iPECS

User Manual

ES-3026 Managed FE Switch
ES-3026P Managed FE PoE Switch
ES-3024G Managed GE Switch
ES-3024GP Managed GE PoE Switch

LG-NORTEL

USER MANUAL

iPECS ES-3000 Series

ES-3026 MANAGED 26-PORT FE SWITCH

Layer 2 Managed Switch
with 24 10/100BASE-TX (RJ-45) Ports,
and 2 Gigabit Combination Ports (RJ-45/SFP)

ES-3026P MANAGED 26-PORT FE POE SWITCH

Layer 2 Managed Switch
with 24 10/100BASE-TX (RJ-45) PoE Ports,
and 2 Gigabit Combination Ports (RJ-45/SFP)

ES-3024G MANAGED 24-PORT GE SWITCH

Layer 2 Managed Switch
with 24 10/100/1000BASE-T (RJ-45) Ports,
and 4 Gigabit Shared Ports (SFP)

ES-3024GP MANAGED 24-PORT GE POE SWITCH

Layer 2 Managed Switch
with 24 10/100/1000BASE-T (RJ-45) PoE Ports,
and 4 Gigabit Shared Ports (SFP)

ES-3026 ES-3026P
ES-3024G ES-3024GP
E122009/ST-R01
149100000038A

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.

December 2009 Revision

This is the first version of this guide. This guide is valid for software release v1.0.0.0.

CONTENTS

ABOUT THIS GUIDE 3
CONTENTS 5
FIGURES 31
TABLES 39

SECTION I GETTING STARTED 45

1 INTRODUCTION 47
Key Features 47
Description of Software Features 48
Configuration Backup and Restore 48
Authentication 48
Access Control Lists 49
Port Configuration 49
Port Mirroring 49
Port Trunking 49
Rate Limiting 49
Storm Control 49
Static Addresses 49
IEEE 802.1D Bridge 50
Store-and-Forward Switching 50
Spanning Tree Algorithm 50
Virtual LANs 51
IEEE 802.1Q Tunneling (QinQ) 51
Traffic Prioritization 51
Quality of Service 52
Multicast Filtering 52
System Defaults 52

2 INITIAL SWITCH CONFIGURATION 55
Connecting to the Switch 55
Configuration Options 55
Required Connections 56
Remote Connections 57
Basic Configuration 58
Console Connection 58
Setting Passwords 58
Setting an IP Address 59
Enabling SNMP Management Access 64
Managing System Files 66
Saving or Restoring Configuration Settings 67

SECTION II WEB CONFIGURATION 69

3 USING THE WEB INTERFACE 71
Connecting to the Web Interface 71
Navigating the Web Browser Interface 72
Home Page 72
Configuration Options 73
Panel Display 73
Main Menu 74
4 BASIC MANAGEMENT TASKS 87
Displaying System Information 87
Displaying Switch Hardware/Software Versions 88
Configuring Support for Jumbo Frames 89
Displaying Bridge Extension Capabilities 90
Managing System Files 92
Copying Files via FTP/TFTP or HTTP 92
Saving the Running Configuration to a Local File 94
Setting The Start-Up File 95
Showing System Files 95
Automatic Operation Code Upgrade 96
Setting the System Clock 100
Setting the Time Manually 100
Configuring SNTP 101

Specifying SNTP Time Servers 102
Setting the Time Zone 103
Console Port Settings 104
Telnet Settings 106
Displaying CPU Utilization 107
Displaying Memory Utilization 108
Resetting the System 109
5 INTERFACE CONFIGURATION 113
Port Configuration 113
Configuring by Port List 113
Configuring by Port Range 115
Displaying Connection Status 116
Configuring Local Port Mirroring 117
Configuring Remote Port Mirroring 119
Showing Port or Trunk Statistics 123
Performing Cable Diagnostics 127
Trunk Configuration 128
Configuring a Static Trunk 129
Configuring a Dynamic Trunk 132
Displaying LACP Port Counters 135
Displaying LACP Settings and Status for the Local Side 137
Displaying LACP Settings and Status for the Remote Side 138
Saving Power 140
Traffic Segmentation 142
Enabling Traffic Segmentation 142
Configuring Uplink and Downlink Ports 143
VLAN Trunking 144
6 VLAN CONFIGURATION 147
IEEE 802.1Q VLANs 147
Configuring VLAN Groups 150
Adding Static Members to VLANs 152
Configuring Dynamic VLAN Registration 157
IEEE 802.1Q Tunneling 160
Enabling QinQ Tunneling on the Switch 164
Adding an Interface to a QinQ Tunnel 165

Protocol VLANs 166
Configuring Protocol VLAN Groups 167
Mapping Protocol Groups to Interfaces 168
Configuring IP Subnet VLANs 171
Configuring MAC-based VLANs 173
Configuring VLAN Mirroring 174
7 ADDRESS TABLE SETTINGS 177
Configuring MAC Address Learning 177
Setting Static Addresses 178
Changing the Aging Time 180
Displaying the Dynamic Address Table 181
Clearing the Dynamic Address Table 182
Configuring MAC Address Mirroring 183
8 SPANNING TREE ALGORITHM 185
Configuring Loopback Detection 187
Configuring Global Settings for STA 189
Displaying Global Settings for STA 194
Configuring Interface Settings for STA 195
Displaying Interface Settings for STA 199
Configuring Multiple Spanning Trees 201
Configuring Interface Settings for MSTP 204
9 RATE LIMIT CONFIGURATION 207
10 STORM CONTROL CONFIGURATION 209
11 CLASS OF SERVICE 211
Layer 2 Queue Settings 211
Setting the Default Priority for Interfaces 211
Selecting the Queue Mode 212
Mapping CoS Values to Egress Queues 215
Layer 3/4 Priority Settings 218
Setting Priority Processing to DSCP or CoS 218
Mapping Ingress DSCP Values to Internal DSCP Values 219
Mapping CoS Priorities to Internal DSCP Values 222
12 QUALITY OF SERVICE 225
Configuring a Class Map 226
Creating QoS Policies 229
Attaching a Policy Map to a Port 239

13 VOIP TRAFFIC CONFIGURATION 241

Configuring VoIP Traffic 241

Configuring Telephony OUI 242

Configuring VoIP Traffic Ports 244

14 SECURITY MEASURES 247

AAA Authorization and Accounting 248

Configuring Local/Remote Logon Authentication **249**

Configuring Remote Logon Authentication Servers 250

Configuring AAA Accounting 255

Configuring AAA Authorization 260

Configuring User Accounts 263

Web Authentication 264

Configuring Global Settings for Web Authentication 265

Configuring Interface Settings for Web Authentication 266

Network Access (MAC Address Authentication) 267

Configuring Global Settings for Network Access 269

Configuring Network Access for Ports 270

Configuring Port Link Detection 272

Configuring a MAC Address Filter 273

Displaying Secure MAC Address Information 275

Configuring HTTPS 277

Configuring Global Settings for HTTPS 277

Replacing the Default Secure-site Certificate 278

Configuring the Secure Shell 280

Configuring the SSH Server 283

Generating the Host Key Pair 284

Importing User Public Keys 286

Access Control Lists 288

Setting A Time Range 289

Showing TCAM Utilizaiton 291

Setting the ACL Name and Type 292

Configuring a Standard IPv4 ACL 294

Configuring an Extended IPv4 ACL 295

Configuring a MAC ACL 297

Configuring an ARP ACL 299

Binding a Port to an Access Control List 301

ARP Inspection 302
Configuring Global Settings for ARP Inspection 303
Configuring VLAN Settings for ARP Inspection 305
Configuring Interface Settings for ARP Inspection 307
Displaying ARP Inspection Statistics 308
Displaying the ARP Inspection Log 309
Filtering IP Addresses for Management Access 310
Configuring Port Security 312
Configuring 802.1X Port Authentication 314
Configuring 802.1X Global Settings 315
Configuring Port Authenticator Settings for 802.1X 317
Configuring Port Supplicant Settings for 802.1X 321
Displaying 802.1X Statistics 323
IP Source Guard 325
Configuring Ports for IP Source Guard 325
Configuring Static Bindings for IP Source Guard 327
Displaying Information for Dynamic IP Source Guard Bindings 329
DHCP Snooping 330
DHCP Snooping Configuration 333
DHCP Snooping VLAN Configuration 334
Configuring Ports for DHCP Snooping 335
Displaying DHCP Snooping Binding Information 336
15 BASIC ADMINISTRATION PROTOCOLS 339
Configuring Event Logging 339
System Log Configuration 339
Remote Log Configuration 342
Sending Simple Mail Transfer Protocol Alerts 343
Link Layer Discovery Protocol 344
Setting LLDP Timing Attributes 345
Configuring LLDP Interface Attributes 347
Displaying LLDP Local Device Information 350
Displaying LLDP Remote Port Information 352
Displaying Device Statistics 354
Power Over Ethernet 356
Displaying the Switch's Overall PoE Power Budget 357
Setting The Port PoE Power Budget 358

