate RP in the election process. The RP candidate with the largest priority is preferred. If the priority values are the same, the candidate with the larger IP address is elected to be the RP. Setting the priority to zero means that this router is not eligible to server as the RP. (Range: 0-255)

DEFAULT SETTING

Address: 224.0.0.0/4, or the entire IPv4 multicast group family
Interval: 60 seconds
Priority: 0

Command Mode

Global Configuration

Command Usage

- When the **ip pim rp-candidate** command is entered, the router periodically sends PIMv2 messages to the BSR advertising itself as a candidate RP for the specified group addresses. The IP address of the designated VLAN is sent as the candidate's RP address. The BSR places information about all of the candidate RPs in subsequent bootstrap messages. The BSR uses the RP-election hash algorithm to select an active RP for each group range. The election process is performed by the BSR only for its own use. Each PIM-SM router that receives the list of RP candidates from the BSR also elects an active RP for each group range using the same election process.

- The election process for each group is based on the following criteria:
  - Find all RPs with the most specific group range.
  - Select those with the highest priority (lowest priority value).
  - Compute a hash value based on the group address, RP address, priority, and hash mask included in the bootstrap messages.
  - If there is a tie, use the candidate RP with the highest IP address.

- This distributed election process provides faster convergence and minimal disruption when an RP fails. It also serves to provide load balancing by distributing groups across multiple RPs. Moreover, when an RP fails, the responsible RPs are re-elected on each router, and the groups automatically distributed to the remaining RPs.

- To improve failover recovery, it is advisable to select at least two core routers in diverse locations, each to serve as both a candidate BSR and candidate RP. It is also preferable to set up one of these routers as both the primary BSR and RP.

Example

The following example configures the router to start advertising itself to the BSR as a candidate RP for the indicated multicast groups.

```
Console(config)#ip pim rp-candidate interface vlan 1 group-prefix 224.0.0.0
  255.0.0.0
Console(config)#end
Console#show ip pim rp mapping
PIM Group-to-RP Mappings
Groups            : 224.0.0.0/8
RP address        : 192.168.0.2/32
Info source       : 192.168.0.2/32, via bootstrap, priority: 0
Uptime            : 00:00:51
Expire            : 00:01:39
Console#
```

ip pim spt-threshold

This command prevents the last-hop PIM router from switching to Shortest Path Source Tree (SPT) mode. Use the **no** form to allow the router to switch over to SPT mode.

SYNTAX

ip pim spt-threshold infinity [**group-prefix** *group-address mask*]

no ip pim spt-threshold infinity

group-address - An IP multicast group address. If a group address is not specified, the command applies to all multicast groups.

mask - Subnet mask that is used for the group address.

DEFAULT SETTING

The last-hop PIM router joins the shortest path tree immediately after the first packet arrives from a new source.

COMMAND MODE

Global Configuration

COMMAND USAGE

- The default path for packets from a multicast source to a receiver is through the RP. However, the path through the RP is not always the shortest path. Therefore, the router uses the RP to forward only the first packet from a new multicast group to its receivers. Afterwards, it calculates the shortest path tree (SPT) directly between the receiver and source, and then uses the SPT to send all subsequent packets from the source to the receiver instead of using the shared tree. Note that when the SPT threshold is not set by this command, the PIM leaf router will join the shortest path tree immediately after receiving the first packet from a new source.

- This command forces the router to use the shared tree for all multicast groups, or just for the specified multicast groups.

- Only one entry is allowed for this command.

EXAMPLE

This example prevents the switch from using the SPT for multicast groups 224.1.0.0~224.1.255.255.

```
Console(config-if)#ip pim sparse-mode
Console(config-if)#exit
Console(config)#ip multicast-routing
Console(config)#router pim
Console(config)#ip pim spt-threshold infinity group-prefix 224.1.0.0
  0.0.255.255
Console#
```

ip pim dr-priority

This command sets the priority value for a Designated Router (DR) candidate. Use the **no** form to restore the default setting.

SYNTAX

ip pim dr-priority *priority-value*

no ip pim dr-priority

priority-value - Priority advertised by a router when bidding to become the DR. (Range: 0-4294967294)

DEFAULT SETTING

1

COMMAND MODE

Interface Configuration (VLAN)

COMMAND USAGE

- More than one PIM-SM router may be connected to an Ethernet or other shared-media LAN. If multicast hosts are directly connected to the LAN, then only one of these routers is elected as the DR, and acts on behalf of these hosts, sending periodic Join/Prune messages toward a group-specific RP for each group. A single DR is elected per interface (LAN or otherwise) using a simple election process.

- The router with the highest priority configured on an interface is elected as the DR. If more than one router attached to this interface uses the same priority, then the router with the highest IP address is elected to serve as the DR.

- If a router does not advertise a priority in its hello messages, it is assumed to have the highest priority and is elected as the DR. If more than one router is not advertising its priority, then the router with the highest IP address is elected to serve as the DR.

EXAMPLE

This example sets the priority used in the bidding process for the DR.

```
Console(config)#interface vlan 1
Console(config-if)#ip pim dr-priority 20
Console(config-if)#end
Console#show ip pim interface
PIM is enabled.
VLAN 1 is up.
 PIM Mode                 :     Sparse Mode
 IP Address               :     192.168.0.2
 Hello Interval           :          30 sec
 Hello HoldTime           :         105 sec
 Triggered Hello Delay    :           5 sec
 Join/Prune Holdtime      :         210 sec
 Lan Prune Delay          :        Disabled
 Propagation Delay        :         500  ms
 Override Interval        :        2500  ms
 DR Priority              :          20
 Join/Prune Interval      :          60 sec
```

```
Console#
```

ip pim join-prune-interval

This command sets the join/prune timer. Use the **no** form to restore the default setting.

SYNTAX

ip pim join-prune-interval *seconds*

no ip pim join-prune-interval

seconds - The interval at which join/prune messages are sent. (Range: 1-65535 seconds)

DEFAULT SETTING

60 seconds

COMMAND MODE

Interface Configuration (VLAN)

COMMAND USAGE

- By default, the switch sends join/prune messages every 210 seconds to inform other PIM-SM routers about clients who want to join or leave a multicast group.

- Use the same join/prune message interval on all the PIM-SM routers in the same PIM-SM domain, otherwise the routing protocol's performance will be adversely affected.

- The multicast interface that first receives a multicast stream from a particular source forwards this traffic only to those interfaces on the router that have requested to join this group. When there are no longer any requesting groups on that interface, the leaf node sends a prune message upstream and enters a prune state for this multicast stream. The protocol maintains both the current join state and the pending Reverse Path Tree (RPT) prune state for this (source, group) pair until the join/prune-interval timer expires.

EXAMPLE

This example sets the priority used in the bidding process for the DR.

```
Console(config)#interface vlan 1
Console(config-if)#ip pim join-prune-interval 210
Console#show ip pim interface
PIM is enabled.
VLAN 1 is up.
 PIM Mode                 :     Sparse Mode
 IP Address               :     192.168.0.2
 Hello Interval           :          30 sec
 Hello HoldTime           :         105 sec
 Triggered Hello Delay    :           5 sec
 Join/Prune Holdtime      :         210 sec
 Lan Prune Delay          :        Disabled
 Propagation Delay      :         500  ms
 Override Interval      :        2500  ms
 DR Priority            :          20
 Join/Prune Interval    :          80  sec

Console#
```

clear ip pim bsr rp-set

This command clears multicast group to RP mapping entries learned through the PIMv2 bootstrap router (BSR).

COMMAND MODE

Privileged Exec

COMMAND USAGE

- This command can be used to update entries in the static multicast forwarding table immediately after making configuration changes to the RP.
- Use the show ip pim rp mapping command to display active RPs that are cached with associated multicast routing entries.

EXAMPLE

This example clears the RP map.

```
Console#clear ip pim bsr rp-set
Console#show ip pim rp mapping
PIM Group-to-RP Mappings
Console#
```

show ip pim bsr-router

This command displays information about the bootstrap router (BSR).

COMMAND MODE

Privileged Exec

COMMAND USAGE

This command displays information about the elected BSR.

EXAMPLE

This example displays information about the BSR.

```
Console#show ip pim bsr-router
PIMv2 Bootstrap information
BSR Address      : 192.168.0.2/32
Uptime           : 01:01:23
BSR Priority     : 200
Hash Mask Length : 20
Expire           : 00:00:42
Role             : Candidate BSR
```

```
State              : Elected BSR
Console#
```

Table 285: show ip pim bsr-router - display description

Field	Description
`BSR Address`	IP address of interface configured as the BSR.
`Uptime`	The time this BSR has been up and running.
`BSR Priority`	Priority assigned to this interface for use in the BSR election process.
`Hash Mask Length`	The number of significant bits used in the multicast group comparison mask. This mask determines the multicast group for which this router can be a BSR.
`Expire`	The time before this entry will be removed.
`Role`	Candidate BSR or Non-candidate BSR.
`State`	Operation state of BSR includes: ◆ No information – No information stored for this device. ◆ Accept Any – The router does not know of an active BSR, and will accept the first bootstrap message it sees as giving the new BSR's identity and the RP-set. ◆ Accept Preferred – The router knows the identity of the current BSR, and is using the RP-set provided by that BSR. Only bootstrap messages from that BSR or from a C-BSR with higher weight than the current BSR will be accepted. ◆ Candidate BSR – Bidding in election process. ◆ Pending-BSR – The router is a candidate to be the BSR for the RP-set. Currently, no other router is the preferred BSR, but this router is not yet the elected BSR. ◆ Elected BSR – elected to serve as BSR

show ip pim rp mapping

This command displays active RPs and associated multicast routing entries.

COMMAND MODE

Privileged Exec

EXAMPLE

This example displays the RP map.

```
Console#show ip pim rp mapping
PIM Group-to-RP Mappings
Groups             : 224.0.0.0/8
RP address         : 192.168.0.2/32
Info source        : 192.168.0.2/32, via bootstrap, priority: 0
Uptime             : 00:31:09
Expire             : 00:02:21
Console#
```

Table 286: show ip pim rp mapping - display description

Field	Description
`Groups`	The multicast group address, mask length managed by the RP.
`RP address`	IP address of the RP used for the listed multicast group
`Info source`	RP that advertised the mapping, how the RP was selected (Static or Bootstrap), and the priority used in the bidding process
`Uptime`	The time this RP has been up and running
`Expire`	The time before this entry will be removed

show ip pim rp-hash

This command displays the RP used for the specified multicast group, and the RP that advertised the mapping.

Syntax

show ip pim rp-hash *group-address*

group-address - An IP multicast group address.

Command Mode

Privileged Exec

Example

This example displays the RP used for the specified group.

```
Console#show ip pim rp-hash 224.0.1.3
RP address          : 192.168.0.2/32
Info source         : 192.168.0.2/32, via (null)
Console#
```

Table 287: show ip pim rp-hash - display description

Field	Description
`RP address`	IP address of the RP used for the specified multicast group
`Info source`	RP that advertised the mapping, and how the RP was selected

IPV6 PIM COMMANDS

This section describes commands used to configure IPv6 PIM dynamic multicast routing on the switch.

Table 288: PIM-DM and PIM-SM Multicast Routing Commands

Command	Function	Mode
Shared Mode Commands		
router pim6	Enables IPv6 PIM globally for the router	GC
ipv6 pim	Enables PIM-DM or PIM-SM on the specified interface	IC
ipv6 pim hello-holdtime	Sets the time to wait for hello messages from a neighboring PIM router before declaring it dead	IC
ipv6 pim hello-interval	Sets the interval between sending PIM hello messages	IC
ipv6 pim join-prune-holdtime	Configures the hold time for the prune state	IC
ipv6 pim lan-prune-delay	Informs downstream routers of the delay before it prunes a flow after receiving a prune request	IC
ipv6 pim override-interval	Specifies the time it takes a downstream router to respond to a lan-prune-delay message	IC
ipv6 pim propagation-delay	Configures the propagation delay required for a LAN prune delay message to reach downstream routers	IC
ipv6 pim trigger-hello-delay	Configures the trigger hello delay	IC
show ipv6 pim interface	Displays information about interfaces configured for PIM	NE, PE
show ipv6 pim neighbor	Displays information about PIM neighbors	NE, PE
PIM-DM Commands		
ipv6 pim graft-retry-interval	Configures the time to wait for a Graft acknowledgement before resending a Graft message	IC
ipv6 pim max-graft-retries	Configures the maximum number of times to resend a Graft message if it has not been acknowledged	IC
ipv6 pim state-refresh origination-interval	Sets the interval between PIM-DM state refresh control messages	IC
PIM-SM Commands		
ipv6 pim bsr-candidate	Configures the switch as a Bootstrap Router (BSR) candidate	GC
ipv6 pim register-rate-limit	Configures the rate at which register messages are sent by the Designated Router (DR)	GC
ipv6 pim register-source	Configure the IP source address of a register message to an address other than the outgoing interface address of the designated router (DR) leading toward the rendezvous point (RP)	GC
ipv6 pim rp-address	Sets a static address for the rendezvous point	GC
ipv6 pim rp-candidate	Configures the switch rendezvous point (RP) candidate	GC
ipv6 pim spt-threshold	Prevents the last-hop PIM router from switching to Shortest Path Source Tree (SPT) mode	GC
ipv6 pim dr-priority	Sets the priority value for a DR candidate	IC
ipv6 pim join-prune-interval	Sets the join/prune timer	IC
clear ipv6 pim bsr rp-set	Clears RP entries learned through the BSR	PE

Table 288: PIM-DM and PIM-SM Multicast Routing Commands (Continued)

Command	Function	Mode
show ipv6 pim bsr-router	Displays information about the BSR	PE
show ipv6 pim rp mapping	Displays active RPs and associated multicast routing entries	PE
show ipv6 pim rp-hash	Displays the RP used for the specified multicast group	PE

PIM6 Shared Mode Commands

router pim6

This command enables IPv6 Protocol-Independent Multicast routing globally on the router. Use the **no** form to disable PIM multicast routing.

SYNTAX

[**no**] **router pim6**

DEFAULT SETTING

Disabled

COMMAND MODE

Global Configuration

COMMAND USAGE

- This command enables PIM-DM and PIM-SM for IPv6 globally for the router. You also need to enable PIM-DM and PIM-SM for each interface that will support multicast routing using the ipv6 pim command, and make any changes necessary to the multicast protocol parameters.
- To use PIMv6, IPv6 multicast routing must be enabled on the switch using the ipv6 multicast-routing command.
- To use IPv6 multicast routing, MLD proxy cannot be enabled on any interface of the device (see the ipv6 mld proxy command).

EXAMPLE

```
Console(config)#router pim6
Console(config)#
```

ipv6 pim

This command enables IPv6 PIM-DM or PIM-SM on the specified interface. Use the **no** form to disable IPv6 PIM-DM or PIM-SM on this interface.

SYNTAX

[**no**] **ipv6 pim** {**dense-mode** | **sparse-mode**}

dense-mode - Enables PIM Dense Mode.

sparse-mode - Enables PIM Sparse Mode.

DEFAULT SETTING

Disabled

COMMAND MODE

Interface Configuration (VLAN)

COMMAND USAGE

- To fully enable PIM, you need to enable multicast routing globally for the router with the ipv6 multicast-routing command, enable PIM globally for the router with the router pim6 command, and also enable PIM-DM or PIM-SM for each interface that will participate in multicast routing with this command.

- If you enable PIM on an interface, you should also enable MLD (see "MLD (Layer 3)" on page 1525) on that interface. PIM mode selection determines how the switch populates the multicast routing table, and how it forwards packets received from directly connected LAN interfaces. Dense mode interfaces are always added to the multicast routing table. Sparse mode interfaces are added only when periodic join messages are received from downstream routers, or a group member is directly connected to the interface.

- Dense-mode interfaces are subject to multicast flooding by default, and are only removed from the multicast routing table when the router determines that there are no group members or downstream routers, or when a prune message is received from a downstream router.

- Sparse-mode interfaces forward multicast traffic only if a join message is received from a downstream router or if group members are directly connected to the interface. When routers want to receive a multicast flow, they periodically send join messages to the Rendezvous Point (RP), and are subsequently added to the shared path for the specified flow back up to the RP. If routers want to join the source path up through the Shortest Path Source Tree (SPT), they periodically send join messages toward the source. They also send prune messages toward the RP to prune the shared path if they have already connected to the source through the SPT, or if there are no longer any group members connected to the interface.

EXAMPLE

```
Console(config)#interface vlan 1
Console(config-if)#ipv6 pim dense-mode
Console(config-if)#end
Console#show ipv6 pim interface
PIM is enabled.
VLAN 1 is up.
 PIM Mode                : Dense Mode
 IPv6 Address            : None
 Hello Interval          : 30 sec
 Hello HoldTime          : 105 sec
 Triggered Hello Delay   : 5 sec
 Join/Prune Holdtime     : 210 sec
 Lan Prune Delay         : Disabled
 Propagation Delay       : 500  ms
 Override Interval       : 2500  ms
```

```
  Graft Retry Interval    : 3 sec
  Max Graft Retries       : 3
  State Refresh Ori Int   : 60 sec

Console#
```

ipv6 pim hello-holdtime

This command configures the interval to wait for hello messages from a neighboring PIM router before declaring it dead. Use the **no** form to restore the default value.

SYNTAX

ipv6 pim hello-holdtime *seconds*

no ipv6 pim hello-interval

seconds - The hold time for PIM hello messages. (Range: 1-65535)

DEFAULT SETTING

105 seconds

COMMAND MODE

Interface Configuration (VLAN)

COMMAND USAGE

The **ip pim hello-holdtime** should be greater than the value of ipv6 pim hello-interval.

EXAMPLE

```
Console(config-if)#ipv6 pim hello-holdtime 210
Console(config-if)#
```

ipv6 pim hello-interval

This command configures the frequency at which PIM hello messages are transmitted. Use the **no** form to restore the default value.

SYNTAX

ipv6 pim hello-interval *seconds*

no pimv6 hello-interval

seconds - Interval between sending PIM hello messages. (Range: 1-65535)

DEFAULT SETTING

30 seconds

COMMAND MODE

Interface Configuration (VLAN)

COMMAND USAGE

Hello messages are sent to neighboring PIM routers from which this device has received probes, and are used to verify whether or not these neighbors are still active members of the multicast tree.

EXAMPLE

```
Console(config-if)#ipv6 pim hello-interval 60
Console(config-if)#
```

ipv6 pim join-prune-holdtime

This command configures the hold time for the prune state. Use the **no** form to restore the default value.

SYNTAX

ipv6 pim join-prune-holdtime *seconds*

no ipv6 pim join-prune-holdtime

seconds - The hold time for the prune state. (Range: 0-65535)

DEFAULT SETTING

210 seconds

COMMAND MODE

Interface Configuration (VLAN)

COMMAND USAGE

The multicast interface that first receives a multicast stream from a particular source forwards this traffic to all other PIM interfaces on the router. If there are no requesting groups on that interface, the leaf node sends a prune message upstream and enters a prune state for this multicast stream. The prune state is maintained until the join-prune-holdtime timer expires or a graft message is received for the forwarding entry.

EXAMPLE

```
Console(config-if)#ipv6 pim join-prune-holdtime 60
Console(config-if)#
```

ipv6 pim lan-prune-delay

This command causes this device to inform downstream routers of how long it will wait before pruning a flow after receiving a prune request. Use the **no** form to disable this feature.

SYNTAX

[**no**] **ipv6 pim lan-prune-delay**

DEFAULT SETTING

Disabled

COMMAND MODE

Interface Configuration (VLAN)

COMMAND USAGE

- When other downstream routers on the same VLAN are notified that this upstream router has received a prune request, they must send a Join to override the prune before the prune delay expires if they want to continue receiving the flow. The message generated by this command effectively prompts any downstream neighbors with hosts receiving the flow to reply with a Join message. If no join messages are received after the prune delay expires, this router will prune the flow.

