Edge-corE®

ECS4610-24F
24-Port Layer 3
Gigabit Ethernet Switch

Management Guide

www.edge-core.com

Management Guide

ECS4610-24F Gigabit Ethernet Switch

Layer 3 Switch,
with 22 1000BASE-X SFP Ports,
and 2 Combination Gigabit Ports (RJ-45/SFP)

ECS4610-24F
E052010/ST-R01
149100000092A

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.

May 2010 Release

This is the first release of this guide. This guide is valid for software release v1.1.2.0.

CONTENTS

ABOUT THIS GUIDE 5

CONTENTS 7

FIGURES 37

TABLES 49

SECTION I GETTING STARTED 55

1 INTRODUCTION 57

Key Features 57

Description of Software Features 58

Configuration Backup and Restore 58

Authentication 58

Access Control Lists 59

DHCP 59

Port Configuration 59

Port Mirroring 59

Port Trunking 59

Rate Limiting 60

Broadcast Storm Control 60

Static Addresses 60

IEEE 802.1D Bridge 60

Store-and-Forward Switching 60

Spanning Tree Algorithm 60

Virtual LANs 61

IEEE 802.1Q Tunneling (QinQ) 61

Traffic Prioritization 62

Quality of Service 62

IP Routing 62

Equal-cost Multipath Load Balancing 63

Router Redundancy 63

Address Resolution Protocol 63
Multicast Filtering 63
Multicast Routing 63
Tunneling 64
System Defaults 64
2 INITIAL SWITCH CONFIGURATION 67
Connecting to the Switch 67
Configuration Options 67
Required Connections 68
Remote Connections 69
Basic Configuration 70
Console Connection 70
Setting Passwords 70
Setting an IP Address 71
Enabling SNMP Management Access 73
Managing System Files 75
Saving or Restoring Configuration Settings 76
SECTION II WEB CONFIGURATION 79
3 USING THE WEB INTERFACE 81
Connecting to the Web Interface 81
Navigating the Web Browser Interface 82
Home Page 82
Configuration Options 83
Panel Display 83
Main Menu 84
4 BASIC MANAGEMENT TASKS 101
Displaying System Information 101
Displaying Switch Hardware/Software Versions 103
Configuring Support for Jumbo Frames 104
Displaying Bridge Extension Capabilities 105
Managing System Files 106
Copying Files via FTP/TFTP or HTTP 106
Saving the Running Configuration to a Local File 108
Setting The Start-Up File 110

Showing System Files 110

Setting the System Clock 111

Setting the Time Manually 111

Configuring SNTP 112

Specifying SNTP Time Servers 113

Setting the Time Zone 114

Console Port Settings 115

Telnet Settings 117

Displaying CPU Utilization 118

Displaying Memory Utilization 119

Resetting the System 120

5 INTERFACE CONFIGURATION 125

Port Configuration 125

Configuring by Port List 125

Configuring by Port Range 128

Displaying Connection Status 128

Configuring Port Mirroring 130

Showing Port or Trunk Statistics 131

Trunk Configuration 135

Configuring a Static Trunk 136

Configuring a Dynamic Trunk 139

Displaying LACP Port Counters 144

Displaying LACP Settings and Status for the Local Side 145

Displaying LACP Settings and Status for the Remote Side 147

Traffic Segmentation 149

Enabling Traffic Segmentation 149

Configuring Uplink and Downlink Ports 150

VLAN Trunking 151

6 VLAN CONFIGURATION 153

IEEE 802.1Q VLANs 153

Configuring VLAN Groups 156

Adding Static Members to VLANs 158

Configuring Dynamic VLAN Registration 163

Private VLANs 166

Creating Private VLANs 167

Associating Private VLANs 168

Configuring Private VLAN Interfaces 169

IEEE 802.1Q Tunneling 171

Enabling QinQ Tunneling on the Switch 175

Adding an Interface to a QinQ Tunnel 176

Protocol VLANs 177

Configuring Protocol VLAN Groups 178

Mapping Protocol Groups to Interfaces 180

Configuring IP Subnet VLANs 182

Configuring MAC-based VLANs 184

7 ADDRESS TABLE SETTINGS 187

Configuring MAC Address Learning 187

Setting Static Addresses 189

Changing the Aging Time 190

Displaying the Dynamic Address Table 191

Clearing the Dynamic Address Table 192

8 SPANNING TREE ALGORITHM 195

Overview 195

Configuring Loopback Detection 198

Configuring Global Settings for STA 199

Displaying Global Settings for STA 204

Configuring Interface Settings for STA 205

Displaying Interface Settings for STA 209

Configuring Multiple Spanning Trees 212

Configuring Interface Settings for MSTP 216

9 RATE LIMIT CONFIGURATION 219

10 STORM CONTROL CONFIGURATION 221

11 QUALITY OF SERVICE 223

Overview 223

Configuring a Class Map 224

Creating QoS Policies 227

Attaching a Policy Map to a Port 237

12 VOIP TRAFFIC CONFIGURATION 239

Overview 239

Configuring VoIP Traffic 239

Configuring Telephony OUI 241

Configuring VoIP Traffic Ports 242

13 SECURITY MEASURES 245

AAA Authorization and Accounting 246

Configuring Local/Remote Logon Authentication **247**

Configuring Remote Logon Authentication Servers 248

Configuring AAA Accounting 253

Configuring AAA Authorization 258

Configuring User Accounts 261

Network Access (MAC Address Authentication) 262

Configuring Global Settings for Network Access 265

Configuring Network Access for Ports 266

Configuring Port Link Detection 268

Configuring a MAC Address Filter 269

Displaying Secure MAC Address Information 270

Configuring HTTPS 272

Configuring Global Settings for HTTPS 272

Replacing the Default Secure-site Certificate 274

Configuring the Secure Shell 275

Configuring the SSH Server 278

Generating the Host Key Pair 279

Importing User Public Keys 281

Access Control Lists 283

Setting A Time Range 284

Setting the ACL Name and Type 286

Configuring a Standard IPv4 ACL 288

Configuring an Extended IPv4 ACL 289

Configuring a Standard IPv6 ACL 292

Configuring an Extended IPv6 ACL 293

Configuring a MAC ACL 296

Configuring an ARP ACL 298

Binding a Port to an Access Control List 300

ARP Inspection 301

Configuring Global Settings for ARP Inspection 302

Configuring VLAN Settings for ARP Inspection 304

Configuring Interface Settings for ARP Inspection 306

Displaying ARP Inspection Statistics 307

Displaying the ARP Inspection Log 308

Filtering IP Addresses for Management Access 309

Configuring Port Security 311

Configuring 802.1X Port Authentication 313

Configuring 802.1X Global Settings 314

Configuring Port Settings for 802.1X 316

Displaying 802.1X Statistics 320

IP Source Guard 321

Configuring Ports for IP Source Guard 321

Configuring Static Bindings for IP Source Guard 323

Displaying Information for Dynamic IP Source Guard Bindings 325

DHCP Snooping 326

DHCP Snooping Configuration 329

DHCP Snooping VLAN Configuration 330

Configuring Ports for DHCP Snooping 331

Displaying DHCP Snooping Binding Information 332

14 BASIC ADMINISTRATION PROTOCOLS 335

Configuring Event Logging 335

System Log Configuration 335

Remote Log Configuration 337

Sending Simple Mail Transfer Protocol Alerts 339

Link Layer Discovery Protocol 340

Setting LLDP Timing Attributes 340

Configuring LLDP Interface Attributes 342

Displaying LLDP Local Device Information 345

Displaying LLDP Remote Port Information 347

Displaying Device Statistics 352

Simple Network Management Protocol 354

Configuring Global Settings for SNMP 356

Setting the Local Engine ID 357

Specifying a Remote Engine ID 358

Setting SNMPv3 Views 360

Configuring SNMPv3 Groups 363

Setting Community Access Strings 366

Configuring Local SNMPv3 Users 368

Configuring Remote SNMPv3 Users 370

Specifying Trap Managers 372

Remote Monitoring 376

Configuring RMON Alarms 377

Configuring RMON Events 380

Configuring RMON History Samples 382

Configuring RMON Statistical Samples 384

15 MULTICAST FILTERING 387

Overview 387

IGMP Protocol 388

Layer 2 IGMP (Snooping and Query) 389

Configuring IGMP Snooping and Query Parameters 391

Specifying Static Interfaces for a Multicast Router 395

Assigning Interfaces to Multicast Services 397

Setting IGMP Snooping Status per Interface 399

Displaying Multicast Groups Discovered by IGMP Snooping 404

Filtering and Throttling IGMP Groups 405

Enabling IGMP Filtering and Throttling 405

Configuring IGMP Filter Profiles 406

Configuring IGMP Filtering and Throttling for Interfaces 409

Layer 3 IGMP (Query used with Multicast Routing) 410

Configuring IGMP Proxy Routing 411

Configuring IGMP Interface Parameters 413

Configuring Static IGMP Group Membership 416

Displaying Multicast Group Information 418

Multicast VLAN Registration 420

Configuring Global MVR Settings 422

Configuring the MVR Group Range 423

Configuring MVR Interface Status 424

Assigning Static Multicast Groups to Interfaces 427

Showing Multicast Groups Assigned to Interfaces 428

16 IP CONFIGURATION 431

Setting the Switch’s IP Address (IP Version 4) 431

17 GENERAL IP ROUTING 435

Overview 435

Initial Configuration 435

IP Routing and Switching 436

Routing Path Management 437

Routing Protocols 438
Configuring IP Routing Interfaces 438
Configuring Local and Remote Interfaces 438
Using the Ping Function 439
Using the Trace Route Function 440
Address Resolution Protocol 441
Basic ARP Configuration 442
Configuring Static ARP Addresses 444
Displaying Dynamic or Local ARP Entries 445
Displaying ARP Statistics 446
Configuring Static Routes 447
Displaying the Routing Table 449
Equal-cost Multipath Routing 450
18 CONFIGURING ROUTER REDUNDANCY 453
Configuring VRRP Groups 454
Displaying VRRP Global Statistics 460
Displaying VRRP Group Statistics 461
19 IP SERVICES 463
Domain Name Service 463
Configuring General DNS Service Parameters 463
Configuring a List of Domain Names 464
Configuring a List of Name Servers 466
Configuring Static DNS Host to Address Entries 467
Displaying the DNS Cache 468
Dynamic Host Configuration Protocol 469
Configuring DHCP Relay Service 470
Configuring the DHCP Server 471
Forwarding UDP Service Requests 478
Enabling the UDP Helper 478
Specifying UDP Destination Ports 479
Specifying The Target Server or Subnet 480
20 UNICAST ROUTING 483
Overview 483
Configuring the Routing Information Protocol 484
Configuring General Protocol Settings 485
Clearing Entries from the Routing Table 488

Specifying Network Interfaces 489
Specifying Passive Interfaces 491
Specifying Static Neighbors 492
Configuring Route Redistribution 493
Specifying an Administrative Distance 495
Configuring Network Interfaces for RIP 496
Displaying RIP Interface Settings 500
Displaying Peer Router Information 501
Resetting RIP Statistics 502
Configuring the Open Shortest Path First Protocol (Version 2) 502
Defining Network Areas Based on Addresses 504
Configuring General Protocol Settings 507
Displaying Adminstrative Settings and Statistics 510
Adding an NSSA or Stub 512
Configuring NSSA Settings 513
Configuring Stub Settings 516
Displaying Information on NSSA and Stub Areas 518
Configuring Area Ranges (Route Summarization for ABRs) 519
Redistributing External Routes 521
Configuring Summary Addresses (for External AS Routes) 523
Configuring OSPF Interfaces 525
Configuring Virtual Links 531
Displaying Link State Database Information 534
Displaying Information on Virtual Links 536
Displaying Information on Neighboring Routers 538
21 MULTICAST ROUTING 541
Overview 541
Configuring Global Settings for Multicast Routing 544
Enabling Multicast Routing Globally 544
Displaying the Multicast Routing Table 544
Configuring PIM for IPv4 548
Enabling PIM Globally 548
Configuring PIM Interface Settings 548
Displaying Neighbor Information 554
Configuring Global PIM-SM Settings 554
Configuring a BSR Candidate 556

Configuring a Static Rendezvous Point 557
Configuring an RP Candidate 559
Displaying the BSR Router 561
Displaying RP Mapping 563

SECTION III COMMAND LINE INTERFACE 565

22 USING THE COMMAND LINE INTERFACE 567
Accessing the CLI 567
Console Connection 567
Telnet Connection 568
Entering Commands 569
Keywords and Arguments 569
Minimum Abbreviation 569
Command Completion 569
Getting Help on Commands 570
Partial Keyword Lookup 571
Negating the Effect of Commands 571
Using Command History 571
Understanding Command Modes 572
Exec Commands 572
Configuration Commands 573
Command Line Processing 575
CLI Command Groups 576
23 GENERAL COMMANDS 579
prompt 579
reload (Global Configuration) 580
enable 581
quit 582
show history 582
configure 583
disable 584
reload (Privileged Exec) 584
show reload 585
end 585
exit 585

24 SYSTEM MANAGEMENT COMMANDS 587
Device Designation 587
hostname 588
System Status 588
show running-config 588
show startup-config 590
show system 590
show users 591
show version 592
Frame Size 592
jumbo frame 592
File Management 593
boot system 594
copy 595
delete 598
dir 598
whichboot 599
Line 600
line 600
databits 601
exec-timeout 602
login 603
parity 604
password 604
password-thresh 605
silent-time 606
speed 606
stopbits 607
timeout login response 608
disconnect 608
show line 609
Event Logging 610
logging facility 610
logging history 611
logging host 612
logging on 612

logging trap 613

clear log 613

show log 614

show logging 615

SMTP Alerts 616

logging sendmail 617

logging sendmail host 617

logging sendmail level 618

logging sendmail destination-email 618

logging sendmail source-email 619

show logging sendmail 619

Time 620

sntp client 620

sntp poll 621

sntp server 622

show sntp 622

clock timezone 623

calendar set 624

show calendar 624

Time Range 625

time-range 625

absolute 626

periodic 626

25 SNMP COMMANDS 629

snmp-server 630

snmp-server community 630

snmp-server contact 631

snmp-server location 631

show snmp 632

snmp-server enable traps 633

snmp-server host 634

snmp-server engine-id 636

snmp-server group 637

snmp-server user 639

snmp-server view 640

show snmp engine-id 641

show snmp group 642
show snmp user 643
show snmp view 644
nlm 644
snmp-server notify-filter 645
show nlm oper-status 646
show snmp notify-filter 647
26 REMOTE MONITORING COMMANDS 649
rmon alarm 650
rmon event 651
rmon collection history 652
rmon collection stats 653
show rmon alarm 654
show rmon event 654
show rmon history 654
show rmon statistics 655
27 AUTHENTICATION COMMANDS 657
User Accounts 657
enable password 658
username 659
Authentication Sequence 660
authentication enable 660
authentication login 661
RADIUS Client 662
radius-server acct-port 662
radius-server auth-port 663
radius-server host 663
radius-server key 664
radius-server retransmit 665
radius-server timeout 665
show radius-server 666
TACACS+ Client 666
tacacs-server 667
tacacs-server host 667
tacacs-server key 668
tacacs-server port 668

show tacacs-server 669

AAA 669

aaa accounting commands 670

aaa accounting dot1x 671

aaa accounting exec 672

aaa accounting update 673

aaa authorization exec 673

aaa group server 674

server 675

accounting dot1x 675

accounting exec 676

authorization exec 676

show accounting 677

Web Server 678

ip http port 678

ip http server 679

ip http secure-server 679

ip http secure-port 681

Telnet Server 681

ip telnet max-sessions 682

ip telnet port 682

ip telnet server 683

show ip telnet 683

Secure Shell 684

ip ssh authentication-retries 687

ip ssh server 687

ip ssh server-key size 688

ip ssh timeout 688

delete public-key 689

ip ssh crypto host-key generate 689

ip ssh crypto zeroize 690

ip ssh save host-key 691

show ip ssh 691

show public-key 692

show ssh 693

802.1X Port Authentication 693

dot1x default 694

dot1x eapol-pass-through 694

dot1x system-auth-control 695

dot1x intrusion-action 695

dot1x max-req 696

dot1x operation-mode 697

dot1x port-control 698

dot1x re-authentication 698

dot1x timeout quiet-period 699

dot1x timeout re-authperiod 699

dot1x timeout supp-timeout 700

dot1x timeout tx-period 700

dot1x re-authenticate 701

show dot1x 702

Management IP Filter 704

management 705

show management 706

28 GENERAL SECURITY MEASURES 707

Port Security 708

mac-learning 708

port security 709

Network Access (MAC Address Authentication) 711

network-access aging 712

network-access mac-filter 712

mac-authentication reauth-time 713

network-access dynamic-qos 714

network-access dynamic-vlan 715

network-access guest-vlan 715

network-access link-detection 716

network-access link-detection link-down 717

network-access link-detection link-up 717

network-access link-detection link-up-down 718

network-access max-mac-count 718

network-access mode mac-authentication 719

network-access port-mac-filter 720

mac-authentication intrusion-action 721

mac-authentication max-mac-count 721

show network-access 722

show network-access mac-address-table 723

show network-access mac-filter 724

DHCP Snooping 724

ip dhcp snooping 725

ip dhcp snooping database flash 727

ip dhcp snooping information option 727

ip dhcp snooping information policy 728

ip dhcp snooping verify mac-address 729

ip dhcp snooping vlan 729

ip dhcp snooping trust 730

clear ip dhcp snooping database flash 731

show ip dhcp snooping 732

show ip dhcp snooping binding 732

IP Source Guard 733

ip source-guard binding 733

ip source-guard 735

ip source-guard max-binding 736

show ip source-guard 737

show ip source-guard binding 737

ARP Inspection 738

ip arp inspection 739

ip arp inspection filter 740

ip arp inspection log-buffer logs 741

ip arp inspection validate 742

ip arp inspection vlan 742

ip arp inspection limit 743

ip arp inspection trust 744

show ip arp inspection configuration 744

show ip arp inspection interface 745

show ip arp inspection log 745

show ip arp inspection statistics 746

show ip arp inspection vlan 746

29 ACCESS CONTROL LISTS 747

IPv4 ACLs 747

access-list ip 748

permit, deny (Standard IP ACL) 749

permit, deny (Extended IPv4 ACL) 750

ip access-group 752

show ip access-group 753

show ip access-list 753

IPv6 ACLs 754

access-list ipv6 754

permit, deny (Standard IPv6 ACL) 755

permit, deny (Extended IPv6 ACL) 756

show ipv6 access-list 758

ipv6 access-group 759

show ipv6 access-group 759

MAC ACLs 760

access-list mac 760

permit, deny (MAC ACL) 761

mac access-group 763

show mac access-group 764

show mac access-list 764

ARP ACLs 765

access-list arp 765

permit, deny (ARP ACL) 766

show arp access-list 767

ACL Information 768

show access-group 768

show access-list 768

30 INTERFACE COMMANDS 769

interface 770

alias 770

capabilities 771

description 772

flowcontrol 773

media-type 774

negotiation 774

shutdown 775
speed-duplex 776
switchport packet-rate 777
clear counters 778
show interfaces counters 778
show interfaces status 780
show interfaces switchport 781
test cable-diagnostics dsp 782
test loop internal 783
show cable-diagnostics 784
show loop internal 784
31 LINK AGGREGATION COMMANDS 787
channel-group 788
lacp 789
lacp admin-key (Ethernet Interface) 790
lacp port-priority 791
lacp system-priority 792
lacp admin-key (Port Channel) 792
show lacp 793
32 PORT MIRRORING COMMANDS 797
Local Port Mirroring Commands 797
port monitor 797
show port monitor 798
33 RATE LIMIT COMMANDS 801
rate-limit 801
34 ADDRESS TABLE COMMANDS 803
mac-address-table aging-time 803
mac-address-table static 804
clear mac-address-table dynamic 805
show mac-address-table 805
show mac-address-table aging-time 806
35 SPANNING TREE COMMANDS 807
spanning-tree 808
spanning-tree forward-time 809
spanning-tree hello-time 809
spanning-tree max-age 810

spanning-tree mode 811
spanning-tree pathcost method 812
spanning-tree priority 813
spanning-tree mst configuration 813
spanning-tree transmission-limit 814
max-hops 814
mst priority 815
mst vlan 816
name 816
revision 817
spanning-tree bpdu-filter 818
spanning-tree bpdu-guard 818
spanning-tree cost 819
spanning-tree edge-port 820
spanning-tree link-type 821
spanning-tree loopback-detection 822
spanning-tree loopback-detection release-mode 822
spanning-tree loopback-detection trap 823
spanning-tree mst cost 824
spanning-tree mst port-priority 825
spanning-tree port-priority 825
spanning-tree root-guard 826
spanning-tree spanning-disabled 827
spanning-tree loopback-detection release 827
spanning-tree protocol-migration 828
show spanning-tree 829
show spanning-tree mst configuration 830
36 VLAN COMMANDS 831
GVRP and Bridge Extension Commands 832
bridge-ext gvrp 832
garp timer 833
switchport forbidden vlan 834
switchport gvrp 834
show bridge-ext 835
show garp timer 835
show gvrp configuration 836

Editing VLAN Groups 836
vlan database 837
vlan 837
Configuring VLAN Interfaces 838
interface vlan 839
switchport acceptable-frame-types 839
switchport allowed vlan 840
switchport ingress-filtering 841
switchport mode 842
switchport native vlan 843
vlan-trunking 843
Displaying VLAN Information 845
show vlan 845
Configuring IEEE 802.1Q Tunneling 846
dot1q-tunnel system-tunnel-control 847
switchport dot1q-tunnel mode 847
switchport dot1q-tunnel tpid 848
show dot1q-tunnel 849
Configuring Port-based Traffic Segmentation 850
traffic-segmentation 850
show traffic-segmentation 851
Configuring Private VLANs 851
private-vlan 853
private vlan association 854
switchport mode private-vlan 854
switchport private-vlan host-association 855
switchport private-vlan mapping 856
show vlan private-vlan 856
Configuring Protocol-based VLANs 857
protocol-vlan protocol-group (Configuring Groups) 858
protocol-vlan protocol-group (Configuring Interfaces) 858
show protocol-vlan protocol-group 859
show interfaces protocol-vlan protocol-group 860
Configuring IP Subnet VLANs 861
subnet-vlan 861
show subnet-vlan 862

Configuring MAC Based VLANs 863

mac-vlan 863

show mac-vlan 864

Configuring Voice VLANs 864

voice vlan 865

voice vlan aging 866

voice vlan mac-address 866

switchport voice vlan 867

switchport voice vlan priority 868

switchport voice vlan rule 868

switchport voice vlan security 869

show voice vlan 870

37 CLASS OF SERVICE COMMANDS 871

Priority Commands (Layer 2) 871

queue cos-map 872

queue mode 873

queue weight 874

switchport priority default 875

show queue cos-map 876

show queue mode 876

show queue weight 877

Priority Commands (Layer 3 and 4) 878

map ip dscp (Global Configuration) 878

map ip port (Global Configuration) 879

map ip precedence (Global Configuration) 879

map ip dscp (Interface Configuration) 880

map ip port (Interface Configuration) 881

map ip precedence (Interface Configuration) 882

show map ip dscp 883

show map ip port 883

show map ip precedence 884

38 QUALITY OF SERVICE COMMANDS 885

class-map 886

description 887

match 888

rename 889

policy-map 889

class 890

police flow 891

police srtcm-color 893

police trtcm-color 895

set cos 897

set phb 898

service-policy 899

show class-map 900

show policy-map 900

show policy-map interface 901

39 MULTICAST FILTERING COMMANDS 903

IGMP Snooping 904

ip igmp snooping 905

ip igmp snooping proxy-reporting 906

ip igmp snooping querier 906

ip igmp snooping router-alert-option-check 907

ip igmp snooping router-port-expire-time 908

ip igmp snooping tcn-flood 908

ip igmp snooping tcn-query-solicit 909

ip igmp snooping unregistered-data-flood 910

ip igmp snooping unsolicited-report-interval 911

ip igmp snooping version 911

ip igmp snooping version-exclusive 912

ip igmp snooping vlan general-query-suppression 913

ip igmp snooping vlan immediate-leave 913

ip igmp snooping vlan last-memb-query-count 914

ip igmp snooping vlan last-memb-query-intvl 915

ip igmp snooping vlan mrd 915

ip igmp snooping vlan proxy-address 916

ip igmp snooping vlan query-interval 917

ip igmp snooping vlan query-resp-intvl 918

ip igmp snooping vlan static 919

show ip igmp snooping 919

show ip igmp snooping group 920

show mac-address-table multicast 921

Static Multicast Routing 922
ip igmp snooping vlan mrouter 922
show ip igmp snooping mrouter 923
IGMP Filtering and Throttling 923
ip igmp filter (Global Configuration) 924
ip igmp profile 925
permit, deny 925
range 926
ip igmp filter (Interface Configuration) 926
ip igmp max-groups 927
ip igmp max-groups action 928
show ip igmp filter 928
show ip igmp profile 929
show ip igmp throttle interface 929
Multicast VLAN Registration 930
mvr 931
mvr immediate-leave 932
mvr type 933
mvr vlan group 934
show mvr 935
IGMP (Layer 3) 937
ip igmp 937
ip igmp last-member-query-interval 938
ip igmp max-resp-interval 939
ip igmp query-interval 940
ip igmp robustval 941
ip igmp static-group 941
ip igmp version 943
clear ip igmp group 943
show ip igmp groups 944
show ip igmp interface 946
IGMP Proxy Routing 947
ip igmp proxy 947
ip igmp proxy unsolicited-report-interval 948
40 LLDP COMMANDS 951
lldp 952

lldp holdtime-multiplier 952
lldp notification-interval 953
lldp refresh-interval 954
lldp reinit-delay 954
lldp tx-delay 955
lldp admin-status 955
lldp basic-tlv management-ip-address 956
lldp basic-tlv port-description 957
lldp basic-tlv system-capabilities 957
lldp basic-tlv system-description 958
lldp basic-tlv system-name 958
lldp dot1-tlv proto-ident 959
lldp dot1-tlv proto-vid 959
lldp dot1-tlv pvid 960
lldp dot1-tlv vlan-name 960
lldp dot3-tlv link-agg 961
lldp dot3-tlv mac-phy 961
lldp dot3-tlv max-frame 962
lldp notification 962
show lldp config 963
show lldp info local-device 964
show lldp info remote-device 965
show lldp info statistics 966
41 DOMAIN NAME SERVICE COMMANDS 969
ip domain-list 969
ip domain-lookup 970
ip domain-name 971
ip host 972
ip name-server 973
ipv6 host 974
clear dns cache 974
clear host 975
show dns 975
show dns cache 976
show hosts 976

42 DHCP COMMANDS 979

DHCP Client 979

ip dhcp restart client 979

DHCP Relay 980

ip dhcp relay server 980

ip dhcp restart relay 981

DHCP Server 982

ip dhcp excluded-address 983

ip dhcp pool 983

service dhcp 984

bootfile 984

client-identifier 985

default-router 986

dns-server 986

domain-name 987

hardware-address 987

host 988

lease 989

netbios-name-server 990

netbios-node-type 991

network 991

next-server 992

clear ip dhcp binding 993

show ip dhcp binding 993

show ip dhcp 994

43 VRRP COMMANDS 995

vrrp authentication 996

vrrp ip 996

vrrp preempt 997

vrrp priority 998

vrrp timers advertise 999

clear vrrp interface counters 1000

clear vrrp router counters 1000

show vrrp 1000

show vrrp interface 1002

show vrrp interface counters 1003

show vrrp router counters 1004

44 IP INTERFACE COMMANDS 1005

IP Interface 1005

Basic IP Configuration 1006

ip address 1006

ip default-gateway 1008

show ip interface 1009

traceroute 1009

ping 1010

ARP Configuration 1011

arp 1011

arp timeout 1012

ip proxy-arp 1013

clear arp-cache 1014

show arp 1014

UDP Helper Configuration 1015

ip forward-protocol udp 1015

ip helper 1016

ip helper-address 1017

show ip helper 1018

45 IP ROUTING COMMANDS 1019

Global Routing Configuration 1019

ip route 1020

maximum-paths 1021

show ip route 1021

show ip route database 1022

show ip traffic 1023

Routing Information Protocol (RIP) 1024

router rip 1025

default-information originate 1026

default-metric 1026

distance 1027

maximum-prefix 1028

neighbor 1029

network 1029

passive-interface 1030

redistribute 1031

timers basic 1032

version 1033

ip rip authentication mode 1034

ip rip authentication string 1035

ip rip receive version 1035

ip rip receive-packet 1036

ip rip send version 1037

ip rip send-packet 1038

ip rip split-horizon 1038

clear ip rip route 1039

show ip protocols rip 1040

show ip rip 1041

Open Shortest Path First (OSPFv2) 1042

router ospf 1043

compatible rfc1583 1044

default-information originate 1045

router-id 1046

timers spf 1047

clear ip ospf process 1048

area default-cost 1048

area range 1049

auto-cost reference-bandwidth 1050

default-metric 1051

redistribute 1052

summary-address 1053

area nssa 1054

area stub 1056

area virtual-link 1057

network area 1059

ip ospf authentication 1060

ip ospf authentication-key 1062

ip ospf cost 1063

ip ospf dead-interval 1064

ip ospf hello-interval 1065

ip ospf message-digest-key 1065

ip ospf priority 1066

ip ospf retransmit-interval 1067

ip ospf transmit-delay 1068

passive-interface 1069

show ip ospf 1069

show ip ospf border-routers 1071

show ip ospf database 1072

show ip ospf interface 1078

show ip ospf neighbor 1080

show ip ospf route 1081

show ip ospf virtual-links 1081

show ip protocols ospf 1082

46 MULTICAST ROUTING COMMANDS 1085

General Multicast Routing 1085

ip multicast-routing 1085

show ip mroute 1086

Static Multicast Routing 1088

ip igmp snooping vlan mrouter 1088

show ip igmp snooping mrouter 1089

PIM Multicast Routing 1090

PIM Commands 1090

router pim 1091

ip pim 1092

ip pim hello-holdtime 1093

ip pim hello-interval 1094

ip pim join-prune-holdtime 1094

ip pim lan-prune-delay 1095

ip pim override-interval 1096

ip pim propagation-delay 1096

ip pim trigger-hello-delay 1097

show ip pim interface 1098

show ip pim neighbor 1098

ip pim graft-retry-interval 1099

ip pim max-graft-retries 1100

ip pim state-refresh origination-interval 1100

ip pim bsr-candidate 1101

ip pim register-rate-limit 1102

ip pim register-source 1103

ip pim rp-address 1104

ip pim rp-candidate 1105

ip pim spt-threshold 1107

ip pim dr-priority 1108

ip pim join-prune-interval 1109

clear ip pim bsr rp-set 1110

show ip pim bsr-router 1110

show ip pim rp mapping 1111

show ip pim rp-hash 1112

SECTION IV APPENDICES 1113

A SOFTWARE SPECIFICATIONS 1115

Software Features 1115

Management Features 1117

Standards 1117

Management Information Bases 1118

B TROUBLESHOOTING 1121

Problems Accessing the Management Interface 1121

Using System Logs 1122

C LICENSE INFORMATION 1123

The GNU General Public License 1123

GLOSSARY 1127

COMMAND LIST 1135

INDEX 1143

FIGURES

Figure 1: Home Page 82

Figure 2: Front Panel Indicators 83

Figure 3: System Information 102

Figure 4: General Switch Information 104

Figure 5: Configuring Support for Jumbo Frames 105

Figure 6: Displaying Bridge Extension Configuration 106

Figure 7: Copy Firmware 108

Figure 8: Saving the Running Configuration 109

Figure 9: Setting Start-Up Files 110

Figure 10: Displaying System Files 111

Figure 11: Manually Setting the System Clock 112

Figure 12: Setting the Polling Interval for SNTP 113

Figure 13: Specifying SNTP Time Servers 114

Figure 14: Setting the Time Zone 115

Figure 15: Console Port Settings 116

Figure 16: Telnet Connection Settings 118

Figure 17: Displaying CPU Utilization 119

Figure 18: Displaying Memory Utilization 119

Figure 19: Restarting the Switch (Immediately) 121

Figure 20: Restarting the Switch (In) 122

Figure 21: Restarting the Switch (At) 122

Figure 22: Restarting the Switch (Regularly) 123

Figure 23: Configuring Connections by Port List 127

Figure 24: Configuring Connections by Port Range 128

Figure 25: Displaying Port Information 129

Figure 26: Configuring Local Port Mirroring 130

Figure 27: Configuring Local Port Mirroring 131

Figure 28: Displaying Local Port Mirror Sessions 131

Figure 29: Showing Port Statistics (Table) 134

Figure 30: Showing Port Statistics (Chart) 135

Figure 31: Configuring Static Trunks 136

Figure 32: Creating Static Trunks 137
Figure 33: Adding Static Trunks Members 138
Figure 34: Configuring Connection Parameters for a Static Trunk 138
Figure 35: Displaying Connection Parameters for Static Trunks 139
Figure 36: Configuring Dynamic Trunks 139
Figure 37: Configuring the LACP Aggregator Admin Key 141
Figure 38: Enabling LACP on a Port 141
Figure 39: Configuring LACP Parameters on a Port 142
Figure 40: Showing Members of a Dynamic Trunk 142
Figure 41: Configuring Connection Settings for Dynamic Trunks 143
Figure 42: Displaying Connection Parameters for Dynamic Trunks 143
Figure 43: Displaying LACP Port Counters 145
Figure 44: Displaying LACP Port Internal Information 147
Figure 45: Displaying LACP Port Remote Information 148
Figure 46: Enabling Traffic Segmentation 149
Figure 47: Configuring Members for Traffic Segmentation 150
Figure 48: Configuring VLAN Trunking 151
Figure 49: Configuring VLAN Trunking 152
Figure 50: VLAN Compliant and VLAN Non-compliant Devices 154
Figure 51: Using GVRP 156
Figure 52: Creating Static VLANs 157
Figure 53: Modifying Settings for Static VLANs 158
Figure 54: Showing Static VLANs 158
Figure 55: Configuring Static Members by VLAN Index 161
Figure 56: Configuring Static VLAN Members by Interface 162
Figure 57: Configuring Static VLAN Members by Interface Range 162
Figure 58: Configuring Global Status of GVRP 164
Figure 59: Configuring GVRP for an Interface 165
Figure 60: Showing Dynamic VLANs Registered on the Switch 165
Figure 61: Showing the Members of a Dynamic VLAN 166
Figure 62: Configuring Private VLANs 167
Figure 63: Showing Private VLANs 168
Figure 64: Associating Private VLANs 169
Figure 65: Showing Associated VLANs 169
Figure 66: Configuring Interfaces for Private VLANs 170
Figure 67: QinQ Operational Concept 172

Figure 68: Enabling QinQ Tunneling 176

Figure 69: Adding an Interface to a QinQ Tunnel 177

Figure 70: Configuring Protocol VLANs 179

Figure 71: Displaying Protocol VLANs 179

Figure 72: Assigning Interfaces to Protocol VLANs 181

Figure 73: Showing the Interface to Protocol Group Mapping 181

Figure 74: Configuring IP Subnet VLANs 183

Figure 75: Showing IP Subnet VLANs 183

Figure 76: Configuring MAC-Based VLANs 185

Figure 77: Showing MAC-Based VLANs 185

Figure 78: Configuring MAC Address Learning 188

Figure 79: Configuring Static MAC Addresses 190

Figure 80: Displaying Static MAC Addresses 190

Figure 81: Setting the Address Aging Time 191

Figure 82: Displaying the Dynamic MAC Address Table 192

Figure 83: Clearing Entries in the Dynamic MAC Address Table 193

Figure 84: STP Root Ports and Designated Ports 196

Figure 85: MSTP Region, Internal Spanning Tree, Multiple Spanning Tree 197

Figure 86: Common Internal Spanning Tree, Common Spanning Tree, Internal Spanning Tree 197

Figure 87: Configuring Port Loopback Detection 199

Figure 88: Configuring Global Settings for STA (STP) 203

Figure 89: Configuring Global Settings for STA (RSTP) 203

Figure 90: Configuring Global Settings for STA (MSTP) 204

Figure 91: Displaying Global Settings for STA 205

Figure 92: Configuring Interface Settings for STA 209

Figure 93: STA Port Roles 211

Figure 94: Displaying Interface Settings for STA 211

Figure 95: Creating an MST Instance 213

Figure 96: Displaying MST Instances 213

Figure 97: Modifying the Priority for an MST Instance 214

Figure 98: Displaying Global Settings for an MST Instance 214

Figure 99: Adding a VLAN to an MST Instance 215

Figure 100: Displaying Members of an MST Instance 215

Figure 101: Configuring MSTP Interface Settings 217

Figure 102: Displaying MSTP Interface Settings 217

Figure 103: Configuring Rate Limits 220

Figure 104: Configuring Broadcast Storm Control 222
Figure 105: Configuring a Class Map 225
Figure 106: Showing Class Maps 226
Figure 107: Adding Rules to a Class Map 226
Figure 108: Showing the Rules for a Class Map 227
Figure 109: Configuring a Policy Map 235
Figure 110: Showing Policy Maps 235
Figure 111: Adding Rules to a Policy Map 236
Figure 112: Showing the Rules for a Policy Map 236
Figure 113: Attaching a Policy Map to a Port 237
Figure 114: Configuring a Voice VLAN 240
Figure 115: Configuring an OUI Telephony List 242
Figure 116: Showing an OUI Telephony List 242
Figure 117: Configuring Port Settings for a Voice VLAN 244
Figure 118: Configuring the Authentication Sequence 248
Figure 119: Authentication Server Operation 248
Figure 120: Configuring Remote Authentication Server (RADIUS) 251
Figure 121: Configuring Remote Authentication Server (TACACS+) 251
Figure 122: Configuring AAA Server Groups 252
Figure 123: Showing AAA Server Groups 252
Figure 124: Configuring Global Settings for AAA Accounting 255
Figure 125: Configuring AAA Accounting Methods 255
Figure 126: Showing AAA Accounting Methods 256
Figure 127: Configuring AAA Accounting Service for 802.1X Service 256
Figure 128: Configuring AAA Accounting Service for Exec Service 257
Figure 129: Displaying a Summary of Applied AAA Accounting Methods 257
Figure 130: Displaying Statistics for AAA Accounting Sessions 257
Figure 131: Configuring AAA Authorization Methods 259
Figure 132: Showing AAA Authorization Methods 259
Figure 133: Configuring AAA Authorization Methods for Exec Service 260
Figure 134: Displaying the Applied AAA Authorization Method 260
Figure 135: Configuring User Accounts 262
Figure 136: Showing User Accounts 262
Figure 137: Configuring Global Settings for Network Access 266
Figure 138: Configuring Interface Settings for Network Access 267
Figure 139: Configuring Link Detection for Network Access 269

Figure 140: Configuring a MAC Address Filter for Network Access 270
Figure 141: Showing the MAC Address Filter Table for Network Access 270
Figure 142: Showing Addresses Authenticated for Network Access 272
Figure 143: Configuring HTTPS 273
Figure 144: Downloading the Secure-Site Certificate 275
Figure 145: Configuring the SSH Server 279
Figure 146: Generating the SSH Host Key Pair 280
Figure 147: Showing the SSH Host Key Pair 281
Figure 148: Copying the SSH User’s Public Key 282
Figure 149: Showing the SSH User’s Public Key 283
Figure 150: Setting the Name of a Time Range 285
Figure 151: Showing a List of Time Ranges 285
Figure 152: Add a Rule to a Time Range 286
Figure 153: Showing the Rules Configured for a Time Range 286
Figure 154: Creating an ACL 287
Figure 155: Showing a List of ACLs 288
Figure 156: Configuring a Standard IPv4 ACL 289
Figure 157: Configuring an Extended IPv4 ACL 291
Figure 158: Configuring a Standard IPv6 ACL 293
Figure 159: Configuring an Extended IPv6 ACL 295
Figure 160: Configuring a MAC ACL 297
Figure 161: Configuring a ARP ACL 299
Figure 162: Binding a Port to an ACL 301
Figure 163: Configuring Global Settings for ARP Inspection 304
Figure 164: Configuring VLAN Settings for ARP Inspection 305
Figure 165: Configuring Interface Settings for ARP Inspection 307
Figure 166: Displaying Statistics for ARP Inspection 308
Figure 167: Displaying the ARP Inspection Log 309
Figure 168: Creating an IP Address Filter for Management Access 310
Figure 169: Showing IP Addresses Authorized for Management Access 311
Figure 170: Configuring Port Security 313
Figure 171: Configuring Port Security 314
Figure 172: Configuring Global Settings for 802.1X Port Authentication 315
Figure 173: Configuring Interface Settings for 802.1X Port Authenticator 319
Figure 174: Showing Statistics for 802.1X Port Authenticator 321
Figure 175: Setting the Filter Type for IP Source Guard 323

Figure 176: Configuring Static Bindings for IP Source Guard 324
Figure 177: Displaying Static Bindings for IP Source Guard 325
Figure 178: Showing the IP Source Guard Binding Table 326
Figure 179: Configuring Global Settings for DHCP Snooping 330
Figure 180: Configuring DHCP Snooping on a VLAN 331
Figure 181: Configuring the Port Mode for DHCP Snooping 332
Figure 182: Displaying the Binding Table for DHCP Snooping 333
Figure 183: Configuring Settings for System Memory Logs 337
Figure 184: Showing Error Messages Looged to System Memory 337
Figure 185: Configuring Settings for Remote Logging of Error Messages 338
Figure 186: Configuring SMTP Alert Messages 340
Figure 187: Configuring LLDP Timing Attributes 342
Figure 188: Configuring LLDP Interface Attributes 345
Figure 189: Displaying Local Device Information for LLDP (General) 347
Figure 190: Displaying Local Device Information for LLDP (Port) 347
Figure 191: Displaying Remote Device Information for LLDP (Port) 351
Figure 192: Displaying Remote Device Information for LLDP (Port Details) 352
Figure 193: Displaying LLDP Device Statistics (General) 354
Figure 194: Displaying LLDP Device Statistics (Port) 354
Figure 195: Configuring Global Settings for SNMP 357
Figure 196: Configuring the Local Engine ID for SNMP 358
Figure 197: Configuring a Remote Engine ID for SNMP 359
Figure 198: Showing Remote Engine IDs for SNMP 360
Figure 199: Creating an SNMP View 361
Figure 200: Showing SNMP Views 361
Figure 201: Adding an OID Subtree to an SNMP View 362
Figure 202: Showing the OID Subtree Configured for SNMP Views 362
Figure 203: Creating an SNMP Group 365
Figure 204: Showing SNMP Groups 366
Figure 205: Setting Community Access Strings 367
Figure 206: Showing Community Access Strings 367
Figure 207: Configuring Local SNMPv3 Users 369
Figure 208: Showing Local SNMPv3 Users 369
Figure 209: Configuring Remote SNMPv3 Users 371
Figure 210: Showing Remote SNMPv3 Users 372
Figure 211: Configuring Trap Managers (SNMPv1) 375

Figure 212: Configuring Trap Managers (SNMPv2c) 375
Figure 213: Configuring Trap Managers (SNMPv3) 376
Figure 214: Showing Trap Managers 376
Figure 215: Configuring an RMON Alarm 379
Figure 216: Showing Configured RMON Alarms 379
Figure 217: Configuring an RMON Event 381
Figure 218: Showing Configured RMON Events 382
Figure 219: Configuring an RMON History Sample 383
Figure 220: Showing Configured RMON History Samples 384
Figure 221: Showing Collected RMON History Samples 384
Figure 222: Configuring an RMON Statistical Sample 385
Figure 223: Showing Configured RMON Statistical Samples 386
Figure 224: Showing Collected RMON Statistical Samples 386
Figure 225: Multicast Filtering Concept 387
Figure 226: IGMP Protocol 389
Figure 227: Configuring General Settings for IGMP Snooping 394
Figure 228: Configuring a Static Interface for a Multicast Router 395
Figure 229: Showing Static Interfaces Attached a Multicast Router 396
Figure 230: Showing Current Interfaces Attached a Multicast Router 396
Figure 231: Assigning an Interface to a Multicast Service 398
Figure 232: Showing Static Interfaces Assigned to a Multicast Service 398
Figure 233: Showing Current Interfaces Assigned to a Multicast Service 399
Figure 234: Configuring IGMP Snooping on an Interface 403
Figure 235: Showing Interface Settings for IGMP Snooping 404
Figure 236: Showing Multicast Groups Learned by IGMP Snooping 405
Figure 237: Enabling IGMP Filtering and Throttling 406
Figure 238: Creating an IGMP Filtering Profile 407
Figure 239: Showing the IGMP Filtering Profiles Created 407
Figure 240: Adding Multicast Groups to an IGMP Filtering Profile 408
Figure 241: Showing the Groups Assigned to an IGMP Filtering Profile 408
Figure 242: Configuring IGMP Filtering and Throttling Interface Settings 410
Figure 243: IGMP Proxy Routing 411
Figure 244: Configuring IGMP Proxy Routing 413
Figure 245: Configuring IGMP Interface Settings 416
Figure 246: Configuring Static IGMP Groups 417
Figure 247: Showing Static IGMP Groups 417

Figure 248: Displaying Multicast Groups Learned from IGMP (Information) 419
Figure 249: Displaying Multicast Groups Learned from IGMP (Detail) 420
Figure 250: MVR Concept 421
Figure 251: Configuring Global Settings for MVR 423
Figure 252: Configuring the Group Range for MVR 424
Figure 253: Showing the Configured Group Range for MVR 424
Figure 254: Configuring Interface Settings for MVR 426
Figure 255: Assigning Static MVR Groups to a Port 427
Figure 256: Showing the Static MVR Groups Assigned to a Port 428
Figure 257: Showing All MVR Groups Assigned to a Port 429
Figure 258: Configuring a Static Address 433
Figure 259: Configuring a Dynamic Address 433
Figure 260: Showing the Configured IP Address for an Interface 434
Figure 261: Virtual Interfaces and Layer 3 Routing 436
Figure 262: Pnging a Network Device 440
Figure 263: Tracing the Route to a Network Device 441
Figure 264: Proxy ARP 442
Figure 265: Configuring General Settings for ARP 443
Figure 266: Configuring Static ARP Entries 445
Figure 267: Displaying Static ARP Entries 445
Figure 268: Displaying Dynamic ARP Entries 446
Figure 269: Displaying Local ARP Entries 446
Figure 270: Displaying ARP Statistics 447
Figure 271: Configuring Static Routes 448
Figure 272: Displaying Static Routes 449
Figure 273: Displaying the Routing Table 450
Figure 274: Setting the Maximum ECMP Numbeer 452
Figure 275: Master Virtual Router with Backup Routers 453
Figure 276: Several Virtual Master Routers Using Backup Routers 453
Figure 277: Several Virtual Master Routers Configured for Mutual Backup and Load Sharing 454
Figure 278: Configuring the VRRP Group ID 458
Figure 279: Showing Configured VRRP Groups 458
Figure 280: Setting the Virtual Router Address for a VRRP Group 459
Figure 281: Showing the Virtual Addresses Assigned to VRRP Groups 459
Figure 282: Configuring Detailed Settings for a VRRP Group 460
Figure 283: Showing Counters for Errors Found in VRRP Packets 461

Figure 284: Showing Counters for Errors Found in a VRRP Group 462
Figure 285: Configuring General Settings for DNS 464
Figure 286: Configuring a List of Domain Names for DNS 465
Figure 287: Showing the List of Domain Names for DNS 465
Figure 288: Configuring a List of Name Servers for DNS 466
Figure 289: Showing the List of Name Servers for DNS 467
Figure 290: Configuring Static Entries in the DNS Table 468
Figure 291: Showing Static Entries in the DNS Table 468
Figure 292: Showing Entries in the DNS Cache 469
Figure 293: Layer 3 DHCP Relay Service 470
Figure 294: Configuring DHCP Relay Service 471
Figure 295: DHCP Server 471
Figure 296: Enabling the DHCP Server 472
Figure 297: Configuring Excluded Addresses on the DHCP Server 473
Figure 298: Showing Excluded Addresses on the DHCP Server 473
Figure 299: Configuring DHCP Server Address Pools (Network) 476
Figure 300: Configuring DHCP Server Address Pools (Host) 476
Figure 301: Showing Configured DHCP Server Address Pools 477
Figure 302: Shows Addresses Assigned by the DHCP Server 477
Figure 303: Enabling the UDP Helper 479
Figure 304: Specifying UDP Destination Ports 480
Figure 305: Showing the UDP Destination Ports 480
Figure 306: Specifying the Target Server or Subnet for UDP Requests 481
Figure 307: Showing the Target Server or Subnet for UDP Requests 482
Figure 308: Configuring RIP 484
Figure 309: Configuring General Settings for RIP 488
Figure 310: Clearing Entries from the Routing Table 489
Figure 311: Adding Network Interfaces to RIP 490
Figure 312: Showing Network Interfaces Using RIP 491
Figure 313: Specifying a Passive RIP Interface 492
Figure 314: Showing Passive RIP Interfaces 492
Figure 315: Specifying a Static RIP Neighbor 493
Figure 316: Showing Static RIP Neighbors 493
Figure 317: Redistributing External Routes into RIP 494
Figure 318: Showing External Routes Redistributed into RIP 495
Figure 319: Setting the Distance Assigned to External Routes 496

Figure 320: Showing the Distance Assigned to External Routes 496
Figure 321: Configuring a Network Interface for RIP 500
Figure 322: Showing RIP Network Interface Settings 500
Figure 323: Showing RIP Interface Settings 501
Figure 324: Showing RIP Peer Information 502
Figure 325: Resetting RIP Statistics 502
Figure 326: Configuring OSPF 503
Figure 327: OSPF Areas 504
Figure 328: Defining OSPF Network Areas Based on Addresses 506
Figure 329: Showing OSPF Network Areas 506
Figure 330: Showing OSPF Process Identifiers 507
Figure 331: AS Boundary Router 509
Figure 332: Configure General Settings for OSPF 510
Figure 333: Showing General Settings for OSPF 511
Figure 334: Adding an NSSA or Stub 512
Figure 335: Showing NSSAs or Stubs 513
Figure 336: OSPF NSSA 513
Figure 337: Configuring Protocol Settings for an NSSA 516
Figure 338: OSPF Stub Area 516
Figure 339: Configuring Protocol Settings for a Stub 518
Figure 340: Displaying Information on NSSA and Stub Areas 519
Figure 341: Route Summarization for ABRs 519
Figure 342: Configuring Route Summaries for an Area Range 520
Figure 343: Showing Configured Route Summaries 521
Figure 344: Redistributing External Routes 521
Figure 345: Importing External Routes 523
Figure 346: Showing Imported External Route Types 523
Figure 347: Summarizing External Routes 524
Figure 348: Showing Summary Addresses for External Routes 525
Figure 349: Configuring Settings for All Interfaces Assigned to a VLAN 529
Figure 350: Configuring Settings for a Specific Area Assigned to a VLAN 530
Figure 351: Showing OSPF Interfaces 530
Figure 352: Showing MD5 Authentication Keys 531
Figure 353: OSPF Virtual Link 531
Figure 354: Adding a Virtual Link 532
Figure 355: Showing Virtual Links 533

Figure 356: Configuring Detailed Settings for a Virtual Link 533
Figure 357: Showing MD5 Authentication Keys 534
Figure 358: Displaying Information in the Link State Database 536
Figure 359: Displaying Virtual Links Stored in the Link State Database 537
Figure 360: Displaying Neighbor Routers Stored in the Link State Database 539
Figure 361: Enabling Multicast Routing 544
Figure 362: Displaying the Multicast Routing Table 547
Figure 363: Displaying Detailed Entries from the Multicast Routing Table 547
Figure 364: Enabling PIM Multicast Routing 548
Figure 365: Configuring PIM Interface Settings (Dense Mode) 553
Figure 366: Configuring PIM Interface Settings (Sparse Mode) 553
Figure 367: Showing PIM Neighbors 554
Figure 368: Configuring Global Settings for PIM-SM 556
Figure 369: Configuring a BSR Candidate 557
Figure 370: Configuring a Static Rendezvous Point 559
Figure 371: Showing Static Rendezvous Points 559
Figure 372: Configuring an RP Candidate 561
Figure 373: Showing Settings for an RP Candidate 561
Figure 374: Showing Information About the BSR 563
Figure 375: Showing RP Mapping 564

TABLES

Table 1: Key Features 57

Table 2: System Defaults 64

Table 3: Web Page Configuration Buttons 83

Table 4: Switch Main Menu 84

Table 5: Port Statistics 132

Table 6: LACP Port Counters 144

Table 7: LACP Internal Configuration Information 145

Table 8: LACP Internal Configuration Information 147

Table 9: Recommended STA Path Cost Range 206

Table 10: Default STA Path Costs 206

Table 11: Dynamic QoS Profiles 264

Table 12: HTTPS System Support 273

Table 13: ARP Inspection Statistics 307

Table 14: ARP Inspection Log 308

Table 15: 802.1X Statistics 320

Table 16: Logging Levels 336

Table 17: Chassis ID Subtype 345

Table 18: System Capabilities 346

Table 19: Port ID Subtype 348

Table 20: Remote Port Auto-Negotiation Advertised Capability 349

Table 21: SNMPv3 Security Models and Levels 355

Table 22: Supported Notification Messages 363

Table 23: Address Resolution Protocol 442

Table 24: ARP Statistics 446

Table 25: VRRP Group Statistics Statistics 461

Table 26: OSPF System Information 510

Table 27: General Command Modes 572

Table 28: Configuration Command Modes 574

Table 29: Keystroke Commands 575

Table 30: Command Group Index 576

Table 31: General Commands 579

Table 32: System Management Commands 587

Table 33: Device Designation Commands 587

Table 34: System Status Commands 588

Table 35: Frame Size Commands 592

Table 36: Flash/File Commands 594

Table 37: File Directory Information 599

Table 38: Line Commands 600

Table 39: Event Logging Commands 610

Table 40: Logging Levels 611

Table 41: show logging flash/ram - display description 615

Table 42: show logging trap - display description 616

Table 43: Event Logging Commands 616

Table 44: Time Commands 620

Table 45: Time Range Commands 625

Table 46: SNMP Commands 629

Table 47: show snmp engine-id - display description 641

Table 48: show snmp group - display description 642

Table 49: show snmp user - display description 643

Table 50: show snmp view - display description 644

Table 51: RMON Commands 649

Table 52: Authentication Commands 657

Table 53: User Access Commands 657

Table 54: Default Login Settings 659

Table 55: Authentication Sequence Commands 660

Table 56: RADIUS Client Commands 662

Table 57: TACACS+ Client Commands 666

Table 58: AAA Commands 669

Table 59: Web Server Commands 678

Table 60: HTTPS System Support 680

Table 61: Telnet Server Commands 681

Table 62: Secure Shell Commands 684

Table 63: show ssh - display description 693

Table 64: 802.1X Port Authentication Commands 693

Table 65: Management IP Filter Commands 704

Table 66: General Security Commands 707

Table 67: Management IP Filter Commands 708

Table 68: Network Access Commands 711

Table 69: Dynamic QoS Profiles 714

Table 70: DHCP Snooping Commands 724

Table 71: IP Source Guard Commands 733

Table 72: ARP Inspection Commands 738

Table 73: Access Control List Commands 747

Table 74: IPv4 ACL Commands 747

Table 75: IPv4 ACL Commands 754

Table 76: MAC ACL Commands 760

Table 77: ARP ACL Commands 765

Table 78: ACL Information Commands 768

Table 79: Interface Commands 769

Table 80: show interfaces switchport - display description 782

Table 81: Link Aggregation Commands 787

Table 82: show lacp counters - display description 794

Table 83: show lacp internal - display description 794

Table 84: show lacp neighbors - display description 795

Table 85: show lacp sysid - display description 796

Table 86: Port Mirroring Commands 797

Table 87: Mirror Port Commands 797

Table 88: Rate Limit Commands 801

Table 89: Address Table Commands 803

Table 90: Spanning Tree Commands 807

Table 91: Recommended STA Path Cost Range 819

Table 92: Default STA Path Costs 820

Table 93: VLAN Commands 831

Table 94: GVRP and Bridge Extension Commands 832

Table 95: Commands for Editing VLAN Groups 836

Table 96: Commands for Configuring VLAN Interfaces 838

Table 97: Commands for Displaying VLAN Information 845

Table 98: 802.1Q Tunneling Commands 846

Table 99: Commands for Configuring Traffic Segmentation 850

Table 100: Private VLAN Commands 852

Table 101: Protocol-based VLAN Commands 857

Table 102: IP Subnet VLAN Commands 861

Table 103: MAC Based VLAN Commands 863

Table 104: Voice VLAN Commands 864

Table 105: Priority Commands 871

Table 106: Priority Commands (Layer 2) 871

Table 107: Default CoS Priority Levels 872

Table 108: Priority Commands (Layer 3 and 4) 878

Table 109: Mapping IP DSCP to CoS Values 880

Table 110: Mapping IP Precedence to CoS Values 882

Table 111: Quality of Service Commands 885

Table 112: Multicast Filtering Commands 903

Table 113: IGMP Snooping Commands 904

Table 114: Static Multicast Interface Commands 922

Table 115: IGMP Filtering and Throttling Commands 923

Table 116: Multicast VLAN Registration Commands 930

Table 117: show mvr - display description 935

Table 118: show mvr interface - display description 936

Table 119: show mvr members - display description 936

Table 120: IGMP Commands (Layer 3) 937

Table 121: show ip igmp groups - display description 945

Table 122: show ip igmp groups detail - display description 945

Table 123: IGMP Proxy Commands 947

Table 124: LLDP Commands 951

Table 125: Address Table Commands 969

Table 126: show dns cache - display description 976

Table 127: show hosts - display description 977

Table 128: DHCP Commands 979

Table 129: DHCP Client Commands 979

Table 130: DHCP Relay Commands 980

Table 131: DHCP Server Commands 982

Table 132: VRRP Commands 995

Table 133: show vrrp - display description 1001

Table 134: show vrrp brief - display description 1002

Table 135: IP Interface Commands 1005

Table 136: Basic IP Configuration Commands 1006

Table 137: Address Resolution Protocol Commands 1011

Table 138: UDP Helper Commands 1015

Table 139: IP Routing Commands 1019

Table 140: Global Routing Configuration Commands 1019
Table 141: Routing Information Protocol Commands 1024
Table 142: Open Shortest Path First Commands 1042
Table 143: show ip ospf - display description 1070
Table 144: show ip ospf database - display description 1073
Table 145: show ip ospf database summary - display description 1074
Table 146: show ip ospf database external - display description 1075
Table 147: show ip ospf database network - display description 1076
Table 148: show ip ospf database router - display description 1077
Table 149: show ip ospf database summary - display description 1078
Table 150: show ip ospf interface - display description 1079
Table 151: show ip ospf neighbor - display description 1080
Table 152: show ip ospf neighbor - display description 1082
Table 153: show ip protocols ospf - display description 1082
Table 154: Multicast Routing Commands 1085
Table 155: General Multicast Routing Commands 1085
Table 156: show ip mroute - display description 1087
Table 157: Static Multicast Routing Commands 1088
Table 158: PIM-DM and PIM-SM Multicast Routing Commands 1090
Table 159: show ip pim neighbor - display description 1099
Table 160: show ip pim bsr-router - display description 1111
Table 161: show ip pim rp mapping - display description 1112
Table 162: show ip pim rp-hash - display description 1112
Table 163: Troubleshooting Chart 1121

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 57
- "Initial Switch Configuration" on page 67

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+ Web – HTTPS Telnet – SSH SNMP v1/2c - Community strings SNMP version 3 – MD5 or SHA password Port – IEEE 802.1X, MAC address filtering
General Security Measures	Private VLANs Port Authentication Port Security DHCP Snooping IP Source Guard
Access Control Lists	Supports up to 36 ACLs per port, 93 rules per port
DHCP	Client, Relay, Server
DNS	Client and Proxy service
Port Configuration	Speed and duplex mode and flow control
Port Trunking	Supports up to 32 trunks using either static or dynamic trunking (LACP)
Port Mirroring	24 sessions, one or more source ports to one analysis port
Congestion Control	Rate Limiting Throttling for broadcast storms
Address Table	Up to 8K MAC addresses in the forwarding table, 1024 static MAC addresses; Up to 4K IPv4 entries in the host table; 4K entries in the ARP cache, 512 static ARP entries; 256 IPv4 entries in the IP routing table, 256 static IP routes, 32 IP interfaces; 1024 L2 multicast groups
IP Version 4	Supports IPv4 addressing, and management

Table 1: Key Features (Continued)

Feature	Description
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 256 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
Router Redundancy	Router backup is provided with the Virtual Router Redundancy Protocol (VRRP)
IP Routing	Routing Information Protocol (RIP), Open Shortest Path First (OSPF), 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, and IGMP for Layer 3, and Multicast VLAN Registration
Multicast Routing	Supports PIM-DM and PIM-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 a FTP/TFTP server (using the 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 web/SNMP/Telnet/web management access, and MAC address filtering for port access.

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 and duplex mode, and flow control used on specific ports, or use auto-negotiation to detect the connection settings used by the attached device. Use the 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).

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 32 trunks.

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. Traffic that falls within the rate limit is transmitted, while packets that exceed the acceptable amount of traffic are dropped.

BROADCAST STORM CONTROL

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

STATIC 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.

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 16K 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 2 MB 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).

VIRTUAL LANS

The switch supports up to 4093 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, 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.

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.

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.

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 OSPF 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 at Layer 2 and IGMP at Layer 3 to manage multicast group registration. It also supports Multicast VLAN Registration (MVR) 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.

MULTICAST ROUTING

Routing for multicast packets is supported by the Protocol-Independent Multicasting - Dense Mode and Sparse Mode (PIM-DM, PIM-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.

TUNNELING

Configures tunnels for customer traffic crossing the service provider's network using IEEE 802.1Q.

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 VLANs 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.

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	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
	HTTPS	Enabled
	SSH	Disabled
	Port Security	Disabled
	IP Filtering	Disabled

Table 2: System Defaults (Continued)

Function	Parameter	Default
Web Management	HTTP Server	Enabled
	HTTP Port Number	80
	HTTP Secure Server	Disabled
	HTTP Secure Server Redirect	Disabled
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)
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)
Address Table	Aging Time	300 seconds
Spanning Tree Algorithm	Status	Enabled, RSTP (Defaults: RSTP standard)
	Edge Ports	Enabled
LLDP	Status	Enabled
Virtual LANs	Default VLAN	1
	PVID	1
	Acceptable Frame Type	All
	Ingress Filtering	Disabled
	Switchport Mode (Egress Mode)	Tagged frames
	GVRP (global)	Disabled
	GVRP (port interface)	Disabled
	QinQ Tunneling	Disabled

Table 2: System Defaults (Continued)

Function	Parameter	Default
Traffic Prioritization	Ingress Port Priority	0
	Queue Mode	Strict
	Weighted Round Robin	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
IP Settings	Management. VLAN	Any VLAN configured with an IP address
	IP Address	DHCP assigned
	Default Gateway	0.0.0.0
	DHCP	Client: Enabled Relay: Disabled Server: Disabled
	DNS	Client/Proxy service: Disabled
	BOOTP	Disabled
	ARP	Enabled Cache Timeout: 20 minutes Proxy: Disabled
Unicast Routing	RIP	Disabled
	OSPFv2	Disabled
Router Redundancy	VRRP	Disabled
Multicast Filtering	IGMP Snooping (Layer 2)	Snooping: Enabled Querier: Disabled
	IGMP (Layer 3) IGMP Proxy (Layer 3)	Disabled Disabled
System Log	Status	Enabled
	Messages Logged	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

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 71.

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 5.x or above, Netscape 6.2 or above, and Mozilla Firefox 2.0.0.0 or above. 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
- Set the speed/duplex mode for 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 4093 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
- Enable port mirroring
- Set storm control on any port for excessive broadcast 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 port to RJ-45 adapter 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 port adapter provided with this package, or use a DB-9 to RJ-45 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 567. For a list of all the CLI commands and detailed information on using the CLI, refer to "CLI Command Groups" on page 576.

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 71.

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

NOTE: Any VLAN group can be assigned an IP interface address (page 71) for managing the switch.

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 5.0 or above, Netscape 6.2 or above, or Mozilla Firefox 2.0.0.0 or above), 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.

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 8 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 ECS4610-24F 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 stack 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.

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: An IPv4 address for this switch 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
```

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
 IP address and netmask: 192.168.1.54 255.255.255.0 on VLAN 1,
 and address mode: DHCP
Console#copy running-config startup-config
Startup configuration file name []: startup
\Write to FLASH Programming.

\Write to FLASH finish.
Success.
```

ENABLING SNMP MANAGEMENT ACCESS

The switch can be configured to accept management commands from Simple Network Management Protocol (SNMP) applications such as EdgeCore ECView. 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 360).

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 634. 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 354, or refer to the specific CLI commands for SNMP starting on page 629

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 76 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 106 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 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 81
- "Basic Management Tasks" on page 101
- "Interface Configuration" on page 125
- "VLAN Configuration" on page 153
- "Address Table Settings" on page 187
- "Spanning Tree Algorithm" on page 195
- "Rate Limit Configuration" on page 219
- "Storm Control Configuration" on page 221
- "Class of Service" on page 223
- "Quality of Service" on page 223
- "VoIP Traffic Configuration" on page 239
- "Security Measures" on page 245
- "Basic Administration Protocols" on page 335
- "Multicast Filtering" on page 387
- "IP Configuration" on page 431
- "General IP Routing" on page 435
- "Configuring Router Redundancy" on page 453
- "IP Services" on page 463

- "Unicast Routing" on page 483
- "Multicast Routing" on page 541

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 5.0 or above, Netscape 6.2 or above, or Mozilla Firefox 2.0.0.0 or above).

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 567."

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 71.)

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 70.)

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 205.

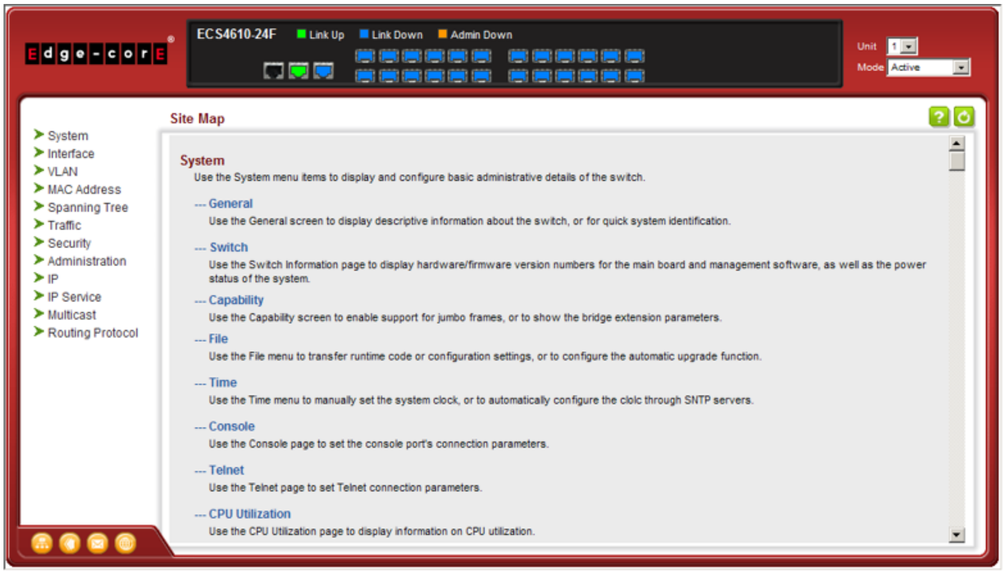
NAVIGATING THE WEB BROWSER INTERFACE

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



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 clolc 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 manufacturer'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 3: Web Page Configuration Buttons

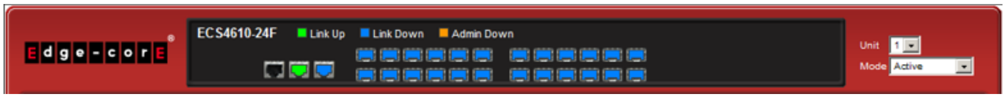
Button	Action
Apply	Sets specified values to the system.
Revert	Cancels specified values and restores current values prior to pressing "Apply."
Help	Links directly to web help.

NOTE: To ensure proper screen refresh, be sure that Internet Explorer 5.x is configured as follows: Under the menu "Tools / Internet Options / General / Temporary Internet Files / Settings," the setting for item "Check for newer versions of stored pages" should be "Every visit to the page."

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 4: Switch Main Menu

Menu	Description	Page
System		
General	Provides basic system description, including contact information	101
Switch	Shows the number of ports, hardware version, power status, and firmware version numbers	103
Capability	Enables support for jumbo frames; shows the bridge extension parameters	104, 105
File		106
Copy	Allows the transfer and copying files	106
Set Startup	Sets the startup file	110
Show	Shows the files stored in flash memory; allows deletion of files	110
Time		111
Configure General		
Manual	Manually sets the current time	111
SNTP	Configures SNTP polling interval	112
Configure Time Server	Configures a list of SNTP servers	113
Configure Time Zone	Sets the local time zone for the system clock	114
Console	Sets console port connection parameters	115
Telnet	Sets Telnet connection parameters	117
CPU Utilization	Displays information on CPU utilization;	118
Memory Status	Shows memory utilization parameters	119
Reset	Restarts the switch immediately, at a specified time, after a specified delay, or at a periodic interval	120
Interface		
Port		
General		
Configure by Port List	Configures connection settings per port	125
Configure by Port Range	Configures connection settings for a range of ports	128
Show Information	Displays port connection status	128
Mirror		
Add	Sets the source and target ports for mirroring	130
Show	Shows the configured mirror sessions	130
Statistics	Shows Interface, Etherlike, RMON and Utilization port statistics	131
Chart	Shows Interface, Etherlike, RMON and Utilization port statistics	131

Table 4: Switch Main Menu (Continued)

Menu	Description	Page
Trunk		
Static		
Configure Trunk		
Add	Creates a trunk, along with the first port member	136
Show	Shows the configured trunk identifiers	136
Add Member	Specifies ports to group into static trunks	136
Show Member	Shows the port members for the selected trunk	136
Configure General		
Configure	Configures trunk connection settings	136
Show Information	Displays trunk connection settings	136
Dynamic		139
Configure Aggregator	Configures administration key for specific LACP groups	139
Configure Aggregation Port		
Configure		
General	Allows ports to dynamically join trunks	139
Actor	Configures parameters for link aggregation group members on the local side	139
Partner	Configures parameters for link aggregation group members on the remote side	139
Show Information		
Counters	Displays statistics for LACP protocol messages	144
Internal	Displays configuration settings and operational state for the local side of a link aggregation	145
Neighbors	Displays configuration settings and operational state for the remote side of a link aggregation	147
Configure Trunk		
Configure	Configures connection settings	139
Show	Displays port connection status	139
Show Member	Shows the active members in a trunk	139
Statistics	Shows Interface, Etherlike, RMON and Utilization trunk statistics	131
Chart	Shows Interface, Etherlike, RMON and Utilization trunk statistics	131
Traffic Segmentation		
Configure Global	Enables traffic segmentation globally	149
Configure Session	Configures the uplink and down-link ports for a segmented group of ports	150
VLAN Trunking	Allows unknown VLAN groups to pass through the specified interface	151

Table 4: Switch Main Menu (Continued)

Menu	Description	Page
VLAN	Virtual LAN	
Static		
Add	Creates VLAN groups	156
Show	Displays configured VLAN groups	156
Modify	Configures group name and administrative status	156
Edit Member by VLAN	Specifies VLAN attributes per VLAN	158
Edit Member by Interface	Specifies VLAN attributes per interface	158
Edit Member by Interface Range	Specifies VLAN attributes per interface range	158
Dynamic		
Configure General	Enables GVRP VLAN registration protocol globally	163
Configure Interface	Configures GVRP status and timers per interface	163
Show Dynamic VLAN		
Show VLAN	Shows the VLANs this switch has joined through GVRP	163
Show VLAN Member	Shows the interfaces assigned to a VLAN through GVRP	163
Private		
Configure VLAN		
Add	Creates primary or community VLANs	167
Show	Display configured primary and community VLANs	167
Add Community VLAN	Associates a community VLAN with a primary VLAN	168
Show Community VLAN	Shows the community VLANs associated with a primary VLAN	168
Configure Interface	Sets the private VLAN interface type, and associates the interfaces with a private VLAN	169
Tunnel	IEEE 802.1Q (QinQ) Tunneling	171
Configure Global	Sets tunnel mode for the switch	175
Configure Interface	Sets the tunnel mode for any participating interface	176
Protocol		
Configure Protocol		
Add	Creates a protocol group, specifying supported protocols	178
Show	Shows configured protocol groups	178
Configure Interface		
Add	Maps a protocol group to a VLAN	180
Show	Shows the protocol groups mapped to each VLAN	180
IP Subnet		
Add	Maps IP subnet traffic to a VLAN	182
Show	Shows IP subnet to VLAN mapping	182

Table 4: Switch Main Menu (Continued)

Menu	Description	Page
MAC-Based		
Add	Maps traffic with specified source MAC address to a VLAN	184
Show	Shows source MAC address to VLAN mapping	184
MAC Address		
Learning Status	Enables MAC address learning on selected interfaces	187
Static		
Add	Configures static entries in the address table	189
Show	Displays static entries in the address table	189
Dynamic		
Configure Aging	Sets timeout for dynamically learned entries	190
Show Dynamic MAC	Displays dynamic entries in the address table	191
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	192
Spanning Tree		
Loopback Detection	Configures Loopback Detection parameters	198
STA	Spanning Tree Algorithm	
Configure Global		
Configure	Configures global bridge settings for STP, RSTP and MSTP	199
Show Informaton	Displays STA values used for the bridge	204
Configure Interface		
Configure	Configures interface settings for STA	205
Show Informaton	Displays interface settings for STA	209
MSTP	Multiple Spanning Tree Algorithm	
Configure Global		
Add	Configures initial VLAN and priority for an MST instance	212
Show	Configures global settings for an MST instance	212
Modify	Modify priority for an MST instance	212
Add Member	Adds VLAN members for an MST instance	212
Show Member	Displays or deletes VLAN members for an MST instance	212
Show Information	Displays MSTP values used for the bridge	212
Configure Interface		
Configure	Configures interface settings for an MST instance	216
Show Informaton	Displays interface settings for an MST instance	216
Traffic		
Rate Limit	Sets the input and output rate limits for a port	219
Storm Control	Sets the broadcast storm threshold for each interface	221

Table 4: Switch Main Menu (Continued)

Menu	Description	Page
DiffServ		
Configure Class		
Add	Creates a class map for a type of traffic	224
Show	Shows configured class maps	224
Modify	Modifies the name of a class map	224
Add Rule	Configures the criteria used to classify ingress traffic	224
Show Rule	Shows the traffic classification rules for a class map	224
Configure Policy		
Add	Creates a policy map to apply to multiple interfaces	227
Show	Shows configured policy maps	227
Modify	Modifies the name of a policy map	227
Add Rule	Sets the boundary parameters used for monitoring inbound traffic, and the action to take for conforming and non-conforming traffic	227
Show Rule	Shows the rules used to enforce bandwidth policing for a policy map	227
Configure Interface	Applies a policy map to an ingress port	237
VoIP	Voice over IP	239
Configure Global	Configures auto-detection of VoIP traffic, sets the Voice VLAN, and VLAN aging time	239
Configure OUI		241
Add	Maps the OUI in the source MAC address of ingress packets to the VoIP device manufacturer	241
Show	Shows the OUI telephony list	241
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	242
Security		245
AAA	Authentication, Authorization and Accounting	
System Authentication	Configures authentication sequence – local, RADIUS, and TACACS	247
Server		248
Configure Server	Configures RADIUS and TACACS server message exchange settings	248
Cconfigure Group		
Add	Specifies a group of authentication servers and sets the priority sequence	248
Show	Shows the authentication server groups and priority sequence	248
Accounting	Enables accounting of requested services for billing or security purposes	253
Configure Global	Specifies the interval at which the local accounting service updates information to the accounting server	253

Table 4: Switch Main Menu (Continued)

Menu	Description	Page
Configure Method		253
Add	Configures accounting for various service types	253
Show	Shows the accounting settings used for various service types	253
Configure Service	Sets the accouning method applied to specific interfaces for 802.1X, CLI command priivilege levels for the console port, and for Telnet	253
Show Information		253
Summary	Shows the configured accounting methods, and the methods applied to specific interfaces	253
Statistics	Shows basic accounting information recorded for user sessions	253
Authorization	Enables authorization of requested services	258
Configure Method		258
Add	Configures authorization for various service types	258
Show	Shows the authorization settings used for various service types	258
Configure Service	Sets the authorization method applied used for the console port, and for Telnet	258
Show Information	Shows the configured authorization methods, and the methods applied to specific interfaces	258
User Accounts		261
Add	Configures user names, passwords, and access levels	261
Show	Shows authorized users	261
Modify	Modifies user attributes	261
Network Access	MAC address-based network access authentication	262
Configure Global	Enables aging for authenticated MAC addresses, and sets the time period after which a connected MAC address must be reauthenticated	265
Configure Interface		266
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	266
Link Detection	Configures detection of changes in link status, and the response (i.e., send trap or shut down port)	268
Configure MAC Filter		269
Add	Specifies MAC addresses exempt from authentication	269
Show	Shows the list of exempt MAC addresses	269
Show Information	Shows the authenticated MAC address list	270
HTTPS	Secure HTTP	272
Configure Global	Enables HTTPs, and specifies the UDP port to use	272
Copy Certificate	Replaces the default secure-site certificate	274
SSH	Secure Shell	275
Configure Global	Configures SSH server settings	278

Table 4: Switch Main Menu (Continued)

Menu	Description	Page
Configure Host Key		279
Generate	Generates the host key pair (public and private)	279
Show	Displays RSA and DSA host keys; deletes host keys	279
Configure User Key		281
Copy	Imports user public keys from TFTP server	281
Show	Displays RSA and DSA user keys; deletes user keys	281
ACL	Access Control Lists	283
Configure Time Range	Confiures the time to apply an ACL	284
Add	Specifies the name of a time range	284
Show	Shows the name of configured time ranges	284
Add Rule		284
Absolute	Sets exact time or time range	284
Periodic	Sets a recurrent time	284
Show Rule	Shows the time specified by a rule	284
Configure ACL		286
Add	Adds an ACL based on IP or MAC addres filtering	286
Show	Shows the name and type of configured ACLs	286
Add Rule	Configures packet filtering based on IP or MAC addresses and other packet attributes	286
Show Rule	Shows the rules specified for an ACL	286
Configure Interface	Binds a port to the specified ACL and time range	300
ARP Inspection		301
Configure General	Enables inspection globally, configures validation of additional address components, and sets the log rate for packet inspection	302
Configure VLAN	Enables ARP inspection on specified VLANs	304
Configure Interface	Sets the trust mode for ports, and sets the rate limit for packet inspection	306
Show Information		
Show Statistics	Displays statistics on the inspection process	307
Show Log	Shows the inspection log list	308
IP Filter		309
Add	Sets IP addresses of clients allowed management access via the web, SNMP, and Telnet	309
Show	Shows the addresses to be allowed management access	309
Port Security	Configures per port security, including status, response for security breach, and maximum allowed MAC addresses	311
Port Authentication	IEEE 802.1X	313
Configure Global	Enables authentication and EAPOL pass-through	314

Table 4: Switch Main Menu (Continued)

Menu	Description	Page
Configure Interface	Sets authentication parameters for individual ports	316
Show Statistics	Displays protocol statistics for the selected port	320
IP Source Guard	Filters IP traffic based on static entries in the IP Source Guard table, or dynamic entries in the DHCP Snooping table	321
Port Configuration	Enables IP source guard and selects filter type per port	321
Static Binding		323
Add	Adds a static addresses to the source-guard binding table	323
Show	Shows static addresses in the source-guard binding table	323
Dynamic Binding	Displays the source-guard binding table for a selected interface	325
Administration		335
Log		335
System		335
Configure Global	Stores error messages in local memory	335
Show System Logs	Shows logged error messages	335
Remote	Configures the logging of messages to a remote logging process	337
SMTP	Sends an SMTP client message to a participating server	339
LLDP	Link Layer Discovery Protocol	340
Configure Global	Configures global LLDP timing parameters	340
Configure Interface	Sets the message transmission mode; enables SNMP notification; and sets the LLDP attributes to advetise	342
Show Local Device Information		345
General	Displays general information about the local device	345
Port/Trunk	Displays information about each interface	345
Show Remote Device Information		347
Port/Trunk	Displays information about a remote device connected to a port on this switch	347
Port/Trunk Details	Displays detailed information about a remote device connected to this switch	347
Show Device Statistics		352
General	Displays statistics for all connected remote devices	352
Port/Trunk	Displays statistics for remote devices on a selected port or trun	352
SNMP	Simple Network Management Protocol	354
Configure Global	Enables SNMP agent status, and sets related trap functions	356
Configure Engine		
Set Engine ID	Sets the SNMP v3 engine ID on this switch	357
Add Remote Engine	Sets the SNMP v3 engine ID for a remote device	358
Show Remote Engine	Shows configured engine ID for remote devices	358

Table 4: Switch Main Menu (Continued)

Menu	Description	Page
Configure View		360
Add View	Adds an SNMP v3 view of the OID MIB	360
Show View	Shows configured SNMP v3 views	360
Add OID Subtree	Specifies a part of the subtree for the selected view	360
Show OID Subtree	Shows the subtrees assigned to each view	360
Configure Group		363
Add	Adds a group with access policies for assigned users	363
Show	Shows configured groups and access policies	363
Configure User		
Add Community	Configures community strings and access mode	366
Show Community	Shows community strings and access mode	366
Add SNMPv3 Local User	Configures SNMPv3 users on this switch	368
Show SNMPv3 Local User	Shows SNMPv3 users configured on this switch	368
Change SNMPv3 Local User Group	Assign a local user to a new group	368
Add SNMPv3 Remote User	Configures SNMPv3 users from a remote device	370
Show SNMPv3 Remote User	Shows SNMPv3 users set from a remote device	370
Configure Trap		372
Add	Configures trap managers to receive messages on key events that occur this switch	372
Show	Shows configured trap managers	372
RMON	Remote Monitoring	376
Configure Global		
Add		
Alarm	Sets threshold bounds for a monitored variable	377
Event	Creates a response event for an alarm	380
Show		
Alarm	Shows all configured alarms	377
Event	Shows all configured events	380
Configure Interface		
Add		
History	Periodically samples statistics on a physical interface	382
Statistics	Enables collection of statistics on a physical interface	384
Show		
History	Shows sampling parameters for each entry in the history group	382
Statistics	Shows sampling parameters for each entry in the statistics group	384

Table 4: Switch Main Menu (Continued)

Menu	Description	Page
Show Details		
History	Shows sampled data for each entry in the history group	382
Statistics	Shows sampled data for each entry in the history group	384
IP		
General		
Routing Interface		
Add	Configures an IP interface for a VLAN	431
Show	Shows the IP interfaces assigned to a VLAN	431
Ping	Sends ICMP echo request packets to another node on the network	439
Trace Route	Shows the route packets take to the specified destination	440
ARP	Address Resolution Protocol	441
Configure General	Sets the protocol timeout, and enables or disables proxy ARP for the specified VLAN	442
Configure Static Address		444
Add	Statically maps a physical address to an IP address	444
Show	Shows the MAC to IP address static table	444
Show Information		
Dynamic Address	Shows dynamically learned entries in the IP routing table	445
Other Address	Shows internal addresses used by the switch	445
Statistics	Shows statistics on ARP requests sent and received	446
Routing		
Static Routes		447
Add	Configures static routing entries	447
Show	Shows static routing entries	447
Modify	Modifies the selected static routing entry	447
Routing Table		
Show Information	Shows all routing entries, including local, static and dynamic routes	449
Configure ECMP Number	Sets the maximum number of equal-cost paths to the same destination that can be installed in the routing table	450
VRRP	Virtual Router Redundancy Protocol	453
Configure Group ID		454
Add	Adds a VRRP group identifier to a VLAN	454
Show	Shows the VRRP group identifier list	454
Add IP Address	Sets a virtual interface address for a VRRP group	454
Show IP Addresses	Shows the virtual interface address assigned to a VRRP group	454

Table 4: Switch Main Menu (Continued)

Menu	Description	Page
Configure Detail	Configure detailed settings, such as advertisement interval, preemption, priority, and authentication	454
Show Statistics		
Global Statistics	Displays global statistics for VRRP protocol packet errors	460
Group Statistics	Displays statistics for VRRP protocol events and errors on the specified VRRP group and interface	461
IP Service		
DNS	Domain Name Service	463
General		
Configure Global	Enables DNS lookup; defines the default domain name appended to incomplete host names	463
Add Domain Name	Defines a list of domain names that can be appended to incomplete host names	464
Show Domain Names	Shows the configurred domain name list	464
Add Name Server	Specifies IP address of name servers for dynamic lookup	466
Show Name Servers	Shows the name server address list	466
Static Host Table		
Add	Configures static entries for domain name to address mapping	467
Show	Shows the list of static mapping entries	467
Modify	Modifies the static address mapped to the selected host name	467
Cache	Displays cache entries discovered by designated name servers	468
DHCP	Dynamic Host Configuration Protocol	469
Relay	Specifies DHCP relay servers	470
Snooping		326
Configure Global	Enables DHCP snooping globally, MAC-address verification, information option;and sets the information policy	329
Configure VLAN	Enables DHCP snooping on a VLAN	330
Configure Interface	Sets the trust mode for an interface	331
Show Information	Displays the DHCP Snooping binding information	332
Server		471
Configure Global	Enables DHCP service on this switch	471
Configure Excluded Address		472
Add	Adds excluded addresses	472
Show	Shows excluded addresses	472
Configure Pool		473
Add		473
Network	Add address pool for network groups	473

Table 4: Switch Main Menu (Continued)

Menu	Description	Page
Host	Add address entry for specified host	473
Show	Shows DHCP pool list	473
Modify	Modifies the specified pool entry	473
Show IP Binding	Displays addresses currently bound to DHCP clients	477
UDP Helper		478
General	Enables UDP helper globally on the switch	478
Forwarding		479
Add	Specifies the UDP destination ports for which broadcast traffic will be forwarded	479
Show	Shows the list of UDP ports to which broadcast traffic will be forwarded	479
Address		480
Add	Specifies the servers to which designated UDP protocol packets are forwarded	480
Show	Shows the servers to which designated UDP protocol packets are forwarded	480
Multicast		387
IGMP Snooping		389
General	Enables multicast filtering; configures parameters for multicast snooping	391
Multicast Router		395
Add Static Multicast Router	Assigns ports that are attached to a neighboring multicast router	395
Show Static Multicast Router	Displays ports statically configured as attached to a neighboring multicast router	395
Show Current Multicast Router	Displays ports attached to a neighboring multicast router, either through static or dynamic configuration	395
IGMP Member		397
Add Static Member	Statically assigns multicast addresses to the selected VLAN	397
Show Static Member	Shows multicast addresses stataically configured on the selected VLAN	397
Show Current Member	Shows multicast addresses associated with the selected VLAN, either through static or dynamic configuration	397
Interface		399
Configure	Configures IGMP snooping per VLAN interface	399
Show	Shows IGMP snooping settings per VLAN interface	399
Forwarding Entry	Displays the current multicast groups learned through IGMP Snooping	404
Filter		405
Configure General	Enables IGMP filtering for the switch	405
Configure Profile		406
Add	Adds IGMP filter profile; and sets access mode	406

Table 4: Switch Main Menu (Continued)

Menu	Description	Page
Show	Shows configured IGMP filter profiles	406
Add Multicast Group Range	Assigns multicast groups to selected profile	406
Show Multicast Group Range	Shows multicast groups assigned to a profile	406
Configure Interface	Assigns IGMP filter profiles to port interfaces and sets throttling action	409
IGMP	Internet Group Management Protocol	410
Proxy	Configures IGMP proxy service for multicast routing	411
Interface	Configures Layer 3 IGMP settings for the selected VLAN interface	413
Static Group		416
Add	Configures the router to be a static member of a multicast group on the specified VLAN interface	416
Show	Shows multicast group statically assigned to a VLAN interface	416
Group Information		418
Show Information	Shows the current multicast groups learned through IGMP for each VLAN	418
Show Detail	Shows detailed information on each multicast group associated with a VLAN interface	418
Multicast Routing		541
General	Globally enables multicast routing	544
Information		544
Show Summary	Shows each multicast route the switch has learned	544
Show Detail	Shows additional information for each multicast route the switch has learned, including upstream router, and downstream interfaces	544
MVR	Multicast VLAN Registration	420
Configure General	Globally enables MVR, sets the MVR VLAN	422
Configure Group Range		
Add	Configures multicast stream addresses	423
Show	Shows multicast stream addresses	423
Configure Interface	Configures MVR interface type and immediate leave status	424
Configure Static Group Member		427
Add	Statically assigns MVR multicast streams to an interface	427
Show	Show MVR multicast streams statically assigned to an interface	427
Show Member	Shows information about the interfaces associated with multicast groups assigned to the MVR VLAN	428

Table 4: Switch Main Menu (Continued)

Menu	Description	Page
Routing Protocol		
RIP	Routing Information Protocol	484
General		485
Configure	Enables or disables RIP, sets the global RIP attributes and timer values	485
Clear Route	Clears the specified route type or network interface from the routing table	488
Network		489
Add	Sets the network interfaces that will use RIP	489
Show	Shows the network interfaces that will use RIP	489
Passive Interface		491
Add	Stops RIP broadcast and multicast messages from being sent on specified network interfaces	491
Show	Shows the configured passive interfaces	491
Neighbor Address		492
Add	Configures the router to directly exchange routing information with a static neighbor	492
Show	Shows adjacent hosts or interfaces configured as a neighboring router	492
Redistribute		493
Add	Imports external routing information from other routing domains (that is, protocols) into the autonomous system	493
Show	Shows the external routing information to be imported from other routing domains	493
Distance		495
Add	Defines an administrative distance for external routes learned from other routing protocols	495
Show	Shows the administrative distances assigned to external routes learned from other routing protocols	495
Interface		496
Add	Configures RIP parameters for each interface, including send and receive versions, authentication, and method of loopback prevention	496
Show	Shows the RIP parameters set for each interface	496
Modify	Modifies RIP parameters for an interface	496
Statistics		
Show Interface Information	Shows RIP settings, and statistics on RIP protocol messages	500
Show Peer Information	Displays information on neighboring RIP routers	501
Reset Statistics	Clears statistics for RIP protocol messages	502

Table 4: Switch Main Menu (Continued)

Menu	Description	Page
OSPF	Open Shortest Path First (Version 2)	502
Network Area		504
Add	Defines OSPF area address, area ID, and process ID	504
Show	Shows configured areas	504
Show Process	Show configured processes	504
System		507
Configure	Configures the Router ID, global settings, and default information	507
Show	Shows LSA statistics, administrative status, ABR/ASBR, area count, and version number	510
Area		512
Configure Area		512
Add Area	Adds NSSA or stub	512
Show Area	Shows configured NSSA or stub	512
Configure NSSA Area	Configures settings for importing routes into or exporting routes out of not-so-stubby areas	513
Configure Stub Area	Configures default cost, and settings for importing routes into a stub	516
Show Information	Shows statistics for each area, including SPF startups, ABR/ASBR count, LSA count, and LSA checksum	518
Area Range		519
Add	Configures route summaries to advertise at an area boundary	519
Show	Shows route summaries advertised at an area boundary	519
Modify	Modifies route summaries advertised at an area boundary	519
Redistribute		521
Add	Redistributes routes from one routing domain to another	521
Show	Shows route types redistributed to another domain	521
Modify	Modifies configuration settings for redistributed routes	521
Summary Address		523
Add	Aggregates routes learned from other protocols for advertising into other autonomous systems	523
Show	Shows configured summary addresses	523
Interface		525
Configure by VLAN	Configures OSPF protocol settings and authentication for specified VLAN	525
Configure by Address	Configures OSPF protocol settings and authentication for specified interface address	525
Show MD5 Key	Shows MD5 key ID used for each areaa	525
Virtual Link		531
Add	Configures a virtual link through a transit area to the backbone	531

Table 4: Switch Main Menu (Continued)

Menu	Description	Page
Show	Shows virtual links, neighbor address, and state	531
Configure Detailed Settings	Configures detailed protocol and authentication settings	531
Show MD5 Key	Shows the MD5 key ID used for each neighbor	531
Information		
LSDB	Shows information about different OSPF Link State Advertisements (LSAs)	534
Virtual Link	Shows information about virtual links	536
Neighbor	Shows information about each OSPF neighbor	538
PIM	Protocol Independent Multicasting	548
General	Enables PIM globally for the switch	548
Interface	Enables PIM per interface, and sets the mode to dense or sparse	548
Neighbor	Displays information neighboring PIM routers	554
PIM-SM	Protocol Independent Multicasting – Sparse Mode	
Configure Global	Configures settings for register messages, and use of the SPT	554
BSR Candidate	Configures the switch as a BSR candidate	556
RP Address		557
Add	Sets a static address for an RP and the associated multicast group(s)	557
Show	Shows the static addresses configured for each RP and the associated multicast groups	557
RP Candidate		559
Add	Advertises the switch as an RP candidate to the BSR for the specified multicast groups	559
Show	Shows the multicast groups for which this switch is advertising itself as an RP candidate to the BSR	559
Show Information		
Show BSR Router	Displays information about the BSR	561
Show RP Mapping	Displays the active RPs and associated multicast routing entries	563

4 Basic Management Tasks

This chapter describes the following topics:

- Displaying System Information – Provides basic system description, including contact information.
- Displaying Switch 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 SNTP servers.
- Console Port Settings – Sets console port connection parameters.
- 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 587
- "SNMP Commands" on page 629

PARAMETERS

These parameters are displayed in the web interface:

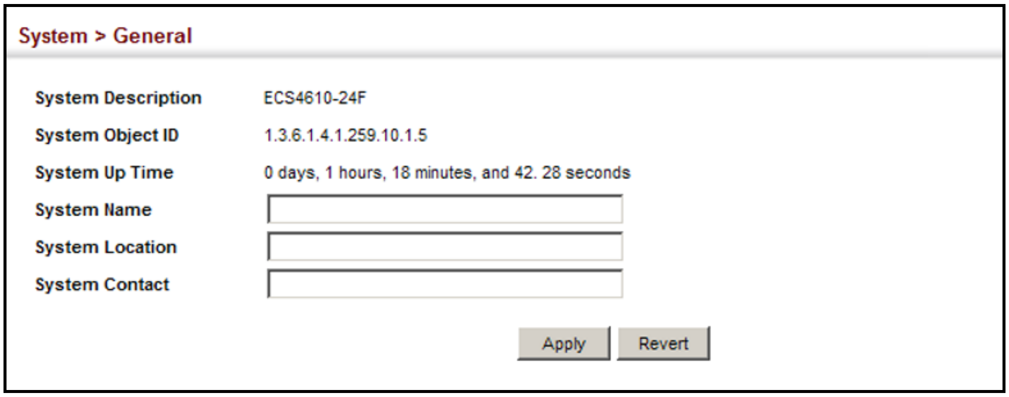
- **System Description** – Brief description of device type.
- **System Object ID** – MIB II object ID for switch's network management subsystem.
- **System Up Time** – Length of time the management agent has been up.
- **System Name** – Name assigned to the switch system.
- **System Location** – Specifies 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	ECS4610-24F
System Object ID	1.3.6.1.4.1.259.10.1.5
System Up Time	0 days, 1 hours, 18 minutes, and 42. 28 seconds
System Name	
System Location	
System Contact	

NOTE: This page also includes a Telnet button that allows access to the Command Line Interface via Telnet.

DISPLAYING SWITCH 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 587

PARAMETERS

The following parameters are displayed in the web interface:

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.
- **Internal Power Status** – Displays the status of the internal power supply.

Management Software Information

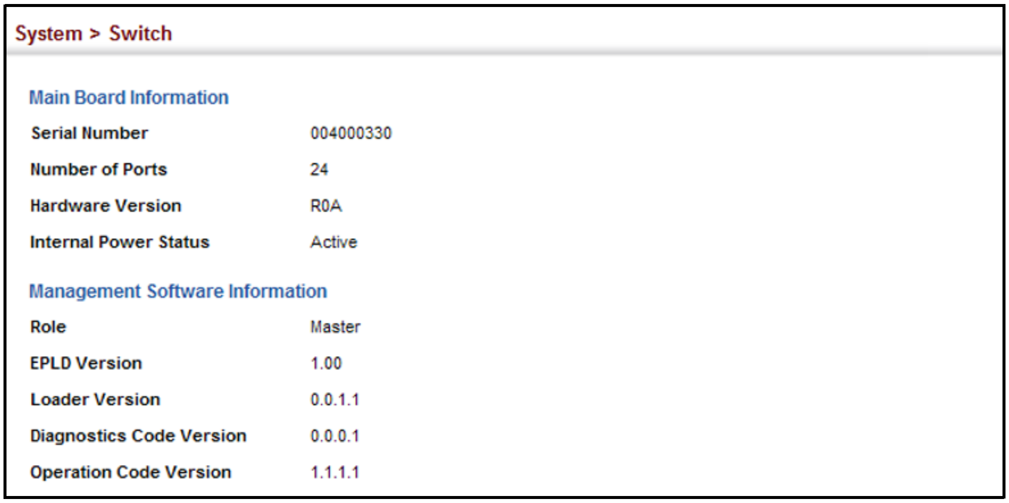
- **Role** – Shows that this switch is operating as Master or Slave.
- **EPLD Version** – Version number of EEPROM Programmable Logic Device.
- **Loader Version** – Version number of loader code.
- **Diagnostics Code Version** – Version of Power-On Self-Test (POST) and boot code.
- **Operation Code Version** – Version number of runtime code.

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	004000330
Number of Ports	24
Hardware Version	R0A
Internal Power Status	Active

Management Software Information

Role	Master
EPLD Version	1.00
Loader Version	0.0.1.1
Diagnostics Code Version	0.0.0.1
Operation Code Version	1.1.1.1

CONFIGURING SUPPORT FOR JUMBO FRAMES

Use the System > Capability page to configure support for jumbo frames. The switch provides more efficient throughput for large sequential data transfers by supporting jumbo frames up to 9216 bytes for Gigabit Ethernet. 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

- "System Management Commands" on page 587

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.

PARAMETERS

The following parameters are displayed in the web interface:

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

WEB INTERFACE

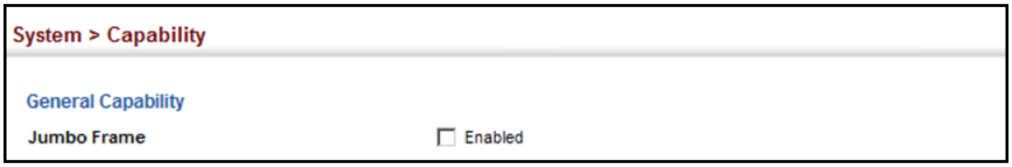
To configure support for jumbo frames:

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 832

PARAMETERS

The following parameters are displayed in the web interface:

- **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 223.)

- **Static Entry Individual Port** – This switch allows static filtering for unicast and multicast addresses. (Refer to "Setting Static Addresses" on page 189.)

- **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 153.)

- **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.

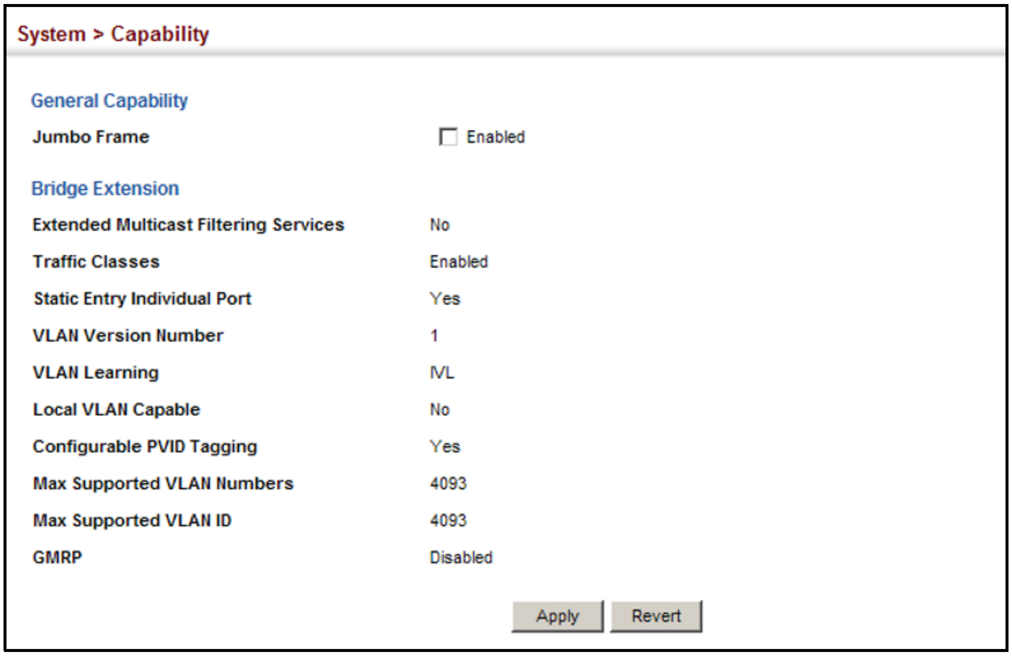
- **GMRP** – GARP Multicast Registration Protocol (GMRP) allows network devices to register end stations with multicast groups. This switch does not support GMRP; it uses the Internet Group Management Protocol (IGMP) to provide automatic multicast filtering.

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	4093
Max Supported VLAN ID	4093
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 or 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 595

PARAMETERS

The following parameters are displayed in the web interface:

- **Copy Type** – The firmware copy operation includes these options:
  - FTP Upgrade – Copies a file from an FTP server to the switch.
  - FTP Download – Copies a file from the switch to an FTP server.
  - HTTP Upgrade – Copies a file from a management station to the switch.
  - HTTP Download – Copies a file from the switch to a management station
  - TFTP Upgrade – 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** – IP address of an FTP or 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 31 characters for files on the switch. (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.

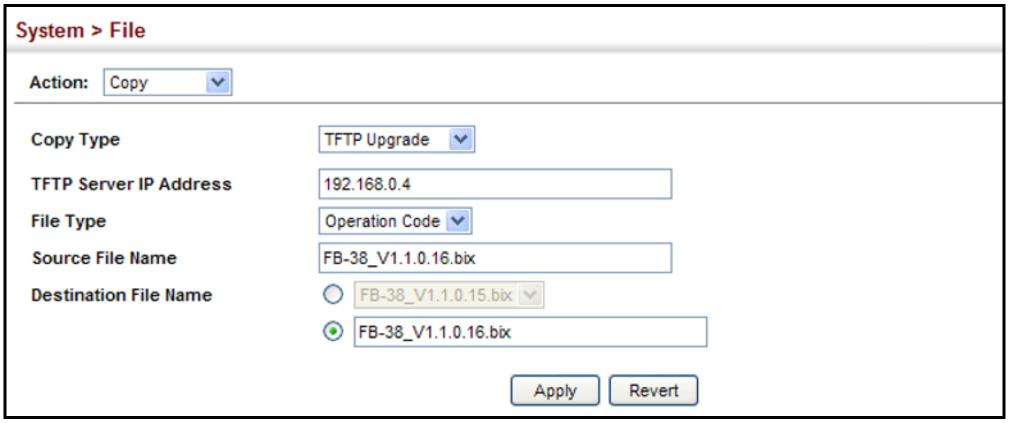
6. Set the file type to Operation Code.

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 Upgrade
TFTP Server IP Address	192.168.0.4
File Type	Operation Code
Source File Name	FB-38_V1.1.0.16.bix
Destination File Name	○ FB-38_V1.1.0.15.bix ● FB-38_V1.1.0.16.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 595

PARAMETERS

The following parameters are displayed in the web interface:

- **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 31 characters for files on the switch. (Valid characters: A-Z, a-z, 0-9, "." , "-", "_")

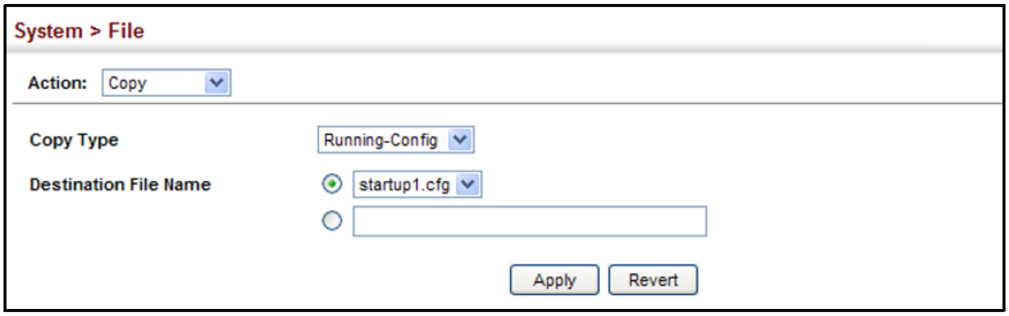
NOTE: The maximum number of user-defined configuration files is limited only by available flash memory space.

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 599
- "boot system" on page 594

WEB INTERFACE

To set a file to use for system initialization:

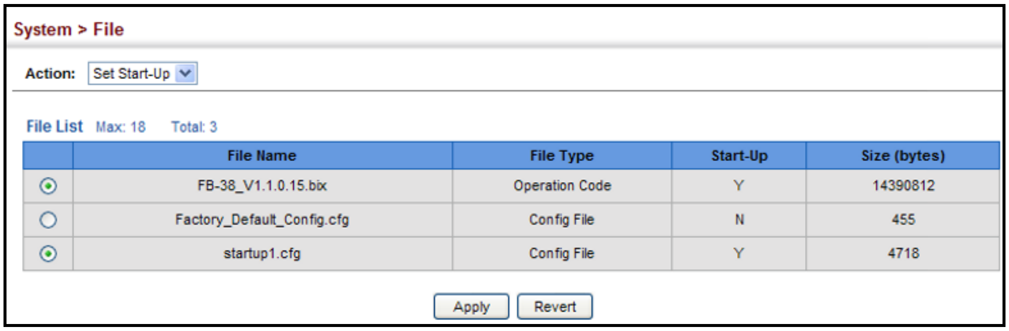
1. Click System, then File.

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



System > File

Action: Set Start-Up

File List Max: 18 Total: 3

	File Name	File Type	Start-Up	Size (bytes)
◉	FB-38_V1.1.0.15.bix	Operation Code	Y	14390812
○	Factory_Default_Config.cfg	Config File	N	455
◉	startup1.cfg	Config File	Y	4718

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 598
- "delete" on page 598

WEB INTERFACE

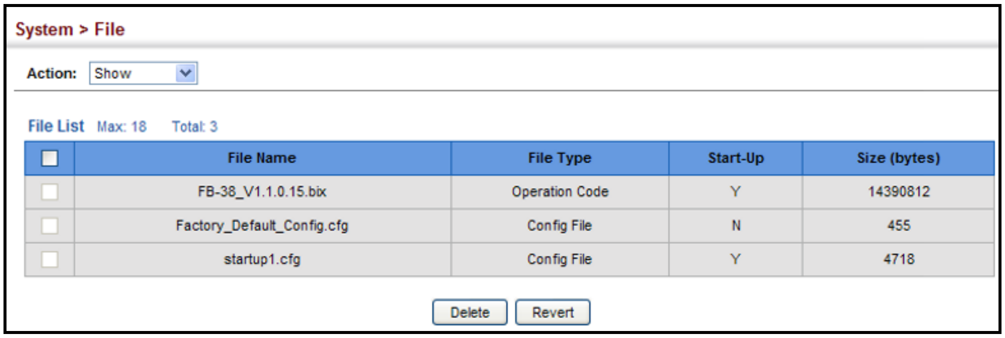
To show the system files:

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



System > File

Action: Show

File List Max: 18 Total: 3

□	File Name	File Type	Start-Up	Size (bytes)
□	FB-38_V1.1.0.15.bix	Operation Code	Y	14390812
□	Factory_Default_Config.cfg	Config File	N	455
□	startup1.cfg	Config File	Y	4718

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 - Manually) page to set the system time on the switch manually without using SNTP.

CLI REFERENCES

- "calendar set" on page 624
- "show calendar" on page 624

PARAMETERS

The following parameters are displayed in the web interface:

- **Current Time** – Shows the current time set on the switch.
- **Hours** – Sets the hour. (Range: 0-23; Default: 0)
- **Minutes** – Sets the minute value. (Range: 0-59; Default: 0)
- **Seconds** – Sets the second value. (Range: 0-59; Default: 0)
- **Month** – Sets the month. (Range: 1-12; Default: 1)

- **Day** – Sets the day of the month. (Range: 1-31; Default: 1)

- **Year** – Sets the year. (Range: 2001-2100; Default: 2009)

WEB INTERFACE

To manually set the system clock:

1. Click System, then Time.

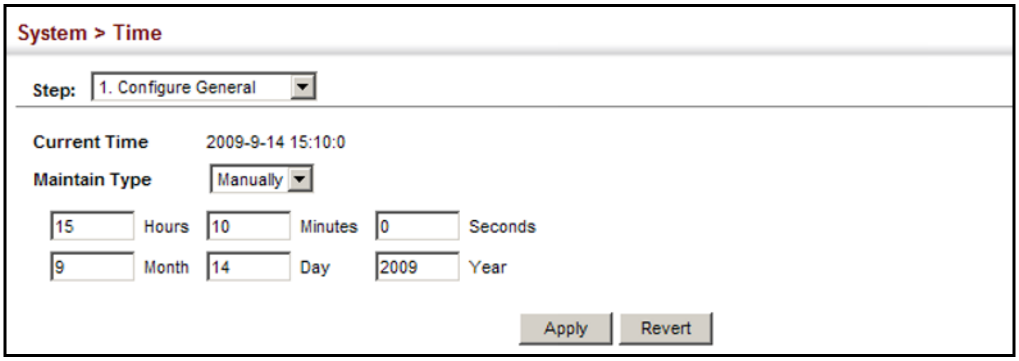
2. Select Configure General from the Action list.

3. Select Manual from the Maintain Type list.

4. Enter the time and date in the appropriate fields.

5. Click Apply

Figure 11: Manually Setting the System Clock



System > Time

Step: 1. Configure General

Current Time 2009-9-14 15:10:0

Maintain Type Manually

15 Hours 10 Minutes 0 Seconds

9 Month 14 Day 2009 Year

CONFIGURING SNTP

Use the System > Time (Configure General - SNTP) page to configure the switch to send time synchronization requests to time servers. Set the SNTP polling interval, SNTP servers, and also the time zone.

CLI REFERENCES

- "Time" on page 620

SETTING THE POLLING INTERVAL

Specify the polling interval at which the switch will query the time servers.