Simple Network Management Protocol 360
Configuring Global Settings for SNMP 362
Setting the Local Engine ID 363
Specifying a Remote Engine ID 364
Setting SNMPv3 Views 365
Configuring SNMPv3 Groups 368
Setting Community Access Strings 372
Configuring Local SNMPv3 Users 373
Configuring Remote SNMPv3 Users 375
Specifying Trap Managers 378
Remote Monitoring 383
Configuring RMON Alarms 383
Configuring RMON Events 386
Configuring RMON History Samples 388
Configuring RMON Statistical Samples 391
Switch Clustering 393
Configuring General Settings for Clusters 394
Cluster Member Configuration 395
Managing Cluster Members 397
16 IP CONFIGURATION 399
Using the Ping Function 399
Address Resolution Protocol 400
Setting the ARP Timeout 401
Displaying ARP Entries 402
Setting the Switch's IP Address (IP Version 4) 402
Setting the Switch's IP Address (IP Version 6) 405
Configuring the IPv6 Default Gateway 405
Configuring IPv6 Interface Settings 406
Configuring an IPv6 Address 409
Showing IPv6 Addresses 412
Showing the IPv6 Neighbor Cache 413
Showing IPv6 Statistics 415
Showing the MTU for Responding Destinations 420
17 IP SERVICES 423
Configuring General DNS Service Parameters 423
Configuring a List of Domain Names 424

Configuring a List of Name Servers 426
Configuring Static DNS Host to Address Entries 427
Displaying the DNS Cache 429
18 MULTICAST FILTERING 431
Layer 2 IGMP (Snooping and Query) 432
Configuring IGMP Snooping and Query Parameters 433
Specifying Static Interfaces for a Multicast Router 437
Assigning Interfaces to Multicast Services 439
Setting IGMP Snooping Status per Interface 441
Displaying Multicast Groups Discovered by IGMP Snooping 446
Filtering and Throttling IGMP Groups 447
Enabling IGMP Filtering and Throttling 447
Configuring IGMP Filter Profiles 448
Configuring IGMP Filtering and Throttling for Interfaces 451
Multicast VLAN Registration 452
Configuring Global MVR Settings 454
Configuring MVR Interface Status 455
Assigning Static Multicast Groups to Interfaces 457

SECTION III COMMAND LINE INTERFACE 459

19 USING THE COMMAND LINE INTERFACE 461
Accessing the CLI 461
Console Connection 461
Telnet Connection 462
Entering Commands 463
Keywords and Arguments 463
Minimum Abbreviation 463
Getting Help on Commands 464
Partial Keyword Lookup 465
Negating the Effect of Commands 465
Using Command History 465
Understanding Command Modes 466
Exec Commands 466
Configuration Commands 467
Command Line Processing 469

CLI Command Groups 470

20 GENERAL COMMANDS 473

prompt 473

reload (Global Configuration) 474

enable 475

quit 476

show history 476

configure 477

disable 478

reload (Privileged Exec) 478

show reload 479

end 479

exit 479

21 SYSTEM MANAGEMENT COMMANDS 481

Device Designation 481

hostname 482

System Status 482

show access-list tcam-utilization 482

show memory 483

show process cpu 483

show running-config 484

show startup-config 485

show system 486

show users 486

show version 487

Frame Size 488

jumbo frame 488

File Management 489

boot system 490

copy 491

delete 494

dir 494

whichboot 495

upgrade opcode auto 496

upgrade opcode path 497

Line 499
line 499
databits 500
exec-timeout 501
login 501
parity 502
password 503
password-thresh 504
silent-time 505
speed 505
stopbits 506
timeout login response 506
disconnect 507
show line 508
Event Logging 508
logging facility 509
logging history 510
logging host 511
logging on 511
logging trap 512
clear log 512
show log 513
show logging 514
SMTP Alerts 515
logging sendmail 516
logging sendmail host 516
logging sendmail level 517
logging sendmail destination-email 517
logging sendmail source-email 518
show logging sendmail 518
Time 519
sntp client 519
sntp poll 520
sntp server 521
show sntp 521
clock timezone 522

calendar set 523
show calendar 523
Time Range 524
time-range 524
absolute 525
periodic 525
show time-range 526
Switch Clustering 527
cluster 528
cluster commander 528
cluster ip-pool 529
cluster member 530
rcommand 530
show cluster 531
show cluster members 531
show cluster candidates 532
22 SNMP COMMANDS 533
snmp-server 534
snmp-server community 535
snmp-server contact 535
snmp-server location 536
show snmp 536
snmp-server enable traps 537
snmp-server host 538
snmp-server engine-id 541
snmp-server group 542
snmp-server user 543
snmp-server view 544
show snmp engine-id 545
show snmp group 546
show snmp user 547
show snmp view 548
nlm 548
snmp-server notify-filter 549
show nlm oper-status 550
show snmp notify-filter 551

23 REMOTE MONITORING COMMANDS 553

rmon alarm 554

rmon event 555

rmon collection history 556

rmon collection stats 557

show rmon alarm 558

show rmon event 558

show rmon history 558

show rmon statistics 559

24 AUTHENTICATION COMMANDS 561

User Accounts 561

enable password 562

username 563

Authentication Sequence 564

authentication enable 564

authentication login 565

RADIUS Client 566

radius-server acct-port 566

radius-server auth-port 567

radius-server host 567

radius-server key 568

radius-server retransmit 569

radius-server timeout 569

show radius-server 570

TACACS+ Client 570

tacacs-server 571

tacacs-server host 571

tacacs-server key 572

tacacs-server port 572

show tacacs-server 573

AAA 573

aaa accounting commands 574

aaa accounting dot1x 575

aaa accounting exec 576

aaa accounting update 577

aaa authorization exec 577

aaa group server 578
server 579
accounting dot1x 579
accounting exec 580
authorization exec 580
show accounting 581
Web Server 582
ip http port 582
ip http server 583
ip http secure-server 583
ip http secure-port 585
Telnet Server 585
ip telnet max-sessions 586
ip telnet port 586
ip telnet server 587
show ip telnet 587
Secure Shell 588
ip ssh authentication-retries 591
ip ssh server 591
ip ssh server-key size 592
ip ssh timeout 592
delete public-key 593
ip ssh crypto host-key generate 593
ip ssh crypto zeroize 594
ip ssh save host-key 595
show ip ssh 595
show public-key 596
show ssh 597
802.1X Port Authentication 597
dot1x default 598
dot1x eapol-pass-through 599
dot1x system-auth-control 599
dot1x intrusion-action 600
dot1x max-req 600
dot1x operation-mode 601
dot1x port-control 602

dot1x re-authentication 602
dot1x timeout quiet-period 603
dot1x timeout re-authperiod 603
dot1x timeout supp-timeout 604
dot1x timeout tx-period 604
dot1x re-authenticate 605
dot1x identity profile 606
dot1x max-start 606
dot1x pae supplicant 607
dot1x timeout auth-period 608
dot1x timeout held-period 608
dot1x timeout start-period 609
show dot1x 609
Management IP Filter 612
management 612
show management 613
25 GENERAL SECURITY MEASURES 615
Port Security 616
mac-learning 616
port security 617
Network Access (MAC Address Authentication) 619
network-access aging 620
network-access mac-filter 620
mac-authentication reauth-time 621
network-access dynamic-qos 622
network-access dynamic-vlan 623
network-access guest-vlan 623
network-access link-detection 624
network-access link-detection link-down 625
network-access link-detection link-up 625
network-access link-detection link-up-down 626
network-access max-mac-count 626
network-access mode mac-authentication 627
network-access port-mac-filter 628
mac-authentication intrusion-action 629
mac-authentication max-mac-count 629

show network-access 630
show network-access mac-address-table 631
show network-access mac-filter 632
Web Authentication 632
web-auth login-attempts 633
web-auth quiet-period 634
web-auth session-timeout 634
web-auth system-auth-control 635
web-auth 635
web-auth re-authenticate (Port) 636
web-auth re-authenticate (IP) 636
show web-auth 637
show web-auth interface 637
show web-auth summary 638
DHCP Snooping 638
ip dhcp snooping 639
ip dhcp snooping database flash 641
ip dhcp snooping information option 641
ip dhcp snooping information policy 642
ip dhcp snooping verify mac-address 643
ip dhcp snooping vlan 643
ip dhcp snooping trust 644
clear ip dhcp snooping database flash 645
show ip dhcp snooping 646
show ip dhcp snooping binding 646
IP Source Guard 647
ip source-guard binding 647
ip source-guard 648
show ip source-guard 650
show ip source-guard binding 650
ARP Inspection 651
ip arp inspection 652
ip arp inspection filter 653
ip arp inspection log-buffer logs 654
ip arp inspection validate 655
ip arp inspection vlan 655

ip arp inspection limit 656
ip arp inspection trust 657
show ip arp inspection configuration 658
show ip arp inspection interface 658
show ip arp inspection log 659
show ip arp inspection statistics 659
show ip arp inspection vlan 659