- Prune delay is the sum of the effective propagation-delay and effective override-interval, where effective propagation-delay is the largest propagation-delay from those advertised by each neighbor (including this switch), and effective override-interval is the largest override-interval from those advertised by each neighbor (including this switch).

EXAMPLE

```
Console(config-if)#ipv6 pim lan-prune-delay
Console(config-if)#
```

RELATED COMMANDS

ipv6 pim override-interval (1955)
ipv6 pim propagation-delay (1956)

ipv6 pim override-interval

This command configures the override interval, or the time it takes a downstream router to respond to a lan-prune-delay message. Use the **no** form to restore the default setting.

SYNTAX

ipv6 pim override-interval *milliseconds*

no ipv6 pim override-interval

milliseconds - The time required for a downstream router to respond to a lan-prune-delay message by sending back a Join message if it wants to continue receiving the flow referenced in the message. (Range: 500-6000 milliseconds)

DEFAULT SETTING

2500 milliseconds

COMMAND MODE

Interface Configuration (VLAN)

COMMAND USAGE

The override interval configured by this command and the propagation delay configured by the ipv6 pim propagation-delay command are used to calculate the LAN prune delay. If a downstream router has group members which want to continue receiving the flow referenced in a LAN prune delay message, then the override interval represents the time required for the downstream router to process the message and then respond by sending a Join message back to the upstream router to ensure that the flow is not terminated.

EXAMPLE

```
Console(config-if)#ipv6 pim override-interval 3500
Console(config-if)#
```

RELATED COMMANDS

ipv6 pim propagation-delay (1956)
ipv6 pim lan-prune-delay (1954)

ipv6 pim propagation-delay

This command configures the propagation delay required for a LAN prune delay message to reach downstream routers. Use the **no** form to restore the default setting.

ipv6 pim propagation-delay *milliseconds*

no ipv6 pim propagation-delay

milliseconds - The time required for a lan-prune-delay message to reach downstream routers attached to the same VLAN interface. (Range: 100-5000 milliseconds)

DEFAULT SETTING

500 milliseconds

COMMAND MODE

Interface Configuration (VLAN)

COMMAND USAGE

The override interval configured by the ipv6 pim override-interval command and the propagation delay configured by this command are used to calculate the LAN prune delay. If a downstream router has group members which want to continue receiving the flow referenced in a LAN prune delay message, then the propagation delay represents the time required for the lan-prune-delay message to be propagated down from the upstream router to all downstream routers attached to the same VLAN interface.

EXAMPLE

```
Console(config-if)#ipv6 pim propagation-delay 600
Console(config-if)#
```

RELATED COMMANDS

ipv6 pim override-interval (1955)
ipv6 pim lan-prune-delay (1954)

ipv6 pim trigger-hello-delay

This command configures the maximum time before transmitting a triggered PIM Hello message after the router is rebooted or PIM is enabled on an interface. Use the **no** form to restore the default value.

SYNTAX

ipv6 pim trigger-hello-delay *seconds*

no ipv6 pim trigger-hello-delay

seconds - The maximum time before sending a triggered PIM Hello message. (Range: 0-5)

DEFAULT SETTING

5 seconds

COMMAND MODE

Interface Configuration (VLAN)

COMMAND USAGE

- When a router first starts or PIM is enabled on an interface, the hello delay is set to random value between 0 and the trigger-hello-delay. This prevents synchronization of Hello messages on multi-access links if multiple routers are powered on simultaneously.

- Also, if a Hello message is received from a new neighbor, the receiving router will send its own Hello message after a random delay between 0 and the trigger-hello-delay.

EXAMPLE

```
Console(config-if)#ipv6 pim trigger-hello-delay 3
Console(config-if)#
```

show ipv6 pim interface

This command displays information about interfaces configured for PIM.

SYNTAX

show ipv6 pim [**interface vlan** *vlan-id*]

vlan-id - VLAN ID (Range: 1-4094)

COMMAND MODE

Normal Exec, Privileged Exec

COMMAND USAGE

This command displays the PIM settings for the specified interface as described in the preceding pages. It also shows the address of the designated PIM router and the number of neighboring PIM routers.

EXAMPLE

```
Console#show ip pim interface vlan 1
PIM is enabled.
VLAN 1 is up.
 PIM Mode                : Dense Mode
 IPv6 Address            : None
 Hello Interval          : 30 sec
 Hello HoldTime          : 105 sec
 Triggered Hello Delay   : 5 sec
 Join/Prune Holdtime     : 210 sec
 Lan Prune Delay         : Disabled
 Propagation Delay       : 500  ms
 Override Interval       : 2500  ms
 Graft Retry Interval    : 3 sec
 Max Graft Retries       : 3
 State Refresh Ori Int   : 60 sec

Console#
```

show ipv6 pim neighbor

This command displays information about PIM neighbors.

SYNTAX

show ipv6 pim neighbor [**interface vlan** *vlan-id*]

vlan-id - VLAN ID (Range: 1-4094)

DEFAULT SETTING

Displays information for all known PIM neighbors.

COMMAND MODE

Normal Exec, Privileged Exec

EXAMPLE

```
Console#show ipv6 pim neighbor
Neighbor Address                        VLAN Interface Uptime   Expire   DR
--------------------------------------- -------------- -------- -------- ---
FF80::0101                              VLAN 1         00:01:23 00:01:23 YES
FF80::0202                              VLAN 2         1d 11h   Never

Console#
```

Table 289: show ipv6 pim neighbor - display description

Field	Description
`Neighbor Address`	IP address of the next-hop router.
`VLAN Interface`	Interface number that is attached to this neighbor.
`Uptime`	The duration this entry has been active.
`Expiration Time`	The time before this entry will be removed.

Table 289: show ipv6 pim neighbor - display description (Continued)

Field	Description
DR	The designated PIM6-SM router. If multicast hosts are directly connected to the LAN, then only one of these routers is elected as the DR, and acts on behalf of these hosts, sending periodic Join/ Prune messages toward a group-specific RP for each group.

PIM6-DM Commands

ipv6 pim graft-retry-interval

This command configures the time to wait for a Graft acknowledgement before resending a Graft. Use the **no** form to restore the default value.

Syntax

ipv6 pim graft-retry-interval *seconds*

no ipv6 pim graft-retry-interval

seconds - The time before resending a Graft. (Range: 1-10 seconds)

Default Setting

3 seconds

Command Mode

Interface Configuration (VLAN)

Command Usage

A graft message is sent by a router to cancel a prune state. When a router receives a graft message, it must respond with an graft acknowledgement message. If this acknowledgement message is lost, the router that sent the graft message will resend it a number of times (as defined by the ipv6 pim max-graft-retries command).

Example

```
Console(config-if)#ipv6 pim graft-retry-interval 9
Console(config-if)#
```

Related Commands

ipv6 pim override-interval (1955)
ipv6 pim propagation-delay (1956)

ipv6 pim max-graft-retries

This command configures the maximum number of times to resend a Graft message if it has not been acknowledged. Use the **no** form to restore the default value.

SYNTAX

ipv6 pim max-graft-retries *retries*

no ipv6 pim max-graft-retries

retries - The maximum number of times to resend a Graft. (Range: 1-10)

DEFAULT SETTING

3

COMMAND MODE

Interface Configuration (VLAN)

EXAMPLE

```
Console(config-if)#ipv6 pim max-graft-retries 5
Console(config-if)#
```

ipv6 pim state-refresh origination-interval

This command sets the interval between sending PIM-DM state refresh control messages. Use the **no** form to restore the default value.

SYNTAX

ipv6 pim state-refresh origination-interval *seconds*

no ipv6 pim max-graft-retries

seconds - The interval between sending PIM-DM state refresh control messages. (Range: 1-100 seconds)

DEFAULT SETTING

60 seconds

COMMAND MODE

Interface Configuration (VLAN)

COMMAND USAGE

- The pruned state times out approximately every three minutes and the entire PIM-DM network is reflooded with multicast packets and prune messages. The state refresh feature keeps the pruned state from timing out by periodically forwarding a control message down the distribution tree, refreshing the prune state on the outgoing interfaces of each router in the tree. This also enables PIM routers to recognize topology changes (sources joining or leaving a multicast group) before the default three-minute state timeout expires.

- This command is only effectively for interfaces of first hop, PIM-DM routers that are directly connected to sources of multicast groups.

EXAMPLE

```
Console(config-if)#ipv6 pim state-refresh origination-interval 30
Console(config-if)#
```

PIM6-SM Commands

ipv6 pim bsr-candidate

This command configures the switch as a Bootstrap Router (BSR) candidate. Use the **no** form to restore the default value.

SYNTAX

ipv6 pim bsr-candidate interface vlan *vlan-id* [**hash** *hash-mask-length*] [**priority** *priority*]

no ipv6 pim bsr-candidate

vlan-id - VLAN ID (Range: 1-4094)

hash-mask-length - Hash mask length (in bits) used for RP selection (see ipv6 pim rp-candidate and ipv6 pim rp-address). The portion of the hash specified by the mask length is ANDed with the group address. Therefore, when the hash function is executed on any BSR, all groups with the same seed hash will be mapped to the same RP. If the mask length is less than 32, then only the first portion of the hash is used, and a single RP will be defined for multiple groups. (Range: 0-32 bits)

priority - Priority used by the candidate bootstrap router in the election process. The BSR candidate with the largest priority is preferred. If the priority values are the same, the candidate with the larger IP address is elected to be the BSR. Setting the priority to zero means that this router is not eligible to server as the BSR. At least one router in the PIM6-SM domain must be set to a value greater than zero. (Range: 0-255)

DEFAULT SETTING

Hash Mask Length: 10
Priority: 0

COMMAND MODE

Global Configuration

COMMAND USAGE

- When the **ipv6 pim bsr-candidate** command is entered, the router starts sending bootstrap messages to all of its PIM6-SM neighbors. The IP address of the designated VLAN is sent as the candidate's BSR address. Each neighbor receiving the bootstrap message compares the BSR address with the address from previous messages. If the current address is the same or a higher address, it accepts the bootstrap message and forwards it. Otherwise, it drops the message.

- This router will continue to be the BSR until it receives a bootstrap message from another candidate with a higher priority (or a higher IP address if the priorities are the same).

- To improve failover recovery, it is advisable to select at least two core routers in diverse locations, each to serve as both a candidate BSR and candidate RP. It is also preferable to set up one of these routers as both the primary BSR and RP.

EXAMPLE

The following example configures the router to start sending bootstrap messages out of the interface for VLAN 1 to all of its PIM-SM neighbors.

```
Console(config)#ipv6 pim bsr-candidate interface vlan 1 hash 20 priority 200
Console(config)#exit
Console#show ipv6 pim bsr-router
PIMv2 Bootstrap information
BSR Address      : 2001:DB8:2222:7272::72
Uptime           : 00:00:08
BSR Priority     : 200
Hash Mask Length : 20
Expire           : 00:00:57
Role             : Candidate BSR
State            : Elected BSR
Console#
```

ipv6 pim register-rate-limit

This command configures the rate at which register messages are sent by the Designated Router (DR) for each (source, group) entry. Use the **no** form to restore the default value.

SYNTAX

ipv6 pim register-rate-limit *rate*

no ipv6 pim register-rate-limit

rate - The maximum number of register packets per second. (Range: 1-65535: Default: 0, which means no limit)

DEFAULT SETTING

0

COMMAND MODE

Global Configuration

COMMAND USAGE

This command can be used to relieve the load on the Designated Router (DR) and RP. However, because register messages exceeding the limit are dropped, some receivers may experience data packet loss within the first few seconds in which register messages are sent from bursty sources.

Example

This example sets the register rate limit to 500 pps.

```
Console(config)#ipv6 pim register-rate-limit 500
Console(config)#
```

ipv6 pim register-source

This command configures the IP source address of a register message to an address other than the outgoing interface address of the designated router (DR) that leads back toward the rendezvous point (RP). Use the **no** form to restore the default setting.

Syntax

ipv6 pim register-source interface vlan *vlan-id*

no ipv6 pim register-source

vlan-id - VLAN ID (Range: 1-4094)

Default Setting

The IP address of the DR’s outgoing interface that leads back to the RP

Command Mode

Global Configuration

Command Usage

When the source address of a register message is filtered by intermediate network devices, or is not a uniquely routed address to which the RP can send packets, the replies sent from the RP to the source address will fail to reach the DR, resulting in PIM6-SM protocol failures. This command can be used to overcome this type of problem by manually configuring the source address of register messages to an interface that leads back to the RP.

Example

This example sets the register source address to the interface address for VLAN 1.

```
Console(config)#ipv6 pim register-source interface vlan 1
Console(config)#
```

ipv6 pim rp-address

This command sets a static address for the Rendezvous Point (RP) for a particular multicast group. Use the **no** form to remove an RP address or an RP address for a specific group.

SYNTAX

[**no**] **ipv6 pim rp-address** *rp-address* [**group-prefix** *group-prefix*]

rp-address - Static IPv6 address of the router that will be an RP for the specified multicast group(s).

group-prefix - An IPv6 network prefix for a multicast group. If a group prefix is not specified, the RP is used for all multicast groups.

DEFAULT SETTING

None

COMMAND MODE

Global Configuration

COMMAND USAGE

- The router specified by this command will act as an RP for all multicast groups in the local PIM6-SM domain if no groups are specified. A static RP can either be configured for the whole multicast group range FF00::/8, or for specific group ranges.

- Using this command to configure multiple static RPs with the same RP address is not allowed. If an IP address is specified that was previously used for an RP, then the older entry is replaced. (

- Multiple RPs can be defined for different groups or group ranges. If a group is matched by more than one entry, the router will use the RP associated with the longer group prefix length. If the prefix lengths are the same, then the static RP with the highest IP address is chosen.

- Static definitions for RP addresses may be used together with RP addresses dynamically learned through the bootstrap router (BSR). If an RP address learned by the BSR and one statically configured using this command are both available for a group range, the RP address learned by the BSR is chosen over the one statically configured with this command.

- All routers within the same PIM6-SM domain must be configured with the same RP(s). Selecting an RP through the dynamic election process is therefore preferable for most situations. Using the dynamic RP election process also allows a backup RP to automatically take over if the active RP router becomes unavailable.

- If the **no** form of this command is used without specifying a multicast group, all multicast groups are removed.

EXAMPLE

In the following example, the first PIM-SM command just specifies the RP address 192.168.1.1 to indicate that it will be used to service all multicast groups. The second PIM-SM command includes the multicast groups to be serviced by the RP.

```
Console(config)#ipv6 pim rp-address 2001:DB8:2222:7272::72
Console(config)#ipv6 pim rp-address 2001:DB8:2222:7272::72 group-prefix
  FFAA::0101/8
Console(config)#end
Console#show ipv6 pim rp mapping
PIM Group-to-RP Mappings
Groups            : FF00::/8
RP address        : 2001:DB8:2222:7272::72/128
Info source       : static
Uptime            : 00:03:10
Expire            : Never
Console#
```

ipv6 pim rp-candidate

This command configures the router to advertise itself as a Rendezvous Point (RP) candidate to the bootstrap router (BSR). Use the **no** form to remove this router as an RP candidate.

SYNTAX

ipv6 pim rp-candidate interface vlan *vlan-id*
[**group-prefix** *group-prefix*] [**interval** *seconds*] [**priority** *value*]

no ipv6 pim rp-candidate interface vlan *vlan-id*

vlan-id - VLAN ID (Range: 1-4094)

group-prefix - An IPv6 network prefix for a multicast group. If a group prefix is not specified, the RP is advertised for all multicast groups.

seconds - The interval at which this device advertises itself as an RP candidate. (Range: 60-16383 seconds)

value - Priority used by the candidate RP in the election process. The RP candidate with the largest priority is preferred. If the priority values are the same, the candidate with the larger IP address is elected to be the RP. Setting the priority to zero means that this router is not eligible to server as the RP. (Range: 0-255)

DEFAULT SETTING

Interval: 60 seconds
Priority: 0

COMMAND MODE

Global Configuration

COMMAND USAGE

- When the **ipv6 pim rp-candidate** command is entered, the router periodically sends PIMv2 messages to the BSR advertising itself as a candidate RP for the specified group addresses. The IP address of the designated VLAN is sent as the candidate’s RP address. The BSR places information about all of the candidate RPs in subsequent bootstrap messages. The BSR uses the RP-election hash algorithm to select an active RP for each group range. The el6ection process is performed by the BSR only for its own use. Each PIM-SM router that receives the list of RP candidates from the BSR also elects an active RP for each group range using the same election process.

- The election process for each group is based on the following criteria:
  - Find all RPs with the most specific group range.
  - Select those with the highest priority (lowest priority value).
  - Compute a hash value based on the group address, RP address, priority, and hash mask included in the bootstrap messages.
  - If there is a tie, use the candidate RP with the highest IP address.
- This distributed election process provides faster convergence and minimal disruption when an RP fails. It also serves to provide load balancing by distributing groups across multiple RPs. Moreover, when an RP fails, the responsible RPs are re-elected on each router, and the groups automatically distributed to the remaining RPs.
- To improve failover recovery, it is advisable to select at least two core routers in diverse locations, each to serve as both a candidate BSR and candidate RP. It is also preferable to set up one of these routers as both the primary BSR and RP.

EXAMPLE

The following example configures the router to start advertising itself to the BSR as a candidate RP for the indicated multicast groups.

```
Console(config)#ipv6 pim rp-candidate interface vlan 1 group-prefix
  FFAA::0101/8
Console(config)#end
Console#show ipv6 pim rp mapping
PIM Group-to-RP Mappings
Groups            : FF00::/8
RP address        : 2001:DB8:2222:7272::72/128
Info source       : 2001:DB8:2222:7272::72/128, via bootstrap, priority: 0
Uptime            : 00:02:35
Expire            : 00:01:55
Console#
```

ipv6 pim spt-threshold

This command prevents the last-hop PIM router from switching to Shortest Path Source Tree (SPT) mode. Use the **no** form to allow the router to switch over to SPT mode.

Syntax

ipv6 pim spt-threshold infinity [**group-prefix** *group-prefix*]

no ipv6 pim spt-threshold infinity

group-prefix - An IPv6 network prefix for a multicast group. If a group address is not specified, the command applies to all multicast groups. (Range: FFXX:X:X:X::X/<8-128>)

Default Setting

The last-hop PIM6 router joins the shortest path tree immediately after the first packet arrives from a new source.

Command Mode

Global Configuration

Command Usage

- The default path for packets from a multicast source to a receiver is through the RP. However, the path through the RP is not always the shortest path. Therefore, the router uses the RP to forward only the first packet from a new multicast group to its receivers. Afterwards, it calculates the shortest path tree (SPT) directly between the receiver and source, and then uses the SPT to send all subsequent packets from the source to the receiver instead of using the shared tree. Note that when the SPT threshold is not set by this command, the PIM leaf router will join the shortest path tree immediately after receiving the first packet from a new source.

- This command forces the router to use the shared tree for all multicast groups, or just for the specified multicast groups.

- Only one entry is allowed for this command.

Example

This example prevents the switch from using the SPT for multicast groups FF01:1::0101/64.

```
Console(config)#interface vlan 1
Console(config-if)#ipv6 pim sparse-mode
Console(config-if)#exit
Console(config)#ipv6 multicast-routing
Console(config)#router pim6
Console(config)#ipv6 pim spt-threshold infinity group-prefix FF01:1::0101/64
Console#
```

ipv6 pim dr-priority

This command sets the priority value for a Designated Router (DR) candidate. Use the **no** form to restore the default setting.