PARAMETERS

The following parameters are displayed in the web interface:

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

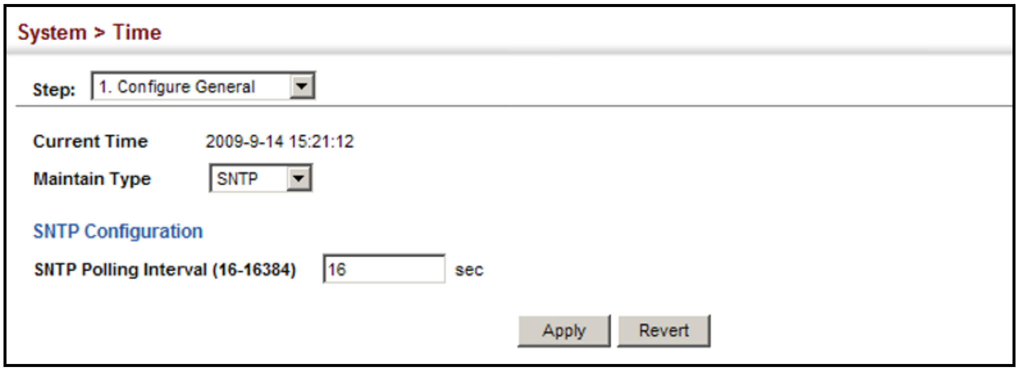
- **SNTP Polling Interval** – Sets the interval between sending requests for a time update from a time server. (Range: 16-16384 seconds; Default: 16 seconds)

WEB INTERFACE

To set the polling interval for SNTP:

1. Click System, then Time.
2. Select Configure General from the Action list.
3. Select SNTP from the Maintain Type list.
4. Modify the polling interval if required.
5. Click Apply

Figure 12: 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

SPECIFYING SNTP TIME SERVERS

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

CLI REFERENCES

- "sntp server" on page 622

PARAMETERS

The following parameters are displayed in the web interface:

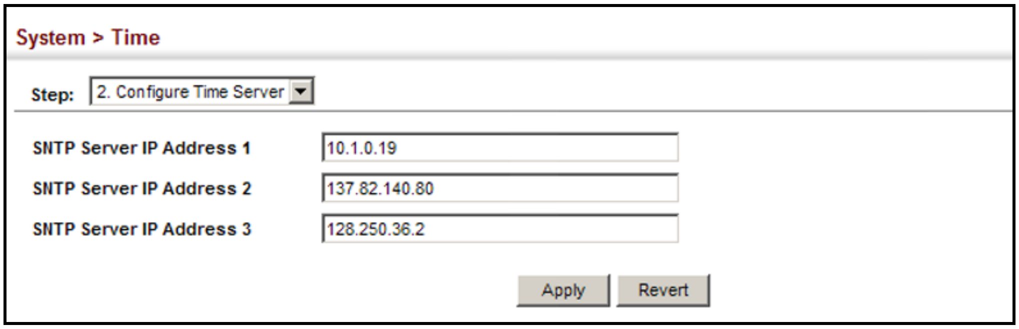
- **SNTP Server IP Address** – Sets the IPv4 or IPv6 address for up to three time servers. The switch attempts to update the time from the first server, if this fails it attempts an update from the next server in the sequence.

WEB INTERFACE

To set the SNTP time servers:

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

Figure 13: Specifying SNTP Time Servers



Step: 2. Configure Time Server

SNTP Server IP Address 1: 10.1.0.19

SNTP Server IP Address 2: 137.82.140.80

SNTP Server IP Address 3: 128.250.36.2

SETTING THE TIME ZONE

Use the System > Time (Configure Time Server) 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 east (before) or west (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.

PARAMETERS

The following parameters are displayed in the web interface:

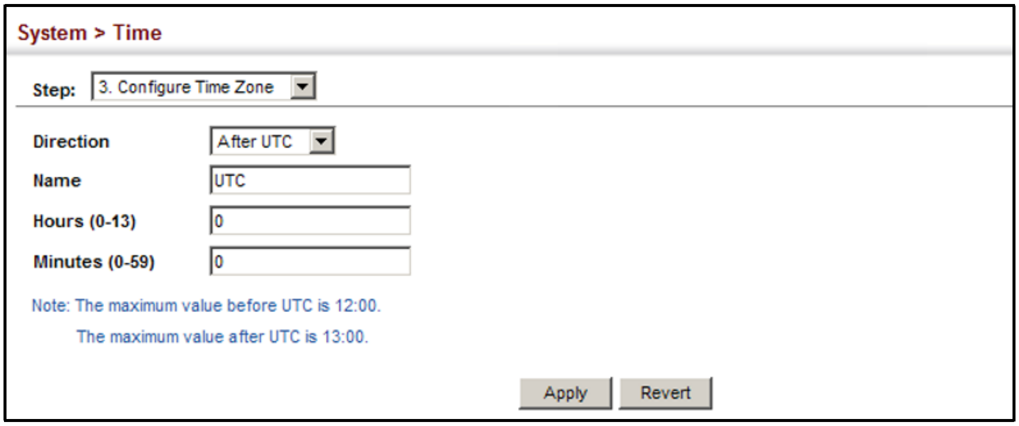
- **Direction**: Configures the time zone to be before (east of) or after (west of) UTC.
- **Name** – Assigns a name to the time zone. (Range: 1-29 characters)
- **Hours** (0-13) – The number of hours before/after UTC. The maximum value before UTC is 12. The maximum value after UTC is 13.
- **Minutes** (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 Action list.
3. Set the offset for your time zone relative to the UTC in hours and minutes.
4. Click Apply.

Figure 14: Setting the Time Zone



Step: 3. Configure Time Zone

Direction: After UTC

Name: UTC

Hours (0-13): 0

Minutes (0-59): 0

Note: The maximum value before UTC is 12:00.
The maximum value after UTC is 13:00.

CONSOLE PORT SETTINGS

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 600

PARAMETERS

The following parameters are displayed in the web interface:

- **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: 0-300 seconds; Default: 0 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: 0-65535 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: 0-120; Default: 3 attempts)

- **Quiet Period** – Sets the amount of time the management console is inaccessible after the number of unsuccessful logon attempts has been exceeded. (Range: 0-65535 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, or 38400 baud; Default: 115200 baud)

NOTE: The password for the console connection can only be configured through the CLI (see "password" on page 604).

NOTE: Password checking can be enabled or disabled for logging in to the console connection (see "login" on page 603). 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

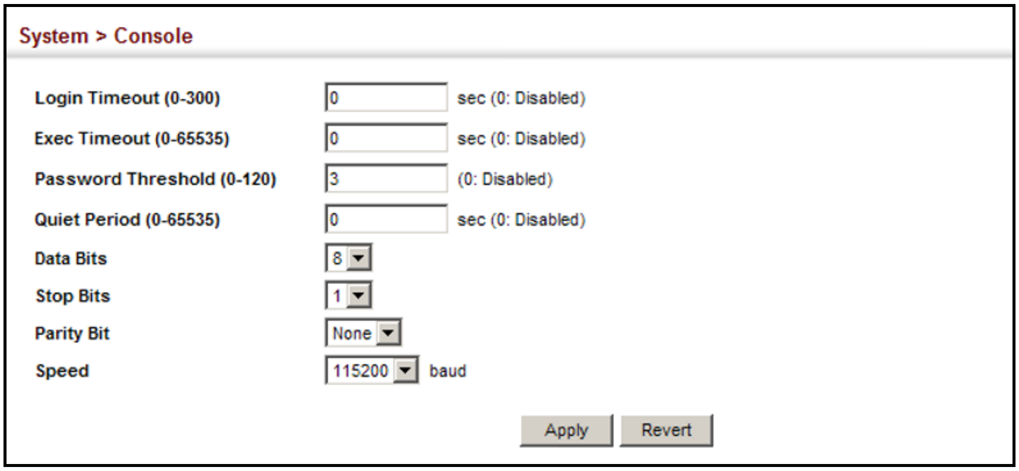
To configure parameters for the console port:

1. Click System, then Console.

2. Specify the connection parameters as required.

3. Click Apply

Figure 15: Console Port Settings



System > Console

Login Timeout (0-300)	0	sec (0: Disabled)
Exec Timeout (0-65535)	0	sec (0: Disabled)
Password Threshold (0-120)	3	(0: Disabled)
Quiet Period (0-65535)	0	sec (0: Disabled)
Data Bits	8	
Stop Bits	1	
Parity Bit	None	
Speed	115200	baud

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 600

PARAMETERS

The following parameters are displayed in the web interface:

- **Telnet Status** – Enables or disables Telnet access to the switch. (Default: Enabled)

- **TCP Port** – Sets the TCP port number for Telnet on the switch. (Default: 23)

- **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: 0-300 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: 0-65535 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: 0-120; Default: 3 attempts)

- **Quiet Period** – Sets the amount of time the management console is inaccessible after the number of unsuccessful logon attempts has been exceeded. (Range: 0-65535 seconds; Default: Disabled)

NOTE: The password for the Telnet connection can only be configured through the CLI (see "password" on page 604).

NOTE: Password checking can be enabled or disabled for login to the console connection (see "login" on page 603). 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

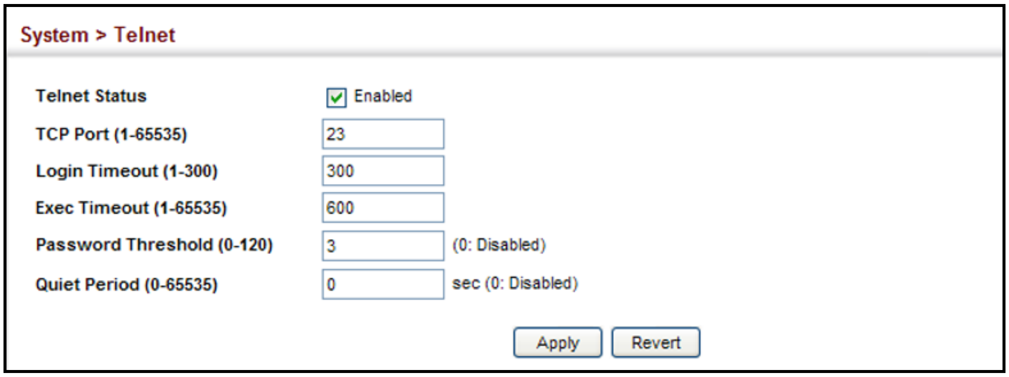
To configure parameters for the console port:

1. Click System, then Telnet.

2. Specify the connection parameters as required.

3. Click Apply

Figure 16: Telnet Connection Settings



System > Telnet

Telnet Status ☑ Enabled

TCP Port (1-65535) 23

Login Timeout (1-300) 300

Exec Timeout (1-65535) 600

Password Threshold (0-120) 3 (0: Disabled)

Quiet Period (0-65535) 0 sec (0: Disabled)

DISPLAYING CPU UTILIZATION

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

CLI REFERENCES

- no comparable command

PARAMETERS

The following parameters are displayed in the web interface:

- **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.

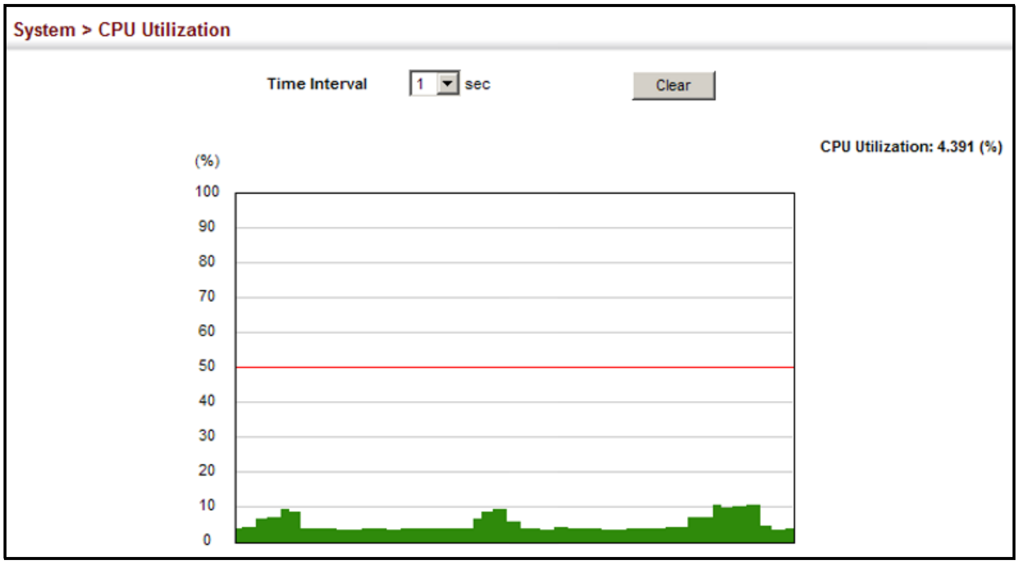
WEB INTERFACE

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 17: Displaying CPU Utilization



DISPLAYING MEMORY UTILIZATION

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

CLI REFERENCES

- no comparable command

PARAMETERS

The following parameters are displayed in the web interface:

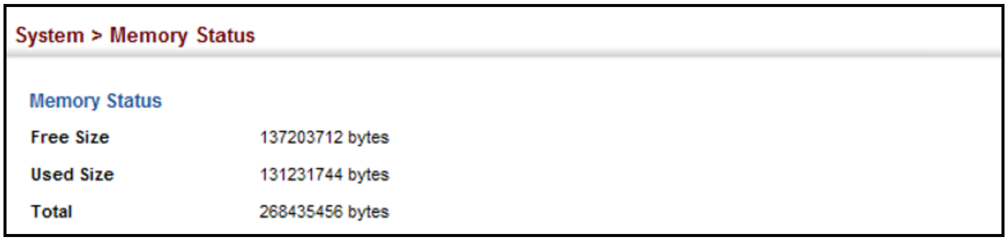
- **Free Size** – The amount of memory currently free for use.
- **Used Size** – The amount of memory allocated to active processes.
- **Total** – The total amount of system memory.

WEB INTERFACE

To display memory utilization:

1. Click System, then Memory Status.

Figure 18: Displaying Memory Utilization



Memory Status

Free Size	137203712 bytes
Used Size	131231744 bytes
Total	268435456 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 584
- "reload (Global Configuration)" on page 580
- "show reload" on page 585

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 595).

PARAMETERS

The following parameters are displayed in the web interface:

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 periodic interval at which to reload the switch.
    - DD - The day of the month at which to reload. (Range: 1-31)
    - MM - The month at which to reload. (january ... december)
    - YYYY - The year at which to reload. (Range: 2001-2050)
    - HH - The hour at which to reload. (Range: 0-23)
    - MM - The minute at which to reload. (Range: 0-59)

- **Regularly** – Specifies a periodic interval at which to reload the switch.

  Time

  - HH - The hour at which to reload. (Range: 0-23)
  - MM - The minute at which to reload. (Range: 0-59)

  Period

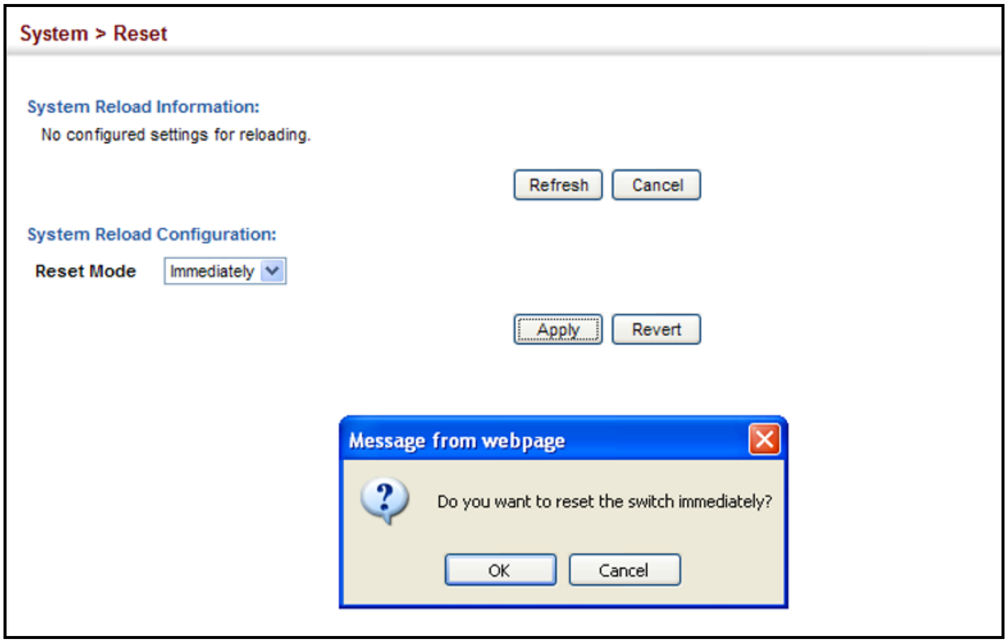
  - Daily - Every day.
  - Weekly - Day of the week at which to reload. (Range: Sunday ... Saturday)
  - Monthly - Day of the month at which to reload. (Range: 1-31)

WEB INTERFACE

To restart the switch:

1. Click System, then Reset.
2. Select the required rest 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 19: Restarting the Switch (Immediately)



System > Reset

System Reload Information:

No configured settings for reloading.

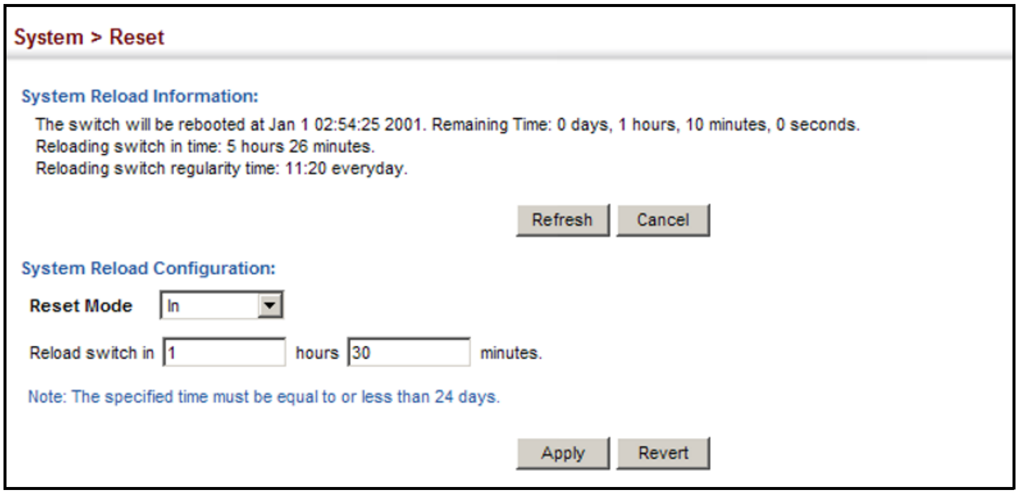
System Reload Configuration:

Reset Mode: Immediately

Message from webpage

Do you want to reset the switch immediately?

Figure 20: 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.

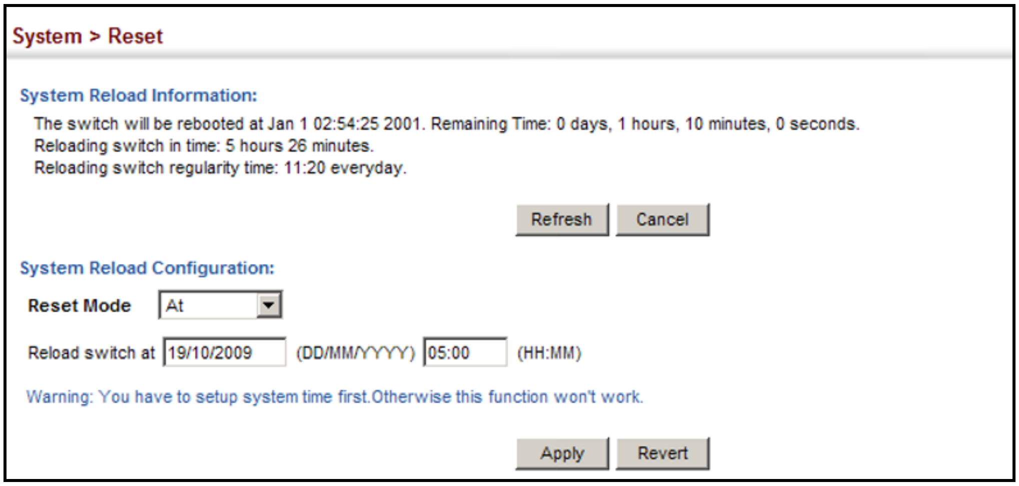
System Reload Configuration:

Reset Mode: In

Reload switch in 1 hours 30 minutes.

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

Figure 21: 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.

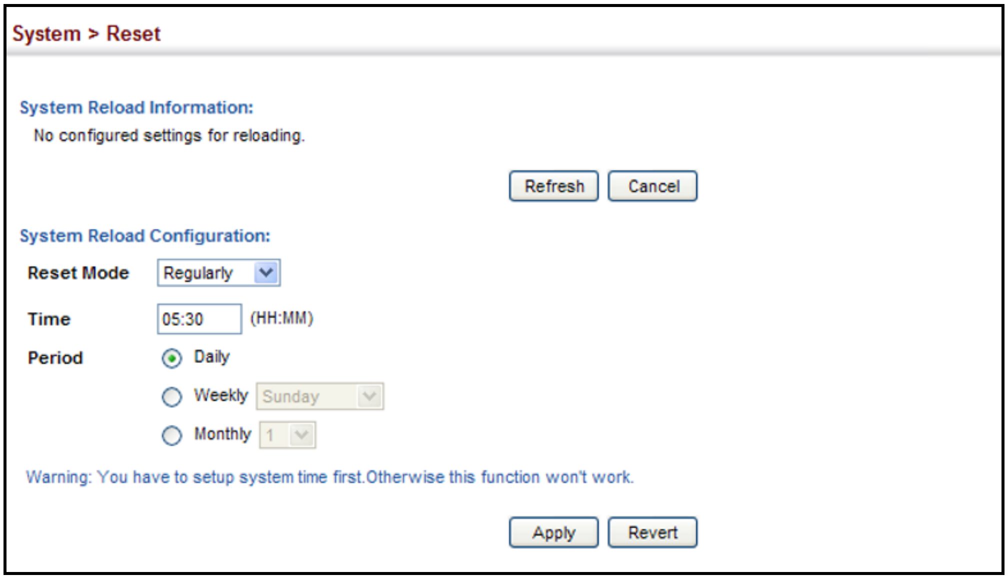
System Reload Configuration:

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 22: 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.
- Port Mirroring – Sets the source and target ports for mirroring on the local switch.
- Displaying Statistics – Shows Interface, Etherlike, and RMON port statistics in table or chart form.
- 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 769

COMMAND USAGE

- Auto-negotiation must be disabled before you can configure or force a Gigabit Ethernet 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 1000BASE-T standard does not support forced mode. Auto-negotiation should always be used to establish a connection over any 1000BASE-T port or trunk. If not used, the success of the link process cannot be guaranteed when connecting to other types of switches.

PARAMETERS

These parameters are displayed in the web interface:

- **Port** – Port identifier.
- **Type** – Indicates the port type. (1000Base-T, 1000Base 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.
- **Media Type** – Configures the forced/preferred port type to use for the combination ports.
  - **Copper-Forced** - Always uses the built-in RJ-45 port.
  - **SFP-Forced** - Always uses the SFP port, even if a module is not installed. (This is the default for Ports 3-24.)
  - **SFP-Preferred-Auto** - Uses SFP port if both combination types are functioning and the SFP port has a valid link. (This is the default for Ports 1-2.)
- **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.
  - **10half** - Supports 10 Mbps half-duplex operation
  - **10full** - Supports 10 Mbps full-duplex operation
  - **100half** - Supports 100 Mbps half-duplex operation
  - **100full** - Supports 100 Mbps full-duplex operation
  - **1000full** (Gigabit ports only) - Supports 1000 Mbps full-duplex operation
  - **Sym** - Check this item to transmit and receive pause frames.
  - **FC** - 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.

Avoid using flow control on a port connected to a hub unless it is actually required to solve a problem. Otherwise back pressure jamming signals may degrade overall performance for the segment attached to the hub.

(Default: Autonegotiation enabled on Gigabit ports, disabled on 10G ports; Advertised capabilities for
1000BASE-T – 10half, 10full, 100half, 100full, 1000full;
1000Base-SX/LX/LH – 1000full)

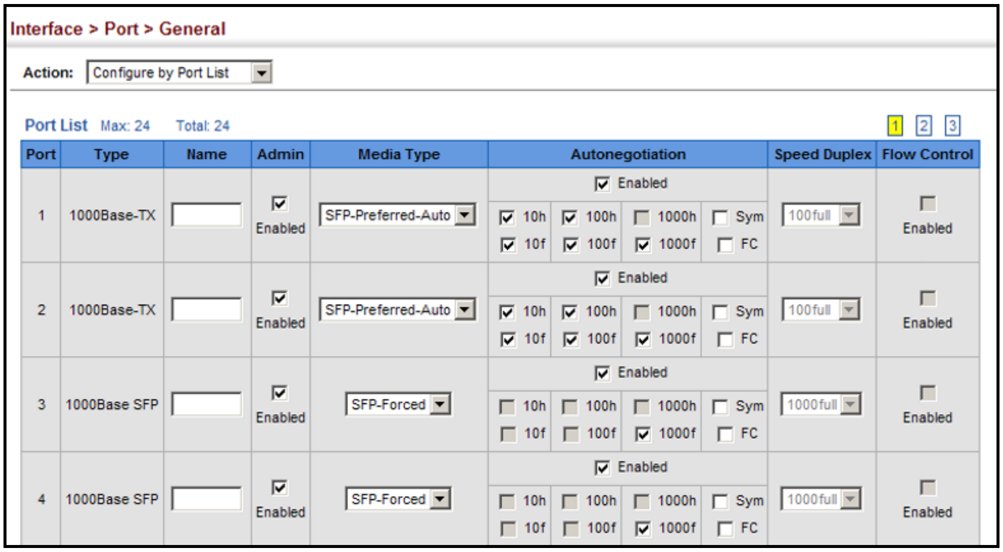
- **Speed/Duplex** – Allows you to manually set the port speed and duplex mode. (i.e., with auto-negotiation disabled)
- **Flow Control** – Allows automatic or manual selection of flow control.

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 23: Configuring Connections by Port List



Interface > Port > General

Action: Configure by Port List

Port List Max: 24 Total: 24

Port	Type	Name	Admin	Media Type	Autonegotiation	Speed Duplex	Flow Control
1	1000Base-TX		☑ Enabled	SFP-Preferred-Auto	☑ Enabled ☑ 10h ☑ 100h ☐ 1000h ☐ Sym ☑ 10f ☑ 100f ☑ 1000f ☐ FC	100full	☐ Enabled
2	1000Base-TX		☑ Enabled	SFP-Preferred-Auto	☑ Enabled ☑ 10h ☑ 100h ☐ 1000h ☐ Sym ☑ 10f ☑ 100f ☑ 1000f ☐ FC	100full	☐ Enabled
3	1000Base SFP		☑ Enabled	SFP-Forced	☑ Enabled ☐ 10h ☐ 100h ☐ 1000h ☐ Sym ☐ 10f ☐ 100f ☑ 1000f ☐ FC	1000full	☐ Enabled
4	1000Base SFP		☑ Enabled	SFP-Forced	☑ Enabled ☐ 10h ☐ 100h ☐ 1000h ☐ Sym ☐ 10f ☐ 100f ☑ 1000f ☐ FC	1000full	☐ Enabled

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 the 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 125.

CLI REFERENCES

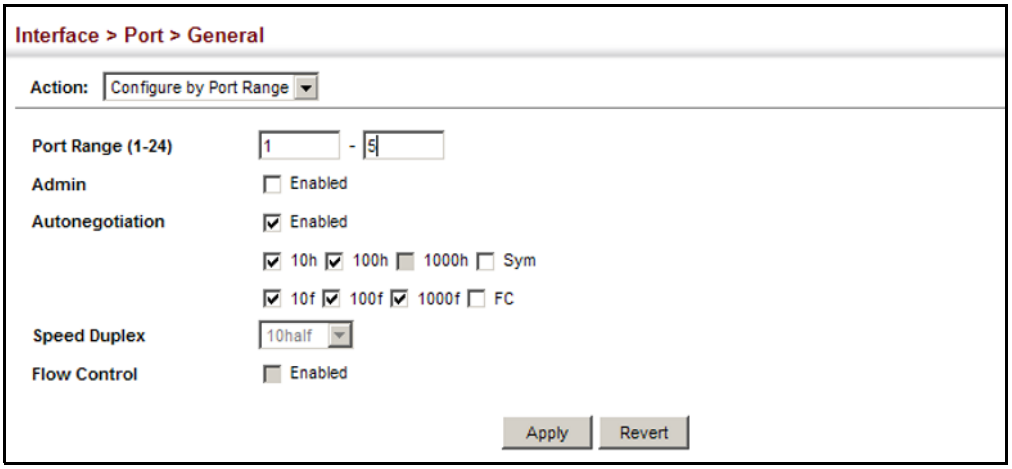
- "Interface Commands" on page 769

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 24: Configuring Connections by Port Range



Interface > Port > General

Action: Configure by Port Range

Port Range (1-24) 1 - 5

Admin □ Enabled

Autonegotiation ☑ Enabled

☑ 10h ☑ 100h □ 1000h □ Sym

☑ 10f ☑ 100f ☑ 1000f □ FC

Speed Duplex 10half

Flow Control □ Enabled

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 780

PARAMETERS

These parameters are displayed in the web interface:

- **Port** – Port identifier.
- **Type** – Indicates the port type. (1000Base-T, 1000Base 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. (Options: Ports 1-2 – Copper-Forced, SFP-Forced, or SFP-Preferred-Auto, Ports 3-24 – SFP-Forced; Default: Ports 1-2 – SFP-Preferred-Auto, Ports 3-24 – SFP-Forced)
- **Autonegotiation** – Shows if auto-negotiation is enabled or disabled.
- **Oper Speed Duplex** – Shows the current speed and duplex mode.
- **Oper Flow Control** – Shows if flow control is enabled or disabled.

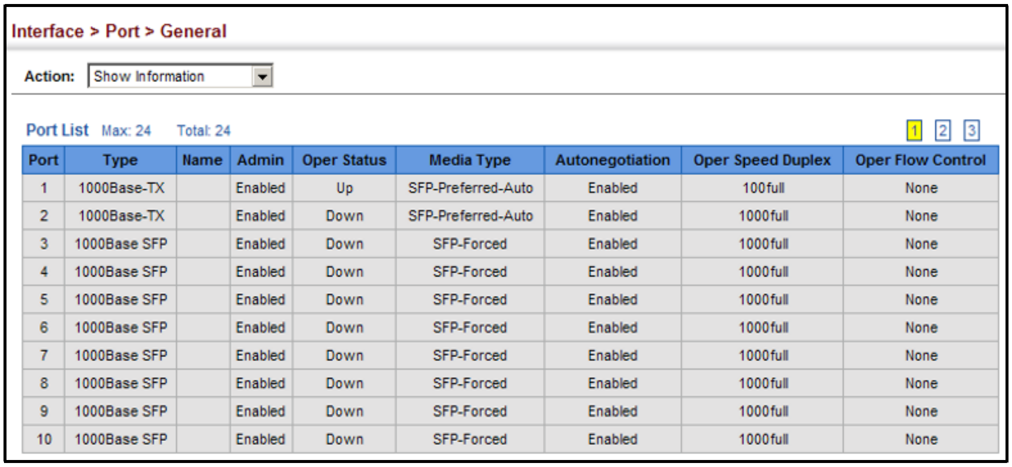
WEB INTERFACE

To display port connection parameters:

1. Click Interface, Port, General.

2. Select Show Information from the Action List.

Figure 25: Displaying Port Information



Interface > Port > General

Action: Show Information

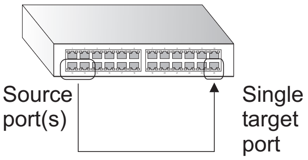
Port List Max: 24 Total: 24

Port	Type	Name	Admin	Oper Status	Media Type	Autonegotiation	Oper Speed Duplex	Oper Flow Control
1	1000Base-TX		Enabled	Up	SFP-Preferred-Auto	Enabled	100full	None
2	1000Base-TX		Enabled	Down	SFP-Preferred-Auto	Enabled	1000full	None
3	1000Base SFP		Enabled	Down	SFP-Forced	Enabled	1000full	None
4	1000Base SFP		Enabled	Down	SFP-Forced	Enabled	1000full	None
5	1000Base SFP		Enabled	Down	SFP-Forced	Enabled	1000full	None
6	1000Base SFP		Enabled	Down	SFP-Forced	Enabled	1000full	None
7	1000Base SFP		Enabled	Down	SFP-Forced	Enabled	1000full	None
8	1000Base SFP		Enabled	Down	SFP-Forced	Enabled	1000full	None
9	1000Base SFP		Enabled	Down	SFP-Forced	Enabled	1000full	None
10	1000Base SFP		Enabled	Down	SFP-Forced	Enabled	1000full	None

CONFIGURING 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 26: Configuring Local Port Mirroring



CLI REFERENCES

- "Local Port Mirroring Commands" on page 797

COMMAND USAGE

- Traffic can be mirrored from one or more source ports to one destination port on the same switch.
- 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 195).

PARAMETERS

These parameters are displayed in the web interface:

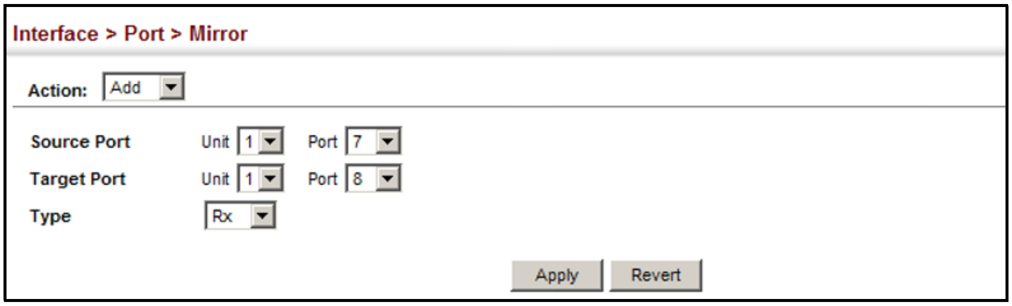
- **Source Port** – The port whose traffic will be monitored. (Range: 1-24)
- **Target Port** – The port that will mirror the traffic on the source port. (Range: 1-24)
- **Type** – Allows you to select which traffic to mirror to the target port, Rx (receive), Tx (transmit), or Both. (Default: Rx)

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 27: Configuring Local Port Mirroring



Interface > Port > Mirror

Action: Add

Source Port Unit 1 Port 7

Target Port Unit 1 Port 8

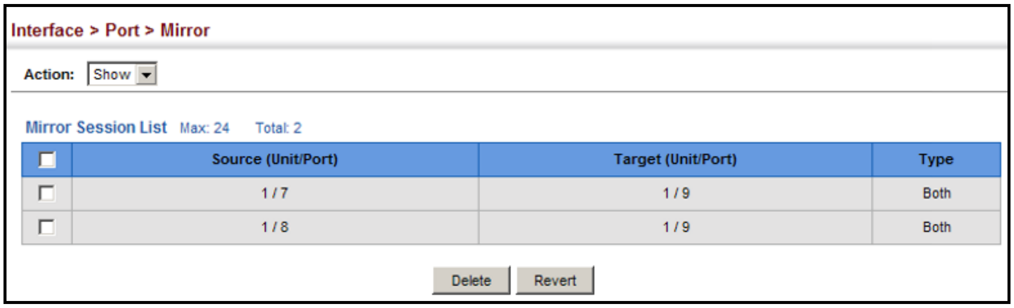
Type Rx

To display the configured mirror sessions:

1. Click Interface, Port, Mirror.

2. Select Show from the Action List.

Figure 28: Displaying Local Port Mirror Sessions



Interface > Port > Mirror

Action: Show

Mirror Session List Max: 24 Total: 2

□	Source (Unit/Port)	Target (Unit/Port)	Type
□	1 / 7	1 / 9	Both
□	1 / 8	1 / 9	Both

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 loading). 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 778

PARAMETERS

These parameters are displayed in the web interface:

Table 5: 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.

Table 5: Port Statistics (Continued)

Parameter	Description
Deferred Transmissions	A count of frames for which the first transmission attempt on a particular interface is delayed because the medium was busy.
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).

Table 5: Port Statistics (Continued)

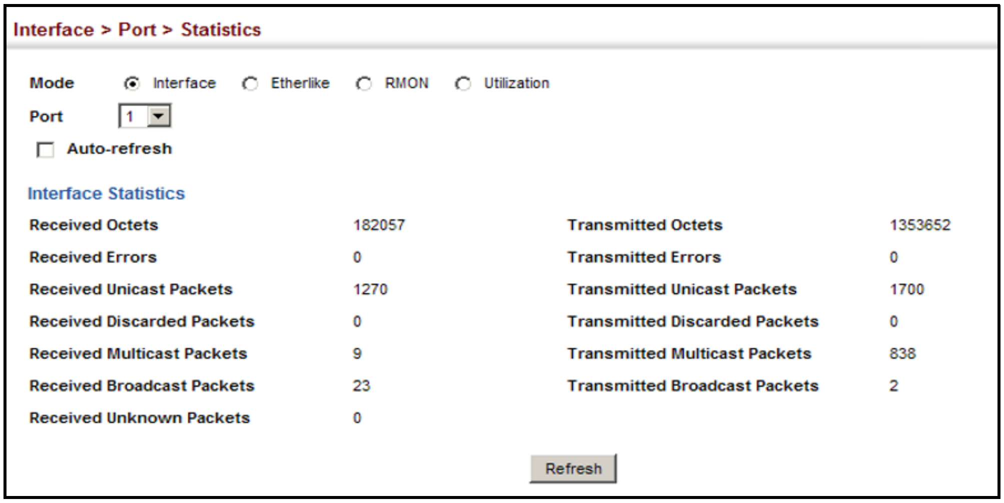
Parameter	Description
65-127 Byte Packets 128-255 Byte Packets 256-511 Byte Packets 512-1023 Byte Packets 1024-1518 Byte Packets 1519-1536 Byte Packets	The total number of packets (including bad packets) received and transmitted where the number of octets fall within the specified range (excluding framing bits but including FCS octets).
Utilization Statistics	
Input Octets per second	Number of octets entering this interface per second.
Input Packets per second	Number of packets entering this interface per second.
Input Utilization	The input utilization rate for this interface.
Output Octets per second	Number of octets leaving this interface per 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 or RMON).
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 29: Showing Port Statistics (Table)



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		

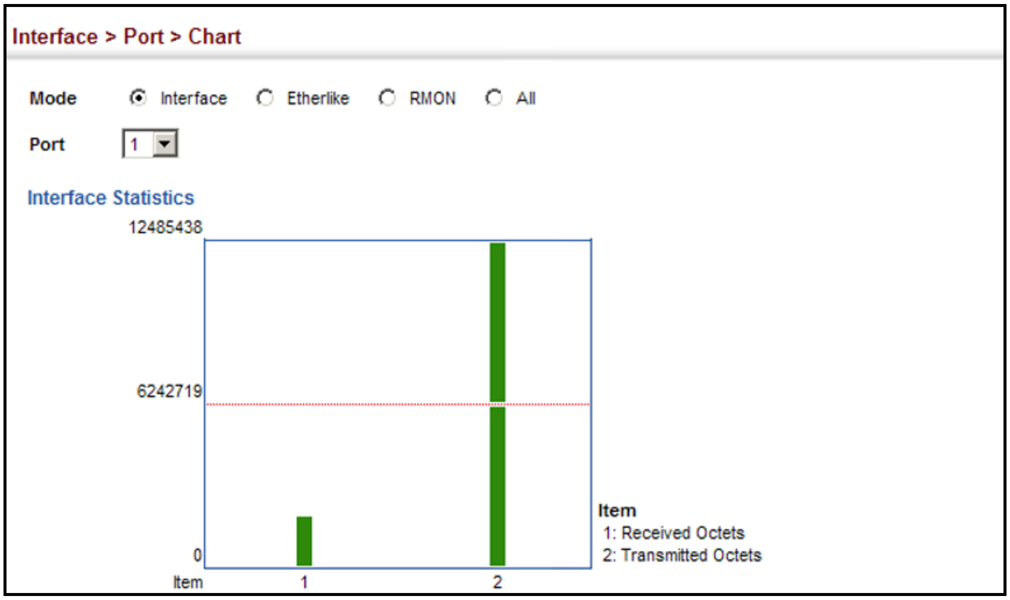
To show a chart of port statistics:

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 30: Showing Port Statistics (Chart)



Interface > Port > Chart

Mode ● Interface ○ Etherlike ○ RMON ○ All

Port 1

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 12 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

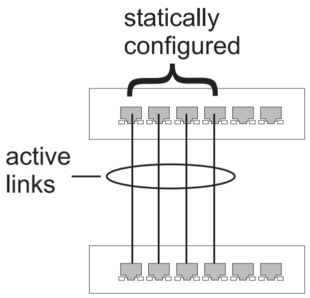
Besides balancing the load across each port in the trunk, the other ports provide redundancy by taking over the load if a port in the trunk fails. However, before making any physical connections between devices, use the web interface or CLI to specify the trunk on the devices at both ends. When using 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 12 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 31: Configuring Static Trunks



CLI REFERENCES

- "Link Aggregation Commands" on page 787
- "Interface Commands" on page 769

COMMAND USAGE

- When configuring static trunks, you may not be able to link switches of different types, depending on the manufacturer'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 in the web interface:

- **Trunk ID** – Trunk identifier. (Range: 1-32)

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

  - **Unit** – Stack unit. (Range: 1)

  - **Port** – Port identifier. (Range: 1-24)

WEB INTERFACE

To create a static trunk:

1. Click Interface, Trunk, Static.

2. Select Configure Trunk from the Step list.

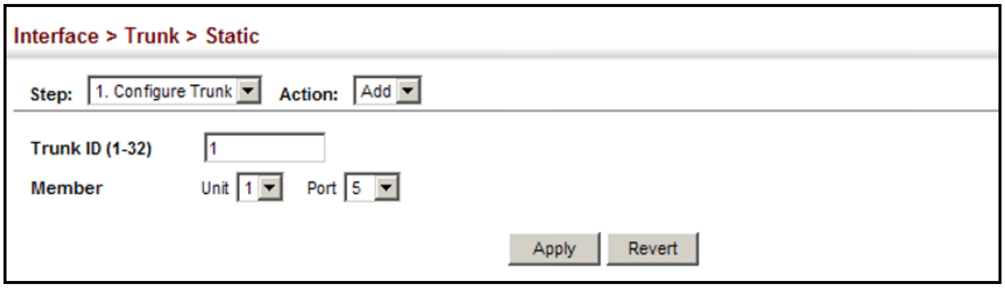
3. Select Add from the Action list.

4. Enter a trunk identifier.

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

6. Click Apply.

Figure 32: Creating Static Trunks



Interface > Trunk > Static

Step: 1. Configure Trunk Action: Add

Trunk ID (1-32): 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.

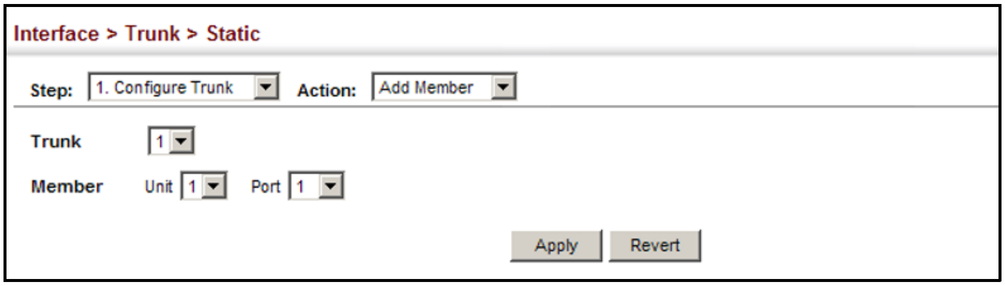
3. Select Add Member from the Action list.

4. Select a trunk identifier.

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

6. Click Apply.

Figure 33: 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.

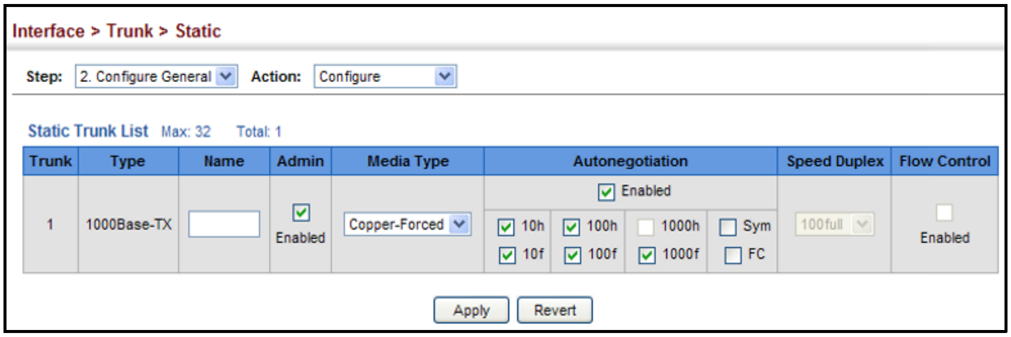
2. Select Configure General from the Step list.

3. Select Configure from the Action list.

4. Modify the required interface settings. (Refer to "Configuring by Port List" on page 125 for a description of the parameters.)

5. Click Apply.

Figure 34: Configuring Connection Parameters for a Static Trunk



Interface > Trunk > Static

Step: 2. Configure General ▾ Action: Configure ▾

Static Trunk List Max: 32 Total: 1

Trunk	Type	Name	Admin	Media Type	Autonegotiation	Speed Duplex	Flow Control
1	1000Base-TX		☑ Enabled	Copper-Forced ▾	☑ Enabled ☑ 10h ☑ 100h □ 1000h □ Sym ☑ 10f ☑ 100f ☑ 1000f □ FC	100full ▾	□ Enabled

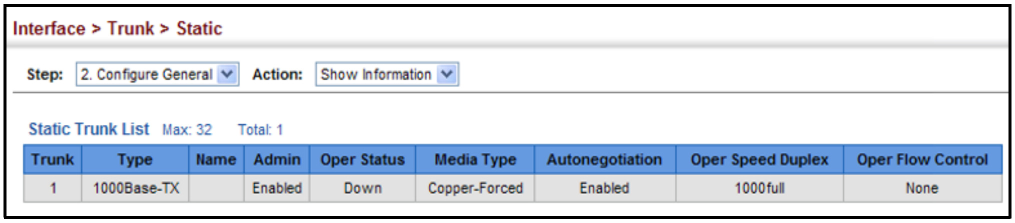
To display trunk connection parameters:

1. Click Interface, Trunk, Static.

2. Select Configure General from the Step list.

3. Select Show Information from the Action list.

Figure 35: Displaying Connection Parameters for Static Trunks



Interface > Trunk > Static

Step: 2. Configure General Action: Show Information

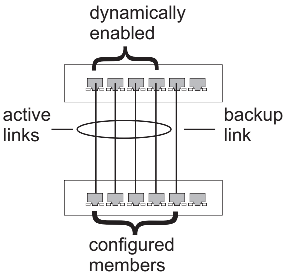
Static Trunk List Max: 32 Total: 1

Trunk	Type	Name	Admin	Oper Status	Media Type	Autonegotiation	Oper Speed Duplex	Oper Flow Control
1	1000Base-TX		Enabled	Down	Copper-Forced	Enabled	1000full	None

CONFIGURING A DYNAMIC TRUNK

Use the Interface > Trunk > Dynamic (Configure Aggregator) page to set the administrative key for an aggregation group, enable LACP on a port, and configure protocol parameters for local and partner ports.

Figure 36: Configuring Dynamic Trunks



CLI REFERENCES

- "Link Aggregation Commands" on page 787

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 793).

PARAMETERS

These parameters are displayed in the web interface:

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)

Configure Aggregation Port - General

- **Port** – Port identifier. (Range: 1-24)
- **LACP Status** – Enables or disables LACP on a port.

Configure Aggregation Port - Actor/Partner

- **Port** – Port number. (Range: 1-24)
- **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: 1)

  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)

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.

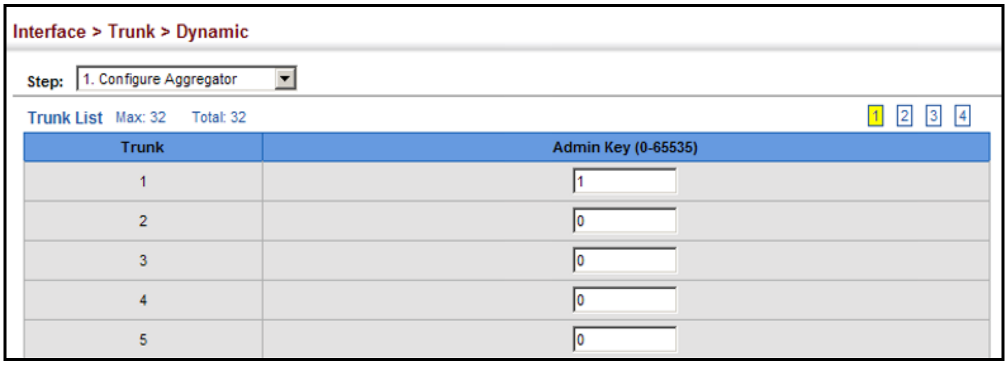
NOTE: Configuring the port partner sets the remote side of an aggregate link; i.e., the ports on the attached device. The command attributes have the same meaning as those used for the port actor.

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 for the required LACP group.
4. Click Apply.

Figure 37: Configuring the LACP Aggregator Admin Key



Interface > Trunk > Dynamic

Step: 1. Configure Aggregator

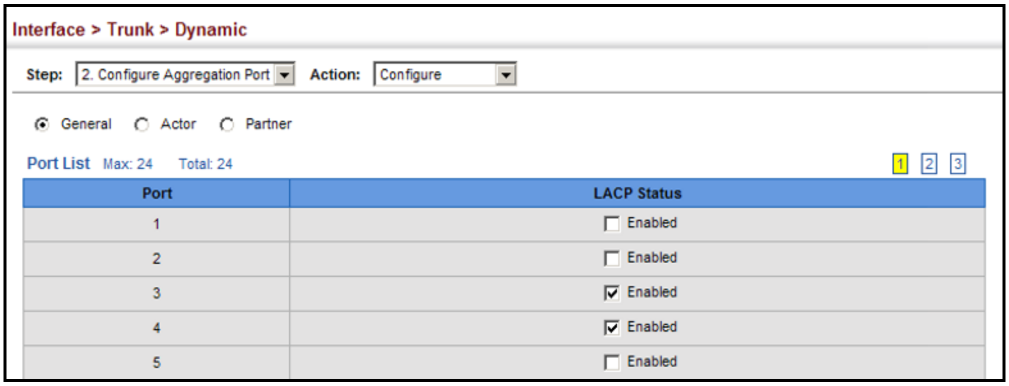
Trunk List Max: 32 Total: 32

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

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 38: Enabling LACP on a Port



Interface > Trunk > Dynamic

Step: 2. Configure Aggregation Port Action: Configure

● General ○ Actor ○ Partner

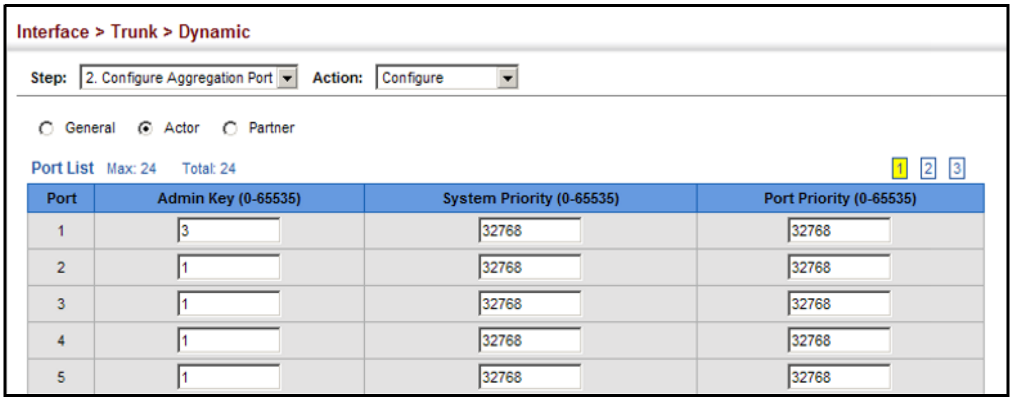
Port List Max: 24 Total: 24

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 39: Configuring LACP Parameters on a Port



Interface > Trunk > Dynamic

Step: 2. Configure Aggregation Port Action: Configure

○ General ● Actor ○ Partner

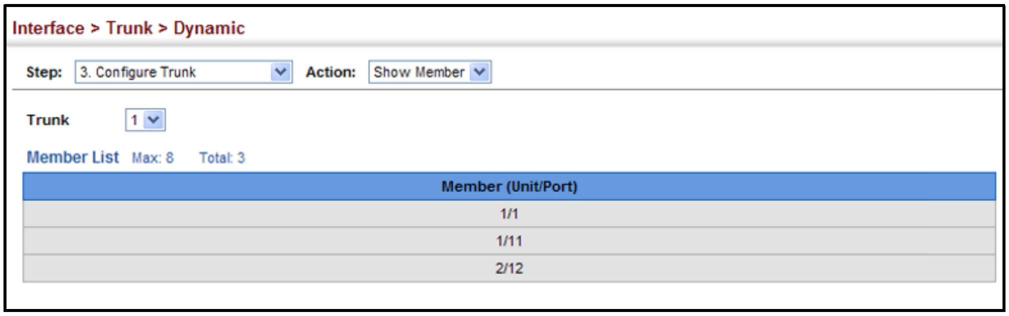
Port List Max: 24 Total: 24

Port	Admin Key (0-65535)	System Priority (0-65535)	Port Priority (0-65535)
1	3	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 40: Showing Members of a Dynamic Trunk



Interface > Trunk > Dynamic

Step: 3. Configure Trunk Action: Show Member

Trunk 1

Member List Max: 8 Total: 3

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

To configure connection parameters for a dynamic trunk:

1. Click Interface, Trunk, Dynamic.

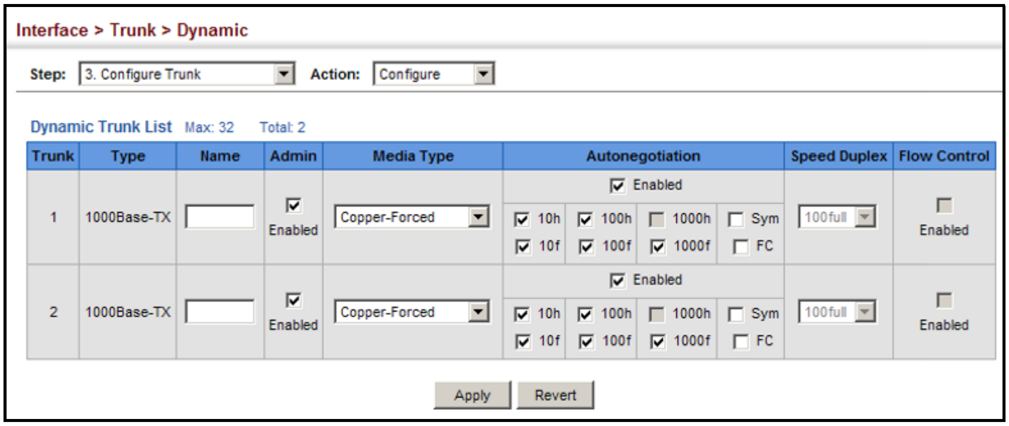
2. Select Configure Trunk from the Step List.

3. Select Configure from the Action List.

4. Modify the required interface settings. (See "Configuring by Port List" on page 125 for a description of the interface settings.)

5. Click Apply.

Figure 41: Configuring Connection Settings for Dynamic Trunks



Interface > Trunk > Dynamic

Step: 3. Configure Trunk   Action: Configure

Dynamic Trunk List Max: 32 Total: 2

Trunk	Type	Name	Admin	Media Type	Autonegotiation	Speed Duplex	Flow Control
1	1000Base-TX		☑ Enabled	Copper-Forced	☑ Enabled ☑ 10h ☑ 100h □ 1000h □ Sym ☑ 10f ☑ 100f ☑ 1000f □ FC	100full	□ Enabled
2	1000Base-TX		☑ Enabled	Copper-Forced	☑ Enabled ☑ 10h ☑ 100h □ 1000h □ Sym ☑ 10f ☑ 100f ☑ 1000f □ FC	100full	□ Enabled

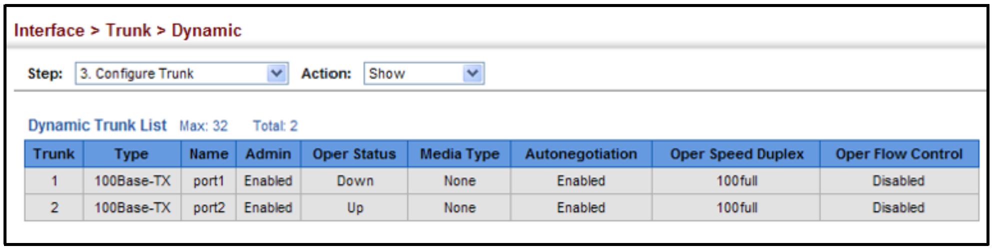
To display connection parameters for a dynamic trunk:

1. Click Interface, Trunk, Dynamic.

2. Select Configure Trunk from the Step List.

3. Select Show from the Action List.

Figure 42: Displaying Connection Parameters for Dynamic Trunks



Interface > Trunk > Dynamic

Step: 3. Configure Trunk   Action: Show

Dynamic Trunk List Max: 32 Total: 2

Trunk	Type	Name	Admin	Oper Status	Media Type	Autonegotiation	Oper Speed Duplex	Oper Flow Control
1	100Base-TX	port1	Enabled	Down	None	Enabled	100full	Disabled
2	100Base-TX	port2	Enabled	Up	None	Enabled	100full	Disabled

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 793

PARAMETERS

These parameters are displayed in the web interface:

Table 6: 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.

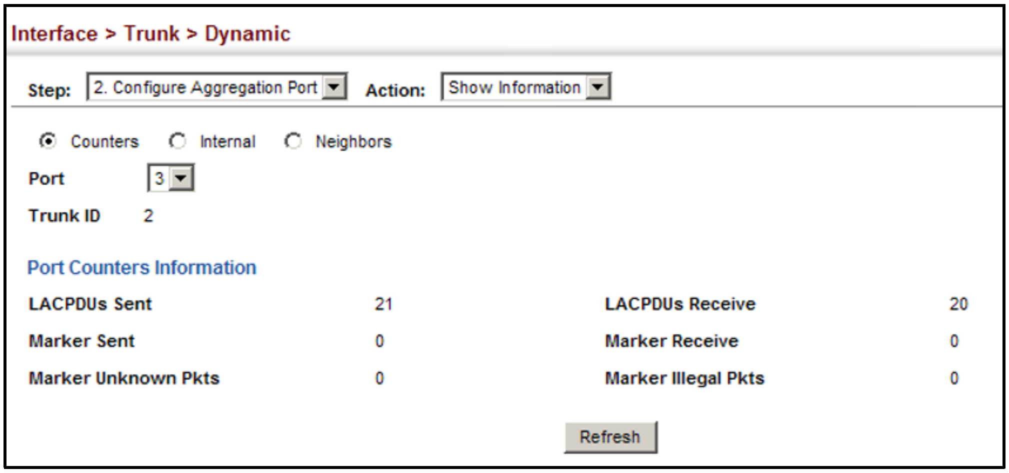
2. Select Configure Aggregation Port from the Step list.

3. Select Show Information from the Action list.

4. Click Counters.

5. Select a group member from the Port list.

Figure 43: Displaying LACP Port Counters



Interface > Trunk > Dynamic

Step: 2. Configure Aggregation Port Action: Show Information

● Counters ○ Internal ○ Neighbors

Port 3

Trunk ID 2

Port Counters Information

LACPDUs Sent	21	LACPDUs Receive	20
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 793

Parameters

These parameters are displayed in the web interface:

Table 7: 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.

Table 7: LACP Internal Configuration Information (Continued)

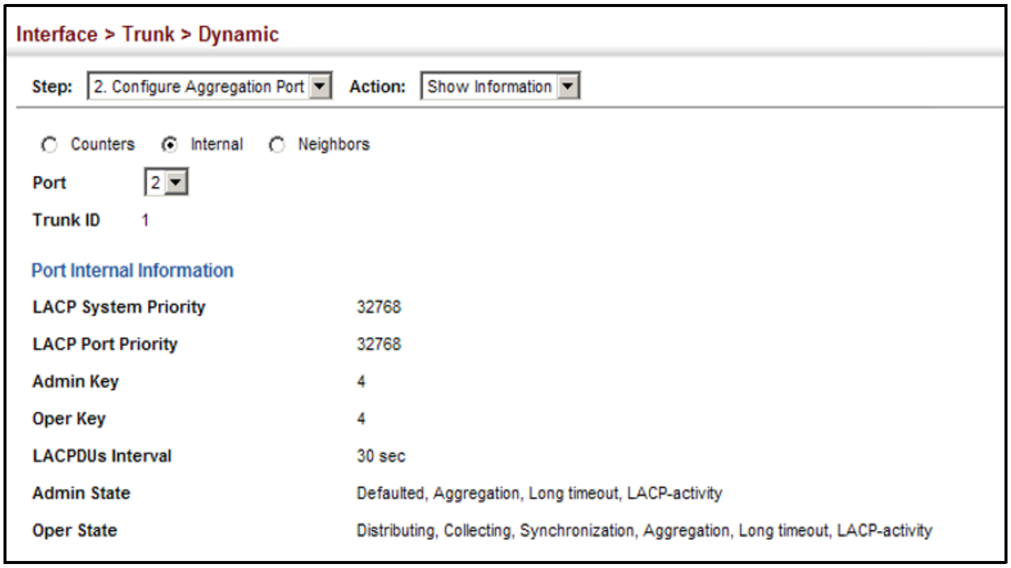
Parameter	Description
Admin State, Oper State	Administrative or operational values of the actor's state parameters: ◆ Expired – The actor's receive machine is in the expired state; ◆ Defaulted – The actor's receive machine is using defaulted operational partner information, administratively configured 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)

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 44: Displaying LACP Port Internal Information



Interface > Trunk > Dynamic

Step: 2. Configure Aggregation Port Action: Show Information

○ Counters ● Internal ○ Neighbors

Port 2

Trunk ID 1

Port Internal Information

LACP System Priority 32768

LACP Port Priority 32768

Admin Key 4

Oper Key 4

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 793

PARAMETERS

These parameters are displayed in the web interface:

Table 8: LACP Internal Configuration Information

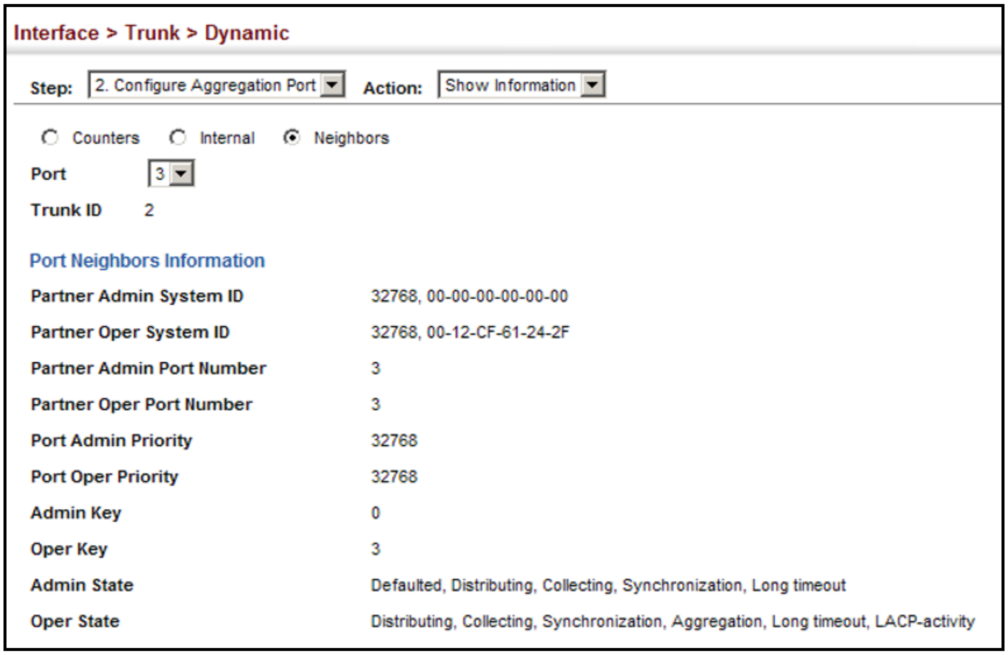
Parameter	Description
Partner Admin System ID	LAG partner’s system ID assigned by the user.
Partner Oper System ID	LAG partner’s system ID assigned by the LACP protocol.
Partner Admin Port Number	Current administrative value of the port number for the protocol Partner.
Partner Oper Port Number	Operational 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 45: 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

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 between clients on different downlink ports. Data traffic on downlink ports is only forwarded to, and from, uplink ports.

ENABLING TRAFFIC SEGMENTATION

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

CLI REFERENCES

- "Configuring Port-based Traffic Segmentation" on page 850

PARAMETERS

These parameters are displayed in the web interface:

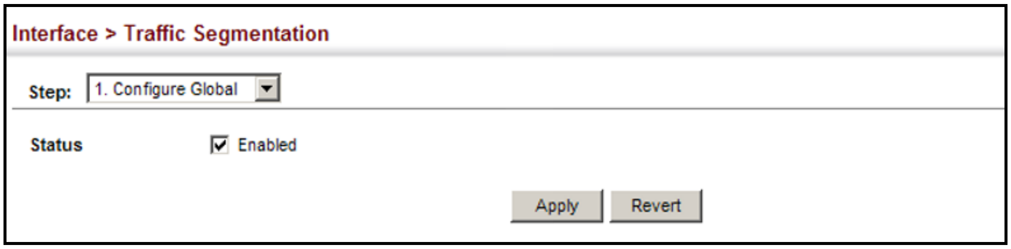
- **Status** – Enables port-based traffic segmentation. (Default: Disabled)

WEB INTERFACE

To enable traffic segmentation:

1. Click Interface, Traffic Segmentation.
2. Select Configure Global from the Step list.
3. Mark the Enabled check box.
4. Click Apply.

Figure 46: Enabling Traffic Segmentation



Interface > Traffic Segmentation

Step: 1. Configure Global

Status ☑ Enabled

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 850

PARAMETERS

These parameters are displayed in the web interface:

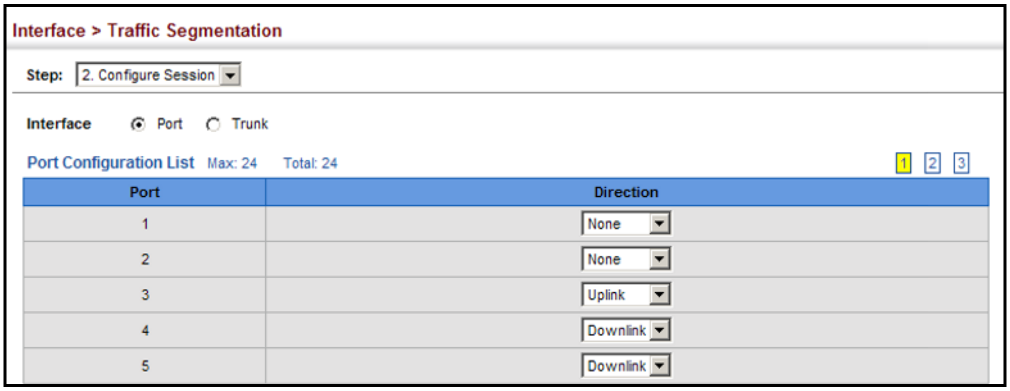
- **Interface** – Displays a list of ports or trunks.
- **Port** – Port Identifier. (Range: 1-24)
- **Trunk** – Trunk Identifier. (Range: 1-32)
- **Direction** – Adds an interface to the segmented group by setting the direction to uplink or downlink. (Default: None)

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. Click Port or Trunk to specify the interface type.
4. Select Uplink or Downlink in the Direction list to add a group member.
5. Click Apply.

Figure 47: Configuring Members for Traffic Segmentation



Interface > Traffic Segmentation

Step: 2. Configure Session

Interface ● Port ○ Trunk

Port Configuration List Max: 24 Total: 24

Port	Direction
1	None
2	None
3	Uplink
4	Downlink
5	Downlink

VLAN TRUNKING

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

CLI REFERENCES

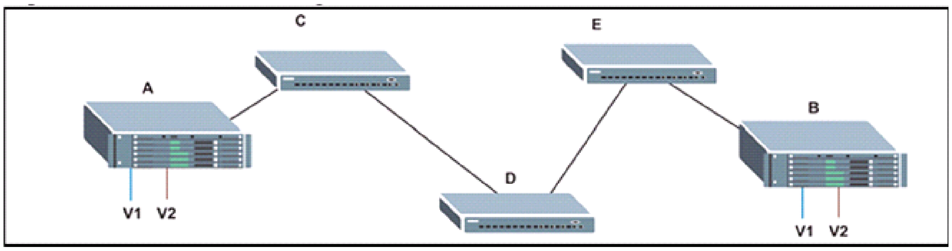
- "vlan-trunking" on page 843

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 48: 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 can only be enabled on Gigabit Ethernet ports or trunks.

- 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 in the web interface:

- **Interface** – Displays a list of ports or trunks.
- **Port** – Port Identifier. (Range: 1-24)

NOTE: VLAN trunking can only be enabled on Gigabit ports.

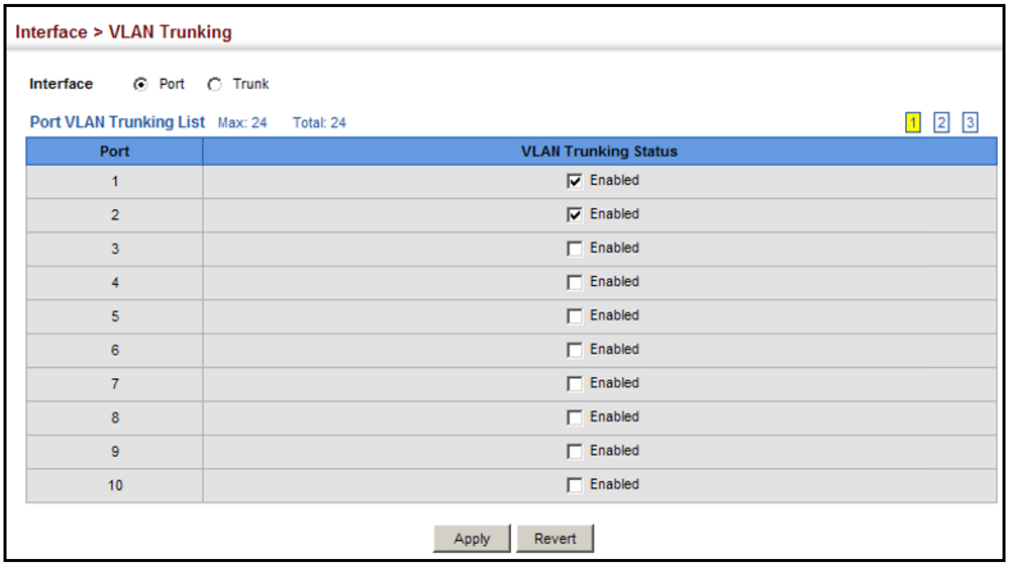
- **Trunk** – Trunk Identifier. (Range: 1-32)
- **VLAN Trunking Status** – Enables VLAN trunking on the selected interface.

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 Gigibit ports or on a trunk containing Gigabit ports.
4. Click Apply.

Figure 49: Configuring VLAN Trunking



Interface > VLAN Trunking

Interface ● Port ○ Trunk

Port VLAN Trunking List Max: 24 Total: 24

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.

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:

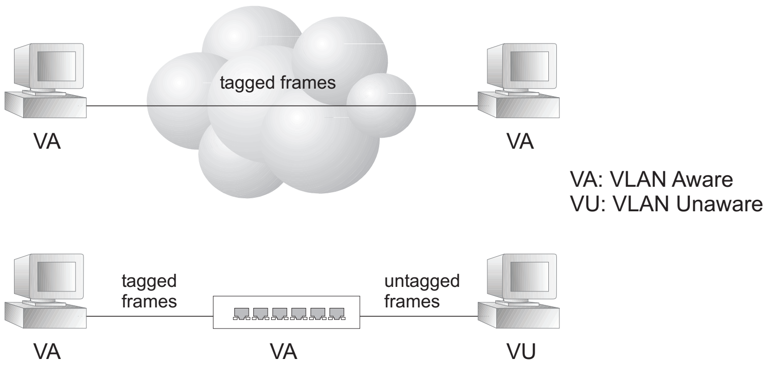
- Up to 4093 VLANs based on the IEEE 802.1Q standard
- Distributed VLAN learning across multiple switches using explicit or implicit tagging and GVRP protocol
- Port overlapping, allowing a port to participate in multiple VLANs
- End stations can belong to multiple VLANs
- Passing traffic between VLAN-aware 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 50: 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.

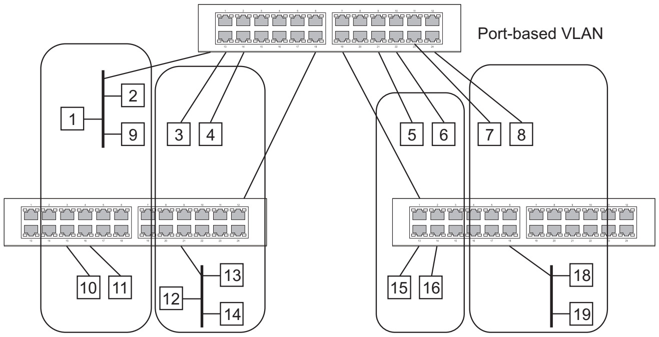
Untagged VLANs – Untagged (or static) VLANs are typically used to reduce broadcast traffic and to increase security. A group of network users assigned to a VLAN form a broadcast domain that is separate from other VLANs configured on the switch. Packets are forwarded only between ports that are designated 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 158). But you can still enable GVRP on these edge switches, as well as on the core switches in the network.

Figure 51: 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. 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 836

PARAMETERS

These parameters are displayed in the web interface:

Add

- **VLAN ID** – ID of VLAN or range of VLANs (1-4093).
- **Status** – Enables or disables the specified VLAN.

Modify

- **VLAN ID** – ID of configured VLAN (1-4093).
- **VLAN Name** – Name of the VLAN (1 to 32 characters).

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

Show

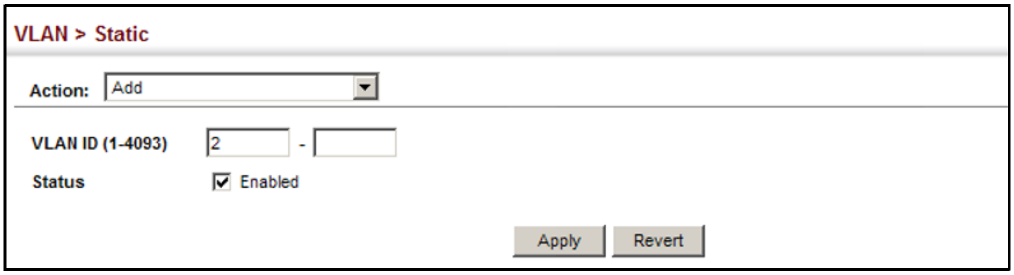
- **VLAN ID** – ID of configured VLAN.
- **VLAN Name** – Name of the VLAN.
- **Status** – Operational status of configured VLAN.

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. Mark Enable to configure the VLAN as operational.
5. Click Apply.

Figure 52: Creating Static VLANs



VLAN > Static

Action: Add

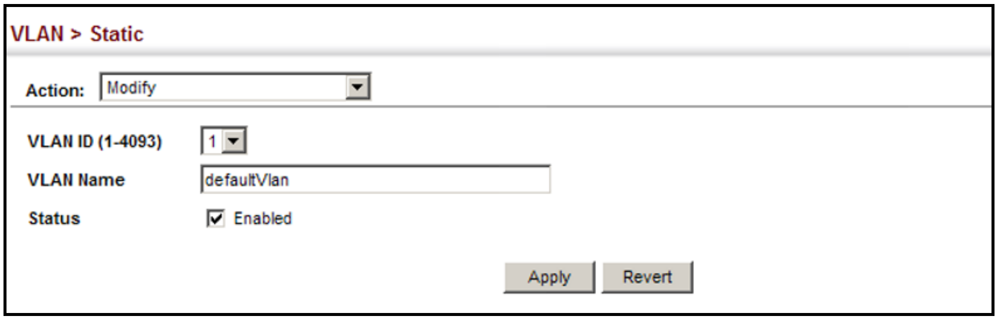
VLAN ID (1-4093) 2 -

Status ☑ 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 or operational status as required.
5. Click Apply.

Figure 53: Modifying Settings for Static VLANs



VLAN > Static

Action: Modify

VLAN ID (1-4093) 1

VLAN Name defaultVlan

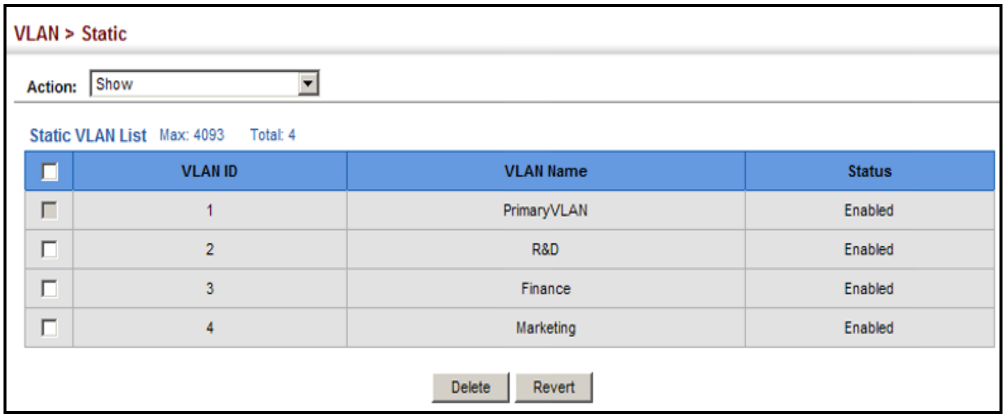
Status ☑ Enabled

To show the configuration settings for VLAN groups:

1. Click VLAN, Static.

2. Select Show from the Action list.

Figure 54: Showing Static VLANs



VLAN > Static

Action: Show

Static VLAN List Max: 4093 Total: 4

□	VLAN ID	VLAN Name	Status
□	1	PrimaryVLAN	Enabled
□	2	R&D	Enabled
□	3	Finance	Enabled
□	4	Marketing	Enabled

ADDING STATIC MEMBERS TO VLANS

Use the VLAN > Static page 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 838
- "Displaying VLAN Information" on page 845

PARAMETERS

These parameters are displayed in the web interface:

Edit Member by VLAN

- **VLAN** – ID of configured VLAN (1-4093).
- **Interface** – Displays a list of ports or trunks.
- **Port** – Port Identifier. (Range: 1-24)
- **Trunk** – Trunk Identifier. (Range: 1-32)
- **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 155.

  - **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, and membership type can only be modified by first assigning a port to another VLAN and then reassigning the default port VLAN ID.

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: 1-24)

- **Trunk Range** – Displays a list of ports. (Range: 1-32)

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.

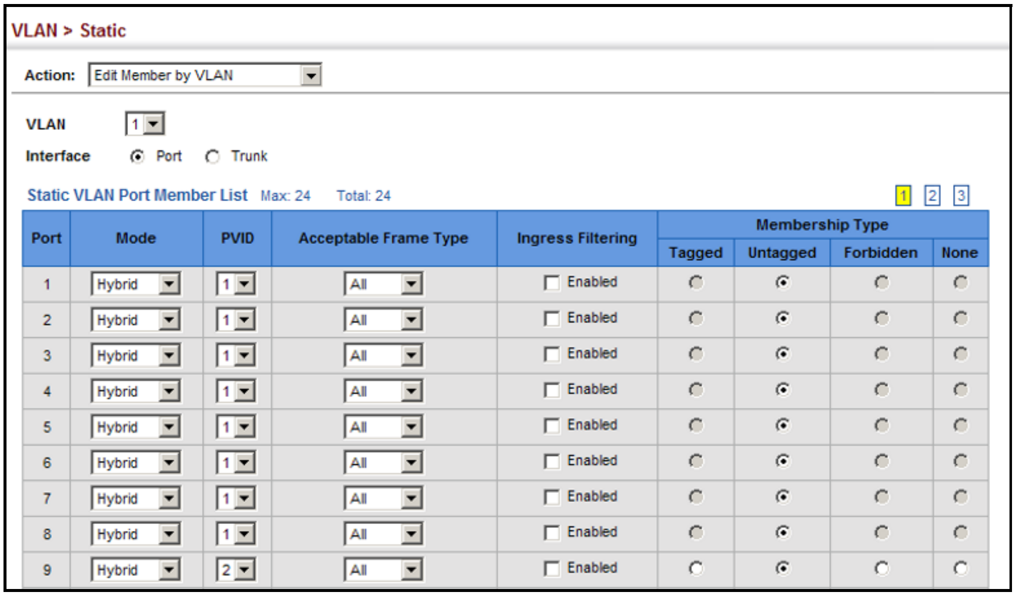
2. Select Edit Member by VLAN from the Step list.

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

4. Modify the settings for any interface as required. Remember that Membership Type cannot be changed until an interface has been added to another VLAN and the PVID changed to anything other than 1.

5. Click Apply.

Figure 55: Configuring Static Members by VLAN Index



VLAN > Static

Action: Edit Member by VLAN

VLAN: 1

Interface: ● Port ○ Trunk

Static VLAN Port Member List Max: 24 Total: 24

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	○	●	○	○
6	Hybrid	1	All	☐ Enabled	○	●	○	○
7	Hybrid	1	All	☐ Enabled	○	●	○	○
8	Hybrid	1	All	☐ Enabled	○	●	○	○
9	Hybrid	2	All	☐ Enabled	○	●	○	○

To configure static members by interface:

1. Click VLAN, Static.

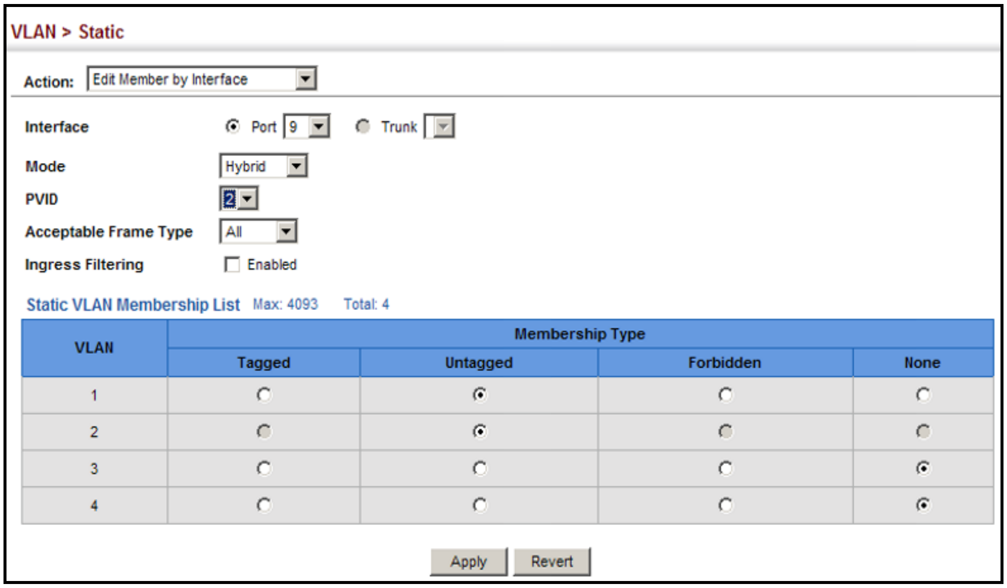
2. Select Edit Member by Interface from the Step list.

3. Select a port or trunk configure.

4. Modify the settings for any interface as required.

5. Click Apply.

Figure 56: Configuring Static VLAN Members by Interface



VLAN > Static

Action: Edit Member by Interface

Interface ● Port 9 ○ Trunk

Mode Hybrid

PVID 2

Acceptable Frame Type All

Ingress Filtering □ Enabled

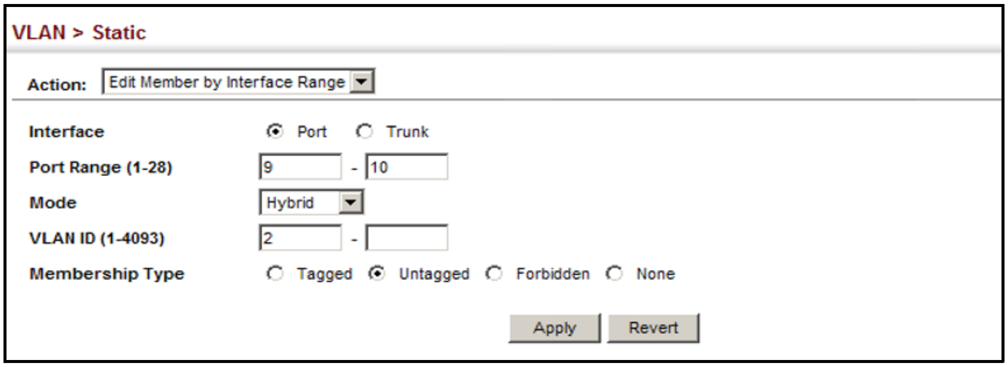
Static VLAN Membership List Max: 4093 Total: 4

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 Step 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 57: 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 (1-4093) 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 832
- "Configuring VLAN Interfaces" on page 838

PARAMETERS

These parameters are displayed in the web interface:

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: Enabled)

Configure Interface

- **Interface** – Displays a list of ports or trunks.
- **Port** – Port Identifier. (Range: 1-24)
- **Trunk** – Trunk Identifier. (Range: 1-32)
- **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:
  2 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

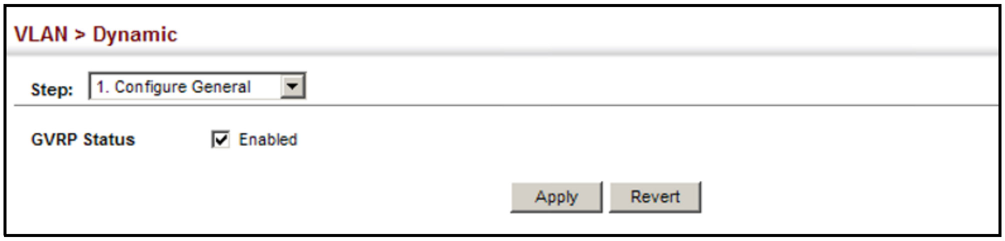
- **VLAN** – Identifier of a VLAN this switch has joined through GVRP.
- **Interface** – Displays a list of ports or trunks which have joined the selected VLAN through GVRP.

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 58: Configuring Global Status of GVRP



VLAN > Dynamic

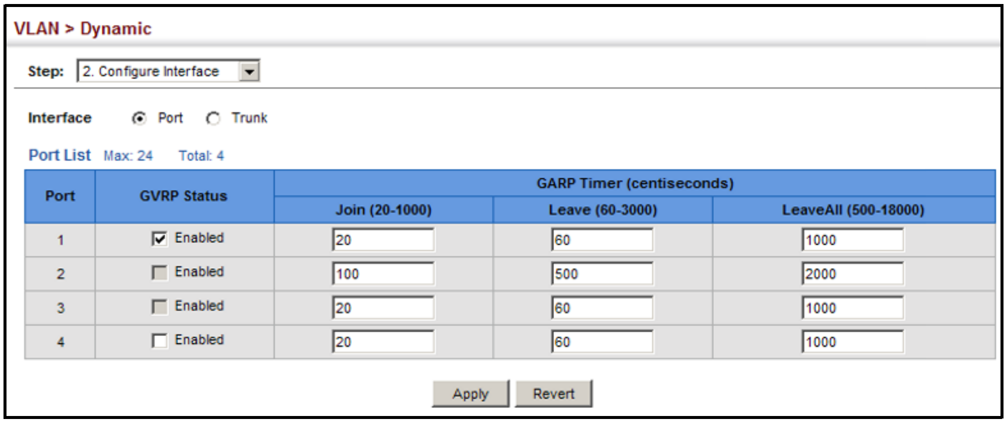
Step: 1. Configure General

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 59: Configuring GVRP for an Interface



VLAN > Dynamic

Step: 2. Configure Interface

Interface ● Port ○ Trunk

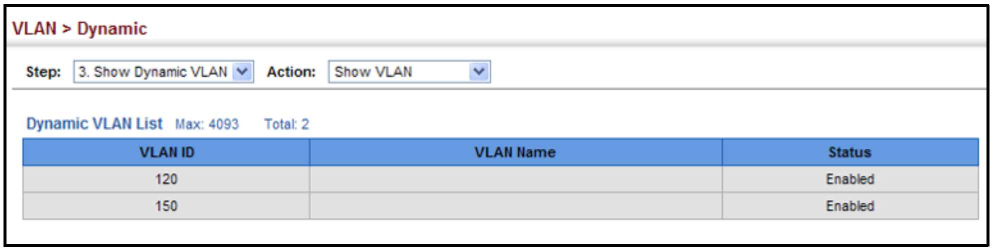
Port List Max: 24 Total: 4

Port	GVRP Status	GARP Timer (centiseconds)		
		Join (20-1000)	Leave (60-3000)	LeaveAll (500-18000)
1	☑ Enabled	20	60	1000
2	□ Enabled	100	500	2000
3	□ Enabled	20	60	1000
4	□ 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 60: Showing Dynamic VLANs Registered on the Switch



VLAN > Dynamic

Step: 3. Show Dynamic VLAN Action: Show VLAN

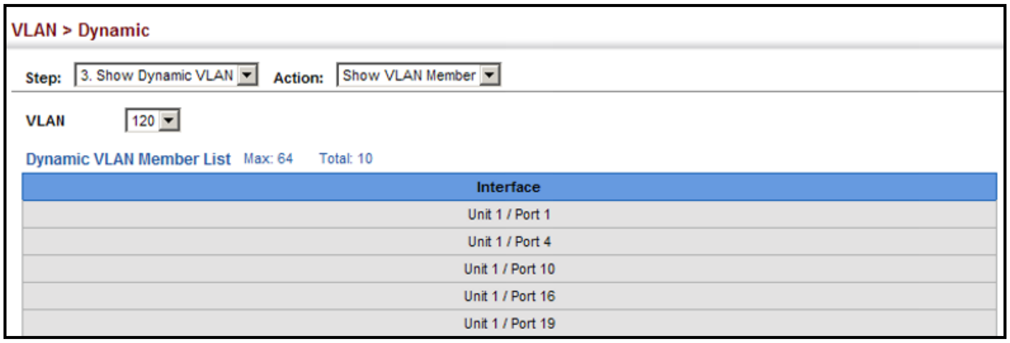
Dynamic VLAN List Max: 4093 Total: 2

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 61: Showing the Members of a Dynamic VLAN



VLAN > Dynamic

Step: 3. Show Dynamic VLAN Action: Show VLAN Member

VLAN 120

Dynamic VLAN Member List Max: 64 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 853

PARAMETERS

These parameters are displayed in the web interface:

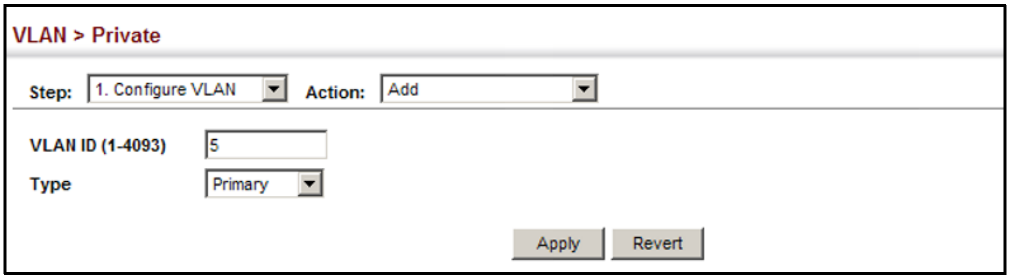
- **VLAN ID** – ID of configured VLAN (2-4093).
- **Type** – There are two types of private VLANs:
  - **Primary** – Conveys traffic between promiscuous ports, and to community ports within secondary (or community) VLANs.
  - **Community** - Conveys traffic between community ports, and to their promiscuous ports in the associated primary VLAN.

WEB INTERFACE

To configure private VLANs:

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. Selecte Primary or Community from the Type list
6. Click Apply.

Figure 62: Configuring Private VLANs



VLAN > Private

Step: 1. Configure VLAN Action: Add

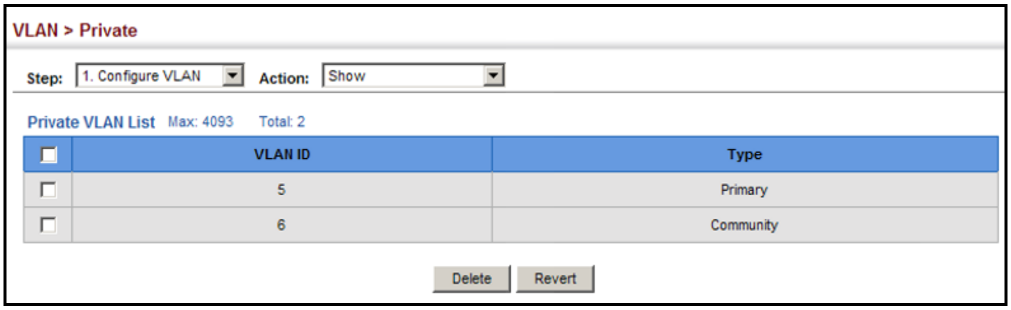
VLAN ID (1-4093) 5

Type Primary

To display a list of private VLANs:

1. Click VLAN, Private.
2. Select Configure VLAN from the Step list.
3. Select Show from the Action list.

Figure 63: Showing Private VLANs



VLAN > Private

Step: 1. Configure VLAN Action: Show

Private VLAN List Max: 4093 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 854

PARAMETERS

These parameters are displayed in the web interface:

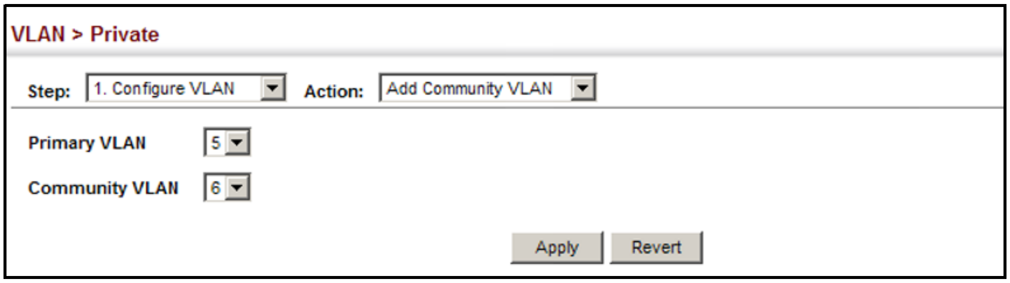
- **Primary VLAN** – ID of primary VLAN (2-4093).
- **Community VLAN** – VLAN associated with the selected primary VLAN.

WEB INTERFACE

To associate a community VLAN with a primary VLAN:

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 64: Associating Private VLANs



VLAN > Private

Step: 1. Configure VLAN　Action: Add Community VLAN

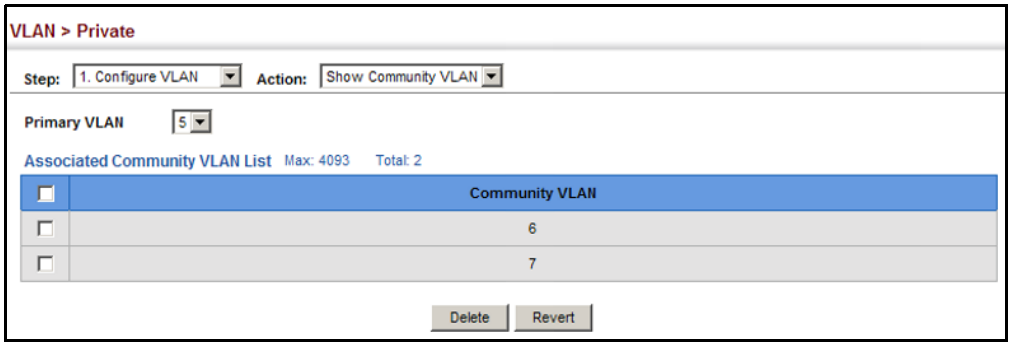
Primary VLAN: 5

Community VLAN: 6

To show a list of community VLANs associated with a primary VLAN:

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 65: Showing Associated VLANs



VLAN > Private

Step: 1. Configure VLAN　Action: Show Community VLAN

Primary VLAN: 5

Associated Community VLAN List　Max: 4093　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 856
- "switchport private-vlan host-association" on page 855

PARAMETERS

These parameters are displayed in the web interface:

- **Interface** – Displays a list of ports or trunks.
- **Port** – Port Identifier. (Range: 1-24)
- **Trunk** – Trunk Identifier. (Range: 1-32)
- **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.

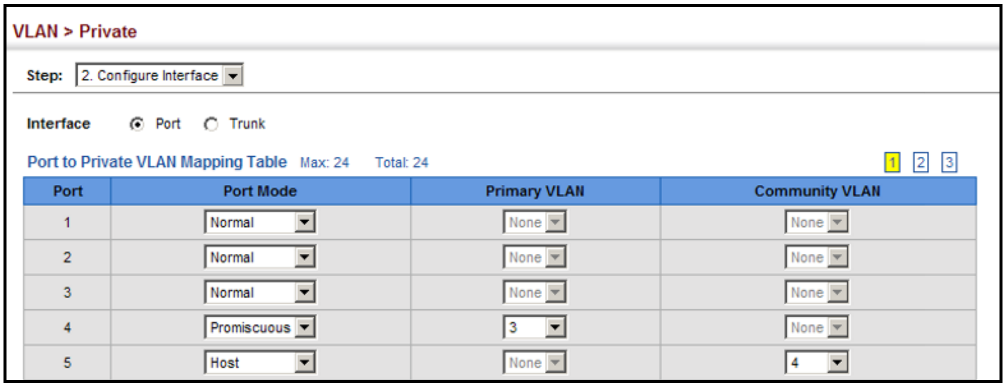
◆ **Community VLAN** – A community VLAN conveys traffic between community ports, and from community ports to their designated promiscuous ports. Set Port Mode to "Host," and then specify the associated Community VLAN.

WEB INTERFACE

To configure a private VLAN port or trunk:

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 66: Configuring Interfaces for Private VLANs



VLAN > Private

Step: 2. Configure Interface

Interface ● Port ○ Trunk

Port to Private VLAN Mapping Table Max: 24 Total: 24

Port	Port Mode	Primary VLAN	Community VLAN
1	Normal	None	None
2	Normal	None	None
3	Normal	None	None
4	Promiscuous	3	None
5	Host	None	4

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.

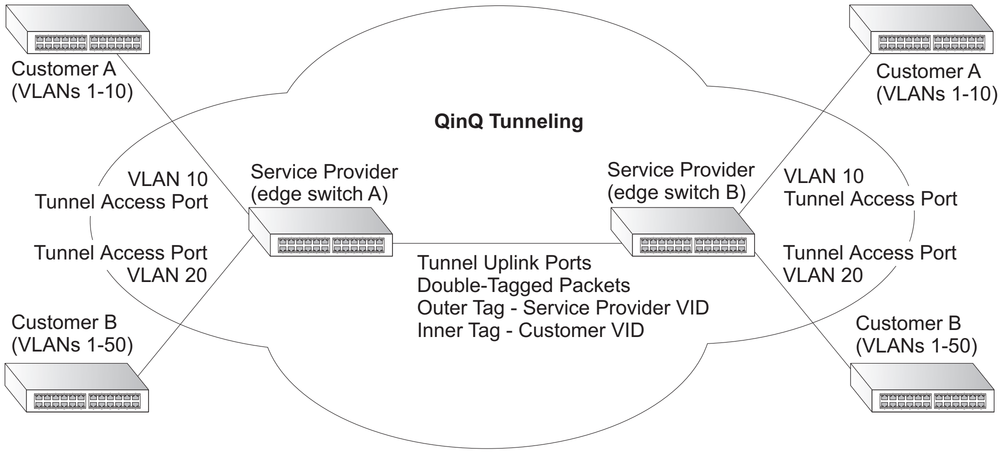
QinQ tunneling uses a single Service Provider VLAN (SPVLAN) for customers who have multiple VLANs. Customer VLAN IDs are preserved and traffic from different customers is segregated within the service provider's network even when they use the same customer-specific VLAN IDs. QinQ tunneling expands VLAN 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 67: 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. New SPVLAN tags are added to all incoming packets, no matter how many tags they already have. The ingress process 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). This outer tag is used for learning and switching packets. 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 175.)

2. Create a Service Provider VLAN, also referred to as an SPVLAN (see "Configuring VLAN Groups" on page 156).

3. Configure the QinQ tunnel access port to Tunnel mode (see "Adding an Interface to a QinQ Tunnel" on page 176).

4. Configure the QinQ tunnel access port to join the SPVLAN as an untagged member (see "Adding Static Members to VLANs" on page 158).

5. Configure the SPVLAN ID as the native VID on the QinQ tunnel access port (see "Adding Static Members to VLANs" on page 158).

6. Configure the QinQ tunnel uplink port to Tunnel Uplink mode (see "Adding an Interface to a QinQ Tunnel" on page 176).

7. Configure the QinQ tunnel uplink port to join the SPVLAN as a tagged member (see "Adding Static Members to VLANs" on page 158).

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 846

PARAMETERS

These parameters are displayed in the web interface:

- **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 0800-FFFF; Default: 8100)

  Use this field to set a custom 802.1Q ethertype value. 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.

  All ports on the switch will be set to the same ethertype.

WEB INTERFACE

To enable QinQ Tunneling on the switch:

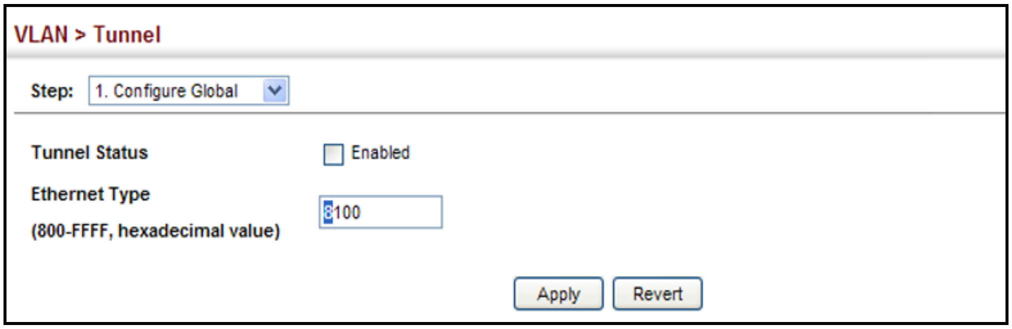
1. Click VLAN, Tunnel.

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 68: Enabling QinQ Tunneling



VLAN > Tunnel

Step: 1. Configure Global

Tunnel Status □ Enabled

Ethernet Type (800-FFFF, hexadecimal value) 8100

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 846

COMMAND USAGE

- Use the Configure Global page to set the switch to QinQ mode before configuring a tunnel port or tunnel uplink port (see "Enabling QinQ Tunneling on the Switch" on page 175). Also 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.

- Then use the Configure Interface page to set the access interface on the edge switch to Tunnel mode, and set the uplink interface on the switch attached to the service provider network to Tunnel Uplink mode.

PARAMETERS

These parameters are displayed in the web interface:

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

- **Port** – Port Identifier. (Range: 1-24)

- **Trunk** – Trunk Identifier. (Range: 1-32)

- **Mode** – Sets the VLAN membership mode of the port.
  - **None** – The port operates in its normal VLAN mode. (This is the default.)
  - **Tunnel** – Configures QinQ tunneling for a client access port to segregate and preserve customer VLAN IDs for traffic crossing the service provider network.
  - **Tunnel 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:

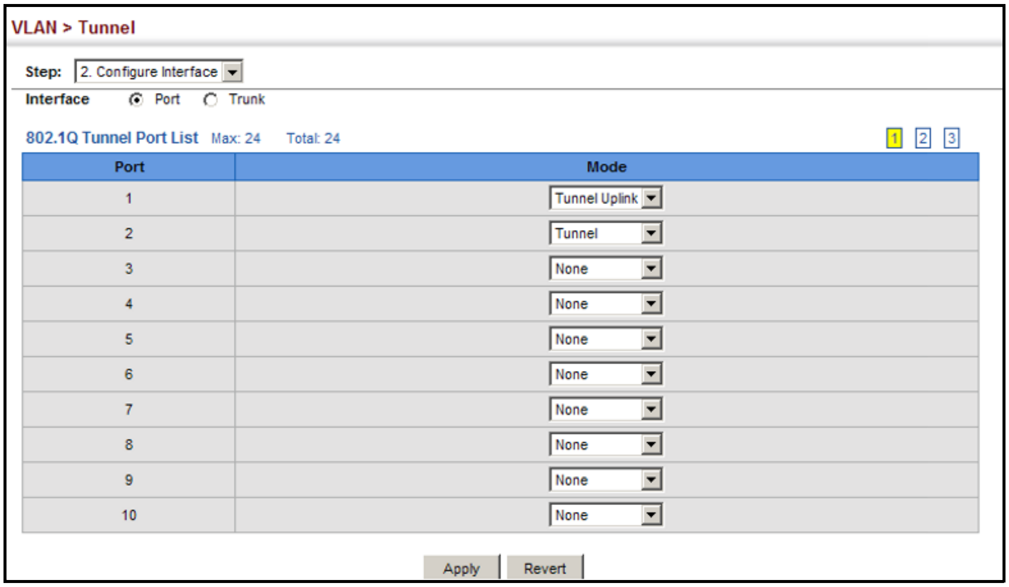
1. Click VLAN, Tunnel.