26 ACCESS CONTROL LISTS 661

IPv4 ACLs 661
access-list ip 662
permit, deny (Standard IP ACL) 663
permit, deny (Extended IPv4 ACL) 664
ip access-group 666
show ip access-group 667
show ip access-list 667
MAC ACLs 668
access-list mac 668
permit, deny (MAC ACL) 669
mac access-group 671
show mac access-group 672
show mac access-list 672
ARP ACLs 673
access-list arp 673
permit, deny (ARP ACL) 674
show arp access-list 675
ACL Information 676
show access-group 676
show access-list 676

27 INTERFACE COMMANDS 677

interface 678
alias 678
capabilities 679
description 680
flowcontrol 681
media-type 682
negotiation 682

shutdown 683
speed-duplex 684
switchport packet-rate 685
clear counters 686
show interfaces brief 686
show interfaces counters 687
show interfaces status 688
show interfaces switchport 689
test cable-diagnostics 691
show cable-diagnostics 692
power-save 692
show power-save 693
28 LINK AGGREGATION COMMANDS 695
channel-group 696
lacp 697
lacp admin-key (Ethernet Interface) 698
lacp port-priority 699
lacp system-priority 700
lacp admin-key (Port Channel) 700
show lacp 701
29 POWER OVER ETHERNET COMMANDS 705
power inline compatible 705
power inline 706
power inline maximum allocation 707
power inline priority 708
show power inline status 709
show power mainpower 710
30 PORT MIRRORING COMMANDS 711
Local Port Mirroring Commands 711
port monitor 711
show port monitor 713
RSPAN Mirroring Commands 713
rspan source 715
rspan destination 716
rspan remote vlan 717
no rspan session 718

show rspan 719

31 RATE LIMIT COMMANDS 721

rate-limit 721

32 AUTOMATIC TRAFFIC CONTROL COMMANDS 723

auto-traffic-control apply-timer 726

auto-traffic-control release-timer 726

auto-traffic-control 727

auto-traffic-control action 728

auto-traffic-control alarm-clear-threshold 729

auto-traffic-control alarm-fire-threshold 730

auto-traffic-control control-release 731

auto-traffic-control auto-control-release 731

snmp-server enable port-traps atc broadcast-alarm-clear 732

snmp-server enable port-traps atc broadcast-alarm-fire 732

snmp-server enable port-traps atc broadcast-control-apply 733

snmp-server enable port-traps atc broadcast-control-release 733

snmp-server enable port-traps atc multicast-alarm-clear 734

snmp-server enable port-traps atc multicast-alarm-fire 734

snmp-server enable port-traps atc multicast-control-apply 735

snmp-server enable port-traps atc multicast-control-release 735

show auto-traffic-control 736

show auto-traffic-control interface 736

33 ADDRESS TABLE COMMANDS 737

mac-address-table aging-time 737

mac-address-table static 738

clear mac-address-table dynamic 739

show mac-address-table 739

show mac-address-table aging-time 740

34 SPANNING TREE COMMANDS 741

spanning-tree 742

spanning-tree forward-time 743

spanning-tree hello-time 743

spanning-tree max-age 744

spanning-tree mode 745

spanning-tree pathcost method 746

spanning-tree priority 747

spanning-tree mst configuration 747
spanning-tree transmission-limit 748
max-hops 748
mst priority 749
mst vlan 750
name 750
revision 751
spanning-tree bpdu-filter 752
spanning-tree bpdu-guard 752
spanning-tree cost 753
spanning-tree edge-port 754
spanning-tree link-type 755
spanning-tree loopback-detection 756
spanning-tree loopback-detection release-mode 756
spanning-tree loopback-detection trap 757
spanning-tree mst cost 758
spanning-tree mst port-priority 759
spanning-tree port-priority 759
spanning-tree root-guard 760
spanning-tree spanning-disabled 761
spanning-tree loopback-detection release 761
spanning-tree protocol-migration 762
show spanning-tree 763
show spanning-tree mst configuration 764
35 VLAN COMMANDS 765
GVRP and Bridge Extension Commands 766
bridge-ext gvrp 766
garp timer 767
switchport forbidden vlan 768
switchport gvrp 768
show bridge-ext 769
show garp timer 769
show gvrp configuration 770
Editing VLAN Groups 770
vlan database 771
vlan 771

Configuring VLAN Interfaces 772
interface vlan 773
switchport acceptable-frame-types 774
switchport allowed vlan 774
switchport ingress-filtering 775
switchport mode 776
switchport native vlan 777
vlan-trunking 778
Displaying VLAN Information 779
show vlan 779
Configuring IEEE 802.1Q Tunneling 780
dot1q-tunnel system-tunnel-control 781
switchport dot1q-tunnel mode 782
switchport dot1q-tunnel tpid 783
show dot1q-tunnel 783
Configuring Port-based Traffic Segmentation 784
traffic-segmentation 784
show traffic-segmentation 785
Configuring Protocol-based VLANs 786
protocol-vlan protocol-group (Configuring Groups) 787
protocol-vlan protocol-group (Configuring Interfaces) 787
show protocol-vlan protocol-group 788
show interfaces protocol-vlan protocol-group 789
Configuring IP Subnet VLANs 790
subnet-vlan 790
show subnet-vlan 791
Configuring MAC Based VLANs 792
mac-vlan 792
show mac-vlan 793
Configuring Voice VLANs 793
voice vlan 794
voice vlan aging 795
voice vlan mac-address 795
switchport voice vlan 796
switchport voice vlan priority 797
switchport voice vlan rule 797

switchport voice vlan security 798
show voice vlan 799
36 CLASS OF SERVICE COMMANDS 801
Priority Commands (Layer 2) 801
queue mode 802
queue weight 803
switchport priority default 804
show queue mode 805
show queue weight 805
Priority Commands (Layer 3 and 4) 806
qos map cos-dscp 806
qos map dscp-mutation 808
qos map phb-queue 809
qos map trust-mode 810
show qos map dscp-mutation 811
show qos map phb-queue 811
show qos map cos-dscp 812
show qos map trust-mode 813
37 QUALITY OF SERVICE COMMANDS 815
class-map 816
description 817
match 818
rename 819
policy-map 819
class 820
police flow 821
police srtcm-color 823
police trtcm-color 825
set cos 827
set ip dscp 828
set phb 829
service-policy 830
show class-map 831
show policy-map 831
show policy-map interface 832

38 MULTICAST FILTERING COMMANDS 833

IGMP Snooping 833

ip igmp snooping 834

ip igmp snooping proxy-reporting 835

ip igmp snooping querier 836

ip igmp snooping router-alert-option-check 836

ip igmp snooping router-port-expire-time 837

ip igmp snooping tcn-flood 838

ip igmp snooping tcn-query-solicit 839

ip igmp snooping unregistered-data-flood 839

ip igmp snooping unsolicited-report-interval 840

ip igmp snooping version 841

ip igmp snooping version-exclusive 841

ip igmp snooping vlan general-query-suppression 842

ip igmp snooping vlan immediate-leave 843

ip igmp snooping vlan last-memb-query-count 844

ip igmp snooping vlan last-memb-query-intvl 844

ip igmp snooping vlan mrd 845

ip igmp snooping vlan proxy-address 846

ip igmp snooping vlan proxy-query-interval 847

ip igmp snooping vlan proxy-query-resp-intvl 848

ip igmp snooping vlan static 848

show ip igmp snooping 849

show ip igmp snooping group 850

Static Multicast Routing 851

ip igmp snooping vlan mrouter 851

show ip igmp snooping mrouter 852

IGMP Filtering and Throttling 852

ip igmp filter (Global Configuration) 853

ip igmp profile 854

permit, deny 854

range 855

ip igmp filter (Interface Configuration) 855

ip igmp max-groups 856

ip igmp max-groups action 857

show ip igmp filter 857

show ip igmp profile 858
show ip igmp throttle interface 858
Multicast VLAN Registration 859
mvr 860
mvr immediate-leave 861
mvr type 862
mvr vlan group 863
show mvr 864
39 LLDP COMMANDS 867
lldp 868
lldp holdtime-multiplier 868
lldp notification-interval 869
lldp refresh-interval 870
lldp reinit-delay 870
lldp tx-delay 871
lldp admin-status 871
lldp basic-tlv management-ip-address 872
lldp basic-tlv port-description 873
lldp basic-tlv system-capabilities 873
lldp basic-tlv system-description 874
lldp basic-tlv system-name 874
lldp dot1-tlv proto-ident 875
lldp dot1-tlv proto-vid 875
lldp dot1-tlv pvid 876
lldp dot1-tlv vlan-name 876
lldp dot3-tlv link-agg 877
lldp dot3-tlv mac-phy 877
lldp dot3-tlv max-frame 878
lldp notification 878
show lldp config 879
show lldp info local-device 880
show lldp info remote-device 881
show lldp info statistics 882
40 DOMAIN NAME SERVICE COMMANDS 885
ip domain-list 885
ip domain-lookup 886

ip domain-name 887
ip host 888
ip name-server 889
ipv6 host 890
clear dns cache 890
clear host 891
show dns 891
show dns cache 892
show hosts 892
41 DHCP COMMANDS 895
DHCP Client 895
ip dhcp client class-id 896
ip dhcp restart client 896
ipv6 dhcp restart client vlan 897
show ipv6 dhcp duid 898
show ipv6 dhcp vlan 899
42 IP INTERFACE COMMANDS 901
IPv4 Interface 901
Basic IPv4 Configuration 902
ip address 902
ip default-gateway 903
show ip default-gateway 904
show ip interface 904
traceroute 904
ping 905
ARP Configuration 906
arp timeout 907
clear arp-cache 908
show arp 908
IPv6 Interface 909
ipv6 default-gateway 910
ipv6 address 911
ipv6 address autoconfig 912
ipv6 address eui-64 913
ipv6 address link-local 915
ipv6 enable 916

ipv6 mtu 917
show ipv6 default-gateway 918
show ipv6 interface 919
show ipv6 mtu 920
show ipv6 traffic 921
clear ipv6 traffic 925
ping6 926
ipv6 nd dad attempts 927
ipv6 nd ns-interval 928
ipv6 nd reachable-time 929
clear ipv6 neighbors 930
show ipv6 neighbors 930