SYNTAX

ipv6 pim dr-priority *priority-value*

no ipv6 pim dr-priority

priority-value - Priority advertised by a router when bidding to become the DR. (Range: 0-4294967294)

DEFAULT SETTING

1

COMMAND MODE

Interface Configuration (VLAN)

COMMAND USAGE

- More than one PIM-SM router may be connected to an Ethernet or other shared-media LAN. If multicast hosts are directly connected to the LAN, then only one of these routers is elected as the DR, and acts on behalf of these hosts, sending periodic Join/Prune messages toward a group-specific RP for each group. A single DR is elected per interface (LAN or otherwise) using a simple election process.

- The router with the highest priority configured on an interface is elected as the DR. If more than one router attached to this interface uses the same priority, then the router with the highest IP address is elected to serve as the DR.

- If a router does not advertise a priority in its hello messages, it is assumed to have the highest priority and is elected as the DR. If more than one router is not advertising its priority, then the router with the highest IP address is elected to serve as the DR.

EXAMPLE

This example sets the priority used in the bidding process for the DR.

```
Console(config)#interface vlan 1
Console(config-if)#ipv6 pim dr-priority 20
Console(config-if)#end
Console#show ipv6 pim interface
PIM is enabled.
VLAN 1 is up.
 PIM Mode                 : Sparse Mode
 IPv6 Address             : FE80::200:E8FF:FE93:82A0
 Hello Interval           : 30 sec
 Hello HoldTime           : 105 sec
 Triggered Hello Delay    : 5 sec
 Join/Prune Holdtime      : 210 sec
 Lan Prune Delay          : Disabled
 Propagation Delay        : 500  ms
 Override Interval        : 2500  ms
 DR Priority              : 20
 Join/Prune Interval      : 60 sec
```

```
Console#
```

ipv6 pim join-prune-interval

This command sets the join/prune timer. Use the **no** form to restore the default setting.

SYNTAX

ipv6 pim join-prune-interval *seconds*

no ipv6 pim join-prune-interval

seconds - The interval at which join/prune messages are sent. (Range: 1-65535 seconds)

DEFAULT SETTING

60 seconds

COMMAND MODE

Interface Configuration (VLAN)

COMMAND USAGE

- By default, the switch sends join/prune messages every 210 seconds to inform other PIM-SM routers about clients who want to join or leave a multicast group.

- Use the same join/prune message interval on all the PIM-SM routers in the same PIM-SM domain, otherwise the routing protocol's performance will be adversely affected.

- The multicast interface that first receives a multicast stream from a particular source forwards this traffic only to those interfaces on the router that have requested to join this group. When there are no longer any requesting groups on that interface, the leaf node sends a prune message upstream and enters a prune state for this multicast stream. The protocol maintains both the current join state and the pending Reverse Path Tree (RPT) prune state for this (source, group) pair until the join/prune-interval timer expires.

EXAMPLE

This example sets the priority used in the bidding process for the DR.

```
Console(config)#interface vlan 1
Console(config-if)#ipv6 pim join-prune-interval 220
Console#show ipv6 pim interface
PIM is enabled.
VLAN 1 is up.
 PIM Mode                : Sparse Mode
 IPv6 Address            : FE80::200:E8FF:FE93:82A0
 Hello Interval          : 30 sec
 Hello HoldTime          : 105 sec
 Triggered Hello Delay   : 5 sec
 Join/Prune Holdtime     : 210 sec
 Lan Prune Delay         : Disabled
```

```
  Propagation Delay       : 500  ms
  Override Interval       : 2500  ms
  DR Priority             : 1
  Join/Prune Interval     : 220 sec

Console#
```

clear ipv6 pim bsr rp-set

This command clears multicast group to RP mapping entries learned through the PIMv2 bootstrap router (BSR).

Command Mode

Privileged Exec

Command Usage

- This command can be used to update entries in the static multicast forwarding table immediately after making configuration changes to the RP.
- Use the show ipv6 pim rp mapping command to display active RPs that are cached with associated multicast routing entries.

Example

This example clears the RP map.

```
Console#clear ipv6 pim bsr rp-set
Console#show ipv6 pim rp mapping
PIM Group-to-RP Mappings
Console#
```

show ipv6 pim bsr-router

This command displays information about the bootstrap router (BSR).

Command Mode

Privileged Exec

Command Usage

This command displays information about the elected BSR.

Example

This example displays information about the BSR.

```
Console#show ipv6 pim bsr-router
PIMv2 Bootstrap information
BSR address       : 2001:DB8:2222:7272::72/128
Uptime            : 00:00:04
BSR Priority      : 200
Hash mask length  : 20
Expire            : 00:02:06
Role              : Candidate BSR
```

```
State             : Elected BSR
Console#
```

Table 290: show ip pim bsr-router - display description

Field	Description
`BSR Address`	IP address of interface configured as the BSR.
`Uptime`	The time this BSR has been up and running.
`BSR Priority`	Priority assigned to this interface for use in the BSR election process.
`Hash Mask Length`	The number of significant bits used in the multicast group comparison mask. This mask determines the multicast group for which this router can be a BSR.
`Expire`	The time before this entry will be removed.
`Role`	Candidate BSR or Non-candidate BSR.
`State`	Operation state of BSR includes: ◆ No information – No information stored for this device. ◆ Accept Any – The router does not know of an active BSR, and will accept the first bootstrap message it sees as giving the new BSR's identity and the RP-set. ◆ Accept Preferred – The router knows the identity of the current BSR, and is using the RP-set provided by that BSR. Only bootstrap messages from that BSR or from a C-BSR with higher weight than the current BSR will be accepted. ◆ Candidate BSR – Bidding in election process. ◆ Pending-BSR – The router is a candidate to be the BSR for the RP-set. Currently, no other router is the preferred BSR, but this router is not yet the elected BSR. ◆ Elected BSR – elected to serve as BSR

show ipv6 pim rp mapping

This command displays active RPs and associated multicast routing entries.

COMMAND MODE

Privileged Exec

EXAMPLE

This example displays the RP map.

```
Console#show ipv6 pim rp mapping
PIM Group-to-RP Mappings
Groups            : FF00::/8
RP address        : 2001:DB8:2222:7272::72/128
Info source       : static
Uptime            : 00:23:21
Expire            : Never
Console#
```

Table 291: show ip pim rp mapping - display description

Field	Description
`Groups`	The multicast group address, mask length managed by the RP.
`RP address`	IP address of the RP used for the listed multicast group
`Info source`	RP that advertised the mapping, how the RP was selected (Static or Bootstrap), and the priority used in the bidding process
`Uptime`	The time this RP has been up and running
`Expire`	The time before this entry will be removed

show ipv6 pim rp-hash

This command displays the RP used for the specified multicast group, and the RP that advertised the mapping.

SYNTAX

show ipv6 pim rp-hash *group-address*

group-address - An IP multicast group address.

COMMAND MODE

Privileged Exec

EXAMPLE

This example displays the RP used for the specified group.

```
Console#show ipv6 pim rp-hash FF00::
RP address          : 2001:DB8:2222:7272::72/128
Info source         : 2001:1::0101, via bootstrap
Console#
```

Table 292: show ip pim rp-hash - display description

Field	Description
`RP address`	IP address of the RP used for the specified multicast group
`Info source`	RP that advertised the mapping, and how the RP was selected

SECTION IV

APPENDICES

This section provides additional information and includes these items:

- "Software Specifications" on page 1975
- "Troubleshooting" on page 1981
- "License Information" on page 1983

A Software Specifications

Software Features

Management Authentication
Local, RADIUS, TACACS+, Port Authentication (802.1X), HTTPS, SSH, Port Security, IP Filter

Client Access Control
Access Control Lists (2048 rules), Port Authentication (802.1X), MAC Authentication, Port Security, DHCP Snooping, IP Source Guard

Port Configuration
100BASE-FX: 100 Mbps full duplex (SFP)
100BASE-TX: 10/100 Mbps half/full duplex (SFP)
1000BASE-T: 10/100 Mbps half/full duplex, 1000 Mbps full duplex (SFP)
1000BASE-SX/LX/LH - 1000 Mbps full duplex (SFP)
10GBASE-SR/LR/ER - 10 Gbps full duplex (XFP)

Flow Control
Full Duplex: IEEE 802.3-2005
Half Duplex: Back pressure

Storm Control
Broadcast, multicast, or unicast traffic throttled above a critical threshold

Port Mirroring
28 sessions, one or more source ports to one destination port

Rate Limits
Input/Output Limits
Range configured per port

Port Trunking
Static trunks (Cisco EtherChannel compliant)
Dynamic trunks (Link Aggregation Control Protocol)

Spanning Tree Algorithm
Spanning Tree Protocol (STP, IEEE 802.1D-2004)
Rapid Spanning Tree Protocol (RSTP, IEEE 802.1D-2004)
Multiple Spanning Tree Protocol (MSTP, IEEE 802.1D-2004)

VLAN SUPPORT Up to 4094 groups; port-based, protocol-based, tagged (802.1Q), private VLANs, voice VLANs, IP subnet, MAC-based, QinQ tunnel, GVRP for automatic VLAN learning

CLASS OF SERVICE Supports eight levels of priority

Strict, Weighted Round Robin (WRR), or combination of strict and weighted queueing

Layer 3/4 priority mapping: IP Port, IP Precedence, IP DSCP

QUALITY OF SERVICE DiffServ[31] supports class maps, policy maps, and service policies

MULTICAST FILTERING IGMP Snooping (Layer 2 IPv4)

MLD Snooping (Layer 2 IPv6)

IGMP (Layer 3)

Multicast VLAN Registration (IPv4/IPv6)

IP ROUTING ARP, Proxy ARP

Static routes

CIDR (Classless Inter-Domain Routing)

RIP, RIPv2, OSPFv2, OSPFv3 unicast routing

PIM-SM, PIM-DM, PIMv6 multicast routing

VRRP (Virtual Router Redundancy Protocol)

ADDITIONAL FEATURES BOOTP Client

Connectivity Fault Management

DHCP Client, Relay, Option 82, Server

DNS Client, Proxy

ERPS (Ethernet Ring Protection Switching)

LLDP (Link Layer Discover Protocol)

OAM (Operation, Administration, and Maintenance)

RMON (Remote Monitoring, groups 1,2,3,9)

SMTP Email Alerts

SNMP (Simple Network Management Protocol)

SNTP (Simple Network Time Protocol)

[31] Currently only supported for IPv4. Will be supported for IPv6 in future release.

MANAGEMENT FEATURES

IN-BAND MANAGEMENT	Telnet, web-based HTTP or HTTPS, SNMP manager, or Secure Shell
OUT-OF-BAND MANAGEMENT	RS-232 DB-9 console port
SOFTWARE LOADING	HTTP, FTP or TFTP in-band, or XModem out-of-band
SNMP	Management access via MIB database Trap management to specified hosts
RMON	Groups 1, 2, 3, 9 (Statistics, History, Alarm, Event)

STANDARDS

Ethernet Service OAM (ITU-T Y.1731) - partial support
IEEE 802.1AB Link Layer Discovery Protocol
IEEE 802.1D-2004 Spanning Tree Algorithm and traffic priorities
  Spanning Tree Protocol
  Rapid Spanning Tree Protocol
  Multiple Spanning Tree Protocol
IEEE 802.1p Priority tags
IEEE 802.1Q VLAN
IEEE 802.1v Protocol-based VLANs
IEEE 802.1X Port Authentication
IEEE 802.3-2005
  Ethernet, Fast Ethernet, Gigabit Ethernet
  Link Aggregation Control Protocol (LACP)
  Full-duplex flow control (ISO/IEC 8802-3)
IEEE 802.3ac VLAN tagging
IEEE 802.1ag Connectivity Fault Management (Amendment 5, D7.1)
ARP (RFC 826)
DHCP Client (RFC 2131)
DHCP Relay (RFC 951, 2132, 3046)
DHCP Server (RFC 2131, 2132)
HTTPS
ICMP (RFC 792)
IGMP (RFC 1112)
IGMPv2 (RFC 2236)

IGMPv3 (RFC 3376) - partial support
IGMP Proxy (RFC 4541)
IPv4 IGMP (RFC 3228)
MLD Snooping (RFC 4541)
NTP (RFC 1305)
OSPF (RFC 2328, 2178, 1587)
OSPFv3 (RFC 2740)
PIM-SM (RFC 4601)
PIM-DM (RFC 3973)
RADIUS+ (RFC 2618)
RIPv1 (RFC 1058)
RIPv2 (RFC 2453)
RIPv2, extension (RFC 1724)
RMON (RFC 2819 groups 1,2,3,9)
SNMP (RFC 1157)
SNMPv2c (RFC 1901, 2571)
SNMPv3 (RFC DRAFT 2273, 2576, 3410, 3411, 3413, 3414, 3415)
SNTP (RFC 2030)
SSH (Version 2.0)
TELNET (RFC 854, 855, 856)
TFTP (RFC 1350)
VRRP (RFC 3768)

MANAGEMENT INFORMATION BASES

Bridge MIB (RFC 1493)
Differentiated Services MIB (RFC 3289)
DNS Resolver MIB (RFC 1612)
ERPS MIB (ITU-T G.8032)
Entity MIB (RFC 2737)
Ether-like MIB (RFC 2665)
Extended Bridge MIB (RFC 2674)
Extensible SNMP Agents MIB (RFC 2742)
Forwarding Table MIB (RFC 2096)
IGMP MIB (RFC 2933)
Interface Group MIB (RFC 2233)
Interfaces Evolution MIB (RFC 2863)
IP MIB (RFC 2011)
IP Forwarding Table MIB (RFC 2096)
IP Multicasting related MIBs
IPV6-MIB (RFC 2065)
IPV6-ICMP-MIB (RFC 2066)
IPV6-TCP-MIB (RFC 2052)

IPV6-UDP-MIB (RFC2054)
Link Aggregation MIB (IEEE 802.3ad)
MAU MIB (RFC 3636)
MIB II (RFC 1213)
OSPF MIB (RFC 1850)
OSPFv3 MIB (draft-ietf-ospf-ospfv3-mib-15.txt)
P-Bridge MIB (RFC 2674P)
Port Access Entity MIB (IEEE 802.1X)
Port Access Entity Equipment MIB
Power Ethernet MIB (RFC 3621)
Private MIB
Q-Bridge MIB (RFC 2674Q)
QinQ Tunneling (IEEE 802.1ad Provider Bridges)
Quality of Service MIB
RADIUS Accounting Server MIB (RFC 2621)
RADIUS Authentication Client MIB (RFC 2619)
RIP1 MIB (RFC 1058)
RIP2 MIB (RFC 2453)
RIP2 Extension (RFC1724)
RMON MIB (RFC 2819)
RMON II Probe Configuration Group (RFC 2021, partial implementation)
SNMP Community MIB (RFC 3584)
SNMP Framework MIB (RFC 3411)
SNMP-MPD MIB (RFC 3412)
SNMP Target MIB, SNMP Notification MIB (RFC 3413)
SNMP User-Based SM MIB (RFC 3414)
SNMP View Based ACM MIB (RFC 3415)
SNMPv2 IP MIB (RFC 2011)
TACACS+ Authentication Client MIB
TCP MIB (RFC 2012)
Trap (RFC 1215)
UDP MIB (RFC 2013)
VRRP MIB (RFC 2787)

B TROUBLESHOOTING

PROBLEMS ACCESSING THE MANAGEMENT INTERFACE

Table 293: Troubleshooting Chart

Symptom	Action
Cannot connect using Telnet, web browser, or SNMP software	◆ Be sure the switch is powered on. ◆ Check network cabling between the management station and the switch. Make sure the ends are properly connected and there is no damage to the cable. Test the cable if necessary. ◆ Check that you have a valid network connection to the switch and that the port you are using has not been disabled. ◆ Be sure you have configured the VLAN interface through which the management station is connected with a valid IP address, subnet mask and default gateway. ◆ Be sure the management station has an IP address in the same subnet as the switch's IP interface to which it is connected. ◆ If you are trying to connect to the switch via the IP address for a tagged VLAN group, your management station, and the ports connecting intermediate switches in the network, must be configured with the appropriate tag. ◆ If you cannot connect using Telnet, you may have exceeded the maximum number of concurrent Telnet/SSH sessions permitted. Try connecting again at a later time.
Cannot connect using Secure Shell	◆ If you cannot connect using SSH, you may have exceeded the maximum number of concurrent Telnet/SSH sessions permitted. Try connecting again at a later time. ◆ Be sure the control parameters for the SSH server are properly configured on the switch, and that the SSH client software is properly configured on the management station. ◆ Be sure you have generated both an RSA and DSA public key on the switch, exported this key to the SSH client, and enabled SSH service. Try using another SSH client or check for updates to your SSH client application. ◆ Be sure you have set up an account on the switch for each SSH user, including user name, authentication level, and password. ◆ Be sure you have imported the client's public key to the switch (if public key authentication is used).
Cannot access the on-board configuration program via a serial port connection	◆ Be sure you have set the terminal emulator program to VT100 compatible, 8 data bits, 1 stop bit, no parity, and the baud rate set to 115200 bps. ◆ Verify that you are using the RJ-45 to DB-9 null-modem serial cable supplied with the switch. If you use any other cable, be sure that it conforms to the pin-out connections provided in the Installation Guide.
Forgot or lost the password	◆ Contact your local distributor.

USING SYSTEM LOGS

If a fault does occur, refer to the Installation Guide to ensure that the problem you encountered is actually caused by the switch. If the problem appears to be caused by the switch, follow these steps:

1. Enable logging.
2. Set the error messages reported to include all categories.
3. Enable SNMP.
4. Enable SNMP traps.
5. Designate the SNMP host that is to receive the error messages.
6. Repeat the sequence of commands or other actions that lead up to the error.
7. Make a list of the commands or circumstances that led to the fault. Also make a list of any error messages displayed.
8. Set up your terminal emulation software so that it can capture all console output to a file. Then enter the “show tech-support” command to record all system settings in this file.
9. Contact your distributor’s service engineer, and send a detailed description of the problem, along with the file used to record your system settings.

For example:

```
Console(config)#logging on
Console(config)#logging history flash 7
Console(config)#snmp-server host 192.168.1.23
⋮
```

C LICENSE INFORMATION

This product includes copyrighted third-party software subject to the terms of the GNU General Public License (GPL), GNU Lesser General Public License (LGPL), or other related free software licenses. The GPL code used in this product is distributed WITHOUT ANY WARRANTY and is subject to the copyrights of one or more authors. For details, refer to the section "The GNU General Public License" below, or refer to the applicable license as included in the source-code archive.

THE GNU GENERAL PUBLIC LICENSE

GNU GENERAL PUBLIC LICENSE
Version 2, June 1991

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users. This General Public License applies to most of the Free Software Foundation's software and to any other program whose authors commit to using it. (Some other Free Software Foundation software is covered by the GNU Library General Public License instead.) You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs; and that you know you can do these things.

To protect your rights, we need to make restrictions that forbid anyone to deny you these rights or to ask you to surrender the rights. These restrictions translate to certain responsibilities for you if you distribute copies of the software, or if you modify it.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must give the recipients all the rights that you have. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

We protect your rights with two steps: (1) copyright the software, and (2) offer you this license which gives you legal permission to copy, distribute and/or modify the software.

Also, for each author's protection and ours, we want to make certain that everyone understands that there is no warranty for this free software. If the software is modified by someone else and passed on, we want its recipients to know that what they have is not the original, so that any problems introduced by others will not reflect on the original authors' reputations.

Finally, any free program is threatened constantly by software patents. We wish to avoid the danger that redistributors of a free program will individually obtain patent licenses, in effect making the program proprietary. To prevent this, we have made it clear that any patent must be licensed for everyone's free use or not licensed at all.

The precise terms and conditions for copying, distribution and modification follow.