2. Select Configure Interface from the Step list.

3. Set the mode for any tunnel access port to Tunnel and the tunnel uplink port to Tunnel Uplink.

4. Click Apply.

Figure 69: Adding an Interface to a QinQ Tunnel



VLAN > Tunnel

Step: 2. Configure Interface

Interface ● Port ○ Trunk

802.1Q Tunnel Port List Max: 24 Total: 24

Port	Mode
1	Tunnel Uplink
2	Tunnel
3	None
4	None
5	None
6	None
7	None
8	None
9	None
10	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 (page 836). 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 858

PARAMETERS

These parameters are displayed in the web interface:

- **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)

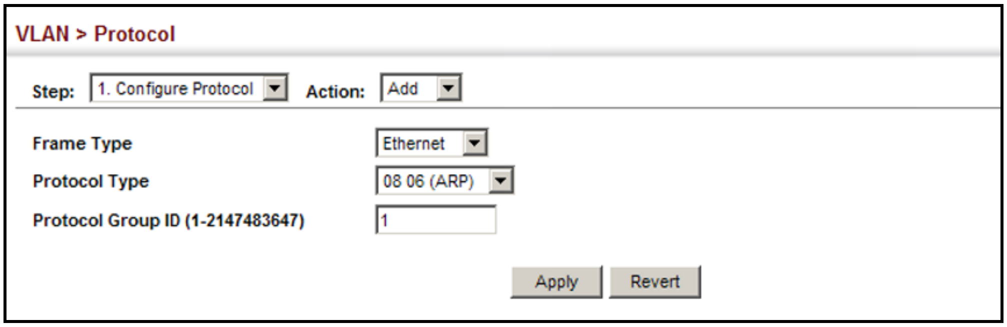
NOTE: Traffic which matches IP Protocol Ethernet Frames is mapped to the VLAN (VLAN 1) that has been configured with the switch's administrative IP. IP Protocol Ethernet traffic must not be mapped to another VLAN or you will lose administrative network connectivity to the switch. If lost in this manner, 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 70: Configuring Protocol VLANs



VLAN > Protocol

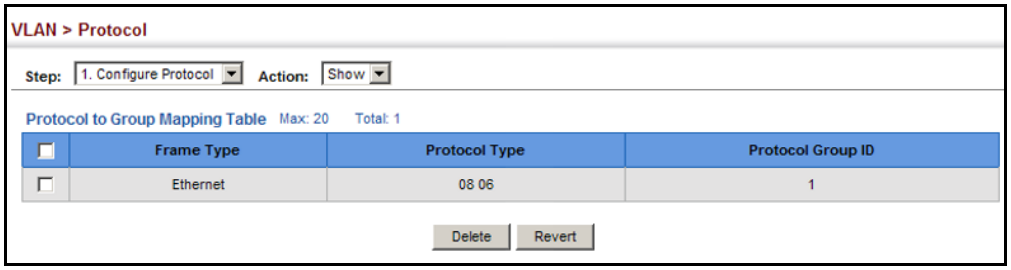
Step: 1. Configure Protocol Action: Add

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 71: Displaying Protocol VLANs



VLAN > Protocol

Step: 1. Configure Protocol Action: Show

Protocol to Group Mapping Table Max: 20 Total: 1

□	Frame Type	Protocol Type	Protocol Group ID
□	Ethernet	08 06	1

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 858

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 158), 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 in the web interface:

- **Interface** – Displays a list of ports or trunks.
- **Port** – Port Identifier. (Range: 1-24)
- **Trunk** – Trunk Identifier. (Range: 1-32)
- **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: 1-4093)

WEB INTERFACE

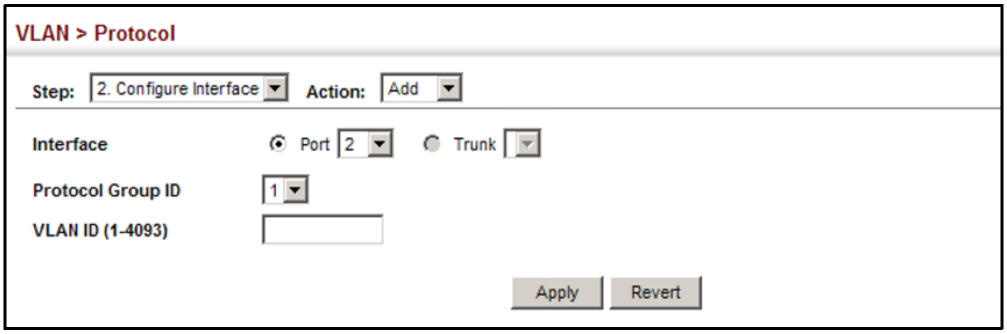
To map a protocol group to a VLAN for a port or trunk:

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 72: Assigning Interfaces to Protocol VLANs



VLAN > Protocol

Step: 2. Configure Interface   Action: Add

Interface   ● Port 2   ○ Trunk

Protocol Group ID   1

VLAN ID (1-4093)

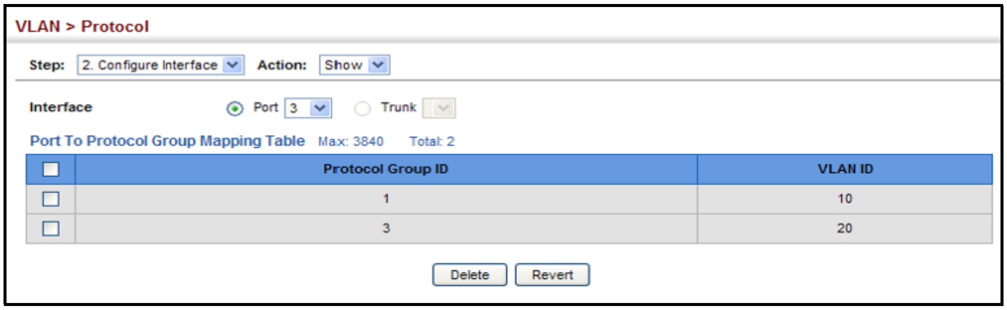
To show the protocol groups mapped to a port or trunk:

1. Click VLAN, Protocol.

2. Select Configure Interface from the Step list.

3. Select Show from the Action list.

Figure 73: Showing the Interface to Protocol Group Mapping



VLAN > Protocol

Step: 2. Configure Interface   Action: Show

Interface   ● Port 3   ○ Trunk

Port To Protocol Group Mapping Table   Max: 3840   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 861

COMMAND USAGE

- Each IP subnet can be mapped to only one VLAN ID. An IP subnet consists of an IP address and a mask.
- 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 in the web interface:

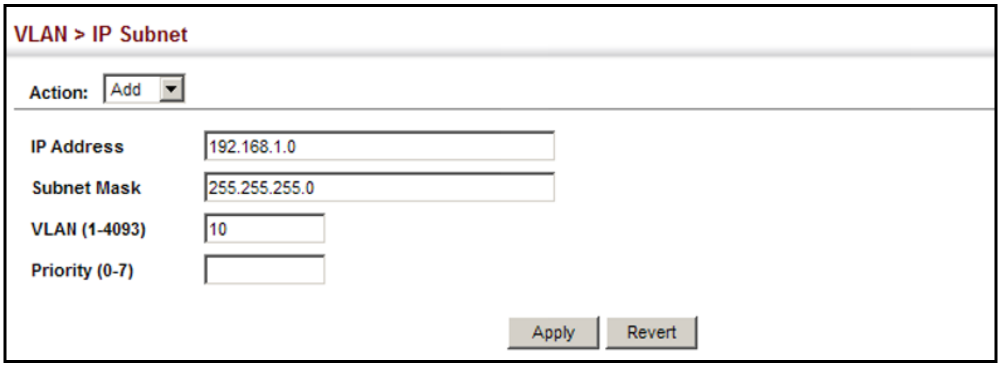
- **IP Address** – The IP address for a subnet. Valid IP addresses consist of four decimal numbers, 0 to 255, separated by periods.
- **Subnet Mask** – This mask identifies the host address bits of the IP subnet.
- **VLAN** – VLAN to which matching IP subnet traffic is forwarded. (Range: 1-4093)
- **Priority** – 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 74: Configuring IP Subnet VLANs


VLAN > IP Subnet

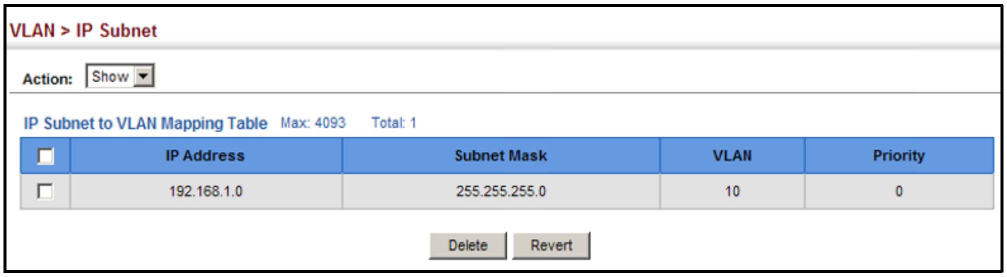
Action: Add

IP Address	192.168.1.0
Subnet Mask	255.255.255.0
VLAN (1-4093)	10
Priority (0-7)	

To show the configured IP subnet VLANs:

1. Click VLAN, IP Subnet.
2. Select Show from the Action list.

Figure 75: Showing IP Subnet VLANs


VLAN > IP Subnet

Action: Show

IP Subnet to VLAN Mapping Table Max: 4093 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 863

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 in the web interface:

- **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.
- **VLAN** – VLAN to which ingress traffic matching the specified source MAC address is forwarded. (Range: 1-4093)
- **Priority** – The priority assigned to untagged ingress traffic. (Range: 0-7, where 7 is the highest priority; Default: 0)

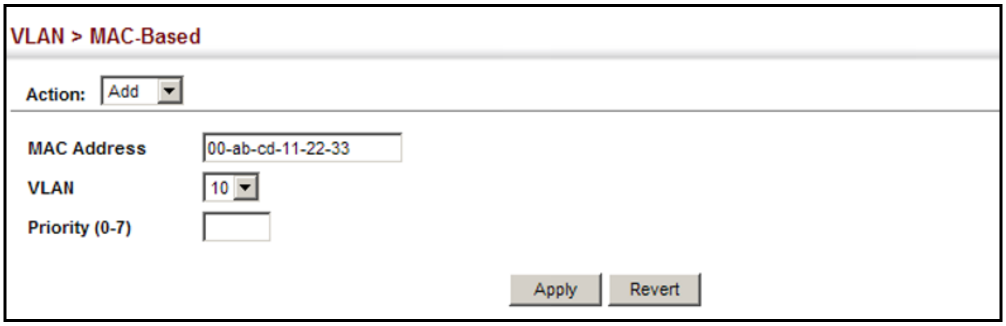
WEB INTERFACE

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 the 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 76: Configuring MAC-Based VLANs



VLAN > MAC-Based

Action: Add

MAC Address 00-ab-cd-11-22-33

VLAN 10

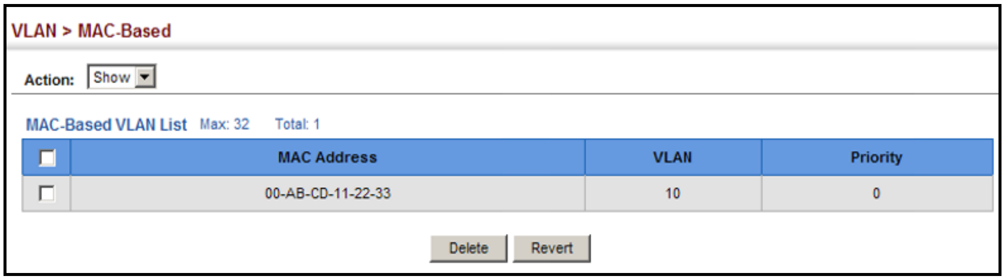
Priority (0-7)

To show the MAC addresses mapped to a VLAN:

1. Click VLAN, MAC-Based.

2. Select Show from the Action list.

Figure 77: Showing MAC-Based VLANs



VLAN > MAC-Based

Action: Show

MAC-Based VLAN List Max: 32 Total: 1

□	MAC Address	VLAN	Priority
□	00-AB-CD-11-22-33	10	0

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 708

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 189) 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 314).
  - Security Status (see "Configuring Port Security" on page 311) is enabled on the same interface.

PARAMETERS

These parameters are displayed in the web interface:

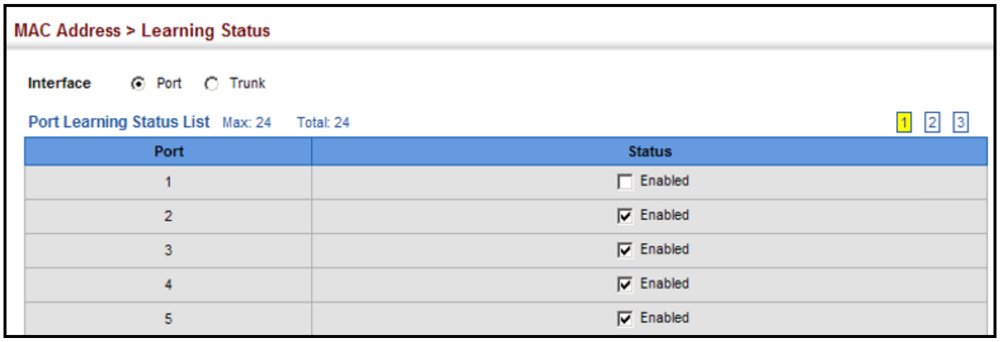
- **Interface** – Displays a list of ports or trunks.
- **Port** – Port Identifier. (Range: 1-26/50)
- **Trunk** – Trunk Identifier. (Range: 1-32)
- **Status** – The status of MAC address learning. (Default: Enabled)

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 78: Configuring MAC Address Learning



MAC Address > Learning Status

Interface ● Port ○ Trunk

Port Learning Status List Max: 24 Total: 24

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 804

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 in the web interface:

- **VLAN** – ID of configured VLAN. (Range: 1-4093)

- **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:

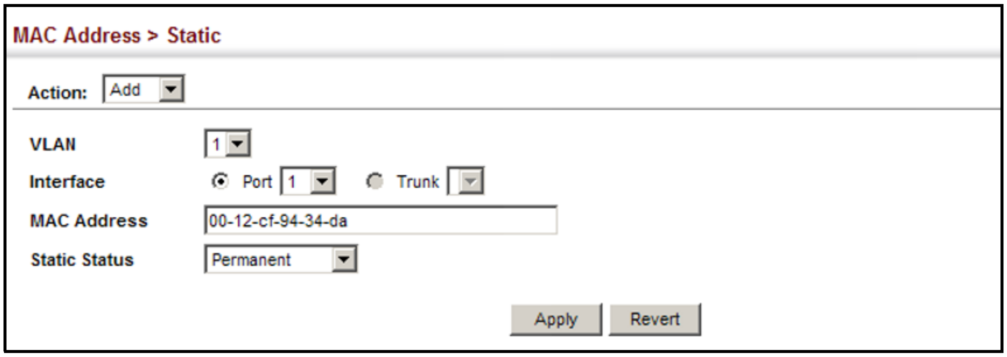
1. Click MAC Address, Static.

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 79: Configuring Static MAC Addresses



MAC Address > Static

Action: Add

VLAN: 1

Interface: ● Port 1 ○ Trunk

MAC Address: 00-12-cf-94-34-da

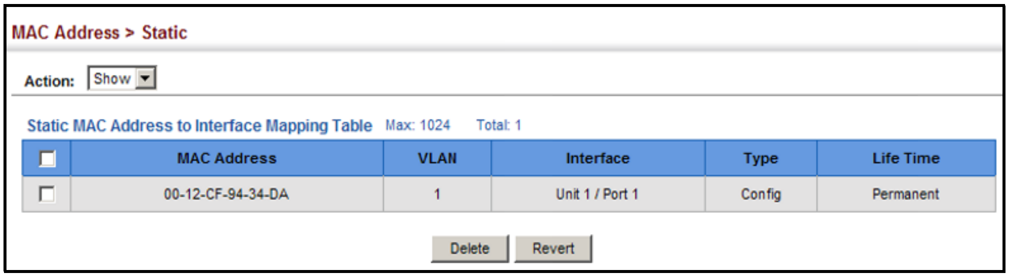
Static Status: Permanent

To show the static addresses in MAC address table:

1. Click MAC Address, Static.

2. Select Show from the Action list.

Figure 80: Displaying Static MAC Addresses



MAC Address > Static

Action: Show

Static MAC Address to Interface Mapping Table Max: 1024 Total: 1

□	MAC Address	VLAN	Interface	Type	Life Time
□	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 803

PARAMETERS

These parameters are displayed in the web interface:

- **Aging Status** – Enables/disables the function.

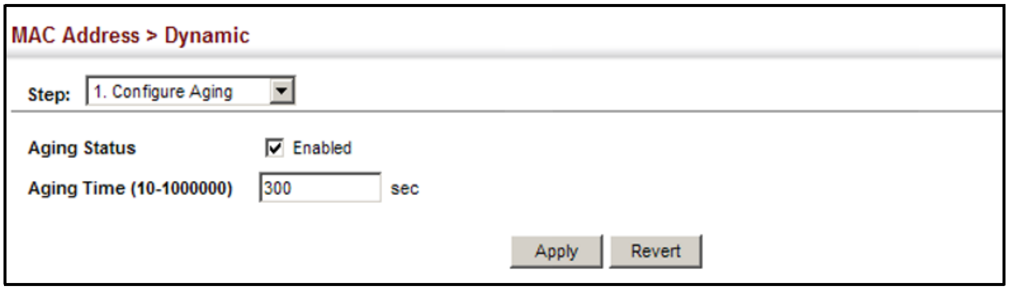
- **Aging Time** – The time after which a learned entry is discarded. (Range: 10-1000000 seconds; Default: 300 seconds)

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 81: Setting the Address Aging Time



MAC Address > Dynamic

Step: 1. 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 805

PARAMETERS

These parameters are displayed in the web interface:

- **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 (1-4093).
- **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.

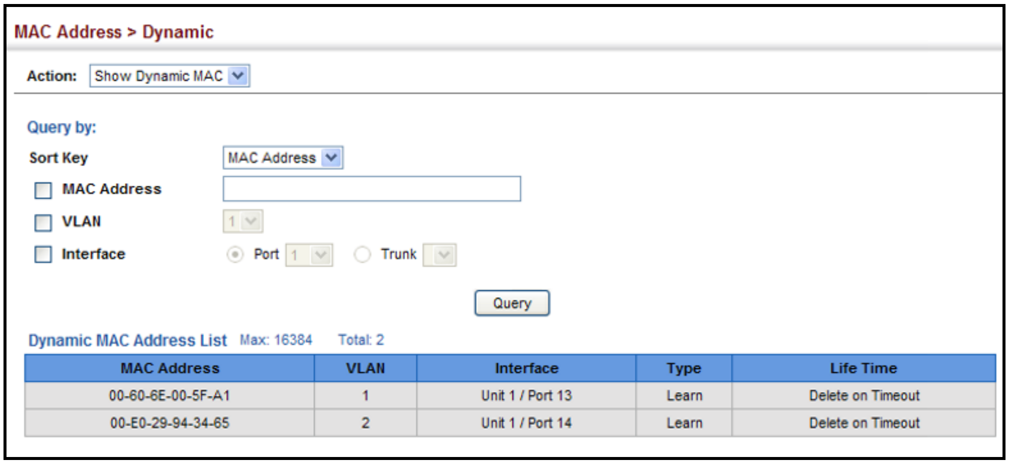
2. Select Show Dynamic MAC from the Action list.

3. Select the Sort Key (MAC Address, VLAN, or Interface).

4. Enter the search parameters (MAC Address, VLAN, or Interface).

5. Click Query.

Figure 82: 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 Max: 16384 Total: 2

MAC Address	VLAN	Interface	Type	Life Time
00-60-6E-00-5F-A1	1	Unit 1 / Port 13	Learn	Delete on Timeout
00-E0-29-94-34-65	2	Unit 1 / Port 14	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 805

PARAMETERS

These parameters are displayed in the web interface:

- **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.

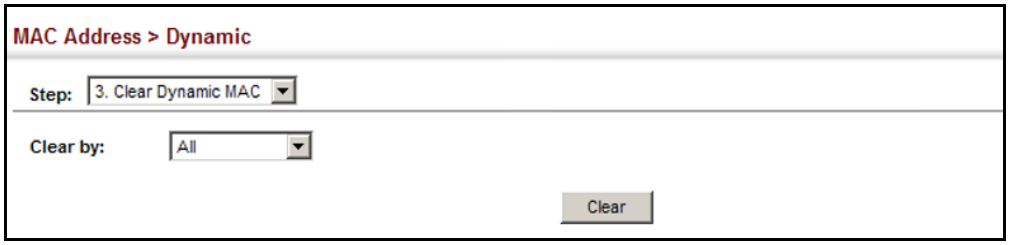
2. Select Clear Dynamic MAC from the Action list.

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 83: 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

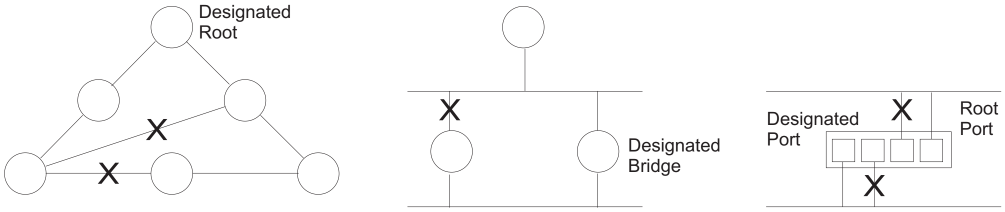
The Spanning Tree Algorithm (STA) can be used to detect and disable network loops, and to provide backup links between switches, bridges or routers. This allows the switch to interact with other bridging devices (that is, an STA-compliant switch, bridge or router) in your network to ensure that only 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 84: STP Root Ports and Designated Ports

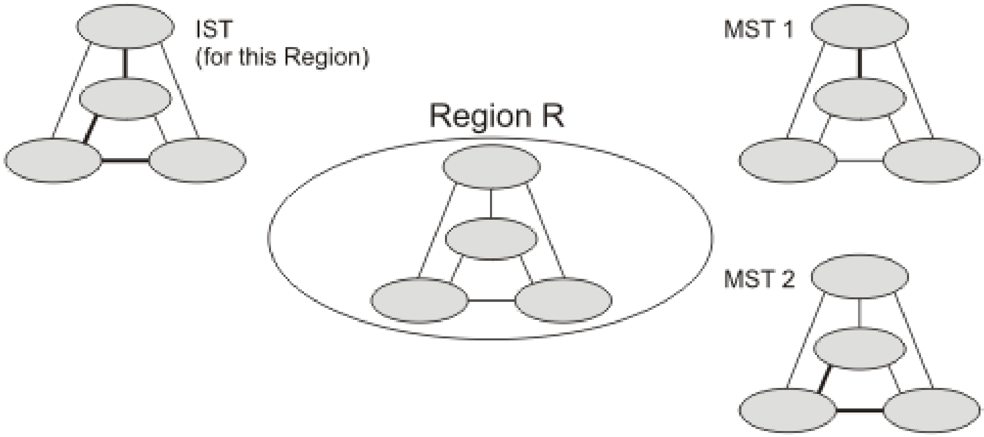


Once a stable network topology has been established, all bridges listen for Hello BPDUs (Bridge Protocol Data Units) transmitted from the Root Bridge. If a bridge does not get a Hello BPDU after a predefined interval (Maximum Age), the bridge assumes that the link to the Root Bridge is down. This bridge 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.

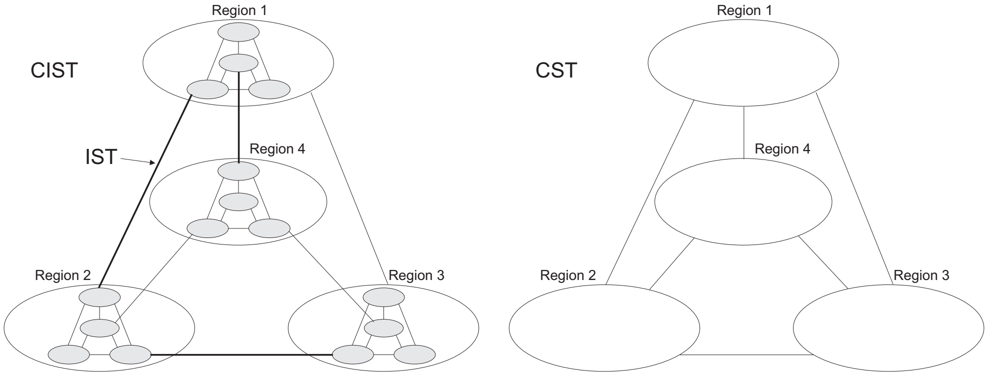
MSTP – When using STP or RSTP, it may be difficult to maintain a stable path between all VLAN members. Frequent changes in the tree structure can easily isolate some of the group members. MSTP (which is based on RSTP for fast convergence) is designed to support independent spanning trees based on VLAN 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 85: 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 212). 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 86: 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

- "Editing VLAN Groups" on page 836

PARAMETERS

These parameters are displayed in the web interface:

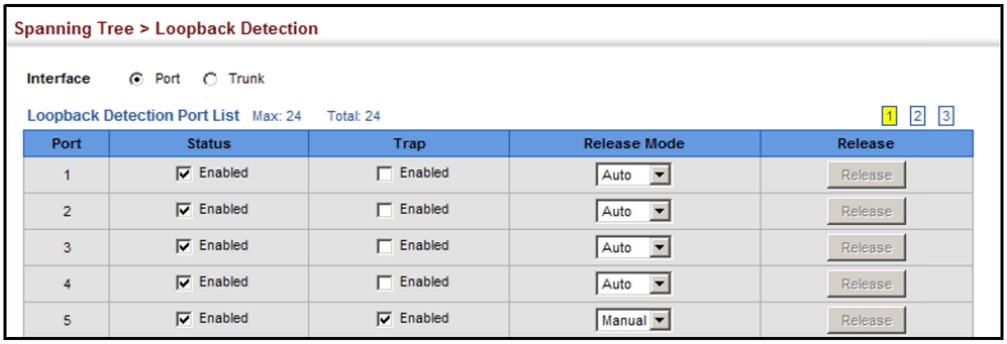
- **Interface** – Displays a list of ports or trunks.
- **Status** – Enables loopback detection on this interface. (Default: Enabled)
- **Trap** – Enables SNMP trap notification for loopback events on this interface. (Default: Disabled)
- **Release Mode** – Configures the interface for automatic or manual 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.

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 87: Configuring Port Loopback Detection



Spanning Tree > Loopback Detection

Interface ● Port ○ Trunk

Loopback Detection Port List Max: 24 Total: 24

Port	Status	Trap	Release Mode	Release
1	☑ Enabled	□ Enabled	Auto	Release
2	☑ Enabled	□ Enabled	Auto	Release
3	☑ Enabled	□ Enabled	Auto	Release
4	☑ Enabled	□ Enabled	Auto	Release
5	☑ Enabled	☑ Enabled	Manual	Release

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 807

COMMAND USAGE

- Spanning Tree Protocol[1]

  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:

[1] STP and RSTP BPDUs are transmitted as untagged frames, and will cross any VLAN boundaries.

    - 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.

    - 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 in the web interface:

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

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 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. (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

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)

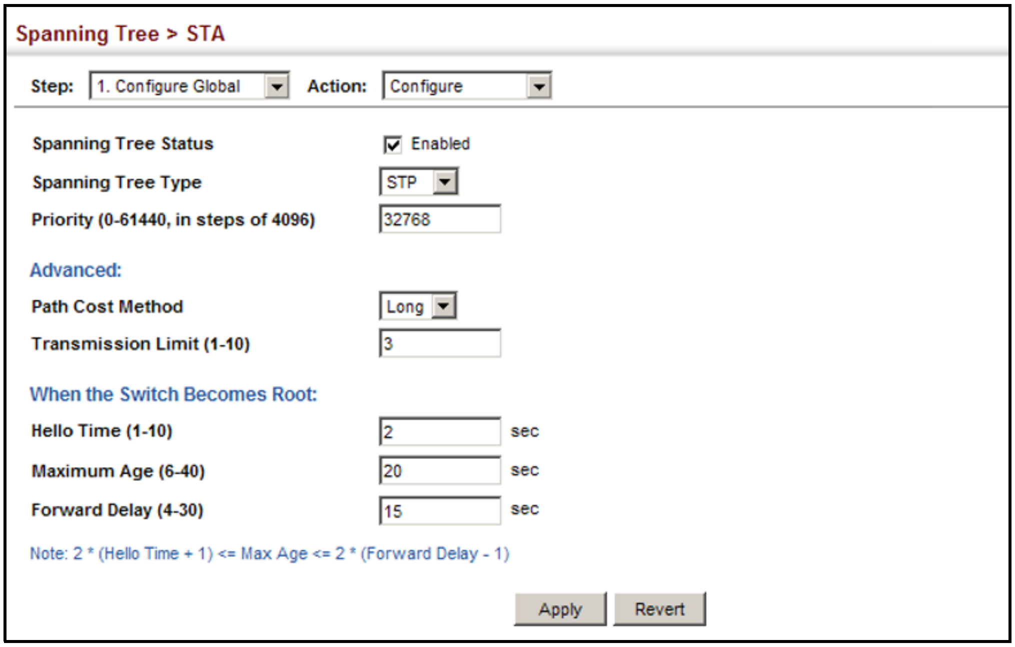
WEB INTERFACE

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 88: 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

Advanced:

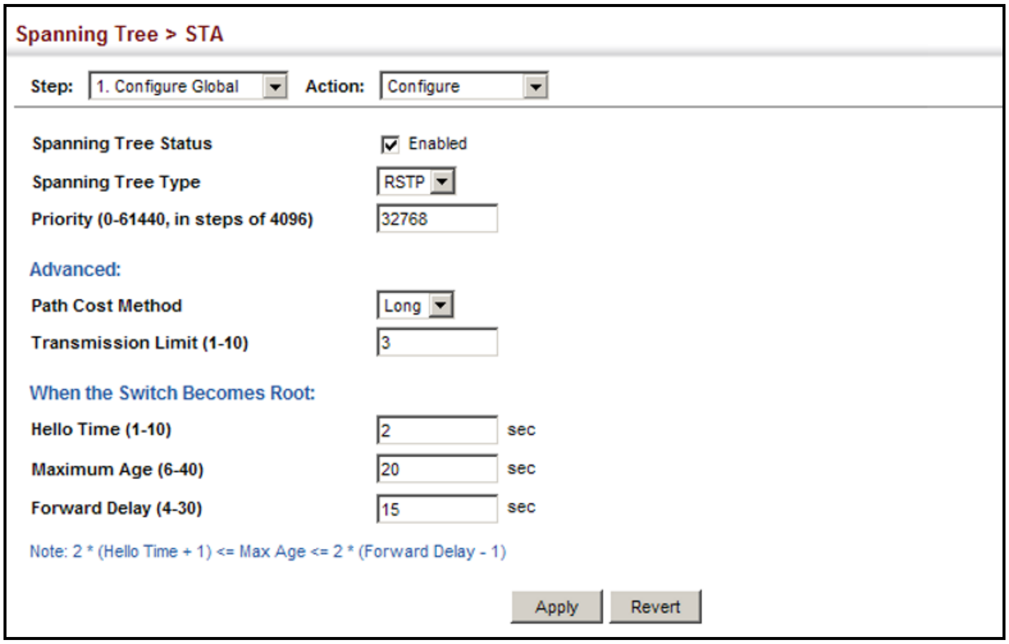
Path Cost Method Long
Transmission Limit (1-10) 3

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 89: 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

Advanced:

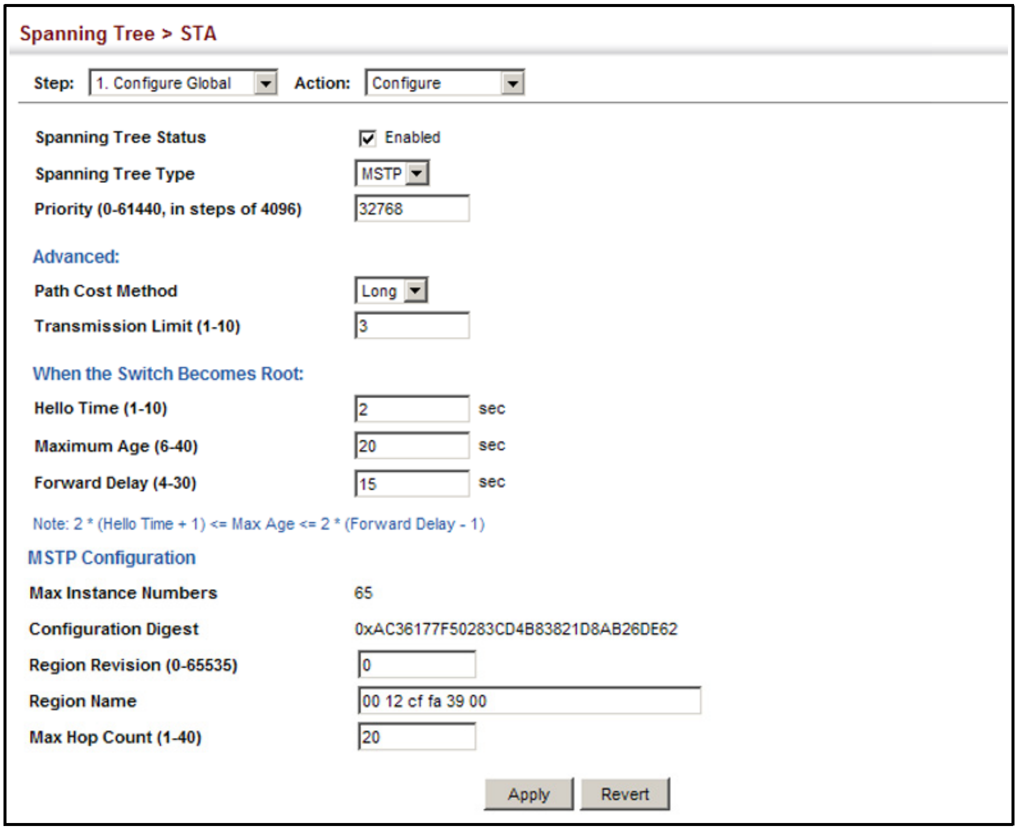
Path Cost Method Long
Transmission Limit (1-10) 3

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 90: 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
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	65
Configuration Digest	0xAC36177F50283CD4B83821D8AB26DE62
Region Revision (0-65535)	0
Region Name	00 12 cf fa 39 00
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 829
- "show spanning-tree mst configuration" on page 830

PARAMETERS

The parameters displayed in the web interface 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

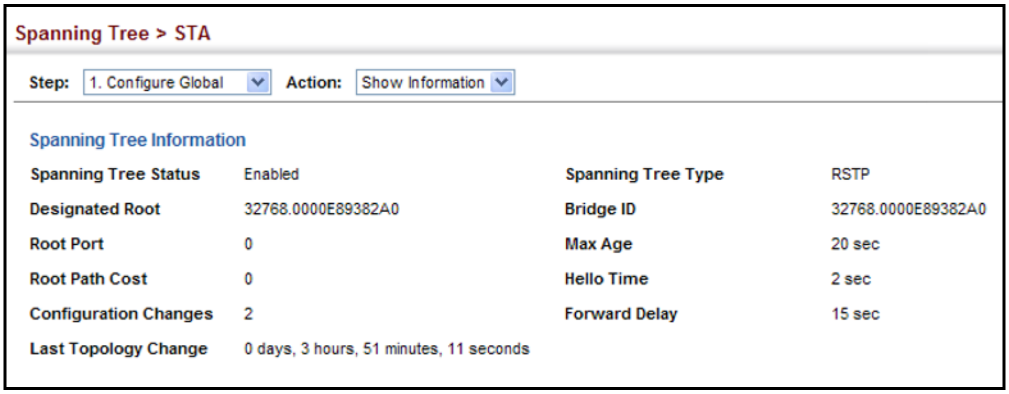
To display global STA settings:

1. Click Spanning Tree, STA.

2. Select Configure Global from the Step list.

3. Select Show Information from the Action list.

Figure 91: Displaying Global Settings for STA



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 807

PARAMETERS

These parameters are displayed in the web interface:

- **Interface** – Displays a list of ports or trunks.
- **Spanning Tree** – Enables/disables STA on this interface. (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. Also, not 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 9: Recommended STA Path Cost Range

Port Type	IEEE 802.1D-1998	IEEE 802.1w-2001
Gigabit Ethernet	3-10	2,000-200,000

Table 10: Default STA Path Costs

Port Type	Short Path Cost (IEEE 802.1D-1998)	Long Path Cost (802.1D-2004)
Gigabit Ethernet	10,000	10,000

- **Admin Link Type** – The link type attached to this interface.
  - Point-to-Point – A connection to exactly one other bridge.

[3] Refer to "Configuring Global Settings for STA" on page 199 for information on setting the path cost method.

  - 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: Disabled)

  - **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 199).

  An interface cannot function as an edge port under the following conditions:

  - If spanning tree mode is set to STP (page 199), edge-port mode cannot automatically transition to operational edge-port state using the automatic setting.

  - If loopback detection is enabled (page 198) 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 209).

- **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.

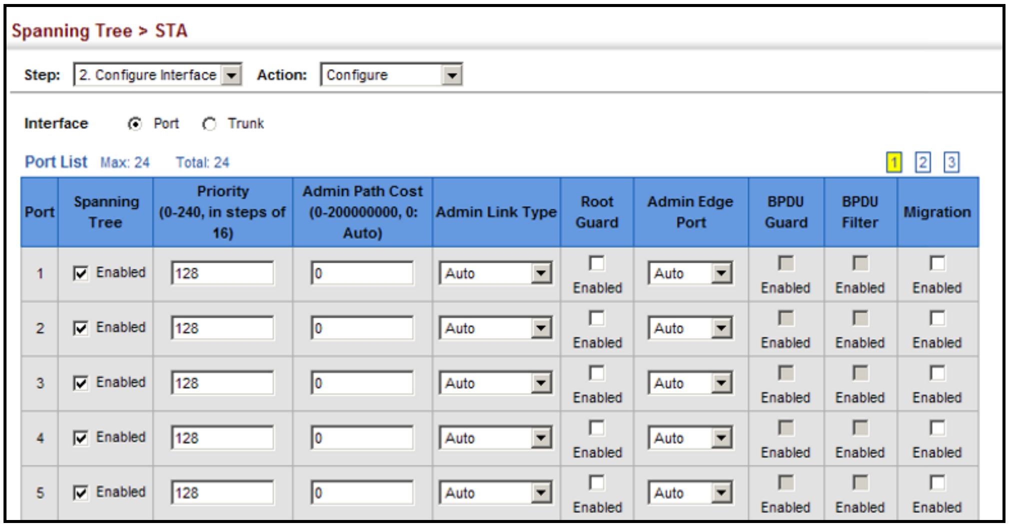
2. Select Configure Interface from the Step list.

3. Select Configure from the Action list.

4. Modify any of the required attributes.

5. Click Apply.

Figure 92: Configuring Interface Settings for STA



Spanning Tree > STA

Step: 2. Configure Interface   Action: Configure

Interface ● Port ○ Trunk

Port List Max: 24 Total: 24

Port	Spanning Tree	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	128	0	Auto	☐ Enabled	Auto	☐ Enabled	☐ Enabled	☐ Enabled
2	☑ Enabled	128	0	Auto	☐ Enabled	Auto	☐ Enabled	☐ Enabled	☐ Enabled
3	☑ Enabled	128	0	Auto	☐ Enabled	Auto	☐ Enabled	☐ Enabled	☐ Enabled
4	☑ Enabled	128	0	Auto	☐ Enabled	Auto	☐ Enabled	☐ Enabled	☐ Enabled
5	☑ 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 829

PARAMETERS

These parameters are displayed in the web interface:

- **Spanning Tree** – Shows if STA has been enabled on this interface.

- **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.

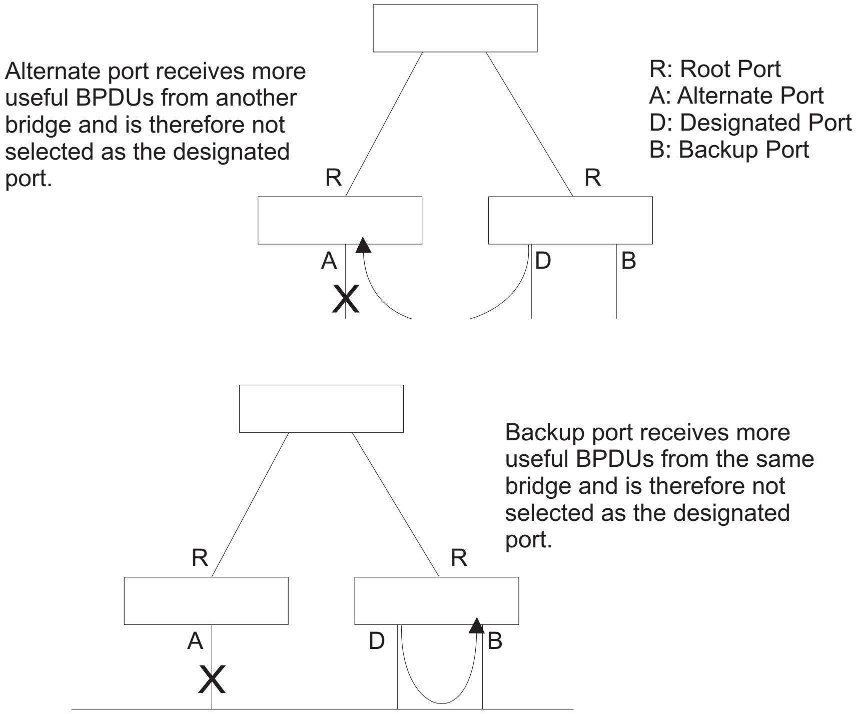
  The rules defining port status are:

  - 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 205.
- **Oper Edge Port** – This parameter is initialized to the setting for Admin Edge Port in STA Port Configuration on page 205 (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 the 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 93: STA Port Roles


Alternate port receives more useful BPDUs from another bridge and is therefore not selected as the designated port.

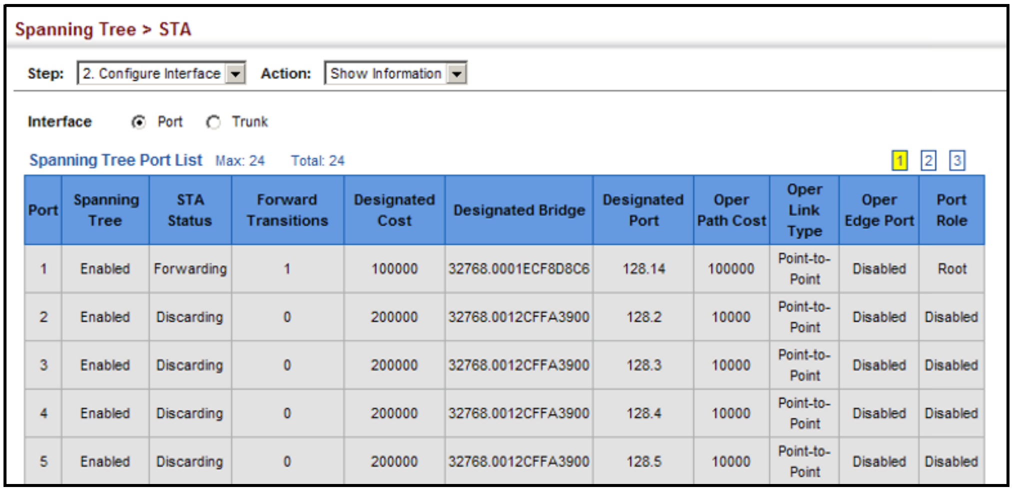
Backup port receives more useful BPDUs from the same bridge and is therefore not selected as the designated port.

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 94: Displaying Interface Settings for STA


Spanning Tree > STA

Step: 2. Configure Interface Action: Show Information

Interface ● Port ○ Trunk

Spanning Tree Port List Max: 24 Total: 24

Port	Spanning Tree	STA Status	Forward Transitions	Designated Cost	Designated Bridge	Designated Port	Oper Path Cost	Oper Link Type	Oper Edge Port	Port Role
1	Enabled	Forwarding	1	100000	32768.0001ECF8D8C6	128.14	100000	Point-to-Point	Disabled	Root
2	Enabled	Discarding	0	200000	32768.0012CFFA3900	128.2	10000	Point-to-Point	Disabled	Disabled
3	Enabled	Discarding	0	200000	32768.0012CFFA3900	128.3	10000	Point-to-Point	Disabled	Disabled
4	Enabled	Discarding	0	200000	32768.0012CFFA3900	128.4	10000	Point-to-Point	Disabled	Disabled
5	Enabled	Discarding	0	200000	32768.0012CFFA3900	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 807

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 199) 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 199).

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 in the web interface:

- **MST ID** – Instance identifier to configure. (Range: 0-4094)

- **VLAN ID** – VLAN to assign to this MST instance. (Range: 1-4093)

- **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.

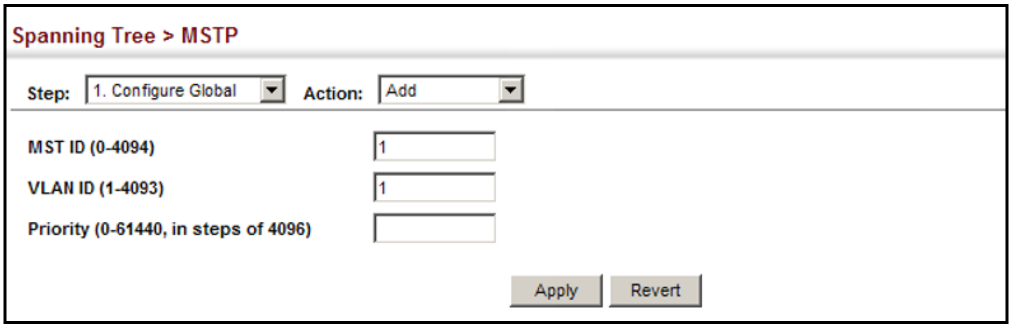
2. Select Configure Global from the Step list.

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 95: Creating an MST Instance



Spanning Tree > MSTP

Step: 1. Configure Global   Action: Add

MST ID (0-4094)	1
VLAN ID (1-4093)	1
Priority (0-61440, in steps of 4096)	

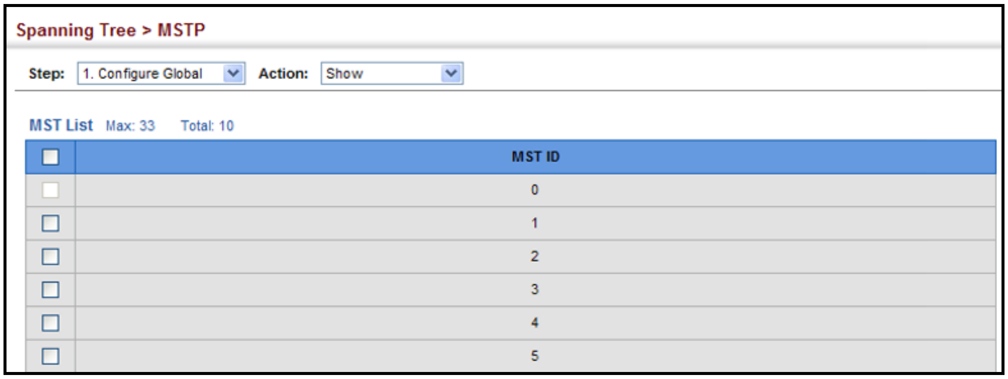
To show the MSTP instances:

1. Click Spanning Tree, MSTP.

2. Select Configure Global from the Step list.

3. Select Show from the Action list.

Figure 96: Displaying MST Instances



Spanning Tree > MSTP

Step: 1. Configure Global   Action: Show

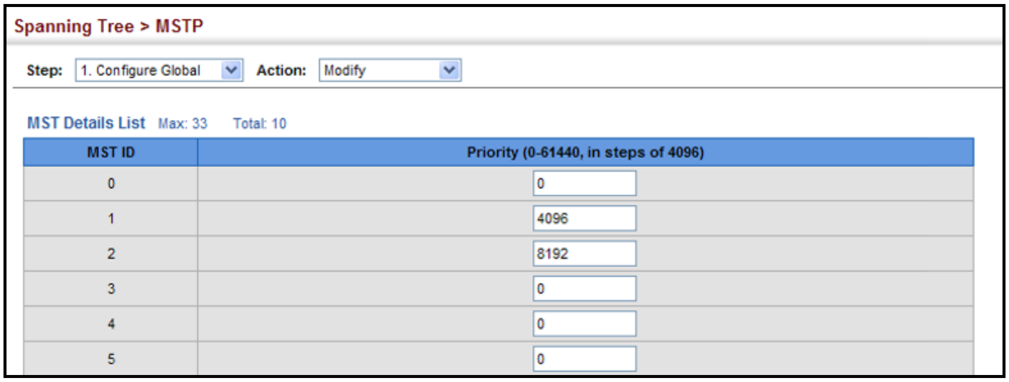
MST List Max: 33 Total: 10

□	MST ID
□	0
□	1
□	2
□	3
□	4
□	5

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 97: Modifying the Priority for an MST Instance



Spanning Tree > MSTP

Step: 1. Configure Global Action: Modify

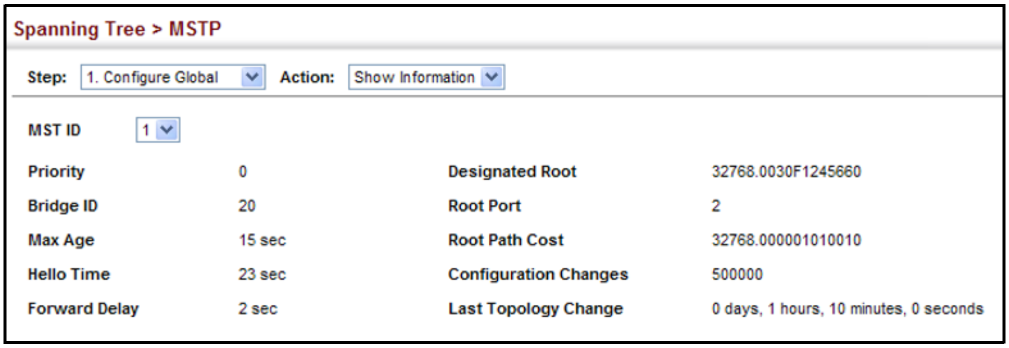
MST Details List Max: 33 Total: 10

MST ID	Priority (0-61440, in steps of 4096)
0	0
1	4096
2	8192
3	0
4	0
5	0

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 204.

Figure 98: Displaying Global Settings for an MST Instance



Spanning Tree > MSTP

Step: 1. Configure Global Action: Show Information

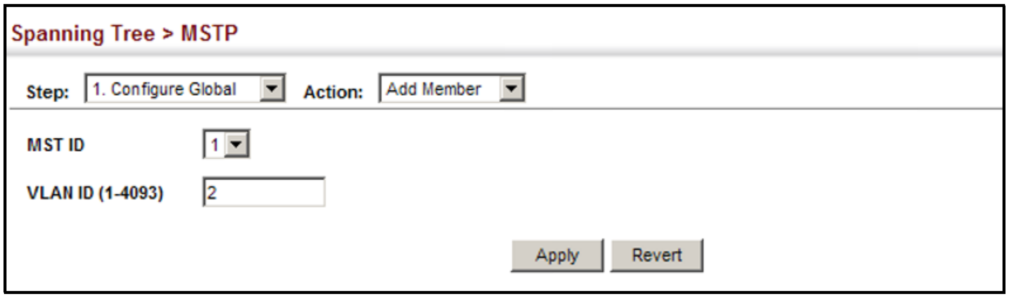
MST ID 1

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 99: Adding a VLAN to an MST Instance



Spanning Tree > MSTP

Step: 1. Configure Global
Action: Add Member

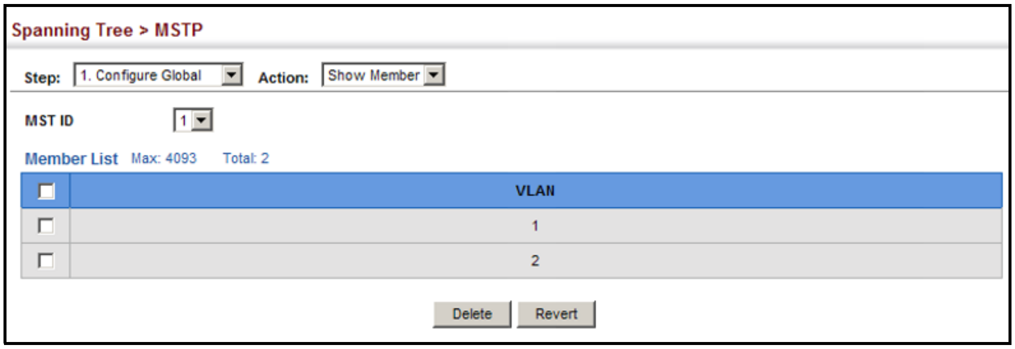
MST ID: 1

VLAN ID (1-4093): 2

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 100: Displaying Members of an MST Instance



Spanning Tree > MSTP

Step: 1. Configure Global
Action: Show Member

MST ID: 1

Member List Max: 4093 Total: 2

□	VLAN
□	1
□	2

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 807

PARAMETERS

These parameters are displayed in the web interface:

- **MST Instance 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 209 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 3-63), 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.

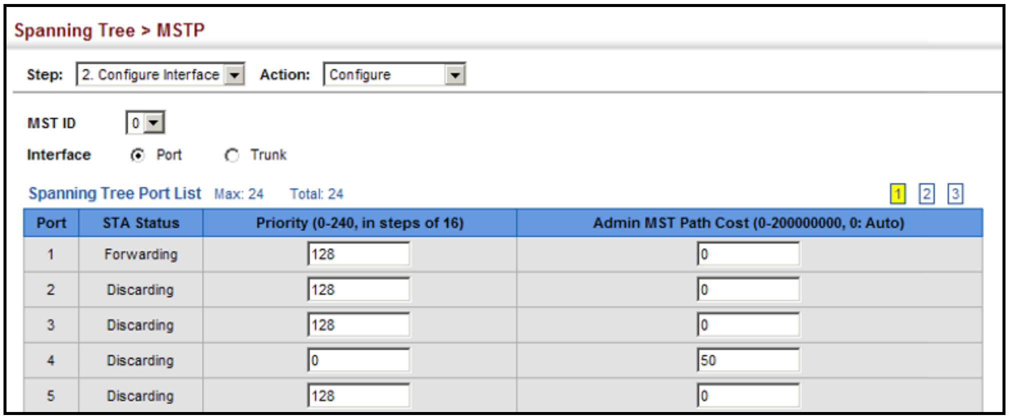
The recommended range is listed in Table 9 on page 206. The default path costs are listed in Table 10 on page 206.

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 101: Configuring MSTP Interface Settings



Spanning Tree > MSTP

Step: 2. Configure Interface Action: Configure

MST ID 0

Interface ● Port ○ Trunk

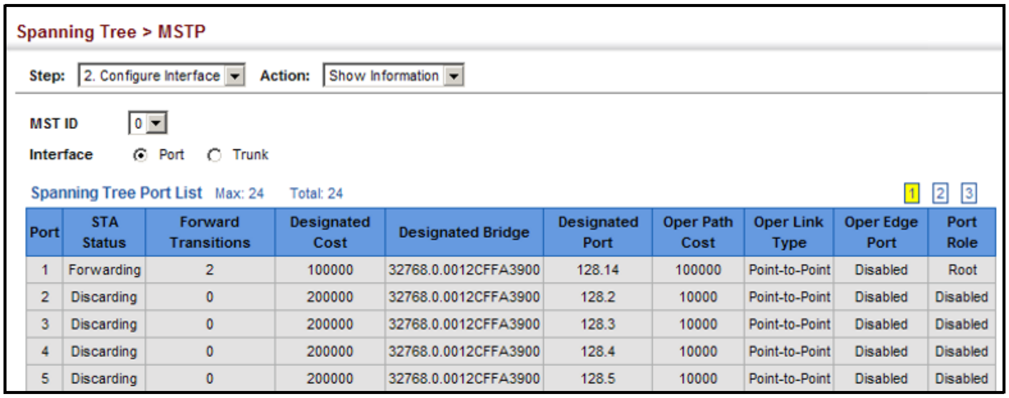
Spanning Tree Port List Max: 24 Total: 24 1 2 3

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	0	50
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 102: Displaying MSTP Interface Settings



Spanning Tree > MSTP

Step: 2. Configure Interface Action: Show Information

MST ID 0

Interface ● Port ○ Trunk

Spanning Tree Port List Max: 24 Total: 24 1 2 3

Port	STA Status	Forward Transitions	Designated Cost	Designated Bridge	Designated Port	Oper Path Cost	Oper Link Type	Oper Edge Port	Port Role
1	Forwarding	2	100000	32768.0.0012CFFA3900	128.14	100000	Point-to-Point	Disabled	Root
2	Discarding	0	200000	32768.0.0012CFFA3900	128.2	10000	Point-to-Point	Disabled	Disabled
3	Discarding	0	200000	32768.0.0012CFFA3900	128.3	10000	Point-to-Point	Disabled	Disabled
4	Discarding	0	200000	32768.0.0012CFFA3900	128.4	10000	Point-to-Point	Disabled	Disabled
5	Discarding	0	200000	32768.0.0012CFFA3900	128.5	10000	Point-to-Point	Disabled	Disabled

9 Rate Limit Configuration

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 801

Parameters

These parameters are displayed in the web interface:

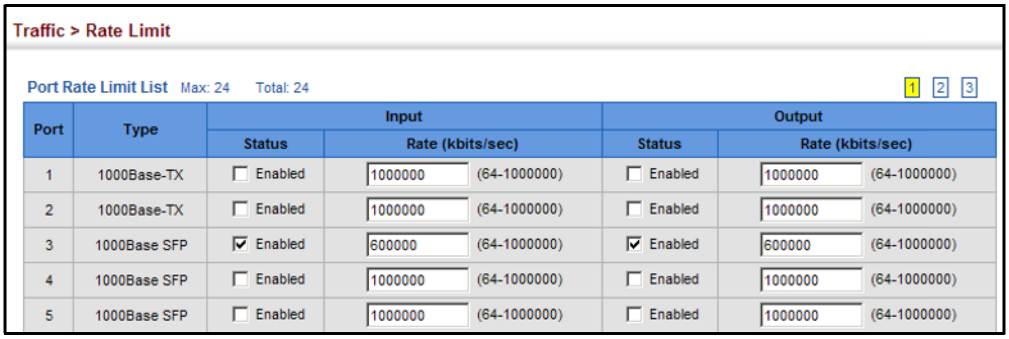
- **Port** – Displays the port number.
- **Type** – Indicates the port type. (1000Base-T, 1000Base SFP)
- **Status** – Enables or disables the rate limit. (Default: Disabled)
- **Rate** – Sets the rate limit level. (Range: 64 - 1,000,000 kbits per second)

Web Interface

To configure rate limits:

1. Click Traffic, Rate Limit.
2. Enable the Rate Limit Status for the required ports.
3. set the rate limit for the individual ports,.
4. Click Apply.

Figure 103: Configuring Rate Limits



Traffic > Rate Limit

Port Rate Limit List Max: 24 Total: 24

Port	Type	Input		Output	
		Status	Rate (kbits/sec)	Status	Rate (kbits/sec)
1	1000Base-TX	□ Enabled	1000000 (64-1000000)	□ Enabled	1000000 (64-1000000)
2	1000Base-TX	□ Enabled	1000000 (64-1000000)	□ Enabled	1000000 (64-1000000)
3	1000Base SFP	☑ Enabled	600000 (64-1000000)	☑ Enabled	600000 (64-1000000)
4	1000Base SFP	□ Enabled	1000000 (64-1000000)	□ Enabled	1000000 (64-1000000)
5	1000Base SFP	□ Enabled	1000000 (64-1000000)	□ Enabled	1000000 (64-1000000)

10 Storm Control Configuration

Use the Traffic > Storm Control page to configure broadcast storm control thresholds. Broadcast 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 broadcast traffic on your network, performance can be severely degraded or everything can come to complete halt.

You can protect your network from broadcast storms by setting a threshold for broadcast traffic. Any broadcast packets exceeding the specified threshold will then be dropped.

CLI References

- "switchport packet-rate" on page 777

Command Usage

- Broadcast Storm Control is enabled by default.
- Broadcast control does not effect IP multicast traffic.

Parameters

These parameters are displayed in the web interface:

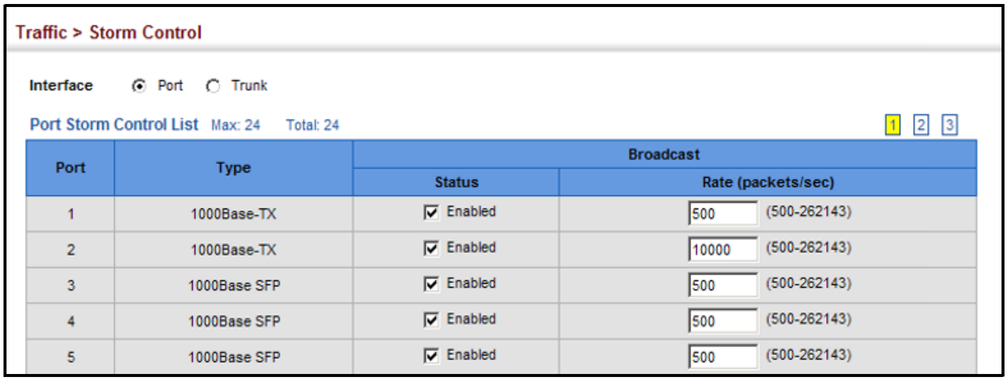
- **Interface** – Displays a list of ports or trunks.
- **Type** – Indicates interface type. (100Base-T, 100Base SFP)
- **Broadcast** – Specifies storm control for broadcast traffic.
- **Status** – Enables or disables storm control. (Default: Enabled)
- **Rate** – Threshold level as a rate; i.e., packets per second. (Range: 500-262143 packets per second; Default: 500 pps)

Web Interface

To configure broadcast storm control:

1. Click Traffic, Storm Control.
2. Set the Status field to enable or disable storm control.
3. Set the required threshold beyond which the switch will start dropping packets.
4. Click Apply.

Figure 104: Configuring Broadcast Storm Control



Traffic > Storm Control

Interface ● Port ○ Trunk

Port Storm Control List Max: 24 Total: 24

Port	Type	Broadcast	
		Status	Rate (packets/sec)
1	1000Base-TX	☑ Enabled	500 (500-262143)
2	1000Base-TX	☑ Enabled	10000 (500-262143)
3	1000Base SFP	☑ Enabled	500 (500-262143)
4	1000Base SFP	☑ Enabled	500 (500-262143)
5	1000Base SFP	☑ Enabled	500 (500-262143)

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, 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 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 nap from the policy rule settings screen (see page 227).

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, or a VLAN.

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 885

COMMAND USAGE

- The class map is used with a policy map (page 227) to create a service policy (page 237) 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 in the web interface:

Add

- **Class Name** – Name of the class map. (Range: 1-16 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

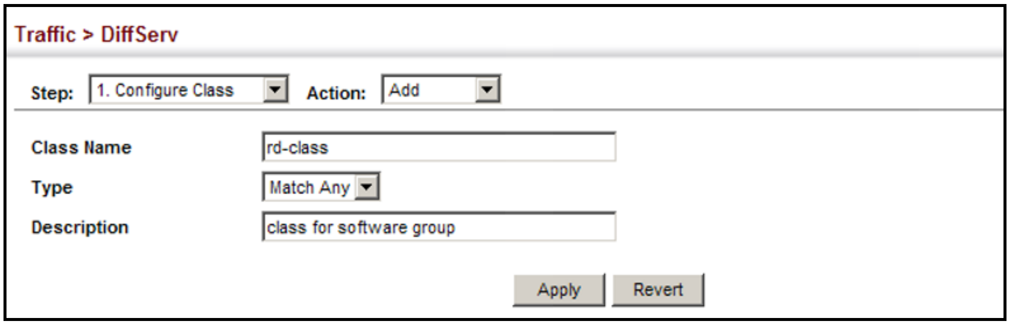
- **Class Name** – Name of the class map.
- **Type** – Only one match command is permitted per class map, so the match-any field refers to the criteria specified by the lone match command.
- **ACL** – Name of an access control list. Any type of ACL can be specified, including standard or extended IP ACLs and MAC ACLs.
- **IP DSCP** – A DSCP value. (Range: 0-63)
- **IP Precedence** – An IP Precedence value. (Range: 0-7)
- **VLAN ID** – A VLAN. (Range:1-4093)

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 105: Configuring a Class Map



Traffic > DiffServ

Step: 1. Configure Class
Action: Add

Class Name: rd-class
Type: Match Any
Description: class for software group

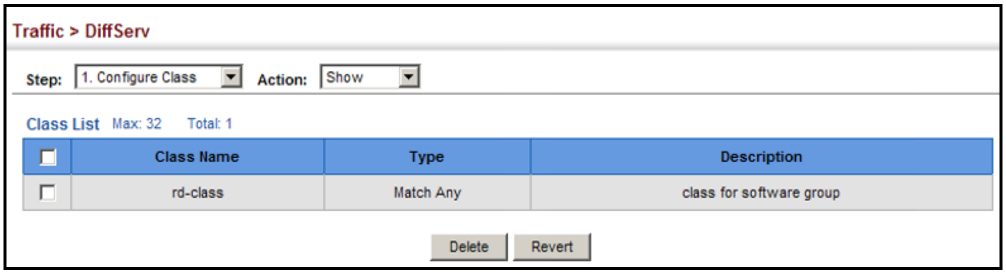
To show the configured class maps:

1. Click Traffic, DiffServ.

2. Select Configure Class from the Step list.

3. Select Show from the Action list.

Figure 106: Showing Class Maps



Traffic > DiffServ

Step: 1. Configure Class Action: Show

Class List Max: 32 Total: 1

□	Class Name	Type	Description
□	rd-class	Match Any	class for software group

To edit the rules for a class map:

1. Click Traffic, DiffServ.

2. Select Configure Class from the Step list.

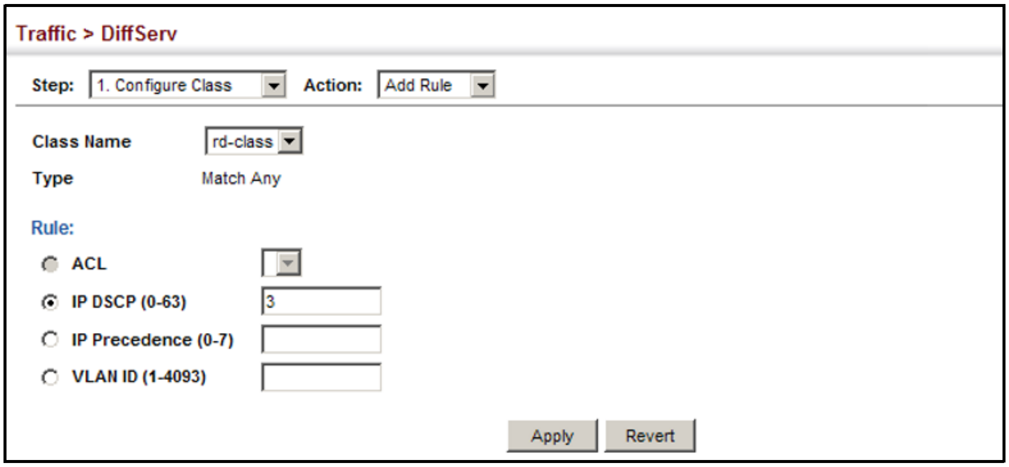
3. Select Add Rule from the Action list.

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, or a VLAN. You can specify up to 16 items to match when assigning ingress traffic to a class map.

6. Click Apply.

Figure 107: Adding Rules to a Class Map



Traffic > DiffServ

Step: 1. Configure Class Action: Add Rule

Class Name: rd-class

Type: Match Any

Rule:

○ ACL

● IP DSCP (0-63): 3

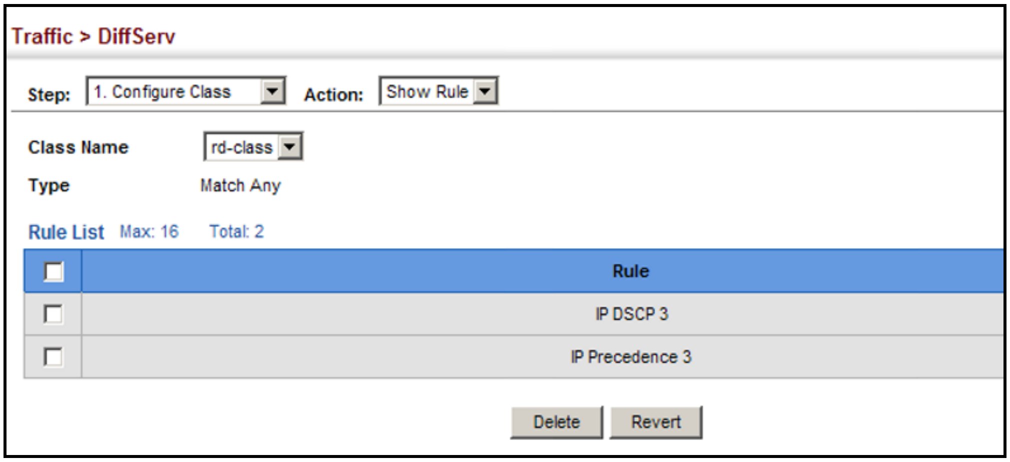
○ IP Precedence (0-7):

○ VLAN ID (1-4093):

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 108: 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 Max: 16 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 224), modify service tagging, and enforce bandwidth policing. A policy map can then be bound by a service policy to one or more interfaces (page 237).

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 which are used to prioritize service to packets of different colors as described below. 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 $Tc(t)-B \geq 0$, 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 $Te(t)-B \geq 0$, 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.

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 which are used to prioritize service to packets of different colors as described below. 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 885

COMMAND USAGE

- A policy map can contain 128 class statements that can be applied to the same interface (page 237). Up to 26 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 237) to take effect.

PARAMETERS

These parameters are displayed in the web interface:

Add

- **Policy Name** – Name of policy map. (Range: 1-16 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** – Configures the service provided to ingress traffic. Packets matching the rule settings for a class map can be remarked as follows:
  - **Set CoS** – Sets a priority bits in the VLAN tag for matching packets. (Range: 0-7)
  - **Set PHB** – Sets the per-hop behavior for a matching packet in the ToS field of the IP header. (Range: 0-7)
- **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: 1-1000000 kbps or maximum port speed, whichever is lower)

      The rate cannot exceed the configured interface speed.
    - **Committed Burst Size** (BC) – Burst in bytes. (Range: 64-524288 bytes)

      The burst size cannot exceed 16 Mbytes.
    - **Conform** – Specifies whether that traffic conforming to the maximum rate (CIR) will be transmitted without any change to the DSCP service level, or if the DSCP service level will be modified.
      - **Transmit** – Transmits in-conformance traffic without any change to the DSCP service level.
      - **Set IP DSCP** – Modifies DSCP priority for in-conformance traffic. (Range: 0-63)

  - **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 prioritize service to packets of different colors.

  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: 1-1000000 kbps or maximum port speed, whichever is lower)

    The rate cannot exceed the configured interface speed.

  - **Committed Burst Size** (BC) – Burst in bytes. (Range: 64-524288 bytes)

    The burst size cannot exceed 16 Mbytes.

  - **Exceeded Burst Size** (BE) – Burst in excess of committed burst size. (Range: 64-524288 bytes)

    The burst size cannot exceed 16 Mbytes.

  - **Conform** – Specifies whether that traffic conforming to the maximum rate (CIR) will be transmitted without any change to the DSCP service level, or if the DSCP service level will be modified.

    - **Transmit** – Transmits in-conformance traffic without any change to the DSCP service level.

    - **Set IP DSCP** – Modifies DSCP priority for in-conformance traffic. (Range: 0-63)

        - **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 prioritize service to packets of different colors.

      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: 1-1000000 kbps or maximum port speed, whichever is lower)

          The rate cannot exceed the configured interface speed.

        - **Peak Information Rate** (PIR) – Rate in kilobits per second. (Range: 1-1000000 kbps or maximum port speed, whichever is lower)

          The rate cannot exceed the configured interface speed.

        - **Committed Burst Size** (BC) – Burst in bytes. (Range: 64-524288 bytes)

          The burst size cannot exceed 16 Mbytes.

- **Peak Burst Size** (BP) – Burst size in bytes.
  (Range: 64-524288 bytes)

  The burst size cannot exceed 16 Mbytes.

- **Conform** – Specifies whether that traffic conforming to the maximum rate (CIR) will be transmitted without any change to the DSCP service level, or if the DSCP service level will be modified.

  - **Transmit** – Transmits in-conformance traffic without any change to the DSCP service level.

  - **Set IP DSCP** – Modifies DSCP priority for in-conformance traffic. (Range: 0-63)

- **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.

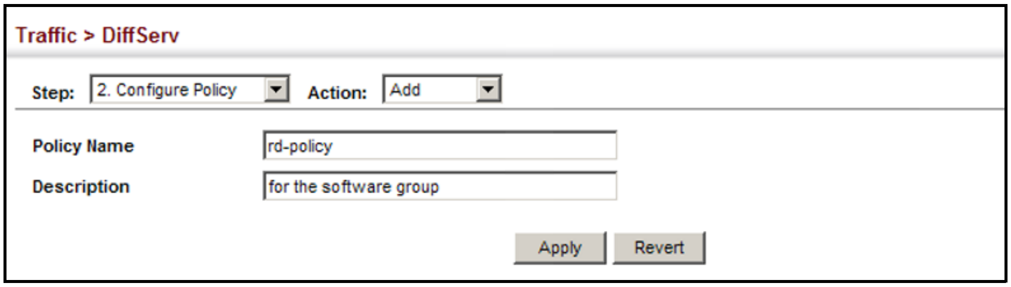
3. Select Add from the Action list.

4. Enter a policy name.

5. Enter a description.

6. Click Add.

Figure 109: Configuring a Policy Map



Traffic > DiffServ

Step: 2. Configure Policy Action: Add

Policy Name: rd-policy

Description: for the software group

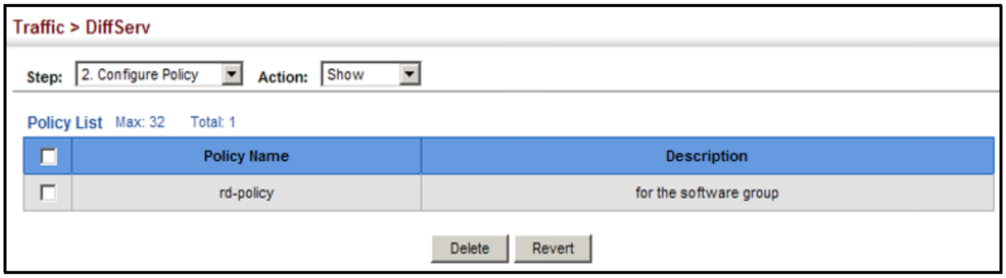
To show the configured policy maps:

1. Click Traffic, DiffServ.

2. Select Configure Policy from the Step list.

3. Select Show from the Action list.

Figure 110: Showing Policy Maps



Traffic > DiffServ

Step: 2. Configure Policy Action: Show

Policy List Max: 32 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.

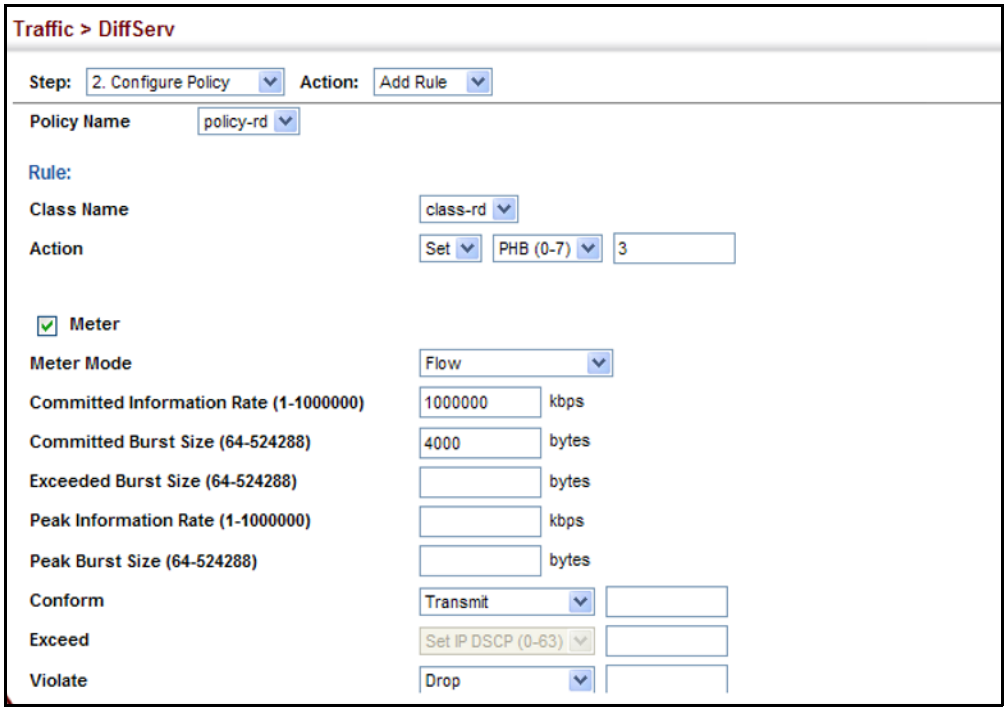
3. Select Add Rule from the Action list.

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 111: Adding Rules to a Policy Map



Traffic > DiffServ

Step: 2. Configure Policy Action: Add Rule

Policy Name policy-rd

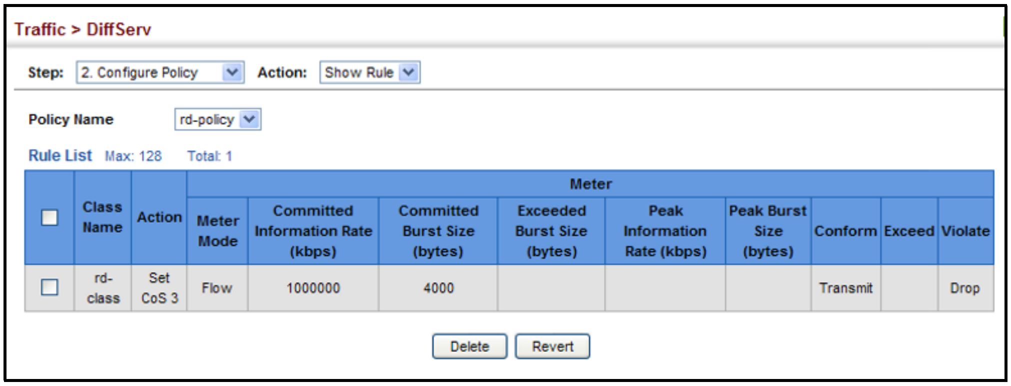
Rule:

Class Name	class-rd	
Action	Set PHB (0-7) 3	
☑ Meter		
Meter Mode	Flow	
Committed Information Rate (1-1000000)	1000000	kbps
Committed Burst Size (64-524288)	4000	bytes
Exceeded Burst Size (64-524288)		bytes
Peak Information Rate (1-1000000)		kbps
Peak Burst Size (64-524288)		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 112: Showing the Rules for a Policy Map



Traffic > DiffServ

Step: 2. Configure Policy Action: Show Rule

Policy Name rd-policy

Rule List Max: 128 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 CoS 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 an ingress port.

CLI REFERENCES

- "Quality of Service Commands" on page 885

COMMAND USAGE

- First define a class map, define a policy map, and bind the service policy to the required interface.
- Only one policy map can be bound to an interface.
- The switch does not allow a policy map to be bound to an interface for egress traffic.

PARAMETERS

These parameters are displayed in the web interface:

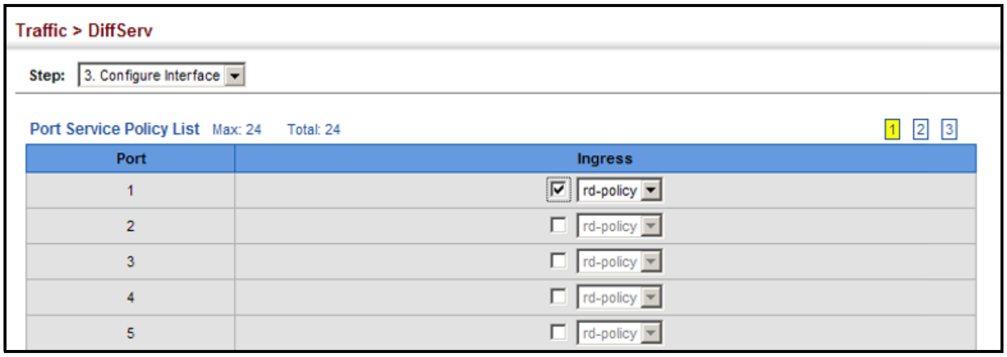
- **Port** – Specifies a port.
- **Ingress** – Applies the selected rule to ingress traffic.

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 field to enable a policy map for a port.
4. Select a policy map from the scroll-down box.
5. Click Apply.

Figure 113: Attaching a Policy Map to a Port



Traffic > DiffServ

Step: 3. Configure Interface

Port Service Policy List Max: 24 Total: 24

Port	Ingress
1	☑ rd-policy
2	☐ rd-policy
3	☐ rd-policy
4	☐ rd-policy
5	☐ 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 864

PARAMETERS

These parameters are displayed in the web interface:

- **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: 1-4093)
- **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)

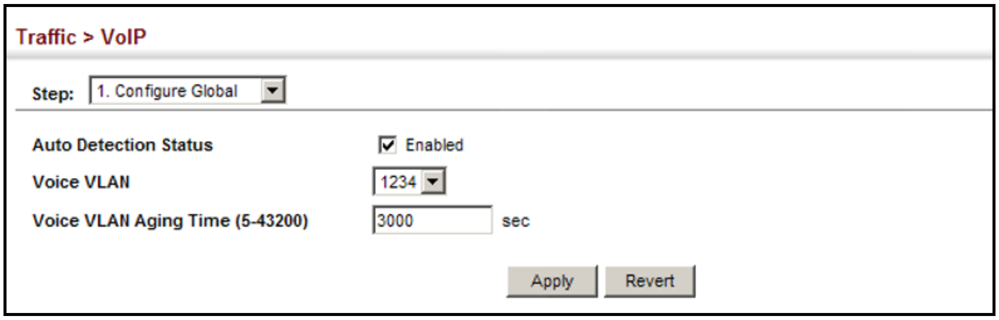
NOTE: The Voice VLAN ID cannot be modified when the global Auto Detection Status is enabled.

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 114: Configuring a Voice VLAN



Traffic > VoIP

Step: 1. Configure Global

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 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. Use the Traffic > VoIP (Configure OUI) page to configure this feature.

CLI REFERENCES

- "Configuring Voice VLANs" on page 864

PARAMETERS

These parameters are displayed in the web interface:

- **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. Selecting 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. Selecting 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.

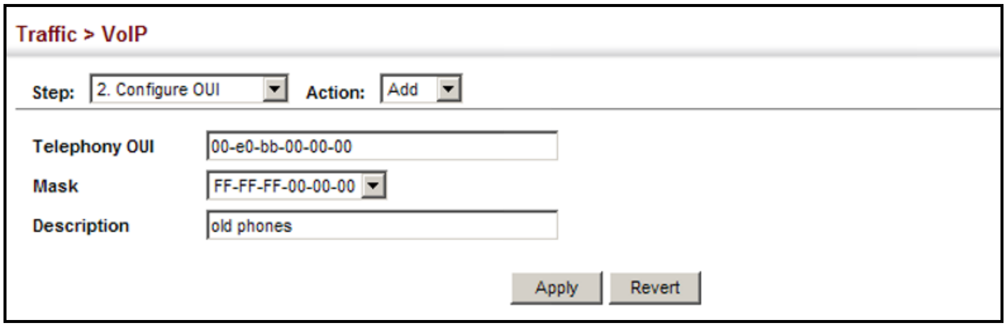
4. Enter a MAC address that specifies the OUI for VoIP devices in the network.

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 115: Configuring an OUI Telephony List



Traffic > VoIP

Step: 2. Configure OUI   Action: Add

Telephony OUI: 00-e0-bb-00-00-00

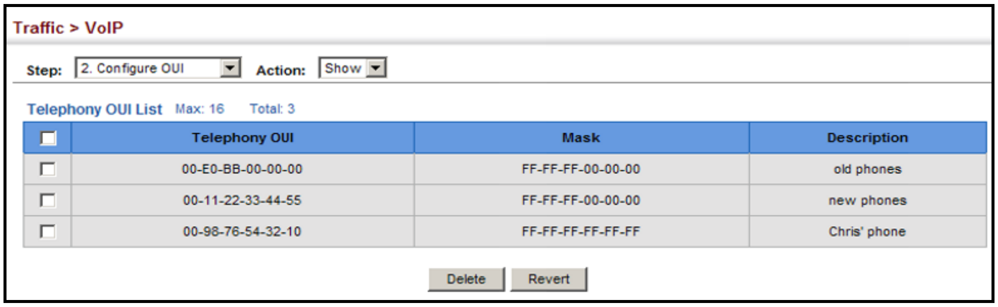
Mask: FF-FF-FF-00-00-00

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 116: Showing an OUI Telephony List



Traffic > VoIP

Step: 2. Configure OUI   Action: Show

Telephony OUI List Max: 16 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 864

PARAMETERS

These parameters are displayed in the web interface:

- **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 manufacturers 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 340 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.

WEB INTERFACE

To configure VoIP traffic settings for a port:

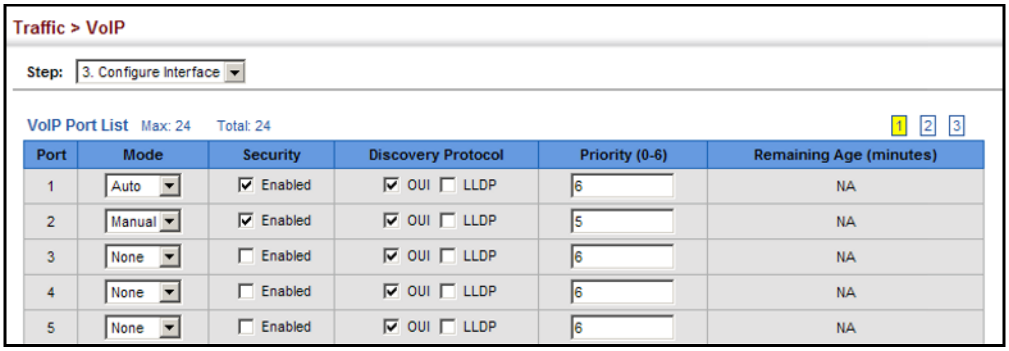
1. Click Traffic, VoIP.

2. Select Configure Interface from the Step list.

3. Configure any required changes to the VoIP settings each port.

4. Click Apply.

Figure 117: Configuring Port Settings for a Voice VLAN



Traffic > VoIP

Step: 3. Configure Interface

VoIP Port List Max: 24 Total: 24

Port	Mode	Security	Discovery Protocol	Priority (0-6)	Remaining Age (minutes)
1	Auto	☑ Enabled	☑ OUI □ LLDP	6	NA
2	Manual	☑ Enabled	☑ OUI □ LLDP	5	NA
3	None	□ Enabled	☑ OUI □ LLDP	6	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.
- Network Access - Configure MAC authentication and dynamic VLAN 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.
- IP Source Guard – Filters untrusted DHCP messages on insecure ports by building and maintaining a DHCP snooping binding table.
- 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, 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 247.
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 660

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 in the web interface:

- **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.

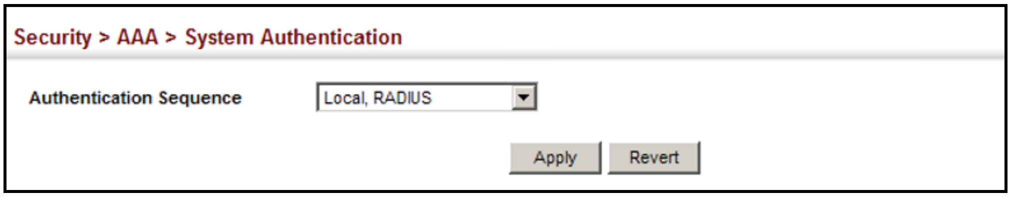
  - [authentication sequence] – User authentication is performed by up to three authentication methods in the indicated sequence.

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 118: Configuring the Authentication Sequence



Security > AAA > System Authentication

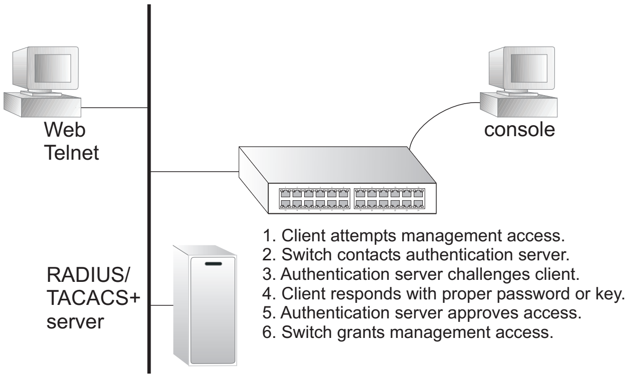
Authentication Sequence: Local, RADIUS

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 119: 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 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 662
- "TACACS+ Client" on page 666
- "AAA" on page 669

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 in the web interface:

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)
  - **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: 1-255 characters)
- **Sequence at Priority** - Specifies the RADIUS server and sequence to use for the group. (Range: 1-5)

  When specifying the priority sequence for a sever, the server index must already be defined (see "Configuring Local/Remote Logon Authentication" on page 247).

WEB INTERFACE

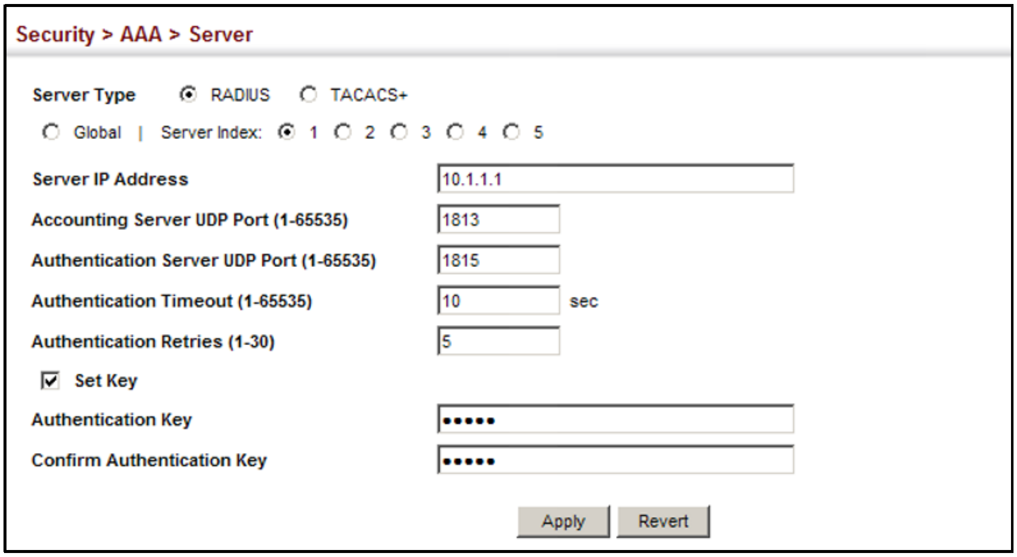
To configure the parameters for RADIUS or TACACS+ authentication:

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 120: Configuring Remote Authentication Server (RADIUS)



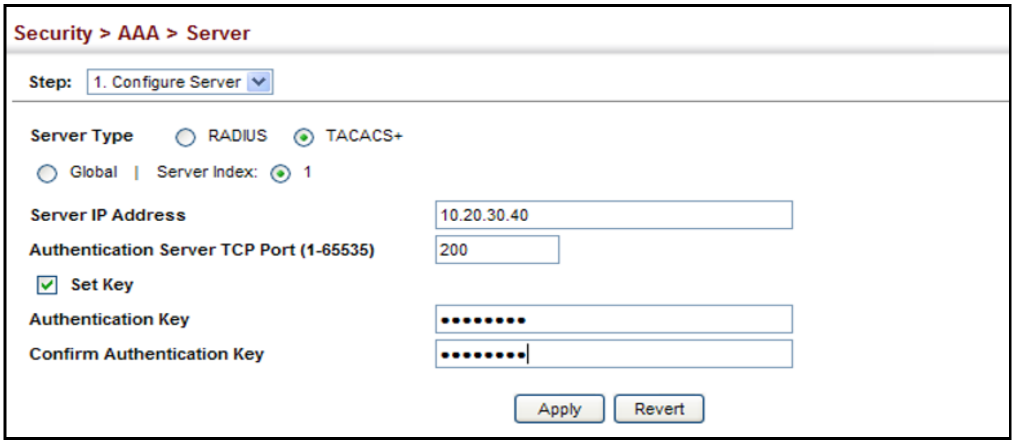
Security > AAA > Server

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 121: 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
☑ 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.

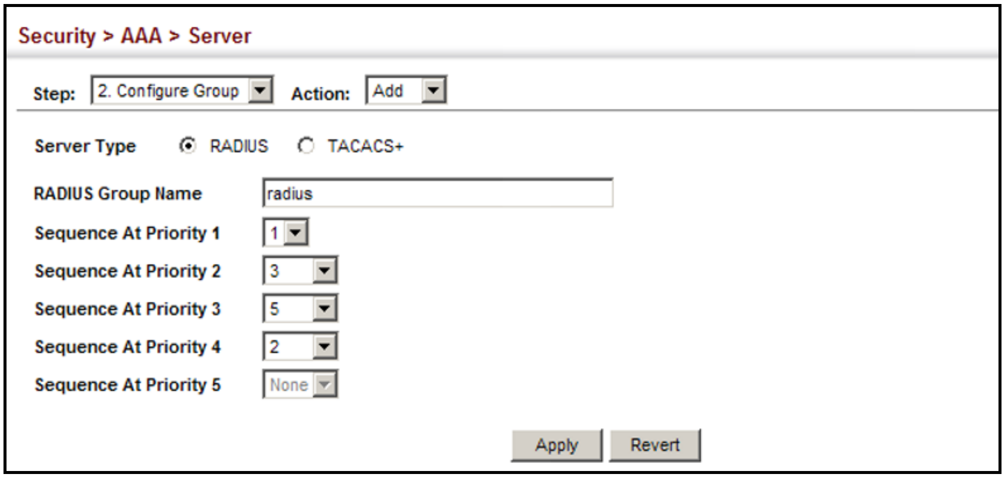
3. Select Add from the Action list.

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 122: 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

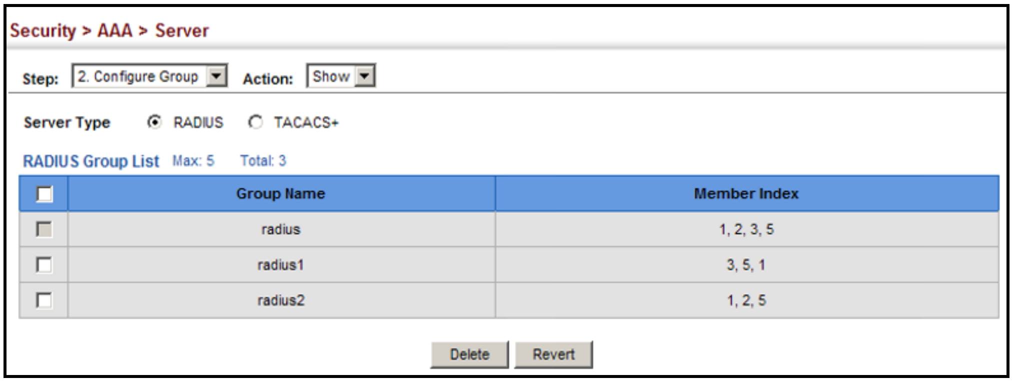
To show the RADIUS or TACACS+ server groups used for accounting and authorization:

1. Click Security, AAA, Server.

2. Select Configure Group from the Step list.

3. Select Show from the Action list.

Figure 123: Showing AAA Server Groups



Security > AAA > Server

Step: 2. Configure Group Action: Show

Server Type ● RADIUS ○ TACACS+

RADIUS Group List Max: 5 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 669

COMMAND USAGE

- AAA authentication through a RADIUS or TACACS+ server must be enabled before accounting is enabled.

PARAMETERS

These parameters are displayed in the web interface:

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: 0-2147483647 minutes; where 0 means disabled)

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: 1-255 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: 1-255 characters)

  The group names “radius” and “tacacs+” specifies all configured RADIUS and TACACS+ hosts (see "Configuring Local/Remote Logon Authentication" on page 247). 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: 1-255 characters)
  - **Exec**
    - **Console Method Name** – Specifies a user defined method name to apply to console connections.
    - **Telnet 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

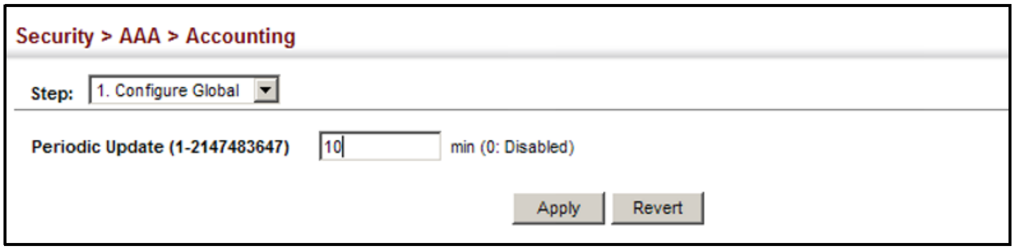
- **User Name** - Displays a registered user name.
- **Accounting Type** - Displays the accounting service.
- **Interface** - Displays the receive port number through which this user accessed the switch.
- **Time Elapsed** - Displays the length of time this entry has been active.

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 124: Configuring Global Settings for AAA Accounting



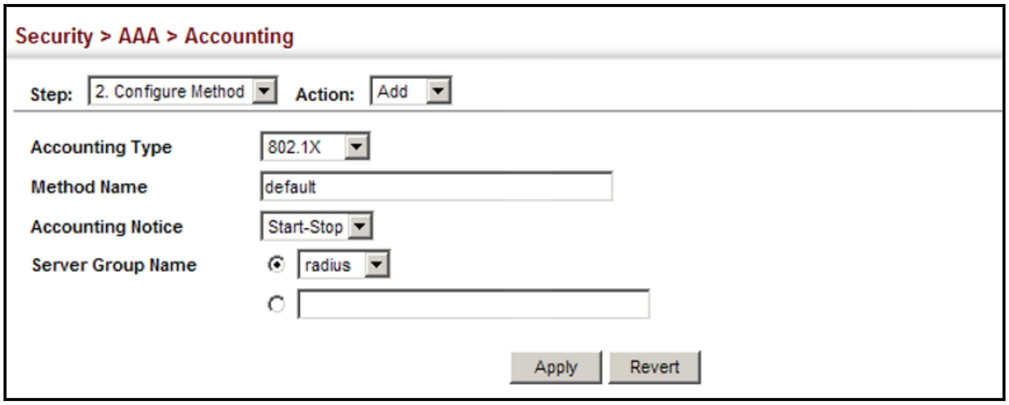
Step: 1. Configure Global

Periodic Update (1-2147483647) 10 min (0: Disabled)

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 125: Configuring AAA Accounting Methods



Step: 2. Configure Method Action: Add

Accounting Type 802.1X

Method Name default

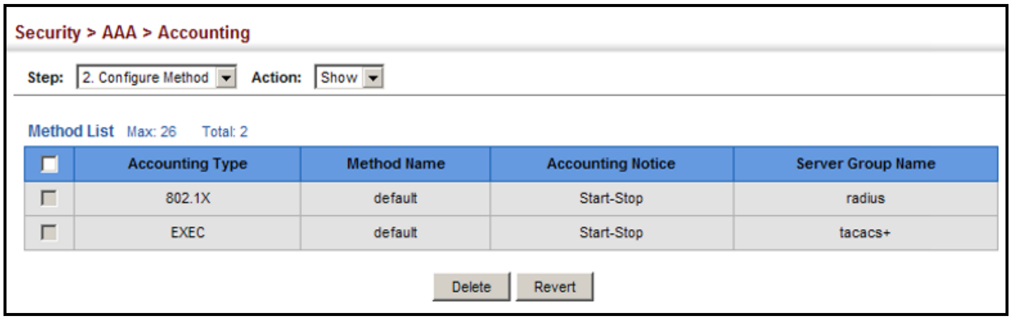
Accounting Notice Start-Stop

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 126: Showing AAA Accounting Methods



Security > AAA > Accounting

Step: 2. Configure Method Action: Show

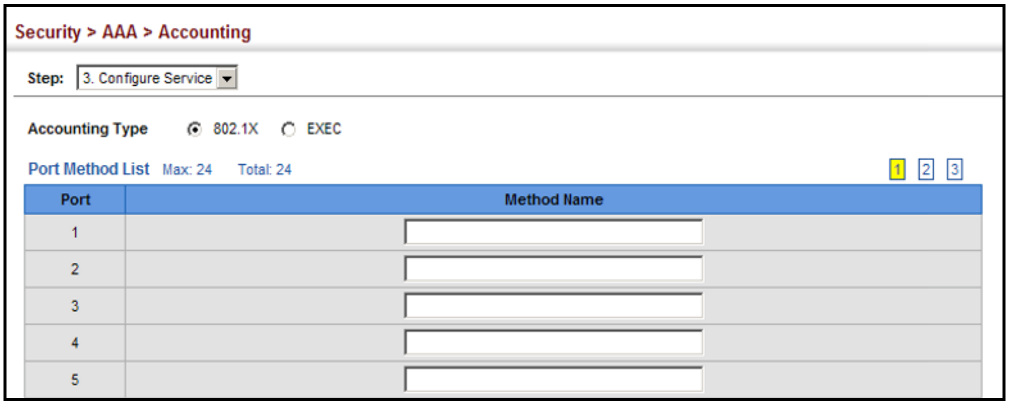
Method List Max: 26 Total: 2

□	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 127: Configuring AAA Accounting Service for 802.1X Service



Security > AAA > Accounting

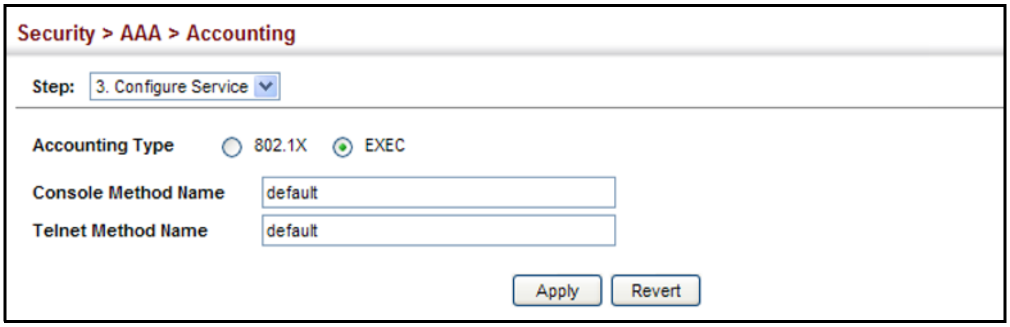
Step: 3. Configure Service

Accounting Type ● 802.1X ○ EXEC

Port Method List Max: 24 Total: 24

Port	Method Name
1	
2	
3	
4	
5	

Figure 128: Configuring AAA Accounting Service for Exec Service



Security > AAA > Accounting

Step: 3. Configure Service

Accounting Type ○ 802.1X ● EXEC

Console Method Name default

Telnet Method Name default

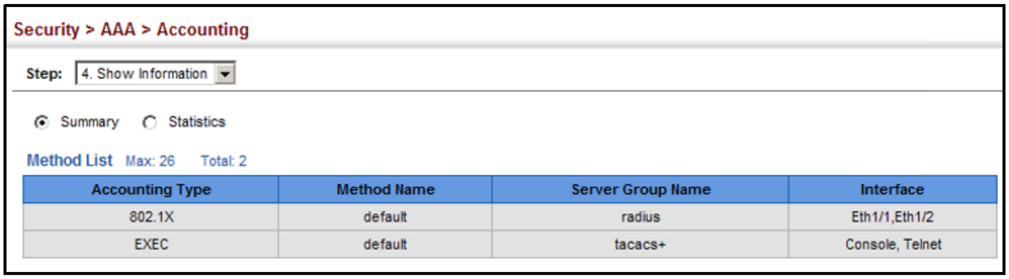
To display a summary of the configured accounting methods and assigned server groups for specified service types:

1. Click Security, AAA, Accounting.

2. Select Show Information from the Step list.

3. Click Summary.

Figure 129: Displaying a Summary of Applied AAA Accounting Methods



Security > AAA > Accounting

Step: 4. Show Information

● Summary ○ Statistics

Method List Max: 26 Total: 2

Accounting Type	Method Name	Server Group Name	Interface
802.1X	default	radius	Eth1/1,Eth1/2
EXEC	default	tacacs+	Console, Telnet

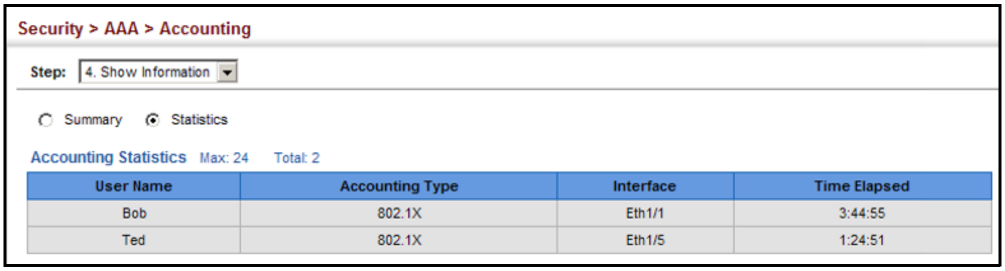
To display basic accounting information and statistics recorded for user sessions:

1. Click Security, AAA, Accounting.

2. Select Show Information from the Step list.

3. Click Statistics.

Figure 130: Displaying Statistics for AAA Accounting Sessions



Security > AAA > Accounting

Step: 4. Show Information

○ Summary ● Statistics

Accounting Statistics Max: 24 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 669

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 in the web interface:

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: 1-255 characters)
- **Server Group Name** - Specifies the authorization server group. (Range: 1-255 characters)

  The group name "tacacs+" specifies all configured TACACS+ hosts (see "Configuring Local/Remote Logon Authentication" on page 247). 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

- **Console Method Name** – Specifies a user defined method name to apply to console connections.
- **Telnet 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.

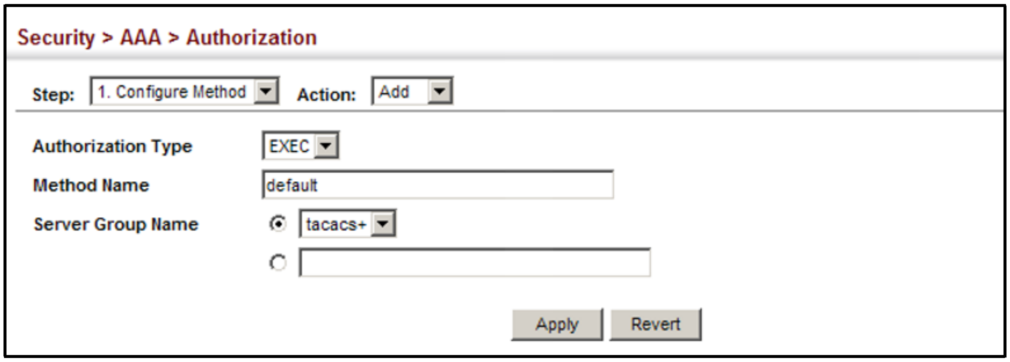
- **Interface** - Displays the console or Telnet interface to which these rules apply. (This field is null if the authorization method and associated server group has not been assigned to an interface.)

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 131: Configuring AAA Authorization Methods



Security > AAA > Authorization

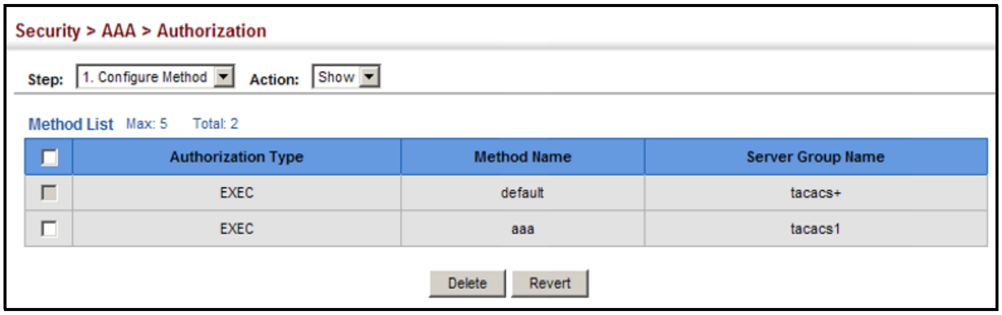
Step: 1. Configure Method Action: Add

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 132: Showing AAA Authorization Methods



Security > AAA > Authorization

Step: 1. Configure Method Action: Show

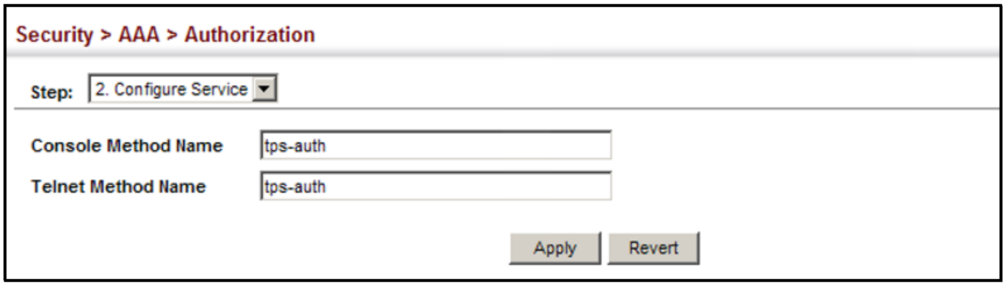
Method List Max: 5 Total: 2

□	Authorization Type	Method Name	Server Group Name
□	EXEC	default	tacacs+
□	EXEC	aaa	tacacs1

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 133: Configuring AAA Authorization Methods for Exec Service



Security > AAA > Authorization

Step: 2. Configure Service

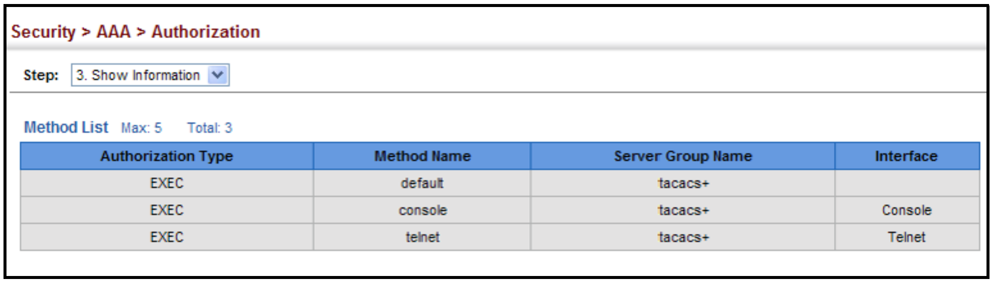
Console Method Name: tps-auth

Telnet 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 134: Displaying the Applied AAA Authorization Method



Security > AAA > Authorization

Step: 3. Show Information

Method List Max: 5 Total: 3

Authorization Type	Method Name	Server Group Name	Interface
EXEC	default	tacacs+	
EXEC	console	tacacs+	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 657

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 in the web interface:

- **User Name** – The name of the user.
  (Maximum length: 8 characters; maximum number of users: 16)

- **Access Level** – Specifies the user level. (Options: 0 - Normal, 15 - Privileged)

  Normal privilege level provides access to a limited number of the commands which display the current status of the switch, as well as several database clear and reset functions. Privileged level provides full access to all commands.

- **Password** – Specifies the user password.
  (Range: 0-8 characters plain text, 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:

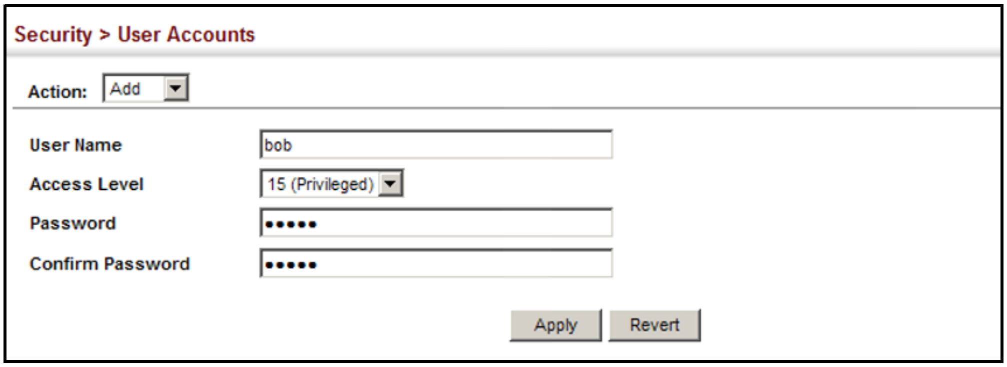
1. Click Security, User Accounts.

2. Select Add from the Action list.

3. Specify a user name, select the user's access level, then enter a password and confirm it.

4. Click Apply.

Figure 135: Configuring User Accounts



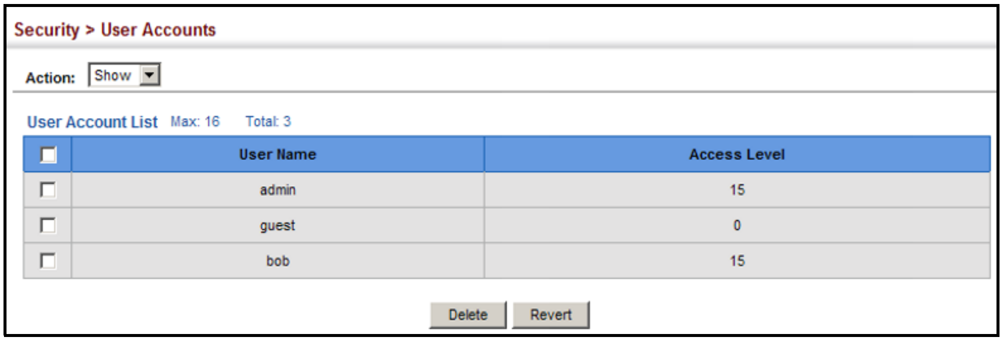
Action:	Add
User Name	bob
Access Level	15 (Privileged)
Password	•••••
Confirm Password	•••••

To show user accounts:

1. Click Security, User Accounts.

2. Select Show from the Action list.

Figure 136: Showing User Accounts



Action: Show

User Account List Max: 16 Total: 3

□	User Name	Access Level
□	admin	15
□	guest	0
□	bob	15

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 248.)