SECTION IV APPENDICES 933

A SOFTWARE SPECIFICATIONS 935
Software Features 935
Management Features 936
Standards 937
Management Information Bases 937
B TROUBLESHOOTING 939
Problems Accessing the Management Interface 939
Using System Logs 940
GLOSSARY 941
COMMAND LIST 949
INDEX 955

FIGURES

Figure 1:	Home Page	72
Figure 2:	Front Panel Indicators	73
Figure 3:	System Information	88
Figure 4:	General Switch Information	89
Figure 5:	Configuring Support for Jumbo Frames	90
Figure 6:	Displaying Bridge Extension Configuration	91
Figure 7:	Copy Firmware	93
Figure 8:	Saving the Running Configuration	94
Figure 9:	Setting Start-Up Files	95
Figure 10:	Displaying System Files	96
Figure 11:	Configuring Automatic Code Upgrade	100
Figure 12:	Manually Setting the System Clock	101
Figure 13:	Setting the Polling Interval for SNTP	102
Figure 14:	Specifying SNTP Time Servers	103
Figure 15:	Setting the Time Zone	104
Figure 16:	Console Port Settings	106
Figure 17:	Telnet Connection Settings	107
Figure 18:	Displaying CPU Utilization	108
Figure 19:	Displaying Memory Utilization	109
Figure 20:	Restarting the Switch (Immediately)	111
Figure 21:	Restarting the Switch (In)	111
Figure 22:	Restarting the Switch (At)	111
Figure 23:	Restarting the Switch (Regularly)	112
Figure 24:	Configuring Connections by Port List	115
Figure 25:	Configuring Connections by Port Range	116
Figure 26:	Displaying Port Information	117
Figure 27:	Configuring Local Port Mirroring	118
Figure 28:	Displaying Local Port Mirror Sessions	119
Figure 29:	Configuring Remote Port Mirroring (Source)	122
Figure 30:	Configuring Remote Port Mirroring (Intermediate)	122
Figure 31:	Configuring Remote Port Mirroring (Destination)	123

Figure 32: Showing Port Statistics (Table) 126
Figure 33: Showing Port Statistics (Chart) 126
Figure 34: Performing Cable Tests 128
Figure 35: Creating Static Trunks 130
Figure 36: Adding Static Trunks Members 131
Figure 37: Configuring Connection Parameters for a Static Trunk 131
Figure 38: Showing Information for Static Trunks 131
Figure 39: Configuring the LACP Aggregator Admin Key 134
Figure 40: Enabling LACP on a Port 134
Figure 41: Configuring LACP Parameters on a Port 135
Figure 42: Displaying LACP Port Counters 136
Figure 43: Displaying LACP Port Internal Information 138
Figure 44: Displaying LACP Port Remote Information 139
Figure 45: Enabling Power Savings 141
Figure 46: Enabling Traffic Segmentation 142
Figure 47: Configuring Members for Traffic Segmentation 143
Figure 48: Configuring VLAN Trunking 145
Figure 49: Creating Static VLANs 151
Figure 50: Modifying Settings for Static VLANs 151
Figure 51: Showing Static VLANs 152
Figure 52: Configuring Static Members by VLAN Index 155
Figure 53: Configuring Static VLAN Members by Interface 156
Figure 54: Configuring Static VLAN Members by Interface Range 156
Figure 55: Configuring Global Status of GVRP 158
Figure 56: Configuring GVRP for an Interface 159
Figure 57: Showing Dynamic VLANs Registered on the Switch 159
Figure 58: Showing the Members of a Dynamic VLAN 159
Figure 59: Enabling QinQ Tunneling 165
Figure 60: Adding an Interface to a QinQ Tunnel 166
Figure 61: Configuring Protocol VLANs 168
Figure 62: Displaying Protocol VLANs 168
Figure 63: Assigning Interfaces to Protocol VLANs 170
Figure 64: Showing the Interface to Protocol Group Mapping 170
Figure 65: Configuring IP Subnet VLANs 172
Figure 66: Showing IP Subnet VLANs 172
Figure 67: Configuring MAC-Based VLANs 174

Figure 68: Showing MAC-Based VLANs 174
Figure 69: Configuring VLAN Mirroring 175
Figure 70: Showing the VLANs to Mirror 176
Figure 71: Configuring MAC Address Learning 178
Figure 72: Configuring Static MAC Addresses 179
Figure 73: Displaying Static MAC Addresses 180
Figure 74: Setting the Address Aging Time 181
Figure 75: Displaying the Dynamic MAC Address Table 182
Figure 76: Clearing Entries in the Dynamic MAC Address Table 183
Figure 77: Mirroring Packets Based on the Source MAC Address 184
Figure 78: Showing the Source MAC Addresses to Mirror 184
Figure 79: Configuring Port Loopback Detection 188
Figure 80: Configuring Global Settings for STA (STP) 192
Figure 81: Configuring Global Settings for STA (RSTP) 193
Figure 82: Configuring Global Settings for STA (MSTP) 193
Figure 83: Displaying Global Settings for STA 195
Figure 84: Configuring Interface Settings for STA 198
Figure 85: Displaying Interface Settings for STA 201
Figure 86: Creating an MST Instance 202
Figure 87: Displaying STA Settings for an MST Instance 203
Figure 88: Adding a VLAN to an MST Instance 203
Figure 89: Displaying Members of an MST Instance 204
Figure 90: Configuring MSTP Interface Settings 206
Figure 91: Displaying MSTP Interface Settings 206
Figure 92: Configuring Rate Limits 208
Figure 93: Configuring Broadcast Storm Control 210
Figure 94: Setting the Default Port Priority 212
Figure 95: Setting the Queue Mode (Strict) 214
Figure 96: Setting the Queue Mode (WRR) 214
Figure 97: Setting the Queue Mode (Strict and WRR) 215
Figure 98: Mapping CoS Values to Egress Queues 217
Figure 99: Showing CoS Values to Egress Queues 217
Figure 100: Setting the Trust Mode 219
Figure 101: Configuring DSCP to DSCP Internal Mapping 221
Figure 102: Showing DSCP to DSCP Internal Mapping 221
Figure 103: Configuring CoS to DSCP Internal Mapping 223

Figure 104: Showing CoS to DSCP Internal Mapping 224
Figure 105: Configuring a Class Map 227
Figure 106: Showing Class Maps 228
Figure 107: Adding Rules to a Class Map 228
Figure 108: Showing the Rules for a Class Map 229
Figure 109: Configuring a Policy Map 237
Figure 110: Showing Policy Maps 237
Figure 111: Adding Rules to a Policy Map 238
Figure 112: Showing the Rules for a Policy Map 238
Figure 113: Attaching a Policy Map to a Port 239
Figure 114: Configuring a Voice VLAN 242
Figure 115: Configuring an OUI Telephony List 243
Figure 116: Showing an OUI Telephony List 244
Figure 117: Configuring Port Settings for a Voice VLAN 245
Figure 118: Configuring the Authentication Sequence 250
Figure 119: Configuring Remote Authentication Server (RADIUS) 253
Figure 120: Configuring Remote Authentication Server (TACACS+) 253
Figure 121: Configuring AAA Server Groups 254
Figure 122: Showing AAA Server Groups 255
Figure 123: Configuring Global Settings for AAA Accounting 257
Figure 124: Configuring AAA Accounting Methods 257
Figure 125: Showing AAA Accounting Methods 258
Figure 126: Configuring AAA Accounting Service for 802.1X Service 258
Figure 127: Configuring AAA Accounting Service for Exec Service 259
Figure 128: Displaying a Summary of Applied AAA Accounting Methods 259
Figure 129: Displaying Statistics for AAA Accounting Sessions 259
Figure 130: Configuring AAA Authorization Methods 261
Figure 131: Showing AAA Authorization Methods 261
Figure 132: Configuring AAA Authorization Methods for Exec Service 262
Figure 133: Displaying the Applied AAA Authorization Method 262
Figure 134: Configuring User Accounts 264
Figure 135: Showing User Accounts 264
Figure 136: Configuring Global Settings for Web Authentication 266
Figure 137: Configuring Interface Settings for Web Authentication 267
Figure 138: Configuring Global Settings for Network Access 270
Figure 139: Configuring Interface Settings for Network Access 272