GNU GENERAL PUBLIC LICENSE TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

1. This License applies to any program or other work which contains a notice placed by the copyright holder saying it may be distributed under the terms of this General Public License. The "Program", below, refers to any such program or work, and a "work based on the Program" means either the Program or any derivative work under copyright law: that is to say, a work containing the Program or a portion of it, either verbatim or with modifications and/or translated into another language. (Hereinafter, translation is included without limitation in the term "modification".) Each licensee is addressed as "you".

   Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running the Program is not restricted, and the output from the Program is covered only if its contents constitute a work based on the Program (independent of having been made by running the Program). Whether that is true depends on what the Program does.

2. You may copy and distribute verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and give any other recipients of the Program a copy of this License along with the Program.

   You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

3. You may modify your copy or copies of the Program or any portion of it, thus forming a work based on the Program, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

   a) You must cause the modified files to carry prominent notices stating that you changed the files and the date of any change.

   b) You must cause any work that you distribute or publish, that in whole or in part contains or is derived from the Program or any part thereof, to be licensed as a whole at no charge to all third parties under the terms of this License.

   c) If the modified program normally reads commands interactively when run, you must cause it, when started running for such interactive use in the most ordinary way, to print or display an announcement including an appropriate copyright notice and a notice that there is no warranty (or else, saying that you provide a warranty) and that users may redistribute the program under these conditions, and telling the user how to view a copy of this License. (Exception: if the Program itself is interactive but does not normally print such an announcement, your work based on the Program is not required to print an announcement.)

   These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Program, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Program, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

   Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Program.

   In addition, mere aggregation of another work not based on the Program with the Program (or with a work based on the Program) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

4. You may copy and distribute the Program (or a work based on it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you also do one of the following:

   a) Accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

   b) Accompany it with a written offer, valid for at least three years, to give any third party, for a charge no more than your cost of physically performing source distribution, a complete machine-readable copy of the corresponding source code, to be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

   c) Accompany it with the information you received as to the offer to distribute corresponding source code. (This alternative is allowed only for noncommercial distribution and only if you received the program in object code or executable form with such an offer, in accord with Subsection b above.)

   The source code for a work means the preferred form of the work for making modifications to it. For an executable work, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the executable. However, as a special exception, the source code distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

   If distribution of executable or object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place counts as distribution of the source code, even though third parties are not compelled to copy the source along with the object code.

5. You may not copy, modify, sublicense, or distribute the Program except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense or distribute the Program is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

6. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Program or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Program (or any work based on the Program), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Program or works based on it.

7. Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.

8. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Program at all. For example, if a patent license would not permit royalty-free redistribution of the Program by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Program.

   If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply and the section as a whole is intended to apply in other circumstances.

   It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system, which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

9. If the distribution and/or use of the Program is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Program under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

10. The Free Software Foundation may publish revised and/or new versions of the General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

    Each version is given a distinguishing version number. If the Program specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of this License, you may choose any version ever published by the Free Software Foundation.

11. If you wish to incorporate parts of the Program into other free programs whose distribution conditions are different, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

1. BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

2. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

Glossary

ACL Access Control List. ACLs can limit network traffic and restrict access to certain users or devices by checking each packet for certain IP or MAC (i.e., Layer 2) information.

ARP Address Resolution Protocol converts between IP addresses and MAC (hardware) addresses. ARP is used to locate the MAC address corresponding to a given IP address. This allows the switch to use IP addresses for routing decisions and the corresponding MAC addresses to forward packets from one hop to the next.

ARP Address Resolution Protocol converts between IP addresses and MAC (i.e., hardware) addresses. ARP is used to locate the MAC address corresponding to a given IP address. This allows the switch to use IP addresses for routing decisions and the corresponding MAC addresses to forward packets from one hop to the next.

BOOTP Boot Protocol. BOOTP is used to provide bootup information for network devices, including IP address information, the address of the TFTP server that contains the devices system files, and the name of the boot file.

CoS Class of Service is supported by prioritizing packets based on the required level of service, and then placing them in the appropriate output queue. Data is transmitted from the queues using weighted round-robin service to enforce priority service and prevent blockage of lower-level queues. Priority may be set according to the port default, the packet’s priority bit (in the VLAN tag), TCP/UDP port number, IP Precedence bit, or DSCP priority bit.

DHCP Dynamic Host Control Protocol. Provides a framework for passing configuration information to hosts on a TCP/IP network. DHCP is based on the Bootstrap Protocol (BOOTP), adding the capability of automatic allocation of reusable network addresses and additional configuration options.

DHCP Option 82 A relay option for sending information about the requesting client (or an intermediate relay agent) in the DHCP request packets forwarded by the switch and in reply packets sent back from the DHCP server. This information can be used by DHCP servers to assign fixed IP addresses, or set other services or policies for clients.

DHCP SNOOPING A technique used to enhance network security by snooping on DHCP server messages to track the physical location of hosts, ensure that hosts only use the IP addresses assigned to them, and ensure that only authorized DHCP servers are accessible.

DIFFSERV Differentiated Services provides quality of service on large networks by employing a well-defined set of building blocks from which a variety of aggregate forwarding behaviors may be built. Each packet carries information (DS byte) used by each hop to give it a particular forwarding treatment, or per-hop behavior, at each network node. DiffServ allocates different levels of service to users on the network with mechanisms such as traffic meters, shapers/droppers, packet markers at the boundaries of the network.

DNS Domain Name Service. A system used for translating host names for network nodes into IP addresses.

DSCP Differentiated Services Code Point Service. DSCP uses a six-bit tag to provide for up to 64 different forwarding behaviors. Based on network policies, different kinds of traffic can be marked for different kinds of forwarding. The DSCP bits are mapped to the Class of Service categories, and then into the output queues.

EAPOL Extensible Authentication Protocol over LAN. EAPOL is a client authentication protocol used by this switch to verify the network access rights for any device that is plugged into the switch. A user name and password is requested by the switch, and then passed to an authentication server (e.g., RADIUS) for verification. EAPOL is implemented as part of the IEEE 802.1X Port Authentication standard.

EUI Extended Universal Identifier is an address format used by IPv6 to identify the host portion of the network address. The interface identifier in EUI compatible addresses is based on the link-layer (MAC) address of an interface. Interface identifiers used in global unicast and other IPv6 address types are 64 bits long and may be constructed in the EUI-64 format. The modified EUI-64 format interface ID is derived from a 48-bit link-layer address by inserting the hexadecimal number FFFE between the upper three bytes (OUI field) and the lower 3 bytes (serial number) of the link layer address. To ensure that the chosen address is from a unique Ethernet MAC address, the 7th bit in the high-order byte is set to 1 (equivalent to the IEEE Global/Local bit) to indicate the uniqueness of the 48-bit address.

GARP Generic Attribute Registration Protocol. GARP is a protocol that can be used by endstations and switches to register and propagate multicast group membership information in a switched environment so that multicast data frames are propagated only to those parts of a switched LAN containing registered endstations. Formerly called Group Address Registration Protocol.

GMRP Generic Multicast Registration Protocol. GMRP allows network devices to register end stations with multicast groups. GMRP requires that any participating network devices or end stations comply with the IEEE 802.1p standard.

GVRP GARP VLAN Registration Protocol. Defines a way for switches to exchange VLAN information in order to register necessary VLAN members on ports along the Spanning Tree so that VLANs defined in each switch can work automatically over a Spanning Tree network.

ICMP Internet Control Message Protocol is a network layer protocol that reports errors in processing IP packets. ICMP is also used by routers to feed back information about better routing choices.

IEEE 802.1D Specifies a general method for the operation of MAC bridges, including the Spanning Tree Protocol.

IEEE 802.1Q VLAN Tagging—Defines Ethernet frame tags which carry VLAN information. It allows switches to assign endstations to different virtual LANs, and defines a standard way for VLANs to communicate across switched networks.

IEEE 802.1p An IEEE standard for providing quality of service (QoS) in Ethernet networks. The standard uses packet tags that define up to eight traffic classes and allows switches to transmit packets based on the tagged priority value.

IEEE 802.1s An IEEE standard for the Multiple Spanning Tree Protocol (MSTP) which provides independent spanning trees for VLAN groups.

IEEE 802.1w An IEEE standard for the Rapid Spanning Tree Protocol (RSTP) which reduces the convergence time for network topology changes to about 10% of that required by the older IEEE 802.1D STP standard. (Now incorporated in IEEE 802.1D-2004)

IEEE 802.1X Port Authentication controls access to the switch ports by requiring users to first enter a user ID and password for authentication.

IEEE 802.3ac Defines frame extensions for VLAN tagging.

IEEE 802.3x Defines Ethernet frame start/stop requests and timers used for flow control on full-duplex links. (Now incorporated in IEEE 802.3-2002)

IGMP Internet Group Management Protocol. A protocol through which hosts can register with their local router for multicast services. If there is more than one multicast switch/router on a given subnetwork, one of the devices is made the "querier" and assumes responsibility for keeping track of group membership.

IGMP Proxy Proxies multicast group membership information onto the upstream interface based on IGMP messages monitored on downstream interfaces, and forwards multicast traffic based on that information. There is no need for multicast routing protocols in an simple tree that uses IGMP Proxy.

IGMP Query On each subnetwork, one IGMP-capable device will act as the querier — that is, the device that asks all hosts to report on the IP multicast groups they wish to join or to which they already belong. The elected querier will be the device with the lowest IP address in the subnetwork.

IGMP Snooping Listening to IGMP Query and IGMP Report packets transferred between IP Multicast Routers and IP Multicast host groups to identify IP Multicast group members.

In-Band Management Management of the network from a station attached directly to the network.

IP Multicast Filtering A process whereby this switch can pass multicast traffic along to participating hosts.

IP Precedence The Type of Service (ToS) octet in the IPv4 header includes three precedence bits defining eight different priority levels ranging from highest priority for network control packets to lowest priority for routine traffic. The eight values are mapped one-to-one to the Class of Service categories by default, but may be configured differently to suit the requirements for specific network applications.

LACP Link Aggregation Control Protocol. Allows ports to automatically negotiate a trunked link with LACP-configured ports on another device.

LAYER 2 Data Link layer in the ISO 7-Layer Data Communications Protocol. This is related directly to the hardware interface for network devices and passes on traffic based on MAC addresses.

LAYER 3 Network layer in the ISO 7-Layer Data Communications Protocol. This layer handles the routing functions for data moving from one open system to another.

LINK AGGREGATION *See Port Trunk.*

LLDP Link Layer Discovery Protocol is used to discover basic information about neighboring devices in the local broadcast domain by using periodic broadcasts to advertise information such as device identification, capabilities and configuration settings.

MD5 MD5 Message-Digest is an algorithm that is used to create digital signatures. It is intended for use with 32 bit machines and is safer than the MD4 algorithm, which has been broken. MD5 is a one-way hash function, meaning that it takes a message and converts it into a fixed string of digits, also called a message digest.

MIB Management Information Base. An acronym for Management Information Base. It is a set of database objects that contains information about a specific device.

MRD Multicast Router Discovery is a A protocol used by IGMP snooping and multicast routing devices to discover which interfaces are attached to multicast routers. This process allows IGMP-enabled devices to determine where to send multicast source and group membership messages.

MSTP Multiple Spanning Tree Protocol can provide an independent spanning tree for different VLANs. It simplifies network management, provides for even faster convergence than RSTP by limiting the size of each region, and prevents VLAN members from being segmented from the rest of the group.

MULTICAST SWITCHING A process whereby the switch filters incoming multicast frames for services for which no attached host has registered, or forwards them to all ports contained within the designated multicast VLAN group.

MVR Multicast VLAN Registration is a method of using a single network-wide multicast VLAN to transmit common services, such as such as television channels or video-on-demand, across a service-provider's network. MVR simplifies the configuration of multicast services by using a common VLAN for distribution, while still preserving security and data isolation for subscribers residing in both the MVR VLAN and other standard or private VLAN groups.

NTP Network Time Protocol provides the mechanisms to synchronize time across the network. The time servers operate in a hierarchical-master-slave configuration in order to synchronize local clocks within the subnet and to national time standards via wire or radio.

OSPF Open Shortest Path First is a link-state routing protocol that functions better over a larger network such as the Internet, as opposed to distance-vector routing protocols such as RIP. It includes features such as unlimited hop count, authentication of routing updates, and Variable Length Subnet Masks (VLSM).

Out-of-Band Management Management of the network from a station not attached to the network.

Port Authentication *See IEEE 802.1X*.

Port Mirroring A method whereby data on a target port is mirrored to a monitor port for troubleshooting with a logic analyzer or RMON probe. This allows data on the target port to be studied unobstructively.

Port Trunk Defines a network link aggregation and trunking method which specifies how to create a single high-speed logical link that combines several lower-speed physical links.

Private VLANs Private VLANs provide port-based security and isolation between ports within the assigned VLAN. Data traffic on downlink ports can only be forwarded to, and from, uplink ports.

QinQ QinQ tunneling is designed for service providers carrying traffic for multiple customers across their networks. It is used to maintain customer-specific VLAN and Layer 2 protocol configurations even when different customers use the same internal VLAN IDs.

QoS Quality of Service. QoS refers to the capability of a network to provide better service to selected traffic flows using features such as data prioritization, queuing, congestion avoidance and traffic shaping. These features effectively provide preferential treatment to specific flows either by raising the priority of one flow or limiting the priority of another flow.

RADIUS Remote Authentication Dial-in User Service. RADIUS is a logon authentication protocol that uses software running on a central server to control access to RADIUS-compliant devices on the network.

RIP Routing Information Protocol seeks to find the shortest route to another device by minimizing the distance-vector, or hop count, which serves as a rough estimate of transmission cost. RIP-2 is a compatible upgrade to RIP. It adds useful capabilities for subnet routing, authentication, and multicast transmissions.

RMON Remote Monitoring. RMON provides comprehensive network monitoring capabilities. It eliminates the polling required in standard SNMP, and can set alarms on a variety of traffic conditions, including specific error types.

RSTP Rapid Spanning Tree Protocol. RSTP reduces the convergence time for network topology changes to about 10% of that required by the older IEEE 802.1D STP standard.

SMTP Simple Mail Transfer Protocol is a standard host-to-host mail transport protocol that operates over TCP, port 25.

SNMP Simple Network Management Protocol. The application protocol in the Internet suite of protocols which offers network management services.

SNTP Simple Network Time Protocol allows a device to set its internal clock based on periodic updates from a Network Time Protocol (NTP) server. Updates can be requested from a specific NTP server, or can be received via broadcasts sent by NTP servers.

SSH Secure Shell is a secure replacement for remote access functions, including Telnet. SSH can authenticate users with a cryptographic key, and encrypt data connections between management clients and the switch.

STA Spanning Tree Algorithm is a technology that checks your network for any loops. A loop can often occur in complicated or backup linked network systems. Spanning Tree detects and directs data along the shortest available path, maximizing the performance and efficiency of the network.

TACACS+ Terminal Access Controller Access Control System Plus. TACACS+ is a logon authentication protocol that uses software running on a central server to control access to TACACS-compliant devices on the network.

TCP/IP Transmission Control Protocol/Internet Protocol. Protocol suite that includes TCP as the primary transport protocol, and IP as the network layer protocol.

TELNET Defines a remote communication facility for interfacing to a terminal device over TCP/IP.

TFTP Trivial File Transfer Protocol. A TCP/IP protocol commonly used for software downloads.

UDP User Datagram Protocol. UDP provides a datagram mode for packet-switched communications. It uses IP as the underlying transport mechanism to provide access to IP-like services. UDP packets are delivered just like IP packets – connection-less datagrams that may be discarded before reaching their targets. UDP is useful when TCP would be too complex, too slow, or just unnecessary.

UTC Universal Time Coordinate. UTC is a time scale that couples Greenwich Mean Time (based solely on the Earth’s rotation rate) with highly accurate atomic time. The UTC does not have daylight saving time.

VLAN Virtual LAN. A Virtual LAN is a collection of network nodes that share the same collision domain regardless of their physical location or connection point in the network. A VLAN serves as a logical workgroup with no physical barriers, and allows users to share information and resources as though located on the same LAN.

VRRP Virtual Router Redundancy Protocol uses a virtual IP address to support a primary router and multiple backup routers. The backups can be configured to take over the workload if the master fails or to load share the traffic. The primary goal of VRRP is to allow a host device which has been configured with a fixed gateway to maintain network connectivity in case the primary gateway goes down.

XMODEM A protocol used to transfer files between devices. Data is grouped in 128-byte blocks and error-corrected.

Command List

A

aaa accounting dot1x 1044
aaa accounting exec 1045
aaa accounting update 1046
aaa authorization exec 1047
aaa group server 1048
abr-type 1793
absolute 958
access-list arp 1181
access-list ip 1164
access-list ipv6 1170
access-list mac 1176
accounting dot1x 1049
accounting exec 1049
aggregate-address 1839
alias 1189
area default-cost 1756
area default-cost 1797
area nssa 1762
area range 1757
area range 1798
area stub 1764
area stub 1801
area virtual-link 1765
area virtual-link 1802
arp 1655
arp timeout 1656
authentication enable 1034
authentication login 1035
authorization exec 1050
auto-cost reference-bandwidth 1758
auto-traffic-control 1247
auto-traffic-control action 1248
auto-traffic-control alarm-clear-threshold 1249
auto-traffic-controlalarm-fire-threshold 1250
auto-traffic-control apply-timer 1246
auto-traffic-controlauto-control-release 1251
auto-traffic-control control-release 1251
auto-traffic-control release-timer 1246

B

banner configure 893
banner configure company 894
banner configure dc-power-info 895
banner configure department 895
banner configure equipment-info 896
banner configure equipment-location 897
banner configure ip-lan 897
banner configure lp-number 898
banner configure manager-info 899
banner configure mux 899
banner configure note 900
bgp always-compare-med 1853
bgp bestpath as-path ignore 1853
bgp bestpath compare-confed-aspath 1854
bgp bestpath compare-routerid 1854
bgp bestpath med 1855
bgp client-to-client reflection 1840
bgp cluster-id 1841
bgp confederation identifier 1842
bgp confederation peer 1843
bgp dampening 1844
bgp default local-preference 1855
bgp deterministic-med 1856
bgp enforce-first-as 1845
bgp fast-external-failover 1845
bgp log-neighbor-changes 1846
bgp network import-check 1846
bgp router-id 1847
bgp scan-time 1848
boot system 913
bootfile 1635
bridge-ext gvrp 1338

C

calendar set 956
call 1900
capabilities 1189
channel-group 1218
class 1412
class-map 1408
clear access-list hardware counters 1184
clear arp-cache 1658
clear counters 1196
clear dns cache 1620
clear efm oam counters 1607
clear efm oam event-log 1608
clear erps statistics 1326
clear ethernet cfm ais mpid 1573
clear ethernet cfm errors 1585

clear ethernet cfm linktrace-cache 1593
clear ethernet cfm maintenance-points remote 1584
clear host 1621
clear ip bgp 1851
clear ip bgp dampening 1852
clear ip dhcp binding 1643
clear ip dhcp snooping binding 1124
clear ip dhcp snooping database flash 1124
clear ip igmp group 1519
clear ip ospf process 1756
clear ip pim bsr rp-set 1947
clear ip rip route 1748
clear ip source-guard binding blocked 1138
clear ipv6 dhcp snooping binding 1131
clear ipv6 dhcp snooping statistics 1132
clear ipv6 mld group 1531
clear ipv6 nd snooping binding 1710
clear ipv6 nd snooping prefix 1710
clear ipv6 neighbors 1694
clear ipv6 pim bsr rp-set 1970
clear ipv6 traffic 1679
clear log 937
clear mac-address-table dynamic 1273
clear mvr6 groups 1506
clear mvr6 statistics 1507
clear network-access 1107
clear pppoe intermediate-agent statistics 1085
clear vrrp interface counters 1718
clear vrrp router counters 1718
client-identifier 1635
clock summer-time (date) 951
clock summer-time (predefined) 953
clock summer-time (recurring) 954
clock timezone 955
cluster 990
cluster commander 990
cluster ip-pool 991
cluster member 992
compatible rfc1583 1752
configure 887
continue 1901
control-vlan 1308
copy 914