NOTE: MAC authentication cannot be configured on trunk ports.

CLI REFERENCES

◆ "Network Access (MAC Address Authentication)" on page 711

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 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 11: 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

- 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 711

PARAMETERS

These parameters are displayed in the web interface:

- **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 Authenticataion 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 316).

  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. (Default: 1800 seconds;
  Range: 120-1000000 seconds)

WEB INTERFACE

To configure aging status and reauthentication time for MAC address authentication:

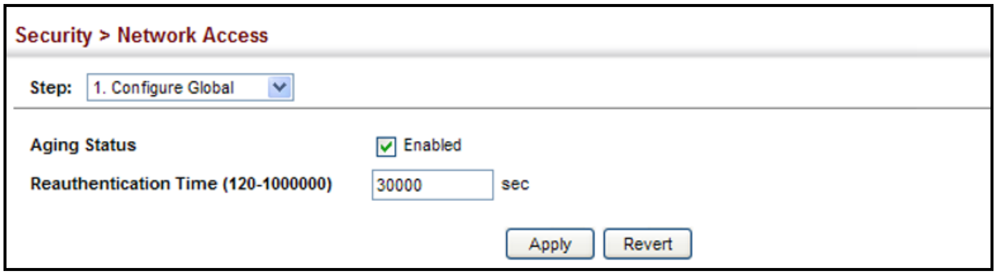
1. Click Security, Network Access.

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 137: 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 711

PARAMETERS

These parameters are displayed in the web interface:

◆ **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: 0-4093, where 0 means disabled; Default: Disabled)

The VLAN must already be created and active (see "Configuring VLAN Groups" on page 156). Also, when used with 802.1X authentication, intrusion action must be set for “Guest VLAN” (see "Configuring Port Settings for 802.1X" on page 316).

[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 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 are cleared from the secure MAC address table.

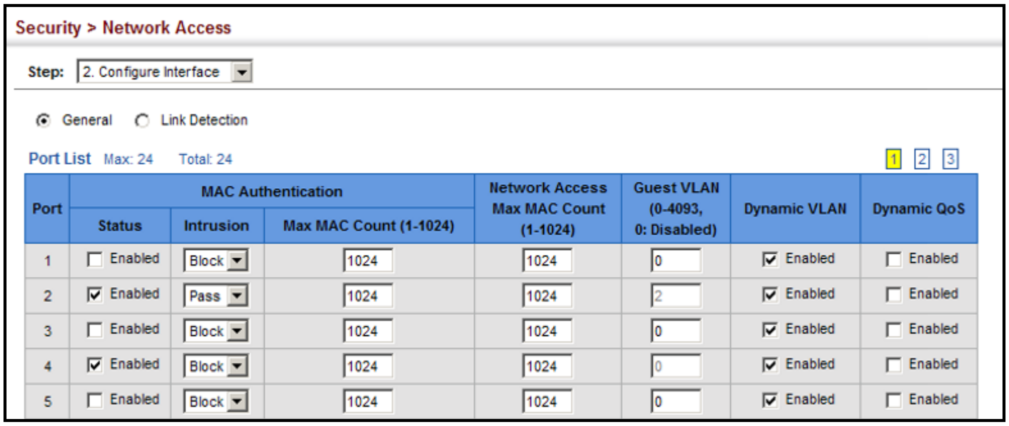
- **Dynamic QoS** – Enables dynamic QoS assignment for an authenticated port. (Default: Disabled)

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 138: Configuring Interface Settings for Network Access



Step: 2. Configure Interface

● General ○ Link Detection

Port List Max: 24 Total: 24

Port	MAC Authentication			Network Access Max MAC Count (1-1024)	Guest VLAN (0-4093, 0: Disabled)	Dynamic VLAN	Dynamic QoS
	Status	Intrusion	Max MAC Count (1-1024)				
1	□ Enabled	Block	1024	1024	0	☑ Enabled	□ Enabled
2	☑ Enabled	Pass	1024	1024	2	☑ 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 711

PARAMETERS

These parameters are displayed in the web interface:

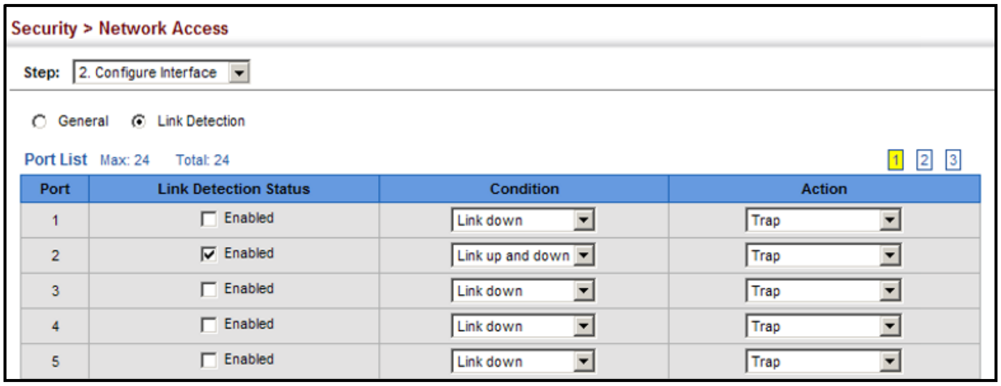
- **Link Detection Status** – Configures whether Link Detection is enabled or disabled for a port.
- **Condition** – The link event type which will trigger the port action.
  - **Link up** – Only link up events will trigger the port action.
  - **Link down** – Only link down events will trigger the port 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 139: Configuring Link Detection for Network Access



Security > Network Access

Step: 2. Configure Interface

○ General ● Link Detection

Port List Max: 24 Total: 24 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 > MAC Authentication (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 711

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 in the web interface:

- **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

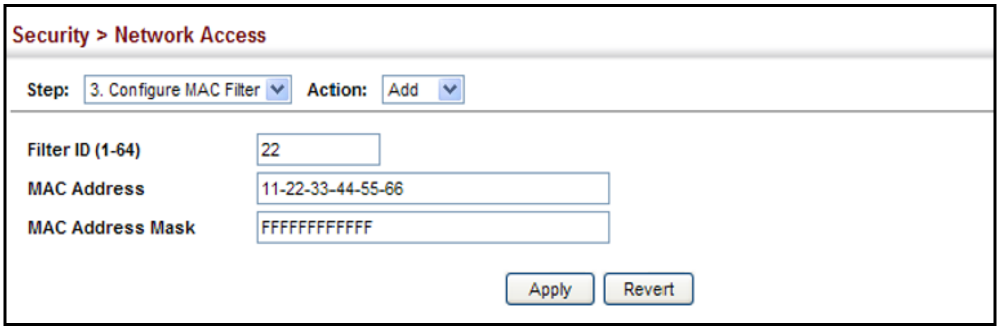
To add a MAC address filter for MAC authentication:

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 140: 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

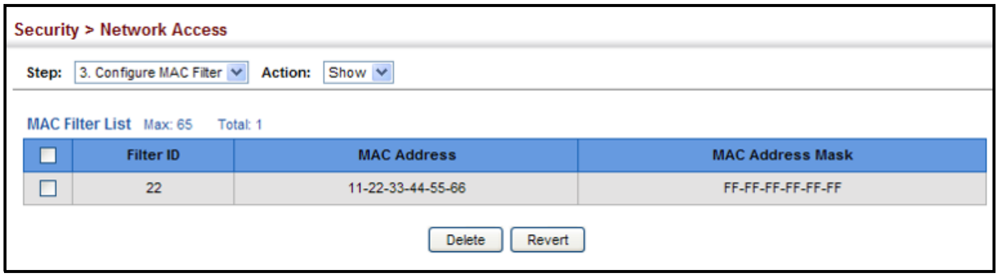
To show the MAC address filter table for MAC authentication:

1. Click Security, Network Access.

2. Select Configure MAC Filter from the Step list.

3. Select Show from the Action list.

Figure 141: Showing the MAC Address Filter Table for Network Access



Security > Network Access

Step: 3. Configure MAC Filter   Action: Show

MAC Filter List Max: 65 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 711

PARAMETERS

These parameters are displayed in the web interface:

- **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.

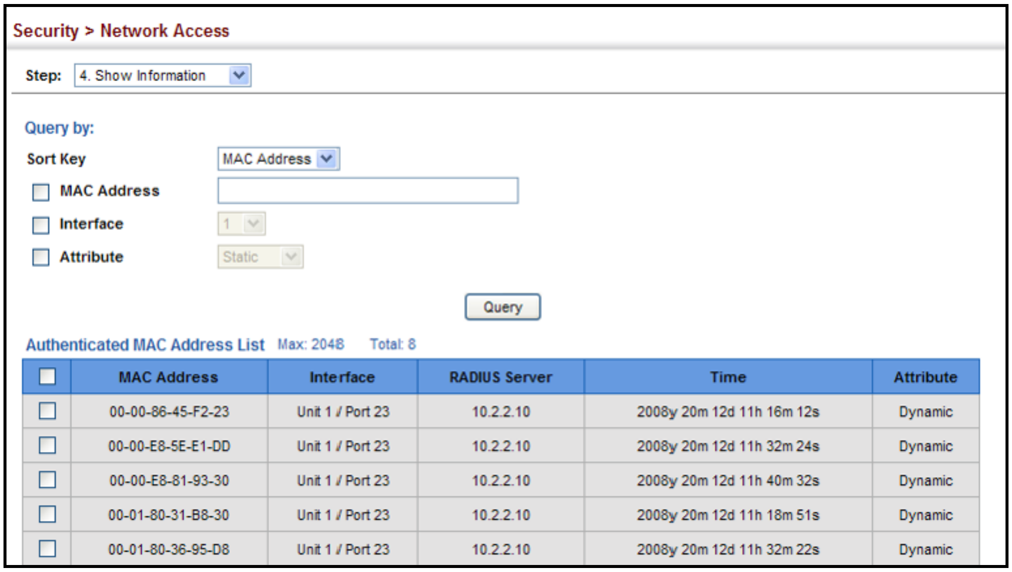
- **Authenticated MAC Address List**
  - **MAC Address** – The authenticated MAC address.
  - **Interface** – The port interface associated with a secure MAC address.
  - **RADIUS Server** – The IP address of the RADIUS server that authenticated the MAC address.
  - **Time** – The time when the MAC address 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 142: 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 Max: 2048 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 678

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 679.)

- 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 5.x or above, Netscape 6.2 or above, and Mozilla Firefox 2.0.0.0 or above.

- The following web browsers and operating systems currently support HTTPS:

Table 12: HTTPS System Support

Web Browser	Operating System
Internet Explorer 5.0 or later	Windows 98,Windows NT (with service pack 6a), Windows 2000, Windows XP, Windows 7
Netscape 6.2 or later	Windows 98,Windows NT (with service pack 6a), Windows 2000, Windows XP, Solaris 2.6
Mozilla Firefox 2.0.0.0 or later	Windows 2000, Windows XP, Linux

- To specify a secure-site certificate, see "Replacing the Default Secure-site Certificate" on page 274.

PARAMETERS

These parameters are displayed in the web interface:

- **HTTPS Status** – Allows you to enable/disable the HTTPS server feature on the switch. (Default: Enabled)

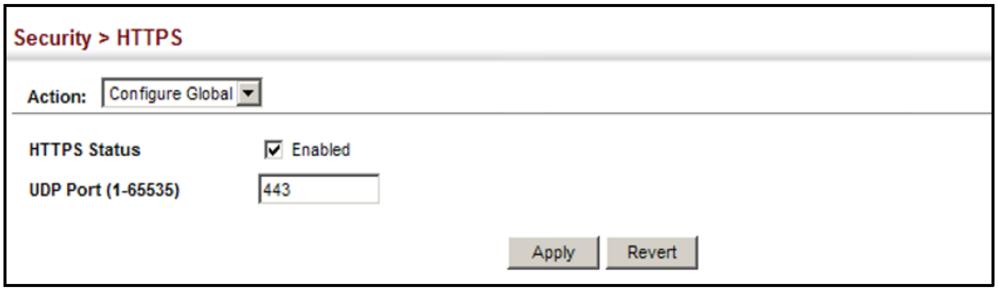
- **HTTPS Port** – Specifies the UDP port number used for HTTPS connection to the switch's web interface. (Default: Port 443)

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 143: 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 Netscape and Internet Explorer display 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 120 or type “reload” at the commad prompt: ES-3026#`reload`

CLI REFERENCES

- "Web Server" on page 678

PARAMETERS

These parameters are displayed in the web interface:

- **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:

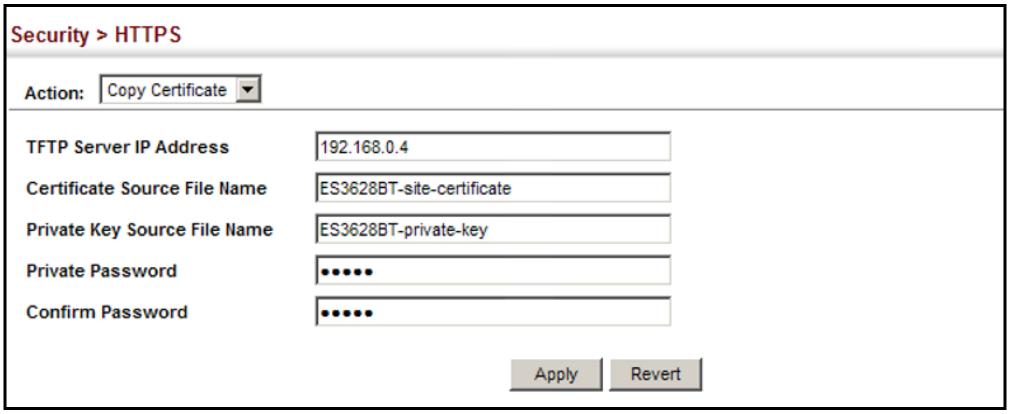
1. Click Security, HTTPS.

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 144: Downloading the Secure-Site Certificate



Security > HTTPS

Action: Copy Certificate

TFTP Server IP Address: 192.168.0.4

Certificate Source File Name: ES3628BT-site-certificate

Private Key Source File Name: ES3628BT-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.

The 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 247). 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 281, or use the copy tftp public-key command (page 595) 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 261.) 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
   13410816856098939210409449201554253476316419218729589211431738
   80055536161631051775940838686311092912322268285192543746031009
   37187721199696317813662774141689851320491172048303392543241016
   37997592371449011938006090253948408482717819437228840253311595
   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 279.

CLI REFERENCES

- "Secure Shell" on page 684

PARAMETERS

These parameters are displayed in the web interface:

- **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.

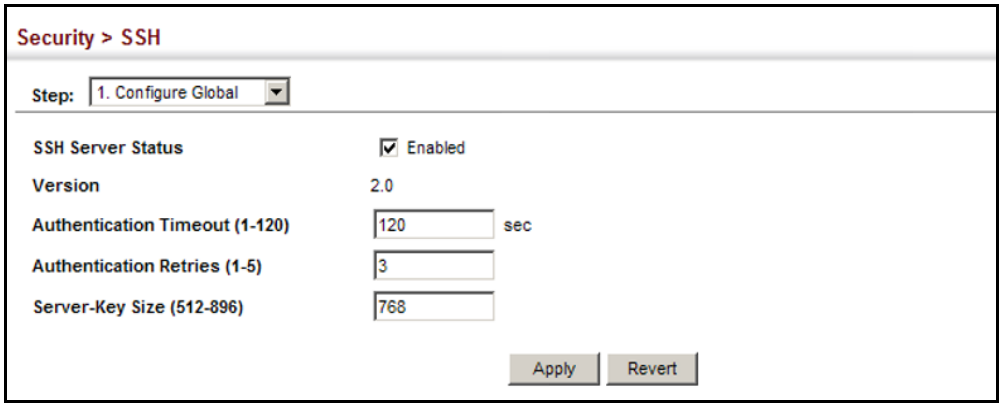
  - The host key is shared with the SSH client, and is fixed at 1024 bits.

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 145: 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 281.

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 278.

CLI REFERENCES

- "Secure Shell" on page 684

PARAMETERS

These parameters are displayed in the web interface:

- **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.

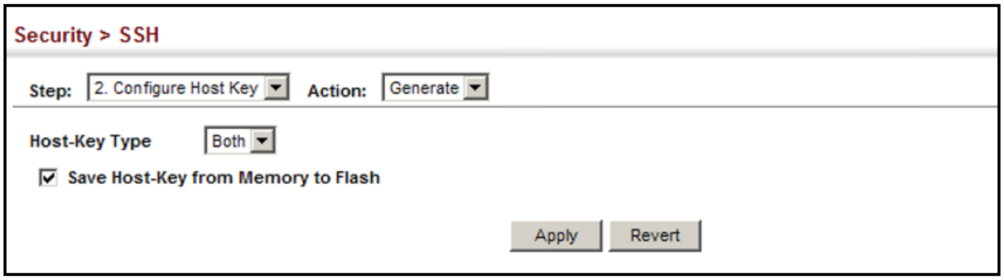
- **Save Host-Key from Memory to Flash** – Saves the host key from RAM (i.e., volatile memory) to flash memory. Otherwise, the host key pair is stored to RAM by default. Note that you must select this item prior to generating the host-key pair. (Default: Disabled)

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 146: Generating the SSH Host Key Pair



Security > SSH

Step: 2. Configure Host Key   Action: Generate

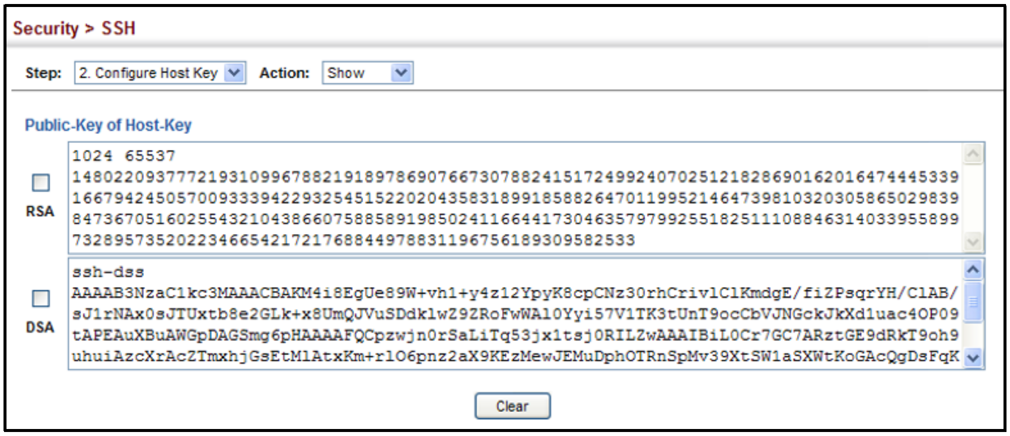
Host-Key Type: Both

☑ 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 Show.

Figure 147: Showing the SSH Host Key Pair



Step: 2. Configure Host Key Action: Show

□ RSA

```
1024 65537
1480220937772193109967882191897869076673078824151724992407025121828690162016474445339
1667942450570093339422932545152202043583189918588264701199521464739810320305865029839
8473670516025543210438660758858919850241166441730463579799255182511108846314033955899
7328957352022346654217217688449788311967561893095825 33
```

□ DSA

```
ssh-dss
AAAAB3NzaC1kc3MAAACBAKM4i8EgUe89W+vh1+y4z12YpyK8cpCNz30rhCrivlClKmdgE/fiZPsqrYH/C1AB/
sJ1rNAx0sJTUxtb8e2GLk+x8UmQJVuSDdklwZ9ZRoFwWA10Yyi57V1TK3tUnT9ocCbVJNGckJkXd1uac4OP09
tAPEAuXBuAWGpDAGSmg6pHAAAAFQCpzwjn0rSaLiTq53jx1tsj0RILZwAAAIBiL0Cr7GC7ARztGE9dRkT9oh9
uhuiAzcXrAcZTmxhjGsEtMlAtxKm+rlO6pnz2aX9KEzMewJEMuDphOTRnSpMv39XtSW1aSXWtKoGAcQgDsFqK
```

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 684

PARAMETERS

These parameters are displayed in the web interface:

- **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 261).
- **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.

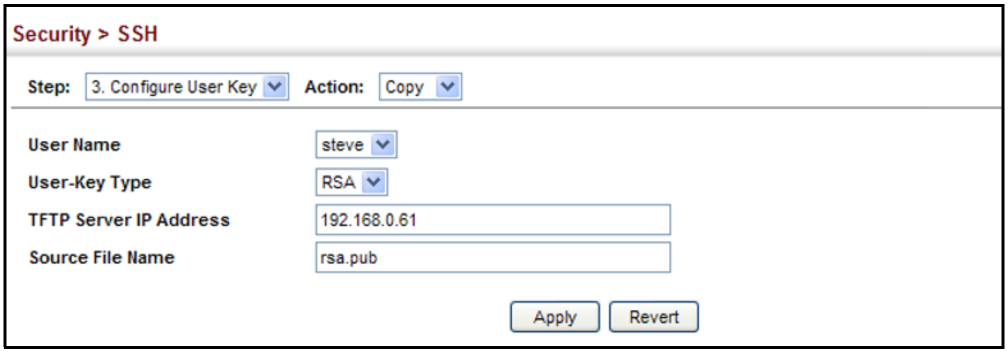
  The switch uses only RSA Version 1 for SSHv1.5 clients and DSA Version 2 for SSHv2 clients.
- **TFTP Server IP Address** – The IP address of the TFTP server that contains the public key file you wish to import.
- **Source File Name** – The public key file to upload.

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 148: Copying the SSH User's Public Key



Security > SSH

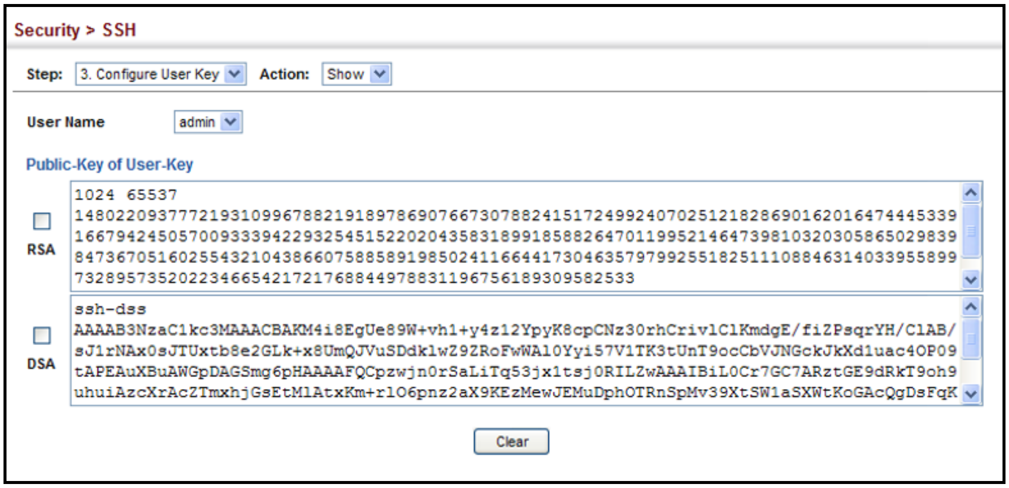
Step: 3. Configure User Key Action: Copy

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 149: Showing the SSH User's Public Key



User Name: admin

Public-Key of User-Key

□ RSA

```
1024 65537
1480220937772193109967882191897869076673078824151724992407025121828690162016474445339
1667942450570093339422932545152202043583189918588264701199521464739810320305865029839
8473670516025543210438660758858919850241166441730463579799255182511108846314033955899
732895735202234665421721768844978831196756189309582533
```

□ DSA

```
ssh-dss
AAAAB3NzaC1kc3MAAACBAKM4i8EgUe89W+vh1+y4z12YpyK8cpCNz30rhCrivlClKmdgE/fiZPsqrYH/ClAB/
sJ1rNAx0sJTUxtb8e2GLk+x8UmQJVuSDdklwZ9ZRoFwWAl0Yyi57V1TK3tUnT9ocCbVJNGckJkXd1uac4OP09
tAPEAuXBuAWGpDAGSmg6pHAAAAFQCpzwjn0rSaLiTq53jx1tsj0RILZwAAAIBiL0Cr7GC7ARztGE9dRkT9oh9
uhuiAzcXrAcZTmxhjGsEtMlAtxKm+rlO6pnz2aX9KEzMewJEMuDphOTRnSpMv39XtSW1aSXWtKoGAcQgDsFqK
```

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, 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 per port is 36.
- The maximum number of rules per port is also 93.

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 625

PARAMETERS

These parameters are displayed in the web interface:

Add

- **Time-Range Name** – Name of a time range. (Range: 1-30 characters)

Add Rule

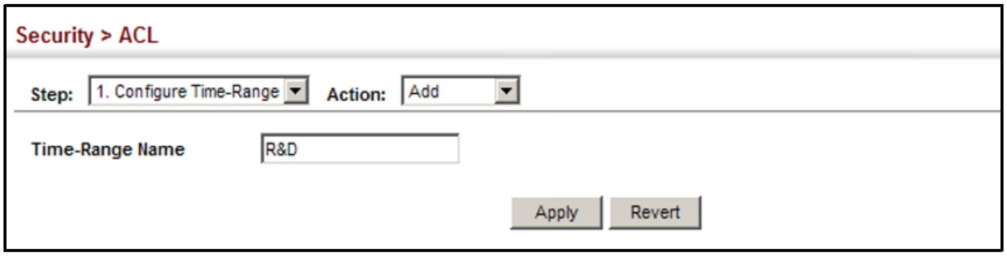
- **Time-Range** – Name of a time range.
- **Mode**
  - **Absolute** – Specifies a specific time or time range.
    - **Start**/**End** – Specifies the hours, minutes, month, day, and year at which to start or end.
  - **Periodic** – Specifies a periodic interval.
    - **Start**/**To** – Specifies the 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 150: Setting the Name of a Time Range



Security > ACL

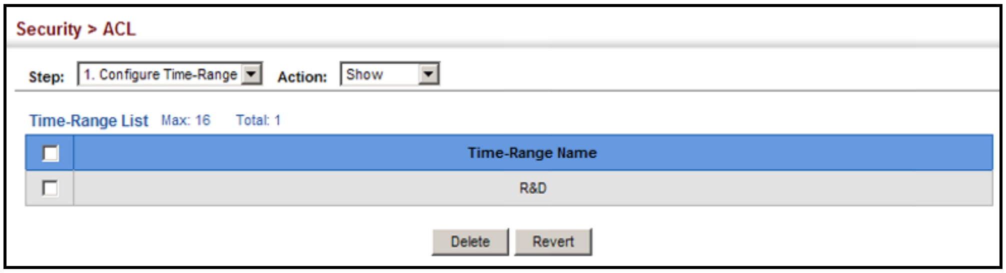
Step: 1. Configure Time-Range Action: Add

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 151: Showing a List of Time Ranges



Security > ACL

Step: 1. Configure Time-Range Action: Show

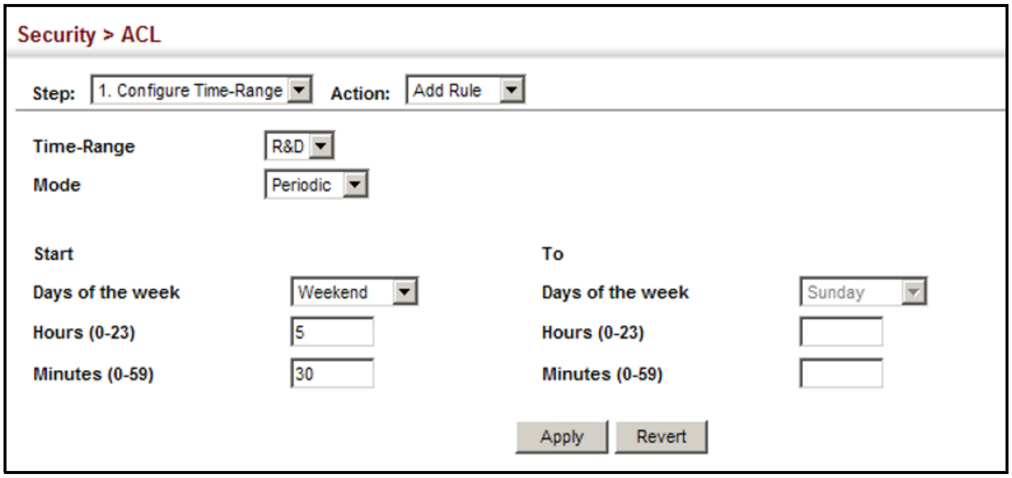
Time-Range List Max: 16 Total: 1

□	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 152: Add a Rule to a Time Range



Security > ACL

Step: 1. Configure Time-Range Action: Add Rule

Time-Range: R&D

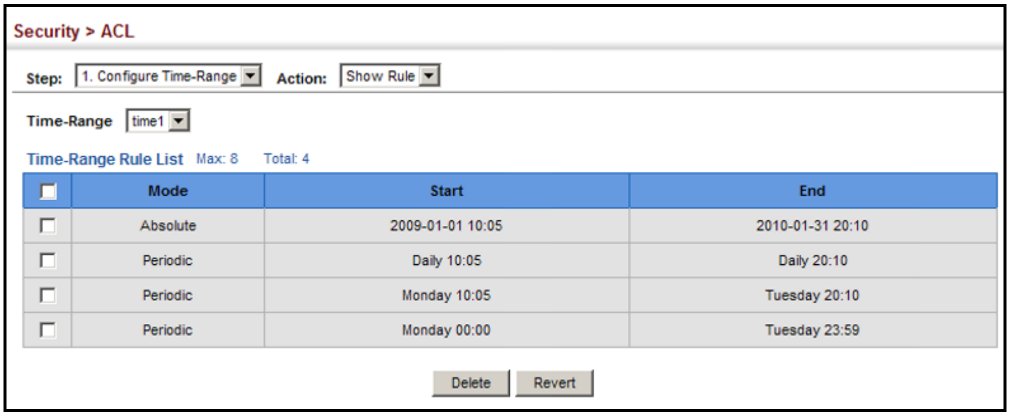
Mode: Periodic

Start		To	
Days of the week	Weekend	Days of the week	Sunday
Hours (0-23)	5	Hours (0-23)	
Minutes (0-59)	30	Minutes (0-59)	

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 153: 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 Max: 8 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

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 748
- "show ip access-list" on page 753

PARAMETERS

These parameters are displayed in the web interface:

- **ACL Name** – Name of the ACL. (Maximum length: 15 characters)

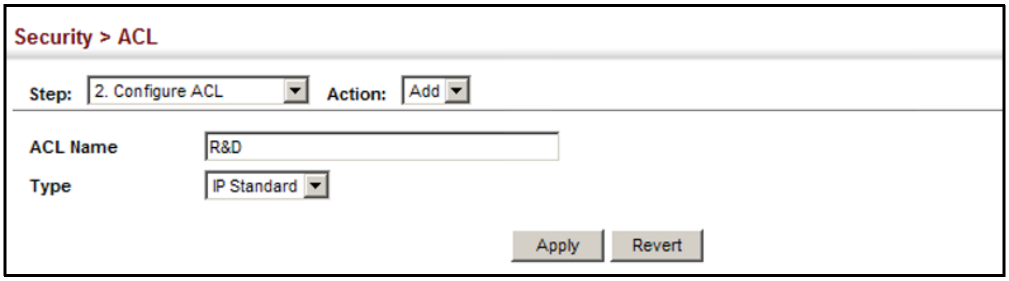
- **Type** – The following filter modes are supported:
  - **IP Standard**: IPv4 ACL mode filters packets based on the source IPv4 address.
  - **IP Extended**: IPv4 ACL mode filters packets based on the source or destination IPv4 address, as well as the protocol type and protocol port number. If the “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 the type of the next header 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 301).

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 154: Creating an ACL



Security > ACL

Step: 2. Configure ACL Action: Add

ACL Name: R&D

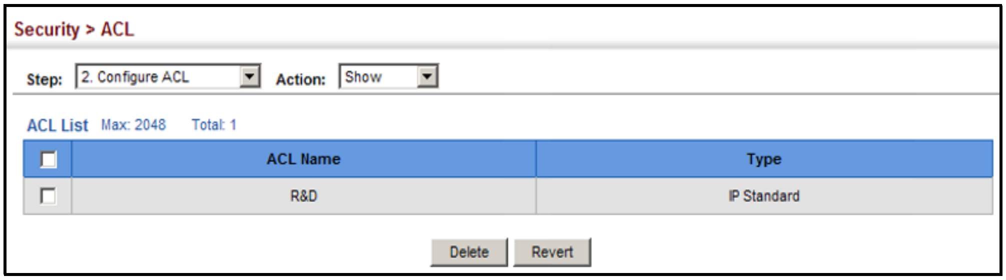
Type: IP Standard

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 155: Showing a List of ACLs



Security > ACL

Step: 2. Configure ACL Action: Show

ACL List Max: 2048 Total: 1

□	ACL Name	Type
□	R&D	IP Standard

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 749
- "show ip access-list" on page 753
- "Time Range" on page 625

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.
- **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.

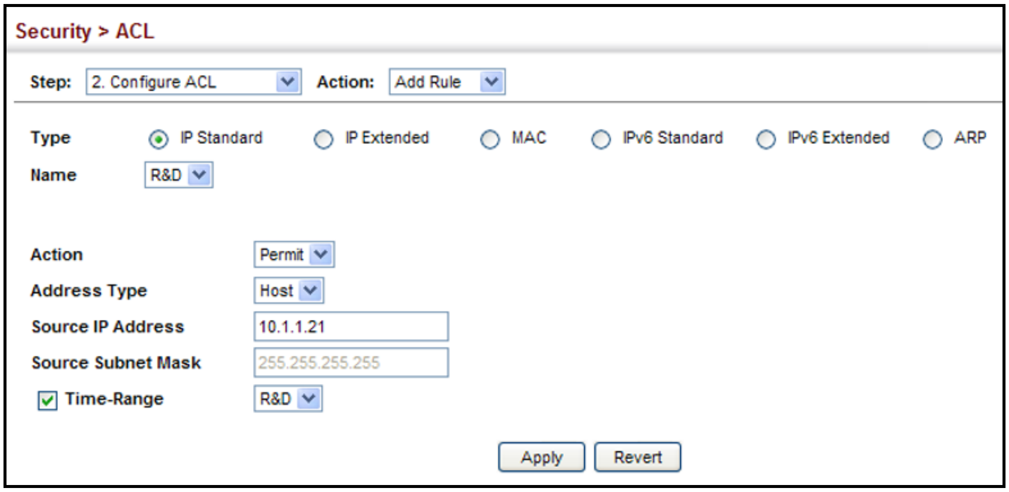
6. Specify the action (i.e., Permit or Deny).

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 156: 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 750
- "show ip access-list" on page 753
- "Time Range" on page 625

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/Destination Address Type** – Specifies the source or destination 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/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 288.)

- **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: TCP)

- **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 Extended 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 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).

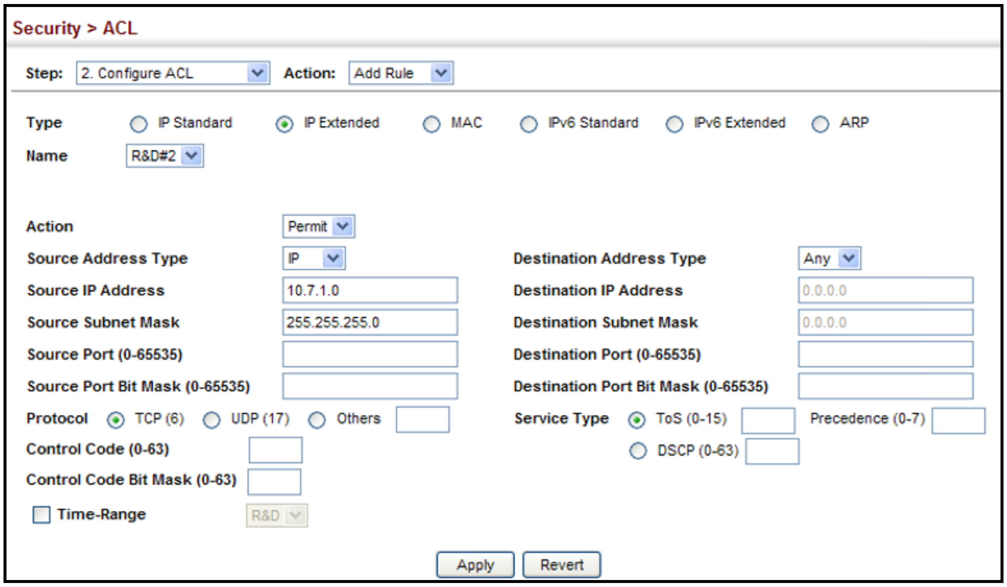
7. Select the address type (Any, Host, or IP).

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 157: 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 R&D#2

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 755
- "show ipv6 access-list" on page 758
- "Time Range" on page 625

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).
- **Time Range** – Name of a time range.

WEB INTERFACE

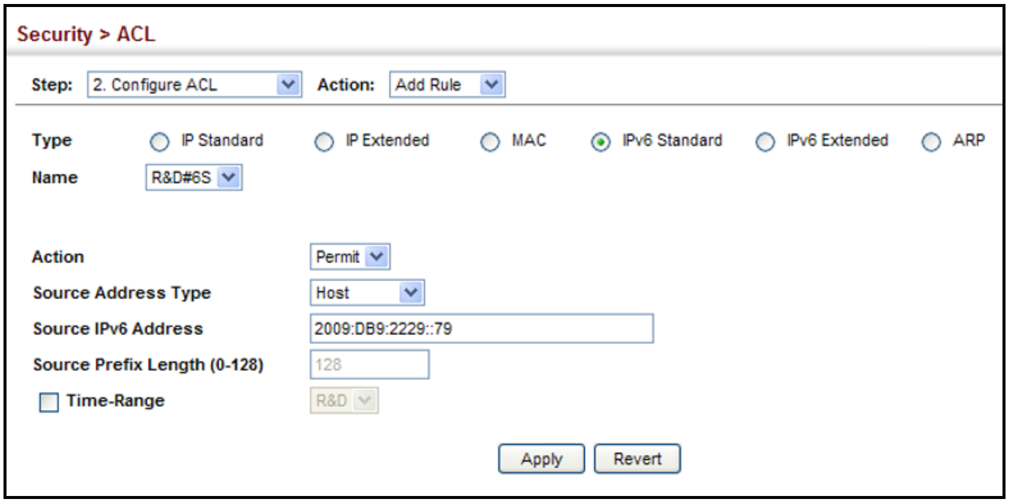
To add rules to a Standard IPv6 ACL:

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 158: 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 756
- "show ipv6 access-list" on page 758
- "Time Range" on page 625

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. 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. (The switch only checks the first 64 bits of the destination address.)

- **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.

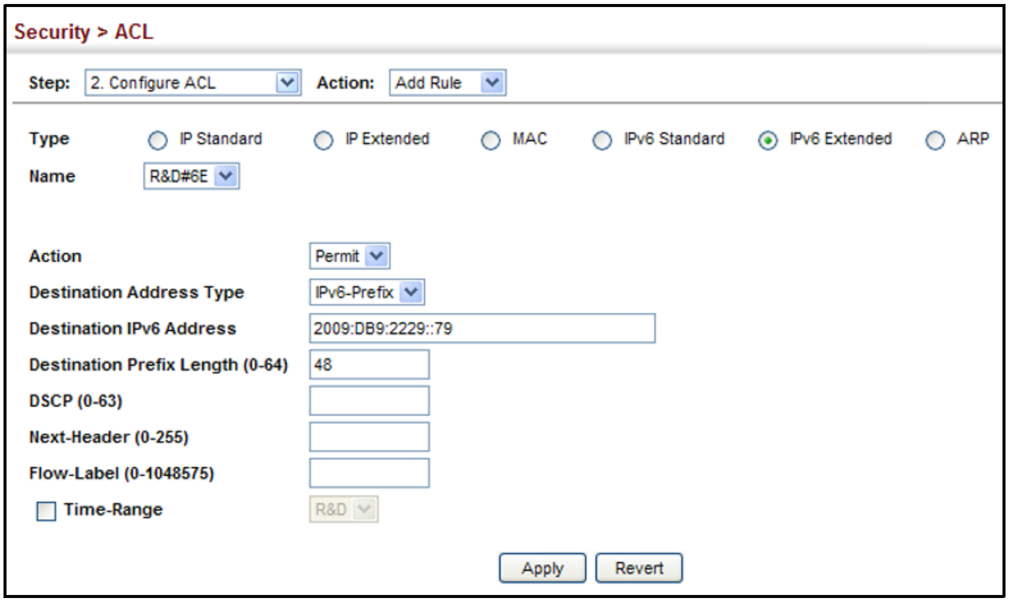
  Hosts or routers that do not support the functions specified by the flow label must set the field to zero when originating a packet, pass the field on unchanged when forwarding a packet, and ignore the field when receiving a packet.

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, or flow label.
10. Click Apply.

Figure 159: 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 R&D#6E

Action	Permit
Destination Address Type	IPv6-Prefix
Destination IPv6 Address	2009:DB9:2229::79
Destination Prefix Length (0-64)	48
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 761
- "show ip access-list" on page 753
- "Time Range" on page 625

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/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: 1-4095)
- **VID Bit Mask** – VLAN bit mask. (Range: 0-4095)
- **Ethernet Type** – This option can only be used to filter Ethernet II formatted packets. (Range: 600-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: 600-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).

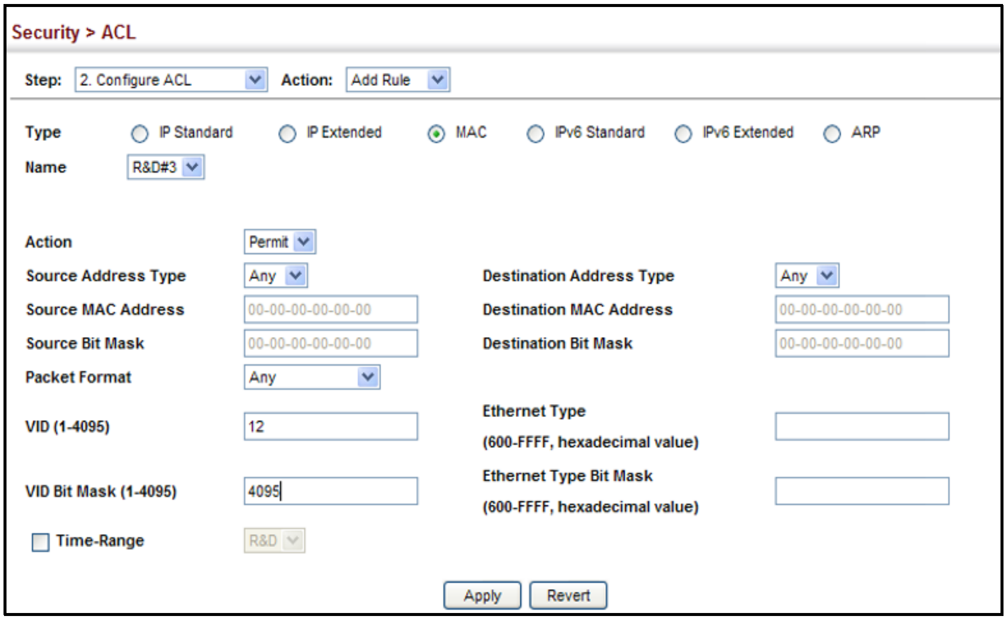
7. Select the address type (Any, Host, or MAC).

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 160: 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 R&D#3

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 (1-4095)	12	Ethernet Type (600-FFFF, hexadecimal value)	
VID Bit Mask (1-4095)	4095	Ethernet Type Bit Mask (600-FFFF, hexadecimal value)	
□ Time-Range	R&D		

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 302).

CLI REFERENCES

- "permit, deny (ARP ACL)" on page 766
- "show ip access-list" on page 753
- "Time Range" on page 625

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.
- **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 288.)
- **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.

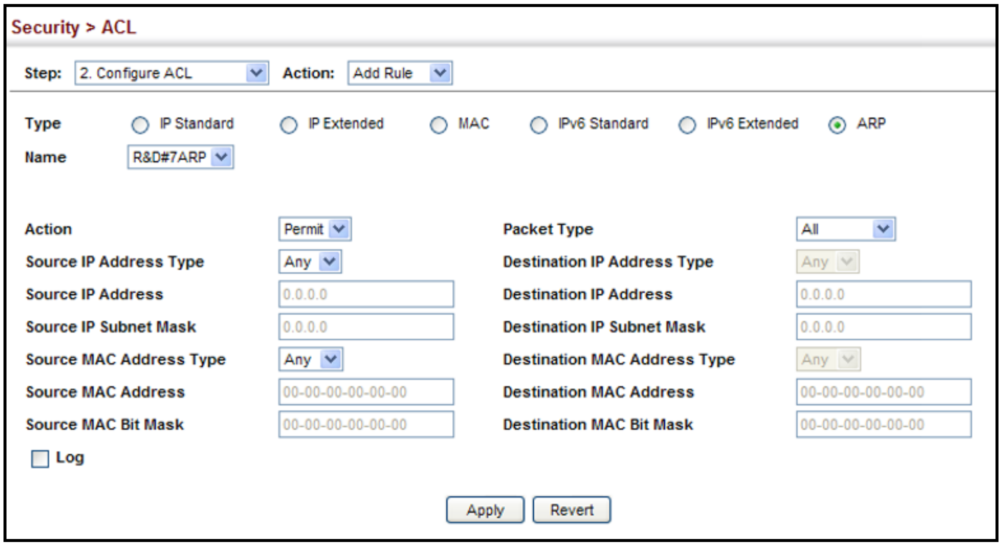
WEB INTERFACE

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 161: 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 752
- "ipv6 access-group" on page 759
- "show ip access-group" on page 753
- "show ipv6 access-group" on page 759
- "mac access-group" on page 763
- "show mac access-group" on page 764
- "Time Range" on page 625

COMMAND USAGE

- This switch supports ACLs for ingress filtering only.
- You only bind one ACL to any port for ingress filtering.

PARAMETERS

These parameters are displayed in the web interface:

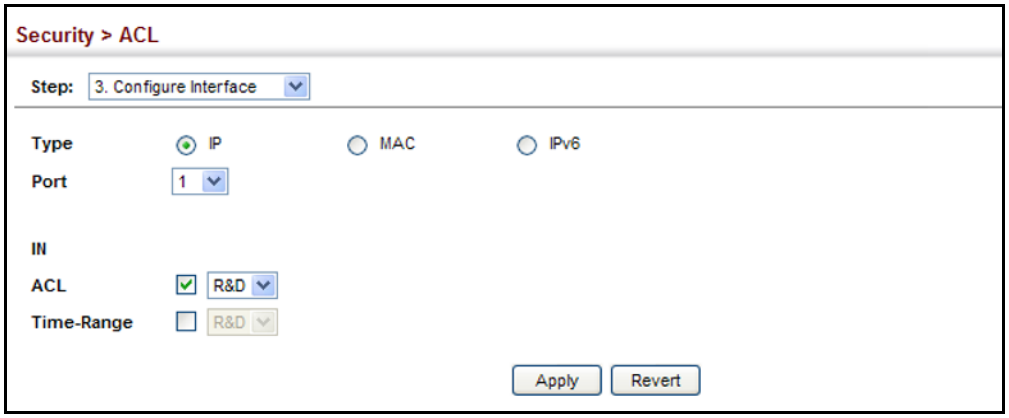
- **Type** – Selects the type of ACLs to bind to a port.
- **Port** – Port identifier
- **ACL** – ACL used for ingress packets.
- **Time Range** – Name of a time range.

WEB INTERFACE

To bind an ACL to a port:

1. Click Security, ACL.
2. Select Configure Interface from the Step list.
3. Select IP or MAC from the Type list.
4. Select the name of an ACL from the ACL list.
5. Click Apply.

Figure 162: Binding a Port to an ACL



Security > ACL

Step: 3. Configure Interface

Type ● IP ○ MAC ○ IPv6

Port 1

IN

ACL ☑ R&D

Time-Range □ R&D

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 329). 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 298).

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 738

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 in the web interface:

- **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.
  - **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:

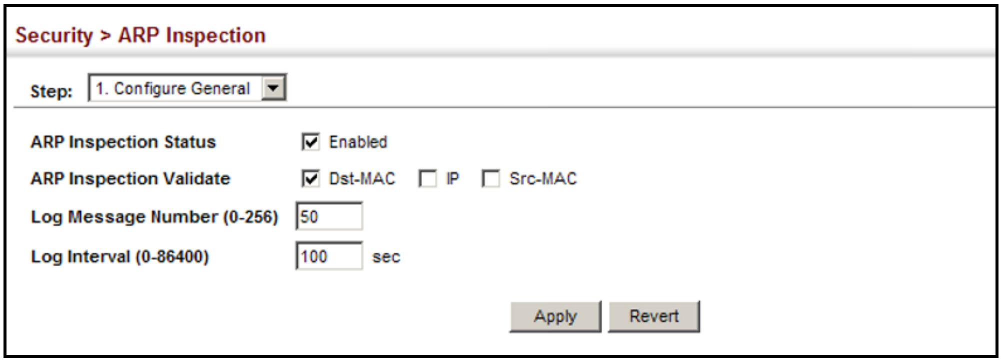
1. Click Security, ARP Inspection.

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 163: Configuring Global Settings for ARP Inspection



Security > ARP Inspection

Step: 1. Configure General

ARP Inspection Status ☑ Enabled

ARP Inspection Validate ☑ Dst-MAC □ IP □ Src-MAC

Log Message Number (0-256) 50

Log Interval (0-86400) 100 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 738

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 298).

- 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 in the web interface:

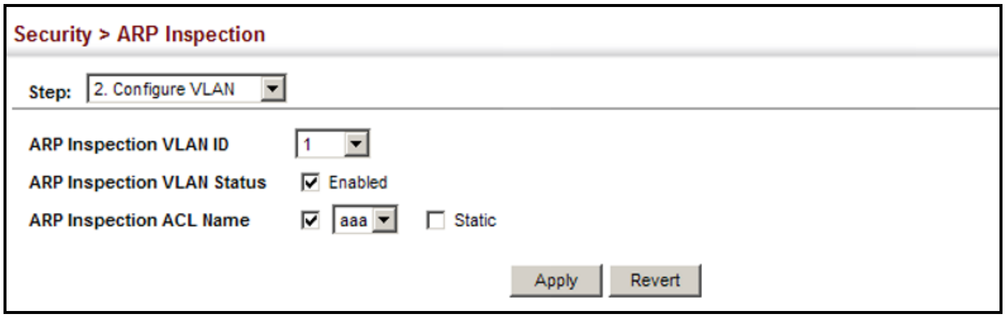
- **ARP Inspection VLAN ID** – Selects any configured VLAN. (Default: 1)
- **ARP Inspection VLAN Status** – Enables ARP Inspection for the selected VLAN. (Default: Disabled)
- **ARP Inspection ACL Name**
  - *ARP ACL* – Allows selection of any configured ARP ACLs. (Default: None)
  - **Static** – When 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 164: 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 738

PARAMETERS

These parameters are displayed in the web interface:

- **Port** – Port 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:

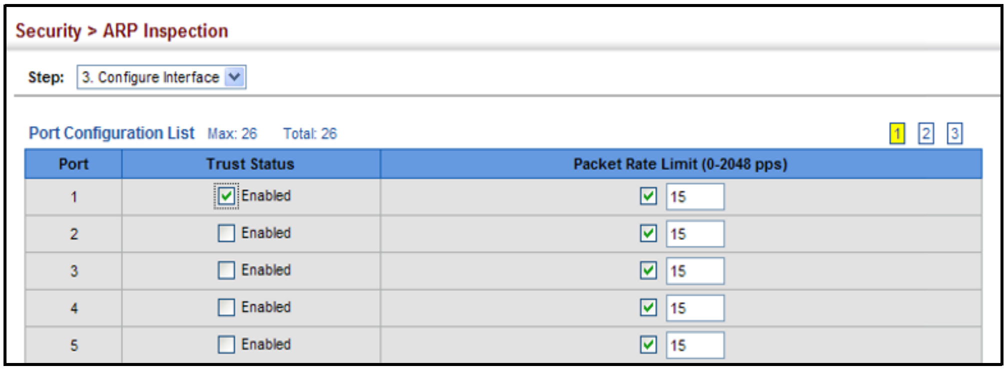
1. Click Security, ARP Inspection.

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 165: Configuring Interface Settings for ARP Inspection



Security > ARP Inspection

Step: 3. Configure Interface

Port Configuration List Max: 26 Total: 26

1 2 3

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 746

PARAMETERS

These parameters are displayed in the web interface:

Table 13: 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.
ARP packets dropped by additional validation (IP)	Count of ARP packets that failed the IP address test.
ARP packets dropped by additional validation (Dst-MAC)	Count of packets that failed the destination MAC address test.
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 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

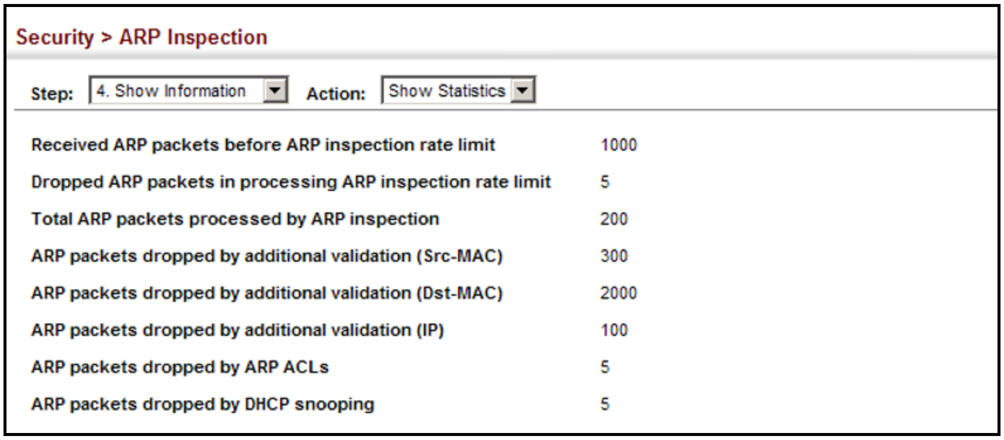
To display statistics for ARP Inspection:

1. Click Security, ARP Inspection.

2. Select Configure Information from the Step list.

3. Select Show Statistics from the Step list.

Figure 166: 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 745

PARAMETERS

These parameters are displayed in the web interface:

Table 14: ARP Inspection Log

Parameter	Description
VLAN ID	The VLAN where this packet was seen.
Port	The port where this packet was seen.
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

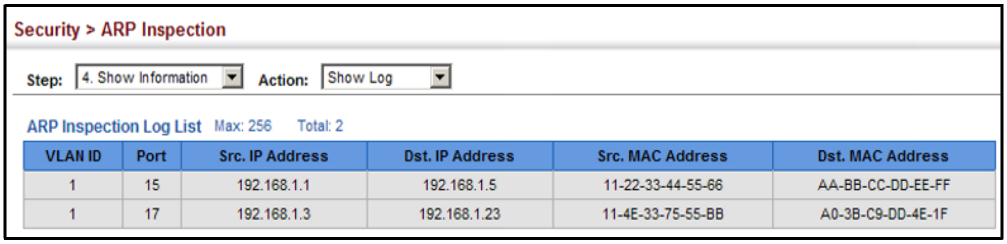
To display the ARP Inspection log:

1. Click Security, ARP Inspection.

2. Select Configure Information from the Step list.

3. Select Show Log from the Step list.

Figure 167: Displaying the ARP Inspection Log



Step: 4. Show Information Action: Show Log

ARP Inspection Log List Max: 256 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 704

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 in the web interface:

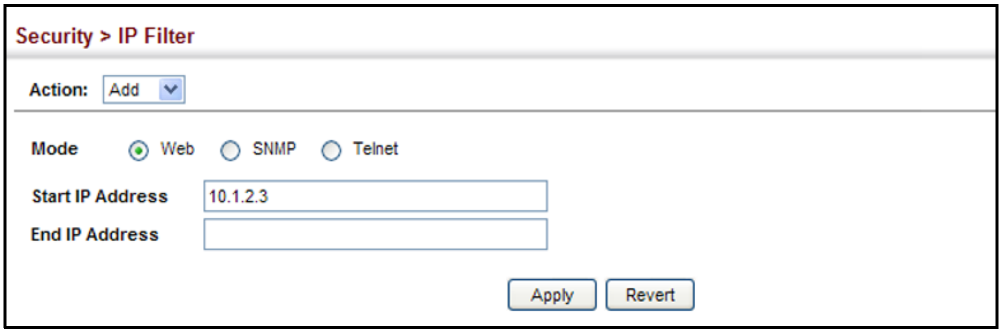
- **Mode**
  - **Web** – Configures IP address(es) for the web group.
  - **SNMP** – Configures IP address(es) for the SNMP group.
  - **Telnet** – Configures IP address(es) for the Telnet group.
- **Start IP Address** – A single IP address, or the starting address of a range.
- **End IP Address** – 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 168: Creating an IP Address Filter for Management Access



Security > IP Filter

Action: Add

Mode ● Web ○ SNMP ○ Telnet

Start IP Address: 10.1.2.3

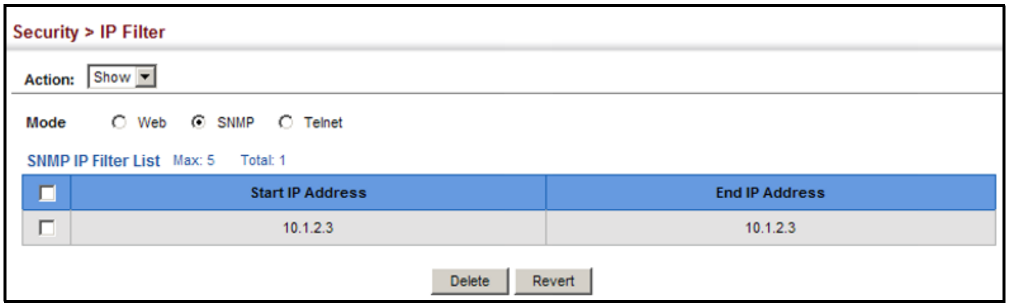
End IP Address:

To show a list of IP addresses authorized for management access:

1. Click Security, IP Filter.

2. Select Show from the Action list.

Figure 169: Showing IP Addresses Authorized for Management Access



Security > IP Filter

Action: Show

Mode ○ Web ● SNMP ○ Telnet

SNMP IP Filter List Max: 5 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 a switch port with one or more device MAC addresses that are authorized to access the network through that port.

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 dynamic or static 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.

To use port security, specify a maximum number of addresses to allow on the port and then let the switch dynamically learn the <source MAC address, VLAN> pair for frames received on the port. Note that you can also manually add secure addresses to the port using the Static Address Table (page 189). When the port has reached the maximum number of MAC addresses, the selected port will stop learning. The MAC addresses already in the address table will be retained and will not age out. Any other device that attempts to use the port will be prevented from accessing the switch.

CLI REFERENCES

- "Port Security" on page 708

COMMAND USAGE

- 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.
- The default maximum number of MAC addresses allowed on a secure port is zero. You must configure a maximum address count from 1-1024 for the port to allow access.
- 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 125).

PARAMETERS

These parameters are displayed in the web interface:

- **Port** – Port number.
- **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.
- **Security Status** – Enables or disables port security on the port. (Default: Disabled)
- **Max MAC Count** – The maximum number of MAC addresses that can be learned on a port. (Range: 0-1024, where 0 means disabled)

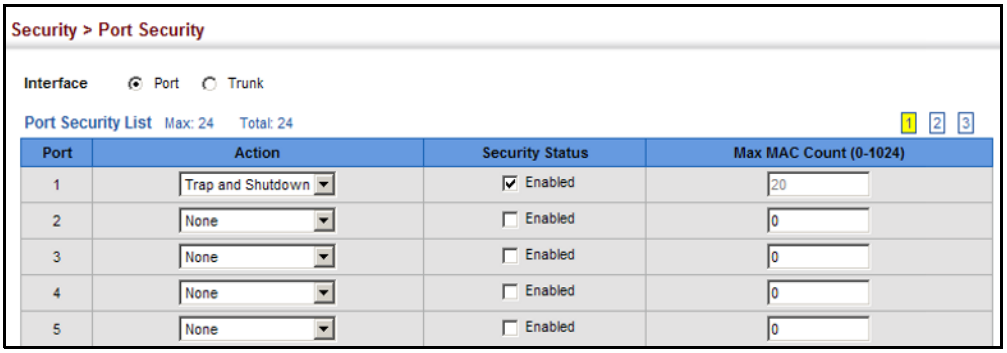
  The maximum address count is effective when port security is enabled or disabled, but can only be set when Security Status is disabled.

WEB INTERFACE

To configure port security:

1. Click Security, Port Security.
2. Set the action to take when an invalid address is detected on a port, mark the check box in the Security Status column to enable security for a port, and set the maximum number of MAC addresses allowed on a port.
3. Click Apply

Figure 170: Configuring Port Security



Security > Port Security

Interface ● Port ○ Trunk

Port Security List Max: 24 Total: 24

Port	Action	Security Status	Max MAC Count (0-1024)
1	Trap and Shutdown	☑ Enabled	20
2	None	□ Enabled	0
3	None	□ Enabled	0
4	None	□ Enabled	0
5	None	□ Enabled	0

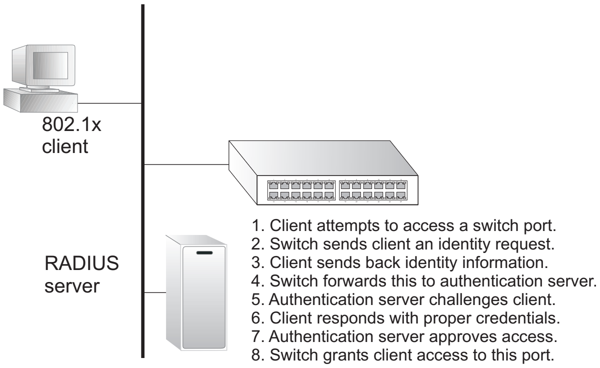
CONFIGURING 802.1X PORT AUTHENTICATION

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 171: 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 XP, and in Windows 2000 with Service Pack 4. 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 693

PARAMETERS

These parameters are displayed in the web interface:

- **Port Authentication Status** – 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.

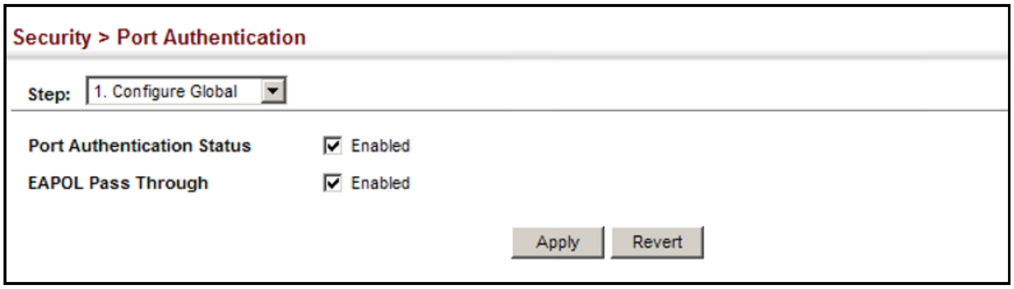
  When this device is functioning as an edge switch but does not require any attached clients to be authenticated, **EAPOL Pass Through** can be disabled to discard unnecessary EAPOL traffic.

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. Then set the user name and password to use when the switch responds an MD5 challenge from the authentication server.
4. Click Apply

Figure 172: Configuring Global Settings for 802.1X Port Authentication



Security > Port Authentication

Step: 1. Configure Global

Port Authentication Status ☑ Enabled

EAPOL Pass Through ☑ Enabled

CONFIGURING PORT 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 693

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.

PARAMETERS

These parameters are displayed in the web interface:

- **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.
  - **No** – Connected client is not authorized.
- **Supplicant** – Indicates the MAC address of a connected client.
- **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 MAC 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. (Fixed Setting: 10 seconds)

- **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)

- **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 156) and mapped on each port (See "Configuring Network Access for Ports" on page 266).

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

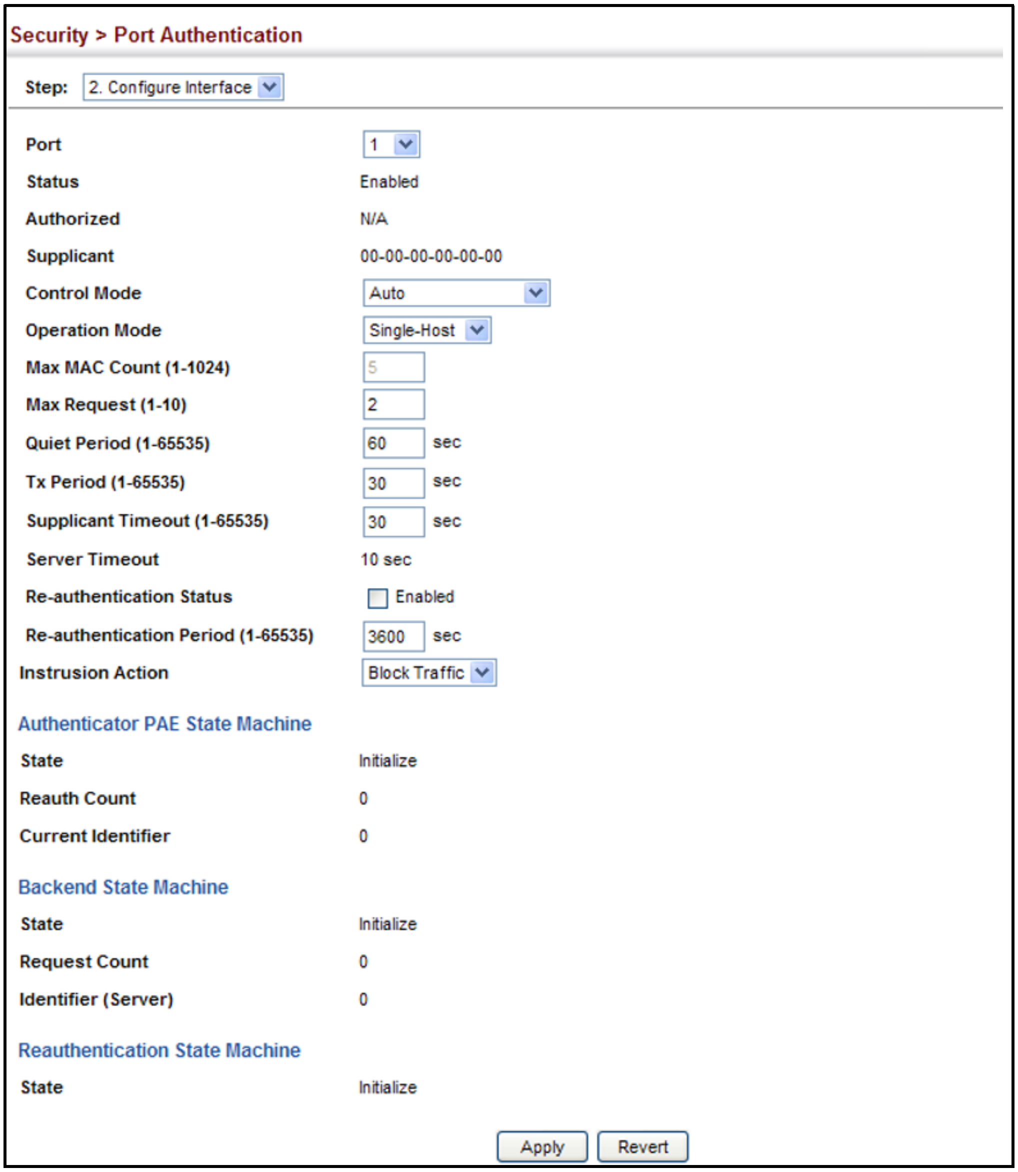
- **State** – Current state (including initialize, reauthenticate).

WEB INTERFACE

To configure port authenticator settings for 802.1X:

1. Click Security, Port Authentication.
2. Select Configure Interface from the Step list.
3. Click Authenticator.
4. Modify the authentication settings for each port as required.
5. Click Apply

Figure 173: Configuring Interface Settings for 802.1X Port Authenticator



Security > Port Authentication

Step: 2. Configure Interface

Port	1
Status	Enabled
Authorized	N/A
Supplicant	00-00-00-00-00-00
Control Mode	Auto
Operation Mode	Single-Host
Max MAC 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
Instrusion Action	Block Traffic

Authenticator PAE State Machine

State	Initialize
Reauth Count	0
Current Identifier	0

Backend State Machine

State	Initialize
Request Count	0
Identifier (Server)	0

Reauthentication State Machine

State	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 702

PARAMETERS

These parameters are displayed in the web interface:

Table 15: 802.1X Statistics

Parameter	Description
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.
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.

WEB INTERFACE

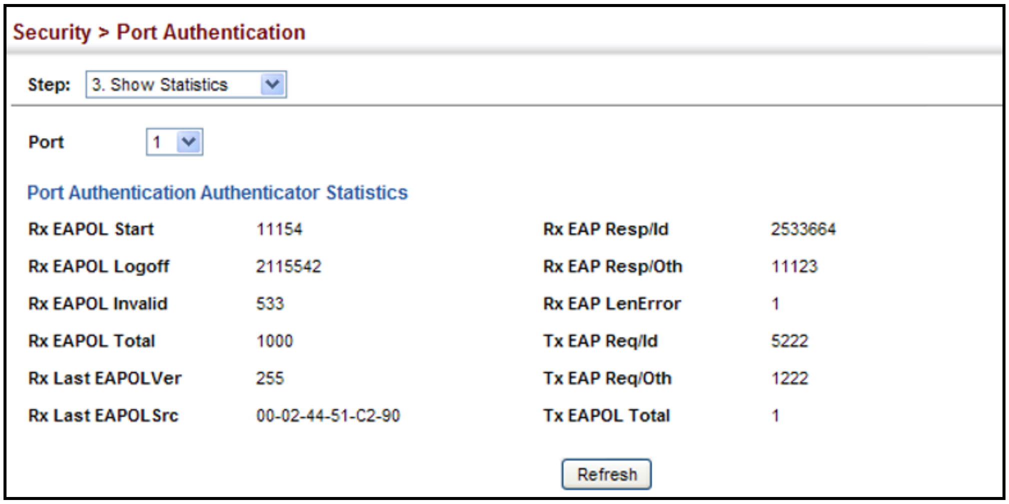
To display port authenticator statistics for 802.1X:

1. Click Security, Port Authentication.

2. Select Show Statistics from the Step list.

3. Click Authenticator.

Figure 174: Showing Statistics for 802.1X Port Authenticator



Step: 3. Show Statistics

Port 1

Port Authentication Authenticator Statistics

Rx EAPOL Start	11154	Rx EAP Resp/Id	2533664
Rx EAPOL Logoff	2115542	Rx EAP Resp/Oth	11123
Rx EAPOL Invalid	533	Rx EAP LenError	1
Rx EAPOL Total	1000	Tx EAP Req/Id	5222
Rx Last EAPOLVer	255	Tx EAP Req/Oth	1222
Rx Last EAPOLSrc	00-02-44-51-C2-90	Tx EAPOL Total	1

IP SOURCE GUARD

IP 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 326). 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 commands used 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 735

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 326), 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 329), 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 in the web interface:

- **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 326) and static entries set by IP source guard (see "Configuring Static Bindings for IP Source Guard" on page 323).

WEB INTERFACE

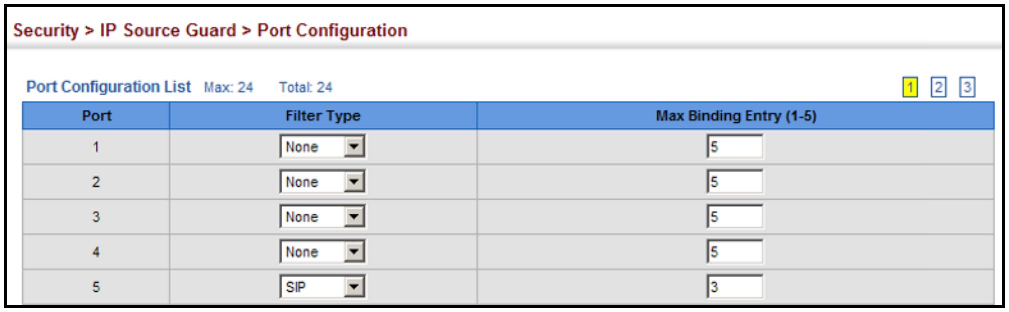
To set the IP Source Guard filter for ports:

1. Click Security, IP Source Guard, Port Configuration.

2. Set the required filtering type for each port.

3. Click Apply

Figure 175: Setting the Filter Type for IP Source Guard



Security > IP Source Guard > Port Configuration

Port Configuration List Max: 24 Total: 24

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 733

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 in the web interface:

- **Port** – The port to which a static entry is bound.

- **VLAN** – ID of a configured VLAN (Range: 1-4093)

- **MAC Address** – A valid unicast MAC address.

- **IP Address** – A valid unicast IP address, including classful types A, B or C.

WEB INTERFACE

To configure static bindings for IP Source Guard:

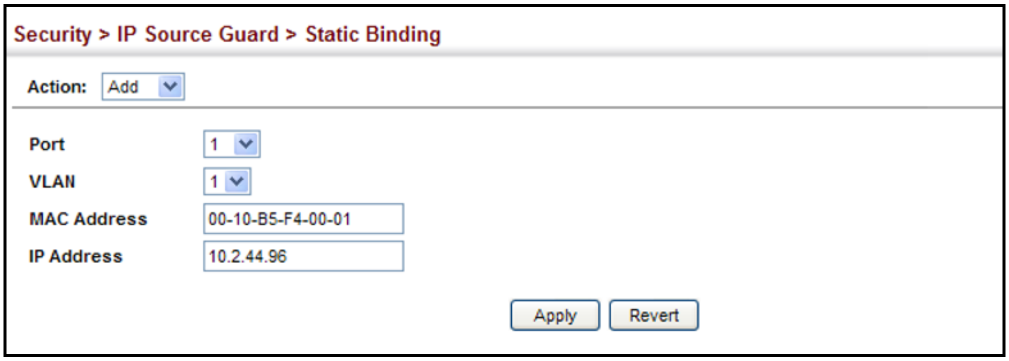
1. Click Security, IP Source Guard, Static Configuration.

2. Select Add from the Action list.

3. Enter the required bindings for each port.

4. Click Apply

Figure 176: Configuring Static Bindings for IP Source Guard



Security > IP Source Guard > Static Binding

Action: Add

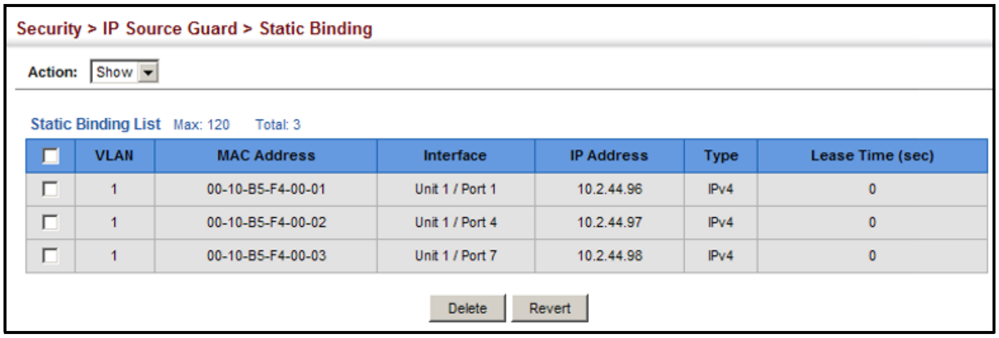
Port	1
VLAN	1
MAC Address	00-10-B5-F4-00-01
IP Address	10.2.44.96

To display static bindings for IP Source Guard:

1. Click Security, IP Source Guard, Static Configuration.

2. Select Show from the Action list.

Figure 177: Displaying Static Bindings for IP Source Guard



Security > IP Source Guard > Static Binding

Action: Show

Static Binding List Max: 120 Total: 3

□	VLAN	MAC Address	Interface	IP Address	Type	Lease Time (sec)
□	1	00-10-B5-F4-00-01	Unit 1 / Port 1	10.2.44.96	IPv4	0
□	1	00-10-B5-F4-00-02	Unit 1 / Port 4	10.2.44.97	IPv4	0
□	1	00-10-B5-F4-00-03	Unit 1 / Port 7	10.2.44.98	IPv4	0

Displaying Information for Dynamic IP 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 732

Parameters

These parameters are displayed in the web interface:

Query by

- **Port** – A port on this switch.
- **VLAN** – ID of a configured VLAN (Range: 1-4093)
- **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.
- **Type** – Static or dynamic binding.
- **Lease Time** – The time for which this IP address is leased to the client.

WEB INTERFACE

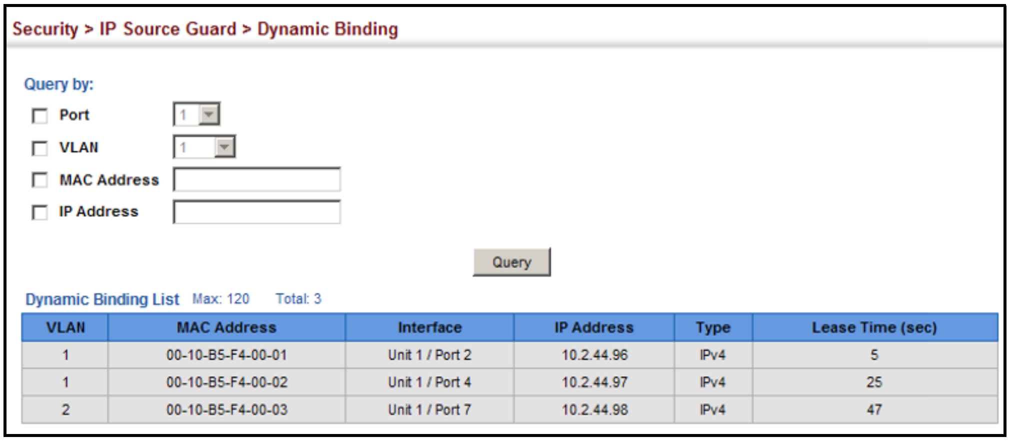
To display the binding table for IP Source Guard:

1. Click Security, IP Source Guard, Dynamic Binding.

2. Mark the search criteria, and enter the required values.

3. Click Query

Figure 178: 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 Max: 120 Total: 3

VLAN	MAC Address	Interface	IP Address	Type	Lease Time (sec)
1	00-10-B5-F4-00-01	Unit 1 / Port 2	10.2.44.96	IPv4	5
1	00-10-B5-F4-00-02	Unit 1 / Port 4	10.2.44.97	IPv4	25
2	00-10-B5-F4-00-03	Unit 1 / Port 7	10.2.44.98	IPv4	47

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

- "DHCP Snooping" on page 724

PARAMETERS

These parameters are displayed in the web interface:

- **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 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:

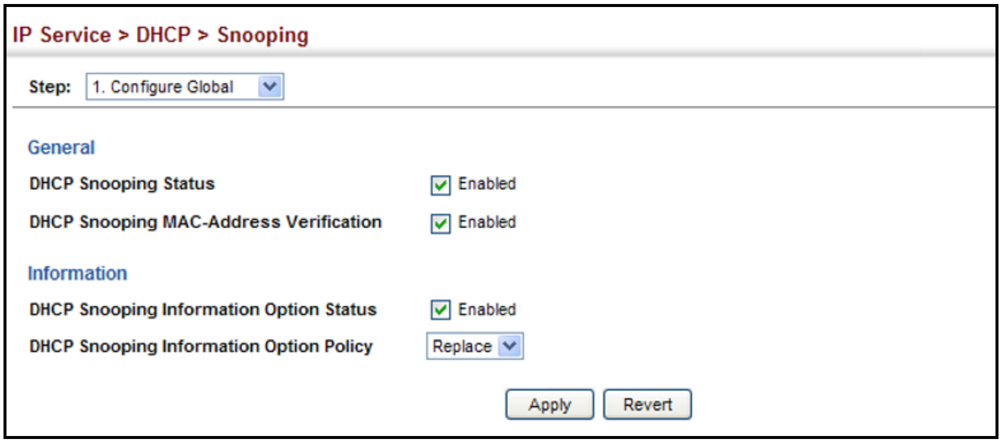
1. Click Security, IP Source Guard, DHCP Snooping.

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 179: 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 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 729

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 in the web interface:

- **VLAN** – ID of a configured VLAN. (Range: 1-4093)

- **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:

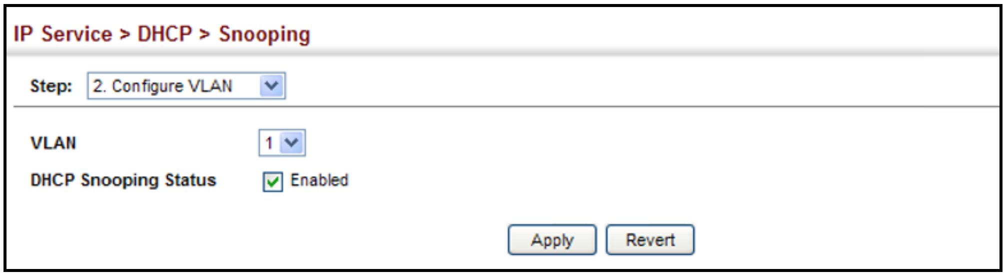
1. Click Security, IP Source Guard, DHCP Snooping.

2. Select Configure VLAN from the Step list.

3. Enable DHCP Snooping on any existing VLAN.

4. Click Apply

Figure 180: 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 730

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 in the web interface:

- **Trust Status** – Enables or disables a port as trusted. (Default: Disabled)

WEB INTERFACE

To configure global settings for DHCP Snooping:

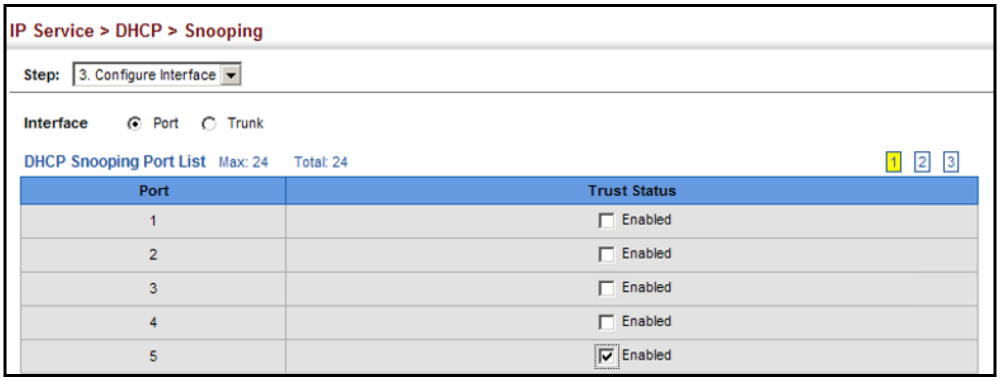
1. Click Security, IP Source Guard, DHCP Snooping.

2. Select Configure Interface from the Step list.

3. Set any ports within the local network or firewall to trusted.

4. Click Apply

Figure 181: Configuring the Port Mode for DHCP Snooping



IP Service > DHCP > Snooping

Step: 3. Configure Interface

Interface ● Port ○ Trunk

DHCP Snooping Port List Max: 24 Total: 24

1 2 3

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

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 732

PARAMETERS

These parameters are displayed in the web interface:

- **MAC Address** – Physical address associated with the entry.
- **IP Address** – IP address corresponding to the client.
- **Lease Time** (seconds) – 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

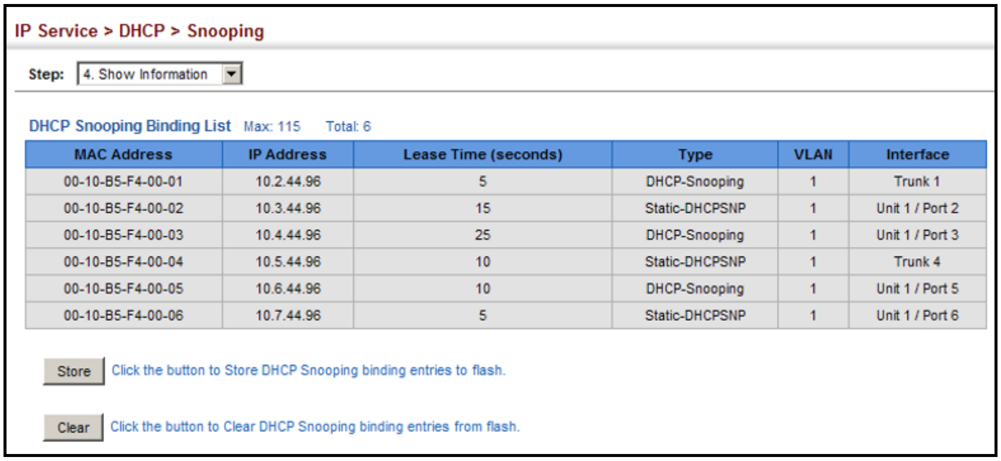
To display the binding table for DHCP Snooping:

1. Click Security, IP Source Guard, DHCP Snooping.

2. Select Show Information from the Step list.

3. Use the Store or Clear function if required.

Figure 182: Displaying the Binding Table for DHCP Snooping



IP Service > DHCP > Snooping

Step: 4. Show Information

DHCP Snooping Binding List Max: 115 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.

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 610

PARAMETERS

These parameters are displayed in the web interface:

- **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 16: 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.

WEB INTERFACE

To configure the logging of error messages to system memory:

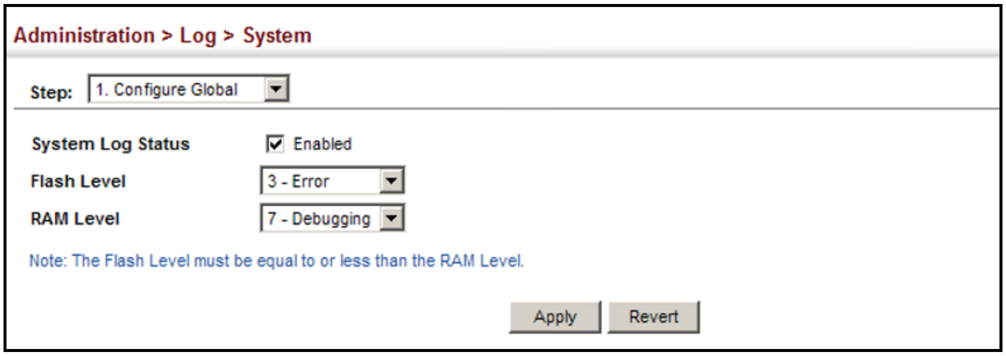
1. Click Administration, Log, System.

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 183: 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

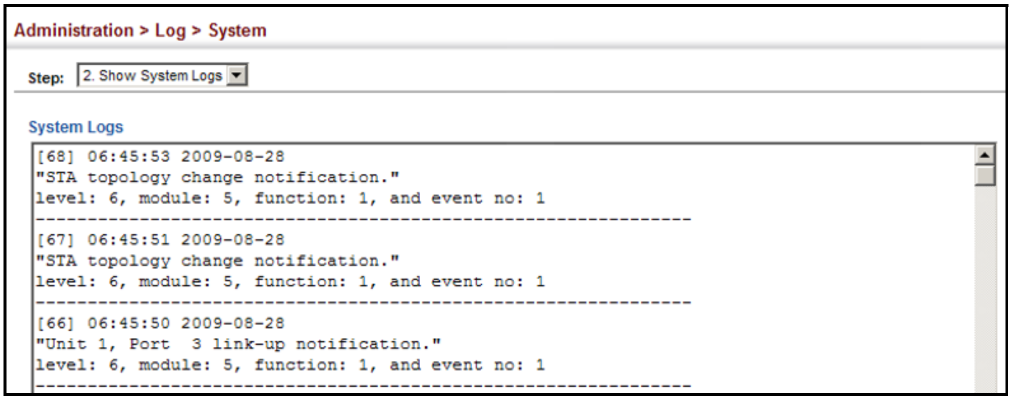
Note: The Flash Level must be equal to or less than the RAM Level.

To show the error messages logged to system memory:

1. Click Administration, Log, System.
2. Select Show System Logs from the Step list.

   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 184: Showing Error Messages Looged to System Memory