Figure 140: Configuring Link Detection for Network Access 273
Figure 141: Configuring a MAC Address Filter for Network Access 274
Figure 142: Showing the MAC Address Filter Table for Network Access 275
Figure 143: Showing Addresses Authenticated for Network Access 276
Figure 144: Configuring HTTPS 278
Figure 145: Downloading the Secure-Site Certificate 280
Figure 146: Configuring the SSH Server 284
Figure 147: Generating the SSH Host Key Pair 285
Figure 148: Showing the SSH Host Key Pair 286
Figure 149: Copying the SSH User's Public Key 287
Figure 150: Showing the SSH User's Public Key 288
Figure 151: Setting the Name of a Time Range 289
Figure 152: Showing a List of Time Ranges 290
Figure 153: Add a Rule to a Time Range 290
Figure 154: Showing the Rules Configured for a Time Range 291
Figure 155: Showing TCAM Utilization 292
Figure 156: Creating an ACL 293
Figure 157: Showing a List of ACLs 293
Figure 158: Configuring a Standard IPv4 ACL 295
Figure 159: Configuring an Extended IPv4 ACL 297
Figure 160: Configuring a MAC ACL 299
Figure 161: Configuring a ARP ACL 301
Figure 162: Binding a Port to an ACL 302
Figure 163: Configuring Global Settings for ARP Inspection 305
Figure 164: Configuring VLAN Settings for ARP Inspection 306
Figure 165: Configuring Interface Settings for ARP Inspection 308
Figure 166: Displaying Statistics for ARP Inspection 309
Figure 167: Displaying the ARP Inspection Log 310
Figure 168: Creating an IP Address Filter for Management Access 311
Figure 169: Showing IP Addresses Authorized for Management Access 312
Figure 170: Configuring Port Security 314
Figure 171: Configuring Global Settings for 802.1X Port Authentication 316
Figure 172: Configuring Interface Settings for 802.1X Port Authenticator 320
Figure 173: Configuring Interface Settings for 802.1X Port Supplicant 322
Figure 174: Showing Statistics for 802.1X Port Authenticator 324
Figure 175: Showing Statistics for 802.1X Port Supplicant 325

Figure 176: Setting the Filter Type for IP Source Guard 327
Figure 177: Configuring Static Bindings for IP Source Guard 328
Figure 178: Displaying Static Bindings for IP Source Guard 329
Figure 179: Showing the IP Source Guard Binding Table 330
Figure 180: Configuring Global Settings for DHCP Snooping 334
Figure 181: Configuring DHCP Snooping on a VLAN 335
Figure 182: Configuring the Port Mode for DHCP Snooping 336
Figure 183: Displaying the Binding Table for DHCP Snooping 337
Figure 184: Configuring Settings for System Memory Logs 341
Figure 185: Showing Error Messages Looged to System Memory 341
Figure 186: Configuring Settings for Remote Logging of Error Messages 343
Figure 187: Configuring SMTP Alert Messages 344
Figure 188: Configuring LLDP Timing Attributes 346
Figure 189: Configuring LLDP Interface Attributes 349
Figure 190: Displaying Local Device Information for LLDP (General) 352
Figure 191: Displaying Local Device Information for LLDP (Port) 352
Figure 192: Displaying Remote Device Information for LLDP (Port) 354
Figure 193: Displaying Remote Device Information for LLDP (Port Details) 354
Figure 194: Displaying LLDP Device Statistics (General) 356
Figure 195: Displaying LLDP Device Statistics (Port) 356
Figure 196: Showing the Switch's PoE Budget 358
Figure 197: Setting a Port's PoE Budget 360
Figure 198: Configuring Global Settings for SNMP 363
Figure 199: Configuring the Local Engine ID for SNMP 364
Figure 200: Configuring a Remote Engine ID for SNMP 365
Figure 201: Showing Remote Engine IDs for SNMP 365
Figure 202: Creating an SNMP View 366
Figure 203: Showing SNMP Views 367
Figure 204: Adding an OID Subtree to an SNMP View 367
Figure 205: Showing the OID Subtree Configured for SNMP Views 368
Figure 206: Creating an SNMP Group 371
Figure 207: Showing SNMP Groups 371
Figure 208: Setting Community Access Strings 372
Figure 209: Showing Community Access Strings 373
Figure 210: Configuring Local SNMPv3 Users 374
Figure 211: Showing Local SNMPv3 Users 375

Figure 212: Configuring Remote SNMPv3 Users 377
Figure 213: Showing Remote SNMPv3 Users 377
Figure 214: Configuring Trap Managers (SNMPv1) 381
Figure 215: Configuring Trap Managers (SNMPv2c) 381
Figure 216: Configuring Trap Managers (SNMPv3) 382
Figure 217: Showing Trap Managers 382
Figure 218: Configuring an RMON Alarm 385
Figure 219: Showing Configured RMON Alarms 385
Figure 220: Configuring an RMON Event 387
Figure 221: Showing Configured RMON Events 388
Figure 222: Configuring an RMON History Sample 389
Figure 223: Showing Configured RMON History Samples 390
Figure 224: Showing Collected RMON History Samples 390
Figure 225: Configuring an RMON Statistical Sample 392
Figure 226: Showing Configured RMON Statistical Samples 392
Figure 227: Showing Collected RMON Statistical Samples 393
Figure 228: Configuring a Switch Cluster 395
Figure 229: Configuring a Cluster Members 396
Figure 230: Showing Cluster Members 396
Figure 231: Showing Cluster Candidates 397
Figure 232: Managing a Cluster Member 398
Figure 233: Pnging a Network Device 400
Figure 234: Setting the ARP Timeout 402
Figure 235: Displaying ARP Entries 402
Figure 236: Configuring a Static IPv4 Address 404
Figure 237: Configuring a Dynamic IPv4 Address 404
Figure 238: Configuring the IPv6 Default Gateway 406
Figure 239: Configuring General Settings for an IPv6 Interface 409
Figure 240: Configuring an IPv6 Address 411
Figure 241: Showing Configured IPv6 Addresses 413
Figure 242: Showing IPv6 Neighbors 414
Figure 243: Showing IPv6 Statistics (IPv6) 419
Figure 244: Showing IPv6 Statistics (ICMPv6) 419
Figure 245: Showing IPv6 Statistics (UDP) 420
Figure 246: Showing Reported MTU Values 421
Figure 247: Configuring General Settings for DNS 424

Figure 248: Configuring a List of Domain Names for DNS 425
Figure 249: Showing the List of Domain Names for DNS 425
Figure 250: Configuring a List of Name Servers for DNS 426
Figure 251: Showing the List of Name Servers for DNS 427
Figure 252: Configuring Static Entries in the DNS Table 428
Figure 253: Showing Static Entries in the DNS Table 428
Figure 254: Showing Entries in the DNS Cache 429
Figure 255: Configuring General Settings for IGMP Snooping 437
Figure 256: Configuring a Static Interface for a Multicast Router 438
Figure 257: Showing Static Interfaces Attached a Multicast Router 438
Figure 258: Showing Current Interfaces Attached a Multicast Router 439
Figure 259: Assigning an Interface to a Multicast Service 440
Figure 260: Showing Static Interfaces Assigned to a Multicast Service 440
Figure 261: Showing Current Interfaces Assigned to a Multicast Service 441
Figure 262: Configuring IGMP Snooping on an Interface 445
Figure 263: Showing Interface Settings for IGMP Snooping 446
Figure 264: Showing Multicast Groups Learned by IGMP Snooping 447
Figure 265: Enabling IGMP Filtering and Throttling 448
Figure 266: Creating an IGMP Filtering Profile 449
Figure 267: Showing the IGMP Filtering Profiles Created 450
Figure 268: Adding Multicast Groups to an IGMP Filtering Profile 450
Figure 269: Showing the Groups Assigned to an IGMP Filtering Profile 451
Figure 270: Configuring IGMP Filtering and Throttling Interface Settings 452
Figure 271: Configuring Global Settings for MVR 455
Figure 272: Configuring Interface Settings for MVR 457
Figure 273: Assigning Static MVR Groups to a Port 458
Figure 274: Showing the Static MVR Groups Assigned to a Port 458