D

databits 925
default-information originate 1734
default-information originate 1753
default-metric 1735
default-metric 1759
default-metric 1799
default-router 1636
delete 917
delete public-key 1062
description 1409
description 1190
description 1901
dir 918
disable 888
discard 1191
disconnect 932
distance 1736
distance 1857
distance bgp 1858
dns-server 1637
domain-name 1637
dos-protection land 1154
dos-protection tcp-null-scan 1155
dos-protection tcp-syn-fin-scan 1155
dos-protection tcp-xmas-scan 1156
dot1q-tunnel system-tunnel-control 1354
dot1x default 1068
dot1x eapol-pass-through 1068
dot1x intrusion-action 1069
dot1x max-reauth-req 1070
dot1x max-req 1070
dot1x operation-mode 1071
dot1x port-control 1072
dot1x re-authenticate 1075
dot1x re-authentication 1072
dot1x system-auth-control 1069
dot1x timeout quiet-period 1073
dot1x timeout re-authperiod 1073
dot1x timeout supp-timeout 1074
dot1x timeout tx-period 1074

E

efm oam 1604
efm oam critical-link-event 1604
efm oam link-monitor frame 1605
efm oam link-monitor frame threshold 1605
efm oam link-monitor frame window 1606
efm oam mode 1607
efm oam remote-loopback 1608
efm oam remote-loopback test 1609
enable 1309
enable 885
enable password 1032
end 889
erps 1307
erps clear 1327
erps domain 1307
erps forced-switch 1327
erps manual-switch 1329
ethernet cfm ais level 1564
ethernet cfm ais ma 1565
ethernet cfm ais period 1566

ethernet cfm ais suppress alarm 1566
ethernet cfm cc enable 1582
ethernet cfm cc ma interval 1581
ethernet cfm delay-measure two-way 1600
ethernet cfm domain 1567
ethernet cfm enable 1569
ethernet cfm linktrace 1592
ethernet cfm linktrace cache 1590
ethernet cfm linktrace cache hold-time 1591
ethernet cfm linktrace cache size 1591
ethernet cfm loopback 1595
ethernet cfm mep 1571
ethernet cfm mep crosscheck 1589
ethernet cfm mep crosscheck start-delay 1586
ethernet cfm port-enable 1572
exec-timeout 925
exit 889

F

fan-speed force-full 910
flowcontrol 1191

G

garp timer 1339
guard-timer 1310

H

hardware-address 1638
history 1192
holdoff-timer 1310
host 1638
hostname 892

I

interface 1188
interface tunnel 1697
interface vlan 1345
ip access-group 1168
ip address 1648
ip arp inspection 1146
ip arp inspection filter 1147
ip arp inspection limit 1151
ip arp inspection log-buffer logs 1148
ip arp inspection trust 1151
ip arp inspection validate 1149
ip arp inspection vlan 1150
ip as-path access-list 1833
ip community-list 1834
ip default-gateway 1650
ip dhcp client class-id 1625
ip dhcp excluded-address 1633
ip dhcp pool 1634
ip dhcp relay server 1629
ip dhcp restart client 1627
ip dhcp restart relay 1630
ip dhcp snooping 1116
ip dhcp snooping database flash 1125
ip dhcp snooping information option 1118
ip dhcp snooping information option circuit-id 1122
ip dhcp snooping information policy 1119
ip dhcp snooping trust 1123
ip dhcp snooping verify mac-address 1120
ip dhcp snooping vlan 1121
ip domain-list 1615
ip domain-lookup 1616
ip domain-name 1617
ip extcommunity-list 1836
ip forward-protocol udp 1659
ip helper 1660
ip helper-address 1661
ip host 1618
ip http port 1052
ip http secure-port 1053
ip http secure-server 1053
ip http server 1052
ip igmp 1514
ip igmp authentication 1451
ip igmp filter (Global Configuration) 1449
ip igmp filter (Interface Configuration) 1453
ip igmp last-member-query-interval 1515
ip igmp max-groups 1454
ip igmp max-groups action 1454
ip igmp max-resp-interval 1515
ip igmp profile 1450
ip igmp proxy 1523
ip igmp proxy unsolicited-report-interval 1524
ip igmp query-drop 1455
ip igmp query-interval 1516
ip igmp robustval 1517
ip igmp snooping 1427
ip igmp snooping priority 1428
ip igmp snooping proxy-reporting 1428
ip igmp snooping querier 1429
ip igmp snooping router-alert-option-check 1429
ip igmp snooping router-port-expire-time 1430
ip igmp snooping tcn-flood 1431
ip igmp snooping tcn-query-solicit 1432
ip igmp snooping unregistered-data-flood 1432

ip igmp snooping unsolicited-report-interval 1433
ip igmp snooping version 1434
ip igmp snooping version-exclusive 1434
ip igmp snooping vlan general-query-suppression 1435
ip igmp snooping vlan immediate-leave 1436
ip igmp snooping vlan last-memb-query-count 1437
ip igmp snooping vlan last-memb-query-intvl 1437
ip igmp snooping vlan mrd 1438
ip igmp snooping vlan mrouter 1447
ip igmp snooping vlan mrouter 1925
ip igmp snooping vlan proxy-address 1439
ip igmp snooping vlan query-interval 1440
ip igmp snooping vlan query-resp-intvl 1441
ip igmp snooping vlan static 1442
ip igmp static-group 1518
ip igmp version 1519
ip multicast-data-drop 1455
ip multicast-routing 1919
ip name-server 1619
ip ospf authentication 1769
ip ospf authentication-key 1770
ip ospf cost 1771
ip ospf dead-interval 1772
ip ospf hello-interval 1772
ip ospf message-digest-key 1773
ip ospf priority 1774
ip ospf retransmit-interval 1775
ip ospf transmit-delay 1776
ip pim 1929
ip pim bsr-candidate 1938
ip pim dr-priority 1945
ip pim graft-retry-interval 1936
ip pim hello-holdtime 1930
ip pim hello-interval 1931
ip pim join-prune-holdtime 1931
ip pim join-prune-interval 1946
ip pim lan-prune-delay 1932
ip pim max-graft-retries 1937
ip pim override-interval 1933
ip pim propagation-delay 1934
ip pim register-rate-limit 1939
ip pim register-source 1940
ip pim rp-address 1941
ip pim rp-candidate 1942
ip pim spt-threshold 1944
ip pim state-refresh origination-interval 1937
ip pim trigger-hello-delay 1934
ip prefix-list 1838
ip proxy-arp 1657
ip rip authentication mode 1742
ip rip authentication string 1743
ip rip receive version 1744
ip rip receive-packet 1745
ip rip send version 1745
ip rip send-packet 1746
ip rip split-horizon 1747
ip route 1724
ip source-guard 1135
ip source-guard binding 1134
ip source-guard max-binding 1137
ip source-guard mode 1138
ip ssh authentication-retries 1060
ip ssh crypto host-key generate 1063
ip ssh crypto zeroize 1064
ip ssh save host-key 1064
ip ssh server 1060
ip ssh server-key size 1061
ip ssh timeout 1062
ip telnet max-sessions 1055
ip telnet port 1056
ip telnet server 1056
ipv6 access-group 1174
ipv6 address 1665
ipv6 address eui-64 1667
ipv6 address link-local 1669
ipv6 default-gateway 1664
ipv6 dhcp client rapid-commit vlan 1628
ipv6 dhcp relay destination 1631
ipv6 dhcp snooping 1126
ipv6 dhcp snooping max-binding 1130
ipv6 dhcp snooping trust 1130
ipv6 dhcp snooping vlan 1129
ipv6 enable 1670
ipv6 hop-limit 1682
ipv6 host 1620
ipv6 mld 1525
ipv6 mld filter (Interface Configuration) 1472
ipv6 mld filter (Global Configuration) 1470
ipv6 mld last-member-query-response-interval 1526
ipv6 mld max-groups 1473
ipv6 mld max-groups action 1474
ipv6 mld max-resp-interval 1527
ipv6 mld profile 1471
ipv6 mld proxy 1534
ipv6 mld proxy unsolicited-report-interval 1535
ipv6 mld query-drop 1474
ipv6 mld query-interval 1528
ipv6 mld robustval 1528
ipv6 mld snooping 1461
ipv6 mld snooping querier 1461
ipv6 mld snooping query-interval 1462
ipv6 mld snooping query-max-response-time 1462

ipv6 mld snooping robustness 1463
ipv6 mld snooping router-port-expire-time 1463
ipv6 mld snooping unknown-multicast mode 1464
ipv6 mld snooping version 1465
ipv6 mld snooping vlan immediate-leave 1466
ipv6 mld snooping vlan mrouter 1465
ipv6 mld snooping vlan static 1466
ipv6 mld static-group 1529
ipv6 mld version 1530
ipv6 mtu 1671
ipv6 multicast-data-drop 1475
ipv6 multicast-routing 1922
ipv6 nd dad attempts 1684
ipv6 nd managed-config-flag 1685
ipv6 nd ns-interval 1687
ipv6 nd other-config-flag 1686
ipv6 nd prefix 1690
ipv6 nd ra interval 1691
ipv6 nd ra lifetime 1692
ipv6 nd ra router-preference 1692
ipv6 nd ra suppress 1693
ipv6 nd raguard 1688
ipv6 nd reachable-time 1689
ipv6 nd snooping 1705
ipv6 nd snooping auto-detect 1706
ipv6 nd snooping auto-detect retransmit count 1707
ipv6 nd snooping auto-detect retransmit interval 1707
ipv6 nd snooping max-binding 1709
ipv6 nd snooping prefix timeout 1708
ipv6 nd snooping trust 1709
ipv6 neighbor 1683
ipv6 ospf cost 1806
ipv6 ospf dead-interval 1807
ipv6 ospf hello-interval 1808
ipv6 ospf priority 1808
ipv6 ospf retransmit-interval 1809
ipv6 ospf transmit-delay 1810
ipv6 pim 1951
ipv6 pim bsr-candidate 1961
ipv6 pim dr-priority 1968
ipv6 pim graft-retry-interval 1959
ipv6 pim hello-holdtime 1953
ipv6 pim hello-interval 1953
ipv6 pim join-prune-holdtime 1954
ipv6 pim join-prune-interval 1969
ipv6 pim lan-prune-delay 1954
ipv6 pim max-graft-retries 1960
ipv6 pim override-interval 1955
ipv6 pim propagation-delay 1956
ipv6 pim register-rate-limit 1962
ipv6 pim register-source 1963
ipv6 pim rp-address 1964
ipv6 pim rp-candidate 1965
ipv6 pim spt-threshold 1967
ipv6 pim state-refresh origination-interval 1960
ipv6 pim trigger-hello-delay 1957
ipv6 route 1730
ipv6 router ospf area 1804
ipv6 router ospf tag area 1805
ipv6 source-guard 1142
ipv6 source-guard binding 1140
ipv6 source-guard max-binding 1143

J

jumbo frame 911

L

l2protocol-tunnel tunnel-dmac 1360
lacp 1218
lacp admin-key (Ethernet Interface) 1220
lacp admin-key (Port Channel) 1222
lacp port-priority 1221
lacp system-priority 1222
lacp timeout 1223
lease 1639
line 924
lldp 1539
lldp admin-status 1543
lldp basic-tlv management-ip-address 1543
lldp basic-tlv port-description 1544
lldp basic-tlv system-capabilities 1545
lldp basic-tlv system-description 1545
lldp basic-tlv system-name 1546
lldp dot1-tlv proto-ident 1546
lldp dot1-tlv proto-vid 1547
lldp dot1-tlv pvid 1547
lldp dot1-tlv vlan-name 1548
lldp dot3-tlv link-agg 1548
lldp dot3-tlv mac-phy 1549
lldp dot3-tlv max-frame 1549
lldp holdtime-multiplier 1539
lldp med-fast-start-count 1540
lldp med-location civic-addr 1550
lldp med-notification 1551
lldp med-tlv inventory 1552
lldp med-tlv location 1553
lldp med-tlv med-cap 1553
lldp med-tlv network-policy 1554
lldp notification 1554
lldp notification-interval 1540
lldp refresh-interval 1541
lldp reinit-delay 1541
lldp tx-delay 1542
logging facility 934
logging history 934
logging host 935
logging on 936

logging sendmail 940
logging sendmail destination-email 942
logging sendmail host 941
logging sendmail level 941
logging sendmail source-email 943
logging trap 936
login 926
loopback detection trap 1262
loopback-detection 1260
loopback-detection action 1260
loopback-detection recover-time 1261
loopback-detection release 1263
loopback-detection transmit-interval 1262

M

ma index name 1570
ma index name-format 1571
mac access-group 1179
mac-address-table aging-time 1271
mac-address-table static 1272
mac-authentication intrusion-action 1106
mac-authentication max-mac-count 1106
mac-authentication reauth-time 1098
mac-learning 1090
mac-vlan 1378
major-domain 1311
management 1079
match 1410
match as-path 1902
match community 1902
match extcommunity 1903
match ip address 1904
match ip next-hop 1904
match ip route-source 1905
match metric 1905
match origin 1906
match pathlimit as 1906
match peer 1907
max-current-dd 1794
max-hops 1285
maximum-paths 1725
maximum-prefix 1736
media-type 1193
meg-level 1312
memory 1015
mep archive-hold-time 1584
mep crosscheck mpid 1588
mep fault-notify alarm-time 1596
mep fault-notify lowest-priority 1597
mep fault-notify reset-time 1598
mep-monitor 1312
mst priority 1286
mst vlan 1286
mvr 1479
mvr associated-profile 1479
mvr domain 1480
mvr immediate-leave 1486
mvr priority 1482
mvr profile 1481
mvr proxy-query-interval 1481
mvr proxy-switching 1483
mvr robustness-value 1484
mvr source-port-mode dynamic 1484
mvr type 1487
mvr upstream-source-ip 1485
mvr vlan 1486
mvr vlan group 1488
mvr6 associated-profile 1497
mvr6 domain 1498
mvr6 immediate-leave 1503
mvr6 profile 1498
mvr6 proxy-query-interval 1499
mvr6 proxy-switching 1500
mvr6 robustness-value 1501
mvr6 source-port-mode dynamic 1501
mvr6 type 1504
mvr6 upstream-source-ip 1502
mvr6 vlan 1503
mvr6 vlan group 1505

N

name 1287
negotiation 1194
neighbor 1737
neighbor activate 1859
neighbor advertisement-interval 1859
neighbor allowas-in 1860
neighbor attribute-unchanged 1861
neighbor capability orf prefix-list 1862
neighbor capability dynamic 1861
neighbor default-originate 1863
neighbor description 1864
neighbor distribute-list 1864
neighbor dont-capability-negotiate 1865
neighbor ebgp-multihop 1866
neighbor enforce-multihop 1866
neighbor filter-list 1867
neighbor interface 1868
neighbor maximum-prefix 1868
neighbor next-hop-self 1869
neighbor override-capability 1870
neighbor passive 1870
neighbor peer-group (Creating) 1871
neighbor peer-group (Group Members) 1872
neighbor port 1872
neighbor prefix-list 1873
neighbor remote-as 1874
neighbor remove-private-as 1874
neighbor route-map 1875
neighbor route-reflector-client 1876

neighbor route-server-client 1877
neighbor send-community 1878
neighbor shutdown 1878
neighbor soft-reconfiguration inbound 1879
neighbor strict-capability-match 1880
neighbor timers 1880
neighbor timers connect 1881
neighbor unsuppress-map 1882
neighbor update-source 1883
neighbor weight 1883
netbios-name-server 1640
netbios-node-type 1641
network 1641
network 1738
network 1848
network area 1768
network-access aging 1096
network-access dynamic-qos 1098
network-access dynamic-vlan 1100
network-access guest-vlan 1100
network-access link-detection 1101
network-access link-detection link-down 1102
network-access link-detection link-up 1102
network-access link-detection link-up-down 1103
network-access mac-filter 1097
network-access max-mac-count 1103
network-access mode mac-authentication 1104
network-access port-mac-filter 1105
next-server 1642
nlm 1012
no rspan session 1236
node-id 1313
non-erps-dev-protect 1314
non-revertive 1315
ntp authenticate 947
ntp authentication-key 948
ntp client 949
ntp server 950

O

on-match 1908

P

parity 927
passive-interface 1738
passive-interface 1777
passive-interface 1811
password 928
password-thresh 929
periodic 959
permit, deny 1450
permit, deny 1471
permit, deny (ARP ACL) 1182
permit, deny (Extended IPv4 ACL) 1166
permit, deny (Extended IPv6 ACL) 1172
permit, deny (MAC ACL) 1177
permit, deny (Standard IP ACL) 1165
permit, deny (Standard IPv6 ACL) 1171
ping 1654
ping6 1679
police flow 1413
police srtcm-color 1415
police trtcm-color 1417
policy-map 1411
port channel load-balance 1216
port monitor 1229
port security 1091
port security mac-address-as-permanent 1093
pppoe intermediate-agent 1081
pppoe intermediate-agent format-type 1082
pppoe intermediate-agent port-enable 1083
pppoe intermediate-agent port-format-type 1083
pppoe intermediate-agent trust 1084
pppoe intermediate-agent vendor-tag strip 1085
private vlan association 1368
private-vlan 1367
process cpu 1016
prompt 883
propagate-tc 1319
protocol-vlan protocol-group (Configuring Groups) 1372
protocol-vlan protocol-group (Configuring Interfaces) 1373
ptp adjust 961
ptp announce-receipt-timeout 966
ptp delay-mechanism 967
ptp domain-number 962
ptp e-latency 962
ptp in-latency 963
ptp log-announce-interval 968
ptp log-min-delay-request-interval 969
ptp log-min-pdelay-request-interval 969
ptp log-sync-interval 970
ptp mode 963
ptp port-enable 971
ptp port-release 973
ptp priority1 965
ptp priority2 966
ptp transport 971

Q

qos map cos-dscp 1393
qos map default-drop-precedence 1394
qos map dscp-cos 1395
qos map dscp-mutation 1396
qos map ip-port-dscp 1398
qos map ip-prec-dscp 1398
qos map phb-queue 1399
qos map trust-mode 1400
queue mode 1388
queue weight 1389
quit 886

R

radius-server acct-port 1036
radius-server auth-port 1037
radius-server host 1037
radius-server key 1038
radius-server retransmit 1039
radius-server timeout 1039
range 1451
range 1472
raps-def-mac 1320
raps-without-vc 1320
rate-limit 1240
rcommand 992
redistribute 1739
redistribute 1760
redistribute 1799
redistribute 1849
reload (Global Configuration) 884
reload (Privileged Exec) 888
rename 1411
revision 1288
ring-port 1322
rmon alarm 1018
rmon collection history 1020
rmon collection rmon1 1021
rmon event 1019
route-map 1899
router bgp 1832
router ipv6 ospf 1792
router ospf 1751
router pim 1928
router pim6 1951
router rip 1734
router-id 1754
router-id 1795
rpl neighbor 1323
rpl owner 1324
rspan destination 1234
rspan remote vlan 1235
rspan source 1233