Administration > Log > System

Step: 2. Show System Logs

System Logs

```
[68] 06:45:53 2009-08-28
"STA topology change notification."
level: 6, module: 5, function: 1, and event no: 1
----------------------------------------------------------------
[67] 06:45:51 2009-08-28
"STA topology change notification."
level: 6, module: 5, function: 1, and event no: 1
----------------------------------------------------------------
[66] 06:45:50 2009-08-28
"Unit 1, Port  3 link-up 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 610

PARAMETERS

These parameters are displayed in the web interface:

- **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

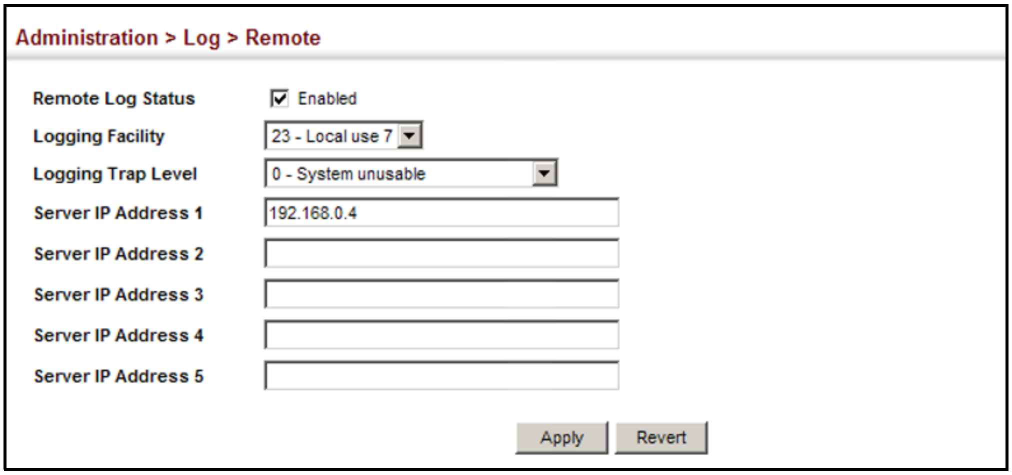
To configure the logging of error messages to remote servers:

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 185: 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 616

PARAMETERS

These parameters are displayed in the web interface:

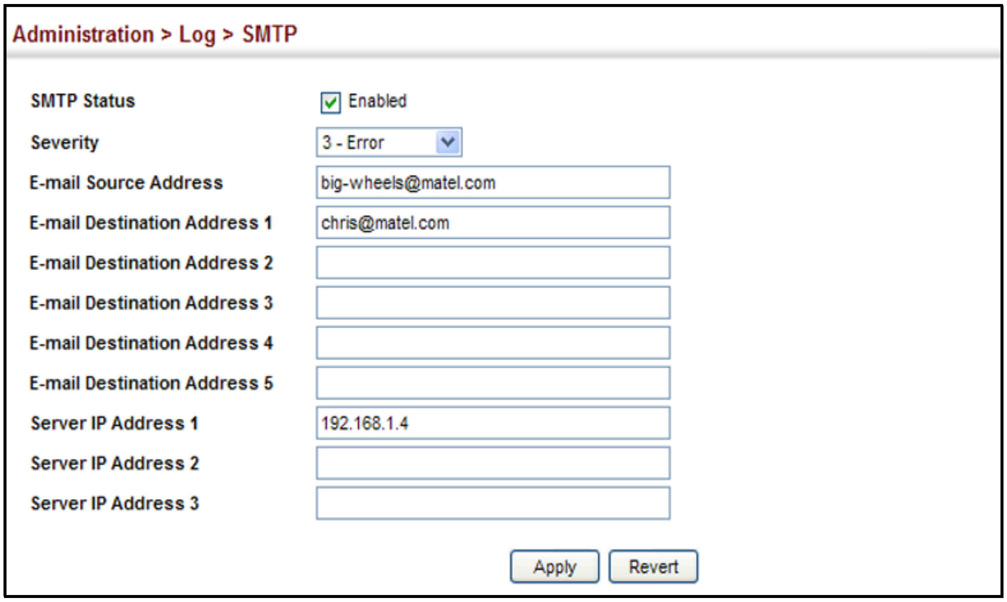
- **SMTP Status** – Enables/disables the SMTP function. (Default: Enabled)
- **Severity** – Sets the syslog severity threshold level (see table on page 336) used to trigger alert messages. All events at this level or higher will be sent to the configured email recipients. For example, using Level 7 will 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. The switch attempts to connect to the other listed servers if the first fails.

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 186: 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.

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 951

PARAMETERS

These parameters are displayed in the web interface:

- **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)

This attribute must comply with the following rule:
(Transmission Interval * Hold Time Multiplier) ≤ 65536, and
Transmission Interval >= (4 * Delay Interval)

- **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:
  (Transmission Interval * Holdtime Multiplier) ≤ 65536.

  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.

WEB INTERFACE

To configure LLDP timing attributes:

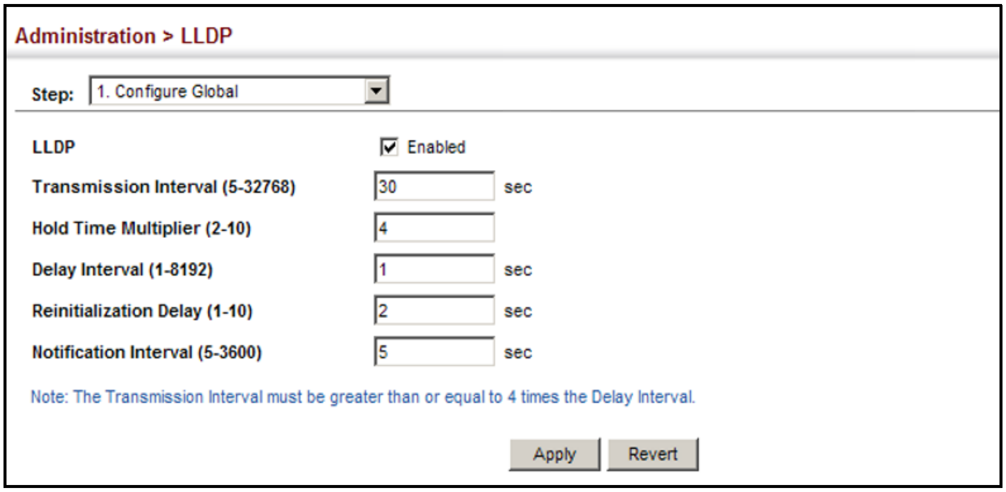
1. Click Administration, LLDP.

2. Select Configure Global from the Step list.

3. Enable LLDP, and modify any of the timing parameters as required.

4. Click Apply.

Figure 187: 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) 1 sec

Reinitialization Delay (1-10) 2 sec

Notification Interval (5-3600) 5 sec

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 951

PARAMETERS

These parameters are displayed in the web interface:

- **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: Enabled)

  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 372.

  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.

- **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 101.

- **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 177).

  - **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 153).

  - **VLAN Name** – The name of all VLANs to which this interface has been assigned(see "IEEE 802.1Q VLANs" on page 153 and "Protocol VLANs" on page 177).

  - **Port And Protocol VLAN ID** – The port-based and protocol-based VLANs configured on this interface (the port-based and protocol-based VLANs configured on this interface (see "IEEE 802.1Q VLANs" on page 153 and "Protocol VLANs" on page 177).

- **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 104 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.

WEB INTERFACE

To configure LLDP interface attributes:

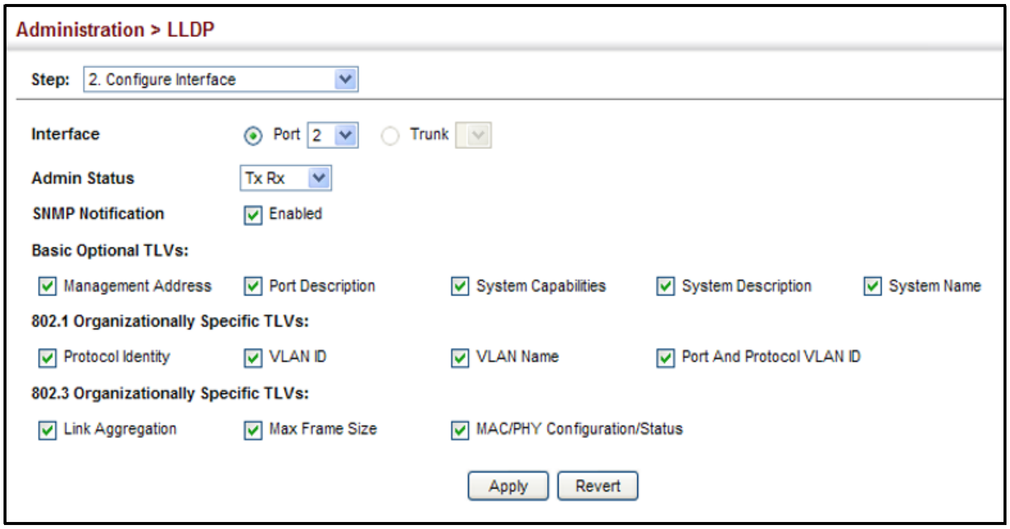
1. Click Administration, LLDP.

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 188: Configuring LLDP Interface Attributes



Administration > LLDP

Step: 2. Configure Interface

Interface ● Port 2 ○ Trunk

Admin Status Tx Rx

SNMP 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

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 964

PARAMETERS

These parameters are displayed in the web interface:

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 17: 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 101).
- **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 18: 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.

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.

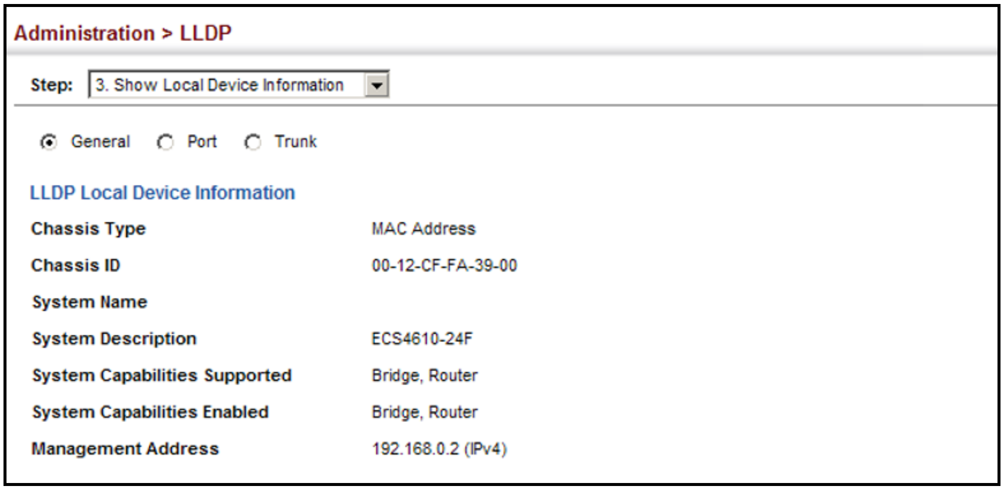
- **Port/Trunk Description** – A string that indicates the port or trunk description. If RFC 2863 is implemented, the ifDescr object should be used for this field.
- **Port/Trunk ID** – A string that contains the specific identifier for the port or trunk from which this LLDPDU was transmitted.

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, or Trunk.

Figure 189: Displaying Local Device Information for LLDP (General)



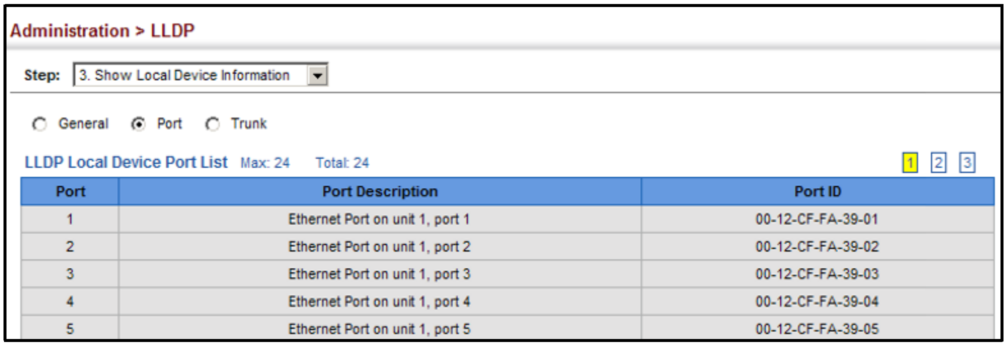
Step: 3. Show Local Device Information

● General ○ Port ○ Trunk

LLDP Local Device Information

Chassis Type	MAC Address
Chassis ID	00-12-CF-FA-39-00
System Name	
System Description	ECS4610-24F
System Capabilities Supported	Bridge, Router
System Capabilities Enabled	Bridge, Router
Management Address	192.168.0.2 (IPv4)

Figure 190: Displaying Local Device Information for LLDP (Port)



Step: 3. Show Local Device Information

○ General ● Port ○ Trunk

LLDP Local Device Port List Max: 24 Total: 24

Port	Port Description	Port ID
1	Ethernet Port on unit 1, port 1	00-12-CF-FA-39-01
2	Ethernet Port on unit 1, port 2	00-12-CF-FA-39-02
3	Ethernet Port on unit 1, port 3	00-12-CF-FA-39-03
4	Ethernet Port on unit 1, port 4	00-12-CF-FA-39-04
5	Ethernet Port on unit 1, port 5	00-12-CF-FA-39-05

DISPLAYING LLDP REMOTE PORT 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 965

PARAMETERS

These parameters are displayed in the web interface:

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

- **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 17, "Chassis ID Subtype," on page 345.)

- **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.

- **Management Address** – The IPv4 address of the remote device. If no management address is available, the address should be the MAC address for the CPU or for the port sending this advertisement.

- **Port Type** – Indicates the basis for the identifier that is listed in the Port ID field.

Table 19: 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 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 18, "System Capabilities," on page 346.)

- **System Capabilities Enabled** – The primary function(s) of the system which are currently enabled. (See Table 18, "System Capabilities," on page 346.)

- **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.

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 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 20: Remote Port Auto-Negotiation Advertised Capability

Bit	Capability
0	other or unknown
1	10BASE-T half duplex mode
2	10BASE-T full duplex mode
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

Table 20: Remote Port Auto-Negotiation Advertised Capability

Bit	Capability
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 Aggregation 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

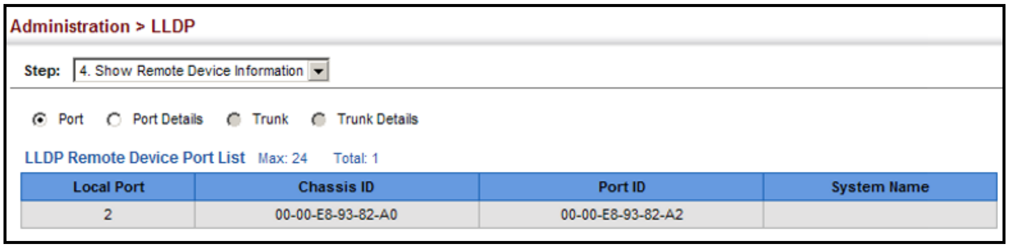
- **Remote Max Frame Size** – An integer value indicating the maximum supported frame size in octets on the port component associated with the remote system.

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.

Figure 191: Displaying Remote Device Information for LLDP (Port)



Administration > LLDP

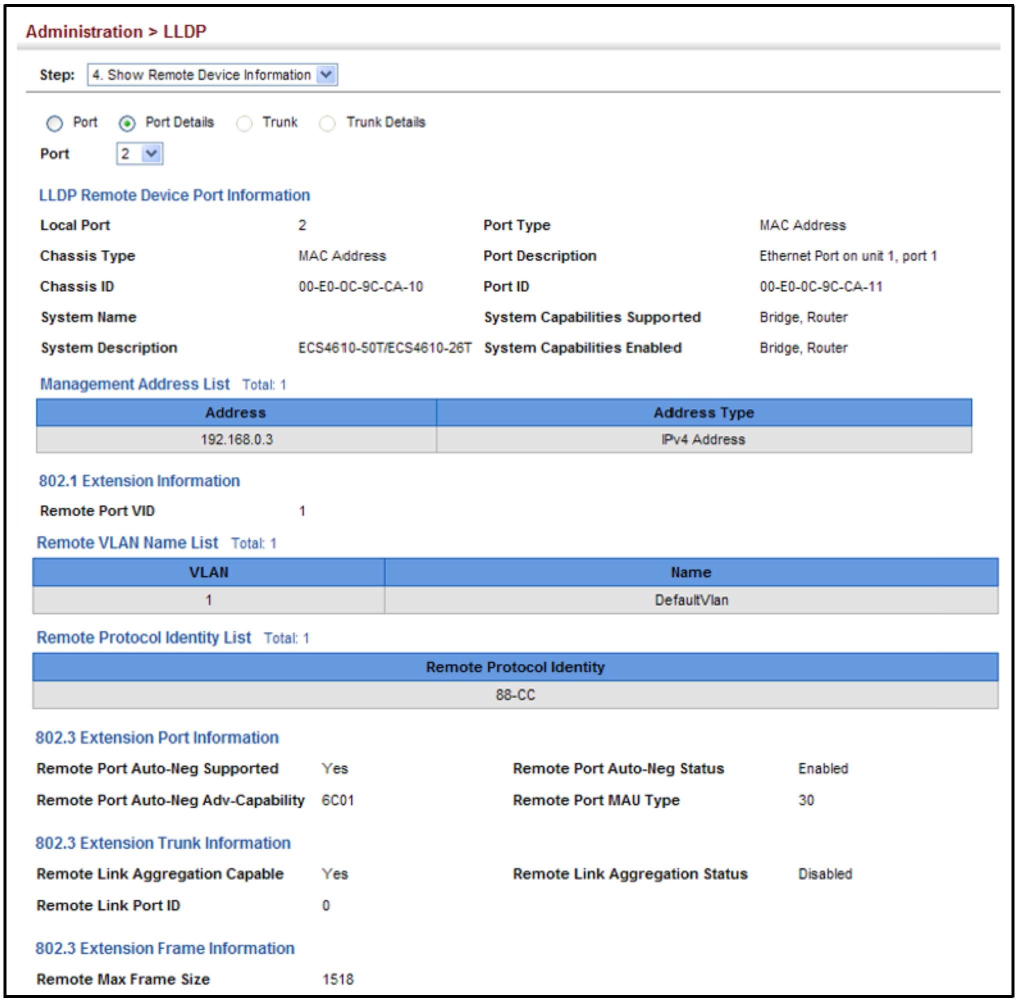
Step: 4. Show Remote Device Information

● Port ○ Port Details ○ Trunk ○ Trunk Details

LLDP Remote Device Port List Max: 24 Total: 1

Local Port	Chassis ID	Port ID	System Name
2	00-00-E8-93-82-A0	00-00-E8-93-82-A2	

Figure 192: 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 1, port 1
Chassis ID	00-E0-0C-9C-CA-10	Port ID	00-E0-0C-9C-CA-11
System Name		System Capabilities Supported	Bridge, Router
System Description	ECS4610-50T/ECS4610-26T	System Capabilities Enabled	Bridge, Router

Management Address List Total: 1

Address	Address Type
192.168.0.3	IPv4 Address

802.1 Extension Information

Remote Port VID 1

Remote VLAN Name List Total: 1

VLAN	Name
1	DefaultVlan

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	6C01	Remote Port MAU Type	30

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

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 966

PARAMETERS

These parameters are displayed in the web interface:

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

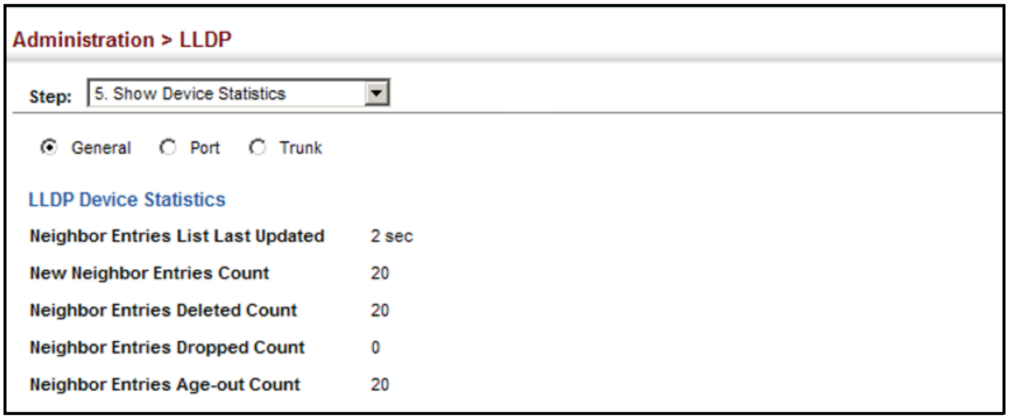
To display statistics for LLDP-capable devices attached to the switch:

1. Click Administration, LLDP.

2. Select Show Device Statistics from the Step list.

3. Select General, Port, or Trunk.

Figure 193: Displaying LLDP Device Statistics (General)



Administration > LLDP

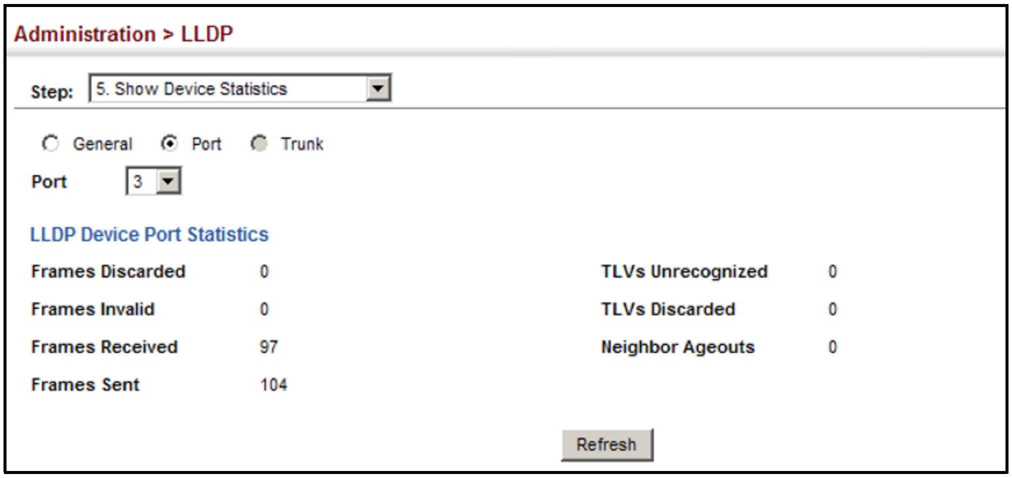
Step: 5. Show Device Statistics

● 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 194: 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 21: 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 630
- "snmp-server enable traps" on page 633

PARAMETERS

These parameters are displayed in the web interface:

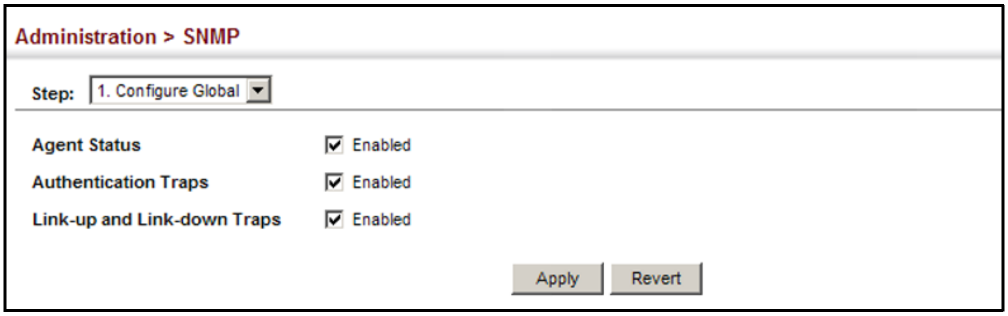
- **Agent Status** – Enables SNMP on the switch. (Default: Enabled)
- **Authentication Traps**[5] – Issues a notification message to specified IP trap managers whenever an invalid community string is submitted during the SNMP access authentication process. (Default: Enabled)
- **Link-up and Link-down Traps**[5] – 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 195: 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 636

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

[5] 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 360).

ID is deleted or changed, all SNMP users will be cleared. You will need to reconfigure all existing users.

PARAMETERS

These parameters are displayed in the web interface:

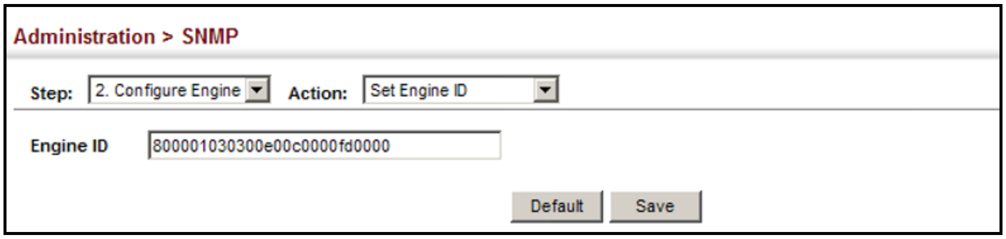
- **Engine ID** – A new engine ID can be specified by entering 9 to 64 hexadecimal characters (5 to 32 octets in hexadecimal format). If an odd number of characters are specified, a trailing zero is added to the value to fill in the last octet. For example, the value "123456789" is equivalent to "1234567890".

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 196: Configuring the Local Engine ID for SNMP



Administration > SNMP

Step: 2. Configure Engine Action: Set Engine ID

Engine ID 800001030300e00c0000fd0000

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 636

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 370.)

PARAMETERS

These parameters are displayed in the web interface:

- **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.

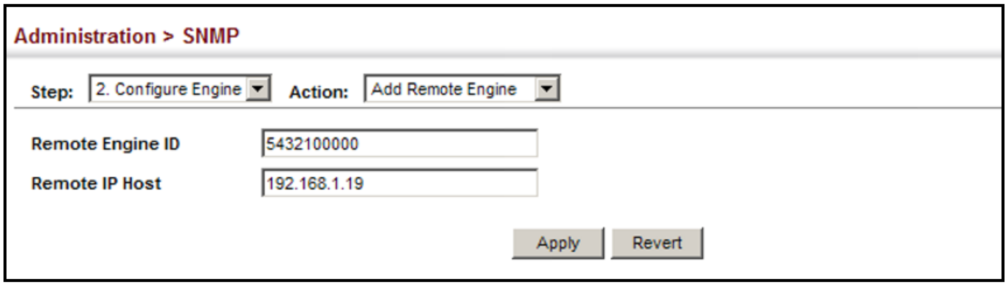
2. Select Configure Engine from the Step list.

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 197: 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

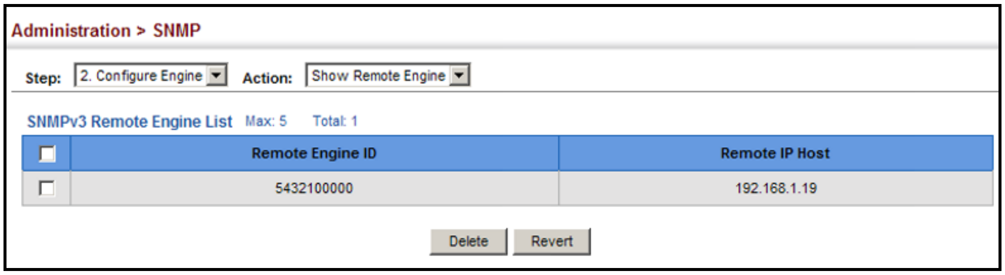
To show the remote SNMP engine IDs:

1. Click Administration, SNMP.

2. Select Configure Engine from the Step list.

3. Select Show Remote Engine from the Action list.

Figure 198: Showing Remote Engine IDs for SNMP



Administration > SNMP

Step: 2. Configure Engine Action: Show Remote Engine

SNMPv3 Remote Engine List Max: 5 Total: 1

□	Remote Engine ID	Remote IP Host
□	5432100000	192.168.1.19

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 640

PARAMETERS

These parameters are displayed in the web interface:

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:

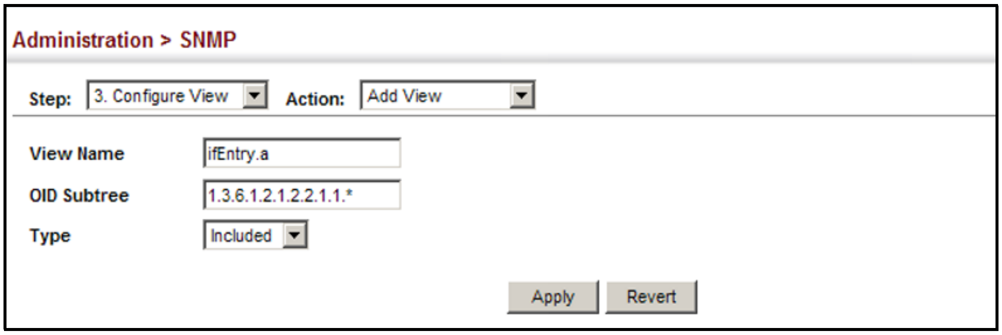
1. Click Administration, SNMP.
2. Select Configure View from the Step list.

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 199: 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

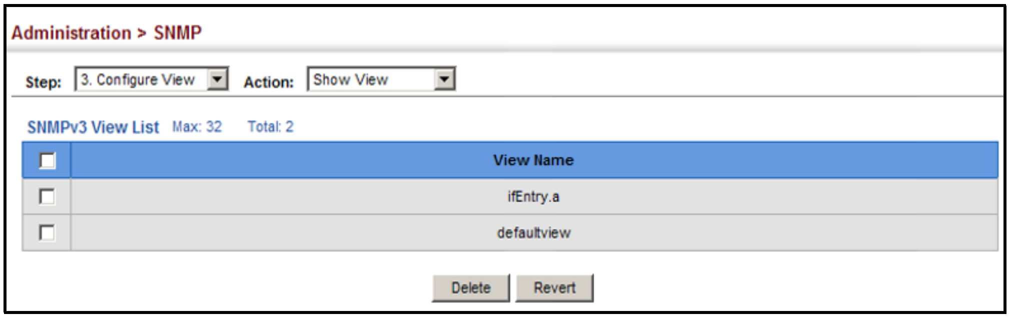
To show the SNMP views of the switch's MIB database:

1. Click Administration, SNMP.

2. Select Configure View from the Step list.

3. Select Show View from the Action list.

Figure 200: Showing SNMP Views



Administration > SNMP

Step: 3. Configure View Action: Show View

SNMPv3 View List Max: 32 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.

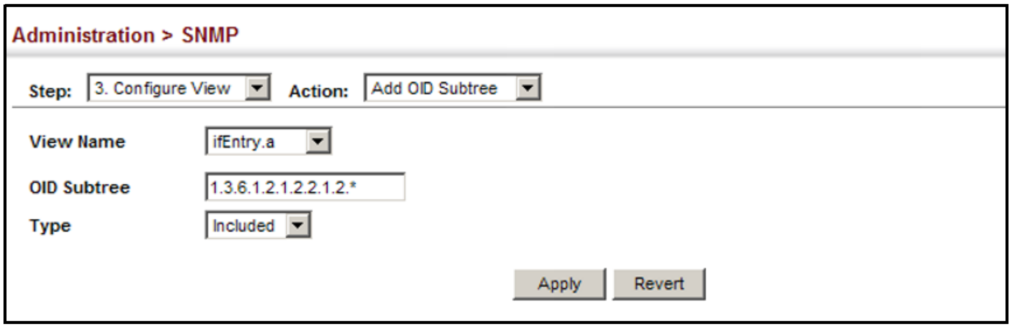
2. Select Configure View from the Step list.

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 201: Adding an OID Subtree to an SNMP View



Administration > SNMP

Step: 3. Configure View Action: Add OID Subtree

View Name: ifEntry.a

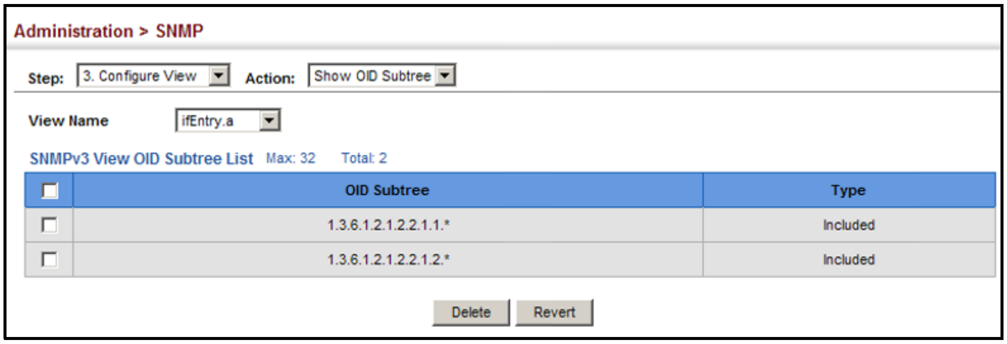
OID Subtree: 1.3.6.1.2.1.2.2.1.2.*

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 202: 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 Max: 32 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 642

PARAMETERS

These parameters are displayed in the web interface:

- **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: 1-64 characters)
- **Write View** – The configured view for write access. (Range: 1-64 characters)
- **Notify View** – The configured view for notifications. (Range: 1-64 characters)

Table 22: 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.

Table 22: Supported Notification Messages (Continued)

Model	Level	Group
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	1.3.6.1.4.1.259.10.1.5.2.1.0.1	This trap is sent when the power state changes.
swPortSecurityTrap	1.3.6.1.4.1.259.10.1.5.2.1.0.36	This trap is sent when the port is being intruded. This trap will only be sent when the portSecActionTrap is enabled.
swIpFilterRejectTrap	1.3.6.1.4.1.259.10.1.5.2.1.0.40	This trap is sent when an incorrect IP address is rejected by the IP Filter.
swSmtpConnFailureTrap	1.3.6.1.4.1.259.10.1.5.2.1.0.41	This trap is triggered if the SMTP system cannot open a connection to the mail server successfully.
swMainBoardVerMismatchNotificaiton	1.3.6.1.4.1.259.10.1.5.2.1.0.56	This trap is sent when the slave board version is mismatched with the master board version. This trap binds two objects, the first object indicates the master version, whereas the second represents the slave version.
swLoginFailureTrap	1.3.6.1.4.1.259.10.1.5.2.1.0.66	This trap is sent when login fails via console,telnet, or web.

Table 22: Supported Notification Messages (Continued)

Model	Level	Group
swLoginSucceedTrap	1.3.6.1.4.1.259.10.1.5.2.1.0.67	This trap is sent when login succeeds via console,telnet, or web.
swLoopbackDetectionTrap	1.3.6.1.4.1.259.10.1.5.2.1.0.95	This trap will be sent when loopback BPDUs have been detected.
networkAccessPortLinkDetectionTrap	1.3.6.1.4.1.259.10.1.5.2.1.0.96	This trap is sent when a networkAccessPortLinkDetection event is triggered.
swCpuUtiRisingNotification	1.3.6.1.4.1.259.10.1.5.2.1.0.107	This notification indicates that the CPU utilization crossed cpuUtiRisingThreshold.
swCpuUtiFallingNotification	1.3.6.1.4.1.259.10.1.5.2.1.0.108	This notification indicates that the CPU utilization crossed cpuUtiFallingThreshold.
swMemoryUtiRisingThresholdNotification	1.3.6.1.4.1.259.10.1.5.2.1.0.109	This notification indicates that the memory utilization crossed memoryUtiRisingThreshold.
swMemoryUtiFallingThresholdNotification	1.3.6.1.4.1.259.10.1.5.2.1.0.110	This notification indicates that the memory utilization crossed memoryUtiFallingThreshold.

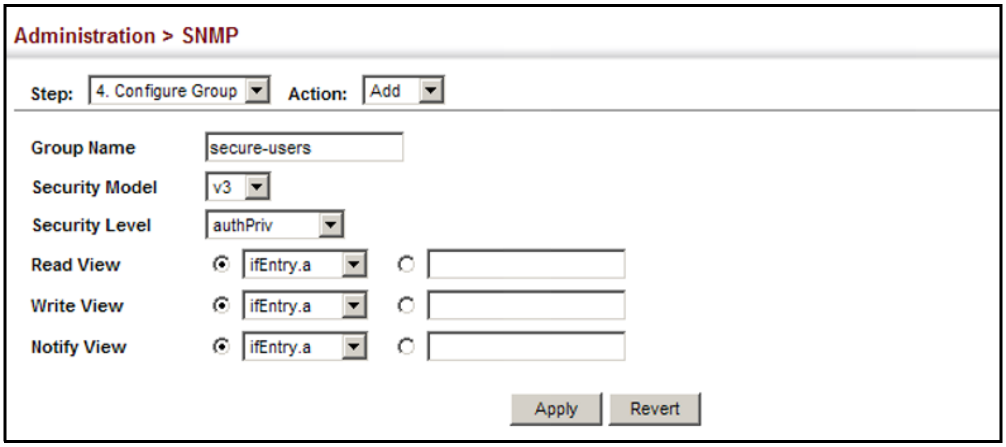
* These are legacy notifications and therefore must be enabled in conjunction with the corresponding traps on the SNMP Configuration menu.

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 203: 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 ○

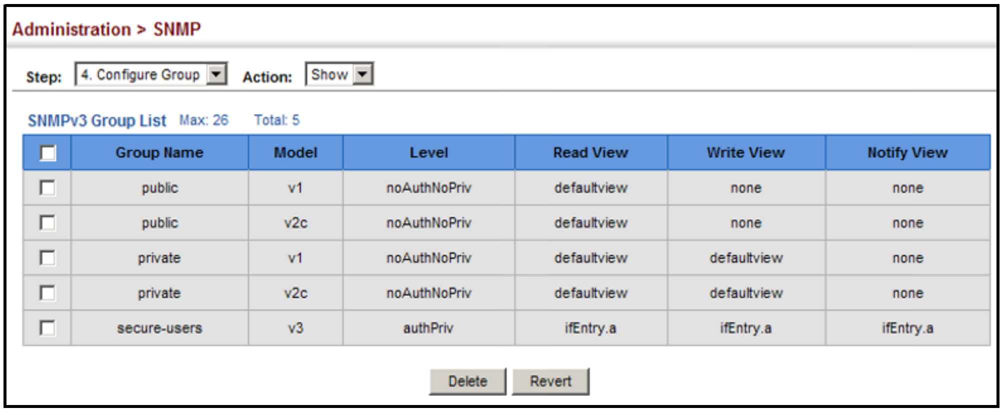
To show SNMP groups:

1. Click Administration, SNMP.

2. Select Configure Group from the Step list.

3. Select Show from the Action list.

Figure 204: Showing SNMP Groups



Administration > SNMP

Step: 4. Configure Group Action: Show

SNMPv3 Group List Max: 26 Total: 5

□	Group Name	Model	Level	Read View	Write View	Notify View
□	public	v1	noAuthNoPriv	defaultview	none	none
□	public	v2c	noAuthNoPriv	defaultview	none	none
□	private	v1	noAuthNoPriv	defaultview	defaultview	none
□	private	v2c	noAuthNoPriv	defaultview	defaultview	none
□	secure-users	v3	authPriv	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 630

PARAMETERS

These parameters are displayed in the web interface:

- **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.

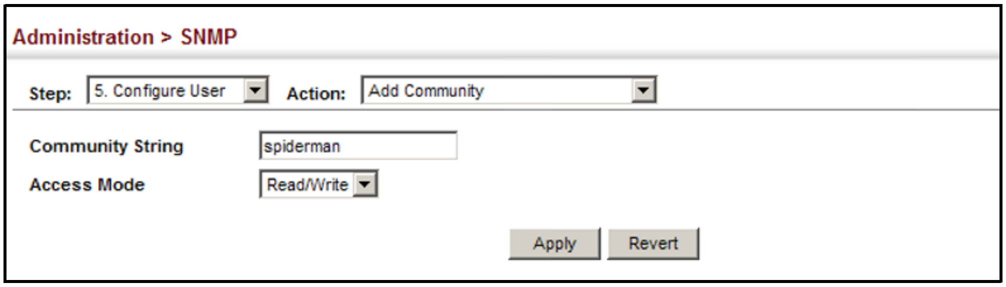
2. Select Configure User from the Step list.

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 205: Setting Community Access Strings



Administration > SNMP

Step: 5. Configure User Action: Add Community

Community String: spiderman

Access Mode: Read/Write

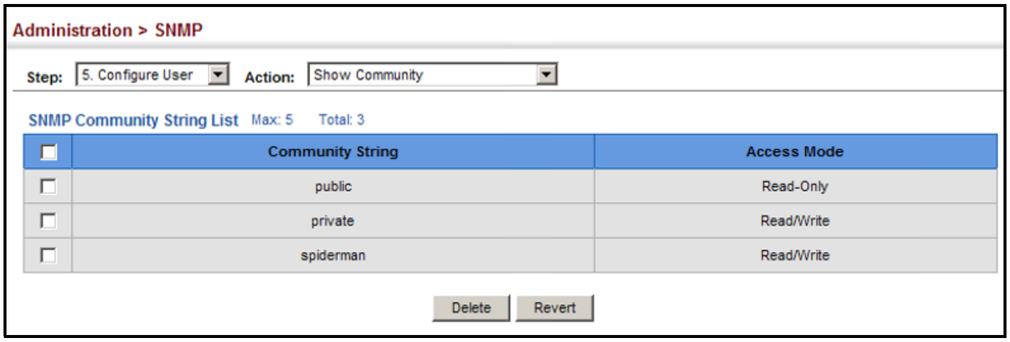
To show the community access strings:

1. Click Administration, SNMP.

2. Select Configure User from the Step list.

3. Select Show Community from the Action list.

Figure 206: Showing Community Access Strings



Administration > SNMP

Step: 5. Configure User Action: Show Community

SNMP Community String List Max: 5 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 639

PARAMETERS

These parameters are displayed in the web interface:

- **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

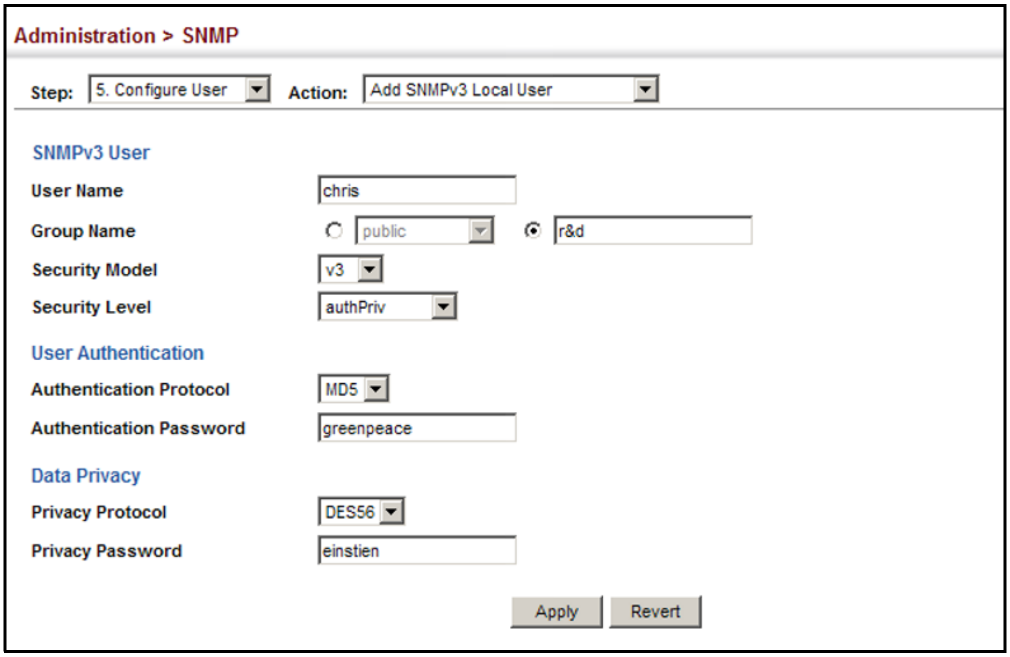
To configure a local SNMPv3 user:

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 207: 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

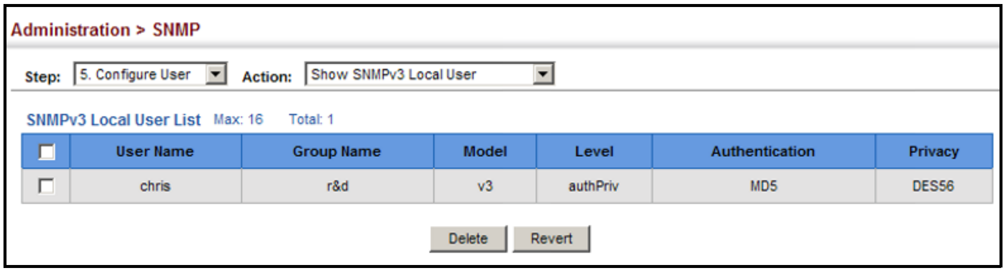
To show local SNMPv3 users:

1. Click Administration, SNMP.

2. Select Configure User from the Step list.

3. Select Show SNMPv3 Local User from the Action list.

Figure 208: Showing Local SNMPv3 Users



Administration > SNMP

Step: 5. Configure User Action: Show SNMPv3 Local User

SNMPv3 Local User List Max: 16 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 639

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 372 and "Specifying a Remote Engine ID" on page 358.)

PARAMETERS

These parameters are displayed in the web interface:

- **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.

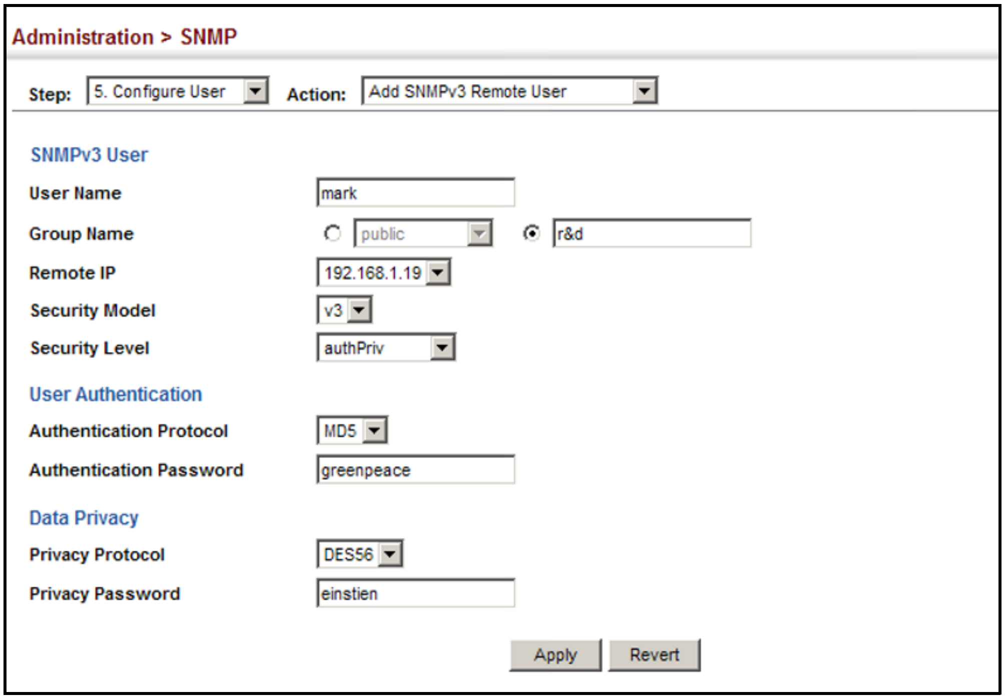
2. Select Configure User from the Step list.

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 209: 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

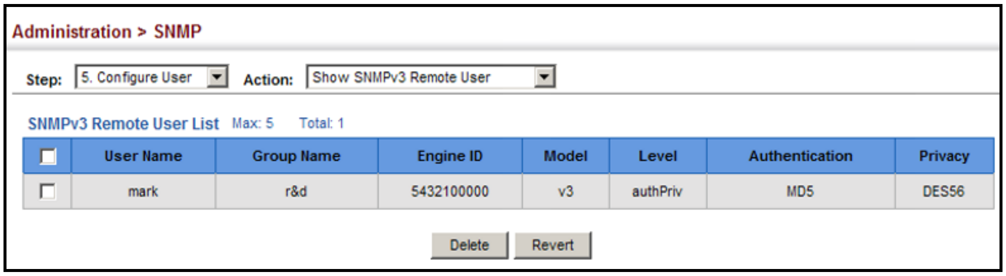
To show remote SNMPv3 users:

1. Click Administration, SNMP.

2. Select Configure User from the Step list.

3. Select Show SNMPv3 Remote User from the Action list.

Figure 210: Showing Remote SNMPv3 Users



Administration > SNMP

Step: 5. Configure User Action: Show SNMPv3 Remote User

SNMPv3 Remote User List Max: 5 Total: 1

□	User Name	Group Name	Engine ID	Model	Level	Authentication	Privacy
□	mark	r&d	5432100000	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 634
- "snmp-server enable traps" on page 633

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 356).
  2. Create a view with the required notification messages (page 360).
  3. Configure the group (matching the community string specified on the Configure Trap - Add page) to include the required notify view (page 363).
  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 356).
  2. Create a local SNMPv3 user to use in the message exchange process (page 368). 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 360).
4. Create a group that includes the required notify view (page 363).
5. Enable trap informs as described in the following pages.

PARAMETERS

These parameters are displayed in the web interface:

SNMP Version 1

- **IP Address** – IP 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** – IP 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** – IP 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 368), 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 370), 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.

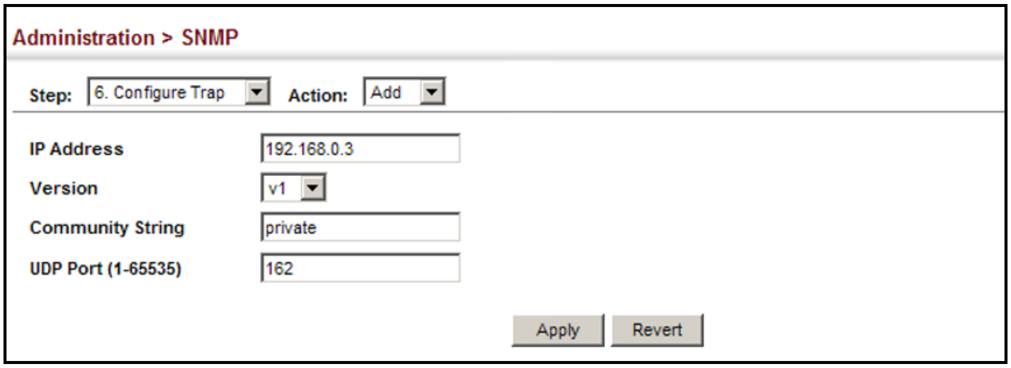
- **AuthNoPriv** – SNMP communications use authentication, but the data is not encrypted.
- **AuthPriv** – SNMP communications use both authentication and encryption.

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 211: Configuring Trap Managers (SNMPv1)

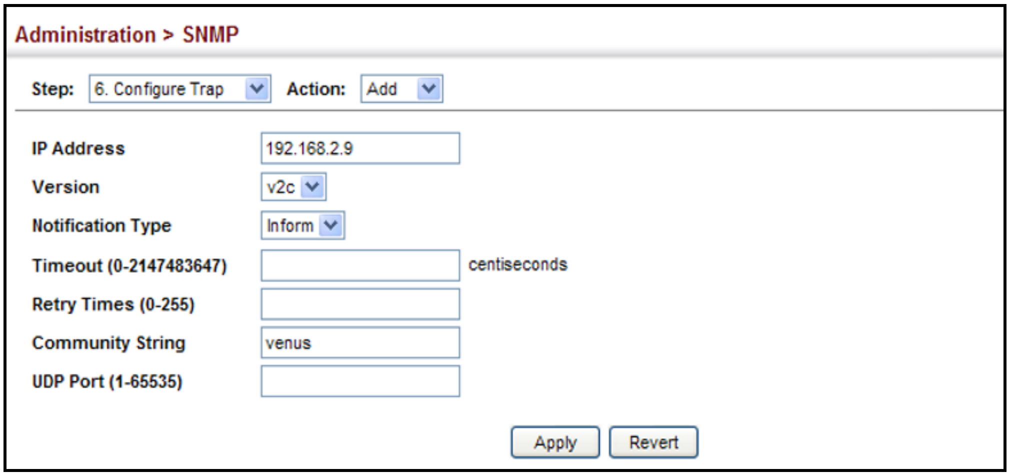


Administration > SNMP

Step: 6. Configure Trap Action: Add

IP Address: 192.168.0.3
Version: v1
Community String: private
UDP Port (1-65535): 162

Figure 212: Configuring Trap Managers (SNMPv2c)

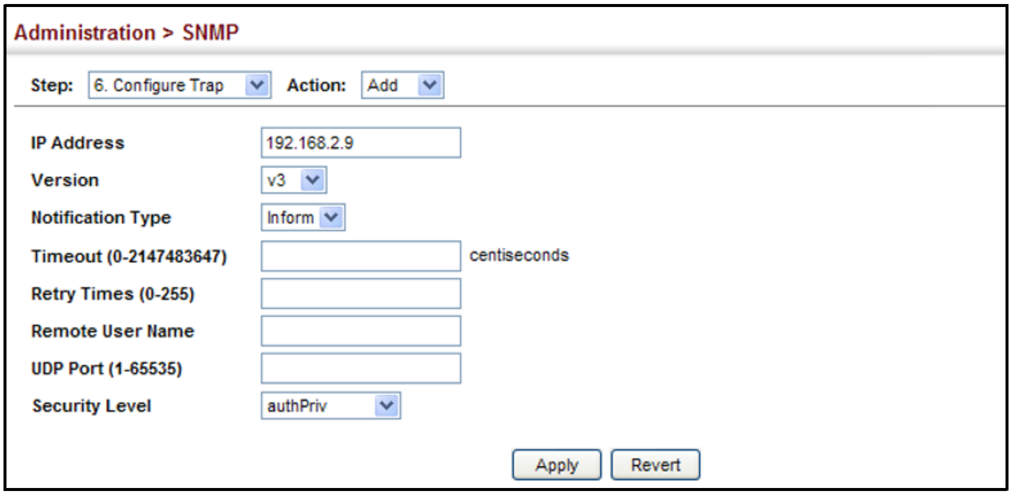


Administration > SNMP

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 213: 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

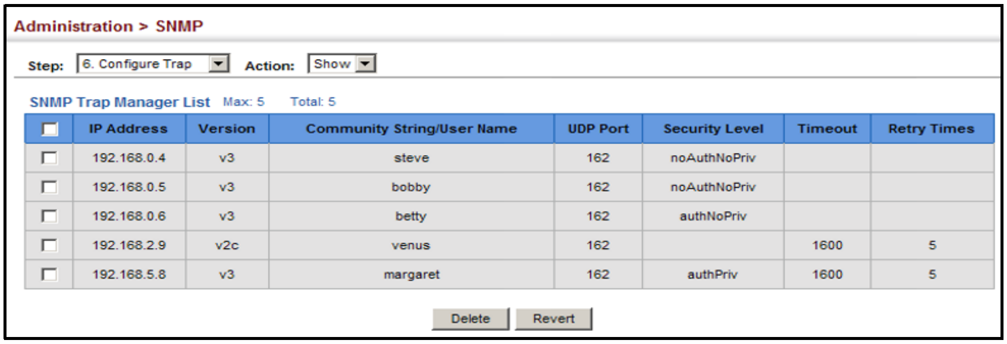
To show configured trap managers:

1. Click Administration, SNMP.

2. Select Configure Trap from the Step list.

3. Select Show from the Action list.

Figure 214: Showing Trap Managers



Administration > SNMP

Step: 6. Configure Trap Action: Show

SNMP Trap Manager List Max: 5 Total: 5

□	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	noAuthNoPriv		
□	192.168.0.6	v3	betty	162	authNoPriv		
□	192.168.2.9	v2c	venus	162		1600	5
□	192.168.5.8	v3	margaret	162	authPriv	1600	5

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 649

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 in the web interface:

- **Index** – Index to this entry. (Range: 1-65535)

- **Status** – The status of this alarm entry. (Displayed data includes: Valid, createRequest, underCreation, or Invalid)

- **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.

- **Last Value** – The value of the statistic during the last sampling period.

- **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: 1-65535)

- **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: 1-65535)

- **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: 1-65535)

- **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: 1-65535)

- **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.

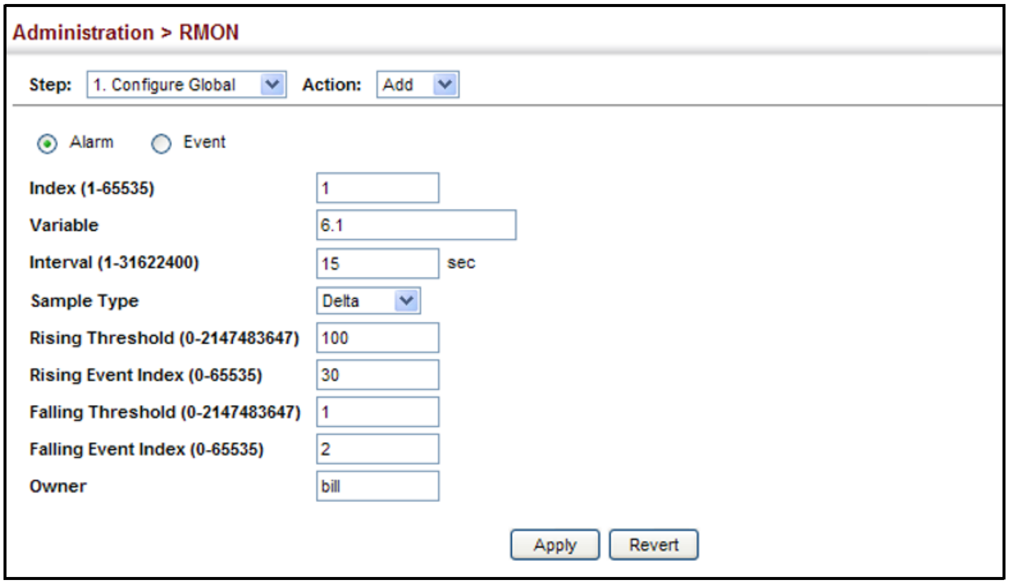
3. Select Add from the Action list.

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 215: Configuring an RMON Alarm



Step: 1. Configure Global
Action: Add

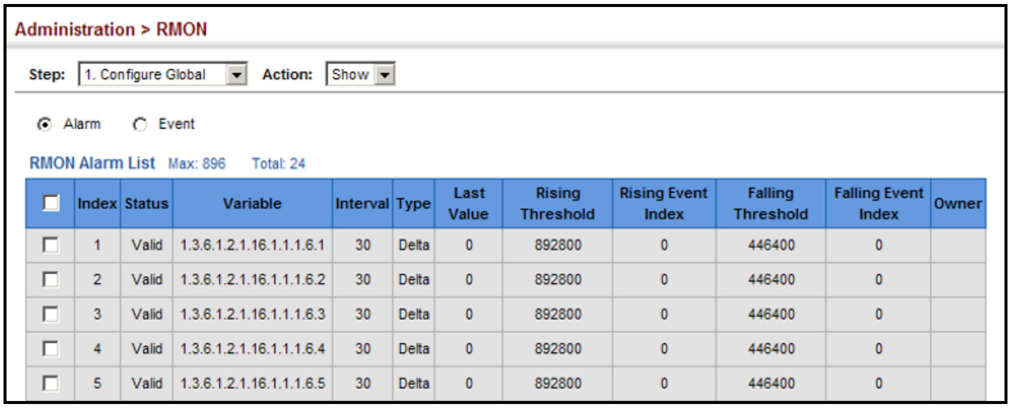
● Alarm ○ Event

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 216: Showing Configured RMON Alarms



Step: 1. Configure Global
Action: Show

● Alarm ○ Event

RMON Alarm List Max: 896 Total: 24

□	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 649

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 in the web interface:

- **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 335).

  - **Trap** – Sends a trap message to all configured trap managers (see "Specifying Trap Managers" on page 372).

  - **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 366) prior to configuring it here. (Range: 1-32 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.

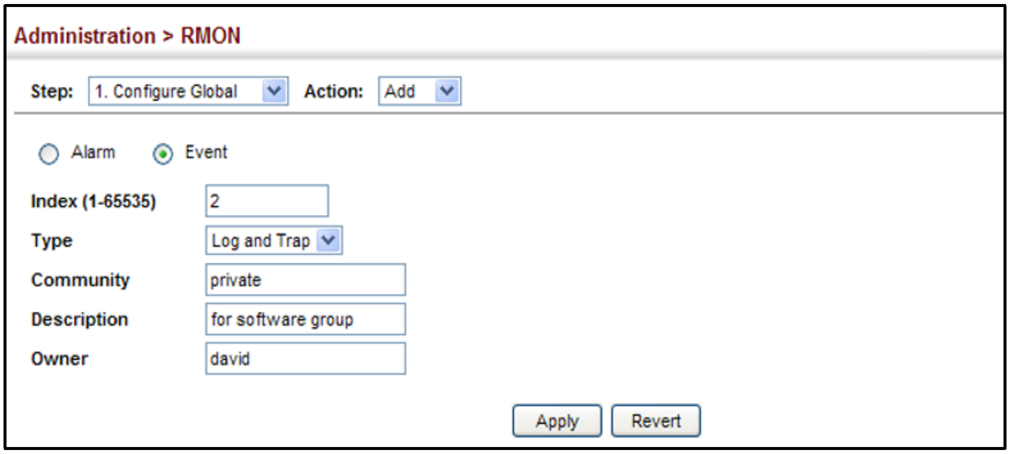
3. Select Add from the Action list.

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 217: 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:

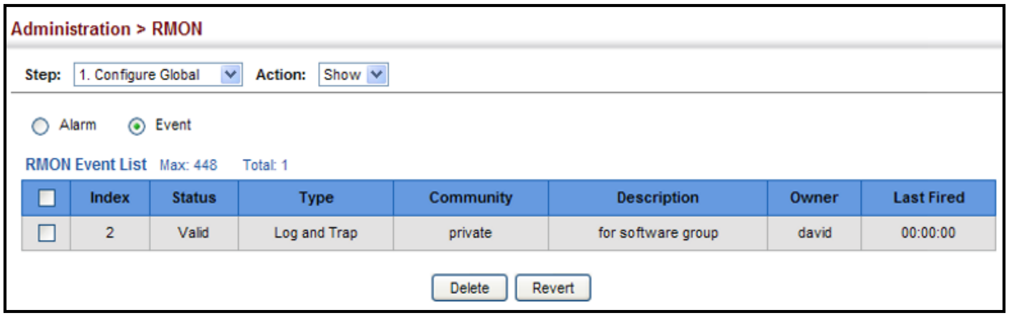
1. Click Administration, RMON.

2. Select Configure Global from the Step list.

3. Select Show from the Action list.

4. Click Event.

Figure 218: Showing Configured RMON Events



Administration > RMON

Step: 1. Configure Global Action: Show

○ Alarm ● Event

RMON Event List Max: 448 Total: 1

□	Index	Status	Type	Community	Description	Owner	Last Fired
□	2	Valid	Log and Trap	private	for software group	david	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 649

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, collisioins, 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 131.

PARAMETERS

These parameters are displayed in the web interface:

- **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.

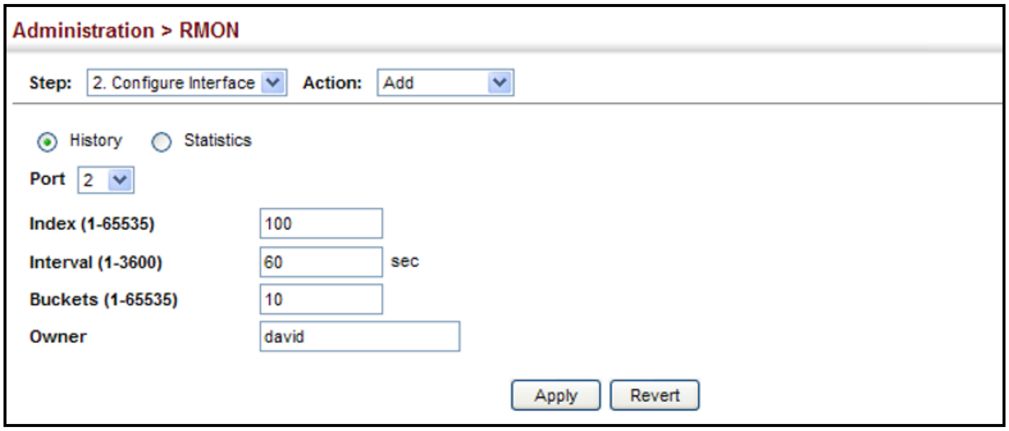
- **Owner** - Name of the person who created this entry. (Range: 1-127 characters)

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 219: Configuring an RMON History Sample



Administration > RMON

Step: 2. Configure Interface Action: Add

● History ○ Statistics

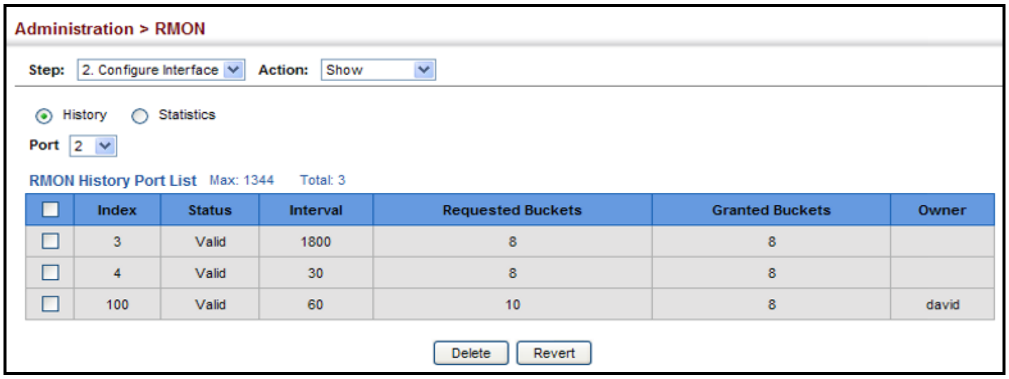
Port 2

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 220: Showing Configured RMON History Samples



Administration > RMON

Step: 2. Configure Interface Action: Show

● History ○ Statistics

Port 2

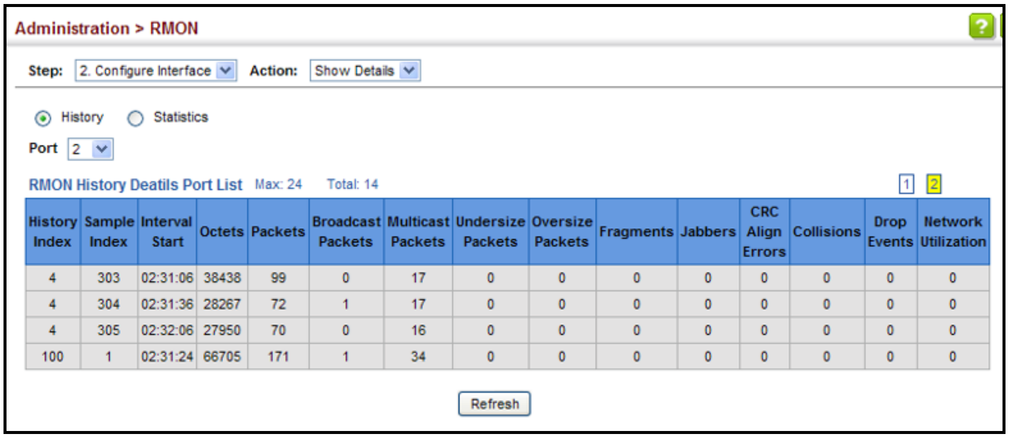
RMON History Port List Max: 1344 Total: 3

□	Index	Status	Interval	Requested Buckets	Granted Buckets	Owner
□	3	Valid	1800	8	8	
□	4	Valid	30	8	8	
□	100	Valid	60	10	8	david

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 221: Showing Collected RMON History Samples



Administration > RMON

Step: 2. Configure Interface Action: Show Details

● History ○ Statistics

Port 2

RMON History Deatils Port List Max: 24 Total: 14

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
4	303	02:31:06	38438	99	0	17	0	0	0	0	0	0	0	0
4	304	02:31:36	28267	72	1	17	0	0	0	0	0	0	0	0
4	305	02:32:06	27950	70	0	16	0	0	0	0	0	0	0	0
100	1	02:31:24	66705	171	1	34	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 649

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, collisioins, drop events, and frames of various sizes.

PARAMETERS

These parameters are displayed in the web interface:

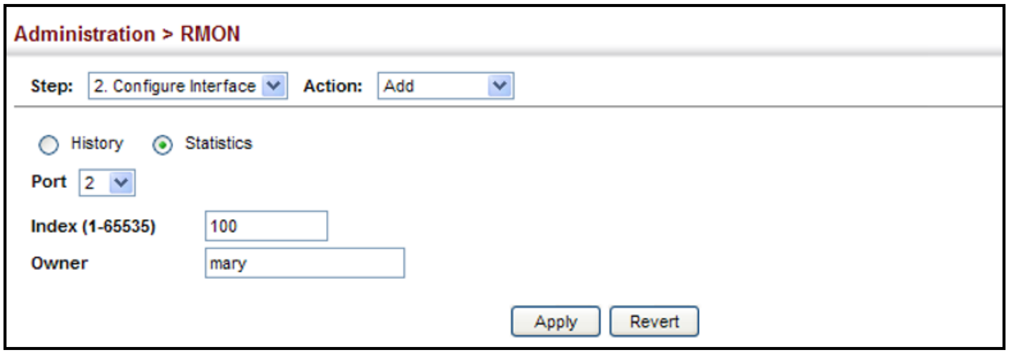
- **Port** – The port number on the switch.
- **Index** - Index to this entry. (Range: 1-65535)
- **Owner** - Name of the person who created this entry. (Range: 1-127 characters)

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 222: Configuring an RMON Statistical Sample



Administration > RMON

Step: 2. Configure Interface Action: Add

○ History ● Statistics

Port 2

Index (1-65535) 100

Owner mary

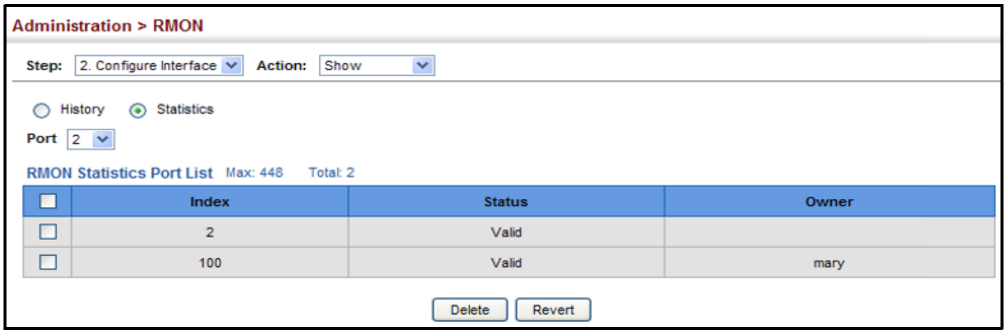
To show configured RMON statistical samples:

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 223: Showing Configured RMON Statistical Samples



Administration > RMON

Step: 2. Configure Interface Action: Show

○ History ● Statistics

Port 2

RMON Statistics Port List Max: 448 Total: 2

□	Index	Status	Owner
□	2	Valid	
□	100	Valid	mary

To show collected RMON statistical samples:

1. Click Administration, RMON.

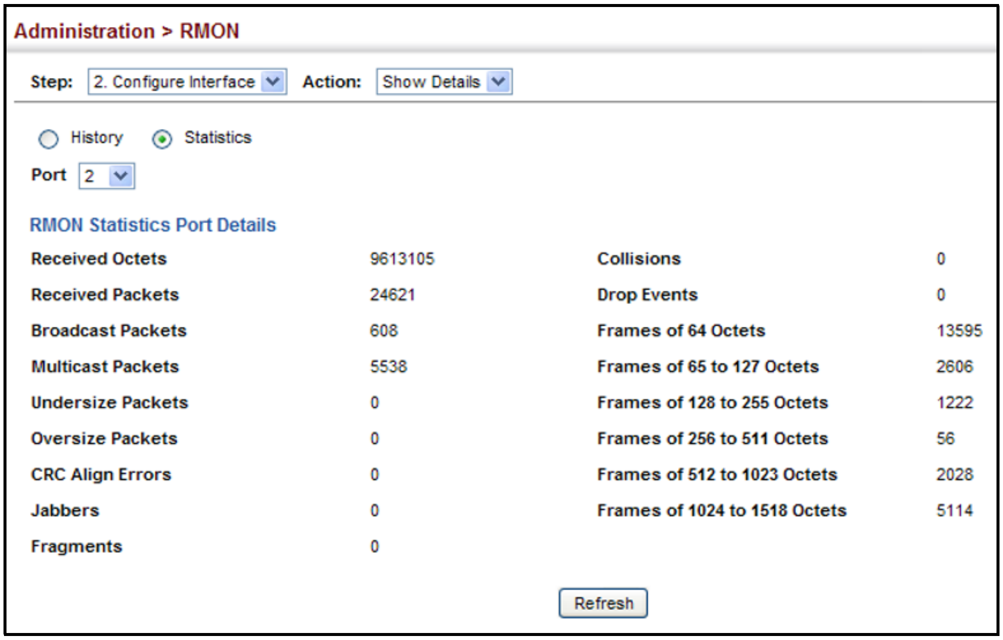
2. Select Configure Interface from the Step list.

3. Select Show Details from the Action list.

4. Select a port from the list.

5. Click Statistics.

Figure 224: Showing Collected RMON Statistical Samples



Administration > RMON

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		

15 Multicast Filtering

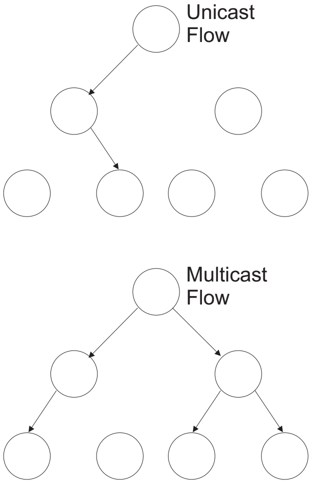
This chapter describes how to configure the following multicast servcies:

- Layer 2 IGMP – Configures snooping and query parameters.
- Filtering and Throttling – Filters specified multicast service, or throttling the maximum of multicast groups allowed on an interface.
- Layer 3 IGMP – Configures IGMP query used with multicast routing.
- Multicast VLAN Registration (MVR) – 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 225: 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).

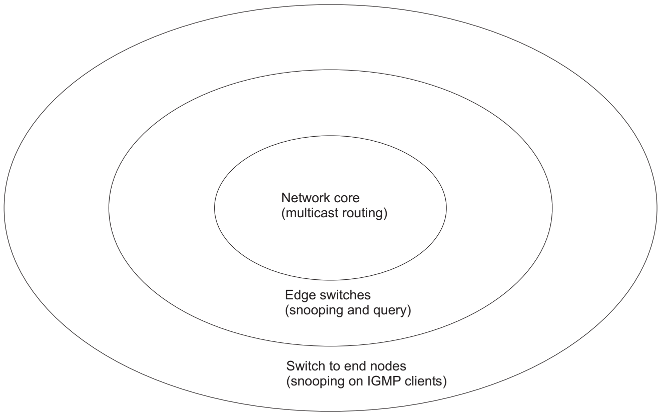
This switch not only supports IP multicast filtering by passively monitoring IGMP query, report messages and multicast routing probe messages to register end-stations as multicast group members, but also supports the Protocol Independent Multicasting (PIM) routing protocol required to forward multicast traffic to other subnets (page 1090).

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" on page 420.

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 226: IGMP Protocol



LAYER 2 IGMP (SNOOPING AND QUERY)

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 391) 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 a Multicast Router" on page 395). 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 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 391).

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 395). 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 397).

IGMP Snooping with Proxy Reporting – The switch supports last leave, and query suppression (as defined in DSL Forum TR-101, April 2006):

- 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 904

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-flooding is disabled (default behavior), or flooded throughout the VLAN if unregistered-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 in the web interface:

- **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: Disabled)

  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 399).

  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 neither specific queries nor general queries are forwarded from an upstream multicast router to hosts downstream from this device.

- **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.

- **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

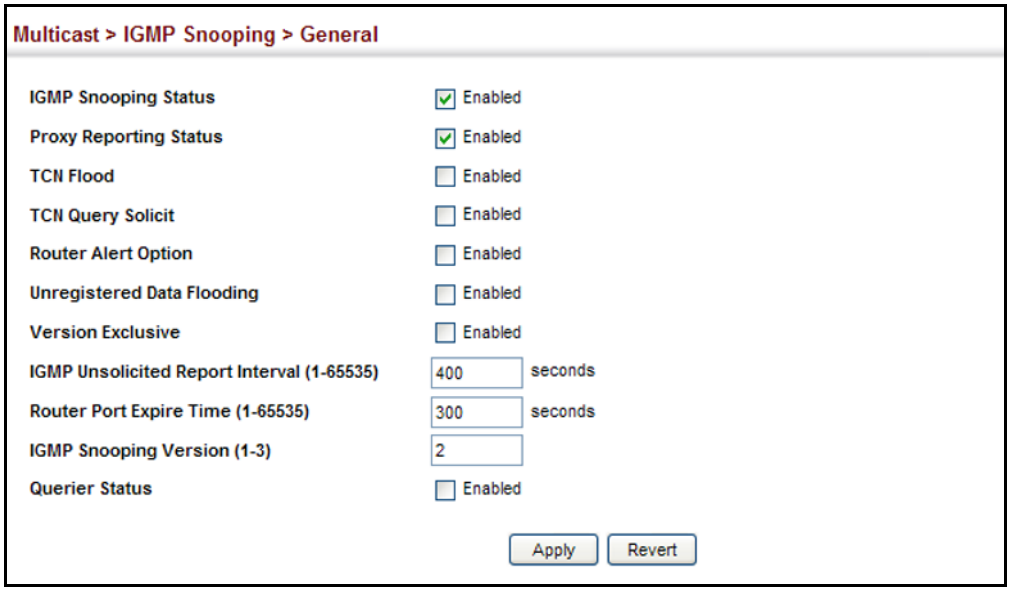
To configure general settings for IGMP Snooping and Query:

1. Click Multicast, IGMP Snooping, General.

2. Adjust the IGMP settings as required.

3. Click Apply.

Figure 227: 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
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 A MULTICAST ROUTER

Use the Multicast > IGMP Snooping > Multicast Router (Add Static Multicast Router) page to statically attach an 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 922

PARAMETERS

These parameters are displayed in the web interface:

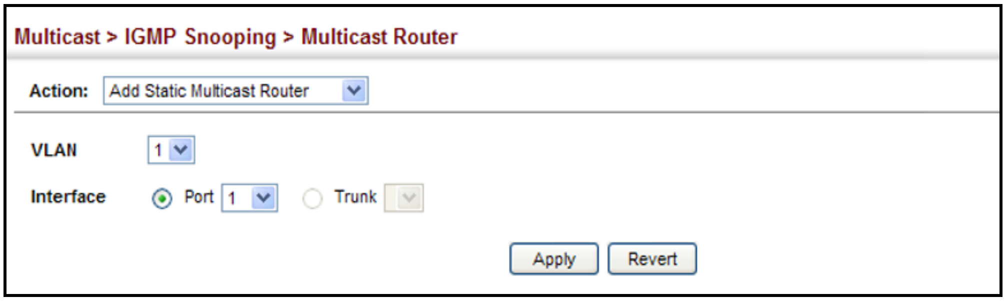
- **VLAN** – Selects the VLAN which is to propagate all multicast traffic coming from the attached multicast router. (Range: 1-4093)
- **Interface** – Activates the Port or Trunk scroll down list.
- **Port** or **Trunk** – Specifies the interface attached to a multicast router.

WEB INTERFACE

To specify a static interface attached to a multicast router:

1. Click Multicast, 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 228: Configuring a Static Interface for a Multicast Router



Multicast > IGMP Snooping > Multicast Router

Action: Add Static Multicast Router

VLAN 1

Interface ● Port 1 ○ Trunk

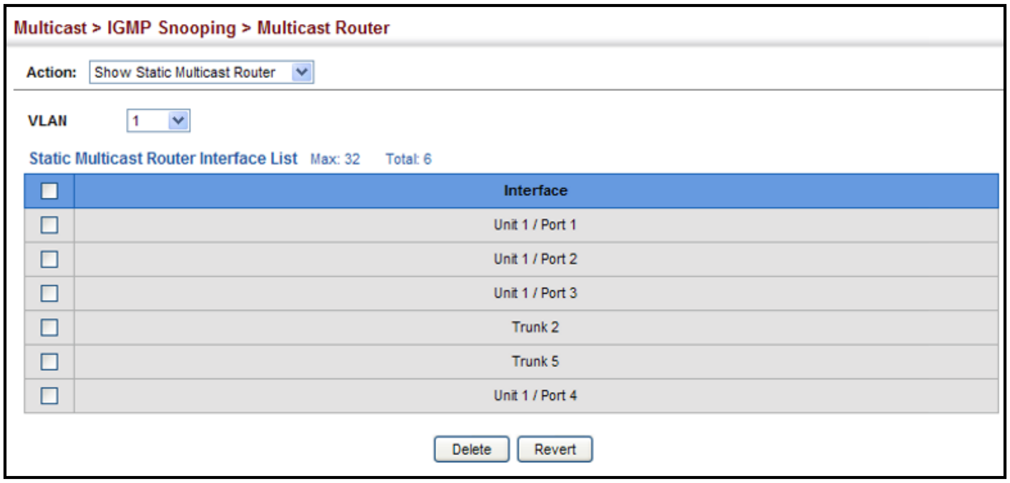
To show the static interfaces attached to a multicast router:

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 229: Showing Static Interfaces Attached a Multicast Router



Multicast > IGMP Snooping > Multicast Router

Action: Show Static Multicast Router

VLAN 1

Static Multicast Router Interface List Max: 32 Total: 6

□	Interface
□	Unit 1 / Port 1
□	Unit 1 / Port 2
□	Unit 1 / Port 3
□	Trunk 2
□	Trunk 5
□	Unit 1 / Port 4

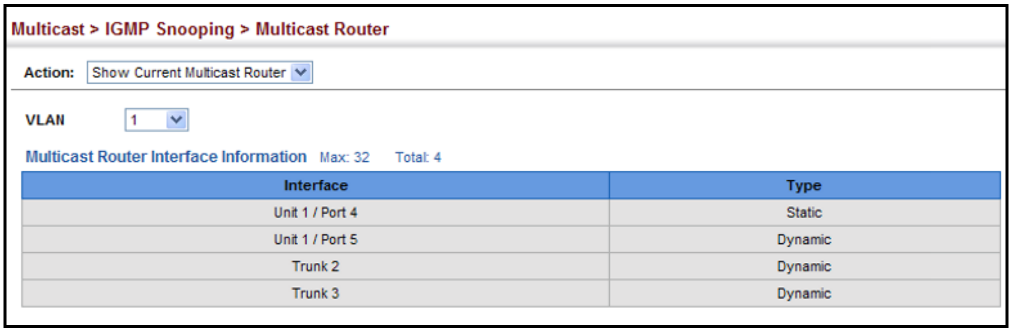
Multicast routers that are attached to ports on the switch use information obtained from IGMP, along with a multicast routing protocol (such as PIM) to support IP multicasting across the Internet. These routers may be dynamically discovered by the switch or statically assigned to an interface on the switch. To show all the interfaces attached to a multicast router:

1. Click Multicast, IGMP Snooping, Multicast Router.

2. Select 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 230: Showing Current Interfaces Attached a Multicast Router



Multicast > IGMP Snooping > Multicast Router

Action: Show Current Multicast Router

VLAN 1

Multicast Router Interface Information Max: 32 Total: 4

Interface	Type
Unit 1 / Port 4	Static
Unit 1 / Port 5	Dynamic
Trunk 2	Dynamic
Trunk 3	Dynamic

Assigning Interfaces to Multicast Services

Use the Multicast > IGMP Snooping > IGMP Member (Add Static Member) page to statically assign a 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 391). 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 919

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 in the web interface:

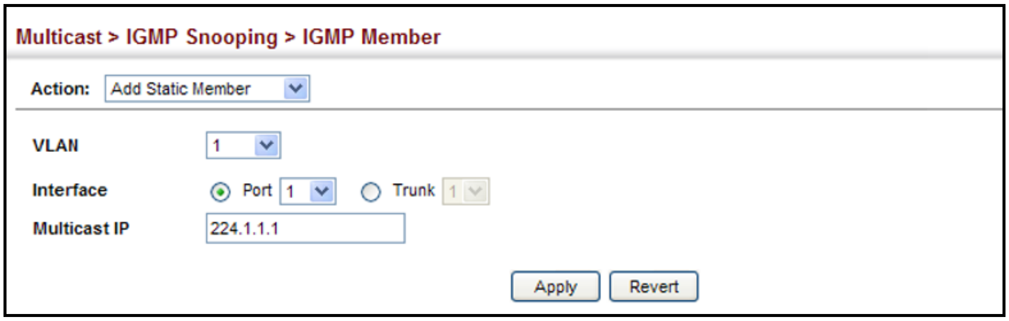
- **VLAN** – Specifies the VLAN which is to propagate the multicast service. (Range: 1-4093)
- **Interface** – Activates the Port or Trunk scroll down list.
- **Port** or **Trunk** – Specifies the interface assigned to a multicast group.
- **Multicast IP** – The IP address for a specific multicast service.

Web Interface

To statically assign an interface to a 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 231: Assigning an Interface to a Multicast Service



Multicast > IGMP Snooping > IGMP Member

Action: Add Static Member

VLAN: 1

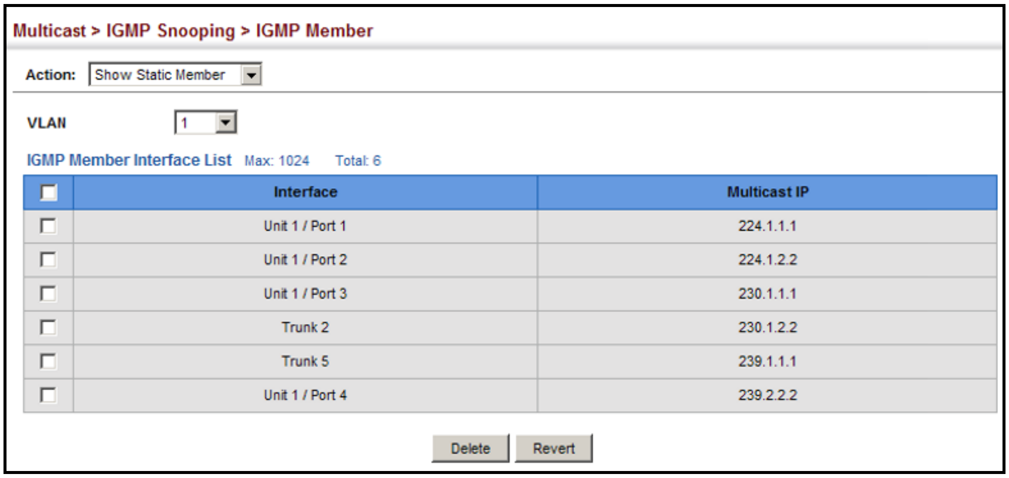
Interface: ● Port 1 ○ Trunk 1

Multicast IP: 224.1.1.1

To show the static interfaces assigned to a 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 232: Showing Static Interfaces Assigned to a Multicast Service



Multicast > IGMP Snooping > IGMP Member

Action: Show Static Member

VLAN: 1

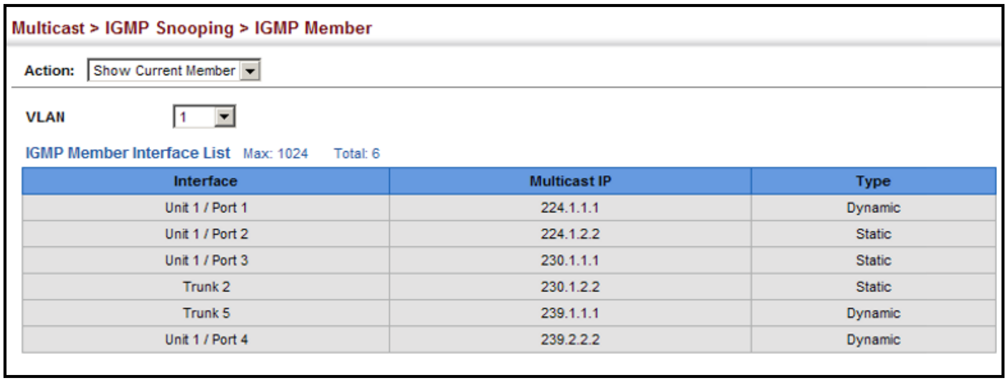
IGMP Member Interface List Max: 1024 Total: 6

□	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

To display information about all multicast groups, IGMP Snooping or multicast routing must first be enabled on the switch. To show all of the interfaces statically or dynamically assigned to a multicast service:

1. Click Multicast, IGMP Snooping, IGMP Member.
2. Select Show Current Member from the Action list.
3. Select the VLAN for which to display this information.

Figure 233: Showing Current Interfaces Assigned to a Multicast Service



Multicast > IGMP Snooping > IGMP Member

Action: Show Current Member

VLAN 1

IGMP Member Interface List Max: 1024 Total: 6

Interface	Multicast IP	Type
Unit 1 / Port 1	224.1.1.1	Dynamic
Unit 1 / Port 2	224.1.2.2	Static
Unit 1 / Port 3	230.1.1.1	Static
Trunk 2	230.1.2.2	Static
Trunk 5	239.1.1.1	Dynamic
Unit 1 / Port 4	239.2.2.2	Dynamic

SETTING IGMP SNOOPING STATUS PER INTERFACE

Use the Multicast > IGMP Snooping > Interface (Configure) page to configure IGMP snooping attributes for a VLAN interface. To configure snooping globally, refer to "Configuring IGMP Snooping and Query Parameters" on page 391.

CLI REFERENCES

- "IGMP Snooping" on page 904

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 in the web interface:

- **VLAN** – ID of configured VLANs. (Range: 1-4093)

- **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: Disabled)

  When IGMP snooping is enabled globally (see page 391), 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 defined by 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: Enabled)

- **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 neither specific queries nor general queries are forwarded from an upstream multicast router to hosts downstream from this device.

If proxy reporting is disabled, report suppression can still be configured by a separate attribute as described above.

- **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 391), or as a proxy host when IGMP snooping proxy reporting is enabled (page 391).

- **Query Response Interval** – The maximum time the system waits for a response to proxy general queries. (Range: 10-31744 tenths of a second; Default: 10 seconds)

  This attribute applies when the switch is serving as the querier (page 391), or as a proxy host when IGMP snooping proxy reporting is enabled (page 391).

- **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 391).

- **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).

WEB INTERFACE

To configure IGMP snooping on a VLAN:

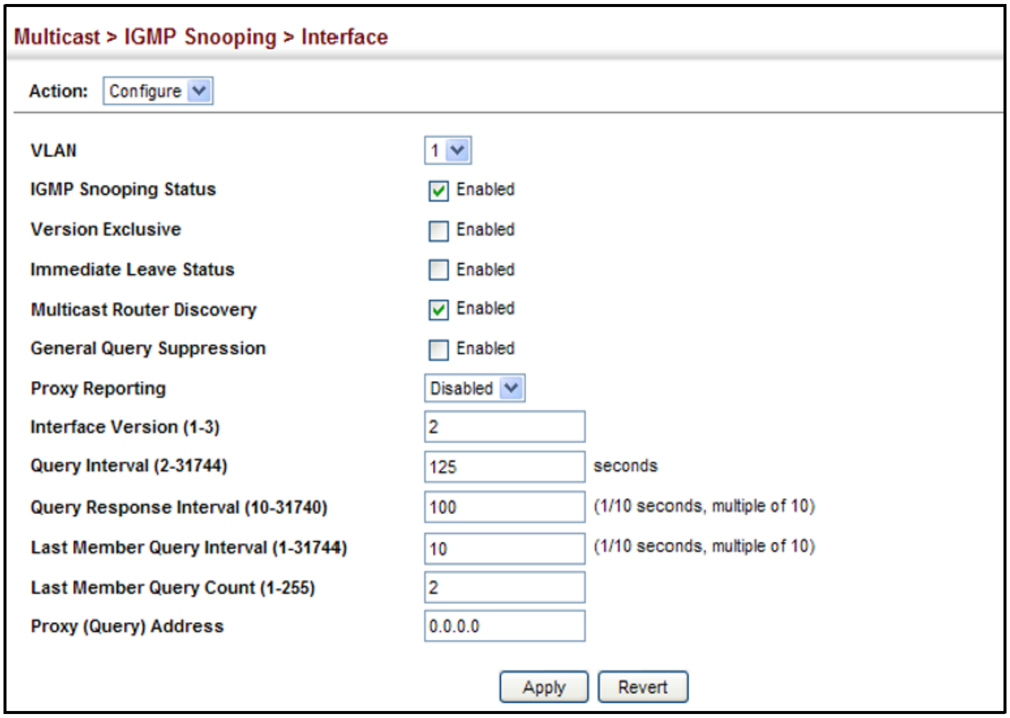
1. Click Multicast, IGMP Snooping, Interface.

2. Select Configure from the Action list.

3. Select the VLAN to configure and update the required parameters.

4. Click Apply.

Figure 234: Configuring IGMP Snooping on an Interface



Multicast > IGMP Snooping > Interface

Action: Configure

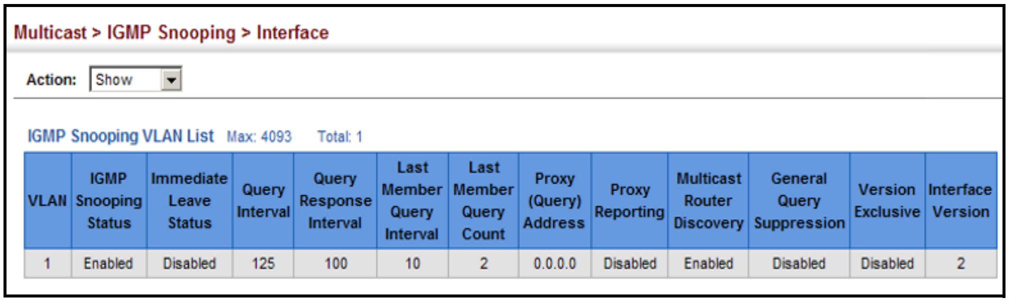
VLAN	1
IGMP Snooping Status	☑ Enabled
Version Exclusive	□ Enabled
Immediate Leave Status	□ Enabled
Multicast Router Discovery	☑ Enabled
General Query Suppression	□ Enabled
Proxy Reporting	Disabled
Interface Version (1-3)	2
Query Interval (2-31744)	125 seconds
Query Response Interval (10-31740)	100 (1/10 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 from the Action list.

Figure 235: Showing Interface Settings for IGMP Snooping



Multicast > IGMP Snooping > Interface

Action: Show

IGMP Snooping VLAN List Max: 4093 Total: 1

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	125	100	10	2	0.0.0.0	Disabled	Enabled	Disabled	Disabled	2

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 920

COMMAND USAGE

To display information about multicast groups, IGMP Snooping must first be enabled on the switch (see page 391).

PARAMETERS

These parameters are displayed in the web interface:

- **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.

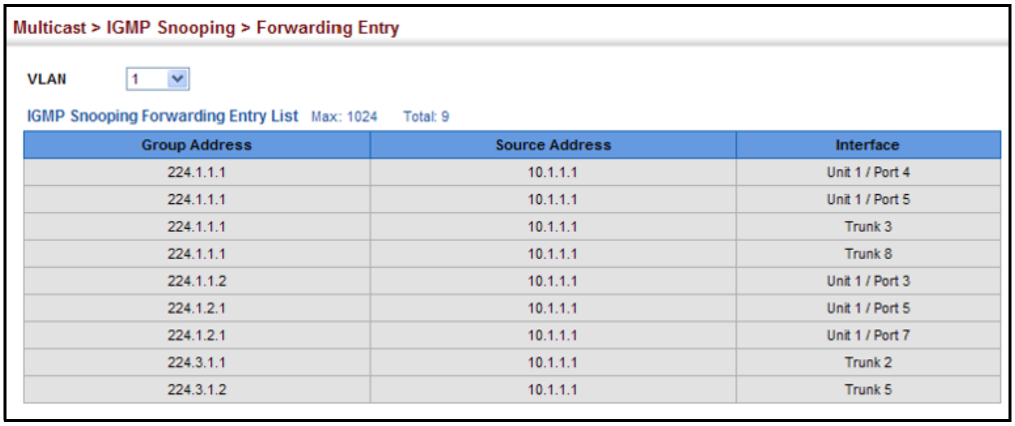
WEB INTERFACE

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 236: Showing Multicast Groups Learned by IGMP Snooping



Multicast > IGMP Snooping > Forwarding Entry
VLAN
1
IGMP Snooping Forwarding Entry List Max: 1024 Total: 9

Group Address	Source Address	Interface
224.1.1.1	10.1.1.1	Unit 1 / Port 4
224.1.1.1	10.1.1.1	Unit 1 / Port 5
224.1.1.1	10.1.1.1	Trunk 3
224.1.1.1	10.1.1.1	Trunk 8
224.1.1.2	10.1.1.1	Unit 1 / Port 3
224.1.2.1	10.1.1.1	Unit 1 / Port 5
224.1.2.1	10.1.1.1	Unit 1 / Port 7
224.3.1.1	10.1.1.1	Trunk 2
224.3.1.2	10.1.1.1	Trunk 5

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 924

PARAMETERS

These parameters are displayed in the web interface:

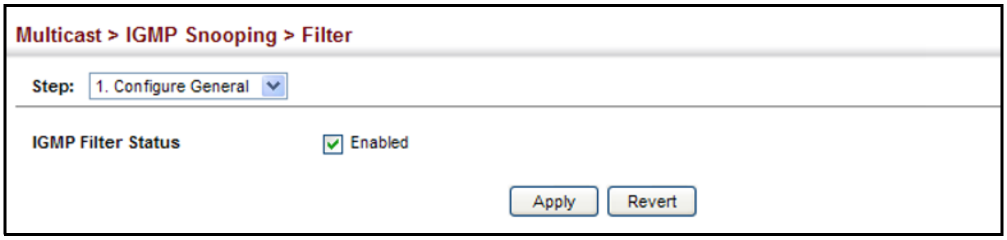
- **IGMP Filter Status** – Enables IGMP filtering and throttling globally for the switch. (Default: Disabled)

WEB INTERFACE

To enables IGMP filtering and throttling on the switch:

1. Click Multicast, IGMP Snooping, Filtering.
2. Select Configure General from the Action list.
3. Enable IGMP Filter Status.
4. Click Apply.

Figure 237: 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 (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 923

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 in the web interface:

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

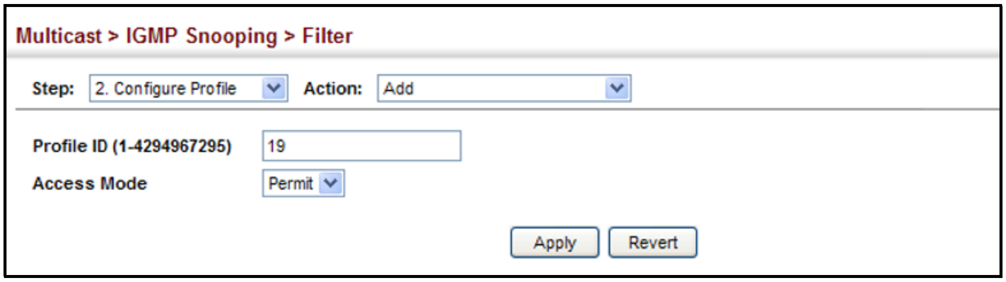
- **Profile ID** – Selects an IGMP profile to configure.
- **Start Multicast IP Address** – Specifies the starting address of a range of multicast groups.
- **End Multicast IP Address** – Specifies the ending address of a range of multicast groups.

WEB INTERFACE

To create an IGMP filter profile and set its access mode:

1. Click Multicast, IGMP Snooping, Filtering.
2. Select Add from the Action list.
3. Enter the number for a profile, and set its access mode.
4. Click Apply.

Figure 238: Creating an IGMP Filtering Profile



Multicast > IGMP Snooping > Filter

Step: 2. Configure Profile Action: Add

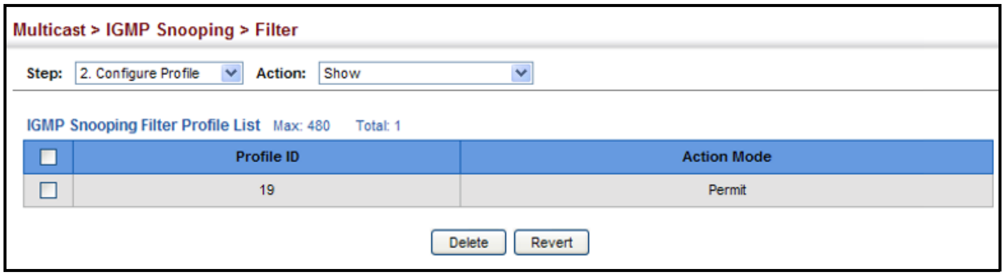
Profile ID (1-4294967295) 19

Access Mode Permit

To show the IGMP filter profiles:

1. Click Multicast, IGMP Snooping, Filtering.
2. Select Show from the Action list.

Figure 239: Showing the IGMP Filtering Profiles Created



Multicast > IGMP Snooping > Filter

Step: 2. Configure Profile Action: Show

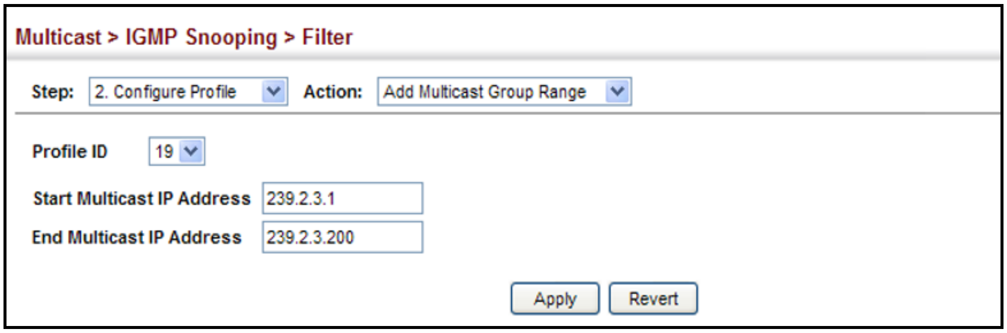
IGMP Snooping Filter Profile List Max: 480 Total: 1

□	Profile ID	Action Mode
□	19	Permit

To add a range of multicast groups to an IGMP filter profile:

1. Click Multicast, IGMP Snooping, Filtering.
2. Select Add Multicast Group Range from the Action list.
3. Select the profile to configure, and add a multicast group address or range of addresses.
4. Click Apply.

Figure 240: Adding Multicast Groups to an IGMP Filtering Profile



Multicast > IGMP Snooping > Filter

Step: 2. Configure Profile   Action: Add Multicast Group Range

Profile ID: 19

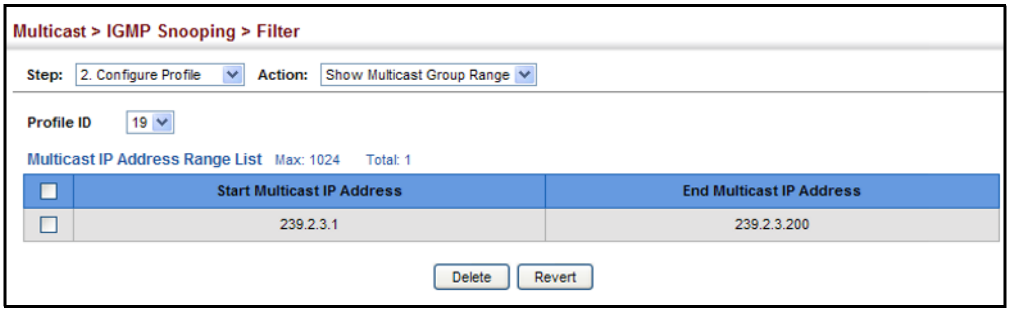
Start Multicast IP Address: 239.2.3.1

End Multicast IP Address: 239.2.3.200

To show the multicast groups configured for an IGMP filter profile:

1. Click Multicast, IGMP Snooping, Filtering.
2. Select Show Multicast Group Range from the Action list.
3. Select the profile for which to display this information.

Figure 241: Showing the Groups Assigned to an IGMP Filtering Profile



Multicast > IGMP Snooping > Filter

Step: 2. Configure Profile   Action: Show Multicast Group Range

Profile ID: 19

Multicast IP Address Range List Max: 1024 Total: 1

□	Start Multicast IP Address	End Multicast IP Address
□	239.2.3.1	239.2.3.200

CONFIGURING IGMP FILTERING AND THROTTLING FOR INTERFACES

Use the Multicast > IGMP Snooping > 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 923

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 in the web interface:

- **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:

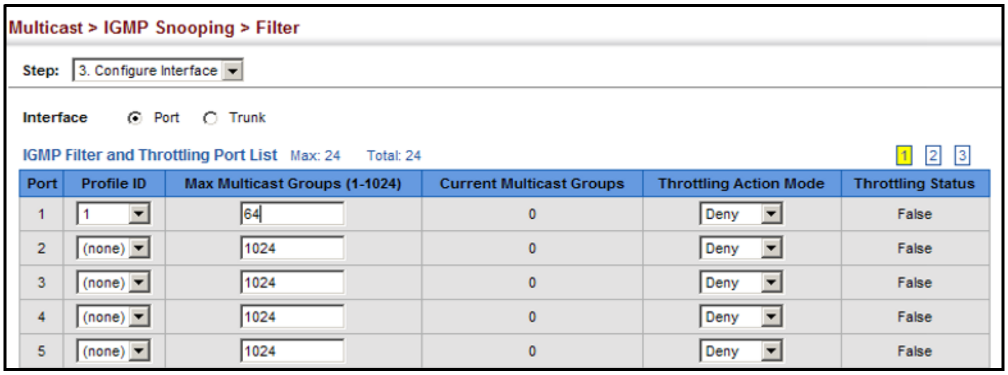
1. Click Multicast, IGMP Snooping, Filtering.

2. Select Configure Interface from the Action 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 242: Configuring IGMP Filtering and Throttling Interface Settings



Multicast > IGMP Snooping > Filter

Step: 3. Configure Interface

Interface ● Port ○ Trunk

IGMP Filter and Throttling Port List Max: 24 Total: 24

Port	Profile ID	Max Multicast Groups (1-1024)	Current Multicast Groups	Throttling Action Mode	Throttling Status
1	1	64	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

LAYER 3 IGMP (QUERY USED WITH MULTICAST ROUTING)

IGMP Snooping – IGMP Snooping (page 391) 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 413).

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 399.)

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

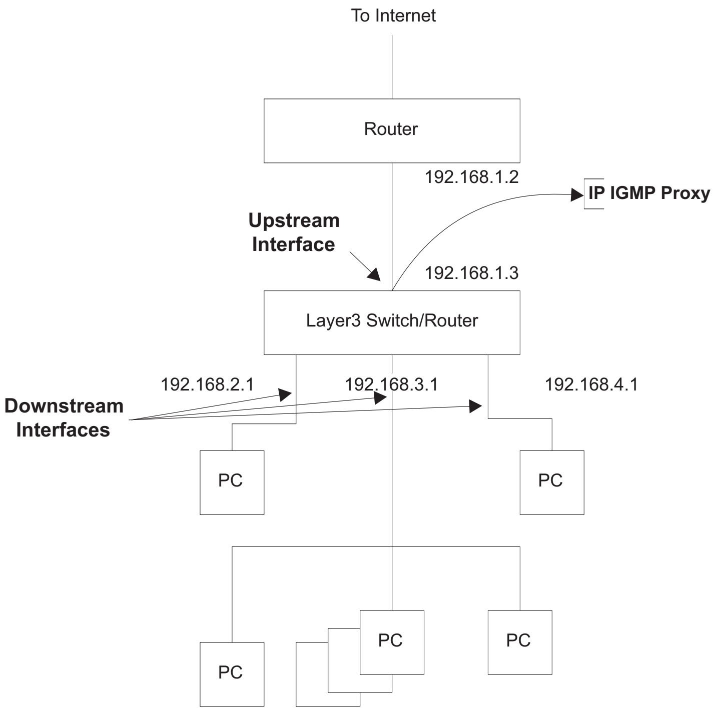
Use the Multicast > IGMP > Proxy page to configure IGMP Proxy Routing.

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 947

Figure 243: 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 544).

2. Enable IGMP on the downstream interfaces which require proxy multicast service (see "Configuring IGMP Interface Parameters" on page 413).

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 in the web interface:

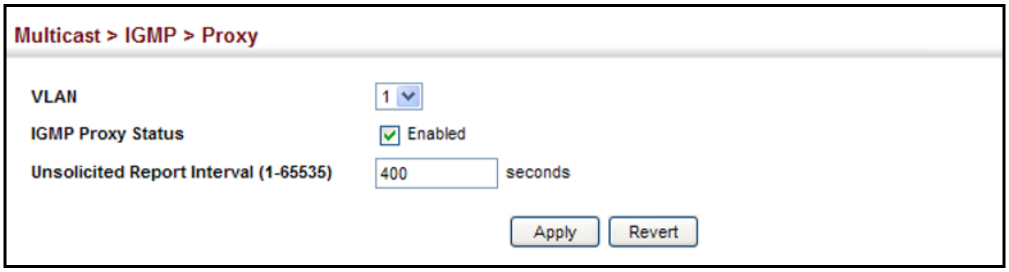
- **VLAN** – VLAN interface on which to configure IGMP proxy service. (Range: 1-4093)
- **IGMP Proxy Status** – Enables IGMP proxy service for multicast routing, forwarding IGMP membership information monitored on downstream interfaces onto the upstream interface in a summarized report. (Default: Disabled)
- **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 244: 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 544).

CLI REFERENCES

- "IGMP (Layer 3)" on page 937

PARAMETERS

These parameters are displayed in the web interface:

- **VLAN** – VLAN interface bound to a primary IP address. (Range: 1-4093)
- **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: 0-255 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

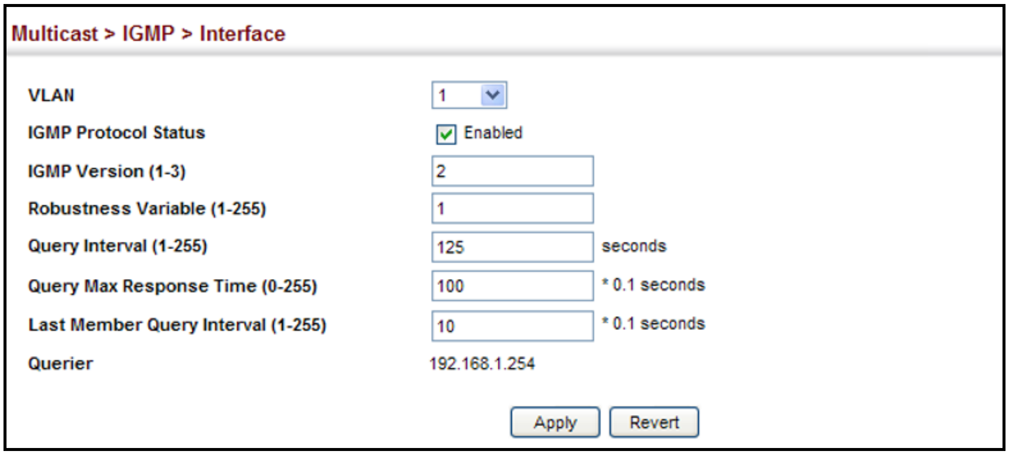
To configure IGMP interface settings:

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 245: 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 941

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 in the web interface:

- **VLAN** – VLAN interface to assign as a static member of the specified multicast group. (Range: 1-4093)

- **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:

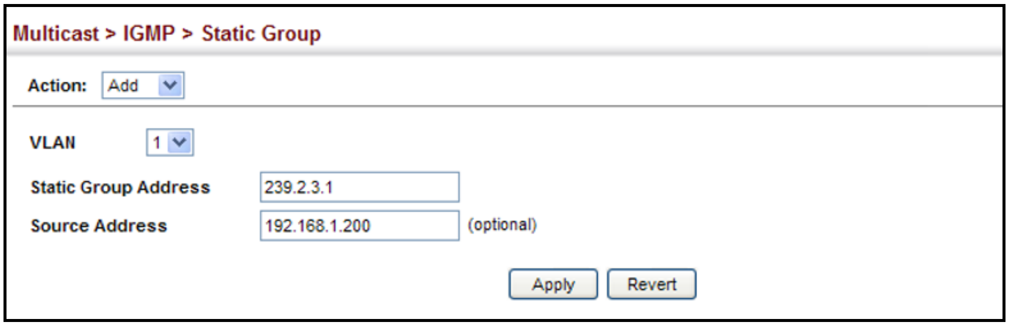
1. Click Multicast, IGMP, Static Group.

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 246: 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)

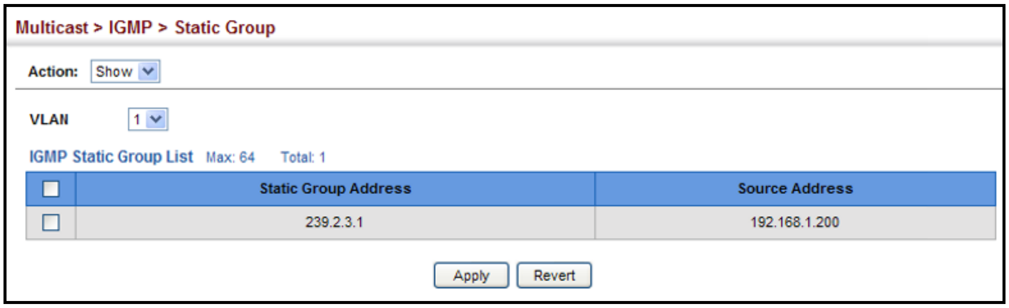
To display configured static IGMP groups:

1. Click Multicast, IGMP, Static Group.

2. Select Show from the Action list.

3. Click Apply.

Figure 247: Showing Static IGMP Groups



Multicast > IGMP > Static Group

Action: Show

VLAN 1

IGMP Static Group List Max: 64 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 404).

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 413), and multicast routing must be enabled globally on the system (see "Configuring Global Settings for Multicast Routing" on page 544).

CLI REFERENCES

- "show ip igmp groups" on page 944

PARAMETERS

These parameters are displayed in the web interface:

Show Information

- **VLAN** – VLAN identifier. The selected entry must be a configured IP interface. (Range: 1-4093)
- **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 Detail

The following additional information is displayed on this page:

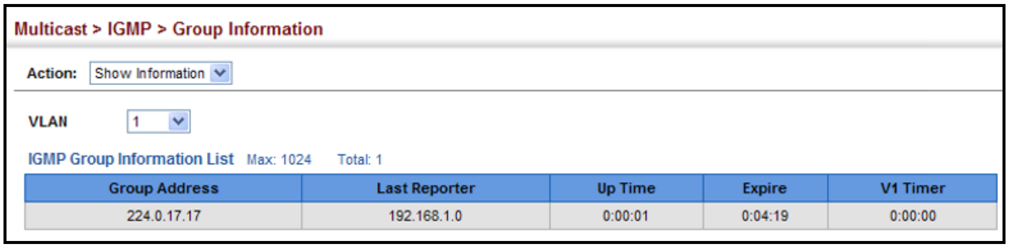
- **Group Address** – IP multicast group address with subscribers directly attached or downstream from the switch, or a static multicast group assigned to this interface.
- **Interface** – The interface on the switch that has received traffic directed to the multicast group address.
- **Group Mode** – 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.
  - **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 248: Displaying Multicast Groups Learned from IGMP (Information)



Multicast > IGMP > Group Information

Action: Show Information

VLAN 1

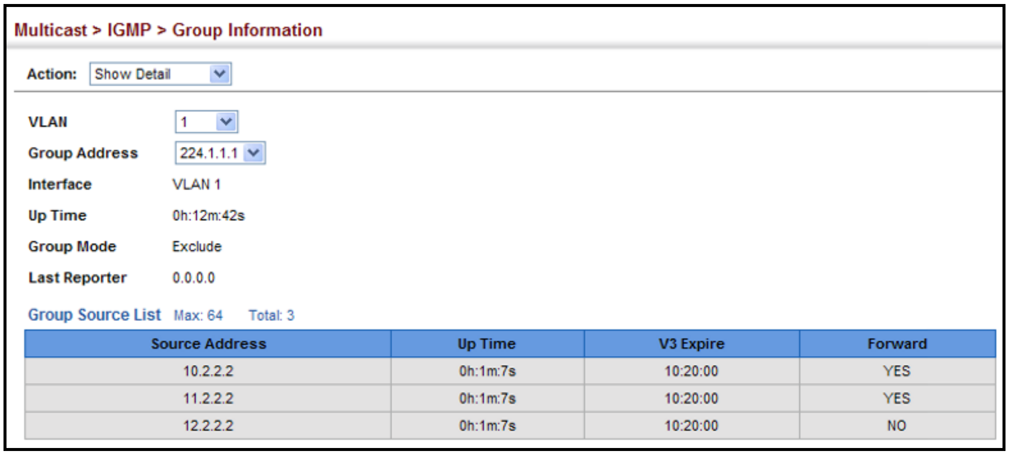
IGMP Group Information List Max: 1024 Total: 1

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 Detail from the Action list.
3. Select a VLAN. The selected entry must be a configured IP interface.

Figure 249: 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 Max: 64 Total: 3

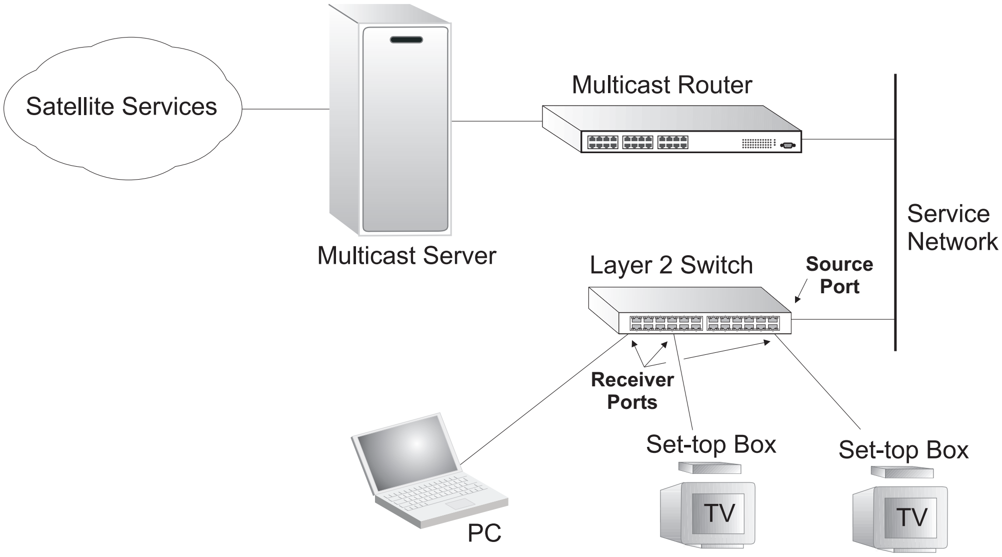
Source Address	Up Time	V3 Expire	Forward
10.2.2.2	0h:1m:7s	10:20:00	YES
11.2.2.2	0h:1m:7s	10:20:00	YES
12.2.2.2	0h:1m:7s	10:20:00	NO

MULTICAST VLAN REGISTRATION

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 250: MVR Concept



COMMAND USAGE

- General Configuration Guidelines for MVR:

  1. Enable MVR globally on the switch, select the MVR VLAN, and add the multicast groups that will stream traffic to attached hosts (see "Configuring Global MVR Settings" on page 422).

  2. Set the interfaces that will join the MVR as source ports or receiver ports (see "Configuring MVR Interface Status" on page 424).

  3. 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 Multicast Groups to Interfaces" on page 427).

- 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 GLOBAL MVR SETTINGS

Use the Multicast > MVR (Configure General) 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

- "Multicast VLAN Registration" on page 930

PARAMETERS

These parameters are displayed in the web interface:

- **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 158), 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 424).

- **MVR Current Groups** – The number of multicast groups currently assigned to the MVR VLAN.

- **MVR Max Supported Groups** – The maximum number of multicast groups supported by this switch.

  IGMP snooping and MVR share a maximum number of 255 groups. Any multicast streams received in excess of this limitation will be flooded to all ports in the associated VLAN.

WEB INTERFACE

To configure global settings for MVR:

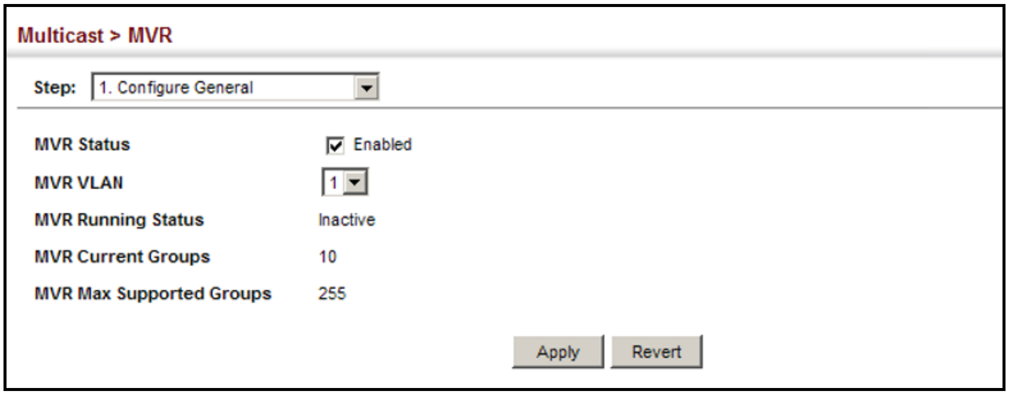
1. Click Multicast, MVR.

2. Select Configure General from the Action list.

3. Enable MVR globally on the switch, and select the MVR VLAN.

4. Click Apply.

Figure 251: Configuring Global Settings for MVR



Multicast > MVR

Step: 1. Configure General

MVR Status ☑ Enabled

MVR VLAN 1

MVR Running Status Inactive

MVR Current Groups 10

MVR Max Supported Groups 255

CONFIGURING THE MVR GROUP RANGE

Use the Multicast > MVR (Configure Group Range) page to assign the multicast group address for each service to the MVR VLAN.

CLI REFERENCES

- "Multicast VLAN Registration" on page 930

COMMAND USAGE

IGMP snooping and MVR share a maximum number of 255 groups. Any multicast streams received in excess of this limitation will be flooded to all ports in the associated VLAN.

PARAMETERS

These parameters are displayed in the web interface:

- **MVR Group IP** – IP address for an MVR multicast group. (Range: 224.0.1.0 - 239.255.255.255; Default: no groups are assigned to the MVR VLAN)

  Any multicast data sent to this address is sent to all source ports on the switch and all receiver ports that have elected to receive data on that multicast address.

  The IP address range of 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 255 groups. Any multicast streams received in excess of this limitation will be flooded to all ports in the associated VLAN.

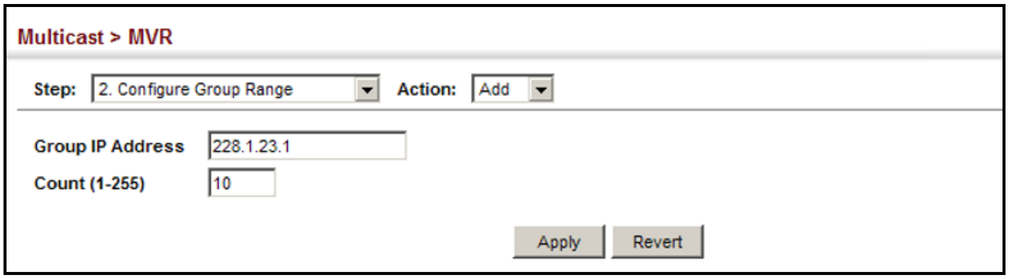
- **Count** – The number of contiguous MVR group addresses. (Range: 1-255; Default: 0)

WEB INTERFACE

To configure multicast groups for the MVR VLAN:

1. Click Multicast, MVR.
2. Select Configure Group Range from the Step list.
3. Select Add from the Action list.
4. Add the multicast groups that will stream traffic to participating hosts.
5. Click Apply.

Figure 252: Configuring the Group Range for MVR



Multicast > MVR

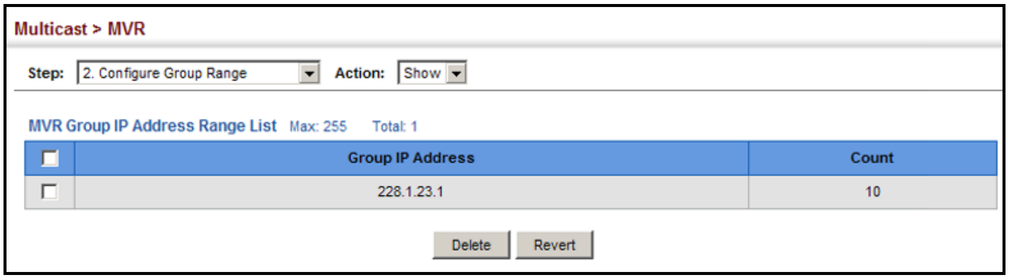
Step: 2. Configure Group Range Action: Add

Group IP Address: 228.1.23.1
Count (1-255): 10

To show the multicast groups assigned to the MVR VLAN:

1. Click Multicast, MVR.
2. Select Configure Group Range from the Step list.
3. Select Show from the Action list.

Figure 253: Showing the Configured Group Range for MVR



Multicast > MVR

Step: 2. Configure Group Range Action: Show

MVR Group IP Address Range List Max: 255 Total: 1

□	Group IP Address	Count
□	228.1.23.1	10

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

- "Multicast VLAN Registration" on page 930

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. IGMP snooping is used to allow 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 Multicast Groups to Interfaces" on page 427).

  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 Multicast Groups to Interfaces" on page 427).

  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 in the web interface:

- **Port** – Port 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 158).

  - **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 Multicast Groups to Interfaces" on page 427).

- **Non-MVR** – An interface that does not participate in the MVR VLAN. (This is the default type.)

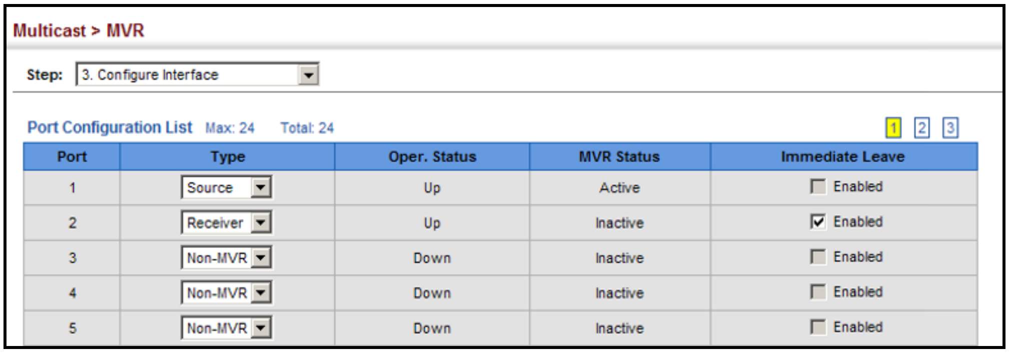
- **Oper. Status** – Shows the link status.
- **MVR Status** – Shows the MVR status. MVR status for source ports is "Active" if MVR is globally enabled on the switch. MVR status for receiver ports is "Active" only if there are subscribers receiving multicast traffic from one of the MVR groups, or a multicast 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 Action list.
3. 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.
4. Click Apply.

Figure 254: Configuring Interface Settings for MVR



Multicast > MVR

Step: 3. Configure Interface

Port Configuration List Max: 24 Total: 24

Port	Type	Oper. Status	MVR Status	Immediate Leave
1	Source	Up	Active	☐ Enabled
2	Receiver	Up	Inactive	☑ Enabled
3	Non-MVR	Down	Inactive	☐ Enabled
4	Non-MVR	Down	Inactive	☐ Enabled
5	Non-MVR	Down	Inactive	☐ Enabled

ASSIGNING STATIC 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 934

PARAMETERS

These parameters are displayed in the web interface:

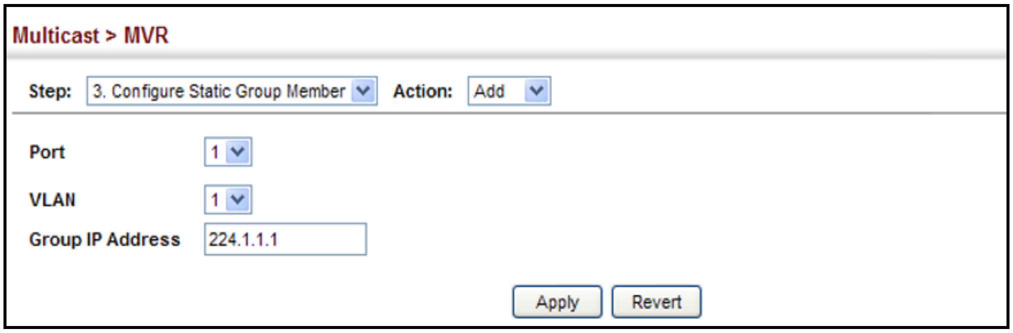
- **Port** – Port identifier.
- **VLAN** – VLAN identifier
- **Group IP Address** – Defines a multicast service sent to the selected port. Multicast groups must be assigned from the MVR group range configured on the Configure General page.

WEB INTERFACE

To assign a static MVR group to a port:

1. Click Multicast, MVR.
2. Select Configure Static Group Member from the Step list.
3. Select Add from the Action list.
4. Select a VLAN and port member to receive the multicast stream, and then enter the multicast group address.
5. Click Apply.

Figure 255: Assigning Static MVR Groups to a Port


Multicast > MVR

Step: 3. Configure Static Group Member Action: Add

Port: 1

VLAN: 1

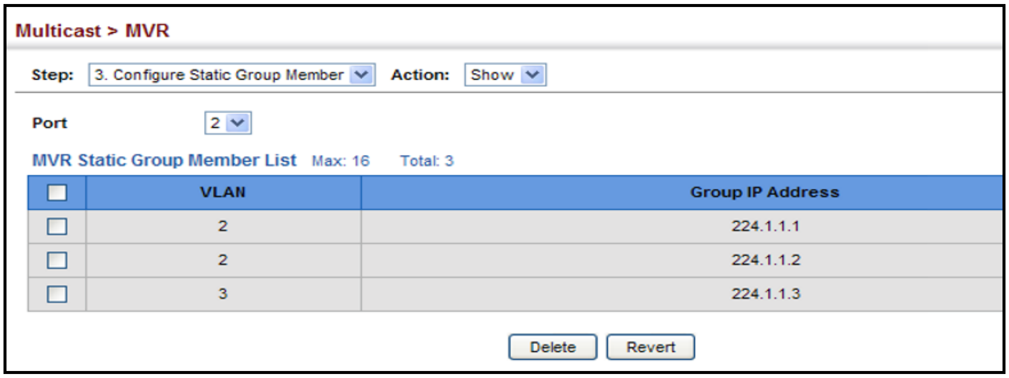
Group IP Address: 224.1.1.1

To show the static MVR groups assigned to a port:

1. Click Multicast, MVR.
2. Select Configure Static Group Member from the Step list.
3. Select Show from the Action list.

4. Select the port for which to display this information.

Figure 256: Showing the Static MVR Groups Assigned to a Port



Multicast > MVR

Step: 3. Configure Static Group Member Action: Show

Port: 2

MVR Static Group Member List Max: 16 Total: 3

□	VLAN	Group IP Address
□	2	224.1.1.1
□	2	224.1.1.2
□	3	224.1.1.3

Showing Multicast Groups Assigned to Interfaces

Use the Multicast > MVR (Show Member) page to show the multicast groups either statically or dynamically assigned to the MVR VLAN on each interface.

CLI References

- "show mvr" on page 935

Parameters

These parameters are displayed in the web interface:

Group IP Address – Multicast groups assigned to the MVR VLAN.

Source IP Address – Indicates the source address of the multicast service, or displays an asterisk if the group address has been statically assigned.

VLAN – Indicates the MVR VLAN receiving the multicast service.

Forwarding Port – Shows the interfaces with subscribers for multicast services provided through the MVR VLAN. Also shows 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.

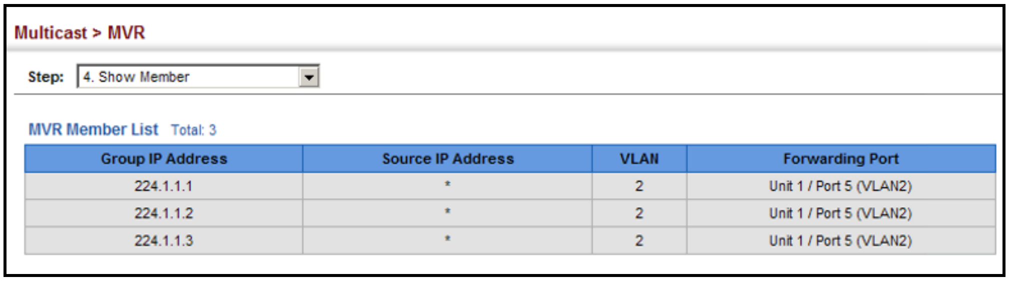
Web Interface

To show all MVR groups assigned to a port:

1. Click Multicast, MVR.

2. Select Show Member from the Step list.

Figure 257: Showing All MVR Groups Assigned to a Port



Step: 4. Show Member

MVR Member List Total: 3

Group IP Address	Source IP Address	VLAN	Forwarding Port
224.1.1.1	*	2	Unit 1 / Port 5 (VLAN2)
224.1.1.2	*	2	Unit 1 / Port 5 (VLAN2)
224.1.1.3	*	2	Unit 1 / Port 5 (VLAN2)

16 IP Configuration

This chapter describes how to configure an initial IP interface for management access to the switch over the network. You can manually configure a specific address or direct the switch to obtain an address from a BOOTP or DHCP server when it is powered on.

Setting the Switch's IP Address (IP Version 4)

Use the IP > General > Routing Interface (Add) page to configure an address for the switch. An 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

- "Basic IP Configuration" on page 1006
- "DHCP Client" on page 979

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 447) or use dynamic routing; i.e., RIP or OSPFv2 (page 484 or 502 respectively).
- The precedence for configuring IP interfaces is the IP > General > Routing Interface (Add) menu, static routes (page 447), and then dynamic routing.

PARAMETERS

These parameters are displayed in the web interface:

- **VLAN** – ID of the configured VLAN (1-4093). 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 (Static), 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** – Specfies a primary or seconday 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 in a network segment uses a secondary address, all other routers in that segment must also use a secondary address from the same network or subnet address space.
- **IP Address** – IP Address of the VLAN. Valid IP addresses consist of four numbers, 0 to 255, separated by periods. (Default: 0.0.0.0)

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.
- **Restart DHCP** – Requests a new IP address from the DHCP server for all enabled VLANs.

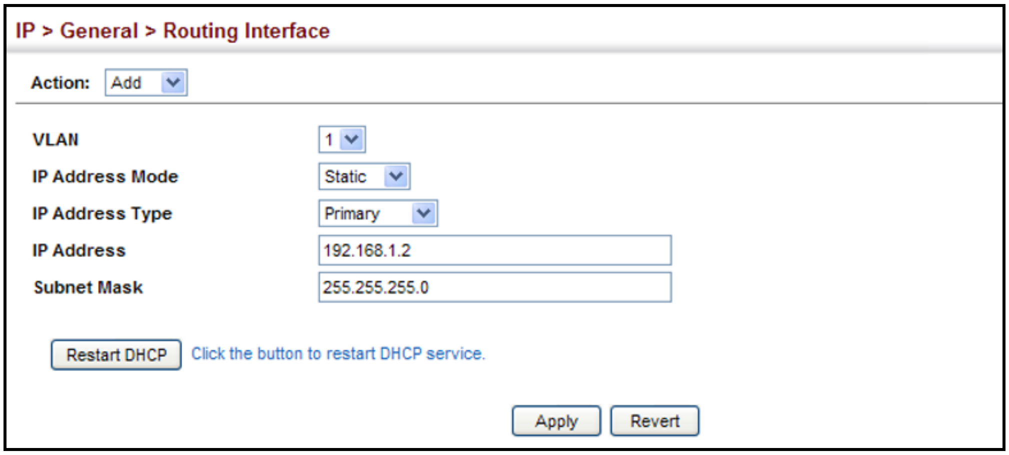
WEB INTERFACE

To set a static address for the switch:

1. Click IP, General, Routing Interface.
2. Select Add from the Action list.
3. Select any configured VLAN, set IP Address Mode to "Static," 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 258: Configuring a Static Address



IP > General > Routing Interface

Action: Add

VLAN: 1

IP Address Mode: Static

IP Address Type: Primary

IP Address: 192.168.1.2

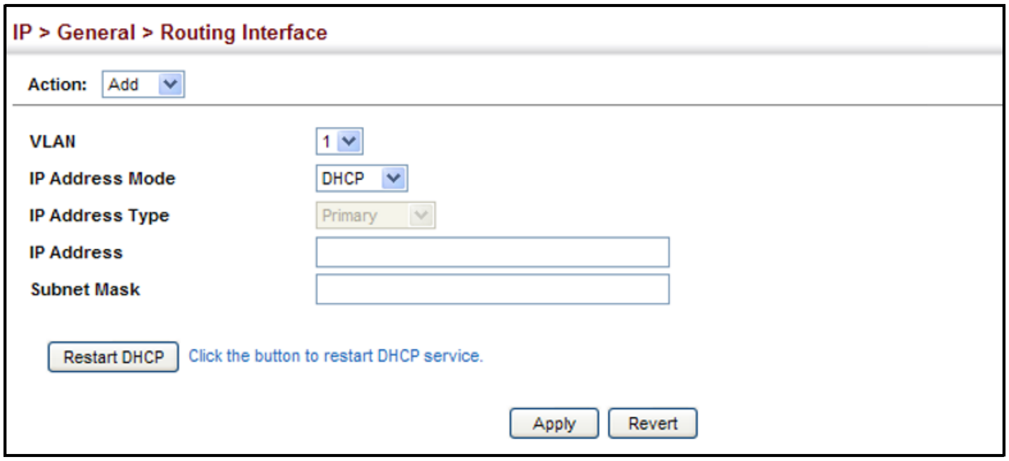
Subnet Mask: 255.255.255.0

To obtain an dynamic address through DHCP/BOOTP for the switch:

1. Click IP, General, Routing Interface.
2. Select Add 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.

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 259: Configuring a Dynamic Address



IP > General > Routing Interface

Action: Add

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.

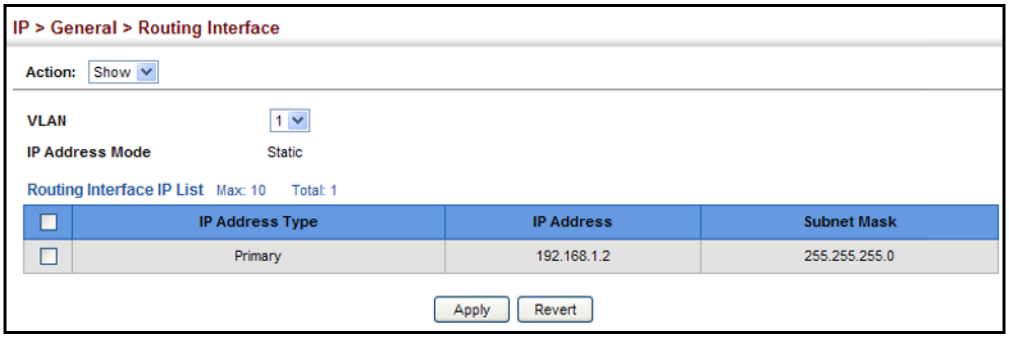
Renewing DCHP – DHCP may lease addresses to clients indefinitely or for a specific period of time. If the address expires or the switch is moved to another network segment, you will lose management access to the switch. In this case, you can reboot the switch or submit a client request to restart DHCP 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 address configured for an interface:

1. Click IP, General, Routing Interface.
2. Select Add from the Action list.
3. Select an entry from the VLAN list.

Figure 260: Showing the Configured IP Address for an Interface



IP > General > Routing Interface

Action: Show

VLAN: 1
IP Address Mode: Static

Routing Interface IP List Max: 10 Total: 1

□	IP Address Type	IP Address	Subnet Mask
□	Primary	192.168.1.2	255.255.255.0

17 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 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

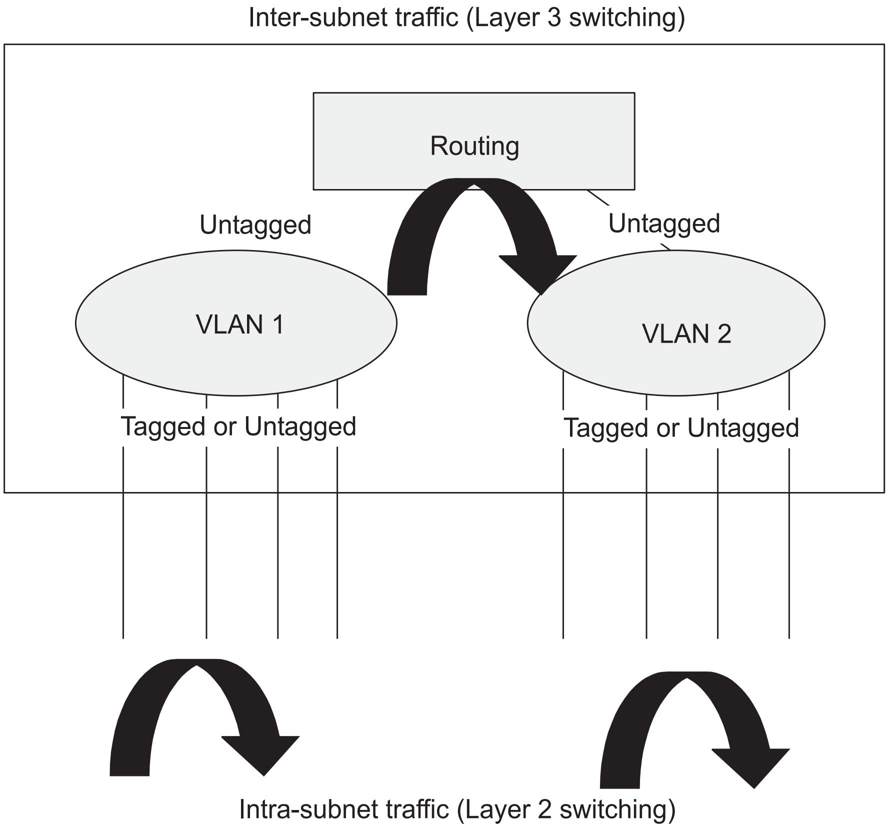
This switch supports IP routing and routing path management via static routing definitions (page 447) and dynamic routing protocols such as RIP, OSPF (page 484 or 502, respectively). When IP routing is is functioning, this switch acts as a wire-speed router, passing traffic between VLANs with different 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 156), assign all ports that belong to the same group to these VLANs (page 158), and then assign an IP interface to each VLAN (page 438). 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.

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 261: 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 page to configure routing interfaces for directly connected subnets (see "Setting the Switch's IP Address (IP Version 4)" on page 431.

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 dirertly connected to this router, you can either configure static routes (see page 447), or use the RIP or OSPF dynamic routing protocols (see page 483) 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 protcol 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, use the static routing table as described on page 447, enter 0.0.0.0 for the IP address and subnet mask, and then specify this switch itself or another router as the gateway.

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 1010

PARAMETERS

These parameters are displayed in the web interface:

- **IP Address** – IP address of the host.
- **Probe Count** – Number of packets to send. (Range: 1-16)
- **Packet Size** – Number of bytes in a packet. (Range: 32-512 bytes)

  The actual packet size will be eight bytes larger than the size specified because the switch adds header information.

COMMAND USAGE

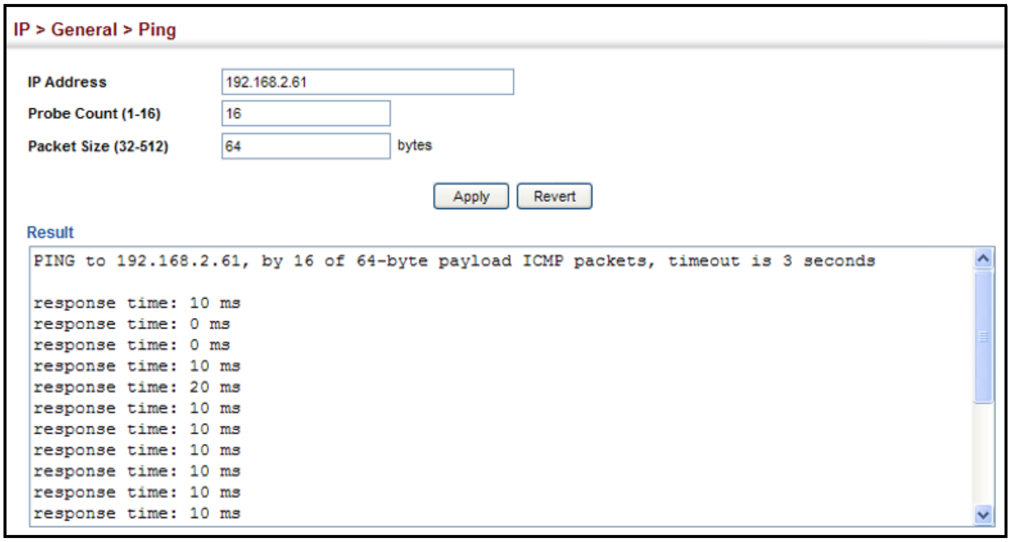
- Use the ping command to see if another site on the network can be reached.
- The following are some results of the **ping** command:
  - *Normal response* - The normal response occurs in one to ten seconds, depending on network traffic.
  - *Destination does not respond* - If the host does not respond, 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.

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 262: Pnging a Network Device



IP Address: 192.168.2.61
Probe Count (1-16): 16
Packet Size (32-512): 64 bytes