TABLES

Table 1:	Key Features	47
Table 2:	System Defaults	52
Table 3:	Web Page Configuration Buttons	73
Table 4:	Switch Main Menu	74
Table 5:	Port Statistics	123
Table 6:	LACP Port Counters	135
Table 7:	LACP Internal Configuration Information	137
Table 8:	LACP Internal Configuration Information	138
Table 9:	Recommended STA Path Cost Range	196
Table 10:	Recommended STA Path Costs	196
Table 11:	Default STA Path Costs	196
Table 12:	IEEE 802.1p Egress Queue Priority Mapping	215
Table 13:	CoS Priority Levels	215
Table 14:	Mapping Internal Per-hop Behavior to Hardware Queues	216
Table 15:	Default Mapping of DSCP Values to Internal PHB/Drop Values	220
Table 16:	Default Mapping of CoS/CFI to Internal PHB/Drop Precedence	223
Table 17:	Dynamic QoS Profiles	268
Table 18:	HTTPS System Support	277
Table 19:	ARP Inspection Statistics	308
Table 20:	ARP Inspection Log	309
Table 21:	802.1X Statistics	323
Table 22:	Logging Levels	340
Table 23:	Chassis ID Subtype	350
Table 24:	System Capabilities	350
Table 25:	Port ID Subtype	353
Table 26:	SNMPv3 Security Models and Levels	361
Table 27:	Supported Notification Messages	369
Table 28:	Address Resolution Protocol	401
Table 29:	Show IPv6 Neighbors - display description	413
Table 30:	Show IPv6 Statistics - display description	415
Table 31:	Show MTU - display description	420

Table 32: General Command Modes 466
Table 33: Configuration Command Modes 468
Table 34: Keystroke Commands 469
Table 35: Command Group Index 470
Table 36: General Commands 473
Table 37: System Management Commands 481
Table 38: Device Designation Commands 481
Table 39: System Status Commands 482
Table 40: Frame Size Commands 488
Table 41: Flash/File Commands 489
Table 42: File Directory Information 495
Table 43: Line Commands 499
Table 44: Event Logging Commands 508
Table 45: Logging Levels 510
Table 46: show logging flash/ram - display description 514
Table 47: show logging trap - display description 515
Table 48: Event Logging Commands 515
Table 49: Time Commands 519
Table 50: Time Range Commands 524
Table 51: Switch Cluster Commands 527
Table 52: SNMP Commands 533
Table 53: show snmp engine-id - display description 545
Table 54: show snmp group - display description 547
Table 55: show snmp user - display description 547
Table 56: show snmp view - display description 548
Table 57: RMON Commands 553
Table 58: Authentication Commands 561
Table 59: User Access Commands 561
Table 60: Default Login Settings 563
Table 61: Authentication Sequence Commands 564
Table 62: RADIUS Client Commands 566
Table 63: TACACS+ Client Commands 570
Table 64: AAA Commands 573
Table 65: Web Server Commands 582
Table 66: HTTPS System Support 584
Table 67: Telnet Server Commands 585

Table 68: Secure Shell Commands 588
Table 69: show ssh - display description 597
Table 70: 802.1X Port Authentication Commands 597
Table 71: Management IP Filter Commands 612
Table 72: General Security Commands 615
Table 73: Management IP Filter Commands 616
Table 74: Network Access Commands 619
Table 75: Dynamic QoS Profiles 622
Table 76: Web Authentication 632
Table 77: DHCP Snooping Commands 638
Table 78: IP Source Guard Commands 647
Table 79: ARP Inspection Commands 651
Table 80: Access Control List Commands 661
Table 81: IPv4 ACL Commands 661
Table 82: MAC ACL Commands 668
Table 83: ARP ACL Commands 673
Table 84: ACL Information Commands 676
Table 85: Interface Commands 677
Table 86: show interfaces switchport - display description 690
Table 87: Link Aggregation Commands 695
Table 88: show lacp counters - display description 702
Table 89: show lacp internal - display description 702
Table 90: show lacp neighbors - display description 703
Table 91: show lacp sysid - display description 704
Table 92: PoE Commands 705
Table 93: show power inline status - display description 709
Table 94: show power mainpower - display description 710
Table 95: Port Mirroring Commands 711
Table 96: Mirror Port Commands 711
Table 97: RSPAN Commands 713
Table 98: Rate Limit Commands 721
Table 99: ATC Commands 723
Table 100: Address Table Commands 737
Table 101: Spanning Tree Commands 741
Table 102: Recommended STA Path Cost Range 753
Table 103: Recommended STA Path Cost 753

Table 104: Default STA Path Costs 754
Table 105: VLAN Commands 765
Table 106: GVRP and Bridge Extension Commands 766
Table 107: Commands for Editing VLAN Groups 770
Table 108: Commands for Configuring VLAN Interfaces 772
Table 109: Commands for Displaying VLAN Information 779
Table 110: 802.1Q Tunneling Commands 780
Table 111: Commands for Configuring Traffic Segmentation 784
Table 112: Protocol-based VLAN Commands 786
Table 113: IP Subnet VLAN Commands 790
Table 114: MAC Based VLAN Commands 792
Table 115: Voice VLAN Commands 793
Table 116: Priority Commands 801
Table 117: Priority Commands (Layer 2) 801
Table 118: Priority Commands (Layer 3 and 4) 806
Table 119: Default Mapping of CoS/CFI to Internal PHB/Drop Precedence 807
Table 120: Default Mapping of DSCP Values to Internal PHB/Drop Values 808
Table 121: Mapping Internal Per-hop Behavior to Hardware Queues 809
Table 122: Quality of Service Commands 815
Table 123: Multicast Filtering Commands 833
Table 124: IGMP Snooping Commands 833
Table 125: Static Multicast Interface Commands 851
Table 126: IGMP Filtering and Throttling Commands 852
Table 127: Multicast VLAN Registration Commands 859
Table 128: show mvr - display description 864
Table 129: show mvr interface - display description 865
Table 130: show mvr members - display description 865
Table 131: LLDP Commands 867
Table 132: Address Table Commands 885
Table 133: show dns cache - display description 892
Table 134: show hosts - display description 893
Table 135: DHCP Commands 895
Table 136: DHCP Client Commands 895
Table 137: IP Interface Commands 901
Table 138: IPv4 Interface Commands 901
Table 139: Basic IP Configuration Commands 902

Table 140: Address Resolution Protocol Commands 906
Table 141: IPv6 Configuration Commands 909
Table 142: show ipv6 interface - display description 919
Table 143: show ipv6 mtu - display description 921
Table 144: show ipv6 traffic - display description 922
Table 145: show ipv6 neighbors - display description 931
Table 146: Troubleshooting Chart 939

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 47
- "Initial Switch Configuration" on page 55

1 INTRODUCTION

This switch provides a broad range of features for Layer 2 switching. 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 512 rules, 64 ACLs, and a maximum of 32 rules for an ACL
DHCP	Client
DNS	Client and Proxy service
Port Configuration	Speed and duplex mode and flow control
Port Trunking	Supports up to 12 trunks – static or dynamic trunking (LACP)
Port Mirroring	26 sessions, one or more source ports to one analysis port
Congestion Control	Rate Limiting Throttling for broadcast, multicast, unknown unicast storms Random Early Detection
Address Table	8K MAC addresses in the forwarding table, 1K static MAC addresses, 256 L2 multicast groups
IP Version 4 and 6	Supports IPv4 and IPv6 addressing, and management
IEEE 802.1D Bridge	Supports dynamic data switching and addresses learning
Store-and-Forward Switching	Supported to ensure wire-speed switching while eliminating bad frames

Table 1: Key Features (Continued)

Feature	Description
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)
Qualify of Service	Supports Differentiated Services (DiffServ)
Link Layer Discovery Protocol	Used to discover basic information about neighboring devices
Multicast Filtering	Supports IGMP snooping and query, and Multicast VLAN Registration

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 provides support for real-time network applications.

Some of the management features are briefly described below.

CONFIGURATION BACKUP AND RESTORE

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

AUTHENTICATION

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

Other authentication options include HTTPS for secure management access via the web, SSH for secure management access over a Telnet-equivalent connection, SNMP Version 3, IP address filtering for 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.

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 12 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.

STORM CONTROL

Broadcast, multicast and unknown unicast storm suppression prevents 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 1 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 255 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 four priority queues with strict priority, Weighted Round Robin (WRR) scheduling, or a combination of strict and weighted queuing. It uses IEEE 802.1p and 802.1Q tags to prioritize incoming traffic based on input from the end-station application. These functions can be used to provide independent priorities for delay-sensitive data and best-effort data.

This switch also supports several common methods of prioritizing layer 3/4 traffic to meet application requirements. Traffic can be prioritized based on the priority bits in the IP frame’s Type of Service (ToS) octet using DSCP, or IP Precedence. 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.

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 to manage multicast group registration.