S

server 1048
service dhcp 1634
service-policy 1421
set aggregator as 1908
set as-path 1909
set atomic-aggregate 1910
set comm-list delete 1910
set community 1911
set cos 1419
set extcommunity 1912
set ip next-hop 1913
set local-preference 1914
set metric 1914
set origin 1915
set originator-id 1916
set pathlimit ttl 1916
set phb 1420
set weight 1917
sflow owner 1025
sflow polling instance 1028
sflow sampling instance 1027
show access-group 1184
show access-list 1185
show access-list arp 1183
show access-list tcam-utilization 902
show accounting 1050
show alarm-status 902
show arp 1658
show auto-traffic-control 1256
show auto-traffic-control interface 1256
show banner 901
show bridge-ext 1341
show calendar 957
show class-map 1422
show cluster 993
show cluster candidates 994
show cluster members 993
show discard 1197
show dns 1621
show dns cache 1622
show dos-protection 1156
show dot1q-tunnel 1359
show dot1x 1076
show efm oam counters interface 1610
show efm oam event-log interface 1611
show efm oam remote-loopback interface 1612
show efm oam status interface 1613
show efm oam status remote interface 1613
show erps 1331
show ethernet cfm configuration 1574
show ethernet cfm errors 1585

show ethernet cfm fault-notify-generator 1599
show ethernet cfm linktrace-cache 1594
show ethernet cfm ma 1576
show ethernet cfm maintenance-points local 1576
show ethernet cfm maintenance-points local detail mep 1577
show ethernet cfm maintenance-points remote crosscheck 1590
show ethernet cfm maintenance-points remote detail 1579
show ethernet cfm md 1575
show garp timer 1341
show gvrp configuration 1342
show history 886
show hosts 1622
show interfaces brief 1197
show interfaces counters 1198
show interfaces history 1199
show interfaces protocol-vlan protocol-group 1374
show interfaces status 1202
show interfaces switchport 1203
show interfaces transceiver 1211
show interfaces transceiver-threshold 1212
show ip access-group 1169
show ip access-list 1169
show ip arp inspection configuration 1152
show ip arp inspection interface 1152
show ip arp inspection log 1153
show ip arp inspection statistics 1153
show ip arp inspection vlan 1153
show ip bgp 1884
show ip bgp attribute-info 1885
show ip bgp cidr-ony 1886
show ip bgp community 1886
show ip bgp community-info 1887
show ip bgp community-list 1888
show ip bgp dampening 1888
show ip bgp filter-list 1890
show ip bgp neighbors 1890
show ip bgp paths 1892
show ip bgp prefix-list 1892
show ip bgp regexp 1893
show ip bgp route-map 1893
show ip bgp scan 1894
show ip bgp summary 1894
show ip community-list 1895
show ip dhcp 1644
show ip dhcp binding 1644
show ip dhcp pool 1644
show ip dhcp snooping 1125
show ip dhcp snooping binding 1126
show ip extcommunity-list 1895
show ip helper 1662
show ip host-route 1726
show ip igmp authentication 1456
show ip igmp filter 1457
show ip igmp groups 1520
show ip igmp interface 1522
show ip igmp profile 1457
show ip igmp query-drop 1458
show ip igmp snooping 1442
show ip igmp snooping group 1443
show ip igmp snooping mrouter 1447
show ip igmp snooping mrouter 1926
show ip igmp snooping statistics 1444
show ip igmp throttle interface 1458
show ip interface 1651
show ip mroute 1920
show ip multicast-data-drop 1459
show ip ospf 1777
show ip ospf border-routers 1779
show ip ospf database 1780
show ip ospf interface 1786
show ip ospf neighbor 1787
show ip ospf route 1788
show ip ospf virtual-links 1789
show ip pim bsr-router 1947
show ip pim interface 1935
show ip pim neighbor 1936
show ip pim rp mapping 1948
show ip pim rp-hash 1949
show ip prefix-list 1896
show ip prefix-list detail 1896
show ip prefix-list summary 1897
show ip protocols ospf 1790
show ip protocols rip 1748
show ip rip 1749
show ip route 1726
show ip route database 1727
show ip route summary 1728
show ip source-guard 1139
show ip source-guard binding 1139
show ip ssh 1065
show ip telnet 1057
show ip traffic 1652
show ip traffic 1728
show ipv6 access-group 1175
show ipv6 access-list 1175
show ipv6 dhcp relay destination 1632
show ipv6 dhcp snooping 1132
show ipv6 dhcp snooping binding 1132
show ipv6 dhcp snooping statistics 1133
show ipv6 interface 1672
show ipv6 mld filter 1475
show ipv6 mld groups 1531
show ipv6 mld interface 1533
show ipv6 mld profile 1476
show ipv6 mld query-drop 1476
show ipv6 mld snooping group 1468
show ipv6 mld snooping group source-list 1468

show ipv6 mld snooping mrouter 1469
show ipv6 mld throttle interface 1477
show ipv6 mld snooping 1467
show ipv6 mroute 1923
show ipv6 mtu 1674
show ipv6 nd raguard 1694
show ipv6 nd snooping 1711
show ipv6 nd snooping binding 1711
show ipv6 nd snooping prefix 1711
show ipv6 neighbors 1694
show ipv6 ospf 1812
show ipv6 ospf database 1813
show ipv6 ospf interface 1814
show ipv6 ospf neighbor 1815
show ipv6 ospf route 1816
show ipv6 ospf virtual-links 1817
show ipv6 pim bsr-router 1970
show ipv6 pim interface 1957
show ipv6 pim neighbor 1958
show ipv6 pim rp mapping 1971
show ipv6 pim rp-hash 1972
show ipv6 route 1731
show ipv6 source-guard 1144
show ipv6 source-guard binding 1145
show ipv6 traffic 1675
show ipv6 tunnel 1702
show l2protocol-tunnel 1364
show lacp 1224
show line 932
show lldp config 1555
show lldp info local-device 1556
show lldp info remote-device 1557
show lldp info statistics 1560
show log 938
show logging 938
show logging sendmail 943
show loopback-detection 1263
show mac access-group 1180
show mac access-list 1180
show mac-address-table 1273
show mac-address-table aging-time 1274
show mac-address-table count 1275
show mac-vlan 1378
show management 1080
show memory 903
show mvr 1489
show mvr associated-profile 1490
show mvr interface 1491
show mvr members 1492
show mvr profile 1493
show mvr statistics 1494
show mvr6 1507
show mvr6 associated-profile 1508
show mvr6 interface 1509
show mvr6 members 1510
show mvr6 profile 1511
show mvr6 statistics 1511
show network-access 1107
show network-access mac-address-table 1108
show network-access mac-filter 1109
show nlm oper-status 1014
show ntp 951
show policy-map 1422
show policy-map interface 1423
show port monitor 1230
show port security 1093
show port-channel load-balance 1228
show pppoe intermediate-agent info 1086
show pppoe intermediate-agent statistics 1087
show process cpu 904
show protocol-vlan protocol-group 1374
show ptp configuration 974
show ptp foreign-master 974
show ptp information 975
show public-key 1065
show qos map cos-dscp 1401
show qos map dscp-cos 1402
show qos map dscp-mutation 1402
show qos map ip-port-dscp 1403
show qos map ip-prec-dscp 1404
show qos map phb-queue 1404
show qos map trust-mode 1405
show queue mode 1391
show queue weight 1391
show radius-server 1040
show reload 889
show rmon alarms 1022
show rmon events 1022
show rmon history 1022
show rmon statistics 1023
show route-map 1917
show rspan 1236
show running-config 904
show sflow 1029
show snmp 999
show snmp engine-id 1009
show snmp group 1010
show snmp notify-filter 1015
show snmp user 1011
show snmp view 1012
show snmp-server enable port-traps 1004
show sntp 947
show spanning-tree 1302
show spanning-tree mst configuration 1304
show ssh 1066
show startup-config 906
show subnet-vlan 1377
show synce 987
show system 906
show tacacs-server 1043
show tech-support 907

show time-range 960
show traffic-segmentation 1161
show udld 1268
show upgrade 923
show users 908
show version 909
show vlan 1352
show vlan private-vlan 1371
show vlan-translation 1366
show voice vlan 1385
show vrrp 1718
show vrrp interface 1720
show vrrp interface counters 1721
show vrrp router counters 1722
show watchdog 909
show web-auth 1114
show web-auth interface 1114
show web-auth summary 1115
shutdown 1194
silent-time 929
snmp-server 997
snmp-server community 997
snmp-server contact 998
snmp-server enable port-traps atc broadcast-alarm-clear 1252
snmp-server enable port-traps atc broadcast-alarm-fire 1252
snmp-server enable port-traps atc broadcast-control-apply 1253
snmp-server enable port-traps atc broadcast-control-release 1253
snmp-server enable port-traps atc multicast-alarm-clear 1254
snmp-server enable port-traps atc multicast-alarm-fire 1254
snmp-server enable port-traps atc multicast-control-apply 1255
snmp-server enable port-traps atc multicast-control-release 1255
snmp-server enable traps ethernet cfm cc 1583
snmp-server enable traps ethernet cfm crosscheck 1587
snmp-server enable port-traps mac-notification 1003
snmp-server enable traps 1000
snmp-server engine-id 1004
snmp-server group 1006
snmp-server host 1001
snmp-server location 998
snmp-server notify-filter 1013
snmp-server user 1007
snmp-server view 1008
sntp client 945
sntp poll 946
sntp server 946
spanning-tree 1278
spanning-tree bpdu-filter 1288
spanning-tree bpdu-guard 1289
spanning-tree cost 1290
spanning-tree edge-port 1291
spanning-tree forward-time 1279
spanning-tree hello-time 1279
spanning-tree link-type 1292
spanning-tree loopback-detection 1293
spanning-tree loopback-detection action 1293
spanning-tree loopback-detection release 1300
spanning-tree loopback-detection release-mode 1294
spanning-tree loopback-detection trap 1295
spanning-tree max-age 1280
spanning-tree mode 1281
spanning-tree mst configuration 1283
spanning-tree mst cost 1295
spanning-tree mst port-priority 1296
spanning-tree pathcost method 1282
spanning-tree port-bpdu-flooding 1297
spanning-tree port-priority 1298
spanning-tree priority 1283
spanning-tree protocol-migration 1301
spanning-tree root-guard 1298
spanning-tree spanning-disabled 1299
spanning-tree system-bpdu-flooding 1284
spanning-tree tc-prop-stop 1300
spanning-tree transmission-limit 1284
speed 930
stopbits 931
subnet-vlan 1376
summary-address 1761
switchport acceptable-frame-types 1346
switchport allowed vlan 1347
switchport block 1242
switchport dot1q-tunnel mode 1355
switchport dot1q-tunnel service match cvid 1356
switchport dot1q-tunnel tpid 1358
switchport forbidden vlan 1340
switchport gvrp 1340
switchport ingress-filtering 1348
switchport l2protocol-tunnel 1363
switchport mode 1349
switchport mode private-vlan 1369
switchport mtu 1195
switchport native vlan 1350
switchport packet-rate 1241
switchport priority default 1390
switchport private-vlan host-association 1370
switchport private-vlan mapping 1370
switchport vlan-translation 1364
switchport voice vlan priority 1383

switchport voice vlan 1382
switchport voice vlan rule 1383
switchport voice vlan security 1384
synce 980
synce auto-clock-source-selecting 983
synce clk-src-ssm 986
synce ethernet 981
synce ethernet clock-source 982
synce force-clock-source-selecting 984
synce ssm ethernet 985

T

tacacs-server host 1041
tacacs-server key 1041
tacacs-server port 1042
tacacs-server retransmit 1042
tacacs-server timeout 1043
timeout login response 931
time-range 957
timers basic 1740
timers bgp 1850
timers spf 1755
timers spf 1796
traceroute 1653
traceroute6 1681
traffic-segmentation 1157
traffic-segmentation session 1158
traffic-segmentation uplink/downlink 1159
traffic-segmentation uplink-to-uplink 1160
transceiver-threshold current 1206
transceiver-threshold rx-power 1207
transceiver-threshold temperature 1208
transceiver-threshold tx-power 1209
transceiver-threshold voltage 1210
transceiver-threshold-auto 1205
transceiver-threshold-monitor 1206
tunnel destination 1698
tunnel mode ipv6ip 1699
tunnel source vlan 1701
tunnel ttl 1702

U

udld aggressive 1266
udld message-interval 1265
udld port 1267
umount usbdisk 919
upgrade opcode auto 920
upgrade opcode path 921
upgrade opcode reload 922
username 1033

V

version 1325
version 1741
vlan 1344
vlan database 1343
vlan-trunking 1350
voice vlan 1379
voice vlan aging 1380
voice vlan mac-address 1381
vrrp authentication 1714
vrrp ip 1714
vrrp preempt 1715
vrrp priority 1716
vrrp timers advertise 1717

W

watchdog software 909
web-auth 1112
web-auth login-attempts 1110
web-auth quiet-period 1111
web-auth re-authenticate (IP) 1113
web-auth re-authenticate (Port) 1113
web-auth session-timeout 1111
web-auth system-auth-control 1112
whichboot 919
wtr-timer 1326

INDEX

NUMERICS

802.1Q tunnel 243, 1353
- access 250, 1355
- configuration, guidelines 246, 1353
- configuration, limitations 246, 1354
- CVID to SVID map 248, 1356
- description 243
- ethernet type 247, 1358
- interface configuration 250, 1355–1358
- mode selection 250, 1355
- status, configuring 247, 1354
- TPID 247, 1358
- uplink 250, 1355

802.1X
- authenticator, configuring 425, 1069–1075
- global settings 424, 1068–1069
- port authentication 423, 1067, 1069
- port authentication accounting 355, 356, 1049

A

AAA
- accounting 802.1X port settings 355, 356, 1049
- accounting exec command privileges 356, 1045
- accounting exec settings 355, 1049
- accounting summary 356, 1050
- accounting update 355, 1046
- accounting, configuring 355, 1044
- authorization & accounting 348, 1044
- authorization exec settings 361, 1047, 1050
- authorization method 361, 1050
- authorization settings 360, 1047
- authorization summary 362, 1050
- RADIUS group settings 356, 1048
- TACACS+ group settings 356, 1048

acceptable frame type 232, 1346

Access Control List *See* ACL

ACL 389, 1163
- ARP 395, 406, 1181
- binding to a port 408, 1168
- IPv4 Extended 395, 398, 1163, 1166
- IPv4 Standard 395, 397, 1163, 1165
- IPv6 Extended 395, 402, 1170, 1172
- IPv6 Standard 395, 400, 1170, 1171
- MAC 395, 404, 1176
- time range 391, 957

Address Resolution Protocol *See* ARP

address table 263, 1271
- address count, displaying 1275
- aging time 267, 1271
- aging time, displaying 267, 1274
- aging time, setting 267, 1271

administrative users, displaying 908

ARP
- ACL 406, 1147
- configuration 748, 1655
- description 748
- proxy 748, 1657
- statistics 753, 1652, 1728

ARP inspection 410, 1145
- ACL filter 413, 1147
- additional validation criteria 412, 1149
- ARP ACL 414, 1181
- enabling globally 412, 1146
- enabling per VLAN 414, 1150
- trusted ports 415, 1151

ATC 298, 951, 1243, 1704
- control response 301, 1248
- functional limitations 299, 1245
- limiting traffic rates 298, 1244
- shutting down a port 299, 1245
- thresholds 301, 1249, 1250
- timers 300, 1246
- usage 298, 1244

authentication
- MAC address authentication 368, 1095, 1104
- MAC, configuring ports 372, 1095
- network access 368, 1095, 1104
- public key 383, 1059
- web 365, 1112
- web authentication port information, displaying 367, 1114
- web authentication, configuring ports 367, 1112
- web authentication, re-authenticating address 367, 1113
- web authentication, re-authenticating ports 367, 1113
- web, configuring 366, 1112

Automatic Traffic Control *See* ATC

B

BGP
- aggregate address 1839
- AS path access list 1833
- cluster ID 1841
- community list 1834
- confederation ID 1842
- configuration guidelines 1827
- description 1818

extended community list 1836
external BGP 1819
internal BGP 1819
IP prefix list 1838
message types 1822
multihop for eBGP neighbors 1866
neighbor configuration 1859
neighbor peer group 1871, 1872
neighbor route map 1875
path attributes 1820
policy-based routing 1897
route map, configuring 1899
route map, neighbor 1875
route metrics 1853
route reflection 1840
route reflector client 1876
route reflectors 1824
route selection 1853
route server client 1877
route servers 1827
router ID 1847
BOOTP 692, 1648
bootstrap router
PIM-SM 842, 1938
PIMv6-SM 858, 1961
Border Gateway Protocol *See* BGP
BPDU 272
filter 285, 1288
flooding when STA disabled on VLAN 277, 1297
flooding when STA globally disabled 277, 1284
guard 285, 1289
ignoring superior BPDUs 284, 1298
selecting protocol based on message format 285, 1301
shut down port on receipt 285, 1289
bridge extension capabilities, displaying 153, 1341
broadcast packets, blocking 296, 1242
broadcast storm, threshold 296, 297, 1241

C

canonical format indicator 317
CDP
discard 1191
CFM
basic operations 550
continuity check errors 584, 1585
continuity check messages 539, 548, 550, 551, 1314, 1561, 1581, 1582
cross-check errors 1583, 1587, 1589
cross-check message 548, 551, 1561, 1586, 1587, 1588, 1589, 1590
cross-check start delay 552, 1586
delay measure request 572, 1600
description 548
domain service access point 548, 560, 565, 1568
fault isolation 548, 1593
fault notification 548, 583, 1561, 1596, 1597, 1598
fault notification generator 551, 557, 583, 1597, 1599
fault verification 548, 1561
link trace cache 581, 1591, 1593, 1594
link trace message 548, 550, 569, 1561, 1590, 1591, 1592
loop back messages 548, 550, 571, 1561, 1595
maintenance association 548, 560, 1561, 1570, 1576
maintenance domain 548, 549, 555, 1561, 1567, 1575
maintenance end point 549, 551, 556, 561, 565, 574, 575, 1569, 1571, 1576
maintenance intermediate point 549, 556, 577, 1567, 1568, 1570, 1576
maintenance level 549, 550, 1567
maintenance point 548, 1561, 1576
MEP archive hold time 558, 1584
MEP direction 565, 1571
remote maintenance end point 551, 560, 567, 575, 578, 579, 1577, 1579, 1584, 1588
service instance 548, 550, 1570
SNMP traps 1583, 1587
class map
description 1409
DiffServ 326, 1408
Class of Service *See* CoS
CLI
command modes 874
showing commands 872
clustering switches, management access 518, 990
command line interface *See* CLI
committed burst size, QoS policy 333, 334, 335, 1413, 1415, 1417
committed information rate, QoS policy 333, 334, 335, 1413, 1415, 1417
community ports 238, 1366
community string 117, 494, 997
community VLANs 239, 240, 242, 1367
configuration file, DHCP download reference 115
configuration files, restoring defaults 155, 912
configuration settings
restoring 119, 157, 158, 912, 914
saving 119, 157, 912, 914
Connectivity Fault Management *See* CFM
console port, required connections 106
continuity check errors, CFM 584, 1585
continuity check messages, CFM 539, 548, 550, 551, 1314, 1561, 1581, 1582
CoS 305, 313, 1400
configuring 305, 1387
default mapping to internal values 316, 1393
enabling 312, 1400
layer 3/4 priorities 312, 1392
priorities, mapping to internal values 316, 1393
queue mapping 309, 1399
queue mode 306, 1388
queue weights, assigning 308, 1389
CoS/CFI to PHB/drop precedence 316, 1393

CPU
- status 175, 904
- utilization, showing 175, 904

CPU utilization, setting trap 1016
cross-check errors, CFM 1583, 1587, 1589
cross-check message, CFM 548, 551, 1561, 1586, 1587, 1588, 1589, 1590
cross-check start delay, CFM 552, 1586
CVLAN to SPVLAN map 248, 1356