```
PING to 192.168.2.61, by 16 of 64-byte payload ICMP packets, timeout is 3 seconds

response time: 10 ms
response time: 0 ms
response time: 0 ms
response time: 10 ms
response time: 20 ms
response time: 10 ms
response time: 10 ms
response time: 10 ms
response time: 10 ms
response time: 10 ms
response time: 10 ms
```

USING THE TRACE ROUTE FUNCTION

Use the IP > General > Trace Route page to to show the route packets take to the specified destination.

CLI REFERENCES

- "traceroute" on page 1009

PARAMETERS

These parameters are displayed in the web interface:

- **Destination IP Address** – IP address of the host.

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.

WEB INTERFACE

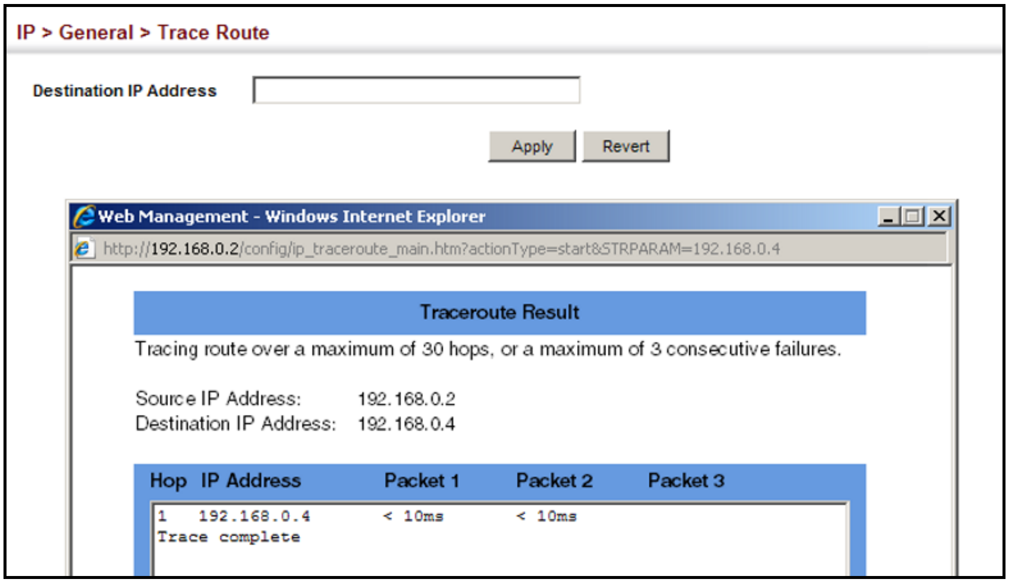
To trace the route to another device on the network:

1. Click IP, General, Trace Route.

2. Specify the target device.

3. Click Apply.

Figure 263: Tracing the Route to a Network Device


IP > General > Trace Route
Destination IP Address
Apply
Revert
Web Management - Windows Internet Explorer
http://192.168.0.2/config/ip_traceroute_main.htm?actionType=start&STRPARAM=192.168.0.4
Traceroute Result

Tracing route over a maximum of 30 hops, or a maximum of 3 consecutive failures.

Source IP Address: 192.168.0.2
Destination IP Address: 192.168.0.4

```
Hop  IP Address           Packet 1     Packet 2     Packet 3
1    192.168.0.4          < 10ms       < 10ms
Trace complete
```

ADDRESS RESOLUTION PROTOCOL

If IP routing is enabled (page 483), 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 23: 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

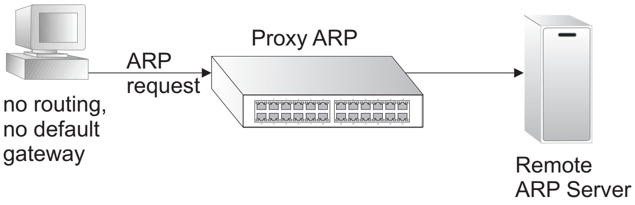
- "arp timeout" on page 1012
- "ip proxy-arp" on page 1013

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 264: Proxy ARP



PARAMETERS

These parameters are displayed in the web interface:

- **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.

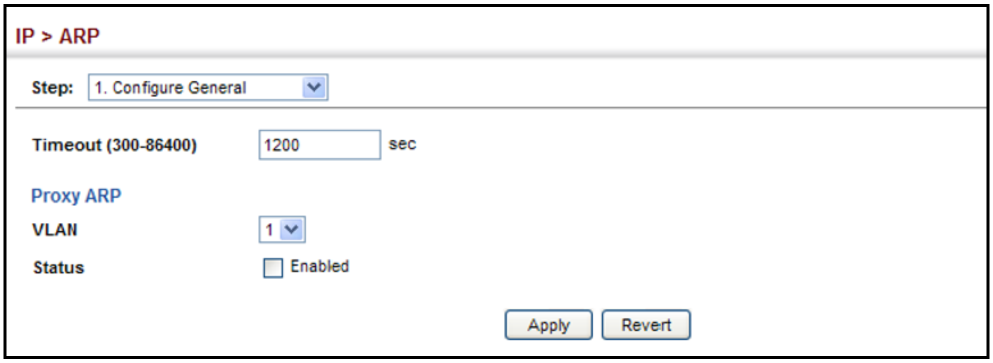
  Extensive use of Proxy ARP can degrade router performance because it may lead to increased ARP traffic and increased search time for larger ARP address tables.

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 265: 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 1011

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.

PARAMETERS

These parameters are displayed in the web interface:

- **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.

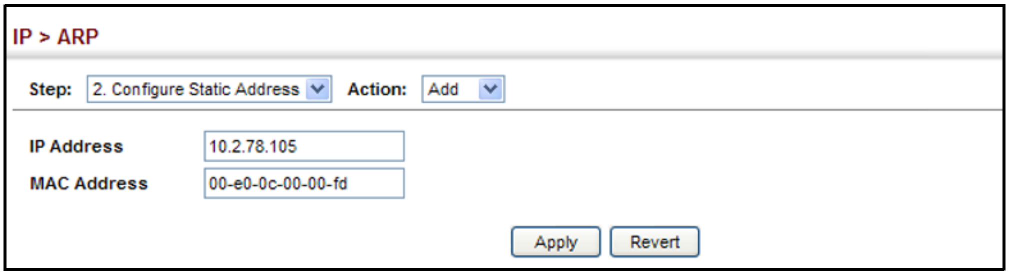
2. Select Configure Static Address from the Step List.

3. Select Add from the Action List.

4. Enter the IP address and the corresponding MAC address.

5. Click Apply.

Figure 266: Configuring Static ARP Entries



Step: 2. Configure Static Address Action: Add

IP Address 10.2.78.105

MAC Address 00-e0-0c-00-00-fd

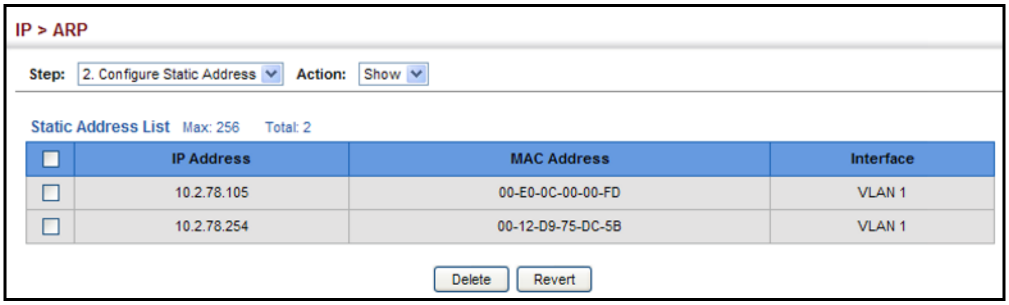
To display static entries in the ARP cache:

1. Click IP, ARP.

2. Select Configure Static Address from the Step List.

3. Select Show from the Action List.

Figure 267: Displaying Static ARP Entries



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

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. Use the IP > ARP (Show Information) page to display dynamic or local entries in the ARP cache.

CLI REFERENCES

◆ "show arp" on page 1014

WEB INTERFACE

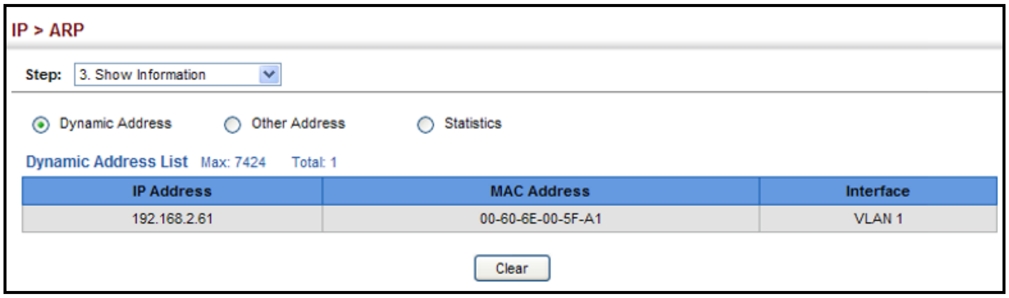
To display all dynamic entries in the ARP cache:

1. Click IP, ARP.

2. Select Show Information from the Step List.

3. Click Dynamic Address.

Figure 268: Displaying Dynamic ARP Entries



IP > ARP

Step: 3. Show Information

● Dynamic Address ○ Other Address ○ Statistics

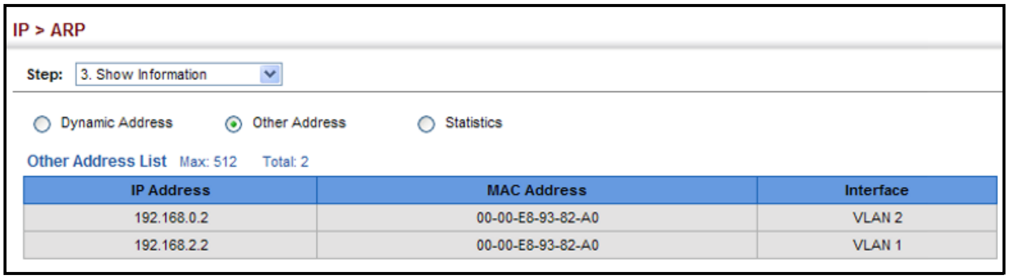
Dynamic Address List Max: 7424 Total: 1

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 269: 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 1023

PARAMETERS

These parameters are displayed in the web interface:

Table 24: ARP Statistics

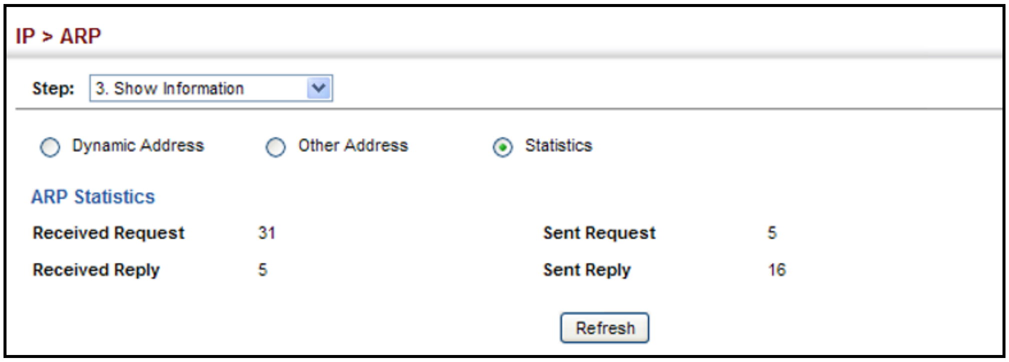
Parameter	Description
Received Request	Number of ARP Request packets received by the router.
Received Reply	Number of ARP Reply packets received by the router.
Sent Request	Number of ARP Request packets sent by the router.
Sent Reply	Number of ARP Reply packets sent by the router.

WEB INTERFACE

To display ARP statistics:

1. Click IP, ARP.
2. Select Show Information from the Step List.
3. Click Statistics.

Figure 270: 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 or OSPF). 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 1020

COMMAND USAGE

- Up to 512 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 450).
- 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 by RIP or OSPF (see page 493 or 521, respectively).

PARAMETERS

These parameters are displayed in the web interface:

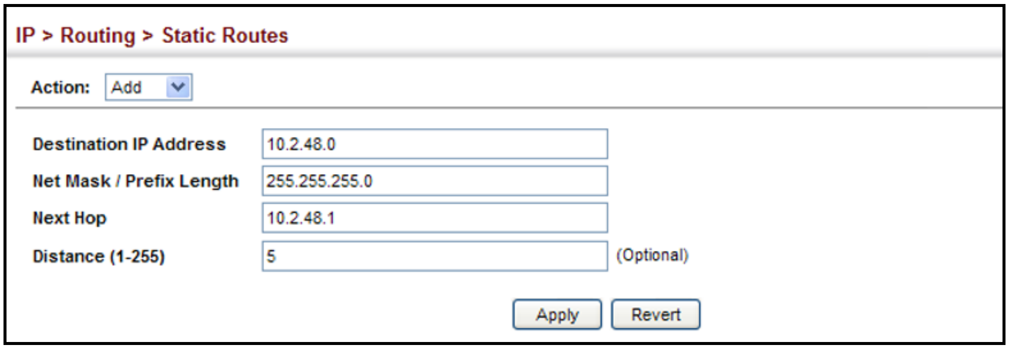
- **Destination IP Address** – IP address of the destination network, subnetwork, or host.
- **Netmask / Prefix Length** – Network mask for the associated IP subnet. This mask identifies the host address bits used for routing to specific subnets.
- **Next Hop** – IP address of the next router hop used 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 271: Configuring Static Routes



IP > Routing > Static Routes

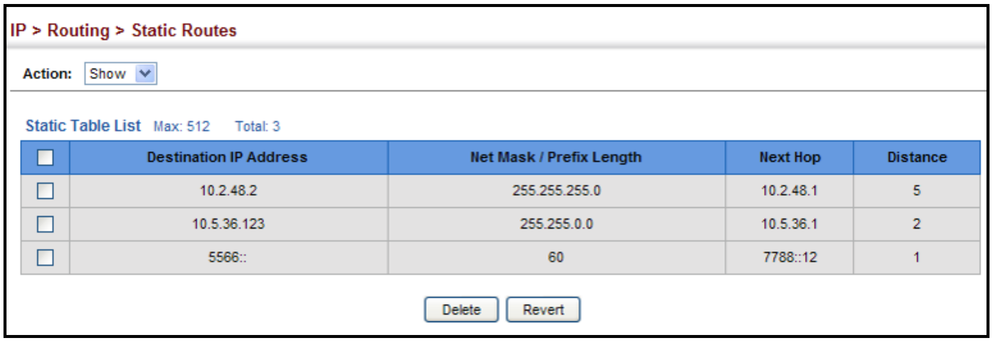
Action: Add

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 272: Displaying Static Routes



IP > Routing > Static Routes

Action: Show

Static Table List Max: 512 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 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 1021

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 in the web interface:

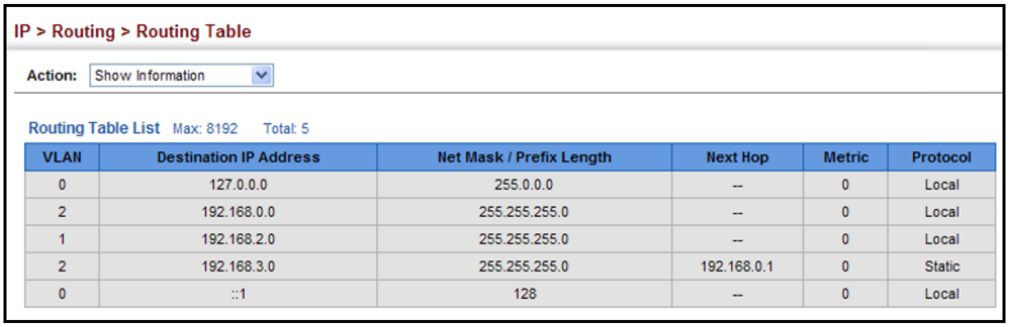
- **VLAN** – VLAN identifier (i.e., configure as a valid IP subnet).
- **Destination IP Address** – IP address of the destination network, subnetwork, or host. Note that the address 0.0.0.0 indicates the default gateway for this router.
- **Net Mask / Prefix Length** – Network mask for the associated 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 273: Displaying the Routing Table



IP > Routing > Routing Table

Action: Show Information

Routing Table List Max: 8192 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 447), or dynamically generated by OSPFv2 (see "Configuring the Open Shortest Path First Protocol (Version 2)" on page 502), 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 1021

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 in the web interface:

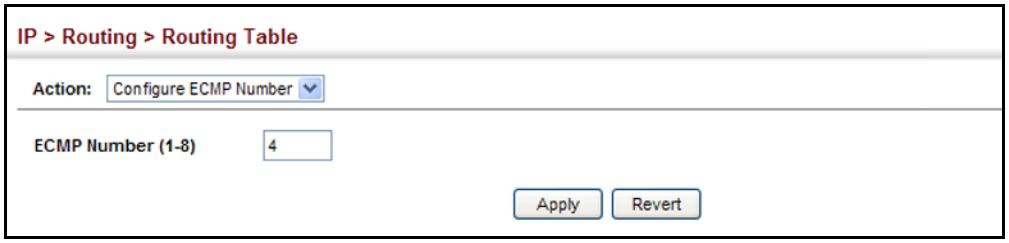
- **ECMP Number** – Sets the maximum number of equal-cost paths to the same destination that can be installed in the routing table. (Range: 1-8; Default: 4)

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 274: Setting the Maximum ECMP Numbeer



IP > Routing > Routing Table

Action: Configure ECMP Number

ECMP Number (1-8) 4

18 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 275: Master Virtual Router with Backup Routers

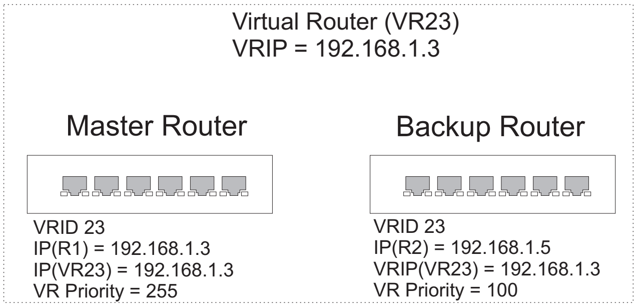


Figure 276: Several Virtual Master Routers Using Backup Routers

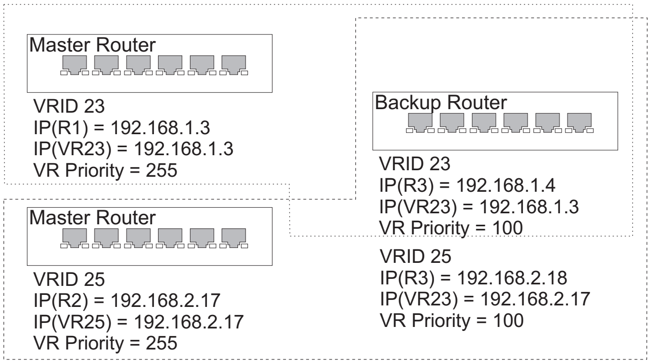
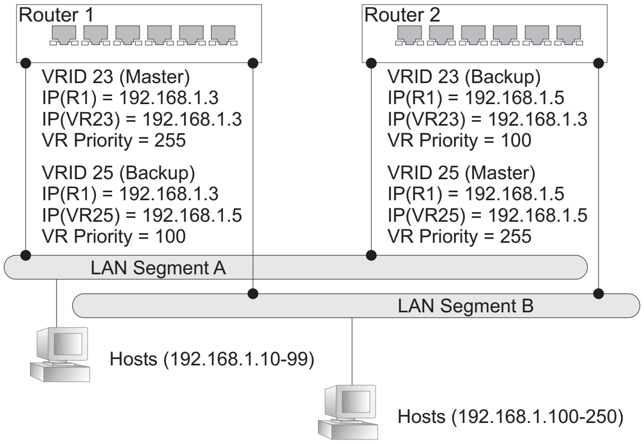


Figure 277: Several Virtual Master Routers Configured for Mutual Backup and Load Sharing



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 473)

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 995

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 in the web interface:

Adding a VRRP Group

- **VRID** – VRRP group identifier. (Range: 1-255)

- **VLAN** – ID of a VLAN configured with an IP interface. (Range: 1-4093; Default: 1)

Adding a Virtual IP Address

- **VLAN ID** – ID of a VLAN configured with an IP interface. (Range: 1-4093)

- **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: 1-4093)

- **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.

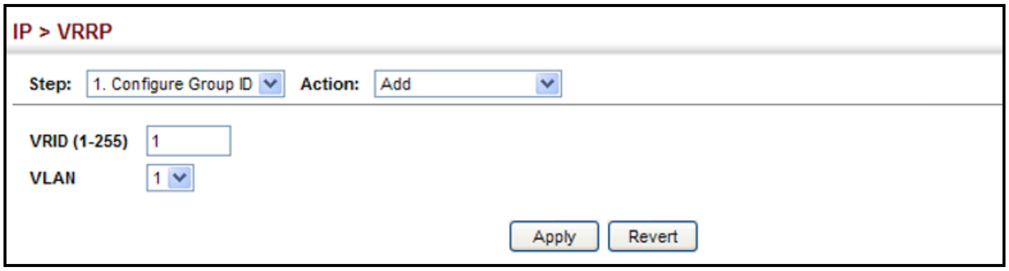
2. Select Configure Group ID from the Step List.

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 278: Configuring the VRRP Group ID


IP > VRRP

Step: 1. Configure Group ID Action: Add

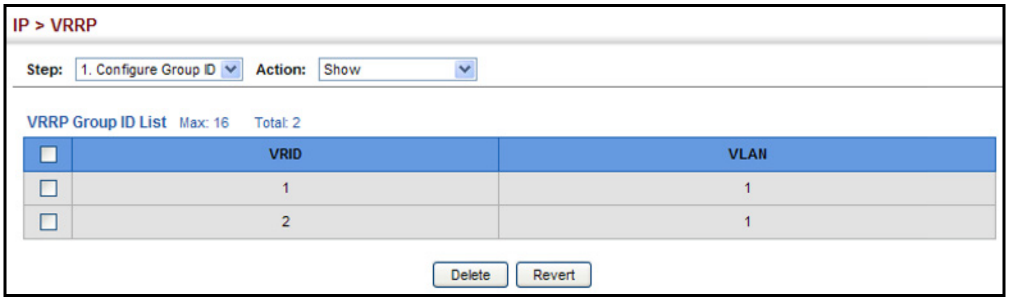
VRID (1-255) 1

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 279: Showing Configured VRRP Groups


IP > VRRP

Step: 1. Configure Group ID Action: Show

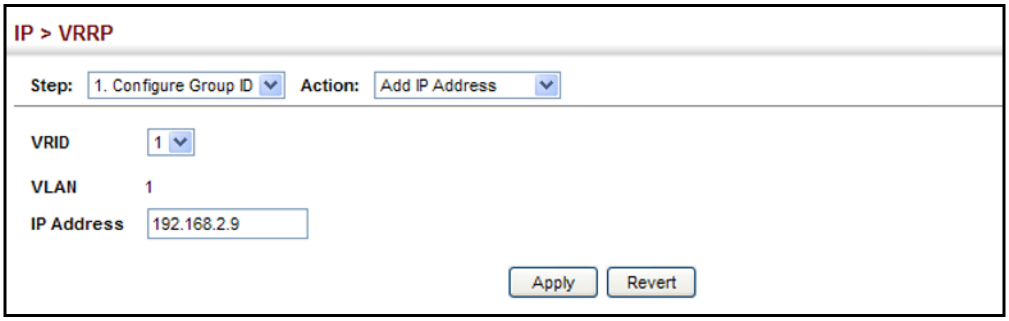
VRRP Group ID List Max: 16 Total: 2

□	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 VRRP group identifier, and enter the IP address for the virtual router.
5. Click Apply.

Figure 280: Setting the Virtual Router Address for a VRRP Group



IP > VRRP

Step: 1. Configure Group ID Action: Add IP Address

VRID 1

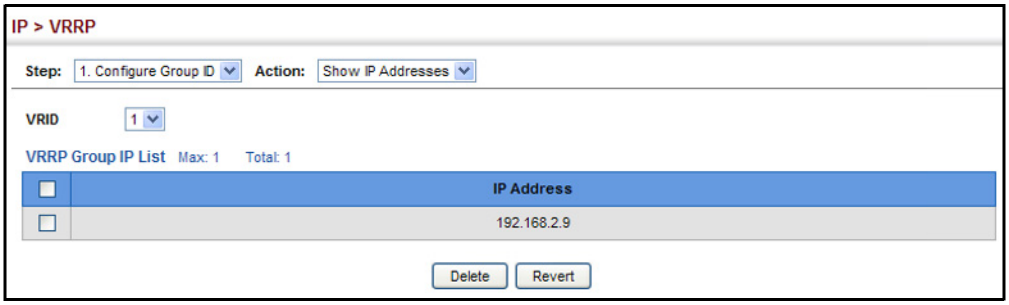
VLAN 1

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.

Figure 281: Showing the Virtual Addresses Assigned to VRRP Groups



IP > VRRP

Step: 1. Configure Group ID Action: Show IP Addresses

VRID 1

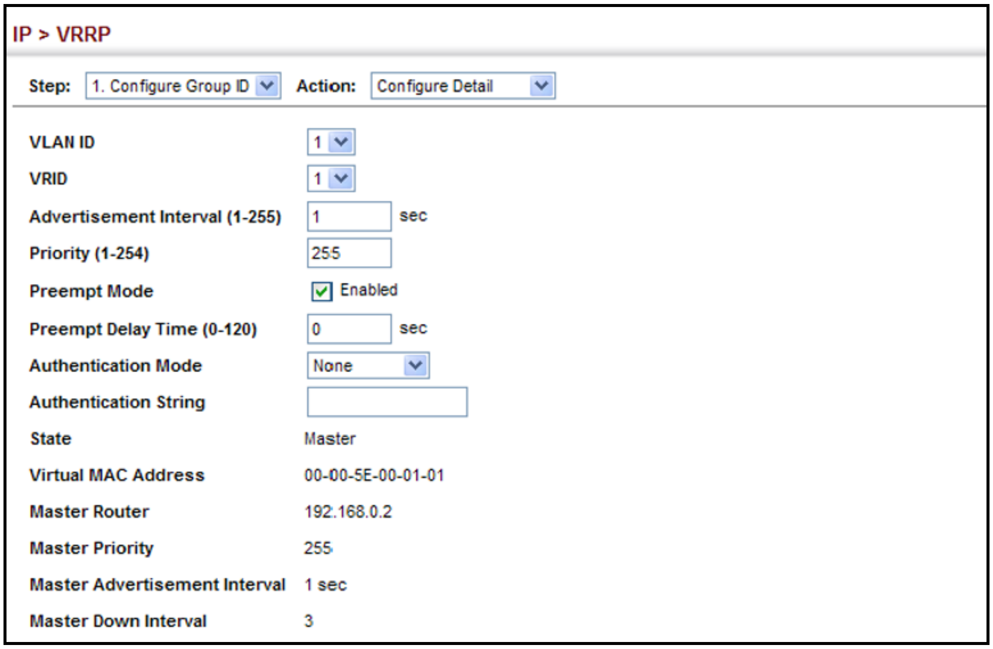
VRRP Group IP List Max: 1 Total: 1

□	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 282: 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 1004

PARAMETERS

These parameters are displayed in the web interface:

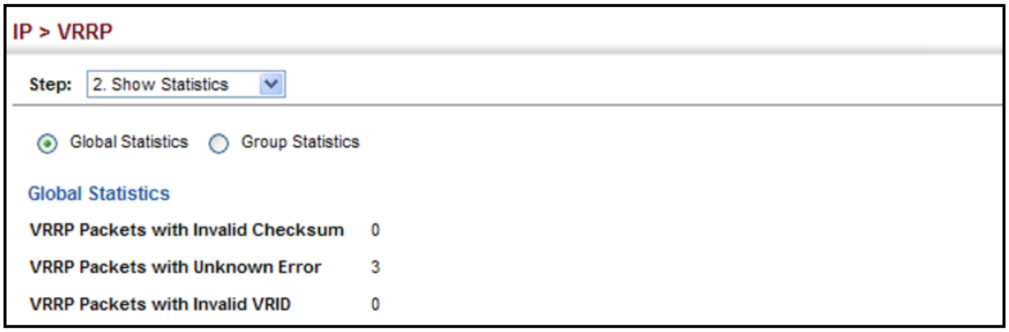
- **VRRP Packets with Invalid Checksum** – The total number of VRRP packets received with an invalid VRRP checksum value.
- **VRRP Packets with Unknown Error** – The total number of VRRP packets received with an unknown or unsupported version number.
- **VRRP Packets with Invalid VRID** – The total number 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 283: Showing Counters for Errors Found in VRRP Packets



IP > VRRP

Step: 2. Show Statistics

● Global Statistics ○ Group Statistics

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 1003

PARAMETERS

These parameters are displayed in the web interface:

- **VLAN ID** – VLAN configured with an IP interface. (Range: 1-4093)
- **VRID** – VRRP group identifier. (Range: 1-255)

The following statistcs are displayed in the web interface:

Table 25: VRRP Group Statistics 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 25: VRRP Group Statistics Statistics (Continued)

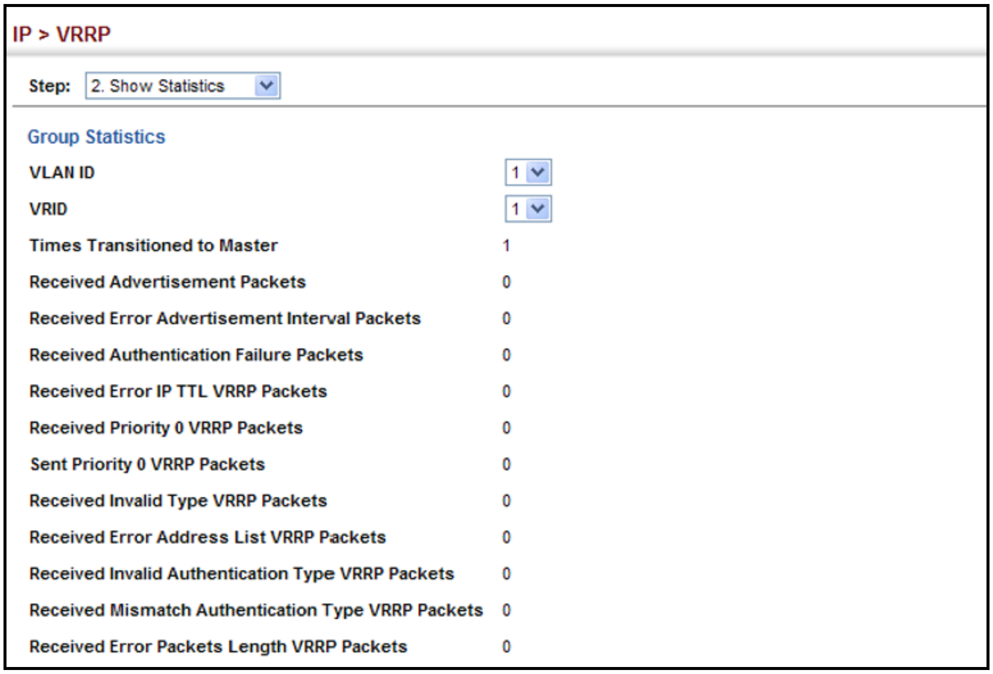
Parameter	Description
Received Invalid Type VRRP Packets	Number of VRRP packets received by the virtual router with an invalid value in the “type” field.
Received Error Address List VRRP Packets	Number of packets received for which the address list does not match the locally configured list for the virtual 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 284: 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

19 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 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.

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 970
- "ip domain-name" on page 971

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 466).

PARAMETERS

These parameters are displayed in the web interface:

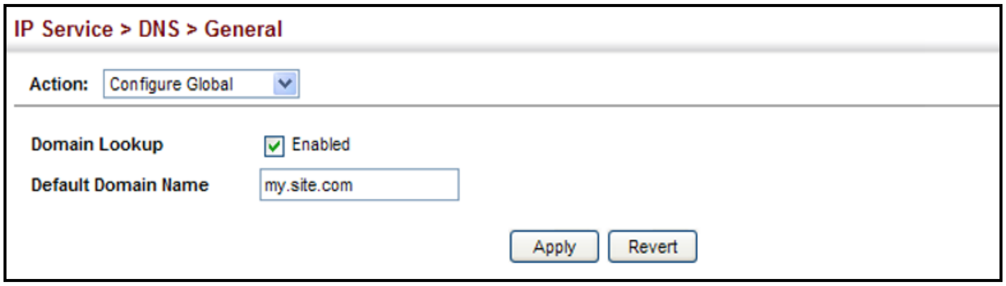
- **Domain Lookup** – Enables DNS host name-to-address translation. (Default: Disabled)
- **Default Domain Name** – Defines the default domain name appended to incomplete host names. Do not include the initial dot that separates the host name from the domain name.
(Range: 1-127 alphanumeric characters)

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 285: 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 969
- "show dns" on page 975

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 463). 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 466).

PARAMETERS

These parameters are displayed in the web interface:

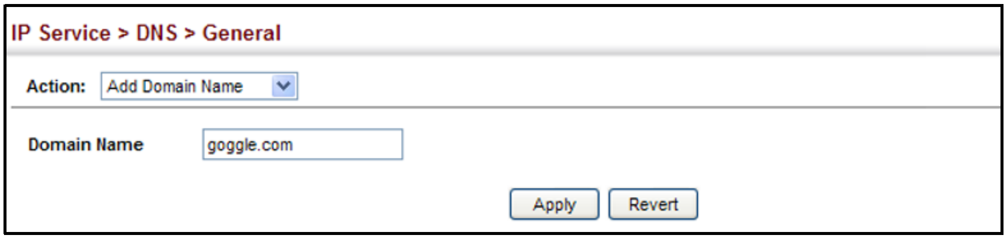
Domain Name – Name of the host. Do not include the initial dot that separates the host name from the domain name.
(Range: 1-68 characters)

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 286: Configuring a List of Domain Names for DNS



IP Service > DNS > General

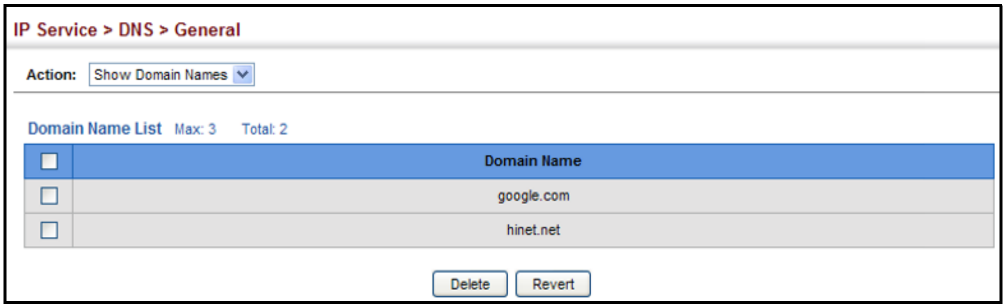
Action: Add Domain Name

Domain Name: goggle.com

To show the list domain names:

1. Click IP Service, DNS.
2. Select Show Domain Names from the Action list.

Figure 287: Showing the List of Domain Names for DNS



IP Service > DNS > General

Action: Show Domain Names

Domain Name List Max: 3 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 973
- "show dns" on page 975

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 463).
- 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 in the web interface:

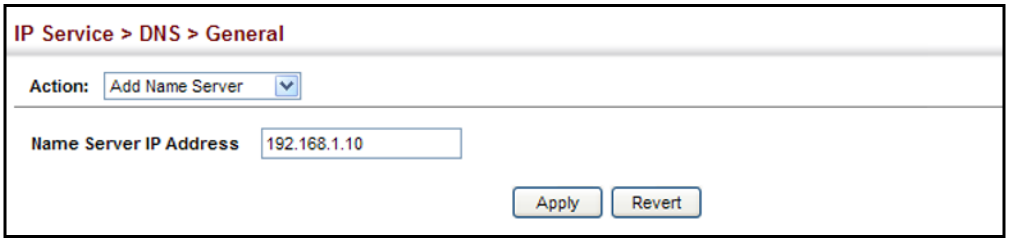
Name Server IP Address – Specifies the address of a domain name server to use for name-to-address resolution. Up to six IP addresses can be added to the name server list.

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 288: Configuring a List of Name Servers for DNS



IP Service > DNS > General

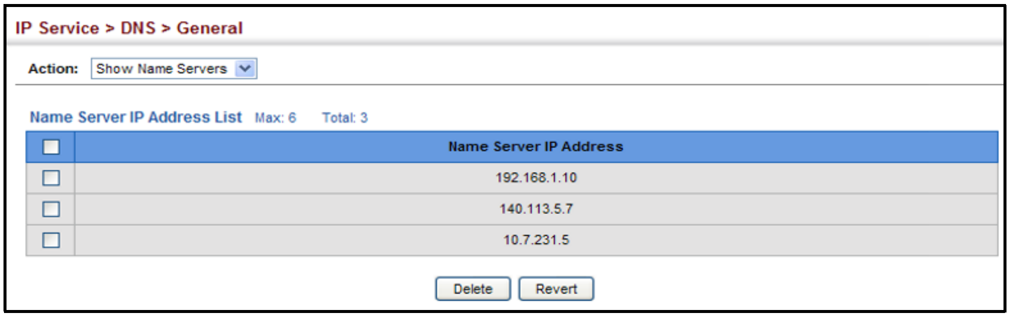
Action: Add Name Server

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 289: Showing the List of Name Servers for DNS


IP Service > DNS > General

Action: Show Name Servers

Name Server IP Address List Max: 6 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 972
- "show hosts" on page 976

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 in the web interface:

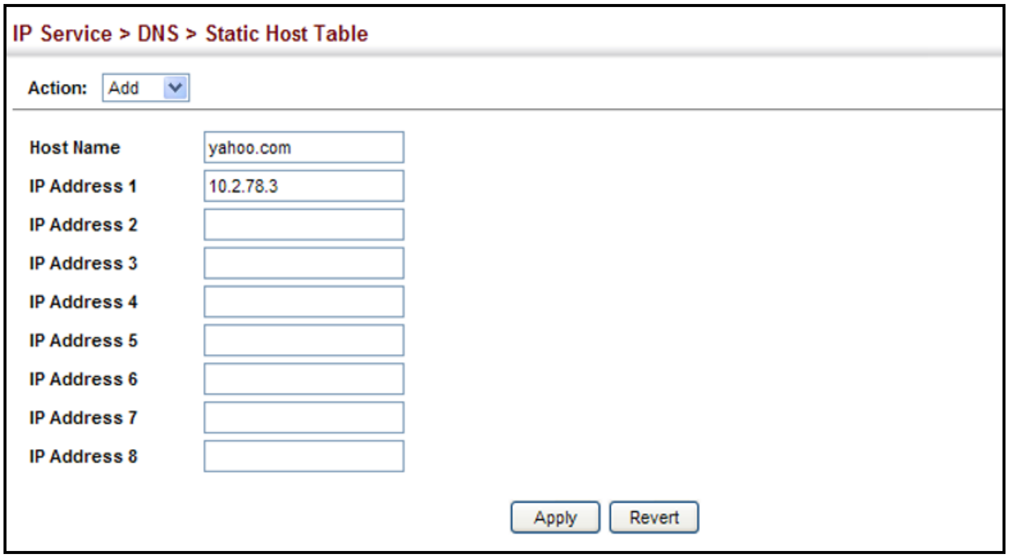
- **Host Name** – Name of a host device that is mapped to one or more IP addresses. (Range: 1-127 characters)
- **IP Address** – Internet address(es) associated with a host name.

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 290: Configuring Static Entries in the DNS Table



IP Service > DNS > Static Host Table

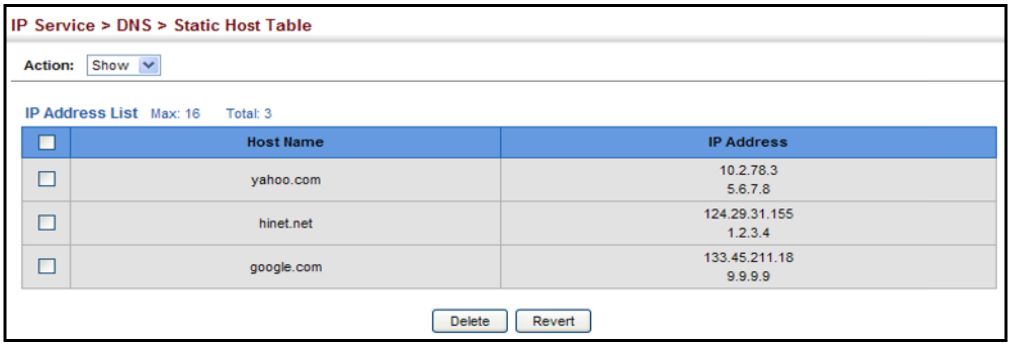
Action: Add

Host Name	yahoo.com
IP Address 1	10.2.78.3
IP Address 2	
IP Address 3	
IP Address 4	
IP Address 5	
IP Address 6	
IP Address 7	
IP Address 8	

To show static entries in the DNS table:

1. Click IP Service, DNS, Static Host Table.
2. Select Show from the Action list.

Figure 291: Showing Static Entries in the DNS Table



IP Service > DNS > Static Host Table

Action: Show

IP Address List Max: 16 Total: 3

□	Host Name	IP Address
□	yahoo.com	10.2.78.3 5.6.7.8
□	hinet.net	124.29.31.155 1.2.3.4
□	google.com	133.45.211.18 9.9.9.9

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 976

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 in the web interface:

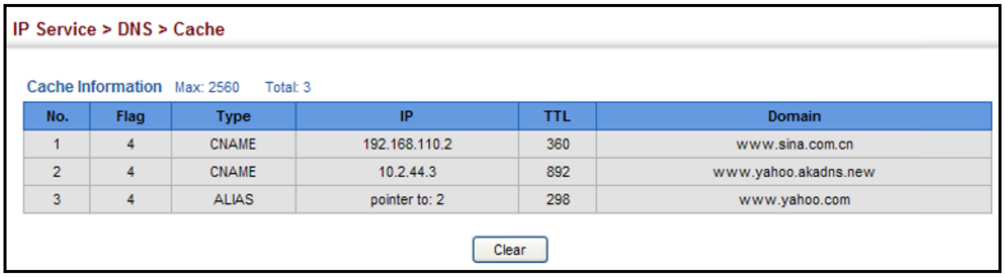
- **No.** – The entry number for each resource record.
- **Flag** – The flag is always "4" indicating a cache entry and therefore unreliable.
- **Type** – This field includes CNAME which specifies the host address for the owner, and ALIAS which specifies an alias.
- **IP** – The IP address associated with this record.
- **TTL** – The time to live reported by the name server.
- **Domain** – The domain name associated with this record.

WEB INTERFACE

To display entries in the DNS cache:

1. Click IP Service, DNS, Cache.

Figure 292: Showing Entries in the DNS Cache



Cache Information Max: 2560 Total: 3

No.	Flag	Type	IP	TTL	Domain
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

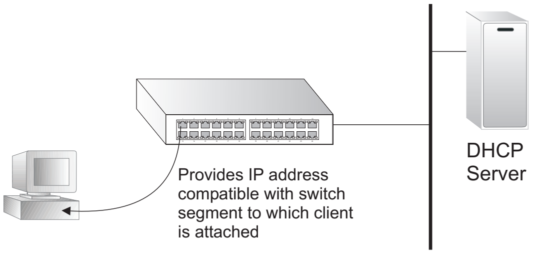
Dynamic Host Configuration Protocol (DHCP) can dynamically allocate an IP address and other configuration information to network clients when they boot up. If a subnet does not already include a BOOTP or DHCP server, you can relay DHCP client requests to a DHCP server on another subnet, or configure 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).

CONFIGURING DHCP RELAY SERVICE

Use the IP Service > DHCP > Relay page to configue 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 293: Layer 3 DHCP Relay Service



CLI REFERENCES

- "ip dhcp relay server" on page 980
- "ip dhcp restart relay" on page 981

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 in the web interface:

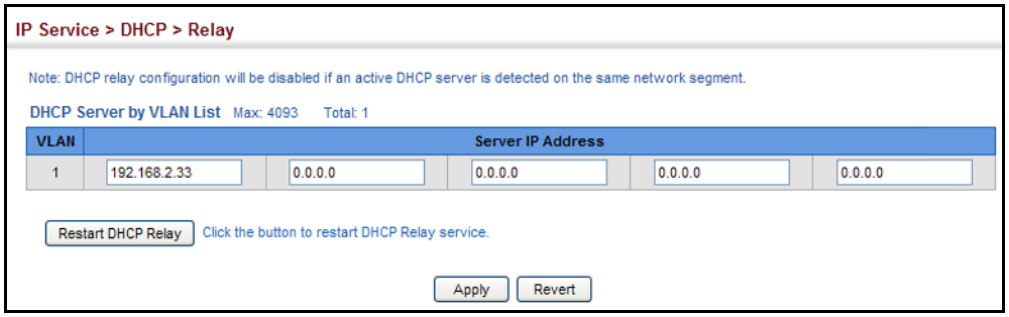
- **VLAN ID** – ID of configured VLAN.
- **Server IP Address** – Addresses of DHCP servers to be used by the switch's DHCP relay agent in order of preference.
- **Restart DHCP Relay** – Use this button to re-initialize DHCP relay service.

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 294: 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 Max: 4093 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

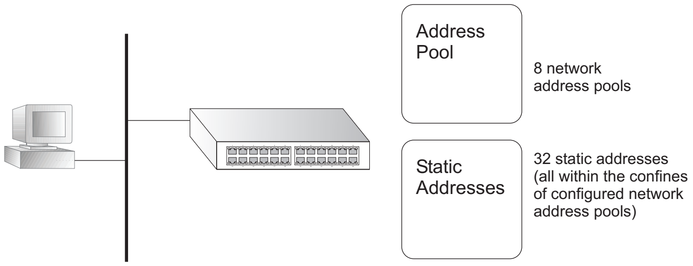
Click the button to restart DHCP Relay service.

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 295: 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 reenable 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 984

Parameters

These parameters are displayed in the web interface:

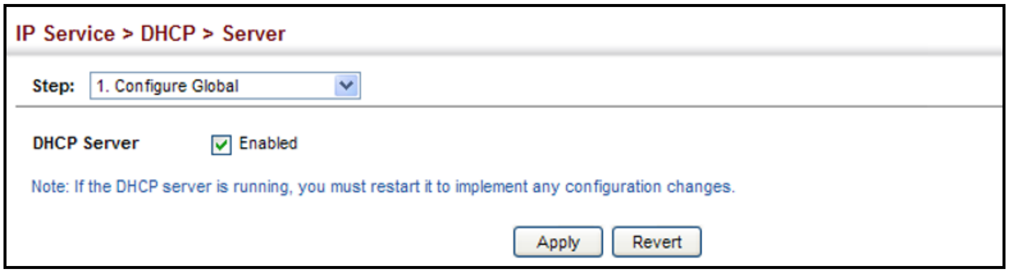
- **DHCP Server** – Enables or disables the DHCP server on this switch. (Default: Disabled)

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 296: Enabling the DHCP Server



IP Service > DHCP > Server

Step: 1. Configure Global

DHCP Server ☑ Enabled

Note: 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 983

Parameters

These parameters are displayed in the web interface:

- **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.

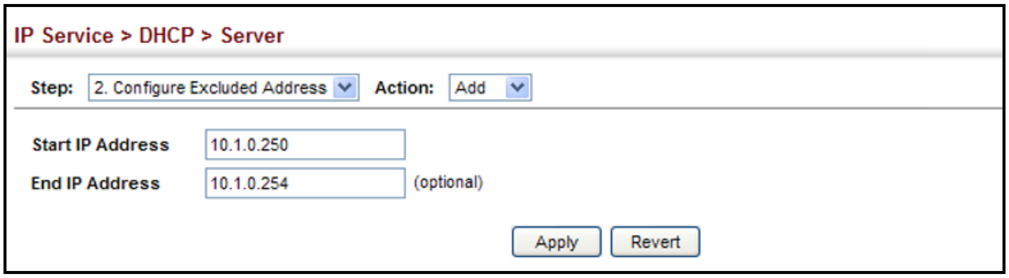
NOTE: Be sure you exclude the address for this switch and other key network devices.

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 297: Configuring Excluded Addresses on the DHCP Server



IP Service > DHCP > Server

Step: 2. Configure Excluded Address   Action: Add

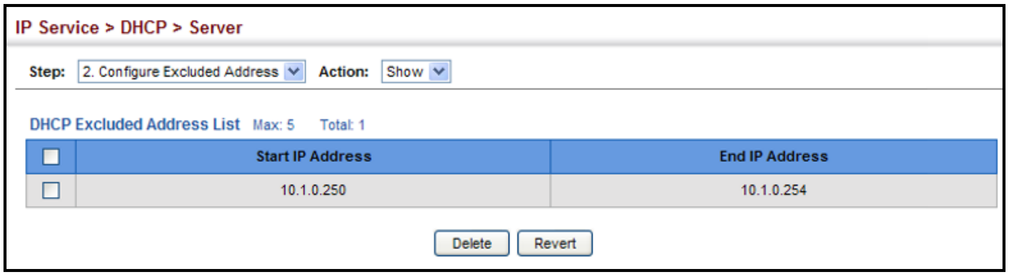
Start IP Address 10.1.0.250

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 298: Showing Excluded Addresses on the DHCP Server



IP Service > DHCP > Server

Step: 2. Configure Excluded Address   Action: Show

DHCP Excluded Address List Max: 5 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 982

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 489). 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 in the web interface:

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.

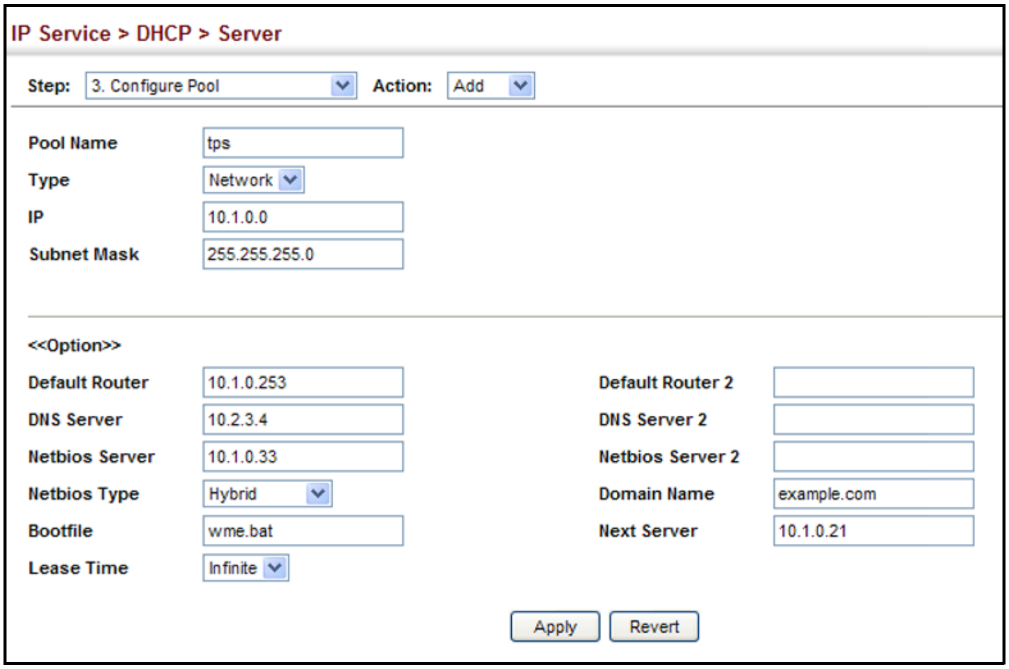
3. Select Add from the Action list.

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 299: Configuring DHCP Server Address Pools (Network)



IP Service > DHCP > Server

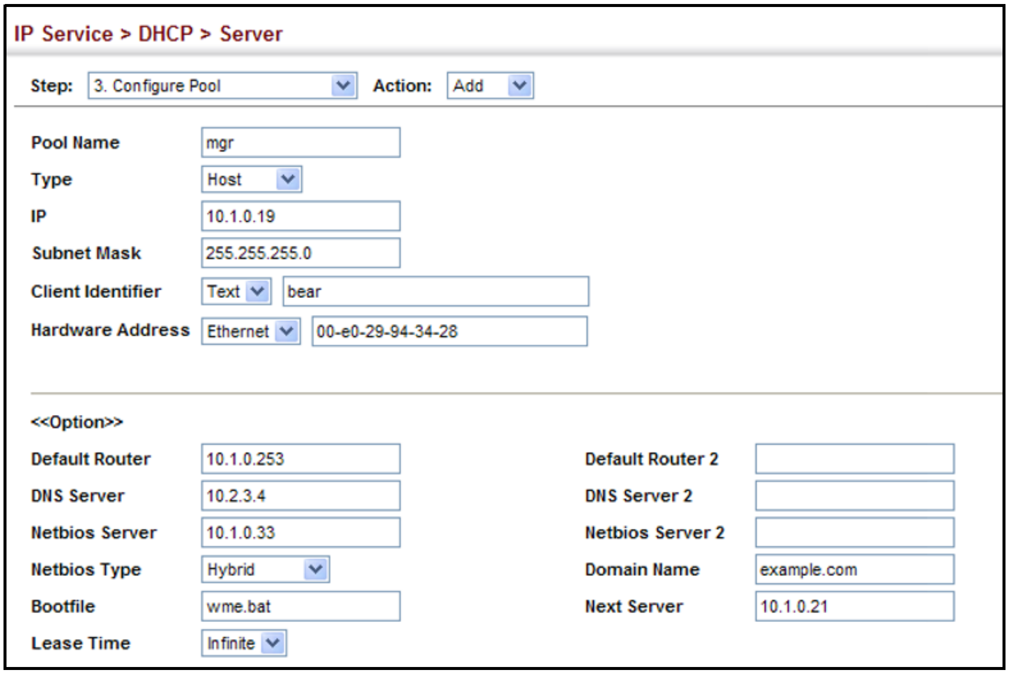
Step: 3. Configure Pool Action: Add

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 300: 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	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		

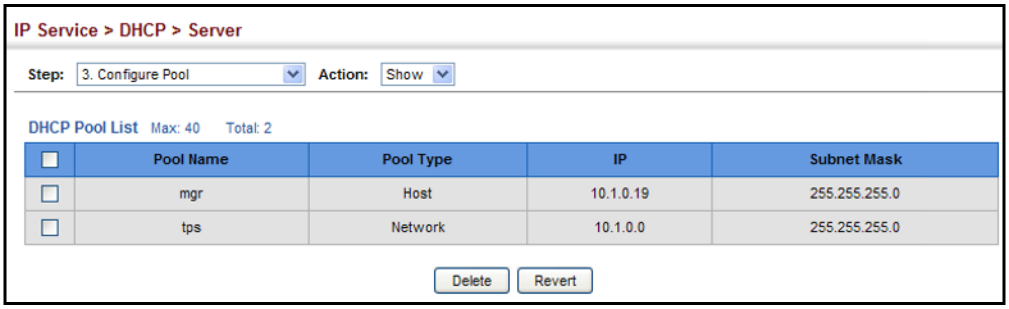
To show the configured DHCP address pools:

1. Click IP Service, DHCP, Server.

2. Select Configure Pool from the Step list.

3. Select Show from the Action list.

Figure 301: Showing Configured DHCP Server Address Pools



IP Service > DHCP > Server

Step: 3. Configure Pool Action: Show

DHCP Pool List Max: 40 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 993

PARAMETERS

These parameters are displayed in the web interface:

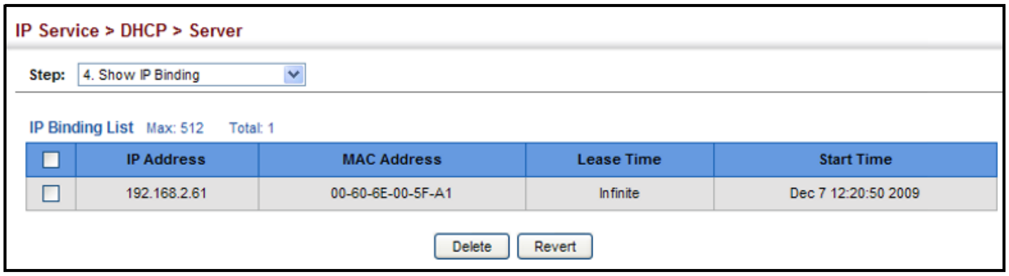
- **IP Address** – IP address assigned to host.
- **MAC Address** – MAC address of host.
- **Lease Time** – Duration that this IP address can be used by the host.
- **Start Time** – Time this address was assigned by the switch.

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 302: Shows Addresses Assigned by the DHCP Server



IP Service > DHCP > Server

Step: 4. Show IP Binding

IP Binding List Max: 512 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 463), specify the UDP destination ports for which broadcast traffic will be forwarded (see "Specifying UDP Destination Ports" on page 479), and specify the remote application servers or the subnet where the servers are located (see "Specifying The Target Server or Subnet" on page 480).

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 1016

PARAMETERS

These parameters are displayed in the web interface:

- **UDP Helper Status** – Enables or disables the UDP helper. (Default: Disabled)

WEB INTERFACE

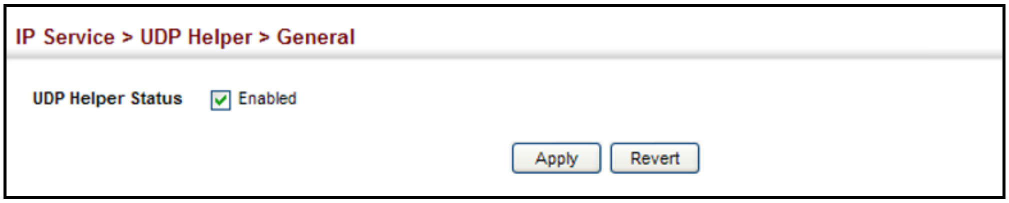
To enable the UDP help:

1. Click IP Service, UDP Helper, General.

2. Mark the Enabled check box.

3. Click Apply.

Figure 303: 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 1015

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 in the web interface:

- **Destination UDP Port** – UDP application port for which UDP service requests are forwarded. (Range: 1-65535)

  The following UDP ports are inlcuded 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:

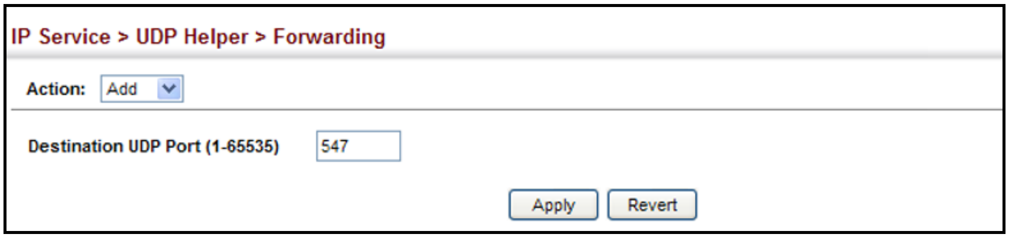
1. Click IP Service, UDP Helper, Forwarding.

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 304: Specifying UDP Destination Ports



IP Service > UDP Helper > Forwarding

Action: Add

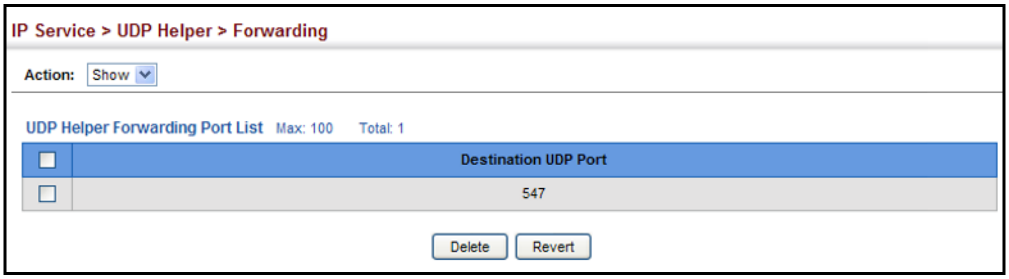
Destination UDP Port (1-65535) 547

To show the configured UDP destination ports:

1. Click IP Service, UDP Helper, Forwarding.

2. Select Show from the Action list.

Figure 305: Showing the UDP Destination Ports



IP Service > UDP Helper > Forwarding

Action: Show

UDP Helper Forwarding Port List Max: 100 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 1017

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 specifed 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 479.

PARAMETERS

These parameters are displayed in the web interface:

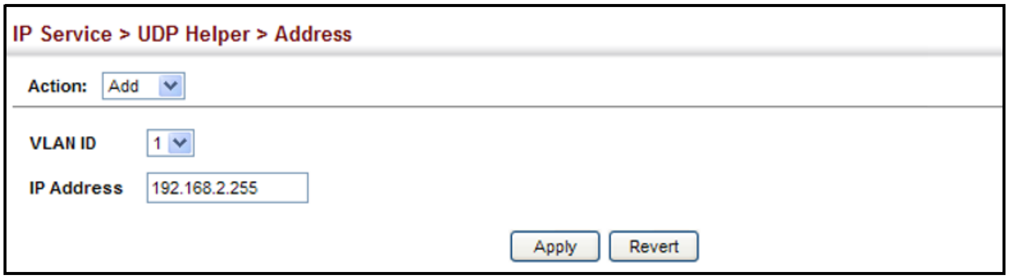
- **VLAN ID** – VLAN identifier (Range: 1-4093)
- **IP Address** – Host address or directed broadcast address to which UDP broadcast packets are forwarded. (Range: 1-65535)

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 306: Specifying the Target Server or Subnet for UDP Requests



IP Service > UDP Helper > Address

Action: Add

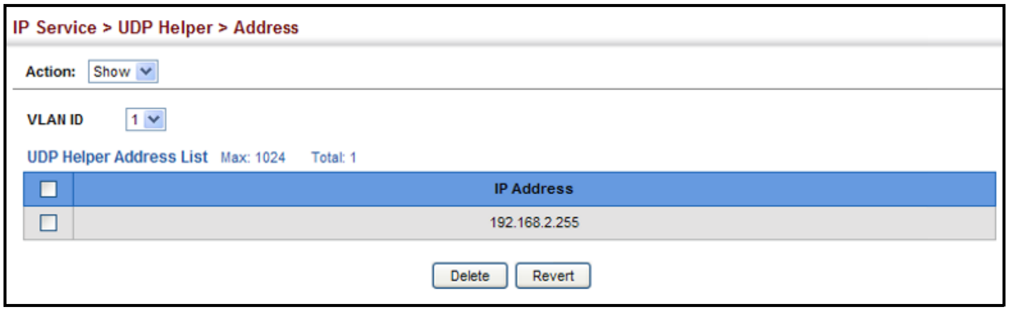
VLAN ID 1

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 307: Showing the Target Server or Subnet for UDP Requests



IP Service > UDP Helper > Address

Action: Show

VLAN ID 1

UDP Helper Address List Max: 1024 Total: 1

□	IP Address
□	192.168.2.255

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. These protocols exchange routing information, calculate routing tables, and can respond to changes in the status or loading of the network.

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.

Note: RIPng, which supports IPv6, will be supported in a future release.

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

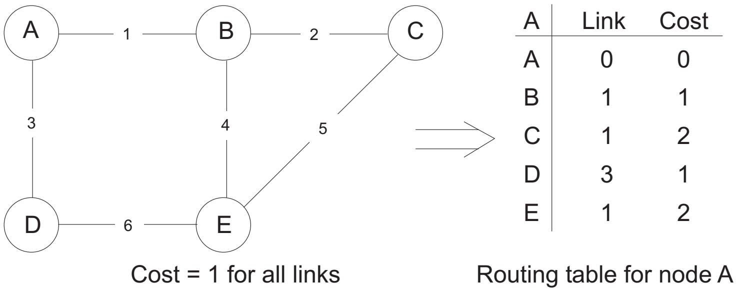
The switch supports IP routing only. Non-IP protocols such as IPX and Appletalk cannot be routed by this switch, and will be confined within their local VLAN group unless bridged by an external router.

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 308: 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 496).

CLI REFERENCES

- "Routing Information Protocol (RIP)" on page 1024

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 496).

PARAMETERS

These parameters are displayed in the web interface:

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 489. (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 496) 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 496) 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 493). 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 495) 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:

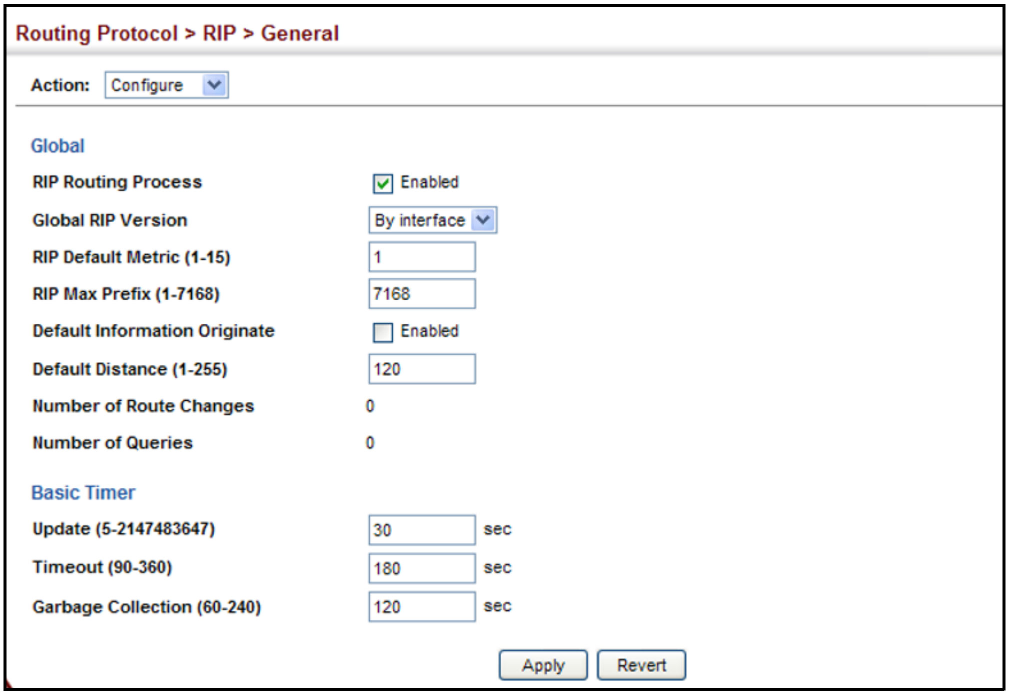
1. Click Routing Protocol, RIP, General.

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 309: 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 1039

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 493) 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 in the web interface:

- **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.

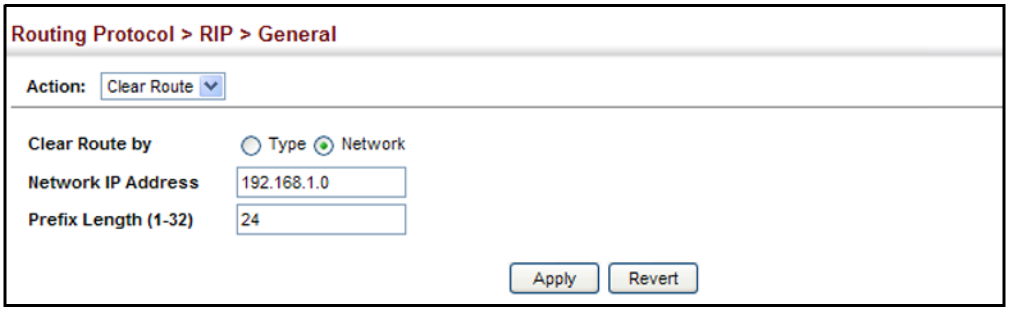
- **Clear Route By Network** – Clears a specific route based on its IP address and prefix length.
  - **Network IP Address** – Deletes all related entries for the specified network address.
  - **Prefix Length** – A decimal value indicating how many contiguous bits (from the left) of the address comprise 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 310: 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 1029

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 in the web interface:

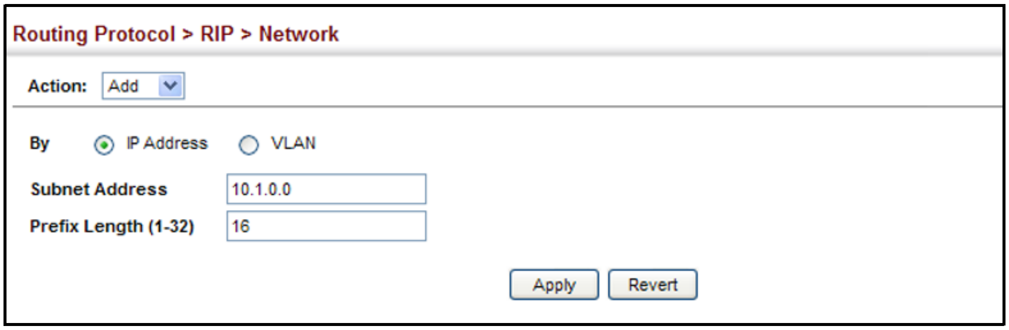
- **By Address** – Adds a network to the RIP routing process.
  - **Subnet Address** – IP address of a network directly connected to this router. (Default: No networks are specified)
  - **Prefix Length** – A decimal value indicating how many contiguous bits (from the left) of the address comprise the 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: 1-4093)

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 311: Adding Network Interfaces to RIP



Routing Protocol > RIP > Network

Action: Add

By ● IP Address ○ VLAN

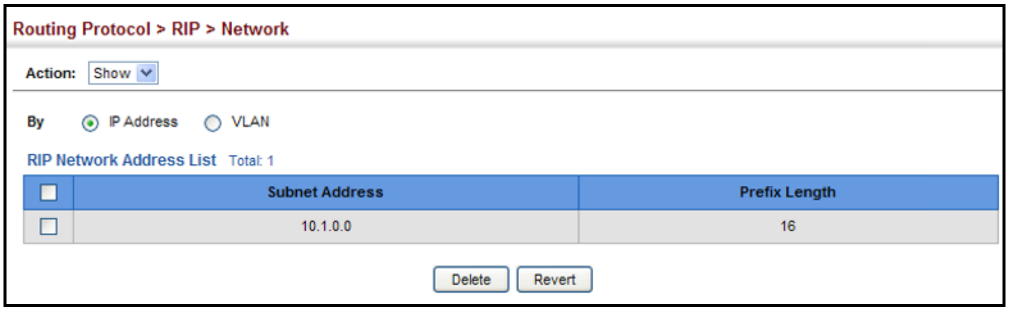
Subnet Address: 10.1.0.0

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 312: 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 1030

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 in the web interface:

- **VLAN** – VLAN interface on which to stop sending RIP updates. (Range: 1-4093)

WEB INTERFACE

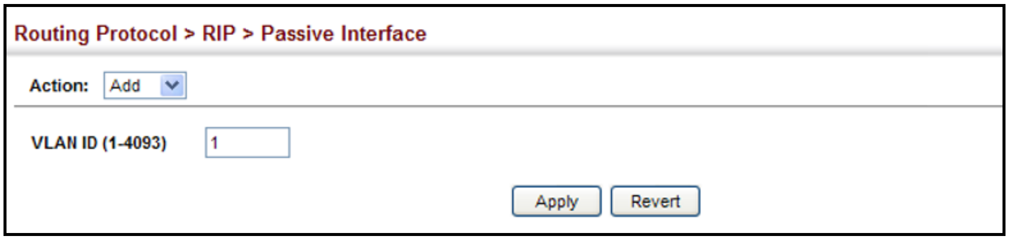
To specify a passive RIP interface:

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.


Routing Protocol > RIP > Passive Interface

Action: Add

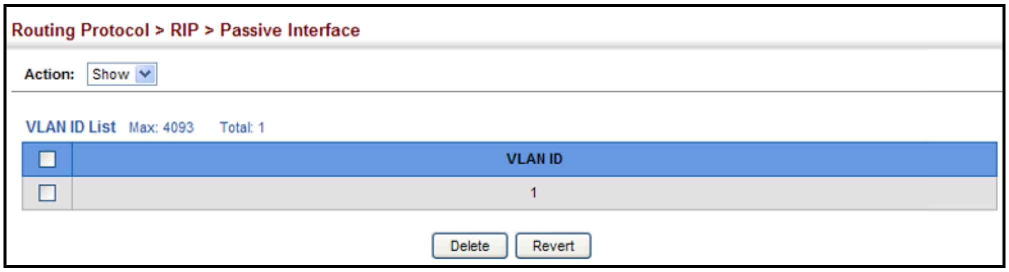
VLAN ID (1-4093) 1

Figure 313: Specifying a Passive RIP Interface

To show the passive RIP interfaces:

1. Click Routing Protocol, RIP, Passive Interface.
2. Select Show from the Action list.

Figure 314: Showing Passive RIP Interfaces


Routing Protocol > RIP > Passive Interface

Action: Show

VLAN ID List Max: 4093 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 1029

PARAMETERS

These parameters are displayed in the web interface:

- **IP Address** – IP address of a static neighboring router with which to exchange routing information.

WEB INTERFACE

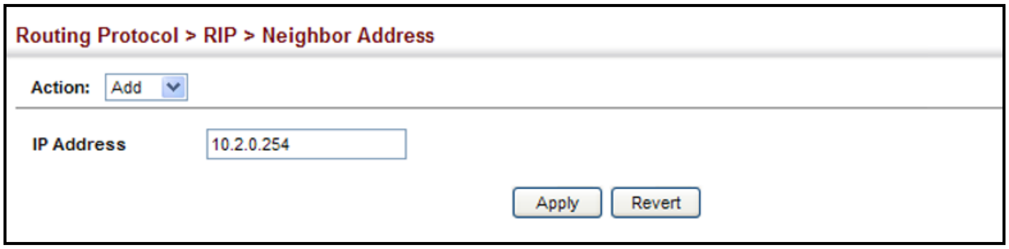
To specify a static RIP neighbor:

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 315: Specifying a Static RIP Neighbor



Routing Protocol > RIP > Neighbor Address

Action: Add

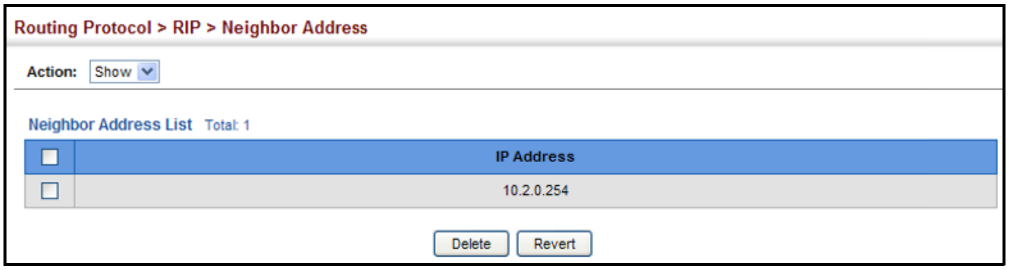
IP Address: 10.2.0.254

To show static RIP neighbors:

1. Click Routing Protocol, RIP, Neighbor Address.

2. Select Show from the Action list.

Figure 316: 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 1031

PARAMETERS

These parameters are displayed in the web interface:

- **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 485.)

  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.

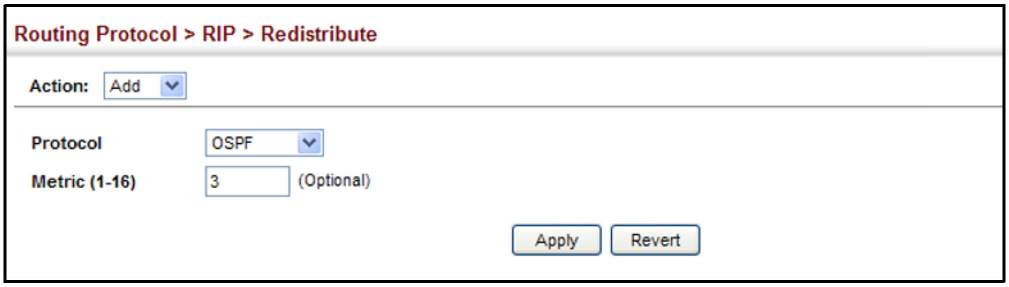
  It is advisable to use a low metric when redistributing routes from another protocol into RIP. Using a high metric limits the usefulness of external routes redistributed into RIP. For example, if a metric of 10 is defined for redistributed routes, these routes can only be advertised to routers up to 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 317: Redistributing External Routes into RIP



Routing Protocol > RIP > Redistribute

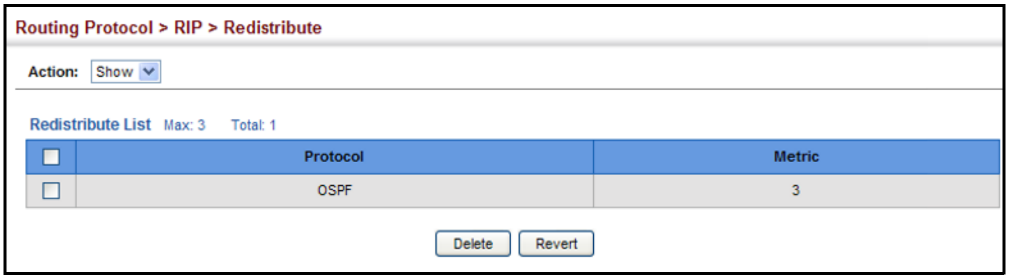
Action: Add

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 318: Showing External Routes Redistributed into RIP



Routing Protocol > RIP > Redistribute

Action: Show

Redistribute List Max: 3 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 1027

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.

- An access list can be used to filter networks according to the IP address of the router supplying the routing information. For example, to filter out unreliable routing information from routers not under your administrative control.

- The administrative distance is applied to all routes learned for the specified network.

PARAMETERS

These parameters are displayed in the web interface:

- **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.

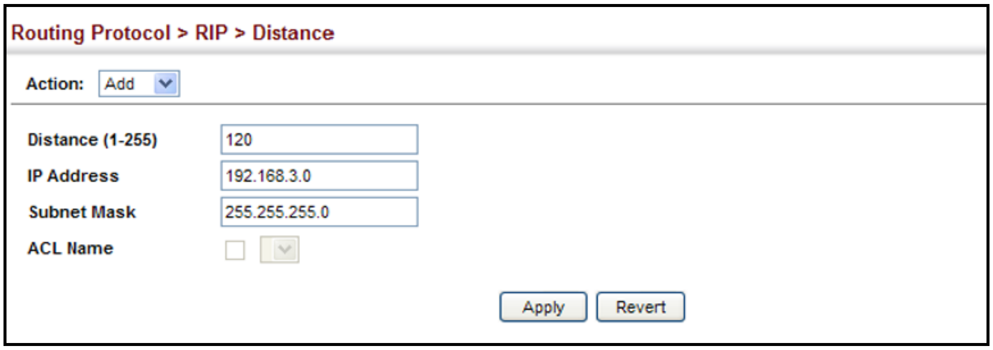
- **ACL Name** – Name of the access control list. Any type of ACL can be specified, including standard or extended IP ACLs and MAC ACLs. (Range: 1-16 characters)

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 319: Setting the Distance Assigned to External Routes



Routing Protocol > RIP > Distance

Action: Add

Distance (1-255): 120

IP Address: 192.168.3.0

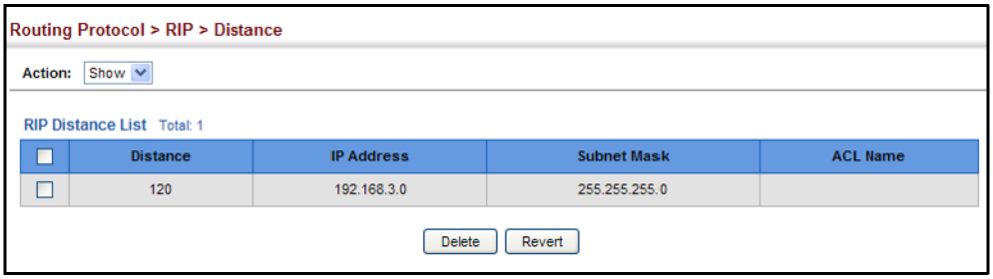
Subnet Mask: 255.255.255.0

ACL Name: □

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 320: Showing the Distance Assigned to External Routes



Routing Protocol > RIP > Distance

Action: Show

RIP Distance List Total: 1

□	Distance	IP Address	Subnet Mask	ACL Name
□	120	192.168.3.0	255.255.255.0	

CONFIGURING NETWORK INTERFACES FOR RIP

Use the Routing Protocol > RIP > Distance (Add) page to configure the send/recieve 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 1035
- "ip rip send version" on page 1037

- "ip rip authentication mode" on page 1034
- "ip rip authentication string" on page 1035
- "ip rip split-horizon" on page 1038

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 485).

- 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 in the web interface:

- **VLAN ID** – Layer 3 VLAN interface. This interface must be configured with an IP address and have an active link. (Range: 1-4093)

- **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 485.)

- **Receive Version** – The RIP version to receive on an interface.

  - **RIPv1**: Accepts only RIPv1 packets.

  - **RIPv2**: Accepts only RIPv2 packets.

  - **RIPv1 or RIPv2**: Accepts RIPv1 or 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 485.)

- **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.

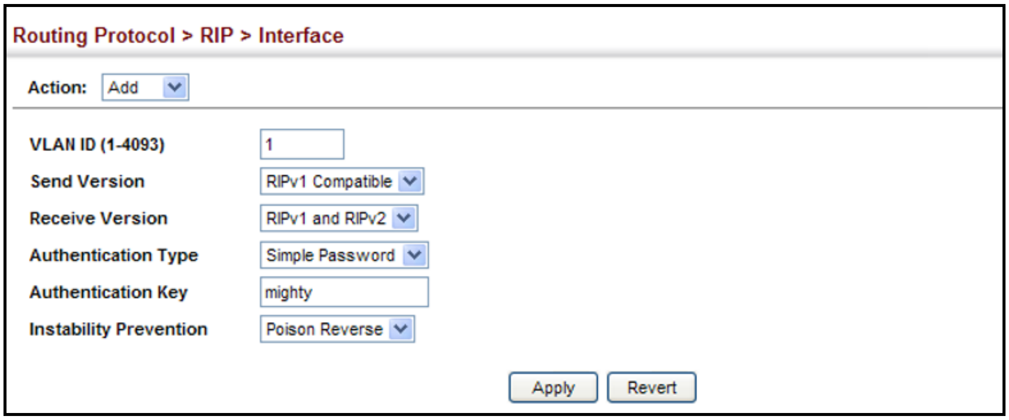
    MD5 is a one-way hash algorithm is that takes the authentication key and produces a 128 bit message digest or “fingerprint.” This makes it computationally infeasible to produce two messages having the same message digest, or to produce any message having a given pre-specified target message digest.
- **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 321: Configuring a Network Interface for RIP



Routing Protocol > RIP > Interface

Action: Add

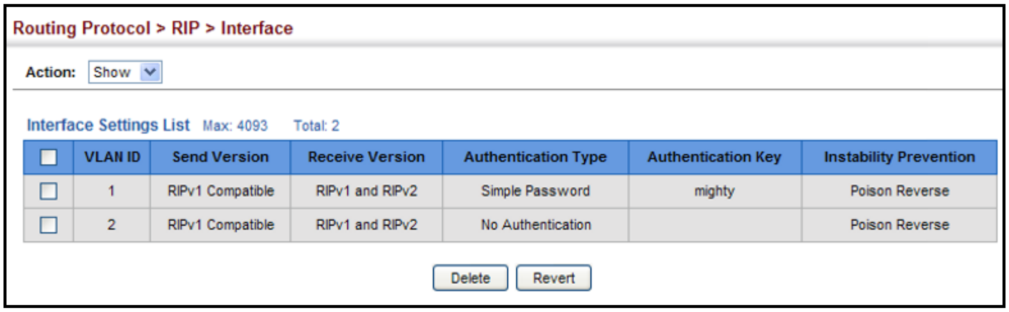
VLAN ID (1-4093)	1
Send Version	RIPv1 Compatible
Receive Version	RIPv1 and RIPv2
Authentication Type	Simple Password
Authentication Key	mighty
Instability Prevention	Poison Reverse

To show the network interface settings configured for RIP:

1. Click Routing Protocol, RIP, Interface.

2. Select Show from the Action list.

Figure 322: Showing RIP Network Interface Settings



Routing Protocol > RIP > Interface

Action: Show

Interface Settings List Max: 4093 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 1041

PARAMETERS

These parameters are displayed in the web interface:

- **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.

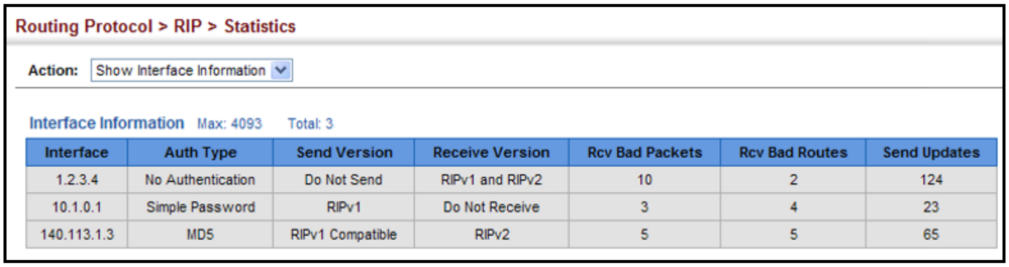
WEB INTERFACE

To display RIP interface configuration settings:

1. Click Routing Protocol, RIP, Statistics.

2. Select Show Interface Information from the Action list.

Figure 323: Showing RIP Interface Settings



Routing Protocol > RIP > Statistics

Action: Show Interface Information

Interface Information Max: 4093 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 1040

PARAMETERS

These parameters are displayed in the web interface:

- **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.

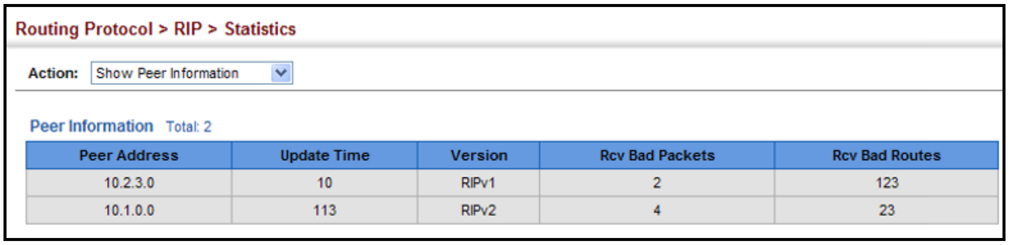
WEB INTERFACE

To display information on neighboring RIP routers:

1. Click Routing Protocol, RIP, Statistics.

2. Select Show Peer Information from the Action list.

Figure 324: 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

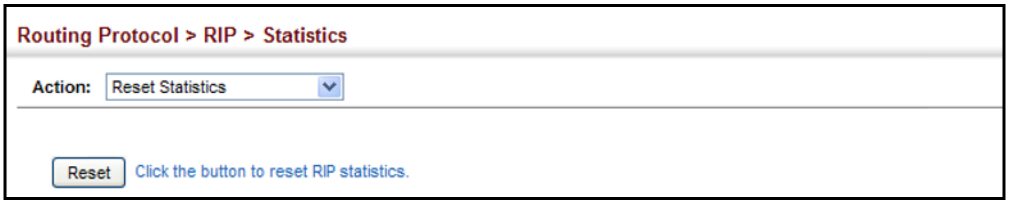
To reset RIP statistics:

1. Click Routing Protocol, RIP, Statistics.

2. Select Reset Statistics from the Action list.

3. Click Reset.

Figure 325: Resetting RIP Statistics



Routing Protocol > RIP > Statistics

Action: Reset Statistics

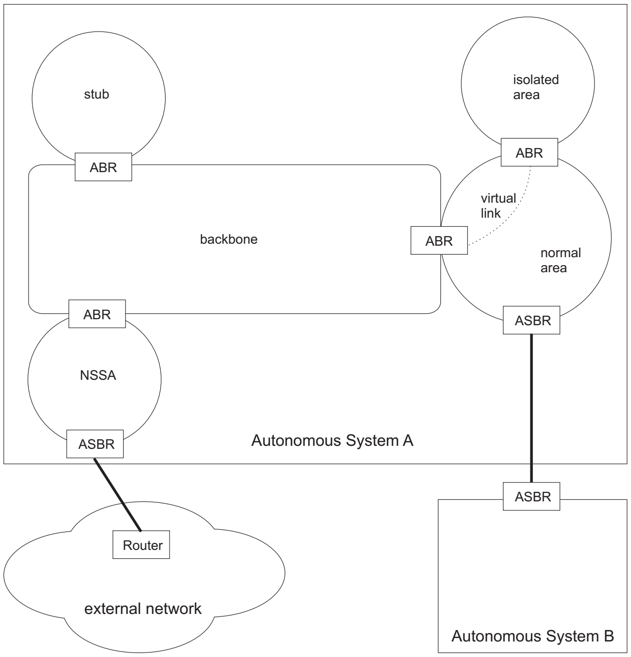
Click the button to reset RIP statistics.

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 326: 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

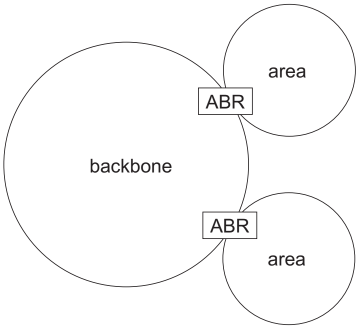
OSPF protocol broadcast messages (i.e., Link State Advertisements or LSAs) are restricted by area to limit their impact on network performance. A large network should be split up into separate OSPF areas to increase network stability, and to reduce protocol traffic by summarizing routing information 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 519). To further reduce the amount of routes passed between areas, an area can be configured as a stub (page 512, page 516) or a not-so-stubby area (page 512, page 513).

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 327: OSPF Areas



CLI REFERENCES

- "router ospf" on page 1043
- "network area" on page 1059

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 519.
- 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 in the web interface:

- **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:

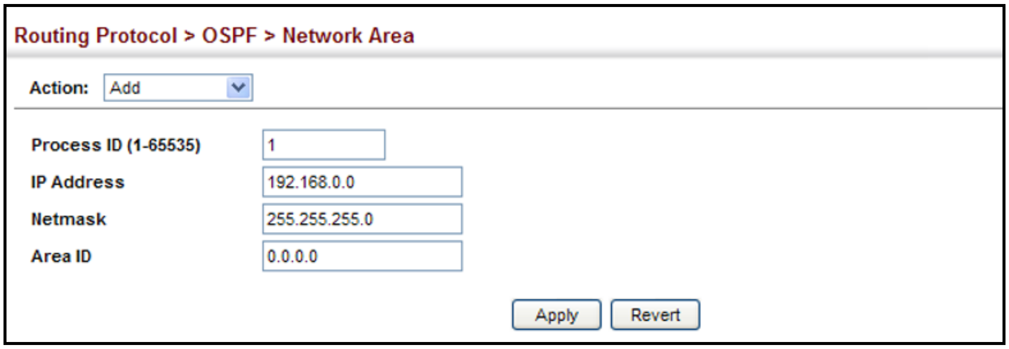
1. Click Routing Protocol, OSPF, Network Area.

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 328: Defining OSPF Network Areas Based on Addresses



Routing Protocol > OSPF > Network Area

Action: Add

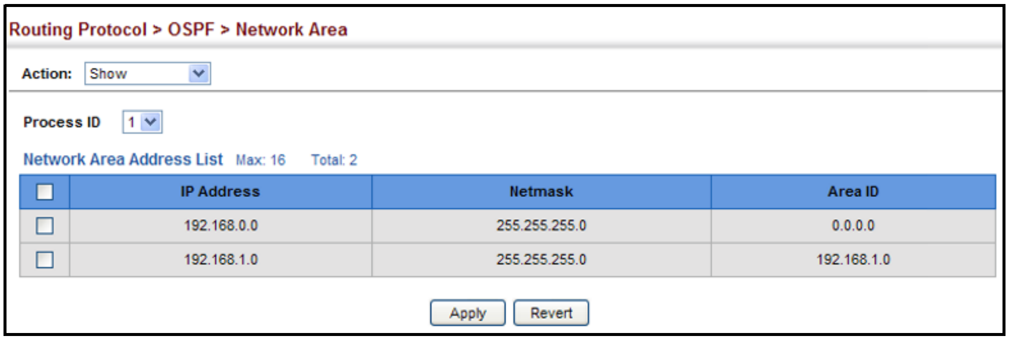
Process ID (1-65535): 1
IP Address: 192.168.0.0
Netmask: 255.255.255.0
Area ID: 0.0.0.0

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 329: Showing OSPF Network Areas



Routing Protocol > OSPF > Network Area

Action: Show

Process ID: 1

Network Area Address List Max: 16 Total: 2

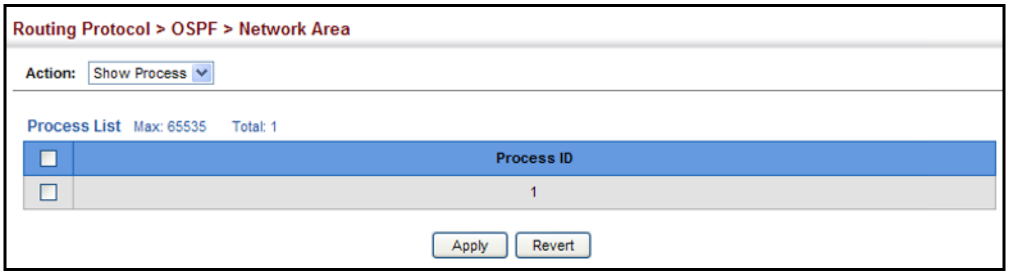
□	IP Address	Netmask	Area ID
□	192.168.0.0	255.255.255.0	0.0.0.0
□	192.168.1.0	255.255.255.0	192.168.1.0

To to show the OSPF process identifiers:

1. Click Routing Protocol, OSPF, Network Area.

2. Select Show Process from the Action list.

Figure 330: Showing OSPF Process Identifiers


Routing Protocol > OSPF > Network Area

Action: Show Process

Process List Max: 65535 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 1042

PARAMETERS

These parameters are displayed in the web interface:

- **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. Also, note that the router ID can 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 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 521). 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.

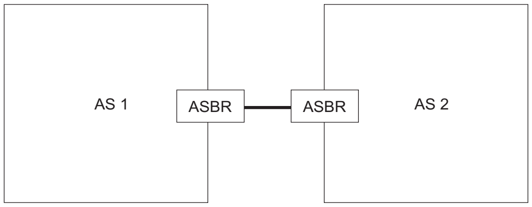
Default Information

- **Originate Default Route**[6] – 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.

[6] These are configured with the default-information originate command.

Figure 331: AS Boundary Router



- **Advertise Default Route**[6] – 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 447.)

  - **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 521.)

- **External Metric Type**[6] – 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**[6] – 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 521).

WEB INTERFACE

To configure general settings for OSPF:

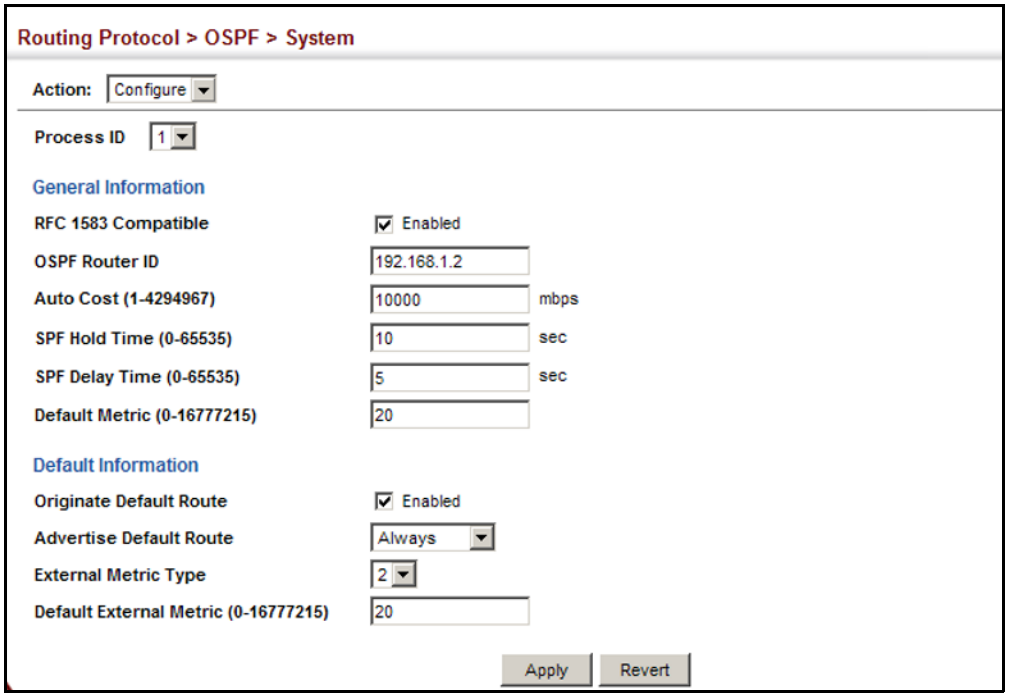
1. Click Routing Protocol, OSPF, System.

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 332: 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 1069
- "show ip protocols ospf" on page 1082

Parameters

These parameters are displayed in the web interface:

Table 26: 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 26: 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.

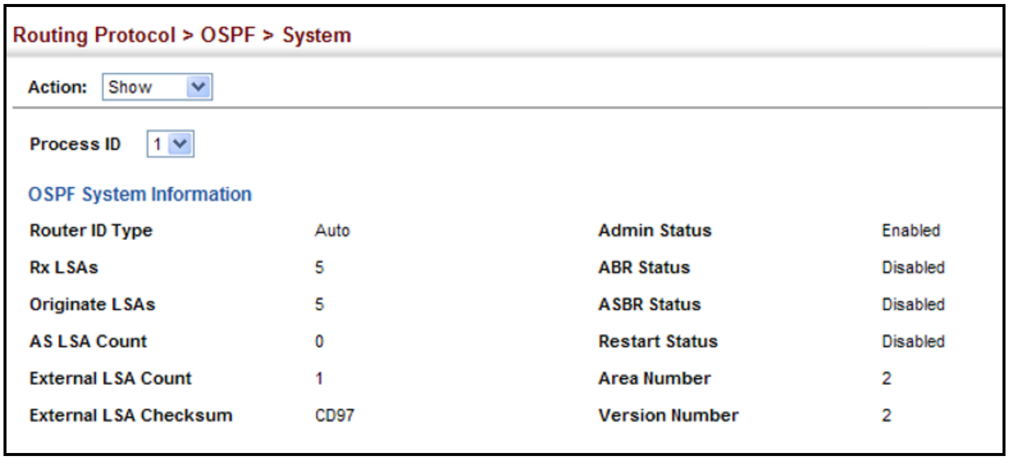
WEB INTERFACE

To show adminstrative 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 333: 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 1043
- "area stub" on page 1056
- "area nssa" on page 1054

COMMAIND USAGE

- This router supports up to 5 stubs or NSSAs.

PARAMETERS

These parameters are displayed in the web interface:

- **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.

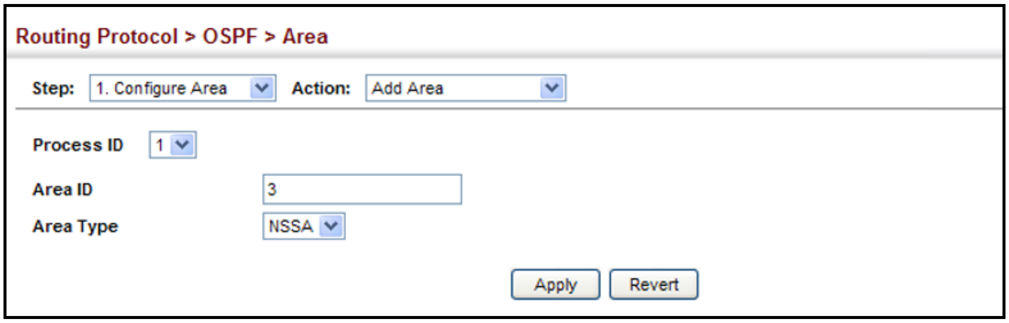
2. Select Configure Area from the Step list.

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 334: Adding an NSSA or Stub



Routing Protocol > OSPF > Area

Step: 1. Configure Area Action: Add Area

Process ID 1

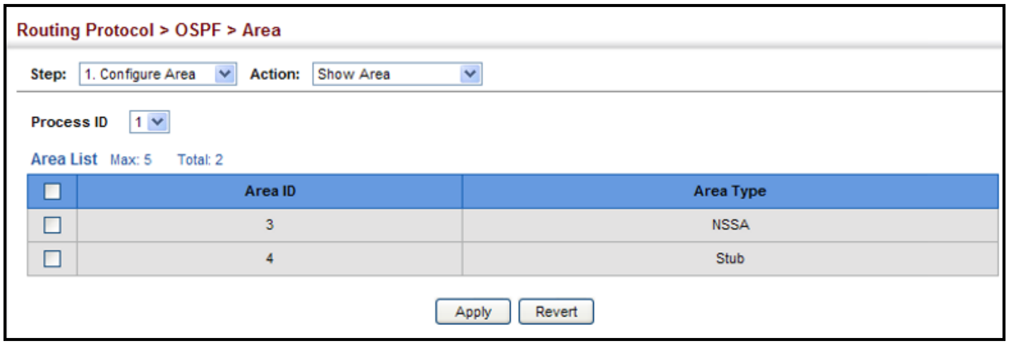
Area ID 3

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 335: Showing NSSAs or Stubs



Routing Protocol > OSPF > Area

Step: 1. Configure Area Action: Show Area

Process ID 1

Area List Max: 5 Total: 2

□	Area ID	Area Type
□	3	NSSA
□	4	Stub

CONFIGURING NSSA SETTINGS

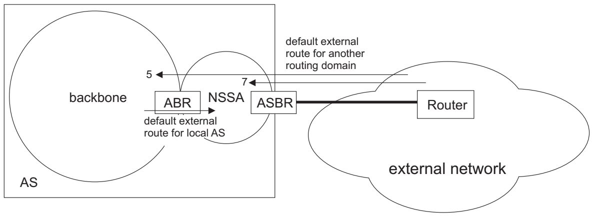
Use the Routing Protocol > OSPF > Area (Configure Area – Configure NSSA Area) page to configure protocol settings for a not-so-stubby area (NSSA).

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 336: OSPF NSSA



CLI REFERENCES

- "router ospf" on page 1043
- "area default-cost" on page 1048
- "area nssa" on page 1054

COMMAND USAGE

- Before creating an NSSA, first specify the address range for the area (see "Defining Network Areas Based on Addresses" on page 504). Then create an NSSA as described under "Adding an NSSA or Stub" on page 512.

- 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 in the web interface:

- **Process ID** – Process ID as configured in the Network Area configuration screen (see page 504).

- **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 521), 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: 1-16777214; 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 whe 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.

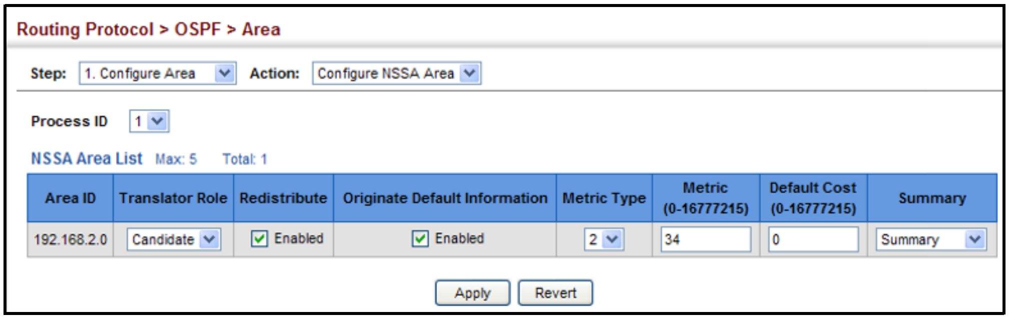
2. Select Configure Area from the Step list.

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 337: Configuring Protocol Settings for an NSSA



Routing Protocol > OSPF > Area

Step: 1. Configure Area   Action: Configure NSSA Area

Process ID 1

NSSA Area List Max: 5 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

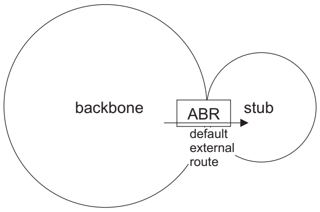
Apply Revert

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 338: 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 1043
- "area default-cost" on page 1048
- "area stub" on page 1056

COMMAND USAGE

- Before creating a stub, first specify the address range for the area (see "Defining Network Areas Based on Addresses" on page 504). Then create a stub as described under "Adding an NSSA or Stub" on page 512.
- 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 in the web interface:

- **Process ID** – Process ID as configured in the Network Area configuration screen (see page 504).
- **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 whe 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.

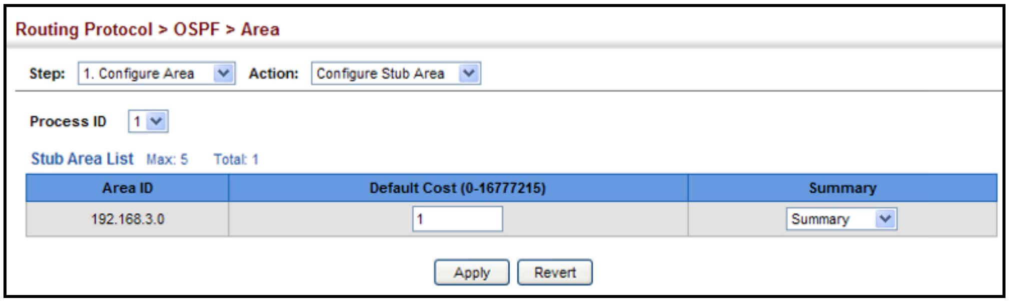
    Define an area as a totally stubby area only if routers in the area do not require summary LSAs from other areas.

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 339: Configuring Protocol Settings for a Stub



Routing Protocol > OSPF > Area

Step: 1. Configure Area Action: Configure Stub Area

Process ID 1

Stub Area List Max: 5 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 1069

PARAMETERS

These parameters are displayed in the web interface:

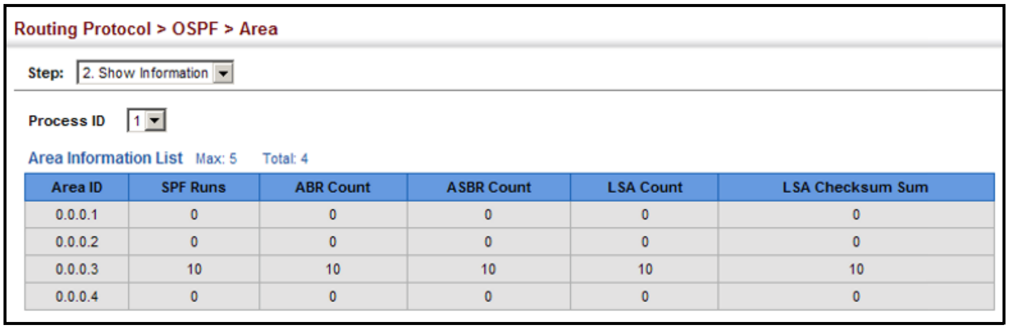
- **Process ID** – Process ID as configured in the Network Area configuration screen (see page 504).
- **Area ID** – Identifier for a not-so-stubby area (NSSA) or stub.
- **SPF Runs** – The number of times the Shortest Path First algorithim has been run for this area.
- **ABR Count** – The number of Area Border Routers attached to this area.
- **ASBR Count** – The number of Autonomous System Boundary Routers attaced 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 340: Displaying Information on NSSA and Stub Areas



Routing Protocol > OSPF > Area

Step: 2. Show Information

Process ID 1

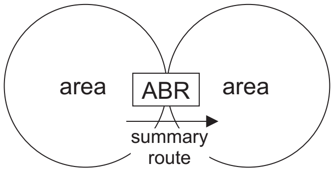
Area Information List Max: 5 Total: 4

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 341: Route Summarization for ABRs



CLI REFERENCES

- "router ospf" on page 1043
- "area range" on page 1049

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 519).

- This router supports up five summary routes for area ranges.

PARAMETERS

These parameters are displayed in the web interface:

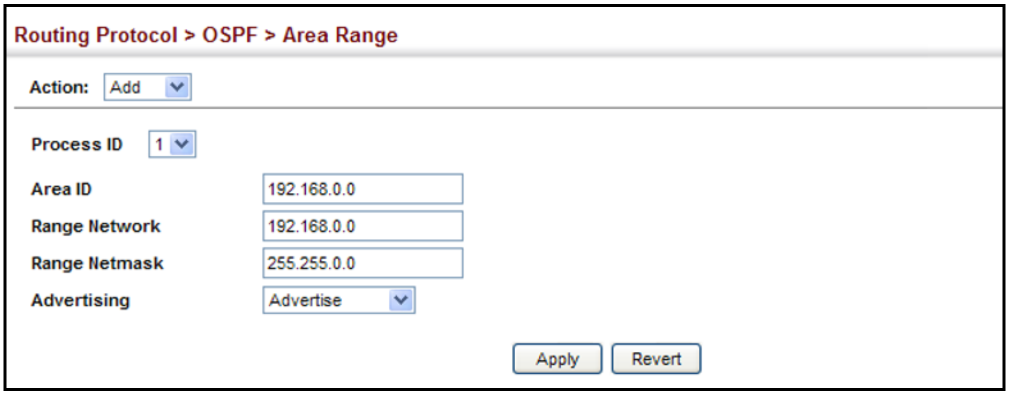
- **Process ID** – Process ID as configured in the Network Area configuration screen (see page 504).
- **Area ID** – Identifies an area for which the routes are summarized. The area ID can be in the form of an IPv4 address, or also as a four octet unsigned integer ranging from 0-4294967295.
- **Range 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 342: Configuring Route Summaries for an Area Range



Routing Protocol > OSPF > Area Range

Action: Add

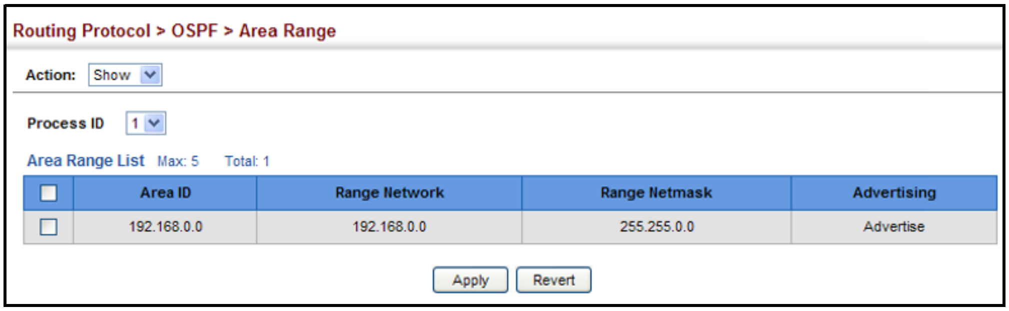
Process ID: 1
Area ID: 192.168.0.0
Range Network: 192.168.0.0
Range Netmask: 255.255.0.0
Advertising: Advertise

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 343: Showing Configured Route Summaries



Routing Protocol > OSPF > Area Range

Action: Show

Process ID 1

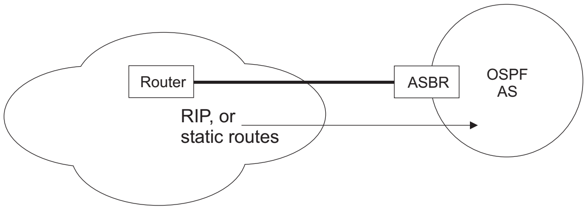
Area Range List Max: 5 Total: 1

□	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 344: Redistributing External Routes



CLI REFERENCES

- "router ospf" on page 1043
- "redistribute" on page 1052

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 507).

PARAMETERS

These parameters are displayed in the web interface:

- **Process ID** – Process ID as configured in the Network Area configuration screen (see page 504).

- **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 507).

- **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:

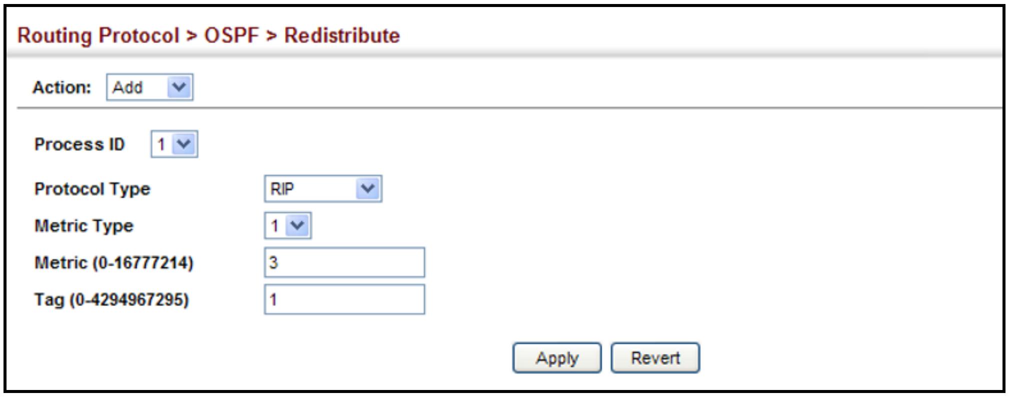
1. Click Routing Protocol, OSPF, Redistribute.

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 345: Importing External Routes


Routing Protocol > OSPF > Redistribute

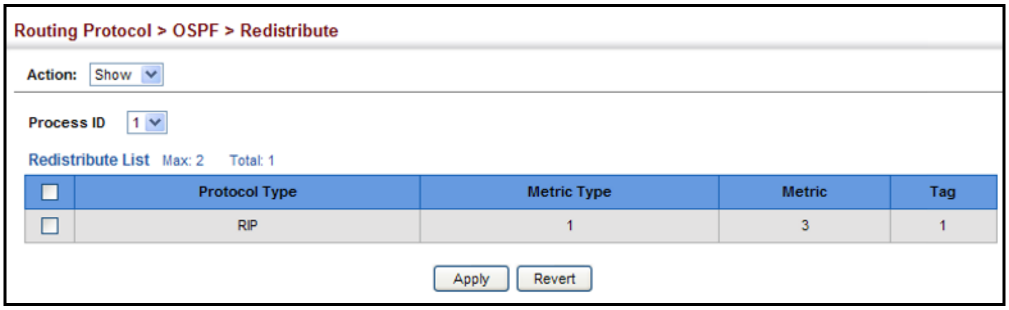
Action: Add

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 346: Showing Imported External Route Types


Routing Protocol > OSPF > Redistribute

Action: Show

Process ID 1

Redistribute List Max: 2 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 numer 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 1043
- "summary-address" on page 1053

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 519).
- This router supports up 20 Type-5 summary routes.

PARAMETERS

These parameters are displayed in the web interface:

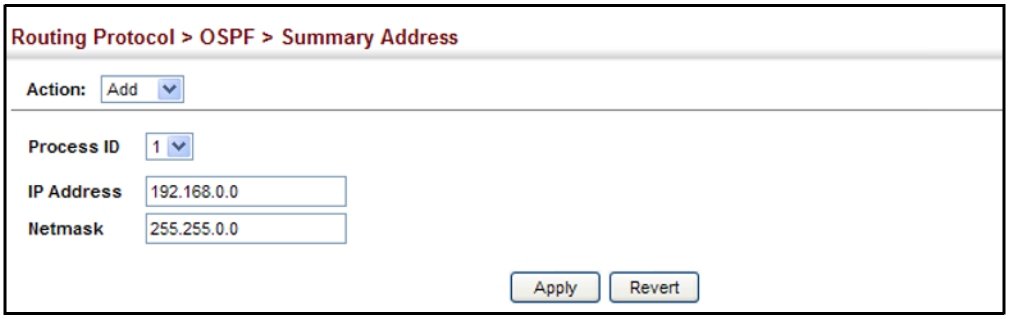
- **Process ID** – Process ID as configured in the Network Area configuration screen (see page 504).
- **IP Address** – Summary address covering a range of addresses.
- **Netmask** – Network mask for the summary route.

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 347: Summarizing External Routes



Routing Protocol > OSPF > Summary Address

Action: Add

Process ID: 1

IP Address: 192.168.0.0

Netmask: 255.255.0.0

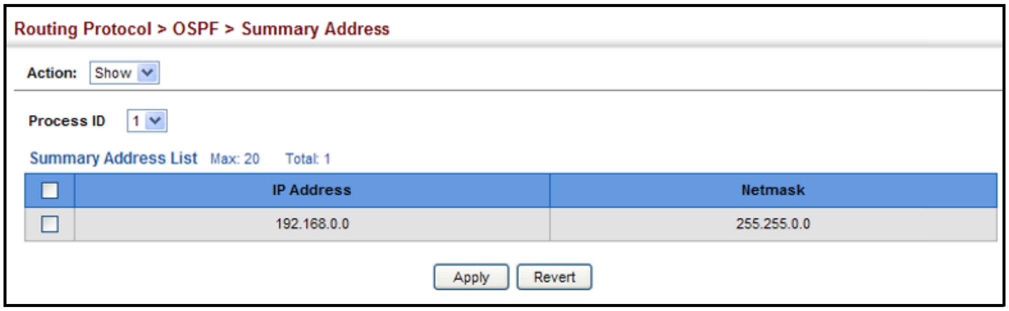
To show the summary addresses for external routes:

1. Click Routing Protocol, OSPF, Summary Address.

2. Select Show from the Action list.

3. Select the process ID.

Figure 348: Showing Summary Addresses for External Routes



Routing Protocol > OSPF > Summary Address

Action: Show

Process ID 1

Summary Address List Max: 20 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 1042

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 504).

- 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 504).

PARAMETERS

These parameters are displayed in the web interface:

- **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 resending 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.

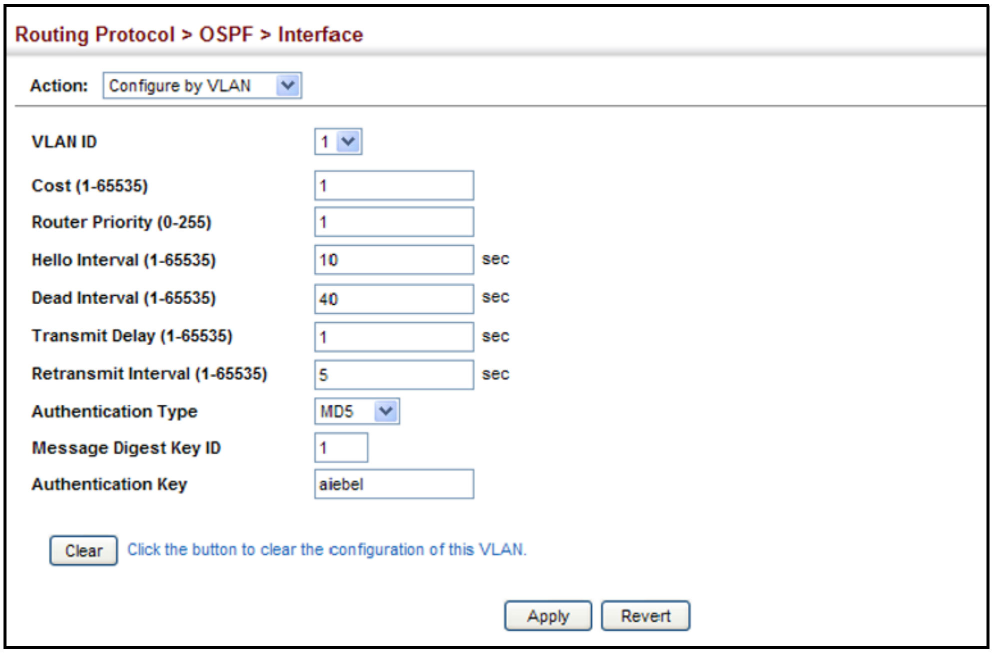
  Before setting a new key indentifier, the current key must first be deleted on the Show MD5 Key page.

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 349: Configuring Settings for All Interfaces Assigned to a VLAN



Routing Protocol > OSPF > Interface

Action: Configure by VLAN

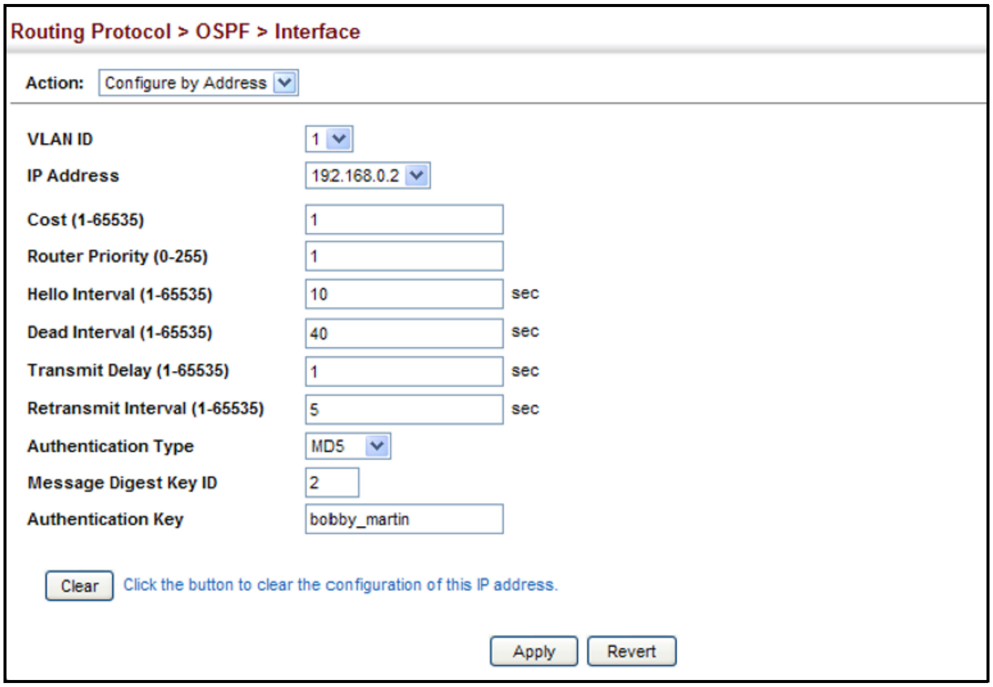
VLAN ID	1	
Cost (1-65535)	1	
Router Priority (0-255)	1	
Hello Interval (1-65535)	10	sec
Dead Interval (1-65535)	40	sec
Transmit Delay (1-65535)	1	sec
Retransmit Interval (1-65535)	5	sec
Authentication Type	MD5	
Message Digest Key ID	1	
Authentication Key	aiebel	

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 350: Configuring Settings for a Specific Area Assigned to a VLAN



Routing Protocol > OSPF > Interface

Action: Configure by Address

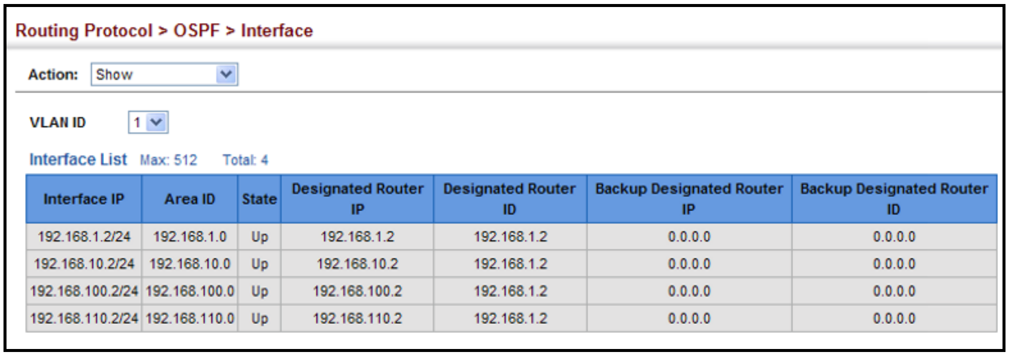
VLAN ID	1
IP Address	192.168.0.2
Cost (1-65535)	1
Router Priority (0-255)	1
Hello Interval (1-65535)	10 sec
Dead Interval (1-65535)	40 sec
Transmit Delay (1-65535)	1 sec
Retransmit Interval (1-65535)	5 sec
Authentication Type	MD5
Message Digest Key ID	2
Authentication Key	bobby_martin

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 351: Showing OSPF Interfaces



Routing Protocol > OSPF > Interface

Action: Show

VLAN ID 1

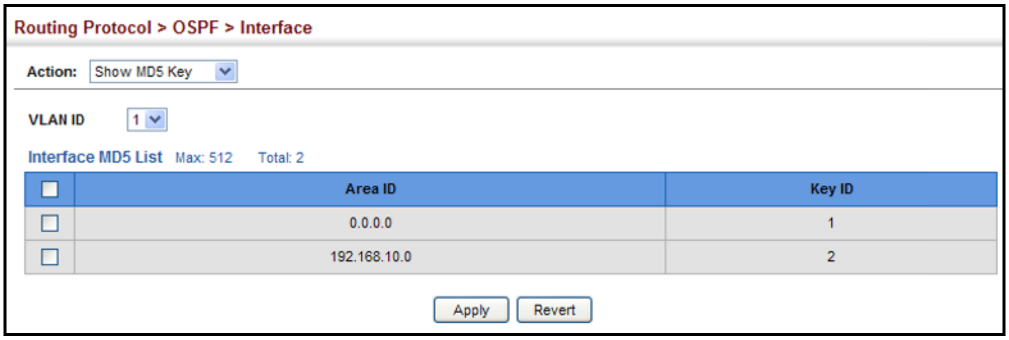
Interface List Max: 512 Total: 4

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 352: Showing MD5 Authentication Keys



Routing Protocol > OSPF > Interface

Action: Show MD5 Key

VLAN ID 1

Interface MD5 List Max: 512 Total: 2

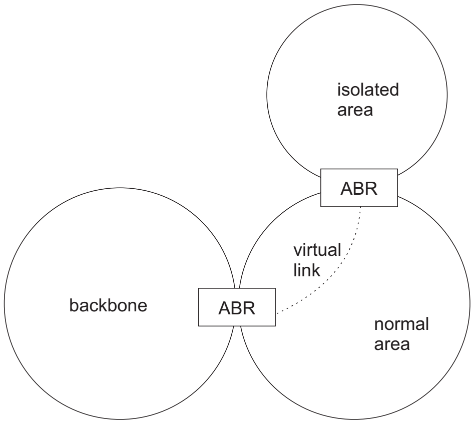
□	Area ID	Key ID
□	0.0.0.0	1
□	192.168.10.0	2

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 353: 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 1043
- "area virtual-link" on page 1057

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 525.

Parameters

These parameters are displayed in the web interface:

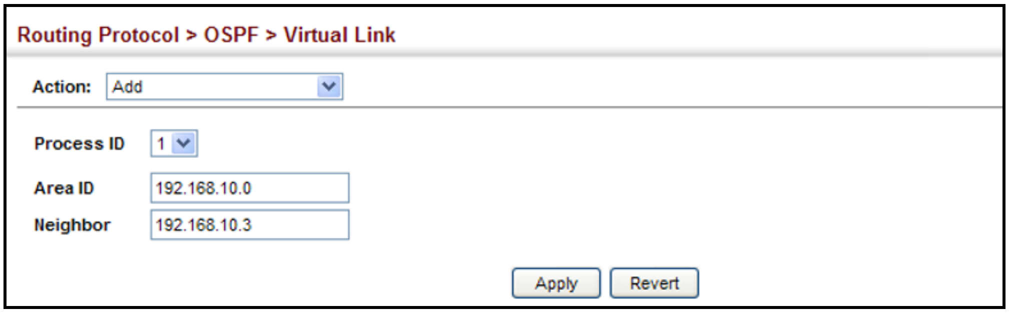
- **Process ID** – Process ID as configured in the Network Area configuration screen (see page 504).
- **Area ID** – Identifies the transit area for the virtual link. The area ID must be in the form of an IPv4 address, or also as a four octet unsigned integer ranging from 0-4294967295.
- **Neighbor** – 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 354: Adding a Virtual Link



Routing Protocol > OSPF > Virtual Link

Action: Add

Process ID: 1

Area ID: 192.168.10.0

Neighbor: 192.168.10.3

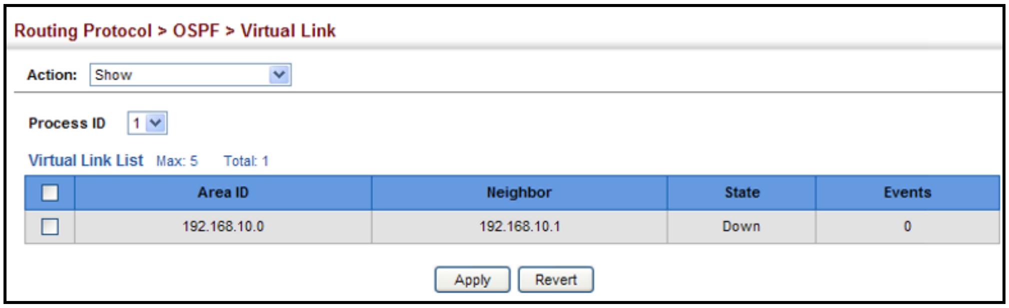
To show virtual links:

1. Click Routing Protocol, OSPF, Virtual Link.

2. Select Show from the Action list.

3. Select the process ID.

Figure 355: Showing Virtual Links



Routing Protocol > OSPF > Virtual Link

Action: Show

Process ID 1

Virtual Link List Max: 5 Total: 1

□	Area ID	Neighbor	State	Events
□	192.168.10.0	192.168.10.1	Down	0

To configure detailed settings for a virtual link:

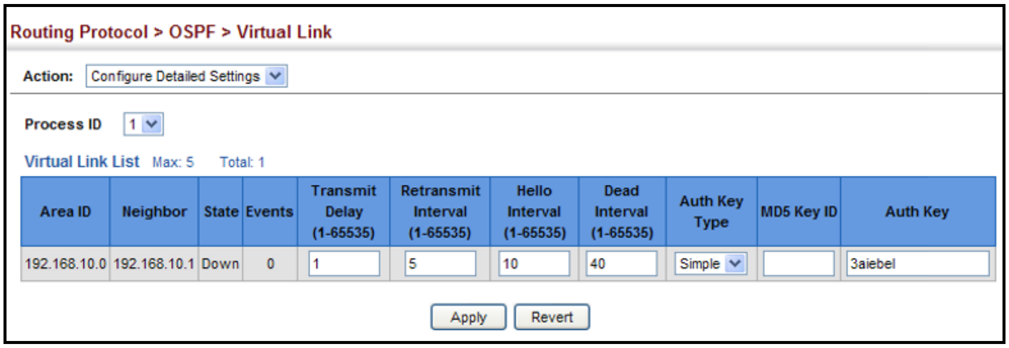
1. Click Routing Protocol, OSPF, Virtual Link.

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 356: Configuring Detailed Settings for a Virtual Link



Routing Protocol > OSPF > Virtual Link

Action: Configure Detailed Settings

Process ID 1

Virtual Link List Max: 5 Total: 1

Area ID	Neighbor	State	Events	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	192.168.10.1	Down	0	1	5	10	40	Simple		3aiebel

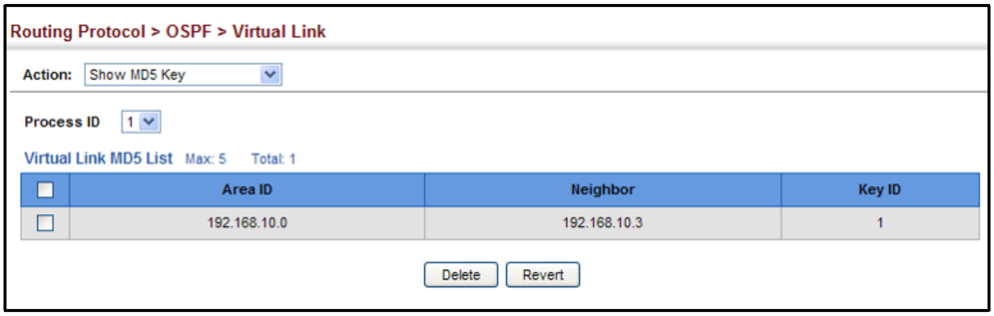
To show the MD5 authentication keys configured for a virtual link:

1. Click Routing Protocol, OSPF, Interface.

2. Select Show MD5 Key from the Action list.

3. Select the VLAN ID.

Figure 357: Showing MD5 Authentication Keys



Routing Protocol > OSPF > Virtual Link

Action: Show MD5 Key

Process ID 1

Virtual Link MD5 List Max: 5 Total: 1

□	Area ID	Neighbor	Key ID
□	192.168.10.0	192.168.10.3	1

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 1072

PARAMETERS

These parameters are displayed in the web interface:

- **Process ID** – Process ID as configured in the Network Area configuration screen (see page 504).
- **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:

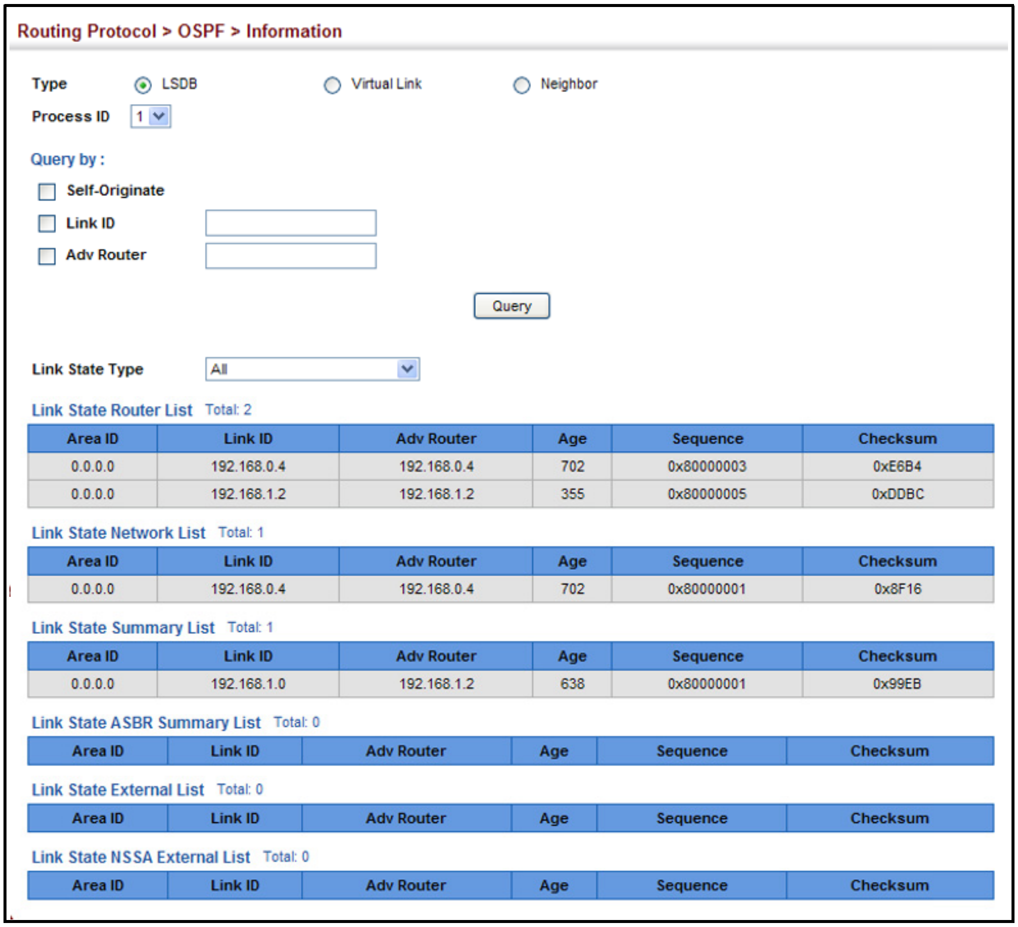
- **Area ID** – Area defined for which LSA information is to be displayed.
- **Link ID** – Network portion described by an LSA. The Link ID is either:
  - An IP network number for Type 3 Summary and Type 5 AS External LSAs. (When an Type 5 AS External LSA is describing a default route, its Link ID is 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 358: Displaying Information in the Link State Database



Routing Protocol > OSPF > Information

Type ● LSDB ○ Virtual Link ○ 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 VIRTUAL LINKS

Use the Routing Protocol > OSPF > Information (Virtual Link) page to show the Link State Advertisements (LSAs) stored in the link state database for virtual links.

CLI REFERENCES

- "show ip ospf virtual-links" on page 1081

PARAMETERS

These parameters are displayed in the web interface:

- **Process ID** – Process ID as configured in the Network Area configuration screen (see page 504).

Information displayed for each LSA entry includes:

- **Name** – Index for LSA entries.

- **Interface** – Interface through which the virtual neighbor can be reached.

- **Transit Area** – Common area the virtual link crosses to reach the target router. This identifier is in the form of an IP address.

- **Router ID** – Virtual neighbor's router ID.

- **Status** – Indicates if the link is up or down.

- **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.

- **Hello Due** – The number of seconds before the next hello message is due. This time is determined by the Hello Interval which must be the same for all router attached to a common network.

- **Adjacency State** – The state of the virtual neighbor relationship:

  - 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

WEB INTERFACE

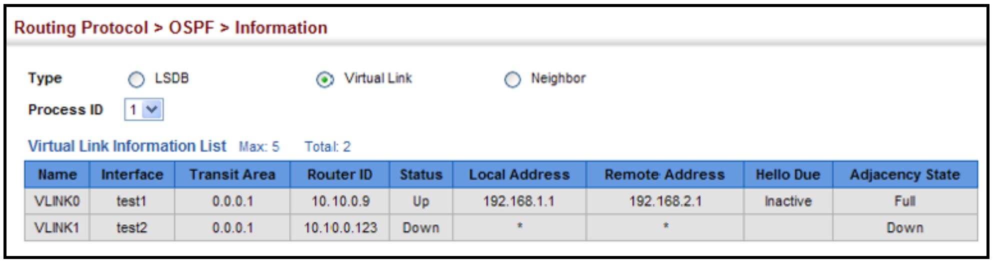
To display information about virtual links stored in the link state database:

1. Click Routing Protocol, OSPF, Information.

2. Click Virtual Link.

3. Select the process identifier.

Figure 359: Displaying Virtual Links Stored in the Link State Database



Type ○ LSDB ● Virtual Link ○ Neighbor

Process ID 1

Virtual Link Information List Max: 5 Total: 2

Name	Interface	Transit Area	Router ID	Status	Local Address	Remote Address	Hello Due	Adjacency State
VLINK0	test1	0.0.0.1	10.10.0.9	Up	192.168.1.1	192.168.2.1	Inactive	Full
VLINK1	test2	0.0.0.1	10.10.0.123	Down	*	*		Down

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 1080

PARAMETERS

These parameters are displayed in the web interface:

- **Process ID** – Process ID as configured in the Network Area configuration screen (see page 504).
- **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.

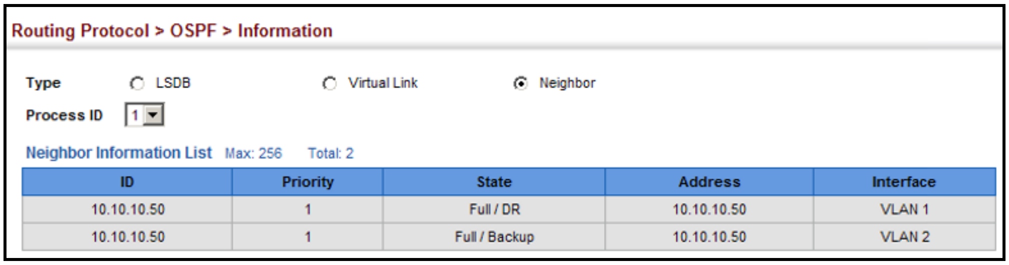
WEB INTERFACE

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 360: Displaying Neighbor Routers Stored in the Link State Database



Routing Protocol > OSPF > Information

Type ○ LSDB ○ Virtual Link ● Neighbor

Process ID 1

Neighbor Information List Max: 256 Total: 2

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.

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 Listerner 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 a Multicast Router" on page 395).

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 on page 548). Note that only one IPv4 multicast routing protocol (PIM-DM or PIM-SM) can be enabled on any given interface.

ENABLING MULTICAST ROUTING GLOBALLY

Use the Multicast > Multicast Routing > General page to enable IP multicast routing globally on the switch.

CLI REFERENCES

- "ip multicast-routing" on page 1085

PARAMETERS

These parameters are displayed in the web interface:

- **Multicast Forwarding Status** – Enables IP multicast routing. (Default: Disabled)

WEB INTERFACE

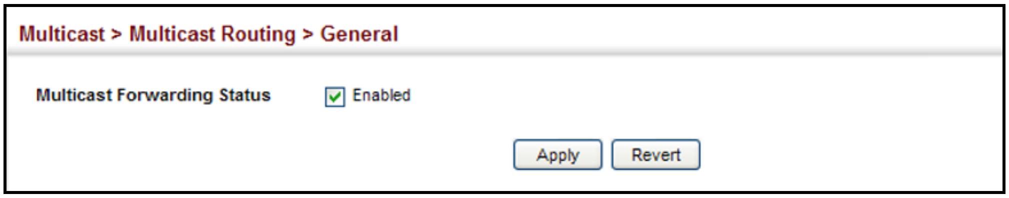
To enable multicast routing:

1. Click Multicast, Multicast Routing, General.

2. Enable Multicast Forwarding Status.

3. Click Apply.

Figure 361: Enabling Multicast Routing



Multicast > Multicast Routing > General

Multicast Forwarding Status ☑ Enabled

DISPLAYING THE MULTICAST ROUTING TABLE

Use the Multicast > Multicast Routing > Information page to display information on each multicast route it 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 1086

PARAMETERS

These parameters are displayed in the web interface:

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.)
- **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).
- **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).
- **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 –

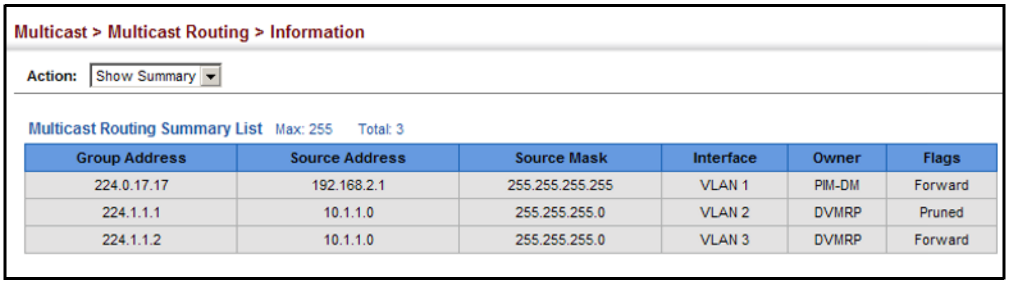
- **Interface** – Interface(s) on which multicast subscribers have been recorded.
- **State** – The flags associated with each downstream interface indicate:
  - **Forward** – Traffic received from the upstream interface is being forwarded to this interface.
  - **Local** – Downstream interface has received 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

To display the multicast routing table:

1. Click Multicast, Multicast Routing, Information.
2. Select Show Summary from the Action List.

Figure 362: Displaying the Multicast Routing Table



Multicast > Multicast Routing > Information

Action: Show Summary

Multicast Routing Summary List Max: 255 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:

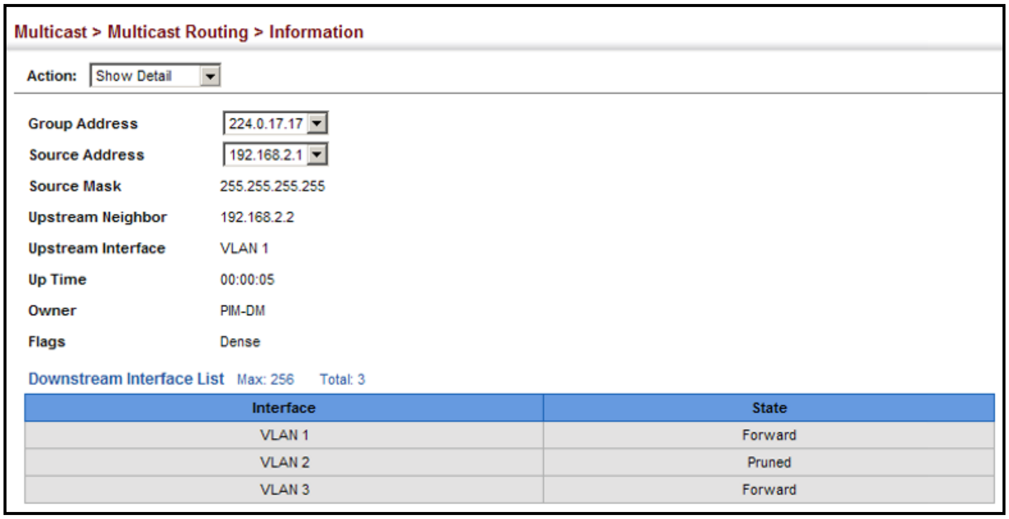
1. Click Multicast, Multicast Routing, Information.

2. Select Show Details from the Action List.

3. Select a Group Address.

4. Select a Source Address.

Figure 363: Displaying Detailed Entries from the Multicast Routing Table



Multicast > Multicast Routing > Information

Action: Show Detail

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 Max: 256 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 1091

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 548), 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 544).

WEB INTERFACE

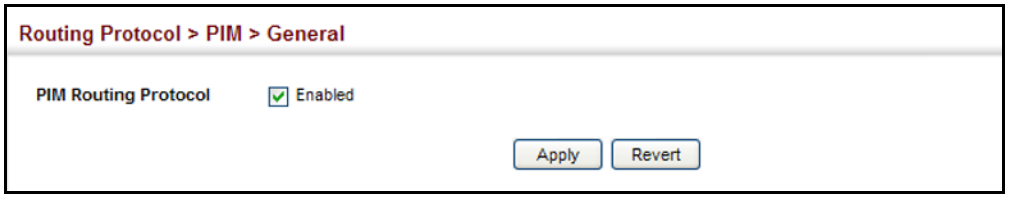
To enable PIM multicast routing:

1. Click Routing Protocol, PIM, General.

2. Enable PIM Routing Protocol.

3. Click Apply.

Figure 364: 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

- "PIM Commands" on page 1090

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 391). 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 in the web interface:

Common Attributes

- **VLAN** – Layer 3 VLAN interface. (Range: 1-4093)

- **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 propogation 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 propogation 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 propgated 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

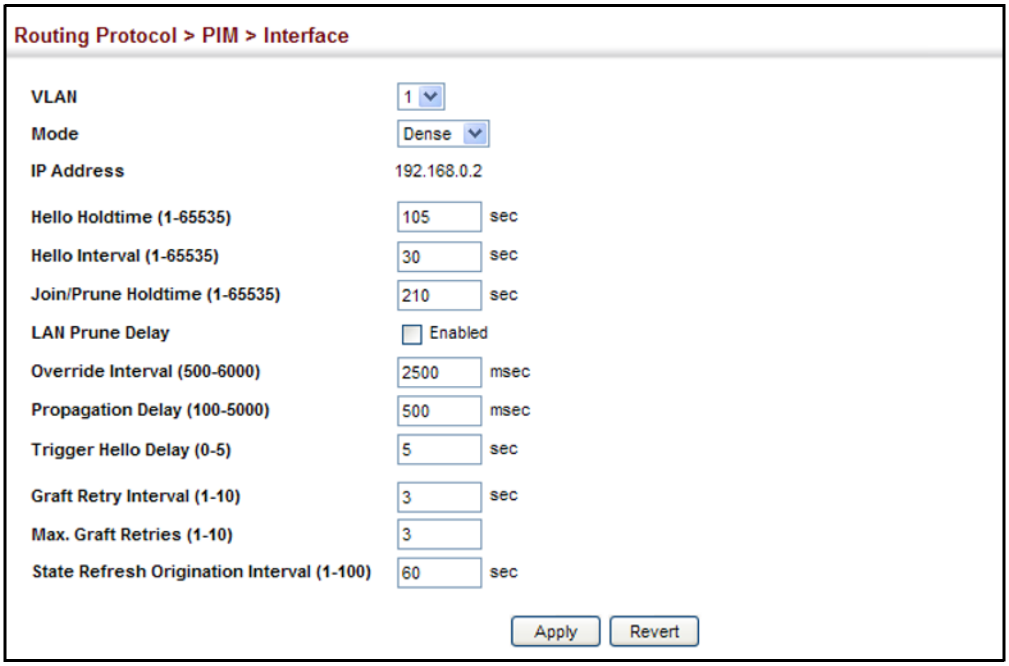
To configure PIM interface settings:

1. Click Routing Protocol, PIM, Interface.

2. Modify any of the protocol parameters as required.

3. Click Apply.

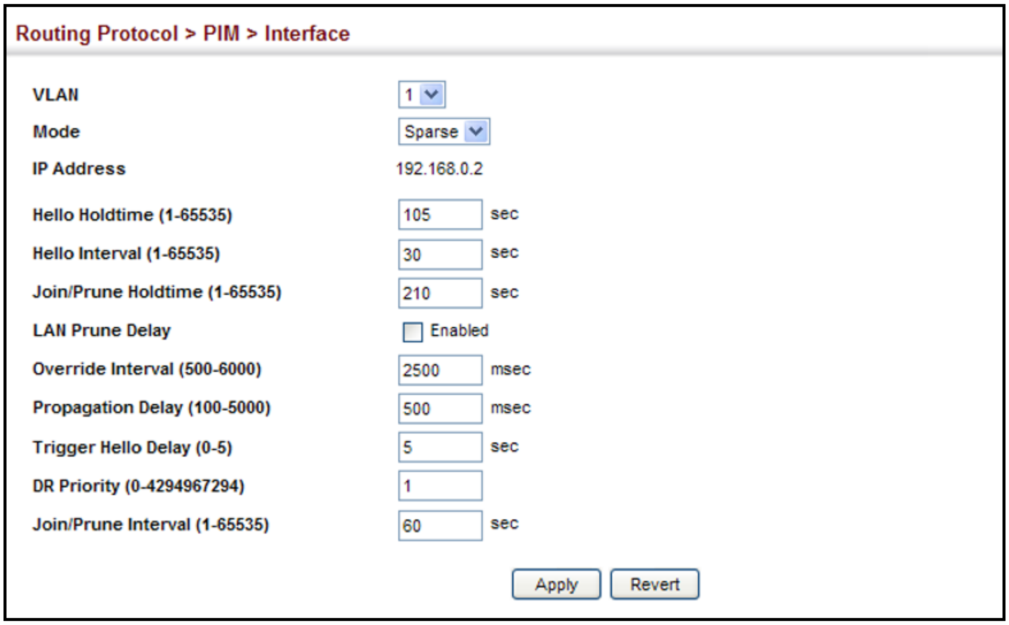
Figure 365: Configuring PIM Interface Settings (Dense Mode)



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 366: 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 NEIGHBOR INFORMATION

Use the Routing Protocol > PIM > Neighbor page to display all neighboring PIM routers.

CLI REFERENCES

- "show ip pim neighbor" on page 1098

PARAMETERS

These parameters are displayed in the web interface:

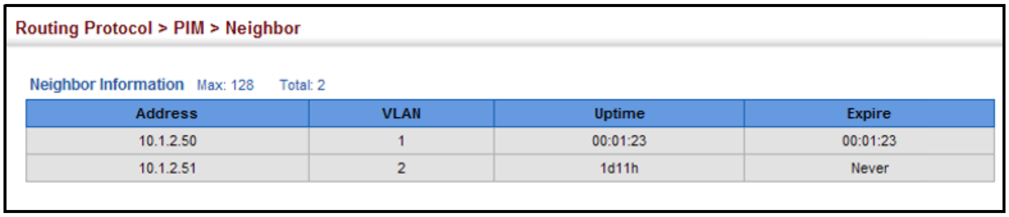
- **Address** – IP address of the next-hop router.
- **VLAN** – VLAN that is attached to this neighbor.
- **Uptime** – The duration this entry has been active.
- **Expire** – The time before this entry will be removed.

WEB INTERFACE

To display neighboring PIM routers:

1. Click Routing Protocol, PIM, Neighbor.

Figure 367: Showing PIM Neighbors



Routing Protocol > PIM > Neighbor

Neighbor Information Max: 128 Total: 2

Address	VLAN	Uptime	Expire
10.1.2.50	1	00:01:23	00:01:23
10.1.2.51	2	1d11h	Never

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

- "PIM Commands" on page 1090

PARAMETERS

These parameters are displayed in the web interface:

- **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 desginated 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, or 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 to force the router to use the shared tree for all multicast groups, or just for the specified multicast groups.

- **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:

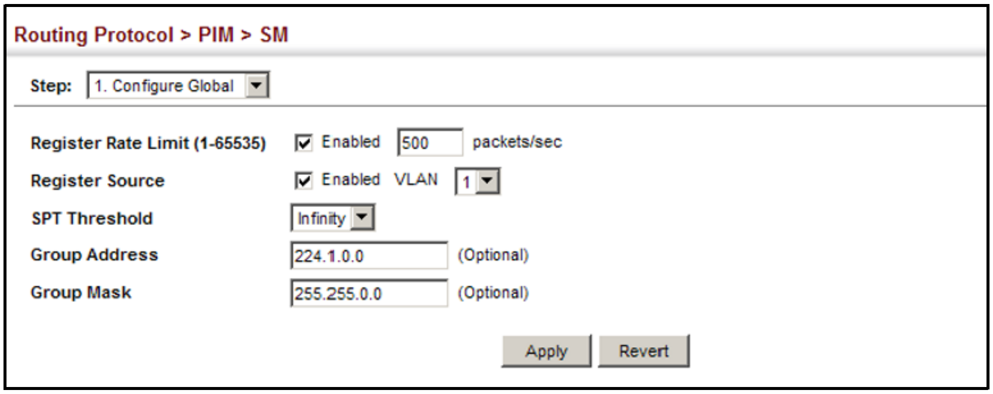
1. Click Multicast, Multicast Routing, SM.

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 368: 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 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 1101

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 in the web interface:

- **BSR Candidate Status** – Configures the switch as a Bootstrap Router (BSR) candidate. (Default: Disabled)

- **VLAN ID** – Identifier of configured VLAN interface. (Range: 1-4093)

- **Hash Mask Length** – Hash mask length (in bits) used for RP selection (see "Configuring a Static Rendezvous Point" on page 557 and "Configuring an RP Candidate" on page 559). 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)

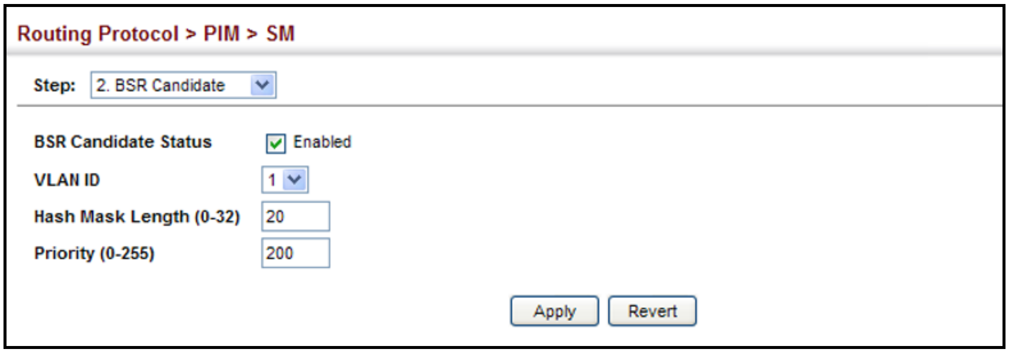
- **Priority** – Priority used by the candidate bootstrap router in the election process. The BSR candidate with the largest priority is preferred. If the priority values are the same, the candidate with the larger IP address is elected to be the BSR. Setting the priority to zero means that this router 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 Multicast, Multicast Routing, 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 369: Configuring a 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 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 1104

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 in the web interface:

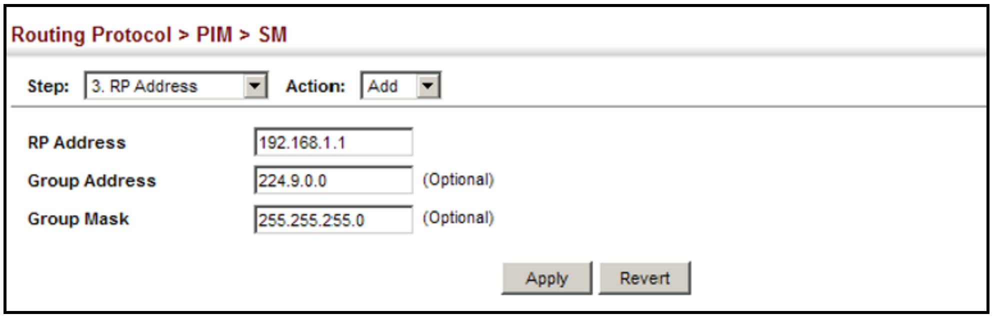
- **RP Address** – Static IP address of the router that will be an RP for the specified multicast group(s).
- **Group Address** – An IP multicast group address. If a group address is not specified, the RP is used for all multicast groups.
- **Group Mask** – Subnet mask that is used for the group address.

WEB INTERFACE

To configure a static rendezvous point:

1. Click Multicast, Multicast Routing, 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 370: Configuring a 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)

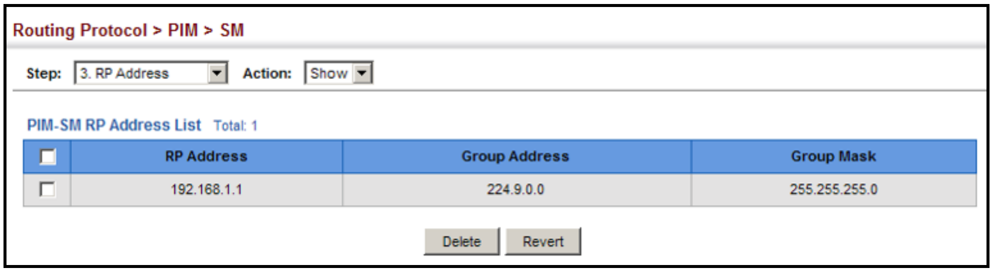
To display static rendezvous points:

1. Click Multicast, Multicast Routing, SM.

2. Select RP Address from the Step list.

3. Select Show from the Action list.

Figure 371: Showing 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 AN 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 1105

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 in the web interface:

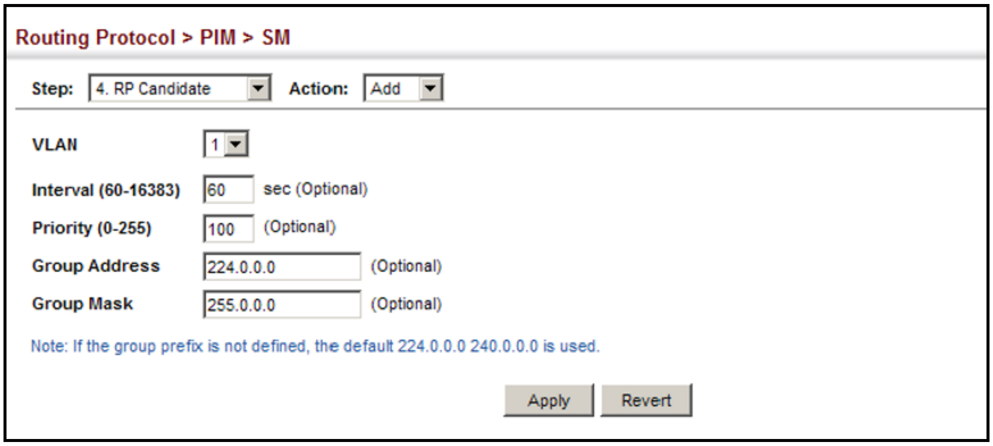
- **VLAN** – Identifier of configured VLAN interface. (Range: 1-4093)
- **Interval** – The interval at which this device advertises itself as an RP candidate. (Range: 60-16383 seconds; Default: 60 seconds)
- **Priority** – Priority used by the candidate RP in the election process. The RP candidate with 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.
- **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 372: Configuring an RP Candidate



Routing Protocol > PIM > SM

Step: 4. RP Candidate Action: Add

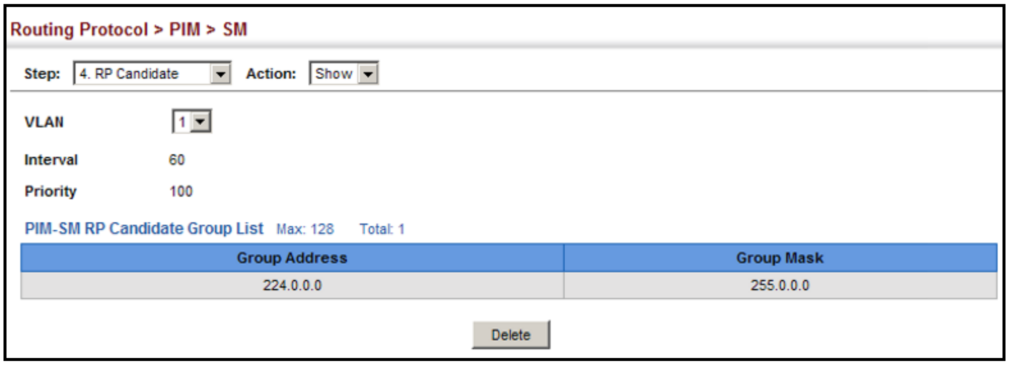
VLAN	1	
Interval (60-16383)	60	sec (Optional)
Priority (0-255)	100	(Optional)
Group Address	224.0.0.0	(Optional)
Group Mask	255.0.0.0	(Optional)

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 Multicast, Multicast Routing, 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 373: Showing Settings for an RP Candidate



Routing Protocol > PIM > SM

Step: 4. RP Candidate Action: Show

VLAN	1
Interval	60
Priority	100

PIM-SM RP Candidate Group List Max: 128 Total: 1

Group Address	Group Mask
224.0.0.0	255.0.0.0

DISPLAYING THE 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 1110

PARAMETERS

These parameters are displayed in the web interface:

- **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**[7] – 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.

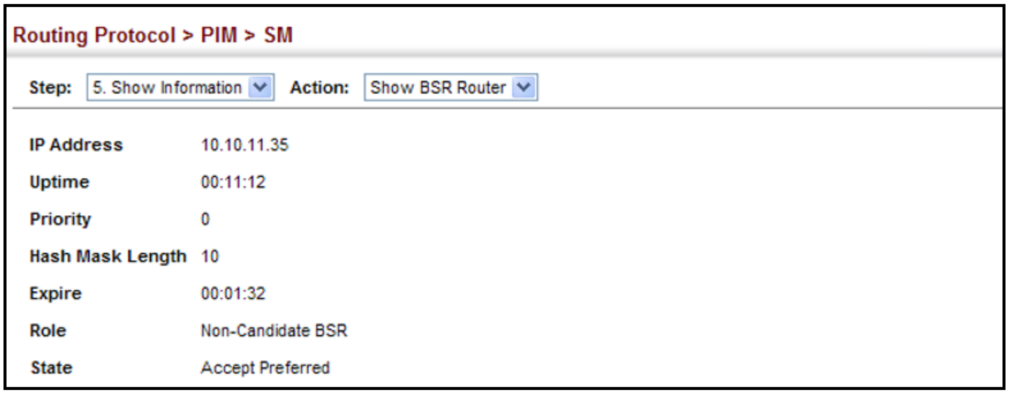
WEB INTERFACE

To display information about the BSR:

1. Click Multicast, Multicast Routing, SM.
2. Select Show Information from the Step list.
3. Select Show BSR Router from the Action list.

[7] These parameters are based on RFC 5059.

Figure 374: Showing Information About the BSR



Routing Protocol > PIM > SM

Step: 5. Show Information Action: Show BSR Router

IP Address	10.10.11.35
Uptime	00:11:12
Priority	0
Hash Mask Length	10
Expire	00:01:32
Role	Non-Candidate BSR
State	Accept Preferred

DISPLAYING 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 1111

PARAMETERS

These parameters are displayed in the web interface:

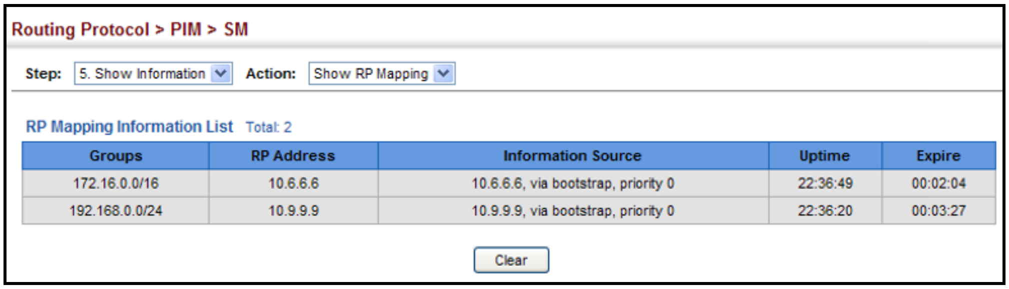
- **Groups** – A multicast group address.
- **RP Address** – IP address of the RP for the listed multicast group.
- **Information Source** – RP that advertised the mapping, how the RP was selected (Static or Bootstrap), and the priority used in the bidding process.
- **Uptime** – The time this RP has 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 375: Showing RP Mapping



Routing Protocol > PIM > SM

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

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:

- "General Commands" on page 579
- "System Management Commands" on page 587
- "SNMP Commands" on page 629
- "Remote Monitoring Commands" on page 649
- "Authentication Commands" on page 657
- "General Security Measures" on page 707
- "Access Control Lists" on page 747
- "Interface Commands" on page 769
- "Link Aggregation Commands" on page 787
- "Port Mirroring Commands" on page 797
- "Rate Limit Commands" on page 801
- "Address Table Commands" on page 803
- "Spanning Tree Commands" on page 807
- "VLAN Commands" on page 831
- "Class of Service Commands" on page 871
- "Quality of Service Commands" on page 885
- "Multicast Filtering Commands" on page 903
- "LLDP Commands" on page 951

- "Domain Name Service Commands" on page 969
- "DHCP Commands" on page 979
- "VRRP Commands" on page 995
- "IP Interface Commands" on page 1005
- "IP Routing Commands" on page 1019
- "Multicast Routing Commands" on page 1085

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 ECS4610-24F 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 ECS4610-24F is opened.
  To end the CLI session, enter [Exit].

Vty-0#
```