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	Enabled
	HTTP Secure Server Port	443
SNMP	SNMP Agent	Enabled
	Community Strings	“public” (read only) “private” (read/write)
	Traps	Authentication traps: enabled Link-up-down events: enabled
	SNMP V3	View: defaultview Group: public (read only); private (read/write)
Port Configuration	Admin Status	Enabled
	Auto-negotiation	Enabled
	Flow Control	Disabled
Port Trunking	Static Trunks	None
	LACP (all ports)	Disabled
Congestion Control	Rate Limiting	Disabled
	Storm Control	Broadcast: Enabled (500 packets/sec) Multicast: Disabled Unknown Unicast: Disabled
Address Table	Aging Time	300 seconds
Spanning Tree Algorithm	Status	Enabled, RSTP (Defaults: RSTP standard)
	Edge Ports	Disabled
LLDP	Status	Enabled
Virtual LANs	Default VLAN	1
	PVID	1
	Acceptable Frame Type	All
	Ingress Filtering	Disabled
	Switchport Mode (Egress Mode)	Access
	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-WRR
	Queue Weight	Queue: 0 1 2 3 Weight: 1 2 4 Strict
	Class of Service	Enabled
	IP Precedence Priority	Disabled
	IP DSCP Priority	Disabled
IP Settings	Management. VLAN	VLAN 1
	IP Address	192.168.1.10
	Subnet Mask	255.255.255.0
	Default Gateway	0.0.0.0
	DHCP	Client: Disabled Snooping: Disabled
	DNS	Proxy service
	BOOTP	Disabled
Multicast Filtering	IGMP Snooping	Snooping: Disabled Querier: Disabled
System Log	Status	Enabled
	Messages Logged to RAM	Levels 0-7 (all)
	Messages Logged to Flash	Levels 0-3
SMTP Email Alerts	Event Handler	Enabled (but no server defined)
SNTP	Clock Synchronization	Disabled

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 59.

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 a management 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 256 IEEE 802.1Q VLANs
- Enable GVRP automatic VLAN registration
- Configure IGMP multicast filtering
- Upload and download system firmware or configuration files via HTTP (using the web interface) or FTP/TFTP (using the command line or web interface)
- Configure Spanning Tree parameters
- Configure Class of Service (CoS) priority queuing
- Configure static or LACP trunks (up to 12)
- Enable port mirroring
- Set storm control on any port for excessive broadcast, multicast, or unknown unicast traffic
- Display system information and statistics

REQUIRED CONNECTIONS

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

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

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

1. Connect the console cable to the serial port on a terminal, or a PC running terminal emulation software, and tighten the captive retaining screws on the DB-9 connector.
2. Connect the other end of the cable to the RS-232 serial port on the switch.
3. Make sure the terminal emulation software is set as follows:
   - Select the appropriate serial port (COM port 1 or COM port 2).
   - Set the baud rates 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 461. For a list of all the CLI commands and detailed information on using the CLI, refer to "CLI Command Groups" on page 470.

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 59.

NOTE: This switch supports four Telnet sessions or four SSH sessions. Telnet and SSH cannot be used concurrently.

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 “ES-3026#” 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 ES-3026* is opened.
 To end the CLI session, enter [Exit].
```

```
ES-3026#configure
ES-3026(config)#username guest password 0 [password]
ES-3026(config)#username admin password 0 [password]
ES-3026(config)#
```

* This manual covers the ES-3026 and ES-3026P Fast Ethernet switches, and the ES-3024G and ES-3024GP Gigabit Ethernet switches. Other than the difference in port types supported by the Fast Ethernet and Gigabit Ethernet switches, and support for PoE (ES-3026P and ES-3024GP), there are no other significant differences. Therefore nearly all of the screen display examples are based on the ES-3026.

SETTING AN IP ADDRESS

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

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

MANUAL CONFIGURATION

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

NOTE: The default IPv4 address for this switch is set to 192.168.1.10, and the subnet mask to 255.255.255.0.

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>.

```
ES-3026(config)#interface vlan 1
ES-3026(config-if)#ip address 192.168.1.5 255.255.255.0
ES-3026(config-if)#exit
ES-3026(config)#ip default-gateway 192.168.1.254
```

ASSIGNING AN IPV6 ADDRESS

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

An IPv6 prefix or address must be formatted according to RFC 2373 “IPv6 Addressing Architecture,” using 8 colon-separated 16-bit hexadecimal values. One double colon may be used to indicate the appropriate number of zeros required to fill the undefined fields. For detailed information on the other ways to assign IPv6 addresses, see "Setting the Switch’s IP Address (IP Version 6)" on page 405.

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

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

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

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

```
ES-3026(config)#interface vlan 1
ES-3026(config-if)#ipv6 address FE80::260:3EFF:FE11:6700 link-local
ES-3026(config-if)#end
ES-3026#show ipv6 interface
Vlan 1 is up
```

```
IPv6 is enable.
Link-local address:
  FE80::260:3EFF:FE11:6700/64
Global unicast address(es):
Joined group address(es):
  FF01::1/16
  FF02::1/16
  FF02::1:FF11:6700/104
MTU is 1500 bytes.
ND DAD is enabled, number of DAD attempts: 1.
ND retransmit interval is 1000 milliseconds
ES-3026#
```

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

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

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

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

1. From the global configuration mode prompt, type “interface vlan 1” to access the interface-configuration mode. Press <Enter>.
2. From the interface prompt, type “ipv6 address *ipv6-address*” or “ipv6 address *ipv6-address*/*prefix-length*,” where “prefix-length” indicates the address bits used to form the network portion of the address. (The network address starts from the left of the prefix and should encompass some of the ipv6-address bits.) The remaining bits are assigned to the host interface. Press <Enter>.
3. Type “exit” to return to the global configuration mode prompt. Press <Enter>.
4. To set the IP address of the IPv6 default gateway for the network to which the switch belongs, type “ipv6 default-gateway *gateway*,” where “gateway” is the IPv6 address of the default gateway. Press <Enter>.

```
ES-3026(config)#interface vlan 1
ES-3026(config-if)#ipv6 address 2001:DB8:2222:7272::/64
```

```
ES-3026(config-if)#exit
ES-3026(config)#ipv6 default-gateway 2001:DB8:2222:7272::254
ES-3026(config)end
ES-3026#show ipv6 interface
Vlan 1 is up
IPv6 is enable.
  FE80::200:E8FF:FE93:82A0/64
Global unicast address(es):
  2001:DB8:2222:7272::/64, subnet is 2001:DB8:2222:7272::/64
  2005::212:CFFF:FE0B:4600, subnet is ::
Joined group address(es):
FF02::1:2
FF02::1:FF00:0
FF02::1:FF93:82A0
FF02::1
IPv6 link MTU is 1280 bytes
ND DAD is enabled, number of DAD attempts: 2.
ND retransmit interval is 1000 milliseconds
ES-3026#show ipv6 default-gateway
ipv6 default gateway:  2001:DB8:2222:7272::254
ES-3026#
```

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>.

```
ES-3026(config)#interface vlan 1
ES-3026(config-if)#ip address dhcp
ES-3026(config-if)#end
ES-3026#show ip interface
 IP address and netmask: 192.168.1.54 255.255.255.0 on VLAN 1,
 and address mode: DHCP
ES-3026#copy running-config startup-config
Startup configuration file name []: startup
\Write to FLASH Programming.

\Write to FLASH finish.
Success.
```

OBTAINING AN IPV6 ADDRESS

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

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

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

2. Type “ipv6 enable” and press <Enter>.

```
ES-3026(config)#interface vlan 1
ES-3026(config-if)#ipv6 enable
ES-3026(config-if)#end
ES-3026#show ipv6 interface
Vlan 1 is up
IPv6 is enable.
Link-local address:
  FE80::200:E8FF:FE90:0/64
Global unicast address(es):
Joined group address(es):
  FF01::1/16
  FF02::1/16
  FF02::1:FF90:0/104
MTU is 1500 bytes.
ND DAD is enabled, number of DAD attempts: 1.
```

```
ND retransmit interval is 1000 milliseconds
ES-3026#
```

Address for Multi-segment Network — To generate an IPv6 address that can be used in a network containing more than one subnet, the switch can be configured to automatically generate a unique host address based on the local subnet address prefix received in router advertisement messages. (DHCP for IPv6 will also be supported in future software releases.)

To dynamically generate an IPv6 host address for the switch, complete the following steps:

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

2. From the interface prompt, type “ipv6 address autoconfig” and press <Enter>.

```
ES-3026(config)#interface vlan 1
ES-3026(config-if)#ipv6 address autoconfig
ES-3026(config-if)#end
ES-3026#show ipv6 interface
Vlan 1 is up
IPv6 is enable.
Link-local address:
  FE80::212:CFFF:FE0B:4600/64
Global unicast address(es):
  2005::212:CFFF:FE0B:4600, subnet is 2005:0:0:0::/64
  3FFE:501:FFFF:100:212:CFFF:FE0B:4600, subnet is 3FFE:501:FFFF:100::/64
Joined group address(es):
  FF01::1/16
  FF02::1/16
  FF02::1:FF0B:4600/104
MTU is 1500 bytes.
ND DAD is enabled, number of DAD attempts: 1.
ND retransmit interval is 1000 milliseconds
ES-3026#
```

ENABLING SNMP MANAGEMENT ACCESS

The switch can be configured to accept management commands from Simple Network Management Protocol (SNMP) applications. 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 365).

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>.

```
ES-3026(config)#snmp-server community admin rw
ES-3026(config)#snmp-server community private
ES-3026(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 538. The following example creates a trap host for each type of SNMP client.

```
ES-3026(config)#snmp-server host 10.1.19.23 batman
ES-3026(config)#snmp-server host 10.1.19.98 robin version 2c
ES-3026(config)#snmp-server host 10.1.19.34 barbie version 3 auth
ES-3026(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.