D

Daylight Savings Time *See* summer time
default IPv4 gateway, configuration 1650
default IPv6 gateway, configuration 696, 1664
default priority, ingress port 305, 1390
default settings, system 102
delay measure request, CFM 572, 1600
designated router
- PIM 835, 1945
- PIMv6 851, 1968

DHCP 692, 719, 1648
- address pool 726, 1634
- class identifier 720, 1625
- client 692, 1625, 1648
- client identifier 720, 1625
- dynamic configuration 113
- relay service 721, 1629
- relay service, enabling 722, 1630
- server 723, 1632

DHCP snooping 444, 1115
- enabling 446, 1116
- global configuration 446, 1116
- information option 446, 1118
- information option policy 447, 1119
- information option, circuit ID 449, 1122
- information option, enabling 446, 1118
- information option, remote ID 446, 1118
- information option, suboption format 446, 1118
- policy selection 447, 1119
- specifying trusted interfaces 449, 1123
- trusted port 449, 1123, 1130
- untrusted port 449, 1123, 1130
- verifying MAC addresses 446, 1120
- VLAN configuration 448, 1121

DHCPv6
- relay service, address 1631, 1632
- relay service, enabling 1631

DHCPv6 snooping 1126
- enabling 1126
- global configuration 1126
- specifying trusted interfaces 1130
- VLAN configuration 1129

Differentiated Code Point Service *See* DSCP
Differentiated Services *See* DiffServ
DiffServ 325, 1407
- binding policy to interface 339, 1421
- class map 326, 1408, 1412
- class map, description 1409
- classifying QoS traffic 326, 1410
- color aware, srTCM 334, 1415
- color aware, trTCM 335, 1417
- color blind, srTCM 334, 1415
- color blind, trTCM 335, 1417
- committed burst size 333, 334, 335, 1413, 1415, 1417
- committed information rate 333, 334, 335, 1413, 1415, 1417
- configuring 325, 1407
- conforming traffic, configuring response 333, 1413, 1415, 1417
- description 1409
- excess burst size 334, 1415
- metering, configuring 329, 330, 331, 1413
- peak burst size 335, 1417
- peak information rate 335, 1417
- policy map 329, 1411
- policy map, description 327, 332, 1409
- QoS policy 329, 1411
- service policy 339, 1421
- setting CoS for matching packets 333, 1419
- setting PHB for matching packets 333, 1420
- single-rate, three-color meter 330, 334, 1415
- srTCM metering 330, 334, 1415
- traffic between CIR and BE, configuring response 334, 1415
- traffic between CIR and PIR, configuring response 335, 1417
- trTCM metering 335, 1417
- two-rate, three-color meter 331, 1417
- violating traffic, configuring response 336, 1413, 1415, 1417

DNS
- default domain name 713, 1617
- displaying the cache 718, 1622
- domain name list 713, 1618
- enabling lookup 713, 1616
- name server list 713, 1619
- static entries, IPv4 717, 1618
- static entries, IPv6 717, 1620

Domain Name Service *See* DNS
domain service access point, CFM 548, 560, 565, 1568
DoS protection 431, 1154
downloading software 155, 914
- automatically 160, 920
- using FTP or TFTP 160, 914

DR priority, PIM-SM 837, 1945
DR priority, PIMv6-SM 853, 1968
drop precedence
- CoS priority mapping 317, 1393
- DSCP ingress map 314, 1396

DSA encryption 385, 387, 1063
DSCP 312, 313, 1400
- enabling 312, 1400
- mapping to internal values 314, 1396

DSCP ingress map, drop precedence 314, 1396
DSCP to PHB/drop precedence 314, 1396

dynamic addresses
  clearing 269, 1273
  displaying 268, 1273
Dynamic Host Configuration Protocol *See* DHCP
dynamic QoS assignment 369, 373, 1098
dynamic VLAN assignment 368, 373, 1100

E

ECMP, maximum paths 757, 1725
edge port, STA 284, 287, 1291
encryption
  DSA 385, 387, 1063
  RSA 385, 387, 1063
engine ID 483, 484, 1004
ERPS
  block ring port, manually 1327, 1329
  configuration guidelines 526, 1306
  control VLAN 531, 1308
  domain configuration 528, 1307
  domain, enabling 530, 1309
  forced mode 544, 1327
  global configuration 527, 1307
  guard timer 540, 1310
  hold-off timer 539, 1310
  major domain 536, 1311
  manual mode 544, 1329
  MEG level 531, 1312
  neighbor node 532, 1323
  node identifier 536, 1313
  node state 531, 1332
  node type 531, 1332
  non-compliant device protection 538, 1314
  non-revertive, from protection state 532, 1315
  propagate topology change 538, 1319
  protection state, clearing 547, 1327
  R-APS default MAC 538, 1320
  R-APS messages, using MAC 538, 1320
  R-APS with virtual channel 536, 1320
  R-APS, without virtual channel 536, 1320
  revertive recovery 532, 1315
  ring configuration 528, 1307
  ring port, east interface 529, 1322
  ring port, west interface 529, 1322
  ring, enabling 530, 1309
  RPL neighbor 532, 1323
  RPL owner 531, 1324
  secondary ring 536, 1311
  statistics, clearing 1326
  status, displaying 543, 1331
  version 530, 1325
  wait-to-block timer 540
  wait-to-restore timer 540, 1326
  WTB timer 540
  WTR timer 540, 1326
Ethernet Ring Protection Switching *See* ERPS
event logging 454, 933
excess burst size, QoS policy 334, 1415, 1417
exec command privileges, accounting 356, 1045
exec settings
  accounting 355, 1049
  authorization 361, 1047, 1050
external BGP 1819

F

fault isolation, CFM 548, 1593
fault notification generator, CFM 551, 557, 583, 1597, 1599
fault notification, CFM 548, 583, 1561, 1596, 1597, 1598
fault verification, CFM 548, 1561
FIB, description 1727
firmware
  displaying version 151, 909
  upgrading 155, 914
  upgrading automatically 160, 920
  upgrading with FTP or TFP 160, 914
  version, displaying 151, 909
forwarding information base *See* FIB

G

GARP VLAN Registration Protocol *See* GVRP
gateway, IPv4 default 1650
gateway, IPv6 default 696, 1664
general security measures 347, 1089
GNU license 1983
GVRP
  enabling 235, 1338
  global setting 235, 1338
  interface configuration 236, 1340

H

hardware version, displaying 151, 909
hash mask length, PIM-SM BSR 842, 1938
hash mask length, PIMv6-SM BSR 858, 1961
hello holdtime
  PIM 835, 1930
  PIMv6 851, 1953
hello interval
  PIM 835, 1931
  PIMv6 851, 1953
HTTP, web server 1052
HTTPS 378, 380, 1053
  configuring 378, 1053
  replacing SSL certificate 380, 914
  secure-site certificate 380, 914
  UDP port, configuring 379, 1053
HTTPS, secure server 378, 1053

I

IEEE 802.1D 271, 1281
IEEE 802.1s 271, 1281
IEEE 802.1w 271, 1281
IEEE 802.1X 423, 1067, 1069

IGMP
clearing groups 1519
enabling per interface 650, 1514
filter profiles, binding to interface 636, 1453
filter profiles, configuration 634, 1450
filter, interface configuration 636, 1453–1454
filter, parameters 634, 636, 1449–1454
filtering & throttling 633, 1448
filtering & throttling, enabling 633, 1449
filtering & throttling, interface configuration 636, 1451–1455
filtering & throttling, status 633, 1449
filtering, configuring profile 634, 1450, 1451
filtering, creating profile 634, 1450
filtering, group range 634, 1451
filtering, interface settings 1453–1454
groups, displaying 621, 654, 1443
interface configuration 650, 1514–1519
interface status, displaying 652, 1522
last member query interval 651, 1515
Layer 2 611, 1426
Layer 3 646, 1513
maximum response time 651, 1515
multicast groups, displaying 654, 1520
proxy 647, 1523
proxy routing 646, 1523
proxy routing, configuring 647, 1523
proxy routing, interface configuration 650, 1513
query 611, 613, 1429
query interval 651, 1516
query, enabling 616, 1429
report delay 651, 1515
robustness value 650, 1517
robustness variable 650, 1517
services, displaying 628, 654
showing groups 654, 1520
snooping 611, 1426
snooping & query, parameters 613, 1426
snooping, configuring 613, 1426
snooping, enabling 614, 1427
snooping, immediate leave 623, 1436
static groups, configuring 652, 1518
version 650, 1519
IGMP proxy
configuration steps 648
enabling 649, 1523
unsolicited report interval 649, 1524
IGMP snooping
configuring 621, 1426
enabling per interface 621, 623, 1427
forwarding entries 628, 1443
forwarding priority 616, 1428
immediate leave, status 623, 1436
interface attached to multicast router 619, 1447
last leave 613
last member query count 625, 1437
last member query interval 624, 1437
proxy query address 625, 1439
proxy query interval 624, 1440
proxy query response interval 624, 1441
proxy reporting 614, 624, 1428
querier timeout 616, 1430
querier, enabling 616, 1429
query suppression 613
router alert option 615, 1429
router port expire time 616, 1430
static host interface 612, 1442
static multicast routing 617, 1446, 1447
static port assignment 619, 1442
static router interface 612, 1447
static router port, configuring 617, 1447
statistics, displaying 629, 1444
TCN flood 614, 1431
unregistered data flooding 615, 1432
unsolitcited report interval 616, 1433
version exclusive 616, 1434
version for interface, setting 624, 1434
version, setting 616, 624, 1434
with proxy reporting 613, 1428
immediate leave, IGMP snooping 623, 1436
immediate leave, MLD snooping 640, 1466
importing user public keys 387, 914, 917
ingress filtering 232, 1348
internal BGP 1819
IP address
BOOTP/DHCP 692, 1627
setting 691, 1647
IP filter, for management access 418, 1079
IP Port to PHB/drop precedence 323, 1398
IP Precedence 313, 1400
enabling 312, 1400
IP precedence to PHB/drop precedence 320, 1398
IP routing 741, 769, 1723
configuring interfaces 744
maximum paths 757, 1725
unicast protocols 744, 1723
IP statistics 706, 1652, 1675, 1728
IPv4 address
BOOTP/DHCP 692, 1648
dynamic configuration 113
manual configuration 110
setting 109, 691, 1648
IPv4 source guard
configuring static entries 435, 1134
setting filter criteria 433, 1135
setting maximum bindings 434, 1137
IPv6
configuring static neighbors 1683
displaying neighbors 705, 1683, 1694
duplicate address detection 705, 1684, 1694
enabling 697, 1670
hop limit, router advertisements 1682
MTU 697, 1671
neighbor solicitation interval 698, 1687
reachability time 699, 1689
router advertisements, blocking 699, 1688
router advertisements, hop limit 1682

IPv6 address
- dynamic configuration (link-local) 114, 697, 1670
- EUI format 702, 1667
- EUI-64 setting 702, 1667
- explicit configuration 697, 1670
- global unicast 701, 1665
- link-local 702, 1669
- manual configuration (global unicast) 110, 701, 1665
- manual configuration (link-local) 110, 702, 1669
- setting 109, 695, 1665

IPv6 source guard
- configuring static entries 440, 1140
- setting filter criteria 438
- setting maximum bindings 439, 1143

IPv6/v4 tunnel 1696
- IPv4 destination, configured 1698
- mode, configured or 6to4 1699
- source VLAN 1701

J

jumbo frame 152, 911

K

key
- private 381, 1057
- public 381, 1057
- user public, importing 387, 914, 917

key pair
- host 381, 1057
- host, generating 385, 1063

L

LACP
- admin key 208, 1220
- configuration 207, 1215
- group attributes, configuring 211, 1222
- group members, configuring 209, 1218–1222
- local parameters 214, 1224
- partner parameters 216, 1224
- protocol message statistics 213, 1224
- protocol parameters 207, 1215
- timeout mode 208, 1223
- timeout, for LACPDU 208, 1223

last member query count, IGMP snooping 625, 1437

last member query interval, IGMP snooping 624, 1437

layer 2, protocol tunnel 1363

license information, GNU 1983

Link Layer Discovery Protocol - Media Endpoint Discovery *See* LLDP-MED

Link Layer Discovery Protocol *See* LLDP

link trace cache, CFM 581, 1591, 1593, 1594

link trace message, CFM 548, 550, 569, 1561, 1590, 1591, 1592

link type, STA 284, 287, 1292

LLDP 458, 1537
- device statistics details, displaying 480, 1560
- device statistics, displaying 478, 1560
- display device information 466, 470, 1557
- displaying remote information 470, 1557
- interface attributes, configuring 461, 1543–1554
- local device information, displaying 466, 1556
- message attributes 461, 1537
- message statistics 478, 1560
- remote information, displaying 477, 478, 1557
- remote port information, displaying 470, 1557
- timing attributes, configuring 459, 1539–1542
- TLV 458, 461
- TLV, 802.1 462, 1546–1548
- TLV, 802.3 462, 1548–1549
- TLV, basic 461, 1543–1546
- TLV, management address 461, 1543
- TLV, port description 462, 1544
- TLV, system capabilities 462, 1545
- TLV, system description 462, 1545
- TLV, system name 462, 1546

LLDP-MED 459, 1537
- end-node, extended power-via-MDI 475, 1559
- end-node, inventory 475, 1559
- end-node, location 474, 1559
- end-node, network policy 474, 1558
- notification, status 461, 1551
- TLV 463, 1537
- TLV, civic address 463, 464
- TLV, inventory 463, 1552
- TLV, location 463, 1550, 1553
- TLV, MED capabilities 463, 1553
- TLV, network policy 463, 1554

local engine ID 483, 1004

logging
- messages, displaying 455, 938
- syslog traps 456, 936
- to syslog servers 456, 935

log-in, web interface 124

logon authentication 363, 1031
- encryption keys 352, 1038, 1041
- RADIUS client 351, 1036
- RADIUS server 351, 1036
- sequence 349, 1034, 1035
- settings 350, 1035
- TACACS+ client 350, 1040
- TACACS+ server 350, 1040

logon authentication, settings 352, 1036, 1040

logon banner, configuring 892

loop back messages, CFM 548, 550, 571, 1561, 1595

loopback detection, non-STA 1259

loopback detection, STA 274, 1293

M

MAC address authentication 368, 1095
- ports, configuring 372, 1095, 1104
- reauthentication 371, 1098

main menu, web interface 126
maintenance association, CFM 548, 560, 1561, 1570, 1576
maintenance domain, CFM 548, 549, 555, 1561, 1567, 1575
maintenance end point, CFM 549, 551, 556, 561, 565, 574, 575, 1569, 1571, 1576
maintenance intermediate point, CFM 549, 556, 577, 1567, 1568, 1570, 1576
maintenance level, CFM 549, 550, 1567
maintenance point, CFM 548, 1561, 1576
management access, filtering per address 418, 1079
management access, IP filter 418, 1078, 1079
Management Information Bases (MIBs) 1978
matching class settings, classifying QoS traffic 327, 1410
media-type 183, 1193
memory
- status 176, 903
- utilization, showing 176, 903

memory utiilzation, setting trap 1015
MEP archive hold time, CFM 558, 1584
mirror port
- configuring local traffic 186, 1229
- configuring remote traffic 188, 1231

mirror port, configuring 186, 1229
MLD
- cache, clearing 1531
- enabling on VLAN 1525
- filter profiles, configuration 1471
- filtering & throttling 1469
- filtering & throttling, configuring profile 1471, 1472
- filtering & throttling, creating profile 1471
- filtering & throttling, enabling 1470
- filtering & throttling, interface configuration 1472–1474
- filtering & throttling, status 1470
- groups, displaying 1531
- last member query response interval 1526
- maximum response interval 1527
- proxy routing
- proxy routing, enabling 1534
- query interval 1528
- robustness value 1528
- static groups, binding 1529
- version 1530

MLD snooping 638, 1460
- configuring 638, 1460
- enabling 638, 1461
- groups, displaying 644, 645
- immediate leave 640, 1466
- immediate leave, status 640, 1466
- interface attached to multicast router 641, 642
- multicast static router port 641, 1465
- querier 638, 1461
- querier, enabling 638, 1461
- query interval 639, 1462
- query, maximum response time 639, 1462
- robustness value 639, 1463
- static port assignment 643, 1466
- static router port 641, 1465
- unknown multicast, handling 639, 1464
- version 639, 1465

MSTP 271, 289, 1281
- global settings, configuring 276, 289, 1277
- global settings, displaying 281, 1302
- interface settings, configuring 282, 293, 1278
- interface settings, displaying 294, 1302
- max hop count 279, 1285
- path cost 293, 1295
- region name 279, 1287
- region revision 279, 1288

MTU for IPv6 697, 1671
multicast filtering 609, 1425
- enabling IGMP snooping 614, 623, 1427
- enabling IGMP snooping per interface 621, 1427
- enabling MLD snooping 638, 1461
- router configuration 617, 1447

multicast for IPv6, filtering and throttling 1470
multicast groups 621, 628, 644, 654, 1443
- displaying 621, 628, 644, 654
- static 619, 621, 643, 644, 1442, 1443

Multicast Listener Discovery *See* MLD
Multicast Listener Discovery *See* MLD snooping
multicast router discovery 622, 1438
multicast router port, displaying 619, 642, 1447
multicast routing 825, 1919
- description 825
- enabling, IPv4 828, 1919
- enabling, IPv6 828, 1922
- global settings, IPv4 828, 1919
- global settings, IPv6 828, 1922
- PIM 833, 1927
- PIM-DM 833, 1927
- PIM-SM 833, 840, 1927
- PIMv6 849, 1950
- PIMv6-SM 856, 1961
- reverse path tree 826, 1946, 1969
- routing table, IPv4 829, 1920
- routing table, IPv6 1923
- upstream interface 829, 1921, 1924

multicast services
- configuring 619, 643, 1442
- displaying 621, 644, 1443

multicast static router port 617, 1447
- configuring 617, 1447
- configuring for MLD snooping 641, 1465

multicast storm, threshold 296, 297, 1241
Multicast VLAN Registration *See* MVR
multicast, filtering and throttling 633, 1449
multicast, static router port 617, 1925
MVR
- assigning static multicast groups 667, 1481, 1488
- configuring 660, 1478, 1486
- description 657
- interface status, configuring 665, 1486–1488

interface status, displaying 666, 1489
IP for control packets sent upstream 661, 1485
proxy query interval 659, 1481
proxy switching 658, 1483
receiver groups, displaying 669, 1492
robust value for proxy switching 659, 1484
setting interface type 666, 1487
setting multicast domain 660, 665, 1480
setting multicast groups 662, 1479, 1481
setting multicast priority 661, 1482
source port mode 659, 1484
specifying a domain 660, 665, 1480
specifying a VLAN 660, 1479, 1486
specifying priority 661, 1482
static binding 667, 1481, 1488
static binding, group to port 667, 1488
statistics, displaying 670, 1494
using immediate leave 666, 1486

MVR6
assigning static multicast groups 684, 1498, 1505
configuring 677, 1496, 1503
interface status, configuring 681, 1503–1505
interface status, displaying 683, 1509
IP for control packets sent upstream 678, 1502
proxy query interval 676
proxy switching 675, 1500
receiver groups, displaying 685, 1510
robust value for proxy switching 675, 1501
setting interface type 682, 1504
setting multicast domain 682, 1498
setting multicast groups 678, 1498
source port mode 676, 1501
specifying a domain 682, 1498
specifying a VLAN 677, 1503
static binding 684, 1498, 1505
static binding, group to port 684, 1505
statistics, displaying 686, 1511
using immediate leave 683, 1503

N

ND snooping
automatic validation 1706–1707
enabling 1705
max bindings 1709
trusted interface 1709