NOTE: You can open up to four 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.

COMMANDCOMPLETION

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 the specified accounting list
  arp                   Information of ARP cache
  authorization         Authorization configurations
  bridge-ext            Bridge extension information
  cable-diagnostics     Shows the information of cable diagnostics
  calendar              Date and time information
  class-map             Displays class maps
  dns                   DNS information
  dot1q-tunnel          802.1Q tunnel
  dot1x                 802.1X content
  garp                  GARP properties
  gvrp                  GVRP interface information
  history               Shows history information
  hosts                 Host information
  interfaces            Shows interface information
  ip                    IP information
  ipv6                  IPv6 information
  lacp                  LACP statistics
  line                  TTY line information
  lldp                  LLDP
  log                   Log records
  logging               Logging setting
  loop                  Shows the information of loopback
  mac                   MAC access list
  mac-address-table     Configuration of the address table
  mac-vlan              MAC-based VLAN information
  management            Shows management information
  map                   Maps priority
  mvr                   Multicast VLAN registration
  network-access        Shows the entries of the secure port
  nlm                   Show notification log
  policy-map            Displays policy maps
  port                  Port characteristics
  protocol-vlan         Protocol-VLAN information
  public-key            Public key information
  queue                 Priority queue information
  radius-server         RADIUS server information
  rmon                  Remote Monitoring Protocol
  running-config        Information on the running configuration
  snmp                  Simple Network Management Protocol configuration and
                        statistics
  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
  system                System information
  tacacs-server         TACACS server information
  users                 Information about users logged in
  version               System hardware and software versions
  vlan                  Shows virtual LAN settings
  voice                 Shows the voice VLAN information
  vrrp                  Shows VRRP
Console#show
```

The command "**show interfaces ?**" will display the following information:

```
Console#show interfaces ?
  counters       Interface counters information
  protocol-vlan  Protocol-VLAN information
  status         Shows interface status
  switchport     Shows interface switchport information
Console#
```

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?
snmp            sntp           spanning-tree   ssh             startup-config
subnet-vlan     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 27: General Command Modes

Class	Mode	
Exec	Normal Privileged	
Configuration	Global*	Access Control List Class Map DHCP IGMP Profile Interface Line Multiple Spanning Tree Policy 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 ECS4610-24F is opened.
  To end the CLI session, enter [Exit].

Console#
```

```
Username: guest
Password: [guest login password]

  CLI session with the ECS4610-24F 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.
- Class Map Configuration - Creates a DiffServ class map for a specified traffic type.
- IGMP Profile - Sets a profile group and enters IGMP filter profile configuration mode.
- DHCP Configuration - These commands are used to configure the DHCP server.
- 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.
- 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 28: Configuration Command Modes

Mode	Command	Prompt	Page

Access Control List	access-list ip standard
	access-list ip extended
	access-list mac
	access-list ipv6 standard
	access-list ipv6 extended
		Console(config-std-acl)
		Console(config-ext-acl)
		Console(config-mac-acl)
		Console(config-std-ipv6-acl)
		Console(config-ext-ipv6-acl)
			748
			748
			760
			755
			756

Class Map	class-map	Console(config-cmap)	886
DHCP	ip dhcp pool	Console(config-dhcp)	983
Line	line {console | vty}	Console(config-line)	600
Interface	interface {ethernet *port* | port-channel *id*| vlan *id*}	Console(config-if)	770
MSTP	spanning-tree mst-configuration	Console(config-mstp)	813
Policy Map	policy-map	Console(config-pmap)	889
Router	router {pim | rip | ospf}	Console(config-router)	1091 1025 1043
Time Range	time-range	Console(config-time-range)	625
VLAN	vlan database	Console(config-vlan)	837

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 29: 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 30: Command Group Index

Command Group	Description	Page
General	Basic commands for entering privileged access mode, restarting the system, or quitting the CLI	579
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, and the system clock	587
Simple Network Management Protocol	Activates authentication failure traps; configures community access strings, and trap receivers	629
Remote Monitoring	Supports statistics, history, alarm and event groups	649
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, and restricted access based on specified IP addresses	657
General Security Measures	Segregates traffic for clients attached to common data ports; and prevents unauthorized access by configuring valid static or dynamic addresses, MAC address authentication, filtering DHCP requests and replies, and discarding invalid ARP responses	707
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, or flow label), or non-IP frames (based on MAC address or Ethernet type)	747
Interface	Configures the connection parameters for all Ethernet ports, aggregated links, and VLANs	769
Link Aggregation	Statically groups multiple ports into a single logical trunk; configures Link Aggregation Control Protocol for port trunks	787
Mirror Port	Mirrors data to another port for analysis without affecting the data passing through or the performance of the monitored port	797
Rate Limit	Controls the maximum rate for traffic transmitted or received on a port	801
Address Table	Configures the address table for filtering specified addresses, displays current entries, clears the table, or sets the aging time	803
Spanning Tree	Configures Spanning Tree settings for the switch	807
VLANs	Configures VLAN settings, and defines port membership for VLAN groups; also enables or configures private VLANs, and protocol VLANs	831
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	871
Quality of Service	Configures Differentiated Services	885

Table 30: Command Group Index (Continued)

Command Group	Description	Page
Multicast Filtering	Configures IGMP multicast filtering, query, profile, and proxy parameters; specifies ports attached to a multicast router; also configures multicast VLAN registration	903
Link Layer Discovery Protocol	Configures LLDP settings to enable information discovery about neighbor devices	951
Domain Name Service	Configures DNS services.	969
Dynamic Host Configuration Protocol	Configures DHCP client, relay and server functions	979
Router Redundancy	Configures router redundancy to create primary and backup routers	995
IP Interface	Configures IP address for the switch interfaces; also configures ARP parameters and static entries	1005
IP Routing	Configures static and dynamic unicast routing	1019
Multicast Routing	Configures multicast routing protocols PIM-DM and PIM-SM	1085

The access mode shown in the following tables is indicated by these abbreviations:

ACL (Access Control List Configuration)
CM (Class Map Configuration)
DC (DHCP Server 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)
VC (VLAN Database Configuration)

23 General Commands

These commands are used to control the command access mode, configuration mode, and other basic functions.

Table 31: 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: 2001-2050)

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 595).

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 572.

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 (584)
enable password (658)

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 572.

DEFAULT SETTING

None

COMMAND MODE

Privileged Exec

EXAMPLE

```
Console#configure
Console(config)#
```

RELATED COMMANDS

end (585)

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 572.

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 (581)

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

These commands are used to control system logs, passwords, user names, management options, and display or configure a variety of other system information.

Table 32: System Management Commands

Command Group	Function
Device Designation	Configures information that uniquely identifies this switch
System Status	Displays system configuration, active managers, and version information
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

Device Designation

This section describes commands used to configure information that uniquely identifies the switch.

Table 33: 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)#
```

SYSTEM STATUS

This section describes commands used to display system information.

Table 34: System Status Commands

Command	Function	Mode
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 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

show running-config

This command displays the configuration information currently in use.

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
  - 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 VLANs
  - Layer 4 precedence settings
  - Routing protocol configuration settings
  - Spanning tree settings
  - Interface settings
  - Any configured settings for the console port and Telnet

EXAMPLE

```
Console#show running-config
Building running configuration. Please wait...
!<stackingDB>0000000000000000</stackingDB>
!<stackingMac>01_00-00-e8-93-82-a0_01</stackingMac>
!<stackingMac>00_00-00-00-00-00-00_00</stackingMac>
!<stackingMac>00_00-00-00-00-00-00_00</stackingMac>
!<stackingMac>00_00-00-00-00-00-00_00</stackingMac>
!<stackingMac>00_00-00-00-00-00-00_00</stackingMac>
!<stackingMac>00_00-00-00-00-00-00_00</stackingMac>
!<stackingMac>00_00-00-00-00-00-00_00</stackingMac>
!<stackingMac>00_00-00-00-00-00-00_00</stackingMac>
!
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
 switchport allowed vlan add 1 untagged
 switchport native vlan 1
:
!
interface vlan 1
 ip address dhcp
!
line console
!
line vty
!
end
```

RELATED COMMANDS

show startup-config (590)

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
  - 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 VLANs
  - Layer 4 precedence settings
  - Routing protocol configuration settings
  - Spanning tree settings
  - 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 (588)

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 101.

EXAMPLE

```
Console#show system
System Description : ECS4610-50T/ECS4610-26T
System OID String  : 1.3.6.1.4.1.259.10.1.1
System Information
 System Up Time         : 0 days, 0 hours, 21 minutes, and 47.6 seconds
 System Name            :
 System Location        :
 System Contact         :
 MAC Address (Unit 1)   : 00-00-E8-93-82-A0
 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
Console#
```

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    User Name                        Idle time (h:m:s) Remote IP addr
  ------- -------------------------------- ----------------- ---------------
* Console admin                                      0:00:00
  SSH 0                                              0:05:59 ::FFFF:192.168.0.61
  VTY 2   admin                                      0:00:03 192.168.0.61

 Web Online Users:
  Line  User Name                        Idle time (h:m:s) Remote IP Addr
  ----- -------------------------------- ----------------- ---------------
  HTTP  admin                                      0:01:24 192.168.0.61

Console#
```

show version

This command displays hardware and software version information for the system.

COMMAND MODE

Normal Exec, Privileged Exec

COMMAND USAGE

See "Displaying Switch Hardware/Software Versions" on page 103 for detailed information on the items displayed by this command.

EXAMPLE

```
Console#show version
Unit 1
 Serial Number           : 004000330
 Hardware Version        : R0A
 EPLD Version            : 1.00
 Number of Ports         : 24
 Main Power Status       : Up
 Redundant Power Status  : Not present
 Role                    : Master
 Loader Version          : 0.0.1.1
 Linux Kernel Version    : 2.6.19.2-0.1
 Boot ROM Version        : 0.0.0.1
 Operation Code Version  : 1.1.1.3

Console#
```

FRAME SIZE

This section describes commands used to configure the Ethernet frame size on the switch.

Table 35: Frame Size Commands

Command	Function	Mode
jumbo frame	Enables support for jumbo frames	GC

jumbo frame

This command enables support for jumbo frames for 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 Ethernet ports 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.

- 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 36: Flash/File Commands

Command	Function	Mode
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
whichboot	Displays the files booted	PE

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 (598)
whichboot (599)

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 running-config {**file** | **ftp** | **startup-config** | **tftp**}
copy startup-config {**file** | **ftp** | **running-config** | **tftp**}
copy tftp {**file** | **https-certificate | public-key** | **running-config** | **startup-config**}

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 684.)

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.

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 31 characters for files on the switch. (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 274. 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: 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
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 or image.

Syntax

delete *filename*

filename - Name of configuration file or code image.

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.

Example

This example shows how to delete the test2.cfg configuration file from flash memory.

```
Console#delete test2.cfg
Console#
```

Related Commands

dir (598)
delete public-key (689)

dir

This command displays a list of files in flash memory.

Syntax

dir {**boot-rom:** | **config:** | **opcode:**} [*filename*]}

boot-rom - Boot ROM (or diagnostic) image file.

config - Switch configuration file.

opcode - Run-time operation code image file.

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 37: File Directory Information

Column Heading	Description
File Name	The name of the file.
Type	File types: Boot-Rom, Operation Code, and Config file.
Startup	Shows if this file is used when the system is started.
Modify Time	The date and time the file was last modified.
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:
ECS4610-24F_V1.1.1.1.bix         OpCode     N    2010-03-08 08:57:13   13793596
ECS4610-24F_V1.1.1.3.bix         OpCode     Y    2010-04-02 05:43:25   13740356
Factory_Default_Config.cfg       Config     N    2010-02-11 04:41:03        455
startup1.cfg                     Config     Y    2010-02-11 04:41:08       3364
 ------------------------------------------------------------------------------
                         Free space for compressed user config files:   5812224
Console#
```

whichboot

This command displays which files were booted when the system powered up.

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:
ECS4610-24F_V1.1.1.3.bix         OpCode     Y    2010-04-02 05:43:25   13740356
startup1.cfg                     Config    Y     2010-02-11 04:41:08      3364
```

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 38: 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
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 (609)
show users (591)

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 (604)

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: 0 - 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 (659)
password (604)

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: 8 characters plain text, 32 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 (603)
password-thresh (605)

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 (606)

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; 0: 30 seconds)

DEFAULT SETTING

The default value is no silent-time.

COMMAND MODE

Line Configuration (console only)

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 (605)

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, or auto)

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. If you select the “auto” option, the switch will automatically detect the baud rate configured on the attached terminal, and adjust the speed accordingly.

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: 0 - 300 seconds; 0: disabled)

DEFAULT SETTING

CLI: Disabled (0 seconds)
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: 0-4)

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 (693)
show users (591)

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          : 115200
  Data Bits          : 8
  Parity             : None
  Stop Bits          : 1

 VTY Configuration:
  Password Threshold : 3 times
  Inactive Timeout   : 600 sec.
  Login Timeout      : 300 sec.
  Silent Time        : Disabled
Console#
```

EVENT LOGGING

This section describes commands used to configure event logging on the switch.

Table 39: 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 40: 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
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 (611)
logging trap (613)
clear log (613)

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 611. 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 (614)

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

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 619).

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 41: 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 42: 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.
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 (619)

SMTP ALERTS

These commands configure SMTP event handling, and forwarding of alert messages to the specified SMTP servers and email recipients.

Table 43: 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 - IP 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 611). 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
-----------------------------------------------
  1. 192.168.1.19
```

```
SMTP Minimum Severity Level: 7

SMTP destination email addresses
-----------------------------------------------
   1. ted@this-company.com

SMTP Source E-mail 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 44: 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
Manual Configuration Commands		
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

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:  Dec 23 02:52:44 2002
Poll Interval: 60
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#
```

RELATED COMMANDS

sntp server (622)
sntp poll (621)
show sntp (622)

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 (620)

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 (620)
sntp poll (621)
show sntp (622)

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
                 137.92.140.81
Console#
```

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 (622)

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, 2002.

```
Console#calendar set 15:12:34 1 February 2002
Console#
```

show calendar

This command displays the system clock.

DEFAULT SETTING

None

COMMAND MODE

Normal Exec, Privileged Exec

EXAMPLE

```
Console#show calendar
 15:12:34 February 1 2002
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 45: 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

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: 1-30 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 (747)

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.

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

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)#
```

25 SNMP COMMANDS

Controls 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 46: 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
SNMPv3 Engine 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
show snmp view	Shows the SNMP views	PE

Table 46: SNMP Commands (Continued)

Command	Function	Mode
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

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 (631)

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 (631)

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

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-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**]

authentication - Keyword to issue authentication failure notifications.

link-up-down - Keyword to issue link-up or link-down notifications.

DEFAULT SETTING

Issue authentication and link-up-down traps.

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 (634)

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 - Internet address of the host (the 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 354 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 630).
  2. Create a view with the required notification messages (page 640).
  3. Create a group that includes the required notify view (page 637).
  4. Allow the switch to send SNMP traps; i.e., notifications (page 633).
  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 630).
  2. Create a local SNMPv3 user to use in the message exchange process (page 639).
  3. Create a view with the required notification messages (page 640).
  4. Create a group that includes the required notify view (page 637).
  5. Allow the switch to send SNMP traps; i.e., notifications (page 633).
  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 (633)

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 639).

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 (634)

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 354 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[8] (read only), private[9] (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 22, "Supported Notification Messages," on page 363. 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.

EXAMPLE

```
Console(config)#snmp-server group r&d v3 auth write daily
Console(config)#
```

[8] No view is defined.
[9] Maps to the defaultview.

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 47: 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.
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    : defaultview
Storage Type   : nonvolatile
Row Status     : active

Group Name     : public
Security Model : v1
Read View      : defaultview
Write View     : No writeview specified
Notify View    : No notifyview specified
Storage Type   : volatile
Row Status     : active

Group Name     : public
Security Model : v2c
Read View      : defaultview
Write View     : No writeview specified
Notify View    : No notifyview specified
Storage Type   : volatile
Row Status     : active

Group Name     : private
Security Model : v1
Read View      : defaultview
Write View     : defaultview
Notify View    : No notifyview specified
Storage Type   : volatile
Row Status     : active

Group Name     : private
Security Model : v2c
Read View      : defaultview
Write View     : defaultview
Notify View    : No notifyview specified
Storage Type   : volatile
Row Status     : active

Console#
```

Table 48: show snmp group - display description

Field	Description
Group Name	Name of an SNMP group.
Security Model	The SNMP version.
Read View	The associated read view.
Write View	The associated write view.

Table 48: show snmp group - display description (Continued)

Field	Description
Notify View	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 49: 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 : nonvolatile
Row Status   : active

View Name    : defaultview
Subtree OID  : 1
View Type    : included
Storage Type : volatile
Row Status   : active

Console#
```

Table 50: 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.

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 those are Traps or Informs that exceed 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(config)
```

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#
```

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.

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.

Table 51: 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 stats	Enables statistics collection	IC
show rmon alarm	Shows the settings for all configured alarms	PE
show rmon event	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** *seconds* {**absolute** | **delta**} **rising-threshold** *threshold* **event** *event-index* **falling-threshold** *threshold* **event** *event-index* [**owner** *name*]

no rmon event *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.

seconds – 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: 1-65535)

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

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.
- 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 1.3.6.1.2.1.16.1.1.1.6.1 interval 15 delta
  rising-threshold 100 event 1 falling-threshold 30 event 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 610).

trap – Sends a trap message to all configured trap managers (see "snmp-server host" on page 634).

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 (page 630) 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

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

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 *index* [**buckets** *number*] |
    [**interval** *seconds*] | [**owner** *name*]

no rmon collection history *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

Enabled
Buckets: 50
Interval: 1800 seconds

COMMAND MODE

Interface Configuration (Ethernet)

COMMAND USAGE

- By default, each index number equates to a port on the ECN430-swich, 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, collisioins, drop events, and network utilization.

EXAMPLE

```
Console(config)#interface  ethenet 1/1
Console(config-if)#rmon collection history 21 buckets 24 interval 60 owner
  mike
Console(config-if)#
```

rmon collection stats

This command enables the collection of statistics on a physical interface. Use the no form to disable statistics collection.

SYNTAX

rmon collection stats *index* [**owner** *name*]

no rmon collection stats *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 swich, 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 packets, bytes, dropped packets, and multicast packets
  output packets, bytes, multicast packets, and broadcast packets.

EXAMPLE

```
Console(config)#interface ethernet 1/1
Console(config-if)#rmon collection stats 1 owner mike
Console(config-if)#
```

show rmon alarm

This command shows the settings for all configured alarms.

COMMAND MODE

Privileged Exec

EXAMPLE

```
Console#show rmon alarm
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 event

This command shows the settings for all configured events.

COMMAND MODE

Privileged Exec

EXAMPLE

```
Console#show rmon event
Event 1 is valid, owned by steve
 Description is for r&d
 Event firing causes log and trap to community public, 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 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[10] to the data ports.

Table 52: 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

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 600), user authentication via a remote authentication server (page 657), and host access authentication for specific ports (page 693).

Table 53: 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

[10] For other methods of controlling client access, see "General Security Measures" on page 707.

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: 8 characters plain text, 32 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 (581)
authentication enable (660)

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: 8 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: 8 characters plain text, 32 encrypted, case sensitive)

DEFAULT SETTING

The default access level is Normal Exec.
The factory defaults for the user names and passwords are:

Table 54: 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 a 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 55: 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 (658)

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 (659)

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 56: 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* [**auth-port** *auth-port*] [**acct-port** *acct_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.

auth-port - RADIUS server UDP port used for authentication messages. (Range: 1-65535)

acct_port - RADIUS server UDP port used for accounting 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
 Auth-port           : 1812
 Acct-port           : 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 57: TACACS+ Client Commands

Command	Function	Mode
tacacs-server	Specifies the TACACS+ server and optional parameters	GC
tacacs-server host	Specifies the TACACS+ server	GC
tacacs-server key	Sets the TACACS+ encryption key	GC
tacacs-server port	Specifies the TACACS+ server network port	GC
show tacacs-server	Shows the current TACACS+ settings	GC

tacacs-server

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*]

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)

DEFAULT SETTING

10.11.12.13

COMMAND MODE

Global Configuration

EXAMPLE

```
Console(config)#tacacs-server host 192.168.1.25
Console(config)#
```

tacacs-server host

This command specifies the TACACS+ server. Use the **no** form to restore the default.

SYNTAX

tacacs-server host *host-ip-address*

no tacacs-server host

host-ip-address - IP address of a TACACS+ server.

DEFAULT SETTING

10.11.12.13

COMMAND MODE

Global Configuration

EXAMPLE

```
Console(config)#tacacs-server host 192.168.1.25
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)#
```

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

Server 1:
 Server IP Address   : 10.11.12.13
 Server Port Number  : 49

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 58: AAA Commands

Command	Function	Mode
aaa accounting commands	Enables accounting of Exec mode commands	GC
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

Table 58: AAA Commands (Continued)

Command	Function	Mode
authorization exec	Applies an authorization method to local console, Telnet or SSH connections	Line
show accounting	Displays all accounting information	PE

aaa accounting commands

This command enables the accounting of Exec mode commands. Use the **no** form to disable the accounting service.

SYNTAX

aaa accounting commands *level* {**default** | *method-name*}
start-stop group {**tacacs+** |*server-group*}

no aaa accounting commands *level* {**default** | *method-name*}

level - The privilege level for executing commands. (Range: 0-15)

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.

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: 1-255 characters)

DEFAULT SETTING

Accounting is not enabled
No servers are specified

COMMAND MODE

Global Configuration

COMMAND USAGE

- The accounting of Exec mode commands is only supported by TACACS+ servers.

- Note that the **default** and *method-name* fields are only used to describe the accounting method(s) configured on the specified TACACS+ server, and do not actually send any information to the server about the methods to use.

EXAMPLE

```
Console(config)#aaa accounting commands 15 default start-stop group tacacs+
Console(config)#
```

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: 1-255 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: 1-255 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: 1-255 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: 1-255 characters)

group - Specifies the server group to use.

tacacs+ - Specifies all TACACS+ hosts configured with the tacacs-server command.

server-group - Specifies the name of a server group configured with the aaa group server command. (Range: 1-255 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: 1-7 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 - Stack unit. (Range: 1)

port - Port number. (Range: 1-24)

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 59: 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-server	Enables HTTPS (HTTP/SSL) for encrypted communications	GC
ip http secure-port	Specifies the UDP port number for HTTPS	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 (679)
show system (590)

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 (678)
show system (590)

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 5.x or above, Netscape Navigator 6.2 or above, and Mozilla Firefox 2.0.0.0 or above.

  The following web browsers and operating systems currently support HTTPS:

Table 60: HTTPS System Support

Web Browser	Operating System
Internet Explorer 5.0 or later	Windows 98,Windows NT (with service pack 6a), Windows 2000, Windows XP, Windows 7
Netscape Navigator 6.2 or later	Windows 98,Windows NT (with service pack 6a), Windows 2000, Windows XP, Solaris 2.6
Mozilla Firefox 2.0.0.0 or later	Windows 2000, Windows XP, Linux

- To specify a secure-site certificate, see “Replacing the Default Secure-site Certificate” on page 274. Also refer to the copy tftp https-certificate command.

EXAMPLE

```
Console(config)#ip http secure-server
Console(config)#
```

RELATED COMMANDS

ip http secure-port (681)
copy tftp https-certificate (595)
show system (590)

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 (679)
show system (590)

TELNET SERVER

This section describes commands used to configure Telnet management access to the switch.

Table 61: 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: 0-4)

DEFAULT SETTING

4 sessions

COMMAND MODE

Global Configuration

COMMAND USAGE

A maximum of four sessions can be concurrently opened for Telnet and Secure Shell (i.e., both Telnet and SSH share a maximum number or four 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 62: 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
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
   134108168560989392104094492015542534763164192187295892114317388
   005553616163105177594083868631109291232226828519254374603100937
   187721199696317813662774141689851320491172048303392543241016379
   975923714490119380060902539484084827178194372288402533115952134
   861022902978982721353267131629432532818915045306393916643
   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 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.

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 (691)

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 (689)
show ssh (693)

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 (602)
show ip ssh (691)

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 (690)
ip ssh save host-key (691)

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 (689)
ip ssh save host-key (691)
no ip ssh server (687)

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 (689)

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 63: 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 64: 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-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

Table 64: 802.1X Port Authentication Commands (Continued)

Command	Function	Mode
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

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)#
```

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-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 (699)

dot1x timeout quiet-period

This command sets the time that a switch port waits after the maximum request count (see page 696) 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 - Stack unit. (Range: 1)

port - Port number. (Range: 1-24)

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#
```

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 - Stack unit. (Range: 1)

port - Port number. (EC-S4626F: 1-26, EC-S4650F: 1-50)

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 695).

- *Authenticator Parameters* – Shows whether or not EAPOL pass-through is enabled (page 694).

- *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 697).
  - Control Mode– Dot1x port control mode (page 698).
  - 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 698).
  - Reauth Period – Time after which a connected client must be re-authenticated (page 699).
  - Quiet Period – Time a port waits after Max Request Count is exceeded before attempting to acquire a new client (page 699).
  - TX Period – Time a port waits during authentication session before re-transmitting EAP packet (page 700).
  - Supplicant Timeout – Supplicant timeout.
  - Server Timeout – Server timeout.
  - 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 696).

- 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 698).
- Intrusion Action– Sets the port response to intrusion when authentication fails (page 695).
- 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– 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
-------- ------------- -------------- ------------------ ----------
1/1        Disabled     Single-Host      ForceAuthorized     N/A
1/2        Disabled     Single-Host      ForceAuthorized     N/A
.
.
.
1/23       Disabled     Single-Host      ForceAuthorized     Yes
1/24       Enabled      Single-Host      Auto                Yes

802.1X Port Details

802.1X Authenticator is enabled on port 1/1

.
.
.
802.1X Authenticator is enabled on port 24
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               : Initialize
  Reauth Count        : 0
  Current Identifier  : 0

 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 65: 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
--------------------------------------- ----------------------------------
192.168.1.19                         192.168.1.19

 SNMP Client:
Start IP Address                        End IP Address
--------------------------------------- -------------------------------------
192.168.1.19          192.168.1.19

 Telnet Client:
Start IP Address                        End IP Address
--------------------------------------- -------------------------------------
192.168.1.19          192.168.1.19

Console#
```

28 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 66: 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
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)
DHCP Snooping*	Filters untrusted DHCP messages on unsecure ports by building and maintaining a DHCP snooping binding table
IP Source Guard*	Filters IP traffic on insecure ports for which the source address cannot be identified via DHCP snooping nor static source bindings
ARP Inspection	Validates the MAC-to-IP address bindings in ARP packets

* The priority of execution for these filtering commands is Port Security, Port Authentication, Network Access, 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 67: 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
show mac-address-table	Displays entries in the bridge-forwarding database	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 (780)

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

- When port security is enabled with this command, 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.

- First use the **port security max-mac-count** command to set the number of addresses, and then use the **port security** command to enable security on the port. (The specified maximum address count is effective when port security is enabled or disabled.)

- Use the **no port security max-mac-count** command to disable port security and reset the maximum number of addresses to the default.

- You can also manually add secure addresses with the mac-address-table static command.

- A secure port has the following restrictions:

  - Cannot be connected to a network interconnection device.
  - Cannot be a trunk port.

- If a port is disabled due to a security violation, it must be manually re-enabled using the no shutdown command.

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 (780)
shutdown (775)
mac-address-table static (804)

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 68: 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
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
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 Authenticataion 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 697).

- 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 69: 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

- 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 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: 1-4093)

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)#
```

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 - Stack unit. (Range: 1)

port - Port number. (Range: 1-24)

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
--------------------------------------------------
--------------------------------------------------
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
Guest VLAN                              : Disabled
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 - Stack unit. (Range: 1)

port - Port number. (Range: 1-24)

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

```
Consoleshownetwork-access mac-filter
Filter ID MAC Address       MAC Mask
--------- ----------------- -----------------
        1 00-00-01-02-03-08 FF-FF-FF-FF-FF-FF
Console#
```

DHCP SNOOPING

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. This section describes commands used to configure DHCP snooping.

Table 70: DHCP Snooping Commands

Command	Function	Mode
ip dhcp snooping	Enables DHCP snooping globally	GC
ip dhcp snooping database flash	Writes all dynamically learned snooping entries to flash memory	GC
ip dhcp snooping information option	Enables or disables DHCP Option 82 information relay	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 trust	Configures the specified interface as trusted	IC
clear ip dhcp snooping database flash	Removes all dynamically learned snooping entries from flash memory.	PE
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 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 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 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 (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 (729)
ip dhcp snooping trust (730)

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(config)#ip dhcp snooping database flash
Console(config)#
```

ip dhcp snooping information option

This command enables the DHCP Option 82 information relay for the switch. Use the **no** form to disable this function.

SYNTAX

[**no**] **ip dhcp snooping information option**

DEFAULT SETTING

Disabled

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 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 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 on the switch for the DHCP Option 82 information to be inserted into packets.

- Use the **ip dhcp snooping information option** command to specify how to handle DHCP client request packets which already contain Option 82 information.

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 (725)
ip dhcp snooping vlan (729)
ip dhcp snooping trust (730)

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: 1-4093)

DEFAULT SETTING

Disabled

COMMAND MODE

Global Configuration

COMMAND USAGE

- When DHCP snooping 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, configuration changes for specific VLANs have the following effects:

  - If DHCP snooping is disabled on a 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 (725)
ip dhcp snooping trust (730)

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 ia 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 (725)
ip dhcp snooping vlan (729)

clear ip dhcp snooping database flash

This command removes all dynamically learned snooping entries from flash memory.

COMMAND MODE

Privileged Exec

EXAMPLE

```
Console(config)#ip dhcp snooping database flash
Console(config)#
```

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: disable
DHCP Snooping Information Option Status: disable
DHCP Snooping Information Policy: replace
DHCP Snooping is configured on the following VLANs:
1
Verify Source Mac-Address: enable
Interface            Trusted
----------           ----------
Eth 1/1              No
Eth 1/2              No
Eth 1/3              No
Eth 1/4              No
Eth 1/5              Yes
.
.
.
```

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
MacAddress        IpAddress       Lease(sec) Type                 VLAN Interface
----------------- --------------- ---------- -------------------- ---- ------
11-22-33-44-55-66 192.168.0.99             0 Dynamic-DHCPSNP       1 Eth 1/5
Console#
```

IP SOURCE GUARD

IP 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 724). 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 commands used to configure IP Source Guard.

Table 71: IP 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
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 binding table. Use the **no** form to remove a static entry.

SYNTAX

ip source-guard binding *mac-address* **vlan** *vlan-id ip-address interface*

no ip source-guard binding *mac-address* **vlan** *vlan-id*

mac-address - A valid unicast MAC address.

vlan-id - ID of a configured VLAN (Range: 1-4093)

ip-address - A valid unicast IP address, including classful types A, B or C.

interface - Specifies a port interface.

ethernet *unit/port*

unit - This is unit 1.

port - Port number. (Range: 1-24)

DEFAULT SETTING

No configured entries

COMMAND MODE

Global Configuration

COMMAND USAGE

- 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 737).
- 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.

```
Console(config)#ip source-guard binding 11-22-33-44-55-66 vlan 1 192.168.0.99
  interface ethernet 1/5
Console(config-if)#
```

RELATED COMMANDS

ip source-guard (735)
ip dhcp snooping (725)
ip dhcp snooping vlan (729)

ip source-guard

This command configures the switch to filter inbound traffic based 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 (page 733) 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 DHCP snooping is disabled (see page 725), 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 (733)
ip dhcp snooping (725)
ip dhcp snooping vlan (729)

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 max-binding *number*

no ip source-guard max-binding

number - The maximum number of IP 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 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.

```
Console(config)#interface ethernet 1/5
Console(config-if)#ip source-guard max-binding 1
Console(config-if)#
```

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
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 ip source-guard binding

This command shows the source guard binding table.

SYNTAX

show ip source-guard binding [**dhcp-snooping** | **static**]

dhcp-snooping - Shows dynamic entries configured with DHCP Snooping commands (see page 724)

static - Shows static entries configured with the ip source-guard binding command (see page 733).

COMMAND MODE

Privileged Exec

EXAMPLE

```
Console#show ip source-guard binding
MacAddress        IpAddress       Lease(sec) Type                 VLAN Interface
----------------- --------------- ---------- -------------------- ---- --------
11-22-33-44-55-66 192.168.0.99             0 Static                  1 Eth 1/5
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 72: 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
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

Table 72: ARP Inspection Commands (Continued)

Command	Function	Mode
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: 1-4093)

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 298.
- 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**] [**src-mac**] | **ip** [**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.

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: 1-4093)

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)

COMMAND USAGE

- This command only applies to 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 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)

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 - Stack unit. (Range: 1)

port - Port number. (Range: 1-24)

Command Mode

Privileged Exec

Example

```
Console#show ip arp inspection interface ethernet 1/1

Port Number        Trust Status             Limit Rate (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 log
Total log entries number is 1

Num VLAN Port Src IP Address  Dst IP Address  Src MAC Address  Dst MAC Address
--- ---- ---- --------------  --------------  ---------------  -----------

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: 1-4093)

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#
```

29 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 73: 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 or DSCP traffic class
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 74: 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: 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 ip standard david
Console(config-std-acl)#
```

RELATED COMMANDS

permit, deny (749)
ip access-group (752)
show ip access-list (753)

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 – 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 (748)
Time Range (625)

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[11] source port number. (Range: 0-65535)

dport – Protocol[11] destination port number. (Range: 0-65535)

[11] 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 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.
- 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 (748)
Time Range (625)

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** [**time-range** *time-range-name*]

no ip access-group *acl-name* **in**

acl-name – Name of the ACL. (Maximum length: 16 characters)

in – Indicates that this list applies to ingress packets.

time-range-name - Name of the time range.
(Range: 1-30 characters)

DEFAULT SETTING

None

COMMAND MODE

Interface Configuration (Ethernet)

COMMAND USAGE

- Only one ACL can be bound to a port.
- 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 (753)
Time Range (625)

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 (752)

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 (749)
ip access-group (752)

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 75: IPv4 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, and flow label	IPv6-EXT-ACL
show ipv6 access-list	Displays the rules for configured IPv6 ACLs	PE
ipv6 access-group	Adds a port to an IPv6 ACL	IC
show ipv6 access-group	Shows port assignments for 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: 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 ipv6 standard david
Console(config-std-ipv6-acl)#
```

RELATED COMMANDS

permit, deny (Standard IPv6 ACL) (755)
permit, deny (Extended IPv6 ACL) (756)
ipv6 access-group (759)
show ipv6 access-list (758)

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 (754)
Time Range (625)

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

[**no**] {**permit** | **deny**}
{**any** | *destination-ipv6-address*[*/prefix-length*]}
[**dscp** *dscp*] [**flow-label** *flow-label*] [**next-header** *next-header*]
[**time-range** *time-range-name*]

any – Any IP address (an abbreviation for the IPv6 prefix ::/0).

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. (The switch only checks the first 64 bits of the destination address.)

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 for source prefix, 0-8 for destination prefix)

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)#
```

RELATED COMMANDS

access-list ipv6 (754)
Time Range (625)

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#
```

RELATED COMMANDS

permit, deny (Standard IPv6 ACL) (755)
permit, deny (Extended IPv6 ACL) (756)
ipv6 access-group (759)

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** [**time-range** *time-range-name*]

no ipv6 access-group *acl-name* **in**

acl-name – Name of the ACL. (Maximum length: 16 characters)

in – Indicates that this list applies to ingress packets.

time-range-name - Name of the time range.
(Range: 1-30 characters)

DEFAULT SETTING

None

COMMAND MODE

Interface Configuration (Ethernet)

COMMAND USAGE

- A port can only be bound to one ACL.
- 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.
- IPv6 ACLs can only be applied to ingress packets.

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 (758)
Time Range (625)

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 access-list david in
Console#
```

RELATED COMMANDS

ipv6 access-group (759)

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 76: 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 (761)
mac access-group (763)
show mac access-list (764)

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[12] – Bitmask for MAC address (in hexadecimal format).

vid – VLAN ID. (Range: 1-4093)

vid-bitmask[12] – VLAN bitmask. (Range: 1-4095)

protocol – A specific Ethernet protocol number.
(Range: 600-ffff hex.)

protocol-bitmask[12] – Protocol bitmask.
(Range: 600-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.

[12] For all bitmasks, “1” means care and “0” means ignore.

- The **ethertype** option can only be used to filter Ethernet II formatted packets.

- 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 (760)
Time Range (625)

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** [**time-range** *time-range-name*]

acl-name – Name of the ACL. (Maximum length: 16 characters)

in – Indicates that this list applies to ingress packets.

time-range-name - Name of the time range.
(Range: 1-30 characters)

DEFAULT SETTING

None

COMMAND MODE

Interface Configuration (Ethernet)

COMMAND USAGE

- Only one ACL can be bound to a port.

- 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 (764)
Time Range (625)

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 (763)

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 (761)
mac access-group (763)

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 (page 742).

Table 77: 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 arp access-list	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.

EXAMPLE

```
Console(config)#access-list arp factory
Console(config-arp-acl)#
```

RELATED COMMANDS

permit, deny (766)
show arp access-list (767)

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-ip* | *source-ip ip-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[13] – IPv4 number representing the address bits to match.

source-mac – Source MAC address.

destination-mac – Destination MAC address range with bitmask.

mac-address-bitmask[13] – 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.

[13] For all bitmasks, binary “1” means care 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 (765)

show arp access-list

This command displays the rules for configured ARP ACLs.

SYNTAX

show arp access-list [*acl-name*]

acl-name – Name of the ACL. (Maximum length: 16 characters)

COMMAND MODE

Privileged Exec

EXAMPLE

```
Console#show arp access-list
ARP access-list factory:
  permit response ip any 192.168.0.0 255.255.0.0 mac any any
Console#
```

RELATED COMMANDS

permit, deny (766)

ACL INFORMATION

This section describes commands used to display ACL information.

Table 78: ACL Information Commands

Command	Function	Mode
show access-group	Shows the ACLs assigned to each port	PE
show access-list	Show all ACLs and associated rules	PE

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.

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
  permit any any
Console#
```

30 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 79: 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
flowcontrol	Enables flow control on a given interface	IC
media-type	Force port type selected for combination ports	IC
negotiation	Enables autonegotiation of a given interface	IC
shutdown	Disables an interface	IC
speed-duplex	Configures the speed and duplex operation of a given interface when autonegotiation is disabled	IC
switchport packet-rate	Configures storm control thresholds	IC
clear counters	Clears statistics on an interface	PE
show interfaces counters	Displays statistics for the specified interfaces	NE, 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
Cable Diagnostics		
test cable-diagnostics dsp	Performs cable diagnostics on the specified port	PE
test loop internal	Performs internal loop back test on the specified port	PE
show cable-diagnostics	Shows the results of a cable diagnostics test	PE
show loop internal	Shows the results of a loop back test	PE

interface

This command configures an interface type and enters interface configuration mode. Use the **no** form with a trunk to remove an inactive interface. Use the **no** form with a Layer 3 VLAN (normal type) to change it back to a Layer 2 interface.

SYNTAX

[**no**] **interface** *interface*

interface

ethernet *unit/port*

unit - Stack unit. (Range: 1)

port - Port number. (Range: 1-24)

port-channel *channel-id* (Range: 1-32)

vlan *vlan-id* (Range: 1-4093)

DEFAULT SETTING

None

COMMAND MODE

Global Configuration

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** {**1000full** | **100full** | **100half** | **10full** | **10half** | **flowcontrol** | **symmetric**}

1000full - Supports 1 Gbps full-duplex operation

100full - Supports 100 Mbps full-duplex operation

100half - Supports 100 Mbps half-duplex operation

10full - Supports 10 Mbps full-duplex operation

10half - Supports 10 Mbps half-duplex operation

flowcontrol - Supports flow control

symmetric (Gigabit only) - When specified, the port transmits and receives pause frames.

DEFAULT SETTING

1000BASE-T: 10half, 10full, 100half, 100full, 1000full
1000BASE-SX/LX/LH (SFP): 1000full

COMMAND MODE

Interface Configuration (Ethernet, Port Channel)

COMMAND USAGE

- The 1000BASE-T standard does not support forced mode. Auto-negotiation should always be used to establish a connection over any 1000BASE-T port or trunk.

- 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 speed-duplex and flowcontrol commands.

Example

The following example configures Ethernet port 5 capabilities to include 100half and 100full.

```
Console(config)#interface ethernet 1/5
Console(config-if)#capabilities 100half
Console(config-if)#capabilities 100full
Console(config-if)#capabilities flowcontrol
Console(config-if)#
```

Related Commands

negotiation (774)
speed-duplex (776)
flowcontrol (773)

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)#
```

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

- 1000BASE-T does not support forced mode. Auto-negotiation should always be used to establish a connection over any 1000BASE-T port or trunk.

- 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

- Avoid using flow control on a port connected to a hub unless it is actually required to solve a problem. Otherwise back pressure jamming signals may degrade overall performance for the segment attached to the hub.

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 (774)
capabilities (flowcontrol, symmetric) (771)

media-type

This command forces the port type selected for combination ports 25-26. Use the **no** form to restore the default mode.

SYNTAX

media-type *mode*

no media-type

mode

copper-forced - Always uses the built-in RJ-45 port.

sfp-forced - Always uses the SFP port (even if module not installed).

sfp-preferred-auto - Uses SFP port if both combination types are functioning and the SFP port has a valid link.

DEFAULT SETTING

sfp-preferred-auto

COMMAND MODE

Interface Configuration (Ethernet - Ports 1-2)

EXAMPLE

This forces the switch to use the built-in RJ-45 port for the combination port 25.

```
Console(config)#interface ethernet 1/25
Console(config-if)#media-type copper-forced
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

- 1000BASE-T does not support forced mode. Auto-negotiation should always be used to establish a connection over any 1000BASE-T port or trunk.

- 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 speed-duplex and flowcontrol commands.

- If auto-negotiation is disabled, auto-MDI/MDI-X pin signal configuration will also be disabled for the RJ-45 ports.