Neighbor Discovery Snooping *See* ND snooping

network access
authentication 368, 1095
dynamic QoS assignment 373, 1098
dynamic VLAN assignment 373, 1100
guest VLAN 372, 1100
MAC address filter 373, 1097
port configuration 372, 1104
reauthentication 371, 1098
secure MAC information 377, 1108, 1109

NTP
authentication keys, specifying 169, 948
setting the system clock 168, 949–951
specifying servers 168, 950

O

OAM
active mode 586, 1607
displaying settings and status 585, 1610–1613
enabling on switch ports 585, 1604
errored frame link events 1605–1606
event log, displaying 589, 1611
message statistics, displaying 588, 1610
mode selection 586, 1607
passive mode 586, 1607
remote device information, displaying 590, 1613
remote loop back test 591, 1609
setting to active mode 586, 1607
setting to passive mode 586, 1607

Open Shortest Path First *See* OSPF

Open Shortest Path First (Version 3) *See* OSPFv3

Operations, Administration and Maintenance *See* OAM

OSPF 788, 1750
ABR route summary 805, 1757
ABR/ASBR routing table, displaying 1779
area border router 790, 797, 799, 801, 803, 804, 805, 818, 1757
AS summary route 809, 1761
authentication key 813, 1770
authentication type 813, 1769
auto cost for an interface 794, 1758
autonomous system boundary router 794, 797, 799, 801, 804, 807, 809, 821, 1753
backbone 789, 790, 791, 799, 817, 819, 1768
configuration settings, displaying 796, 817, 1777
cost for interface 812, 1771
default cost for summary route 801, 803, 1756
default external route 795, 1753
default metric for external routes 794, 1759
enabling 791, 1751
general settings 793, 796, 1750
hello interval 812, 1772
interface summary information, displaying 817, 1786
LSA advertisement interval 813, 1775
LSA database, displaying 820, 1780
message digest key 814, 1773
neighboring router information, diplaying 1787
neighboring router information, displaying 823
network area 790, 1768
normal area 790, 1768
NSSA 798, 799, 804, 1762
process ID 791, 793, 798, 800, 803, 804, 806, 807, 810, 1751
process parameters, displaying 796, 1790
redistributing external routes 807, 1760
retransmit interval 813, 1775
RFC 1583 compatible 793, 1752
route summary, ABR 805, 1757

router ID 793, 1754
router priority 812, 1774
routing table, displaying 820, 1788
SPF timers 794, 1755
stub 798, 802, 1764
transit area 790, 791, 800, 802, 817, 818, 1765
transmit delay over interface 813, 1776
virtual link 817, 1765
virtual links, displaying 819, 1789
OSPFv3 1790
ABR route summary 1798
area border router 1798
backbone 1804, 1805
configuration settings, displaying 1812
enabling 1792
general settings 1790
interface summary information, displaying 1814
LSA database, displaying 1813
neighboring router information, displaying 1815
network area 1804
normal area 1804, 1805
process ID 1792
redistributing external routes 1799
route summary, ABR 1798
router ID 1795
routing table, displaying 1816
SPF timers 1796
stub 1801
transit area 1802
virtual link 1802
virtual links, displaying 1817

P

packet block
broadcast 297, 1242
multicast 296, 1242
unknown multicast 297, 1242
unknown unicast 296, 297, 1242
password, line 928
passwords 108, 363, 1032
administrator setting 363, 1033
path cost 287, 1290
method 278, 1282
STA 283, 287, 1282, 1290
peak burst size, QoS policy 335, 1417
peak information rate, QoS policy 335, 1417
per-hop behavior, DSCP ingress map 314, 1396
PHB/drop precedence to CoS/CFI 318, 1395
PIM 833, 1927
configuring 833, 1927
dense-mode attributes 837, 1927, 1936
designated router 835, 1945
enabling for interfaces 834, 835, 1929
enabling globally 833, 1928
hello holdtime 835, 1930
hello interval 835, 1931
interface settings 834, 1929–1946
neighbor routers, displaying 839, 1936
sparse-mode attributes 837, 1928, 1938
PIM-DM 833, 1927
configuring 833, 1927
global configuration 835–837, 840, 1928
interface settings 837, 1929–1936
neighbor routers 839, 1936
PIM-SM 833, 840, 1927
bootstrap router 842, 1938
BSR candidate 842, 1938
BSR elected, displaying 847, 1947, 1970
configuring 833, 840, 1927
DR priority 837, 1945
global configuration 837, 1928
hash mask length for BSR 842, 1938
interface settings 837, 1929–1936
neighbor routers 839, 1936
register rate limit for DR 840, 1939
rendezvous point 843, 1941, 1942
RP candidate 845, 1942
RP candidate, advertising 845, 1942
RP mapping, displaying 848, 1948, 1971
shared tree 841, 1921, 1924, 1944
shortest path tree 840, 1921, 1924, 1944
SPT threshold 840, 1944
static RP, configuring 843, 1941
PIMv6 849, 1950
configuring 849, 1950
dense mode, enabling 851, 1951
dense-mode attributes 853, 1950, 1959
designated router 851, 1968
enabling for interfaces 850, 1951
enabling globally 849, 1951
global configuration 849, 1951
graft retry interval 853, 1959
hello holdtime 851, 1953
hello interval 851, 1953
interface configuration, displaying 855
interface settings 850, 1951–1957, 1968–1969
max graft retries 853, 1960
neighbor routers 856, 1958
neighbor routers, displaying 856, 1958
prune delay 852, 1954
prune state, hold time 852, 1954
sparse-mode attributes 853, 1950, 1961
state refresh message interval 853, 1960
triggered hello delay 853, 1957
PIMv6-DM
global configuration 851, 856, 1928
interface settings 853, 1959
PIMv6-SM 856, 1961
bootstrap router 858, 1961
BSR candidate 858, 1961
BSR elected, displaying 863, 1970
configuring 856, 1961
DR priority 853, 1968
global configuration 853, 1961–1967
hash mask length for BSR 858, 1961
interface settings 853, 1968
register rate limit for DR 856, 1962

rendezvous point 859, 1964, 1965
RP candidate 861, 1965
RP candidate, advertising 861, 1965
RP mapping, displaying 865, 1971
shared tree 857, 1967
shortest path tree 857, 1967
SPT threshold 857, 1967
static RP, configuring 859, 1964
policing traffic, QoS policy 329, 333
policy map
description 332, 1409
DiffServ 329, 1411
port authentication 423, 1067, 1069
port priority
configuring 305, 1387
default ingress 305, 1390
STA 283, 1296, 1298
port security, configuring 420, 1090
ports
autonegotiation 183, 1194
broadcast storm threshold 296, 297, 1241
capabilities 183, 1189
configuring 182, 1187
discard CDP/PVST 1191
duplex mode 184
flow control 184, 1191
forced selection of media type 1193
forced selection of media-type 183
mirroring 186, 1229
mirroring local traffic 186, 1229
mirroring remote traffic 188, 1231
mtu 184, 1195
multicast storm threshold 296, 297, 1241
speed 184
statistics 192, 1198
transceiver threshold, auto-set 202, 1205
transceiver threshold, trap 202, 1206
unknown unicast storm threshold 296, 297, 1241
PPPoE 735–739
PPPoE IA 1081–1087
circuit-id 1083
enabling 1081
enabling per interace 1083
node identifier, setting 1082
remote-id 1083
trust mode 1084
primary VLAN 239, 240, 242, 1367
priority, default port ingress 305, 1390
private key 381, 1057
private VLANs, configuring 239, 1366
private VLANs, displaying 240, 1371
problems, troubleshooting 1981
promiscuous ports 238, 1366
protocol migration 285, 1301
protocol tunnel, layer 2 1363
protocol VLANs 251, 1371
configuring 252, 1371
configuring groups 252, 1372
configuring interfaces 253, 1373
group configuration 252, 1372
interface configuration 253, 1373
proxy ARP 748, 1657
proxy query address, IGMP snooping 625, 1439
proxy query interval, IGMP snooping 624, 1440
proxy query response interval, IGMP snooping 624, 1441
proxy reporting, IGMP snooping 624, 1428
PTP
foreign master 607, 974
interface settings 598, 966–971
public key 381, 1057
PVID, port native VLAN 232, 1350
PVLAN
association 240, 1368
community ports 238, 1366
configuring 239, 1366
displaying 240, 1371
interface configuration 242, 1369, 1370
primary VLAN 240, 1367
promiscuous ports 238, 1366
PVST, discard 1191

Q

QinQ Tunneling *See* 802.1Q tunnel
QoS 325, 1407
configuration guidelines 326, 1408
configuring 325, 1407
CoS/CFI to PHB/drop precedence 316, 1393
DSCP to PHB/drop precedence 314, 1396
dynamic assignment 373, 1098
IP Port to PHB/drop precedence 323, 1398
IP precedence to PHB/drop precedence 320, 1398
matching class settings 327, 1410
PHB to drop precedence, for untagged packets 1394
PHB to queue 309, 1399
PHB/drop precedence to CoS/CFI 318, 1395
selecting CoS, DSCP, IP Precedence 312, 1400
QoS policy
committed burst size 333, 334, 335, 1413, 1415, 1417
excess burst size 334, 1415
peak burst size 335, 1417
policing flow 329, 333
srTCM 330, 1415
srTCM police meter 334, 1415
trTCM 331, 1417
trTCM police meter 335, 1417
QoS policy, committed information rate 333, 334, 335, 1413, 1415, 1417
QoS policy, peak information rate 335, 1417
Quality of Service *See* QoS
queue mode, setting 306, 1388
queue weight, assigning to CoS 308, 1389

R

RADIUS
  logon authentication 351, 1036
  settings 351, 1036
rate limit
  port 295, 1240
  setting 295, 1239
register rate limit, PIM-SM 840, 1939
register rate limit, PIMv6-SM 856, 1962
remote engine ID 484, 1004
remote logging 456, 936
remote maintenance end point, CFM 551, 560, 567, 575, 578, 579, 1577, 1579, 1584, 1588
Remote Monitoring *See* RMON
rename, DiffServ 1411
rendezvous point
  PIM-SM 843, 1941, 1942
  PIMv6-SM 859, 1964, 1965
restarting the system 177, 884, 888, 889
  at scheduled times 177, 884
RIP 770, 1733
  authentication key 785, 1743
  authentication mode 784, 1742
  clearing routes 774, 1748
  configuration settings, displaying 1749
  configuring 770, 1734–1749
  default external route 772, 1734
  default metric 772, 1735
  description 769
  global settings 771, 1734–1740
  interface protocol settings 782, 1738–1747
  interface, enabling 775, 1738
  neighbor router 778, 787, 1737
  passively monitoring updates 777, 1738
  poison reverse 770, 785, 1747
  process parameters, displaying 1748
  protocol packets, receiving 784, 1745
  protocol packets, sending 784, 1746
  receive version 784, 1744
  redistributing external routing information 779, 1739
  routes, clearing 774, 1748
  routes, displaying 787, 1749
  routing table, clearing 774, 1748
  send version 784, 1745
  specifying interfaces 775, 1738
  split horizon 770, 785, 1747
  timers 773, 1740
  version 771, 1741
RMON 508, 1017
  alarm, displaying settings 511, 1022
  alarm, setting thresholds 509, 1018
  commands 1017
  event settings, displaying 513, 1022
  response to alarm setting 511, 1019
  statistics history, collection 513, 1020
  statistics history, displaying 515, 1022
  statistics, collection 516, 1021
  statistics, displaying 517, 1023
root guard 284, 1298
router alert option, IGMP snooping 615, 1429
router redundancy
  protocols 759, 1713
  VRRP 759, 1713
routing information base, description 1727
Routing Information Protocol *See* RIP
routing table, displaying 755, 1726
RSA encryption 385, 387, 1063
RSTP 271, 1281
  global settings, configuring 276, 1281
  global settings, displaying 281, 1302
  interface settings, configuring 282, 1288–1299
  interface settings, displaying 286, 1302
running configuration files, displaying 904

S

secure shell 381, 1057
  configuration 381, 1058
security, general measures 347, 1089
serial port, configuring 172, 923
service instance, CFM 548, 550, 1570
sFlow
  destination 1026
  owner 1025
  polling period 1028
  samping period 1027
  timeout 1026
shared tree
  PIM-SM 841, 1921, 1924, 1944
  PIMv6-SM 857, 1967
shortest path tree
  PIM-SM 840, 1921, 1924, 1944
  PIMv6-SM 857, 1967
Simple Mail Transfer Protocol *See* SMTP
Simple Network Management Protocol *See* SNMP
single rate three color meter *See* srTCM
SMTP
  event handling 457, 940
  sending log events 457, 940
SNMP 480, 995
  community string 494, 997
  enabling traps 500, 1000
  filtering IP addresses 418, 1079
  global settings, configuring 482, 997
  trap manager 500, 1001
  users, configuring 495, 497
SNMP traps, CFM 1583, 1587
SNMPv3 1004–1007
  engine ID 483, 484, 1004
  engine identifier, local 483, 1004
  engine identifier, remote 484, 1004
  groups 489, 1006
  local users, configuring 495, 1007
  remote users, configuring 497, 1007
  user configuration 495, 497, 1007
  views 486, 1008

SNTP
  setting the system clock 165, 945–947
  specifying servers 167, 946
software
  displaying version 151, 909
  downloading 155, 914
  version, displaying 151, 909
Spanning Tree Protocol *See* STA
specifications, software 1975
SPT threshold, PIM-SM 840, 1944
SPT threshold, PIMv6-SM 857, 1967
srTCM
  police meter 334, 1415
  QoS policy 330, 1415
SSH 381, 1057
  authentication retries 384, 1060
  configuring 381, 1058
  downloading public keys for clients 387, 914, 917
  generating host key pair 385, 1063
  server, configuring 384, 1060
  timeout 384, 1062
SSL, replacing certificate 380
STA 271, 1277
  BPDU filter 285, 1288
  BPDU flooding 277, 283, 1297
  BPDU shutdown 285, 1289
  detecting loopbacks 274, 1293
  edge port 284, 287, 1291
  forward delay 278, 1279
  global settings, configuring 276, 1278–1284
  global settings, displaying 281, 1302
  hello time 278, 1279
  interface settings, configuring 282, 1288–1299
  interface settings, displaying 286, 1302
  link type 284, 287, 1292
  loopback detection 274, 1293
  maximum age 278, 1280
  MSTP interface settings, configuring 293, 1295, 1296
  MSTP path cost 293, 1295
  path cost 283, 287, 1282, 1290
  path cost method 278, 1282
  port priority 283, 1296, 1298
  port/trunk loopback detection 274, 1293
  protocol migration 285, 1301
  transmission limit 278, 1284
standards, IEEE 1977
startup files
  creating 155, 914
  displaying 155, 906, 919
  setting 155, 913
static addresses, setting 265, 1272
static routes, configuring 753, 1724
statistics
  ARP 753, 1652, 1728
  history for port 196, 1199
  history for trunk 196, 1199
  ICMP 1652, 1728
  IP 1652, 1728
  port 192, 1198
  TCP 1652, 1728
  UDP 1652, 1728
  VLAN 1198
STP 276, 1281
  Also see STA
summary, accounting 356, 1050
summer time, setting 951–954
switch clustering, for management 518, 989
switch settings
  restoring 157, 912
  saving 157, 912
SyncE
  automatic clock source selection 983
  clock source selection 982
  clock source selection, forced 984
  clock source selection, SSM 986
  enabling on compatible ports 980, 981
  SSM, enabling 985
  Synchronization Status Messages (SSM) 985
Synchronous Ethernet 979
Synchronous Ethernet *See* SyncE
system clock
  setting 164, 944
  setting manually 164, 956
  setting the time zone 171, 955
  setting with NTP 168, 949–951
  setting with SNTP 165, 945–947
  summer time 951–954
system logs 454, 936
system software, downloading from server 155, 914

T

TACACS+
  logon authentication 350, 1040
  settings 352, 1040
TCN
  flood 614, 1431
  general query solicitation 615, 1432
Telnet
  configuring 174, 1055
  server, enabling 174, 1056
telnet connection, configuring 174, 923
time range, ACL 391, 957
time zone, setting 171, 955
time, setting 164, 944
TPID 247, 1358
traffic segmentation 219, 1157
  assigning ports 219, 1157, 1158, 1159
  enabling 219, 1157, 1158, 1159
  sessions, assigning ports 221, 1157, 1158, 1159
  sessions, creating 220, 1157, 1158, 1159
transceiver data, displaying 200
transceiver thresholds
  configuring 201, 1206–1210
  displaying 201, 1211–1212
trap manager 118, 500, 1001
troubleshooting 1981

trTCM
- police meter 335, 1417
- QoS policy 331, 1417

trunk
- configuration 204, 1215
- LACP 207, 1215, 1218
- load balancing 1216
- static 205, 1218

tunneling unknown VLANs, VLAN trunking 222, 1350
two rate three color meter *See* trTCM
Type Length Value *See* LLDP TLV

U

UDP helper 730, 1659
- application port 731, 1659
- application server 733, 1661
- description 730
- destination port 731, 1659
- enabling 731, 1660
- forward destination 733, 1661
- target subnet 733, 1661
- UDP ports 731, 1659

unicast routing 769, 1723
- ECMP 757, 1725
- ECMP maximum paths 757, 1725

unidirectional link detection 1265
unknown multicast packets, blocking 296, 1242
unknown unicast packets, blocking 296, 1242
unknown unicast storm, threshold 296, 297, 1241
unregistered data flooding, IGMP snooping 615, 1432
upgrading software 155, 914, 920
upstream interface, multicast route 829, 1921, 1924
user account 363, 1032, 1033
user password 363, 1032, 1033

V

VLAN trunking 222, 1350
VLANs 225–261, 1337–1385
- 802.1Q tunnel mode 250, 1355
- acceptable frame type 232, 1346
- adding static members 231, 1347
- basic information, displaying 1341
- configuring port members, by interface 1346–1350
- configuring port members, VLAN index 234
- creating 228, 1344
- description 225, 261
- displaying port members 234, 1352
- displaying port members by interface 234
- displaying port members by interface range 235
- displaying port members by VLAN index 234
- dynamic assignment 373, 1100
- egress mode 231, 1349
- ingress filtering 232, 1348
- interface configuration 231, 1346–1350
- IP subnet-based 256, 1375
- MAC-based 258, 1377
- port members, displaying 234, 1352
- private 238, 1366
- protocol 251, 1371
- protocol, configuring 252, 1371
- protocol, configuring groups 252, 1372
- protocol, configuring interfaces 253, 1373
- protocol, group configuration 252, 1372
- protocol, interface configuration 253, 1373
- PVID 232, 1350
- statistics 1198
- tag swapping 259, 1364
- translation, customer and service provider 259, 1364
- tunneling unknown groups 222, 1350
- voice 341, 1379

voice VLANs 341, 1379
- detecting VoIP devices 342, 1379
- enabling for ports 345, 1382–1384
- identifying client devices 343, 1381

VoIP traffic 341, 1379
- ports, configuring 345, 1382–1384
- telephony OUI, configuring 343, 1381
- voice VLAN, configuring 342, 1379

VoIP, detecting devices 345, 1383
VRRP 759, 1713
- authentication 763, 1714
- configuration settings 759, 760, 1713
- group statistics 767, 1718
- preemption 761, 762, 1715
- priority 761, 762, 1716
- protocol message statistics 766, 1722
- timers 762, 1717
- virtual address 760, 1714

W

web authentication 365, 1112
- address, re-authenticating 367, 1113
- configuring 366, 1112
- configuring ports 367, 1112
- port information, displaying 367, 368, 1114
- ports, configuring 367, 1112
- ports, re-authenticating 367, 1113

web interface
- access requirements 123
- configuration buttons 125
- home page 124
- menu list 126
- panel display 125

ECS4660-28F
E102013/ST-R03
149100000140A