EXAMPLE

The following example configures port 11 to use auto-negotiation.

```
Console(config)#interface ethernet 1/11
Console(config-if)#negotiation
Console(config-if)#
```

RELATED COMMANDS

capabilities (771)
speed-duplex (776)

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)#
```

speed-duplex

This command configures the speed and duplex mode of a given interface when auto-negotiation is disabled. Use the **no** form to restore the default.

SYNTAX

speed-duplex {**1000full** | **100full** | **100half** | **10full** | **10half**}

no speed-duplex

1000full - Forces 1 Gbps full-duplex operation

100full - Forces 100 Mbps full-duplex operation

100half - Forces 100 Mbps half-duplex operation

10full - Forces 10 Mbps full-duplex operation

10half - Forces 10 Mbps half-duplex operation

DEFAULT SETTING

- Auto-negotiation is enabled by default on the Gigabit ports.
- When auto-negotiation is disabled on the Gigabit ports, the default speed-duplex setting is 100full.
- The speed-duplex setting on the 10 Gigabit ports is fixed at 10Gfull regardless of the setting for auto-negotiation.

COMMAND MODE

Interface Configuration (Ethernet, Port Channel)

COMMAND USAGE

- The 1000BASE-T standard does not support forced mode. Auto-negotiation should always be used to establish a connection over any 1000BASE-T port or trunk. If not used, the success of the link process cannot be guaranteed when connecting to other types of switches.
- To force operation to the speed and duplex mode specified in a **speed-duplex** 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 set the speed/duplex mode under auto-negotiation, the required mode must be specified in the capabilities list for an interface.

EXAMPLE

The following example configures port 5 to 100 Mbps, half-duplex operation.

```
Console(config)#interface ethernet 1/5
Console(config-if)#speed-duplex 100half
Console(config-if)#no negotiation
Console(config-if)#
```

RELATED COMMANDS

negotiation (774)
capabilities (771)

switchport packet-rate

This command configures broadcast storm control. Use the **no** form to restore the default setting.

SYNTAX

switchport broadcast packet-rate *rate*

no switchport broadcast

rate - Threshold level as a rate; i.e., packets per second. (Range: 500-262143)

DEFAULT SETTING

Enabled, packet-rate limit: 500 pps

COMMAND MODE

Interface Configuration (Ethernet)

COMMAND USAGE

- When traffic exceeds the threshold specified for broadcast traffic, packets exceeding the threshold are dropped until the rate falls back down beneath the threshold.

- Using both rate limiting and storm control on the same interface may lead to unexpected results. For example, suppose broadcast storm control is set to 500 pps by the command "switchport broadcast packet-rate 500" and the rate limit is set to 200 Mbps by the command "rate-limit input 20" on a port. Since 200 Mbps is 1/5 of line speed (1000 Mbps), the received rate will actually be 100 pps, or 1/5 of the 500 pps limit set by the storm control command. 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)#
```

clear counters

This command clears statistics on an interface.

SYNTAX

clear counters *interface*

interface

ethernet *unit/port*

unit - Stack unit. (Range: 1)

port - Port number. (Range: 1-24)

port-channel *channel-id* (Range: 1-32)

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 interfaces counters

This command displays interface statistics.

SYNTAX

show interfaces counters [*interface*]

interface

ethernet *unit/port*

unit - Stack unit. (Range: 1)

port - Port number. (Range: 1-24)

port-channel *channel-id* (Range: 1-32)

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 131.

EXAMPLE

```
Console#show interfaces counters ethernet 1/17
Ethernet 1/ 1
 ===== IF table Stats =====
                  138550 Octets Input
                  820500 Octets Output
                     734 Unicast Input
                     932 Unicast Output
                      12 Discard Input
                       0 Discard Output
                       0 Error Input
                       0 Error Output
                       0 Unknown Protos Input
                       0 QLen Output
 ===== Extended Iftable Stats =====
                      38 Multi-cast Input
                    1342 Multi-cast Output
                     210 Broadcast Input
                       2 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
 ===== RMON Stats =====
                       0 Drop Events
                  959114 Octets
                    3259 Packets
                     212 Broadcast PKTS
                    1381 Multi-cast PKTS
                       0 Undersize PKTS
                       0 Oversize PKTS
                       0 Fragments
                       0 Jabbers
                       0 CRC Align Errors
                       0 Collisions
                    2142 Packet Size <= 64 Octets
                     303 Packet Size 65 to 127 Octets
                     140 Packet Size 128 to 255 Octets
                      75 Packet Size 256 to 511 Octets
                     140 Packet Size 512 to 1023 Octets
                     459 Packet Size 1024 to 1518 Octets
 ===== Port Utilization =====
                      35 Octets Input per seconds
                       0 Packets Input per seconds
                    0.00 % Input Utilization
                      56 Octets Output per seconds
                       0 Packets Output per second
                    0.00 % Output Utilization
Console#
```

show interfaces status

This command displays the status for an interface.

SYNTAX

show interfaces status [*interface*]

interface

ethernet *unit*/*port*

unit - Stack unit. (Range: 1)

port - Port number. (Range: 1-24)

port-channel *channel-id* (Range: 1-32)

vlan *vlan-id* (Range: 1-4093)

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 128.

EXAMPLE

```
Console#show interfaces status ethernet 1/1
 Basic Information:
  Port Type               : 1000T
  Mac Address             : 00-00-E8-93-82-A1
 Configuration:
  Name                    :
  Port Admin              : Up
  Speed-duplex            : Auto
  Capabilities            : 10half, 10full, 100half, 100full, 1000full
  Broadcast Storm         : Enabled
  Broadcast Storm Limit   : 500 packets/second
  Flow Control            : Disabled
  VLAN Trunking           : Disabled
  LACP                    : Disabled
  Mac-Learning            : Yes
  Port Security           : Disabled
  Max MAC Count           : 0
  Port Security Action    : None
  Media Type              : SFP preferred auto
  MTU                        : 1518
 Current Status:
  Link Status                : Up
  Port Operation Status      : Up
  Operation Speed-duplex     : 100full
  Flow Control Type          : None
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 - Stack unit. (Range: 1)

port - Port number. (Range: 1-24)

port-channel *channel-id* (Range: 1-32)

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 21.

```
Console#show interfaces switchport ethernet 1/21
Information of Eth 1/1
 Broadcast Threshold             : Enabled, 500 packets/second
 LACP Status                     : Disabled
 Ingress Rate Limit              : Disabled, 1000M bits per second
 Egress Rate Limit               : Disabled, 1000M bits 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:             Disable
 802.1Q-tunnel Mode:               NORMAL
 802.1Q-tunnel TPID:               8100(Hex)
```

```
Console#
```

Table 80: 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 777).
LACP Status	Shows if Link Aggregation Control Protocol has been enabled or disabled (page 789).
Ingress/Egress Rate Limit	Shows if rate limiting is enabled, and the current rate limit (page 801).
VLAN Membership Mode	Indicates membership mode as Trunk or Hybrid (page 842).
Ingress Rule	Shows if ingress filtering is enabled or disabled (page 841).
Acceptable Frame Type	Shows if acceptable VLAN frames include all types or tagged frames only (page 839).
Native VLAN	Indicates the default Port VLAN ID (page 843).
Priority for Untagged Traffic	Indicates the default priority for untagged frames (page 875).
GVRP Status	Shows if GARP VLAN Registration Protocol is enabled or disabled (page 834).
Allowed VLAN	Shows the VLANs this interface has joined, where "(u)" indicates untagged and "(t)" indicates tagged (page 840).
Forbidden VLAN	Shows the VLANs this interface can not dynamically join via GVRP (page 834).
Private-VLAN Mode	Shows the private VLAN mode as host, promiscuous, or none (854).
Private VLAN host-association	Shows the secondary (or community) VLAN with which this port is associated (855).
Private VLAN mapping	Shows the primary VLAN mapping for a promiscuous port (856).
802.1Q-tunnel Status	Shows if 802.1Q tunnel is enabled on this interface (847).
802.1Q-tunnel Mode	Shows the tunnel mode as Normal, 802.1Q Tunnel or 802.1Q Tunnel Uplink (847).
802.1Q-tunnel TPID	Shows the Tag Protocol Identifier used for learning and switching packets (848).

test cable-diagnostics dsp

This command performs cable diagnostics on the specified port to diagnose any cable faults (short, open, etc.) and report the cable length.

SYNTAX

test cable-diagnostics dsp interface *interface*

interface

ethernet *unit/port*

unit - Unit identifier. (Range: 1)

port - Port number. (Range: 1-24)

COMMAND MODE

Privileged Exec

COMMAND USAGE

- Cable diagnostics are performed using Digital Signal Processing (DSP) test methods.
- This cable test is only accurate for cables 7 - 140 meters long.
- The test takes approximately 5 seconds. The switch displays the results of the test immediately upon completion, including common cable failures, as well as the status and approximate length of each cable pair.
- Potential conditions which may be listed by the diagnostics include:
  - OK: Correctly terminated pair
  - Open: Open pair, no link partner
  - Short: Shorted pair
  - Not Supported: This message is displayed for any Fast Ethernet ports that are linked up, or for any Gigabit Ethernet ports linked up at a speed lower than 1000 Mbps.
  - Impedance mismatch: Terminating impedance is not in the reference range.
- Ports are linked down while running cable diagnostics.

EXAMPLE

```
Console#test cable-diagnostics dsp interface ethernet 1/10
Console#show cable-diagnostics dsp interface e 1/10
Port     Type Link Status Pair A (meters)  Pair B (meters)  Last Update
-------- ---- ----------- ---------------- ---------------- -----------------
Eth 1/10   GE  Up          OK (21)          OK (21)         2009-11-13 09:44:19
Console#
```

test loop internal

This command performs an internal loop back test on the specified port.

SYNTAX

test loop internal interface *interface*

interface

ethernet *unit/port*

unit - Stack unit. (Range: 1)

port - Port number. (Range: 1-24)

COMMAND MODE

Privileged Exec

COMMAND USAGE

When performing an internal loopback test, packets from the specified interface are looped back into its internal PHY. Outgoing data is looped back to the receiver without actually being transmitted. Internal loopback makes it possible to check that an interface is working properly without having to make any network connections.

EXAMPLE

```
Console#test loop internal interface ethernet 1/1
Internal loopback test: succeeded
Console#
```

show cable-diagnostics

This command shows the results of a cable diagnostics test.

SYNTAX

show cable-diagnostics interface [*interface*]

interface

ethernet *unit*/*port*

unit - Unit identifier. (Range: 1)

port - Port number. (Range: 1-24)

COMMAND MODE

Privileged Exec

EXAMPLE

```
Console#show cable-diagnostics interface ethernet 1/10
Console#show cable-diagnostics interface e 1/10
Port     Type Link Status Pair A (meters)  Pair B (meters)  Last Update
-------- ---- ----------- ---------------- ---------------- -----------------
Eth 1/10   GE  Up          OK (21)          OK (21)          2009-11-13 09:44:19
Console#
```

show loop internal

This command shows the results of a loop back test.

SYNTAX

show loop internal interface [*interface*]

interface

ethernet *unit*/*port*

unit - Stack unit. (Range: 1)

port - Port number. (Range: 1-24)

COMMAND MODE

Privileged Exec

EXAMPLE

```
Console#show loop internal interface ethernet 1/1

 Port      Test Result     Last Update
 --------  --------------- --------------------
 Eth 1/1        Succeeded  2024-07-15 15:26:56
Console#
```

31 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 12 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 81: Link Aggregation Commands

Command	Function	Mode
Manual Configuration Commands		
interface port-channel	Configures a trunk and enters interface configuration mode for the trunk	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)
Trunk Status Display Commands		
show interfaces status port-channel	Shows trunk information	NE, PE
show lacp	Shows LACP information	PE

Guidelines for Creating Trunks

General Guidelines –

- Finish configuring port 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.

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: 1-32)

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 11:

```
Console(config)#interface port-channel 1
Console(config-if)#exit
Console(config)#interface ethernet 1/11
Console(config-if)#channel-group 1
Console(config-if)#
```

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 10-12. 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 1/10
Console(config-if)#lacp
Console(config-if)#interface ethernet 1/11
Console(config-if)#lacp
Console(config-if)#interface ethernet 1/12
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            : 10half, 10full, 100half, 100full, 1000full
  Flow Control            : Disabled
  Port Security           : Disabled
  Max MAC Count           : 0
 Current status:
  Created By              : LACP
  Link Status             : Up
  Port Operation Status   : Up
  Operation speed-duplex  : 100full
  Flow control Type       : None
  Member Ports            : Eth1/10, Eth1/11, Eth1/12,
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

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.
- 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)#
```

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: 1-32)

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 82: 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
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 83: 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.
LACP System Priority	LACP system priority assigned to this port channel.

Table 83: show lacp internal - display description (Continued)

Field	Description
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 84: 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.
Partner Oper Port Number	Operational port number assigned to this aggregation port by the port's protocol partner.

Table 84: show lacp neighbors - display description (Continued)

Field	Description
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 85: 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.

32 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 86: 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

Local Port Mirroring Commands

This section describes how to mirror traffic from a source port to a target port.

Table 87: 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 - Stack unit. (Range: 1)

port - Port number. (Range: 1-24)

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.

- 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.

EXAMPLE

The following example configures the switch to mirror all packets from port 6 to 11:

```
Console(config)#interface ethernet 1/11
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*]

interface - **ethernet** *unit*/*port* (source port)

unit - Stack unit. (Range: 1)

port - Port number. (Range: 1-24)

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 11:

```
Console(config)#interface ethernet 1/11
Console(config-if)#port monitor ethernet 1/6
Console(config-if)#end
Console#show port monitor
Port Mirroring
-------------------------------------
 Destination Port (listen port): Eth1/1
 Source Port (monitored port):   Eth1/6
 Mode                          :RX/TX
Console#
```

33 RATE LIMIT COMMANDS

This function allows 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 88: 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 Mbps.
(Range: 1-1000 Mbps)

DEFAULT SETTING

1000 Mbps

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. For example, suppose broadcast storm control is set to 500 pps by the command “switchport broadcast packet-rate 500,” and the rate limit is set to 20 Mbps by the command “rate-limit input 20" on a port. Since 20 Mbps is 1/5 of line speed (100 Mbps), the received rate will actually be 100 pps, or 1/5 of the

500 pps limit set by the storm control command. 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 (781)

34 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 89: 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

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 - Stack unit. (Range: 1)

port - Port number. (Range: 1-24)

port-channel *channel-id* (Range: 1-32)

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

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 - Stack unit. (Range: 1)

port - Port number. (Range: 1-24)

port-channel *channel-id* (Range: 1-32)

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

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 8K.

EXAMPLE

```
Console#show mac-address-table
 Interface MAC Address       VLAN Type     Life Time
 --------- ----------------- ---- -------- -----------------
  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#
```

35 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 90: 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 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 release-mode	Configures loopback release mode for a port	IC
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

Table 90: Spanning Tree Commands (Continued)

Command	Function	Mode
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 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) the root 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 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 (809)
spanning-tree max-age (810)

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 (809)
spanning-tree hello-time (809)

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
  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 819) takes precedence over port priority (page 825).

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 (816)
mst priority (815)
name (816)

revision (817)
max-hops (814)

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: 1-4093)

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 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 816) 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 817) 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 (817)

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 816) 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 (816)

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 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 (820)

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 to disable this feature.

SYNTAX

[**no**] **spanning-tree bpdu-guard**

DEFAULT SETTING

Disabled

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.

- 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 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 (820)
spanning-tree spanning-disabled (827)

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[14], 1-200,000,000 for long path cost method)

Table 91: Recommended STA Path Cost Range

Port Type	Short Path Cost (IEEE 802.1D-1998)	Long Path Cost (802.1D-2004)
Fast Ethernet	10-60	20,000-2,000,000
Gigabit Ethernet	3-10	2,000-200,000

[14] Use the spanning-tree pathcost method command on page 812 to set the path cost method.

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.

Table 92: Default STA Path Costs

Port Type	Short Path Cost (IEEE 802.1D-1998)	Long Path Cost (802.1D-2004)
Fast Ethernet	100,000	100,000
Gigabit Ethernet	10,000	10,000

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 812) 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

[**no**] **spanning-tree edge-port**

DEFAULT SETTING

Disabled

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 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 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, no leading zeroes)

cost - Path cost for an interface. (Range: 0 for auto-configuration, 1-65535 for short path cost method[15], 1-200,000,000 for long path cost method)

The recommended path cost range is listed in Table 91 on page 819.

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. The default path costs are listed in Table 92 on page 820.

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 (825)

[15] Use the spanning-tree pathcost method command to set the path cost method.

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, no leading zeroes)

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 (824)

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 (819)

spanning-tree root-guard

This command prevents a designated port[16] 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)

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.

[16] See Port Role under "Displaying Interface Settings for STA" on page 209.

EXAMPLE

```
Console(config)#interface ethernet 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 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 - Stack unit. (Range: 1)

port - Port number. (Range: 1-24)

port-channel *channel-id* (Range: 1-32)

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 - Stack unit. (Range: 1)

port - Port number. (Range: 1-24)

port-channel *channel-id* (Range: 1-32)

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) or for an instance within the multiple spanning tree (MST).

SYNTAX

show spanning-tree [*interface* | **mst** *instance-id*]

interface

ethernet *unit/port*

unit - Stack unit. (Range: 1)

port - Port number. (Range: 1-24)

port-channel *channel-id* (Range: 1-32)

instance-id - Instance identifier of the multiple spanning tree. (Range: 0-4094, no leading zeroes)

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** *instance-id* command to display the spanning tree configuration for an instance within the Multiple Spanning Tree (MST).

- For a description of the items displayed under "Spanning-tree information," see "Configuring Global Settings for STA" on page 199. For a description of the items displayed for specific interfaces, see "Displaying Interface Settings for STA" on page 209.

EXAMPLE

```
Console#show spanning-tree
Spanning Tree Information
---------------------------------------------------------------
 Spanning Tree Mode                 : MSTP
 Spanning Tree Enabled/Disabled     : Enabled
 Instance                           : 0
 VLANs Configuration                : 1-4093
 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
---------------------------------------------------------------
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
 Fast Forwarding                 : Disabled
 Forward Transitions             : 4
 Admin Edge Port                 : Disabled
 Oper Edge Port                  : Disabled
 Admin Link Type                 : Auto
 Oper Link Type                  : Point-to-point
 Spanning-Tree Status            : Enabled
 Loopback Detection Status       : Enabled
 Loopback Detection Release Mode : Auto
 Loopback Detection Trap         : Disabled
 Root Guard Status               : Disabled
 BPDU Guard Status               : Disabled
 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    1-4093
Console#
```

36 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 93: 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 Port-based Traffic Segmentation	Configures traffic segmentation for different client sessions based on specified downlink and uplink ports
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

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 94: 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 >= (2 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 (835)

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. Do not enter leading zeros. (Range: 1-4093).

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 105 for a description of the displayed items.

EXAMPLE

```
Console#show bridge-ext
 Maximum Supported VLAN Numbers         : 4093
 Maximum Supported VLAN ID              : 4093
 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
 GMRP                                   : 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 - Stack unit. (Range: 1)

port - Port number. (Range: 1-24)

port-channel *channel-id* (Range: 1-32)

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 (833)

show gvrp configuration

This command shows if GVRP is enabled.

SYNTAX

show gvrp configuration [*interface*]

interface

ethernet *unit*/*port*

unit - Stack unit. (Range: 1)

port - Port number. (Range: 1-24)

port-channel *channel-id* (Range: 1-32)

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 95: 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 (845)

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**}]

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: 1-4093, no leading zeroes)

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.

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 4093 VLANs on the switch.

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 (845)

CONFIGURING VLAN INTERFACES

Table 96: Commands for Configuring VLAN Interfaces

Command	Function	Mode
interface vlan	Enters interface configuration mode for a specified VLAN	GC
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: 1-4093, no leading zeroes)

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 (775)
interface (770)
vlan (837)

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 (842)

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: 1-4093).

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**}

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.

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 (839)

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: 1-4093, no leading zeroes)

DEFAULT SETTING

VLAN 1

COMMAND MODE

Interface Configuration (Ethernet, Port Channel)

COMMAND USAGE

- 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, an interface must first be configured as an untagged member before you can assign its PVID to that group.

- 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

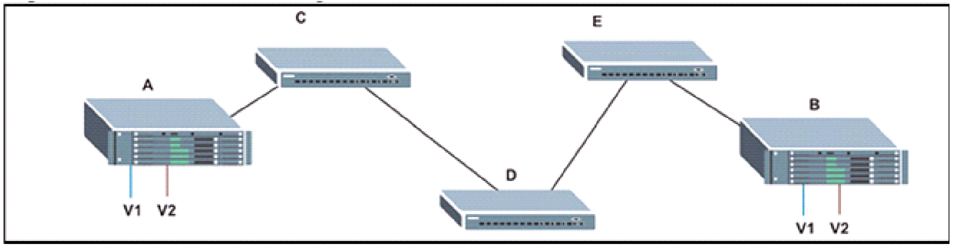
COMMAND MODE

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.



  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.

- The following restrictions apply to this feature:

  - VLAN trunking can only be enabled on Gigabit Ethernet ports or trunks.

  - VLAN trunking is mutually exclusive with the “access” switchport mode (see the switchport mode command). 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).

EXAMPLE

The following example enables VLAN trunking on ports 27 and 28 to establish a path across the switch for unknown VLAN groups:

```
Console(config)#interface ethernet 1/27
Console(config-if)#vlan-trunking
Console(config-if)#interface ethernet 1/28
Console(config-if)#vlan-trunking
Console(config-if)#
```

DISPLAYING VLAN INFORMATION

This section describes commands used to display VLAN information.

Table 97: 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*]

id - Keyword to be followed by the VLAN ID.

vlan-id - ID of the configured VLAN. (Range: 1-4093, no leading zeroes)

name - Keyword to be followed by the VLAN name.

vlan-name - ASCII string from 1 to 32 characters.

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)
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 98: 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 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 (849)
show interfaces switchport (781)

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 (849)
show interfaces switchport (781)

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.

- All ports on the switch will be set to the same ethertype.

EXAMPLE

```
Console(config)#interface ethernet 1/1
Console(config-if)#switchport dot1q-tunnel tpid 9100
Console(config-if)#
```

RELATED COMMANDS

show interfaces switchport (781)

show dot1q-tunnel

This command displays information about QinQ tunnel ports.

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

Current double-tagged status of the system is Enabled
The dot1q-tunnel mode of the set interface 1/1 is Access mode, TPID is 0x8100.
The dot1q-tunnel mode of the set interface 1/2 is Uplink mode, TPID is 0x8100.
The dot1q-tunnel mode of the set interface 1/3 is Normal mode, TPID is 0x8100.
 .
 .
 .
```

RELATED COMMANDS

switchport dot1q-tunnel mode (847)

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.

Table 99: Commands for Configuring Traffic Segmentation

Command	Function	Mode
traffic-segmentation	Enables and configures traffic segmentation	GC
show traffic-segmentation	Displays the configured traffic segments	PE

traffic-segmentation

This command enables traffic segmentation globally, or configures the uplink and down-link ports for a segmented group of ports. Use the **no** form to disable traffic segmentation globally.

SYNTAX

[**no**] **traffic-segmentation** [**uplink** *interface-list*
downlink *interface-list*]

uplink – Specifies an uplink interface.

downlink – Specifies a downlink interface.

DEFAULT SETTING

Disabled globally
No segmented port groups are defined.

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.

- Any port can be defined as an uplink port or downlink port, but cannot be configured to serve both roles.

- 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.

- Enter the **traffic-segmentation** command without any parameters to enable traffic segmentation. Then set the interface members for segmented groups.

- Enter **no traffic-segmentation** to disable traffic segmentation and clear the configuration settings for segmented groups.

EXAMPLE

This example enables traffic segmentation, and then sets port 12 as the uplink and ports 5-8 as downlinks.

```
Console(config)#traffic-segmentation
Console(config)#traffic-segmentation uplink ethernet 1/12
  downlink ethernet 1/5-8
Console(config)#
```

show traffic-segmentation

This command displays the configured traffic segments.

COMMAND MODE

Privileged Exec

EXAMPLE

```
Console#show traffic-segmentation
Private VLAN status: Disabled
Up-link Port:
 Ethernet 1/12
Down-link Port:
 Ethernet 1/5
 Ethernet 1/6
 Ethernet 1/7
 Ethernet 1/8
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 100: 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: 1-4093, no leading zeroes).

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 842.)

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: 1-4093, no leading zeroes).

secondary-vlan-id - ID of secondary (i.e, community) VLAN. (Range: 1-4093, no leading zeroes).

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: 1-4093, no leading zeroes).

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: 1-4093, no leading zeroes).

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 101: 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 837). 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[17] - 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.

DEFAULT SETTING

No protocol groups are configured.

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: 1-4093)

DEFAULT SETTING

No protocol groups are mapped for any interface.

[17] SNAP frame types are not supported by this switch due to hardware limitations.

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 - Stack unit. (Range: 1)

port - Port number. (ES3526MA: 1-26, ES4524MA: 1-24)

port-channel *channel-id* (Range: 1-12)

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 102: 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: 1-4093)

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.

- 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 103: 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: 1-4093)

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 104: 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

Table 104: Voice VLAN Commands (Continued)

Command	Function	Mode
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: 1-4093)

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.

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.

- Selecting 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. Selecting 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 951 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#
```

37 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 105: 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)	Maps TCP ports, IP precedence tags, or IP DSCP tags to class of service values

Priority Commands (Layer 2)

This section describes commands used to configure Layer 2 traffic priority on the switch.

Table 106: Priority Commands (Layer 2)

Command	Function	Mode
queue cos-map	Assigns class-of-service values to the priority queues	IC
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 cos-map	Shows the class-of-service map	PE
show queue mode	Shows the current queue mode	PE
show queue weight	Shows weights assigned to the weighted queues	PE

queue cos-map

This command assigns class of service (CoS) values to the priority queues (i.e., hardware output queues 0 - 7). Use the **no** form set the CoS map to the default values.

SYNTAX

queue cos-map *queue_id* [*cos1 ... cosn*]

no queue cos-map

queue_id - The ID of the priority queue.
Ranges are 0 to 7, where 7 is the highest priority queue.

cos1 ... cosn - The CoS values that are mapped to the queue ID. It is a space-separated list of numbers. The CoS value is a number from 0 to 7, where 7 is the highest priority.

DEFAULT SETTING

This switch supports Class of Service by using eight priority queues, with Weighted Round Robin queuing for each port. Eight separate traffic classes are defined in IEEE 802.1p. The default priority levels are assigned according to recommendations in the IEEE 802.1p standard as shown below.

Table 107: Default CoS Priority Levels

Priority	0	1	2	3	4	5	6	7
Queue	0	1	2	3	4	5	6	7

COMMAND MODE

Interface Configuration (Ethernet, Port Channel)

COMMAND USAGE

- CoS values assigned at the ingress port are also used at the egress port.
- This command sets the CoS priority for all interfaces.

EXAMPLE

The following example shows how to change the CoS assignments to a one-to-one mapping:

```
Console(config)#interface ethernet 1/1
Console(config-if)#queue cos-map 0 0
Console(config-if)#queue cos-map 1 1
Console(config-if)#queue cos-map 2 2
Console(config-if)#exit
Console#show queue cos-map ethernet 1/1
Information of Eth 1/1
 CoS Value:      0 1 2 3 4 5 6 7
 Priority Queue: 2 0 1 3 4 5 6 7
Console#
```

RELATED COMMANDS

show queue cos-map (876)

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 Weighted Round-Robin 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

Weighted Round Robin

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.

EXAMPLE

The following example sets the queue mode to strict priority service mode:

```
Console(config)#interface ge1/1
Console(config-if)#queue mode strict
Console(config-if)#
```

RELATED COMMANDS

queue weight (874)
show queue mode (876)

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 the queuing mode that uses a combination of strict and weighted queuing (page 873).
- 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)#interface ge1/1
Console(config-if)#queue weight 1 2 3 4 5 6 7 8
Console(config-if)#
```

RELATED COMMANDS

queue mode (873)
show queue weight (877)

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 (781)

show queue cos-map

This command shows the class of service priority map.

SYNTAX

show queue cos-map [*interface*]

ethernet *unit*/*port*

unit - Stack unit. (Range: 1)

port - Port number. (Range: 1-24)

port-channel *channel-id* (Range: 1-32)

DEFAULT SETTING

None

COMMAND MODE

Privileged Exec

EXAMPLE

```
Console#show queue cos-map ethernet 1/1
Information of Eth 1/1
 CoS Value:      0 1 2 3 4 5 6 7
 Priority Queue: 2 0 1 3 4 5 6 7
Console#
```

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: 1-24)

port-channel *channel-id* (Range: 1-32)

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: 1-24)

port-channel *channel-id* (Range: 1-32)

Command Mode

Privileged Exec

Example

```
Console#show queue weight ethernet 1/1
Information of Eth 1/1
 Queue ID  Weight
 --------  ------
        0       1
        1       2
        2       4
        3       6
        4       8
        5      10
        6      12
        7      14
Console#
```

PRIORITY COMMANDS (LAYER 3 AND 4)

This section describes commands used to configure Layer 3 and 4 traffic priority mapping on the switch.

Table 108: Priority Commands (Layer 3 and 4)

Command	Function	Mode
map ip dscp	Enables IP DSCP class of service mapping	GC
map ip port	Enables TCP/UDP class of service mapping	GC
map ip precedence	Enables IP precedence class of service mapping	GC
map ip dscp	Maps IP DSCP value to a class of service	IC
map ip port	Maps TCP/UDP socket to a class of service	IC
map ip precedence	Maps IP precedence value to a class of service	IC
show map ip dscp	Shows the IP DSCP map	PE
show map ip port	Shows the IP port map	PE
show map ip precedence	Shows the IP precedence map	PE

map ip dscp (Global Configuration)

This command enables IP DSCP mapping (i.e., Differentiated Services Code Point mapping). Use the **no** form to disable IP DSCP mapping.

SYNTAX

[**no**] **map ip dscp**

DEFAULT SETTING

Disabled

COMMAND MODE

Global Configuration

COMMAND USAGE

- The precedence for priority mapping is IP Port, IP Precedence or IP DSCP, and default switchport priority.
- IP Precedence and IP DSCP cannot both be enabled. Enabling one of these priority types will automatically disable the other type.

EXAMPLE

The following example shows how to enable IP DSCP mapping globally:

```
Console(config)#map ip dscp
Console(config)#
```

map ip port (Global Configuration)

This command enables IP port mapping (i.e., class of service mapping for TCP/UDP sockets). Use the **no** form to disable IP port mapping.

SYNTAX

[**no**] **map ip port**

DEFAULT SETTING

Disabled

COMMAND MODE

Global Configuration

COMMAND USAGE

The precedence for priority mapping is IP Port, IP Precedence or IP DSCP, and default switchport priority.

EXAMPLE

The following example shows how to enable TCP/UDP port mapping globally:

```
Console(config)#map ip port
Console(config)#
```

map ip precedence (Global Configuration)

This command enables IP precedence mapping (i.e., IP Type of Service). Use the **no** form to disable IP precedence mapping.

SYNTAX

[**no**] **map ip precedence**

DEFAULT SETTING

Disabled

COMMAND MODE

Global Configuration

COMMAND USAGE

- The precedence for priority mapping is IP Port, IP Precedence or IP DSCP, and default switchport priority.

- IP Precedence and IP DSCP cannot both be enabled. Enabling one of these priority types will automatically disable the other type.

EXAMPLE

The following example shows how to enable IP precedence mapping globally:

```
Console(config)#map ip precedence
Console(config)#
```

map ip dscp (Interface Configuration)

This command sets IP DSCP priority (i.e., Differentiated Services Code Point priority). Use the **no** form to restore the default table.

SYNTAX

map ip dscp *dscp-value* **cos** *cos-value*

no map ip dscp

dscp-value - 8-bit DSCP value. (Range: 0-63)

cos-value - Class-of-Service value (Range: 0-7)

DEFAULT SETTING

The DSCP default values are defined in the following table. Note that all the DSCP values that are not specified are mapped to CoS value 0.

Table 109: Mapping IP DSCP to CoS Values

IP DSCP Value	CoS Value
0	0
8	1
10, 12, 14, 16	2
18, 20, 22, 24	3
26, 28, 30, 32, 34, 36	4
38, 40, 42	5
48	6
46, 56	7

COMMAND MODE

Interface Configuration (Ethernet, Port Channel)

COMMAND USAGE

- The precedence for priority mapping is IP Port, IP Precedence or IP DSCP, and default switchport priority.
- DSCP priority values are mapped to default Class of Service values according to recommendations in the IEEE 802.1p standard, and then subsequently mapped to the eight hardware priority queues.
- This command sets the IP DSCP priority for all interfaces.

EXAMPLE

The following example shows how to map IP DSCP value 1 to CoS value 0:

```
Console(config)#interface ethernet 1/5
Console(config-if)#map ip dscp 1 cos 0
Console(config-if)#
```

map ip port (Interface Configuration)

This command sets IP port priority (i.e., TCP/UDP port priority). Use the **no** form to remove a specific setting.

SYNTAX

map ip port *port-number* **cos** *cos-value*

no map ip port *port-number*

port-number - 16-bit TCP/UDP port number. (Range: 0-65535)

cos-value - Class-of-Service value (Range: 0-7)

DEFAULT SETTING

None

COMMAND MODE

Interface Configuration (Ethernet, Port Channel)

COMMAND USAGE

- The precedence for priority mapping is IP Port, IP Precedence or IP DSCP, and default switchport priority.
- Up to 8 entries can be specified for IP Port priority mapping.
- This command sets the IP port priority for all interfaces.

EXAMPLE

The following example shows how to map HTTP traffic to CoS value 0:

```
Console(config)#interface ethernet 1/5
Console(config-if)#map ip port 80 cos 0
Console(config-if)#
```

map ip precedence (Interface Configuration)

This command sets IP precedence priority (i.e., IP Type of Service priority). Use the **no** form to restore the default table.

SYNTAX

map ip precedence *ip-precedence-value* **cos** *cos-value*

no map ip precedence

precedence-value - 3-bit precedence value. (Range: 0-7)

cos-value - Class-of-Service value (Range: 0-7)

DEFAULT SETTING

The list below shows the default priority mapping.

Table 110: Mapping IP Precedence to CoS Values

IP Precedence Value	0	1	2	3	4	5	6	7
CoS Value	0	1	2	3	4	5	6	7

COMMAND MODE

Interface Configuration (Ethernet, Port Channel)

COMMAND USAGE

- The precedence for priority mapping is IP Port, IP Precedence or IP DSCP, and default switchport priority.

- IP Precedence values are mapped to default Class of Service values on a one-to-one basis according to recommendations in the IEEE 802.1p standard, and then subsequently mapped to the eight hardware priority queues.

- This command sets the IP Precedence for all interfaces.

EXAMPLE

The following example shows how to map IP precedence value 1 to CoS value 0:

```
Console(config)#interface ethernet 1/5
Console(config-if)#map ip precedence 1 cos 0
Console(config-if)#
```

show map ip dscp

This command shows the IP DSCP priority map.

Syntax

show map ip dscp [*interface*]

interface

ethernet *unit*/*port*

unit - Stack unit. (Range: 1)

port - Port number. (Range: 1-24)

port-channel *channel-id* (Range: 1-32)

Default Setting

None

Command Mode

Privileged Exec

Example

```
Console#show map ip dscp ethernet 1/1
DSCP mapping status: Disabled

 Port      DSCP CoS
 --------- ---- ---
  Eth 1/ 1    0   0
  Eth 1/ 1    1   0
  Eth 1/ 1    2   0
  Eth 1/ 1    3   0
⋮
  Eth 1/ 1   61   0
  Eth 1/ 1   62   0
  Eth 1/ 1   63   0
Console#
```

show map ip port

This command shows the IP port priority map.

Syntax

show map ip port [*interface*]

interface

ethernet *unit*/*port*

unit - Stack unit. (Range: 1)

port - Port number. (Range: 1-24)

port-channel *channel-id* (Range: 1-32)

Command Mode

Privileged Exec

EXAMPLE

The following shows that HTTP traffic has been mapped to CoS value 0:

```
Console#show map ip port
TCP port mapping status: disabled

 Port      IP Port  CoS
 --------- -------- ---
  Eth 1/ 5       80   0
Console#
```

show map ip precedence

This command shows the IP precedence priority map.

SYNTAX

show map ip precedence [*interface*]

interface

ethernet *unit/port*

unit - Stack unit. (Range: 1)

port - Port number. (Range: 1-24)

port-channel *channel-id* (Range: 1-32)

COMMAND MODE

Privileged Exec

EXAMPLE

```
Console#show map ip precedence ethernet 1/5
Precedence mapping status: Disabled

 Port      Precedence CoS
 --------- ---------- ---
  Eth 1/ 5          0   0
  Eth 1/ 5          1   1
  Eth 1/ 5          2   2
  Eth 1/ 5          3   3
  Eth 1/ 5          4   4
  Eth 1/ 5          5   5
  Eth 1/ 5          6   6
  Eth 1/ 5          7   7
Console#
```

38 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 111: 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 in the packet's VLAN tag	PM-C
set phb	Services IP traffic by setting a per-hop behavior value for matching packets in the ToS field of the IP header	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 specifc type of traffic based on an access list, a DSCP or IP Precedence value, or a VLAN.

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 or class of service 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: 1-16 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 889). The policy map is then bound by a service policy to an interface (page 899). 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 (900)

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* | **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 IP ACLs and MAC ACLs. (Range: 1-16 characters)

dscp - A Differentiated Service Code Point value. (Range: 0-63)

ip-precedence - An IP Precedence value. (Range: 0-7)

vlan - A VLAN. (Range:1-4093)

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: 1-16 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: 1-16 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 889) 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 ip dscp 3
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: 1-16 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: 64-1000000 kbps at a granularity of 64 kbps or maximum port speed, whichever is lower)

committed-burst - Committed burst size (BC) in bytes. (Range: 4000-16000000 at a granularity of 4k 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: 64-1000000 kbps at a granularity of 64 kbps or maximum port speed, whichever is lower)

committed-burst - Committed burst size (BC) in bytes.
(Range: 4000-16000000 at a granularity of 4k bytes)

excess-burst - Excess burst size (BE) in bytes.
(Range: 4000-1600000 at a granularity of 4k 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: 64-1000000 kbps at a granularity of 64 kbps or maximum port speed, whichever is lower)

committed-burst - Committed burst size (BC) in bytes. (Range: 4000-16000000 at a granularity of 4k bytes)

peak-rate - Peak information rate (PIR) in kilobits per second. (Range: 64-1000000 kbps at a granularity of 64 kbps or maximum port speed, whichever is lower)

peak-burst - Burst size (BP) in bytes. (Range: 4000-16000000 at a granularity of 4k 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.)

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* 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) in the ToS field of the IP header. 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 the per-hop behavior value in the IP header 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 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 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.

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.
- The switch does not allow a policy map to be bound to an interface for egress traffic.

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: 1-16 characters)

class-map-name - Name of the class map. (Range: 1-16 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 - Stack unit. (Range: 1)

port - Port number. (Range: 1-24)

port-channel *channel-id* (Range: 1-32)

COMMAND MODE

Privileged Exec

EXAMPLE

```
Console#show policy-map interface 1/5 input
Service-policy rd-policy
Console#
```

39 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 112: 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
Multicast VLAN Registration	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

IGMP SNOOPING

This section describes commands used to configure IGMP snooping on the switch.

Table 113: IGMP Snooping Commands

Command	Function	Mode
ip igmp snooping	Enables IGMP snooping	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 report suppression/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 proxy general queries	GC
ip igmp snooping vlan query-resp-intvl	Configures the maximum time the system waits for a response to proxy general queries	GC
ip igmp snooping vlan static	Adds an interface as a member of a multicast group	GC

Table 113: IGMP Snooping Commands (Continued)

Command	Function	Mode
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 mac-address-table multicast	Shows known multicast addresses	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: 1-4093)

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 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: 1-4093)

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 report suppression, last leave, and query suppression. Report suppression intercepts, absorbs and summarizes IGMP reports coming from downstream hosts. Last leave sends out a proxy query when the last member leaves a multicast group, and query suppression means that neither specific queries nor general queries are 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 report suppression/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 906).

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: 1-4093)

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: 1-4093)

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: 1-4093)

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: 1-4093)

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: 1-4093)

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 is enabled (page 906).

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: 1-4093)

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 906).

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: 1-4093)

DEFAULT SETTING

Enabled

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: 1-4093)

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.

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: 1-4093)

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 906), or as a proxy host when IGMP snooping proxy reporting is enabled (page 906).

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: 1-4093)

interval - The maximum time the system waits for a response to general queries. (Range: 10-31744 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 906), or as a proxy host when IGMP snooping proxy reporting is enabled (page 906).

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: 1-4093)

ip-address - IP address for multicast group

interface

ethernet *unit/port*

unit - Stack unit. (Range: 1)

port - Port number. (Range: 1-24)

port-channel *channel-id* (Range: 1-32)

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.

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 391 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 (Disabled)
 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 [**vlan** *vlan-id* [**user** | **igmp-snp**]] [**user** | **igmpsnp**]

vlan-id - VLAN ID (1-4093)

user - Display only the user-configured multicast entries.

igmpsnp - Display only entries learned through IGMP snooping.

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
VLAN     Group            Source           Port List
-------- ---------------- ---------------- ---------------------------------
       1 239.255.255.250  *                Eth1/ 1(D) Eth1/13(D)
       1 224.1.1.12       *                Eth 1/23(D)
Console#
```

show mac-address-table multicast

This command shows known multicast addresses.

SYNTAX

show mac-address-table multicast
[**vlan** *vlan-id* [**user** | **igmp-snp**]] [**user** | **igmp-snooping**]

vlan-id - VLAN ID (1 to 4093)

user - Display only the user-configured multicast entries.

igmp-snooping - Display only entries learned through IGMP snooping.

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 mac-address-table multicast vlan 1
 VLAN M'cast IP addr. Member ports Type
 ---- --------------- ------------ -------
    1       224.1.2.3      Eth1/11    IGMP
Console#
```

STATIC MULTICAST ROUTING

This section describes commands used to configure static multicast routing on the switch.

Table 114: 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: 1-4093)

interface

ethernet *unit/port*

unit - Stack unit. (Range: 1)

port - Port number. (Range: 1-24)

port-channel *channel-id* (Range: 1-32)

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.

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: 1-4093)

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
 ---- ------------------ -------
    1           Eth 1/11  Static
    2           Eth 1/12  Dynamic
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 115: 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 filter	Assigns an IGMP filter profile to an interface	IC
ip igmp max-groups	Specifies an IGMP throttling number for an interface	IC

Table 115: IGMP Filtering and Throttling Commands (Continued)

Command	Function	Mode
ip igmp max-groups action	Sets the IGMP throttling action for an interface	IC
show ip igmp filter	Displays the IGMP filtering status	PE
show ip igmp profile	Displays IGMP profiles and settings	PE
show ip igmp throttle interface	Displays the IGMP throttling setting for interfaces	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 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: 0-64)

DEFAULT SETTING

64

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 {**replace** | **deny**}

replace - The new multicast group replaces an existing group.

deny - The new multicast group join report is dropped.

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)#
```

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 - Stack unit. (Range: 1)

port - Port number. (Range: 1-24)

port-channel *channel-id* (Range: 1-32)

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 throttle interface

This command displays the interface settings for IGMP throttling.

SYNTAX

show ip igmp throttle interface [*interface*]

interface

ethernet *unit/port*

unit - Stack unit. (Range: 1)

port - Port number. (Range: 1-24)

port-channel *channel-id* (Range: 1-32)

DEFAULT SETTING

None

COMMAND MODE

Privileged Exec

COMMAND USAGE

Using this command without specifying an interface displays 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#
```

MULTICAST VLAN REGISTRATION

This section describes commands used to configure Multicast VLAN Registration (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 116: Multicast VLAN Registration Commands

Command	Function	Mode
mvr	Globally enables MVR, statically configures MVR group address(es), or specifies the MVR VLAN identifier	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 receviever VLAN	IC
show mvr	Shows information about the global MVR configuration settings, interfaces attached to the MVR VLAN, or the multicast groups assigned to the MVR VLAN	PE

mvr

This command enables Multicast VLAN Registration (MVR) globally on the switch, statically configures MVR multicast group IP address(es) using the **group** keyword, or specifies the MVR VLAN identifier using the **vlan** keyword. Use the **no** form of this command without any keywords to globally disable MVR. Use the **no** form with the **group** keyword to remove a specific address or range of addresses. Or use the **no** form with the **vlan** keyword to restore the default MVR VLAN.

SYNTAX

[**no**] **mvr** [**group** *ip-address* [*count*] | **vlan** *vlan-id*]

group - Defines a multicast service sent to all attached subscribers.

ip-address - IP address for an MVR multicast group.
(Range: 224.0.1.0 - 239.255.255.255)

count - The number of contiguous MVR group addresses.
(Range: 1-255)

vlan - Specifies the VLAN through which MVR multicast data is received. This is also the VLAN to which all source ports must be assigned.

vlan-id - MVR VLAN ID (Range: 1-4093)

DEFAULT SETTING

MVR is disabled.
No MVR group address is defined.
The default number of contiguous addresses is 0.
MVR VLAN ID is 1.

COMMAND MODE

Global Configuration

COMMAND USAGE

- Use the **mvr group** 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, and 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.

- 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.

- IGMP snooping must be enabled to a allow a subscriber to dynamically join or leave an MVR group (see the ip igmp snooping command). Note that only IGMP version 2 or 3 hosts can issue multicast join or leave messages.

- IGMP snooping and MVR share a maximum number of 255 groups. Any multicast streams received in excess of this limitation will be flooded to all ports in the associated VLAN.

EXAMPLE

The following example enables MVR globally, and configures a range of MVR group addresses:

```
Console(config)#mvr
Console(config)#mvr group 228.1.23.1 10
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 immediate**

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 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.

EXAMPLE

The following enables immediate leave on a receiver port.

```
Console(config)#interface ethernet 1/5
Console(config-if)#mvr immediate
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 type** {**receiver** | **source**}

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 be configured as a member of the MVR VLAN. IGMP snooping can be used to allow a receiver port to dynamically join or leave multicast groups sourced through the MVR VLAN. Also, note that VLAN membership for MVR receiver ports cannot be set to trunk 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 IGMP snooping or which have been assigned through the mvr group (Global Configuration) command.

- IGMP snooping must be enabled to a allow a subscriber to dynamically join or leave an MVR group (see the ip igmp snooping command). Note that only IGMP version 2 or 3 hosts can issue multicast join or leave messages.

EXAMPLE

The following configures one source port and several receiver ports on the switch.

```
Console(config)#interface ethernet 1/5
Console(config-if)#mvr type source
Console(config-if)#exit
Console(config)#interface ethernet 1/6
Console(config-if)#mvr type receiver
Console(config-if)#exit
Console(config)#interface ethernet 1/7
Console(config-if)#mvr 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 vlan** *vlan-id* **group** *ip-address*

vlan-id - Receiver VLAN to which the specified multicast traffic is flooded. (Range: 1-4093)

group - Defines a multicast service sent to the selected port.

ip-address - Statically configures an interface to receive multicast traffic from the IP 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.
- IGMP snooping must be enabled to a allow a subscriber to dynamically join or leave an MVR group (see the ip igmp snooping command). Note that only IGMP version 2 or 3 hosts can issue multicast join or leave messages.

EXAMPLE

The following statically assigns a multicast group to a receiver port:

```
Console(config)#interface ethernet 1/7
Console(config-if)#mvr type receiver
Console(config-if)#mvr vlan 3 group 225.0.0.5
Console(config-if)#
```

show mvr

This command shows information about the global MVR configuration settings when entered without any keywords, the interfaces attached to the MVR VLAN using the **interface** keyword, or the multicast groups assigned to the MVR VLAN using the **members** keyword.

SYNTAX

show mvr [**interface** [*interface*] | **members** [*ip-address*]]

interface

ethernet *unit*/*port*

unit - Stack unit. (Range: 1)

port - Port number. (Range: 1-24)

port-channel *channel-id* (Range: 1-32)

ip-address - IP address for an MVR multicast group. (Range: 224.0.1.0 - 239.255.255.255)

DEFAULT SETTING

Displays global configuration settings for MVR when no keywords are used.

COMMAND MODE

Privileged Exec

COMMAND USAGE

Enter this command without any keywords to display the global settings for MVR. Use the **interface** keyword to display information about interfaces attached to the MVR VLAN. Or use the **members** keyword to display information about multicast groups assigned to the MVR VLAN.

EXAMPLE

The following shows the global MVR settings:

```
Console#show mvr
 MVR Config Status    : Enabled
 MVR Running Status   : Active
 MVR Multicast VLAN   : 1
 MVR Group Address    : 225.0.0.5
 MVR Group Count      : 10
Console#
```

Table 117: show mvr - display description

Field	Description
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.

Table 117: show mvr - display description (Continued)

Field	Description
MVR Group Address	A multicast service sent to all attached subscribers
MVR Group Count	The number of contiguous MVR group addresses.

The following displays information about the interfaces attached to the MVR VLAN:

```
Console#show mvr interface
 Port        Type        Status          Immediate   Static Group Address
 --------    --------    -------------   ---------   --------------------
 Eth1/ 2     Source      Active/Up
 Eth1/ 3     Source      Inactive/Down
 Eth1/ 1     Receiver    Active/Up       Disabled    225.0.0.1(VLAN1)
                                                     225.0.0.9(VLAN3)
 Eth1/ 4     Receiver    Active/Down     Disabled

Console#
```

Table 118: show mvr 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 Leave	Shows if immediate leave is enabled or disabled.
Static Group Address	Shows any static MVR group assigned to an interface, and the receiver VLAN.

The following shows information about the interfaces associated with multicast groups assigned to the MVR VLAN:

```
Console#show mvr members
 MVR Forwarding Entry Count:1
 Group Address     Source Address    VLAN  Forwarding Port
 -------------     --------------    ----  --------------
 225.0.0.9         *                 2     Eth1/ 1(VLAN3)    Eth1/ 2(VLAN2)
Console#
```

Table 119: show mvr members - display description

Field	Description
MVR Forwarding Entry Count	The number of multicast services currently being forwarded from the MVR VLAN.
Group Address	Multicast groups assigned to the MVR VLAN.

Table 119: show mvr members - display description (Continued)

Field	Description
Source Address	Indicates the source address of the multicast service, or displays an asterisk if the group address has been statically assigned.
VLAN	Indicates the MVR VLAN receiving the multicast service.
Forwarding Port	Shows the interfaces with subscribers for multicast services provided through the MVR VLAN. Also shows 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.

IGMP (Layer 3)

This section describes commands used to configure Layer 3 Internet Group Management Protocol (IGMP) on the switch.

Table 120: 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 - Dense Mode, 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 (905)
show ip igmp snooping (919)

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 940).

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 (943)
ip igmp query-interval (940)

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 (939)

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: 1-4093)

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: 1-4093)

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
GroupAddress    InterfaceVlan   Lastreporter    Uptime   Expire   V1Timer
--------------- --------------- --------------- -------- -------- --------
    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
GroupAddress    InterfaceVlan   Lastreporter    Uptime   Expire   V1Timer
--------------- --------------- --------------- -------- -------- --------
    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
GroupAddress    VLAN   LastReporter    Uptime   Expire   V1 Timer
--------------- ------ --------------- -------- -------- --------
    224.0.17.17      1    192.168.1.10    0:0:1   0:4:19    0:0:0
Console#
```

Table 121: show ip igmp groups - display description

Field	Description
Group Address	IP multicast group address with subscribers directly attached or downstream from the switch.
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 122: 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 122: 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: 1-4093)

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.

```
Console#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 :
Console#
```

IGMP PROXY ROUTING

This section describes commands used to configure IGMP Proxy Routing on the switch.

Table 123: 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.

```
Console(config)#interface vlan
Console(config-if)#ip igmp proxy unsolicited-report-interval 5
Console(config)#
```

40 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.

Table 124: 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 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
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 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

Table 124: LLDP Commands (Continued)

Command	Function	Mode
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 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 (holdtime-multiplier * refresh-interval) ≤ 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 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

COMMAND USAGE

This attribute must comply with the following rule:
(refresh-interval * holdtime-multiplier) ≤ 65536

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 related 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 and protocol-based VLANs configured on this interface (see "Configuring VLAN Interfaces" on page 838 and "Configuring Protocol-based VLANs" on page 857).

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 840 and "protocol-vlan protocol-group (Configuring Interfaces)" on page 858.

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

Enabled

COMMAND MODE

Interface Configuration (Ethernet, Port Channel)

COMMAND USAGE

Refer to "Frame Size" on page 592 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 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

Enabled

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 - Stack unit. (Range: 1)

port - Port number. (Range: 1-24)

port-channel *channel-id* (Range: 1-32)

COMMAND MODE

Privileged Exec

EXAMPLE

```
Console#show lldp config

LLDP Global Configuation

 LLDP Enable                : Yes
 LLDP Transmit interval     : 30
 LLDP Hold Time Multiplier  : 4
 LLDP Delay Interval        : 2
 LLDP Reinit Delay          : 2
 LLDP Notification Interval : 5
 LLDP MED fast start counts : 4


LLDP Port Configuration
  Interface |AdminStatus NotificationEnabled
  --------- + ----------- -------------------
  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
  *poe
  *link-agg
  *max-frame

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 - Stack unit. (Range: 1)

port - Port number. (Range: 1-24)

port-channel *channel-id* (Range: 1-32)

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 : ECS4610-50T/ECS4610-26T
  System Capabilities Support : Bridge
  System Capabilities Enable  : Bridge
  Management Address : 192.168.0.101 (IPv4)

 LLDP Port Information
 Interface |PortID Type      PortID            PortDesc
 --------- + ---------------- ----------------- ---------------------------
 Eth 1/1   |MAC Address      00-01-02-03-04-06 Ethernet Port on unit 1, port 1
 Eth 1/2   |MAC Address      00-01-02-03-04-07 Ethernet Port on unit 1, port 2
 Eth 1/3   |MAC Address      00-01-02-03-04-08 Ethernet Port on unit 1, port 3
 Eth 1/4   |MAC Address      00-01-02-03-04-09 Ethernet Port on unit 1, port 4
.
.
.
Console#show lldp info local-device detail ethernet 1/1

LLDP Port Information Detail

 Port      : Eth 1/1
 Port Type : MAC Address
 Port ID   : 00-01-02-03-04-06
 Port Desc : Ethernet Port on unit 1, port 1

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 - Stack unit. (Range: 1)

port - Port number. (Range: 1-24)

port-channel *channel-id* (Range: 1-32)

COMMAND MODE

Privileged Exec

EXAMPLE

```
Console#show lldp info remote-device

 LLDP Remote Devices Information

  Interface | ChassisId         PortId            SysName
  --------- + ----------------- ----------------- ---------------------
  Eth 1/1   | 00-01-02-03-04-05 00-01-02-03-04-06

Console#show lldp info remote-device detail ethernet 1/1

 LLDP Remote Devices Information Detail

----------------------------------------------------------------
  Local PortName       : Eth 1/1
  Chassis Type         : MAC Address
  Chassis Id           : 00-01-02-03-04-05
  PortID Type        : MAC Address
  PortID             : 00-01-02-03-04-06
  SysName            :
  System Description : ECS4610-50T/ECS4610-26T
  Port Description   : Ethernet Port on unit 1, port 1
  SystemCapSupported : Bridge, Router
  SystemCapEnabled   : Bridge, Router
  Remote Management Address :
    192.168.0.2 (IPv4)
  Remote Port VID : 1
  Remote VLAN Name :
    VLAN-1 : DefaultVlan
  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) : 6C01
    Remote port MAU type : 30
  Remote Link Aggregation :
    Remote link aggregation capable : Yes
    Remote link aggragation enable : No
  Remote link aggragation port id : 0
  Remote Max Frame Size : 1518

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 - Stack unit. (Range: 1)

port - Port number. (Range: 1-24)

port-channel *channel-id* (Range: 1-32)

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
  Interface | NumFramesRecvd NumFramesSent NumFramesDiscarded
  --------- + -------------- ------------- ------------------
  Eth 1/1   | 10             11            0
  Eth 1/2   | 0              0             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#
```

41 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 125: 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: 1-68 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 (971)

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 (971)
ip name-server (973)

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 (969)
ip name-server (973)
ip domain-lookup (970)

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 - IP address of domain-name server.

server-address2 … *server-address6* - IP 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 (971)
ip domain-lookup (970)

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 the **clear host** command to clear dynamic entries, or the no ip host command to clear static entries.

Example

This example clears all static 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     Domain
------- ------- ------- --------------- ------- --------
      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 126: 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.
Domain	The domain 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 127: 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.

42 DHCP Commands

These commands are used to configure Dynamic Host Configuration Protocol (DHCP) client, relay, and server functions. Any VLAN interface can be configured to automatically obtain an address through DHCP. This switch can 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 128: 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 129: DHCP Client Commands

Command	Function	Mode
DHCP for IPv4		
ip dhcp restart client	Submits a BOOTP or DHCP client request	PE

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 (bia 12-34-12-34-12-34)
  Index: 1001, MTU: 1500, Bandwidth: 1g
  Address Mode is DHCP
  IP Address: 192.168.0.9 Mask: 255.255.255.0
  Proxy ARP is disabled
Console#
```

RELATED COMMANDS

ip address (1006)

DHCP RELAY

This section describes commands used to configure DHCP relay functions for host devices attached to the switch.

Table 130: DHCP Relay Commands

Command	Function	Mode
ip dhcp relay server	Specifies DHCP server addresses for relay	IC
ip dhcp restart relay	Enables DHCP relay agent	PE

ip dhcp relay server

This command specifies the addresses of DHCP servers 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: 1-3 addresses)

DEFAULT SETTING

None

Command Mode

Interface Configuration (VLAN)

Usage Guidelines

- 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.
- 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)#
```

Related Commands

ip dhcp restart relay (981)

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(config)#ip dhcp restart relay
Console(config)#end
Console#show ip interface

Vlan 1 is up, addressing mode is Dhcp
  Interface address is 10.1.0.254, mask is 255.255.255.0, Primary
  MTU is 1500 bytes
  Proxy ARP is disabled
  Split horizon is enabled
Console#
```

RELATED COMMANDS

ip dhcp relay server (980)

DHCP SERVER

This section describes commands used to configure client address pools for the DHCP service.

Table 131: 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
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 binding	Displays address bindings on the DHCP server	PE, NE
show ip dhcp	Dsplays 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 (991)
host (988)

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 (992)

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 (988)

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 (988)

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 991). 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 (985)
hardware-address (987)

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 (991)

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 (990)

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 (984)

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 (993)

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

Normal Exec, 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

This command displays 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#
```

43 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 132: 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 (998)

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 (997)

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: 1-4093)

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 133: 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

Table 133: show vrrp - display description (Continued)

Field	Description
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
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 134: 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: 1-4093)

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: 1-4093)

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 461 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#
```

44 IP Interface Commands

An IP address may be used for management access to the switch over the network. You can manually configure a specific address or direct the switch to obtain an address from a BOOTP or DHCP server when it is powered on.

An address for this switch is obtained via DHCP by default for VLAN 1. You may also need to a establish a default gateway between this device and management stations that exist on another network segment.

IP 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 135: IP Interface Commands

Command Group	Function
Basic IP 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 IP CONFIGURATION

This section describes commands used to configure IP addresses for VLAN interfaces on the switch.

Table 136: 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 router 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
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

ip address {*ip-address netmask* | **bootp** | **dhcp**} [**secondary**]

no ip address

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.

bootp - Obtains IP address from BOOTP.

dhcp - Obtains IP address from DHCP.

secondary - Specifies a secondary IP address.

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 in a network segment uses a secondary address, all other routers 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. Therefore, if routing is enabled, 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)#
```

RELATED COMMANDS

ip dhcp restart client (979)

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 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.

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
```

RELATED COMMANDS

ip route (1020)
show ip route (1021)

show ip interface

This command displays the settings of an IPv4 interface.

COMMAND MODE

Privileged Exec

EXAMPLE

```
Console#show ip interface
Loopback 0 is Administrative Up - Link Up
  Address is 00-00-00-00-00-00 (via 00-00-00-00-00-00)
  Index: 746, MTU: 0, Bandwidth: 1g
  Address Mode is User specified
  Proxy ARP is disabled
Vlan 1 is Administrative Up - Link Up
  Address is 00-00-E8-93-82-A0 (via 00-00-E8-93-82-A0)
  Index: 1001, MTU: 1280, Bandwidth: 1g
  Address Mode is User specified
  IP Address: 192.168.1.3 Mask: 255.255.255.0
  Proxy ARP is disabled
Console#
```

RELATED COMMANDS

ip address (1006)

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.

EXAMPLE

```
Console#traceroute 192.168.0.1
Press "ESC" to abort.

Source address:         192.168.0.9
Destination address:    192.168.0.1

Hop    IP Address             Packet 1           Packet 2           Packet 3
----------------------------------------------------------------------------
1    192.168.0.1                 <10 ms             <10 ms             <10 ms

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 enabled (see page 970). If necessary, local devices can also be specified in the DNS static host table (see page 972).

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 (770)

ARP CONFIGURATION

This section describes commands used to configure the Address Resolution Protocol (ARP) on the switch.

Table 137: 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 (1014)
show arp (1014)

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.

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 VLAN 1
     10.1.0.254 00-00-ab-cd-00-00     other VLAN 1
     10.1.0.255 ff-ff-ff-ff-ff-ff     other VLAN 1
  123.20.10.123 02-10-20-30-40-50    static VLAN 2
   345.30.20.23 09-50-40-30-20-10   dynamic VLAN 3

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 138: 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 inlcuded 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 specifed 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 desginated 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:
  192.168.1.44
  192.168.2.255
Total helper number now is: 2
Console#
```

45 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 139: 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

Global Routing Configuration

Table 140: Global Routing Configuration Commands

Command	Function	Mode
ip route	Configures static routes	GC
maximum-paths	Sets the maximum number of paths allowed	GC
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
show ip traffic	Displays statistics for IP, ICMP, UDP, TCP and ARP protocols	PE

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 and 120 for RIP.
(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 and OSPF updates periodically sent by the router if this feature is enabled by the RIP or OSPF redistribute command (see page 1031 or page 1052, 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 route

This command displays information in the Forwarding Information Base (FIB).

SYNTAX

show ip route [**connected** | **ospf** | **rip** | **static** | **summary**]

connected – Displays all currently connected entries.

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

```
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

C       127.0.0.0/8 is directly connected, lo
C       192.168.0.0/24 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 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 datarams
                     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#
```

ROUTING INFORMATION PROTOCOL (RIP)

Table 141: 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

Table 141: Routing Information Protocol Commands (Continued)

Command	Function	Mode
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 (1029)

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 (1020)
redistribute (1031)

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 (1031)

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* [*acl-name*]

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.

acl-name - Name of the access control list. Any type of ACL can be specified, including standard or extended IP ACLs and MAC ACLs. (Range: 1-16 characters)

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.

- An access list can be used to filter networks according to the IP address of the router supplying the routing information. For example, to filter out unreliable routing information from routers not under your administrative control.

- 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 (1030)

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: 1-4093)

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 (1025)

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: 1-4093)

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 (1029)

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** (**connected** | **ospf** | **static**} [**metric** *metric-value*]

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 (1026)

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 (1035)
ip rip send version (1037)

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 prespecified 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 (1035)

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 (1034)

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 or 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 (1033)

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 (1038)

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 (1033)

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 (1036)

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: 1-4093)

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 142: 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 142: 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

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 (1059)

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 1020.)

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 (1020)
redistribute (1052)

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 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 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 (1043)

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#
```

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 (1056)
area nssa (1054)

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 (1063)

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 (1052)

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 {**connected** | **rip** | **static**} [**metric** *metric-value*] [**metric-type** *type-value*] [**tag** *tag-value*]

no redistribute {**connected** | **rip** | **static**} [**metric**] [**metric-type**] [**tag**]

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 (1045)

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 (1049)
redistribute (1052)

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: 1-16777214: 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 (1048)

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 (1082)

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)#
```

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 (1062)
ip ospf message-digest-key (1065)

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 (1060)

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 (1065)

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 (1060)

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 priority [*ip-address*]

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: 1-4093)

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)#
```

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 incomming 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 143: 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.

Table 143: show ip ospf - display description (Continued)

Field	Description
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.
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 144: 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 os 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 145: 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 146: 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 addres. 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 147: 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 148: 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.
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 149: 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
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: 1-4093)

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 150: 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
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
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 151: 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 152: show ip ospf neighbor - 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 (1057)

show ip protocols ospf

This command displays OSPF process parameters.

SYNTAX

show ip ospf virtual-links

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 153: 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.

Table 153: show ip protocols ospf - display description (Continued)

Field	Description
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).

46 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 154: 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 155: General Multicast Routing Commands

Command	Function	Mode
ip multicast-routing	Enables IP multicast routing	GC
show ip mroute	Shows the IP multicast routing table	PE

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 IP 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 947).

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 IP multicast group address with subscribers directly attached or downstream from this router.

source - The IP 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 156: 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 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#
```

STATIC MULTICAST ROUTING

This section describes commands used to configure static multicast routes on the switch.

Table 157: 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: 1-4093)

interface

ethernet *unit/port*

unit - This is device 1.

port - Port number.

port-channel *channel-id* (Range: 1-32)

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: 1-4093)

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.

PIM Commands

This section describes commands used to configure IP PIM-DM and PIM-SM dynamic multicast routing on the switch.

Table 158: PIM-DM and PIM-SM Multicast Routing Commands

Command	Function	Mode
Common 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
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

Table 158: PIM-DM and PIM-SM Multicast Routing Commands (Continued)

Command	Function	Mode
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

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 can not 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 on the specified interface. Use the **no** form to disable PIM-DM 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#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 (page 1094).

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 (1096)
ip pim propagation-delay (1096)

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 propogation 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 (1096)
ip pim lan-prune-delay (1095)

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 propogation 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 propgated 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 (1096)
ip pim lan-prune-delay (1095)

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 triggerr-hello-delay *seconds*

no ip pim triggerr-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 159: 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.

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)#
```

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 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.

- 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 interface vlan *vlan-id*

vlan-id - VLAN ID (Range: 1-4094)

group-address - An IP multicast group address.

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

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)#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 groups.

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 160: 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 161: 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           : 224.0.1.3
Info source          : 192.168.0.2/32, via (null)
Console#
```

Table 162: 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 1115
- "Troubleshooting" on page 1121
- "License Information" on page 1123

A Software Specifications

Software Features

Management Authentication

Local, RADIUS, TACACS+, Port Authentication (802.1X), HTTPS, SSH, Port Security, IP Filter

General Security Measures

Access Control Lists (36 ACLs per port, 93 rules per port), Port Authentication (802.1X), MAC Authentication, Port Security, DHCP Snooping, IP Source Guard

Port Configuration

1000BASE-T: 10/100 Mbps at half/full duplex, 1000 Mbps at full duplex

1000BASE-SX/LX/LH/LHX/ZX - 1000 Mbps at full duplex (SFP)

Flow Control

Full Duplex: IEEE 802.3-2005

Half Duplex: Back pressure

Storm Control

Broadcast traffic throttled above a critical threshold

Port Mirroring

24 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 4093 groups; port-based, protocol-based, tagged (802.1Q), private VLANs, voice VLANs, IP subnet, MAC-based, GVRP for automatic VLAN learning

CLASS OF SERVICE

Supports eight levels of priority

Strict, Weighted Round Robin, or hybrid queuing

Layer 3/4 priority mapping: IP Port, IP Precedence, IP DSCP

QUALITY OF SERVICE

DiffServ[18] supports class maps, policy maps, and service policies

MULTICAST FILTERING

IGMP Snooping (Layer 2)

IGMP (Layer 3)

IGMP Proxy

Multicast VLAN Registration

IP ROUTING

ARP, Proxy ARP

Static routes

CIDR (Classless Inter-Domain Routing)

RIP, RIPv2, OSPFv2 unicast routing

PIM-SM, PIM-DM multicast routing

VRRP (Virtual Router Redundancy Protocol)

ADDITIONAL FEATURES

BOOTP Client

DHCP Client, Relay, Option 82, Server

DNS Client, Proxy

LLDP (Link Layer Discover Protocol)

RMON (Remote Monitoring, groups 1,2,3,9)

SMTP Email Alerts

SNMP (Simple Network Management Protocol)

SNTP (Simple Network Time Protocol)

[18] 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

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, and
- 10 Gigabit Ethernet (fiber and short-haul copper)
- Link Aggregation Control Protocol (LACP)
- Full-duplex flow control (ISO/IEC 8802-3)

IEEE 802.3ac VLAN tagging

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)
OSPF (RFC 2328, 2178, 1587)
OSPFv3 (RFC 2740)
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)
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)
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
Private MIB
Q-Bridge MIB (RFC 2674Q)
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 163: Troubleshooting Chart

Symptom	Action
Cannot connect using Telnet, web browser, or SNMP software	◆ Be sure the switch is powered up. ◆ Check network cabling between the management station and the switch. ◆ 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. ◆ 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). ◆ Check that the null-modem serial cable 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. Contact your distributor's service engineer.

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

Copyright (C) 1989, 1991 Free Software Foundation, Inc.
59 Temple Place, Suite 330, Boston, MA 02111-1307 USA

Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

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.

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)

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.

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 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 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 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.

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.

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.

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 commands 670
aaa accounting dot1x 671
aaa accounting exec 672
aaa accounting update 673
aaa authorization exec 673
aaa group server 674
absolute 626
access-list arp 765
access-list ip 748
access-list ipv6 754
access-list mac 760
accounting dot1x 675
accounting exec 676
alias 770
area default-cost 1048
area nssa 1054
area range 1049
area stub 1056
area virtual-link 1057
arp 1011
arp timeout 1012
authentication enable 660
authentication login 661
authorization exec 676
auto-cost reference-bandwidth 1050

B

boot system 594
bootfile 984
bridge-ext gvrp 832

C

calendar set 624
capabilities 771
channel-group 788
class 890
class-map 886
clear arp-cache 1014
clear counters 778
clear dns cache 974
clear host 975
clear ip dhcp binding 993
clear ip dhcp snooping database flash 731
clear ip igmp group 943
clear ip ospf process 1048
clear ip pim bsr rp-set 1110
clear ip rip route 1039
clear log 613
clear mac-address-table dynamic 805
clear vrrp interface counters 1000
clear vrrp router counters 1000
client-identifier 985
clock timezone 623
compatible rfc1583 1044
configure 583
copy 595

D

databits 601
default-information originate 1026
default-information originate 1045
default-metric 1026
default-metric 1051
default-router 986
delete 598
delete public-key 689
description 887
description 772
dir 598
disable 584
disconnect 608
distance 1027
dns-server 986
domain-name 987
dot1q-tunnel system-tunnel-control 847
dot1x default 694
dot1x eapol-pass-through 694
dot1x intrusion-action 695
dot1x max-req 696
dot1x operation-mode 697
dot1x port-control 698
dot1x re-authenticate 701
dot1x re-authentication 698
dot1x system-auth-control 695
dot1x timeout quiet-period 699
dot1x timeout re-authperiod 699
dot1x timeout supp-timeout 700
dot1x timeout tx-period 700

E

enable 581
enable password 658
end 585

exec-timeout 602
exit 585

F

flowcontrol 773

G

garp timer 833

H

hardware-address 987
host 988
hostname 588

I

interface vlan 839
ip access-group 752
ip address 1006
ip arp inspection 739
ip arp inspection filter 740
ip arp inspection limit 743
ip arp inspection log-buffer logs 741
ip arp inspection trust 744
ip arp inspection validate 742
ip arp inspection vlan 742
ip default-gateway 1008
ip dhcp excluded-address 983
ip dhcp pool 983
ip dhcp relay server 980
ip dhcp restart client 979
ip dhcp restart relay 981
ip dhcp snooping 725
ip dhcp snooping database flash 727
ip dhcp snooping information option 727
ip dhcp snooping information policy 728
ip dhcp snooping trust 730
ip dhcp snooping verify mac-address 729
ip dhcp snooping vlan 729
ip domain-list 969
ip domain-lookup 970
ip domain-name 971
ip forward-protocol udp 1015
ip helper 1016
ip helper-address 1017
ip host 972
ip http port 678
ip http secure-port 681
ip http secure-server 679
ip http server 679
ip igmp 937
ip igmp filter (Global Configuration) 924
ip igmp filter (Interface Configuration) 926
ip igmp last-member-query-interval 938
ip igmp max-groups 927
ip igmp max-groups action 928
ip igmp max-resp-interval 939
ip igmp profile 925
ip igmp proxy 947
ip igmp proxy unsolicited-report-interval 948
ip igmp query-interval 940
ip igmp robustval 941
ip igmp snooping 905
ip igmp snooping proxy-reporting 906
ip igmp snooping querier 906
ip igmp snooping router-alert-option-check 907
ip igmp snooping router-port-expire-time 908
ip igmp snooping tcn-flood 908
ip igmp snooping tcn-query-solicit 909
ip igmp snooping unregistered-data-flood 910
ip igmp snooping unsolicited-report-interval 911
ip igmp snooping version 911
ip igmp snooping version-exclusive 912
ip igmp snooping vlan general-query-suppression 913
ip igmp snooping vlan immediate-leave 913
ip igmp snooping vlan last-memb-query-count 914
ip igmp snooping vlan last-memb-query-intvl 915
ip igmp snooping vlan mrd 915
ip igmp snooping vlan mrouter 1088
ip igmp snooping vlan mrouter 922
ip igmp snooping vlan proxy-address 916
ip igmp snooping vlan query-interval 917
ip igmp snooping vlan query-resp-intvl 918
ip igmp snooping vlan static 919
ip igmp static-group 941
ip igmp version 943
ip multicast-routing 1085
ip name-server 973
ip ospf authentication 1060
ip ospf authentication-key 1062
ip ospf cost 1063
ip ospf dead-interval 1064
ip ospf hello-interval 1065
ip ospf message-digest-key 1065

ip ospf priority 1066
ip ospf retransmit-interval 1067
ip ospf transmit-delay 1068
ip pim 1092
ip pim bsr-candidate 1101
ip pim dr-priority 1108
ip pim graft-retry-interval 1099
ip pim hello-holdtime 1093
ip pim hello-interval 1094
ip pim join-prune-holdtime 1094
ip pim join-prune-interval 1109
ip pim lan-prune-delay 1095
ip pim max-graft-retries 1100
ip pim override-interval 1096
ip pim propagation-delay 1096
ip pim register-rate-limit 1102
ip pim register-source 1103
ip pim rp-address 1104
ip pim rp-candidate 1105
ip pim spt-threshold 1107
ip pim state-refresh origination-interval 1100
ip pim trigger-hello-delay 1097
ip proxy-arp 1013
ip rip authentication mode 1034
ip rip authentication string 1035
ip rip receive version 1035
ip rip receive-packet 1036
ip rip send version 1037
ip rip send-packet 1038
ip rip split-horizon 1038
ip route 1020
ip source-guard 735
ip source-guard binding 733
ip source-guard max-binding 736
ip ssh authentication-retries 687
ip ssh crypto host-key generate 689
ip ssh crypto zeroize 690
ip ssh save host-key 691
ip ssh server 687
ip ssh server-key size 688
ip ssh timeout 688
ip telnet max-sessions 682
ip telnet port 682
ip telnet server 683
ipv6 access-group 759
ipv6 host 974

J

interface 770
jumbo frame 592

L

lacp 789
lacp admin-key (Ethernet Interface) 790
lacp admin-key (Port Channel) 792
lacp port-priority 791
lacp system-priority 792
lease 989
line 600
lldp 952
lldp admin-status 955
lldp basic-tlv management-ip-address 956
lldp basic-tlv port-description 957
lldp basic-tlv system-capabilities 957
lldp basic-tlv system-description 958
lldp basic-tlv system-name 958
lldp dot1-tlv proto-ident 959
lldp dot1-tlv proto-vid 959
lldp dot1-tlv pvid 960
lldp dot1-tlv vlan-name 960
lldp dot3-tlv link-agg 961
lldp dot3-tlv mac-phy 961
lldp dot3-tlv max-frame 962
lldp holdtime-multiplier 952
lldp notification 962
lldp notification-interval 953
lldp refresh-interval 954
lldp reinit-delay 954
lldp tx-delay 955
logging facility 610
logging history 611
logging host 612
logging on 612
logging sendmail 617
logging sendmail destination-email 618
logging sendmail host 617
logging sendmail level 618
logging sendmail source-email 619
logging trap 613
login 603

M

mac access-group 763
mac-address-table aging-time 803
mac-address-table static 804
mac-authentication intrusion-action 721
mac-authentication max-mac-count 721
mac-authentication reauth-time 713
mac-learning 708
mac-vlan 863
management 705
map ip dscp (Global Configuration) 878
map ip dscp (Interface Configuration) 880
map ip port (Global Configuration) 879
map ip port (Interface Configuration) 881

map ip precedence (Global Configuration) 879
map ip precedence (Interface Configuration) 882
match 888
max-hops 814
maximum-paths 1021
maximum-prefix 1028
media-type 774
mst priority 815
mst vlan 816
mvr 931
mvr immediate-leave 932
mvr type 933
mvr vlan group 934

N
name 816
negotiation 774
neighbor 1029
netbios-name-server 990
netbios-node-type 991
network 1029
network 991
network area 1059
network-access aging 712
network-access dynamic-qos 714
network-access dynamic-vlan 715
network-access guest-vlan 715
network-access link-detection 716
network-access link-detection link-down 717
network-access link-detection link-up 717
network-access link-detection link-up-down 718
network-access mac-filter 712
network-access max-mac-count 718
network-access mode mac-authentication 719
network-access port-mac-filter 720
next-server 992
nlm 644

P
parity 604
passive-interface 1030
passive-interface 1069
password 604
password-thresh 605
periodic 626
permit, deny 925
permit, deny (ARP ACL) 766
permit, deny (Extended IPv4 ACL) 750
permit, deny (Extended IPv6 ACL) 756
permit, deny (MAC ACL) 761
permit, deny (Standard IP ACL) 749
permit, deny (Standard IPv6 ACL) 755
ping 1010
police flow 891
police srtcm-color 893
police trtcm-color 895
policy-map 889
port monitor 797
port security 709
private vlan association 854
private-vlan 853
prompt 579
protocol-vlan protocol-group (Configuring Groups) 858
protocol-vlan protocol-group (Configuring Interfaces) 858

Q
queue cos-map 872
queue mode 873
queue weight 874
quit 582

R
radius-server acct-port 662
radius-server auth-port 663
radius-server host 663
radius-server key 664
radius-server retransmit 665
radius-server timeout 665
range 926
rate-limit 801
redistribute 1031
redistribute 1052
reload (Global Configuration) 580
reload (Privileged Exec) 584
rename 889
revision 817
rmon alarm 650
rmon collection history 652
rmon collection stats 653
rmon event 651
router ospf 1043
router pim 1091
router rip 1025
router-id 1046

S
server 675
service dhcp 984
service-policy 899
set cos 897
set phb 898

show access-group 768
show access-list 768
show accounting 677
show arp 1014
show arp access-list 767
show bridge-ext 835
show cable-diagnostics 784
show calendar 624
show class-map 900
show dns 975
show dns cache 976
show dot1q-tunnel 849
show dot1x 702
show garp timer 835
show gvrp configuration 836
show history 582
show hosts 976
show interfaces counters 778
show interfaces protocol-vlan protocol-group 860
show interfaces status 780
show interfaces switchport 781
show ip access-group 753
show ip access-list 753
show ip arp inspection configuration 744
show ip arp inspection interface 745
show ip arp inspection log 745
show ip arp inspection statistics 746
show ip arp inspection vlan 746
show ip dhcp 994
show ip dhcp binding 993
show ip dhcp snooping 732
show ip dhcp snooping binding 732
show ip helper 1018
show ip igmp filter 928
show ip igmp groups 944
show ip igmp interface 946
show ip igmp profile 929
show ip igmp snooping 919
show ip igmp snooping group 920
show ip igmp snooping mrouter 1089
show ip igmp snooping mrouter 923
show ip igmp throttle interface 929
show ip interface 1009
show ip mroute 1086
show ip ospf 1069
show ip ospf border-routers 1071
show ip ospf database 1072
show ip ospf interface 1078
show ip ospf neighbor 1080
show ip ospf route 1081
show ip ospf virtual-links 1081
show ip pim bsr-router 1110
show ip pim interface 1098
show ip pim neighbor 1098
show ip pim rp mapping 1111
show ip pim rp-hash 1112
show ip protocols ospf 1082
show ip protocols rip 1040
show ip rip 1041
show ip route 1021
show ip route database 1022
show ip source-guard 737
show ip source-guard binding 737
show ip ssh 691
show ip telnet 683
show ip traffic 1023
show ipv6 access-group 759
show ipv6 access-list 758
show lacp 793
show line 609
show lldp config 963
show lldp info local-device 964
show lldp info remote-device 965
show lldp info statistics 966
show log 614
show logging 615
show logging sendmail 619
show loop internal 784
show mac access-group 764
show mac access-list 764
show mac-address-table 805
show mac-address-table aging-time 806
show mac-address-table multicast 921
show mac-vlan 864
show management 706
show map ip dscp 883
show map ip port 883
show map ip precedence 884
show mvr 935
show network-access 722
show network-access mac-address-table 723
show network-access mac-filter 724
show nlm oper-status 646
show policy-map 900
show policy-map interface 901
show port monitor 798
show protocol-vlan protocol-group 859
show public-key 692
show queue cos-map 876
show queue mode 876
show queue weight 877
show radius-server 666
show reload 585
show rmon alarm 654
show rmon event 654
show rmon history 654
show rmon statistics 655
show running-config 588
show snmp 632
show snmp engine-id 641
show snmp group 642
show snmp notify-filter 647
show snmp user 643

show snmp view 644
show sntp 622
show spanning-tree 829
show spanning-tree mst configuration 830
show ssh 693
show startup-config 590
show subnet-vlan 862
show system 590
show tacacs-server 669
show traffic-segmentation 851
show users 591
show version 592
show vlan 845
show vlan private-vlan 856
show voice vlan 870
show vrrp 1000
show vrrp interface 1002
show vrrp interface counters 1003
show vrrp router counters 1004
shutdown 775
silent-time 606
snmp-server 630
snmp-server community 630
snmp-server contact 631
snmp-server enable traps 633
snmp-server engine-id 636
snmp-server group 637
snmp-server host 634
snmp-server location 631
snmp-server notify-filter 645
snmp-server user 639
snmp-server view 640
sntp client 620
sntp poll 621
sntp server 622
spanning-tree 808
spanning-tree bpdu-filter 818
spanning-tree bpdu-guard 818
spanning-tree cost 819
spanning-tree edge-port 820
spanning-tree forward-time 809
spanning-tree hello-time 809
spanning-tree link-type 821
spanning-tree loopback-detection 822
spanning-tree loopback-detection release 827
spanning-tree loopback-detection release-mode 822
spanning-tree loopback-detection trap 823
spanning-tree max-age 810
spanning-tree mode 811
spanning-tree mst configuration 813
spanning-tree mst cost 824
spanning-tree mst port-priority 825
spanning-tree pathcost method 812
spanning-tree port-priority 825
spanning-tree priority 813
spanning-tree protocol-migration 828
spanning-tree root-guard 826
spanning-tree spanning-disabled 827
spanning-tree transmission-limit 814
speed 606
speed-duplex 776
stopbits 607
subnet-vlan 861
summary-address 1053
switchport acceptable-frame-types 839
switchport allowed vlan 840
switchport dot1q-tunnel mode 847
switchport dot1q-tunnel tpid 848
switchport forbidden vlan 834
switchport gvrp 834
switchport ingress-filtering 841
switchport mode 842
switchport mode private-vlan 854
switchport native vlan 843
switchport packet-rate 777
switchport priority default 875
switchport private-vlan host-association 855
switchport private-vlan mapping 856
switchport voice vlan 867
switchport voice vlan priority 868
switchport voice vlan rule 868
switchport voice vlan security 869

T

tacacs-server 667
tacacs-server host 667
tacacs-server key 668
tacacs-server port 668
test cable-diagnostics dsp 782
test loop internal 783
timeout login response 608
time-range 625
timers basic 1032
timers spf 1047
traceroute 1009
traffic-segmentation 850

U

username 659

V

version 1033
vlan 837
vlan database 837
vlan-trunking 843
voice vlan 865
voice vlan aging 866
voice vlan mac-address 866

vrrp authentication 996
vrrp ip 996
vrrp preempt 997
vrrp priority 998
vrrp timers advertise 999

W

whichboot 599

INDEX

NUMERICS

802.1Q tunnel 171, 846
- access 176, 847
- configuration, guidelines 174, 846
- configuration, limitations 174, 847
- description 171
- ethernet type 175, 848
- interface configuration 176, 847–848
- mode selection 176, 847
- status, configuring 175, 847
- TPID 175, 848
- uplink 176, 847

802.1X
- authenticator, configuring 316, 693
- global settings 314, 694–695
- port authentication 313, 693, 695
- port authentication accounting 253, 254, 675

A

AAA
- accounting 802.1X port settings 253, 254, 675
- accounting exec command privileges 254, 672
- accounting exec settings 253, 676
- accounting summary 254, 677
- accounting update 253, 673
- accounting, configuring 253, 669
- authorization & accounting 246, 669
- authorization exec settings 258, 673, 676
- authorization method 258, 676
- authorization settings 258, 673
- authorization summary 259, 677
- RADIUS group settings 253, 674
- TACACS+ group settings 253, 674

acceptable frame type 159, 839

Access Control List *See* ACL

ACL 283, 747
- ARP 287, 298, 765
- binding to a port 300, 752
- IPv4 Extended 287, 289, 747, 750
- IPv4 Standard 287, 288, 747, 749
- IPv6 Extended 287, 293, 754, 756
- IPv6 Standard 287, 292, 754, 755
- MAC 287, 296, 760
- time range 284, 625

Address Resolution Protocol *See* ARP

address table 187, 803
- aging time 190, 803
- aging time, displaying 190, 806
- aging time, setting 190, 803

administrative users, displaying 591

ARP
- ACL 298, 740
- configuration 442, 1011
- description 441
- proxy 442, 1013
- statistics 446, 1023

ARP inspection 301, 738
- ACL filter 304, 740
- additional validation criteria 303, 742
- ARP ACL 305, 765
- enabling globally 303, 739
- enabling per VLAN 305, 742
- trusted ports 306, 744

authentication
- MAC address authentication 262, 711, 719
- MAC, configuring ports 266, 711
- network access 262, 711, 719
- public key 277, 686

B

BOOTP 432, 1006

bootstrap router
- PIM-SM 556, 1101

BPDU 196
- filter 208, 818
- guard 208, 818
- ignoring superior BPDUs 207, 826
- selecting protocol based on message format 208, 828
- shut down port on receipt 208, 818

bridge extension capabilities, displaying 105, 835

broadcast storm, threshold 221, 777

C

cable diagnostics 782

class map
- description 225, 887
- DiffServ 224, 886

CLI
- command modes 572
- showing commands 570

command line interface *See* CLI

committed burst size, QoS policy 231, 232, 233, 891, 893, 895

committed information rate, QoS policy 231, 232, 233, 891, 893, 895

community ports 166, 851

community string 73, 366, 630
community VLANs 166, 853
configuration files, restoring defaults 106, 593
configuration settings
  restoring 76, 108, 110, 593, 595
  saving 76, 108, 593, 595
console port, required connections 68
CoS
  configuring 871
  DSCP mapping 878
  IP port priority 879
  IP precedence 879
  layer 3/4 priorities 878
  queue mapping 872
  queue mode 873
CPU
  status 118
  utilization, showing 118

D

default IPv4 gateway, configuration 1008
default priority, ingress port 875
default settings, system 64
designated router
  PIM 550, 1108
  PIMv6 1108
DHCP 432, 469, 1006
  address pool 473, 983
  client 432, 979, 1006
  dynamic configuration 72
  relay service 470, 980
  relay service, enabling 470, 981
  server 471, 982
DHCP snooping 326, 724
  enabling 329, 725
  global configuration 329, 725
  information option 329, 727
  information option policy 329, 728
  information option, enabling 329, 727
  policy selection 329, 728
  specifying trusted interfaces 331, 730
  verifying MAC addresses 329, 729
  VLAN configuration 330, 729
Differentiated Services *See* DiffServ
DiffServ 223, 885
  binding policy to interface 237, 899
  class map 224, 886, 890
  class map, description 225, 887
  classifying QoS traffic 224, 888
  color aware, srTCM 232, 893
  color aware, trTCM 233, 895
  color blind, srTCM 232, 893
  color blind, trTCM 233, 895
  committed burst size 231, 232, 233, 891, 893, 895
  committed information rate 231, 232, 233, 891, 893, 895
  configuring 223, 885
  conforming traffic, configuring response 231, 891, 893, 895
  description 887
  excess burst size 232, 893
  metering, configuring 227, 228, 229, 891
  peak burst size 234, 895
  peak information rate 233, 895
  policy map 227, 889
  policy map, description 230, 887
  QoS policy 227, 889
  service policy 237, 899
  setting CoS for matching packets 231, 897
  setting PHB for matching packets 231, 898
  single-rate, three-color meter 228, 232, 893
  srTCM metering 228, 232, 893
  traffic between CIR and BE, configuring response 232, 893
  traffic between CIR and PIR, configuring response 233, 895
  trTCM metering 233, 895
  two-rate, three-color meter 229, 895
  violating traffic, configuring response 234, 891, 893, 895
DNS
  default domain name 463, 971
  displaying the cache 468, 976
  domain name list 463, 972
  enabling lookup 463, 970
  name server list 463, 973
  static entries, IPv4 467, 972
  static entries, IPv6 974
Domain Name Service *See* DNS
downloading software 106, 595
DR priority, PIM-SM 552, 1108
DSA encryption 279, 281, 689
DSCP
  enabling 878
  mapping priorities 880
dynamic addresses, clearing 192, 805
dynamic addresses, displaying 191, 805
Dynamic Host Configuration Protocol *See* DHCP
dynamic QoS assignment 263, 267, 714
dynamic VLAN assignment 263, 267, 715

E

ECMP, maximum paths 450, 1021
edge port, STA 207, 210, 820
encryption
  DSA 279, 281, 689
  RSA 279, 281, 689
engine ID 357, 358, 636
event logging 335, 610
excess burst size, QoS policy 232, 893
exec command privileges, accounting 254, 672
exec settings
  accounting 253, 676
  authorization 258, 673, 676

F

FIB, description 1022
firmware
  displaying version 103, 592
  upgrading 106, 595
  version, displaying 103, 592
forwarding information base *See* FIB

G

GARP VLAN Registration Protocol *See* GVRP
gateway, IPv4 default 1008
general security measures 245, 707
GNU license 1123
GVRP
  enabling 163, 832
  global setting 163, 832
  interface configuration 163, 834

H

hardware version, displaying 103, 592
hash mask length, PIM-SM BSR 556, 1101
hello holdtime
  PIM 549, 1093
hello interval
  PIM 549
HTTP, web server 679
HTTPS 272, 274, 679
  configuring 272, 679
  replacing SSL certificate 274, 595
  secure-site certificate 274, 595
  UDP port, configuring 273, 681
HTTPS, secure server 272, 679

I

IEEE 802.1D 195, 811
IEEE 802.1s 195, 811
IEEE 802.1w 195, 811
IEEE 802.1X 313, 693, 695
IGMP
  clearing the cache 943
  enabling per interface 414, 937
  filter profiles, binding to interface 409, 926
  filter profiles, configuration 406, 925
  filter, interface configuration 409, 926–928
  filter, parameters 406
  filtering & throttling 405, 923
  filtering & throttling, enabling 406, 924
  filtering & throttling, interface configuration 409, 926
  filtering & throttling, status 405, 924
  filtering, configuring profile 925, 926
  filtering, creating profile 406, 925
  filtering, group range 407, 926
  filtering, interface settings 926–928
  groups, displaying 398, 418, 920, 921, 944
  interface configuration 414, 937
  interface status, displaying 416, 946
  last member query interval 415, 938
  Layer 2 389, 904
  Layer 3 410, 937
  maximum response time 415, 939
  multicast groups, displaying 418, 944
  proxy 411, 947
  proxy routing 410, 947
  proxy routing, configuring 411, 947
  proxy routing, interface configuration 413, 947–948
  query 389, 391, 906
  query interval 414, 940
  query, enabling 394, 906
  report delay 415, 939
  robustness variable 414, 941
  services, displaying 404, 418, 944
  snooping 389, 904
  snooping & query, parameters 391, 904
  snooping, configuring 391, 904
  snooping, enabling 391, 905
  snooping, immediate leave 401, 913
  static group 416, 941
  static groups, configuring 416, 941
  version 414, 943
IGMP proxy
  configuration steps 412, 947
  enabling 413, 947
  unsolicited report interval 413, 948
IGMP snooping
  configuring 399, 904
  enabling per interface 399, 400, 905
  forwarding entries 404, 920
  immediate leave, status 401, 913
  interface attached to multicast router 396, 923
  last leave 390
  last member query count 402, 914
  last member query interval 402, 915
  proxy query address 403, 916
  proxy query interval 402, 917
  proxy query response interval 402, 918
  proxy reporting 392, 401, 906
  querier timeout 393, 908
  querier, enabling 394, 906
  query suppression 390
  router port expire time 393, 908
  static host interface 390
  static multicast routing 395, 922
  static port assignment 397, 922
  static router interface 390, 922
  static router port, configuring 395, 922
  TCN flood 392, 908
  unregistered data flooding 393, 910
  versioin for interface, setting 402, 911
  version exclusive 393, 912
  version, setting 393, 911
  with proxy reporting 390, 906
immediate leave, IGMP snooping 401, 913

importing user public keys 281, 595
ingress filtering 159, 841
IP address
  BOOTP/DHCP 432, 979
  setting 431, 1005
IP filter, for management access 309, 705
IP port priority
  enabling 879
  mapping priorities 881
IP precedence
  enabling 879
  mapping priorities 882
IP routing 435, 483, 1019
  configuring interfaces 438, 1006
  maximum paths 1021
  unicast protocols 438, 1019
IP source guard
  configuring static entries 323, 733
  setting filter criteria 322, 735
  setting maximum bindings 323, 736
IP statistics 1023
IPv4 address
  BOOTP/DHCP 432, 1006
  dynamic configuration 72
  manual configuration 71
  setting 71, 431, 1006
IPv6 address
  setting 71

J

jumbo frame 104, 592

K

key
  private 275, 684
  public 275, 684
  user public, importing 281, 595
key pair
  host 275, 684
  host, generating 279, 689

L

LACP
  configuration 139, 787
  group attributes, configuring 142, 792
  group members, configuring 140, 789–792
  local parameters 145, 793
  partner parameters 147, 793
  protocol message statistics 144, 793
  protocol parameters 139, 787
last member query count, IGMP snooping 402, 914
last member query interval, IGMP snooping 402, 915
license information, GNU 1123
Link Layer Discovery Protocol *See* LLDP
link type, STA 206, 210, 821
LLDP 340, 951
  device statistics details, displaying 354, 966
  device statistics, displaying 352, 966
  display device information 345, 347, 965
  displaying remote information 347, 965
  interface attributes, configuring 342, 955–962
  local device information, displaying 345, 964
  message attributes 342, 951
  message statistics 352, 966
  remote information, displaying 352, 965
  remote port information, displaying 347, 965
  timing attributes, configuring 340, 952–955
  TLV 340, 343
  TLV, 802.1 343, 959–960
  TLV, 802.3 344, 961–962
  TLV, basic 343, 956–958
  TLV, management address 343, 956
  TLV, port description 343, 957
  TLV, system capabilities 343, 957
  TLV, system description 343, 958
  TLV, system name 343, 958
local engine ID 357, 636
logging
  messages, displaying 337, 614
  syslog traps 338, 613
  to syslog servers 338, 612
log-in, Web interface 82
logon authentication 261, 657
  encryption keys 250, 664, 668
  RADIUS client 249, 662
  RADIUS server 249, 662
  sequence 247, 660, 661
  settings 248, 661
  TACACS+ client 248, 666
  TACACS+ server 248, 666
logon authentication, settings 249, 250, 662, 666
loopback detection, STA 198, 822
loopback test, port 783

M

MAC address authentication 262, 711
  ports, configuring 266, 711, 719
  reauthentication 265, 713
main menu, web interface 84
management access, filtering per address 309, 705
management access, IP filter 309, 704, 705
Management Information Bases (MIBs) 1118
matching class settings, classifying QoS traffic 225, 888
media-type 126, 774
memory
  status 119
  utilization, showing 119
mirror port
  configuring 130, 797
  configuring local traffic 130, 797
MSTP 195, 212, 811
  global settings, configuring 199, 212, 807

global settings, displaying 204, 829
interface settings, configuring 205, 216, 807
interface settings, displaying 217, 829
max hop count 202, 814
path cost 216, 824
region name 202, 816
region revision 202, 817
multicast filtering 387, 903
enabling IGMP snooping 391, 905
enabling IGMP snooping per interface 399, 905
router configuration 395, 922
multicast groups 398, 404, 418, 920, 921, 944
displaying 398, 404, 418, 921, 944
static 397, 398, 919, 920, 921
multicast router discovery 399, 915
multicast router port, displaying 396, 923
multicast routing 541, 1085
description 541
ECMP 450, 1021
ECMP maximum paths 450, 1021
enabling 544
enabling, IPv4 1085
global settings 544
global settings, IPv4 1085
PIM 548
PIM-DM 548, 1090
PIM-SM 548, 554, 1090
reverse path tree 542, 1109
routing table 544
routing table, IPv4 1086
upstream interface 545, 1087
multicast services
configuring 397, 919
displaying 398, 920, 921
multicast static router port 395, 922
configuring 395, 922
Multicast VLAN Registration *See* MVR
multicast, filtering and throttling 405, 924
multicast, static router port 395, 1088
MVR
assigning static multicast groups 427, 931, 934
configuring 422, 930
description 420
interface status, configuring 424, 932–934
interface status, displaying 426, 936
setting interface type 425, 933
setting multicast groups 422, 931
specifying a VLAN 422, 931
static binding 427, 931, 934
static binding, group to port 934
using immediate leave 426, 932

N

network access
authentication 262, 711
dynamic QoS assignment 267, 714
dynamic VLAN assignment 267, 715
guest VLAN 266, 715
port configuration 266, 719
reauthentication 265, 713
secure MAC information 270, 723, 724

O

Open Shortest Path First *See* OSPF
OSPF 502, 1042
ABR/ASBR routing table, displaying 1071
area border router 504, 511, 513, 515, 517, 518, 519, 532, 1049
AS summary route 523, 1053
authentication key 527, 1062
authentication type 527, 1060
auto cost for an interface 508, 1050
autonomous system boundary router 508, 511, 513, 515, 518, 521, 523, 534, 1045
backbone 503, 504, 505, 513, 531, 532, 537, 1060
configuration settings, displaying 510, 530, 1069
cost for interface 526, 1063
default cost for summary route 515, 517, 1048
default external route 509, 1045
default metric for external routes 508, 1051
enabling 1043
general settings 507, 510, 1042
hello interval 526, 1065
interface summary information, displaying 530, 1078
LSA advertisement interval 527, 1067
LSA database, displaying 534, 1072
message digest key 528, 1065
neighboring router information, diplaying 538, 1080
network area 504, 1059
normal area 504, 1059
NSSA 512, 513, 518, 1054
process ID 505, 507, 512, 514, 517, 518, 520, 521, 524, 1043
process parameters, displaying 510, 1082
redistributing external routes 521, 1052
retransmit interval 527, 1067
RFC 1583 compatible 507, 1044
router ID 507, 1046
router priority 526, 1066
routing table, displaying 534, 1081
SPF timers 508, 1047
stub 512, 516, 1056
transit area 504, 505, 514, 516, 531, 532, 537, 1057
transmit delay over interface 527, 1068
virtual link 531, 1057
virtual links, displaying 536, 1081

P

password, line 604

passwords 70, 657
  administrator setting 261, 659
path cost 210, 819
  method 201, 812
  STA 206, 210, 812, 819
peak burst size, QoS policy 233, 895
peak information rate, QoS policy 233, 895
PIM 548
  configuring 548
  dense-mode attributes 551, 1090
  designated router 550, 1108
  enabling for interfaces 548, 549, 1092
  enabling globally 548, 1091
  hello holdtime 549, 1093
  hello interval 549
  interface settings 548, 1092–1109
  neighbor routers, displaying 554, 1098
  sparse-mode attributes 552, 1090
PIM-DM 548, 1090
  configuring 548, 1090
  global configuration 549–551, 554, 1091
  interface settings 551, 1092–1099
  neighbor routers 554, 1098
PIM-SM 548, 554, 1090
  bootstrap router 556, 1101
  BSR candidate 556, 1101
  BSR elected, displaying 561, 1110
  configuring 548, 554, 1090
  DR priority 552, 1108
  global configuration 552, 1091
  hash mask length for BSR 556, 1101
  interface settings 552, 1092–1099
  neighbor routers 1098
  register rate limit for DR 554, 1102
  rendezvous point 557, 1104, 1105
  RP candidate 559, 1105
  RP candidate, advertising 559, 1105
  RP mapping, displaying 563, 1111
  shared tree 555, 1087, 1107
  shortest path tree 555, 1087, 1107
  SPT threshold 555, 1107
  static RP, configuring 557, 1104
PIMv6
  designated router 1108
policing traffic, QoS policy 227, 231, 893, 895
policy map
  description 230, 887
  DiffServ 227, 889
port authentication 313, 693, 695
port priority
  configuring 871
  default ingress 875
  STA 206, 825
port security, configuring 311, 708
ports
  autonegotiation 126, 774
  broadcast storm threshold 221, 777
  capabilities 126, 771
  configuring 125, 769
  duplex mode 127, 776
  flow control 127, 773
  forced selection on combo ports 126, 774
  loopback test 783
  mirroring 130, 797
  mirroring local traffic 130, 797
  speed 127, 776
  statistics 131, 778
primary VLAN 166, 167, 168, 170, 853
priority, default port ingress 875
private key 275, 684
private VLANs, configuring 166, 167, 851
private VLANs, displaying 168, 169, 856
problems, troubleshooting 1121
promiscuous ports 166, 851
protocol migration 208, 828
protocol VLANs 177, 857
  configuring 178, 857
  configuring groups 178, 858
  configuring interfaces 180, 858
  group configuration 178, 858
  interface configuration 180, 858
proxy ARP 442, 1013
proxy query address, IGMP snooping 403, 916
proxy query interval, IGMP snooping 402, 917
proxy query response interval, IGMP snooping 402, 918
proxy reporting, IGMP snooping 401, 906
public key 275, 684
PVID, port native VLAN 159, 843
PVLAN
  association 168, 854
  community ports 166, 851
  configuring 166, 167, 851
  displaying 168, 169, 856
  interface configuration 169, 854, 855
  primary VLAN 167, 168, 170, 853
  promiscuous ports 166, 851

Q

QinQ Tunneling *See* 802.1Q tunnel
QoS 223, 885
  configuration guidelines 224, 886
  configuring 223, 885
  dynamic assignment 267, 714
  matching class settings 225, 888
QoS policy
  committed burst size 231, 232, 233, 891, 893, 895
  excess burst size 232, 893
  peak burst size 233, 895
  policing flow 227, 231, 893, 895
  srTCM 228, 893
  srTCM police meter 232, 893
  trTCM 229, 895
  trTCM police meter 233, 895
QoS policy, committed information rate 231, 232, 233, 891, 893, 895

QoS policy, peak information rate 233, 895
Quality of Service *See* QoS
queue mode, setting 873

R

RADIUS
 logon authentication 249, 662
 settings 249, 662
rate limit
 port 219, 801
 setting 219, 801
register rate limit, PIM-SM 554, 1102
remote engine ID 358, 636
remote logging 338, 613
Remote Monitoriing *See* RMON
rename, DiffServ 889
rendezvous point
 PIM-SM 557, 1104, 1105
restarting the system 120, 580, 584, 585
 at scheduled times 120, 580
RIP 484, 1024
 authentication key 499, 1035
 authentication mode 499, 1034
 clearing routes 1039
 configuration settings, displaying 1041
 configuring 484, 1025–1041
 default external route 486, 1026
 default metric 486, 1026
 description 483
 global settings 485, 1025–1032
 interface protocol settings 496, 1029–1038
 interface, enabling 489, 1029
 neighbor router 492, 501, 1029
 passively monitoring updates 491, 1030
 poison reverse 484, 499, 1038
 process parameters, displaying 1040
 protocol packets, receiving 498, 1036
 protocol packets, sending 498, 1038
 receive version 498, 1035
 redistributing external routing information 493, 1031
 routes, clearing 1039
 routes, displaying 501, 1041
 routing table, clearing 488, 1039
 send version 498, 1037
 specifying interfaces 489, 1029
 split horizon 484, 499, 1038
 timers 487, 1032
 version 485, 1033
RMON 376, 649
 alarm, displaying settings 379, 654
 alarm, setting thresholds 377, 650
 commands 649
 event settings, displaying 381, 654
 response to alarm setting 380, 651
 statistics history, collection 382, 652
 statistics history, displaying 383, 654
 statistics, collection 384, 653
 statistics, displaying 385, 655
root guard 207, 826
router redundancy
 protocols 453, 995
 VRRP 453, 995
Routing Information Protocol *See* RIP
routing nformation base, description 1022
routing table, displaying 449, 1021
RSA encryption 279, 281, 689
RSTP 195, 811
 global settings, configuring 199, 811
 global settings, displaying 204, 829
 interface settings, configuring 205, 818–827
 interface settings, displaying 209, 829
running configuration files, displaying 588

S

secure shell 275, 684
 configuration 275, 684
security, general measures 245, 707
serial port, configuring 115, 600
shared tree
 PIM-SM 555, 1087, 1107
shortest path tree
 PIM-SM 555, 1087, 1107
Simple Mail Transfer Protocol *See* SMTP
Simple Network Management Protocol *See* SNMP
single rate three color meter *See* srTCM
SMTP
 event handling 339, 616
 sending log events 339, 616
SNMP 354, 629
 community string 366, 630
 enabling traps 372, 633
 filtering IP addresses 309, 705
 global settings, configuring 356
 trap manager 372, 634
 users, configuring 368, 370
SNMPv3 636–639
 engine ID 357, 358, 636
 engine identifier, local 357, 636
 engine identifier, remote 358, 636
 groups 363, 637
 local users, configuring 368, 639
 remote users, configuring 370, 639
 user configuration 368, 370, 639
 views 360, 640
SNTP
 setting the system clock 112, 620–622
 specifying servers 113, 622
software
 displaying version 103, 592
 downloading 106, 595
 version, displaying 103, 592
Spanning Tree Protocol *See* STA
specifications, software 1115
SPT threshold, PIM-SM 555, 1107

srTCM
  police meter 232, 893
  QoS policy 228, 893
SSH 275, 684
  authentication retries 278, 687
  configuring 275, 684
  downloading public keys for clients 281, 595
  generating host key pair 279, 689
  server, configuring 278, 687
  timeout 278, 688
SSL, replacing certificate 274
STA 195, 807
  BPDU filter 208, 818
  BPDU shutdown 208, 818
  detecting loopbacks 198, 822
  edge port 207, 210, 820
  forward delay 201, 809
  global settings, configuring 199, 808–814
  global settings, displaying 204, 829
  hello time 201, 809
  interface settings, configuring 205, 818–827
  interface settings, displaying 209, 829
  link type 206, 210, 821
  loopback detection 198, 822
  maximum age 201, 810
  MSTP interface settings, configuring 216, 824, 825
  MSTP path cost 216, 824
  path cost 206, 210, 812, 819
  path cost method 201, 812
  port priority 206, 825
  port/trunk loopback detection 198, 822
  protocol migration 208, 828
  transmission limit 201, 814
standards, IEEE 1117
startup files
  creating 106, 595
  displaying 106, 590, 599
  setting 106, 594
static addresses, setting 189, 804
static routes, configuring 447, 1020
statistics
  ARP 446, 1023
  ICMP 1023
  IP 1023
  TCP 1023
  UDP 1023
statistics, port 131, 778
STP 200, 811
  Also see STA
summary, accounting 254, 677
switch settings
  restoring 108, 593
  saving 108, 593
system clock
  setting 111, 620
  setting manually 111, 624
  setting the time zone 114, 623
  setting with SNTP 112, 620–622
system logs 335, 612
system software, downloading from server 106, 595

T

TACACS+
  logon authentication 248, 666
  settings 250, 666
TCN
  flood 392, 908
  general query solicitation 392, 909
Telnet
  configuring 117, 681
  server, enabling 117, 683
telnet connection, configuring 117, 600
time range, ACL 284, 625
time zone, setting 114, 623
time, setting 111, 620
TPID 175, 848
traffic segmentation 149, 850
  assigning ports 149, 850
  enabling 149, 850
  sessions, assigning ports 150, 850
  sessions, creating 150, 850
trap manager 74, 372, 634
troubleshooting 1121
trTCM
  police meter 233, 895
  QoS policy 229, 895
trunk
  configuration 135, 787
  LACP 139, 787, 789
  static 136, 788
tunneling unknown VLANs, VLAN trunking 151, 843
two rate three color meter *See* trTCM
Type Length Value *See* LLDP TLV

U

UDP helper
  description 478
  enabling 478, 1016
  forward destination 480, 1017
  UDP ports 479, 1015
unicast routing 483, 1019
unregistered data flooding, IGMP snooping 393, 910
upgrading software 106, 595
upstream interface, multicast route 545, 1087
user account 261, 657, 659
user password 261, 658, 659

V

VLAN trunking 151, 843
VLANs 153–184, 831–870
  802.1Q tunnel mode 176, 847
  adding static members 158, 840
  basic information, displaying 835

- configuring port members, by interface 162, 839–843
- configuring port members, VLAN index 161
- creating 156, 837
- description 153
- displaying port members 845
- dynamic assignment 267, 715
- egress mode 159, 842
- interface configuration 158, 839–843
- IP subnet-based 182, 861
- MAC-based 184, 863
- port members, displaying 845
- private 166, 851
- protocol 177, 857
- protocol, configuring 178, 857
- protocol, configuring groups 178, 858
- protocol, configuring interfaces 180, 858
- protocol, group configuration 178, 858
- protocol, interface configuration 180, 858
- PVID 159, 843
- tunneling unknown groups 151, 843
- voice 239, 864

voice VLANs 239, 864
- detecting VoIP devices 240, 865
- enabling for ports 242, 867–869
- identifying client devices 241, 866

VoIP traffic 239, 864
- ports, configuring 242, 867–869
- telephony OUI, configuring 241, 866
- voice VLAN, configuring 239, 864

VoIP, detecting devices 243, 868

VRRP 453, 995
- authentication 457, 996
- configuration settings 453, 454, 995
- group statistics 461, 1000
- preemption 455, 456, 997
- priority 455, 456, 998
- protocol message statistics 460, 1004
- timers 456, 999
- virtual address 454, 996

W

Web interface
- access requirements 81
- configuration buttons 83
- home page 82
- menu list 84
- panel display 83

ECS4610-24F
E052010/ST-R01
149100000092A