```
ES-3026(config)#snmp-server view mib-2 1.3.6.1.2.1 included
ES-3026(config)#snmp-server view 802.1d 1.3.6.1.2.1.17 included
ES-3026(config)#snmp-server group r&d v3 auth mib-2 802.1d
ES-3026(config)#snmp-server user steve group r&d v3 auth md5 greenpeace priv
  des56 einstien
ES-3026(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 360, or refer to the specific CLI commands for SNMP starting on page 533.

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 master unit 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 67 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 92 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>.

```
ES-3026#copy running-config startup-config
Startup configuration file name []: startup
\Write to FLASH Programming.

\Write to FLASH finish.
Success.

ES-3026#
```

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>.

```
ES-3026#copy file startup-config
ES-3026#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.
ES-3026#
```

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 71
- "Basic Management Tasks" on page 87
- "Interface Configuration" on page 113
- "VLAN Configuration" on page 147
- "Address Table Settings" on page 177
- "Spanning Tree Algorithm" on page 185
- "Rate Limit Configuration" on page 207
- "Storm Control Configuration" on page 209
- "Class of Service" on page 211
- "Quality of Service" on page 225
- "VoIP Traffic Configuration" on page 241
- "Security Measures" on page 247
- "Basic Administration Protocols" on page 339
- "IP Configuration" on page 399
- "IP Services" on page 423

◆ "Multicast Filtering" on page 431

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 461.

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 59.)

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 58.)

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 195.

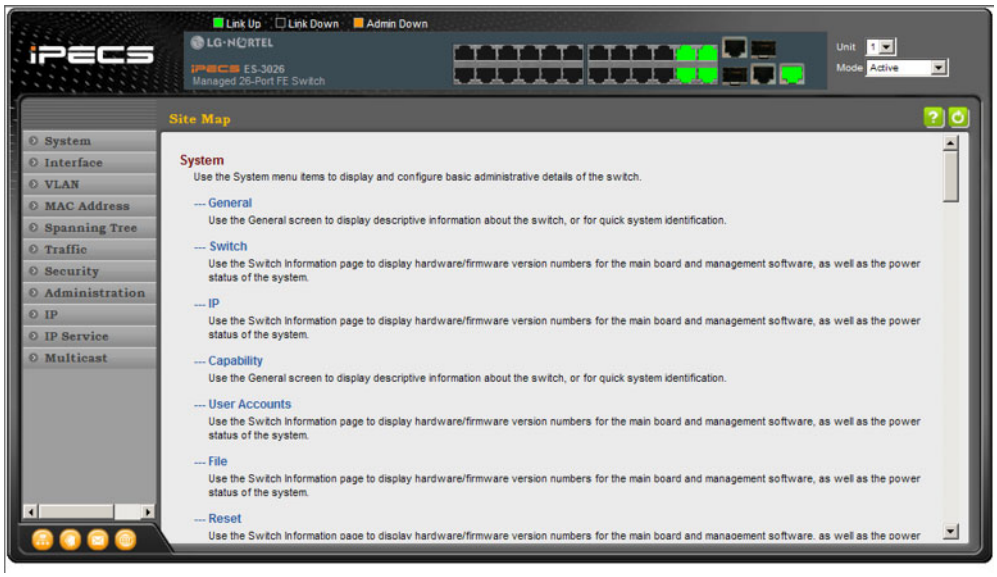
NAVIGATING THE WEB BROWSER INTERFACE

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



NOTE: This manual covers the ES-3026 and ES-3026P Fast Ethernet switches, and the ES-3024G and ES-3024GP Gigabit Ethernet switches. Other than the difference in port types supported by the Fast Ethernet and Gigabit Ethernet switches, and support for PoE (ES-3026P, ES-3024GP), there are no other significant differences. Therefore nearly all of the screen display examples are based on the ES-3026. The panel graphics for all of switch types are shown on the following page.

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."

NOTE: When using Internet Explorer 5.0, you may have to manually refresh the screen after making configuration changes by pressing the browser's refresh button.

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

ES-3026

ES-3026P

ES-3024G

ES-3024GP

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	87
Switch	Shows the number of ports, hardware version, power status, and firmware version numbers	88
IP	Sets the IPv4 address for management access	402
Capability	Enables support for jumbo frames; shows the bridge extension parameters	89, 90
File		92
Copy	Allows the transfer and copying files	92
Set Startup	Sets the startup file	95
Show	Shows the files stored in flash memory; allows deletion of files	95
Automatic Operation Code Upgrade	Automatically upgrades operation code if a newer version is found on the server	96
Time		100
Configure General		
Manual	Manually sets the current time	100
SNTP	Configures SNTP polling interval	101
Configure Time Server	Configures a list of SNTP servers	102
Configure Time Zone	Sets the local time zone for the system clock	103
Console	Sets console port connection parameters	104
Telnet	Sets Telnet connection parameters	106
CPU Utilization	Displays information on CPU utilization	107
Memory Status	Shows memory utilization parameters	108
Reset	Restarts the switch immediately, at a specified time, after a specified delay, or at a periodic interval	109
Interface		113
Port		113
General		
Configure by Port List	Configures connection settings per port	113
Configure by Port Range	Configures connection settings for a range of ports	115
Show Information	Displays port connection status	116
Mirror		117
Show	Shows the configured mirror sessions	117
Add	Sets the source and target ports for mirroring	117
Statistics	Shows Interface, Etherlike, and RMON port statistics	123

Table 4: Switch Main Menu (Continued)

Menu	Description	Page
Chart	Shows Interface, Etherlike, and RMON port statistics	123
Cable Test	Performs cable diagnostics for selected port to diagnose any cable faults (short, open etc.) and report the cable length	127
Trunk		
Static		129
Configure Trunk		129
Add	Creates a trunk, along with the first port member	129
Show	Shows the configured trunk identifiers	129
Add Member	Specifies ports to group into static trunks	129
Show Member	Shows the port members for the selected trunk	129
Configure General		129
Show Information	Displays trunk connection settings	129
Configure	Configures trunk connection settings	129
Dynamic		132
Configure Aggregator	Configures administration key for specific LACP groups	132
Configure Aggregation Port		129
Configure		129
General	Allows ports to dynamically join trunks	132
Actor	Configures parameters for link aggregation group members on the local side	132
Partner	Configures parameters for link aggregation group members on the remote side	132
Show Information		135
Counters	Displays statistics for LACP protocol messages	135
Internal	Displays configuration settings and operational state for the local side of a link aggregation	137
Neighbors	Displays configuration settings and operational state for the remote side of a link aggregation	138
Statistics	Shows Interface, Etherlike, and RMON port statistics	123
Chart	Shows Interface, Etherlike, and RMON port statistics	123
Green Ethernet	Adjusts the power provided to ports based on the length of the cable used to connect to other devices	140
RSPAN	Mirrors traffic from remote switches for analysis at a destination port on the local switch	119
Traffic Segmentation		142
Configure Global	Enables traffic segmentation globally	142
Configure Session	Configures the uplink and down-link ports for a segmented group of ports	143
VLAN Trunking	Allows unknown VLAN groups to pass through the specified interface	144

Table 4: Switch Main Menu (Continued)

Menu	Description	Page
VLAN	Virtual LAN	147
Static		
Add	Creates VLAN groups	150
Show	Displays configured VLAN groups	150
Modify	Configures group name and administrative status	150
Edit Member by VLAN	Specifies VLAN attributes per VLAN	152
Edit Member by Interface	Specifies VLAN attributes per interface	152
Edit Member by Interface Range	Specifies VLAN attributes per interface range	152
Dynamic		
Configure General	Enables GVRP VLAN registration protocol globally	157
Configure Interface	Configures GVRP status and timers per interface	157
Show Dynamic VLAN		157
Show VLAN	Shows the VLANs this switch has joined through GVRP	157
Show VLAN Member	Shows the interfaces assigned to a VLAN through GVRP	157
Tunnel	IEEE 802.1Q (QinQ) Tunneling	160
Configure Global	Sets tunnel mode for the switch	164
Configure Interface	Sets the tunnel mode for any participating interface	165
Protocol		166
Configure Protocol		167
Add	Creates a protocol group, specifying supported protocols	167
Show	Shows configured protocol groups	167
Configure Interface		168
Add	Maps a protocol group to a VLAN	168
Show	Shows the protocol groups mapped to each VLAN	168
IP Subnet		171
Add	Maps IP subnet traffic to a VLAN	171
Show	Shows IP subnet to VLAN mapping	171
MAC-Based		173
Add	Maps traffic with specified source MAC address to a VLAN	173
Show	Shows source MAC address to VLAN mapping	173
Mirror		174
Add	Mirrors traffic from one or more source VLANs to a target port	174
Show	Shows mirror list	174
MAC Address		177
Learning Status	Enables MAC address learning on selected interfaces	177

Table 4: Switch Main Menu (Continued)

Menu	Description	Page
Static		178
Add	Configures static entries in the address table	178
Show	Displays static entries in the address table	178
Dynamic		
Configure Aging	Sets timeout for dynamically learned entries	180
Show Dynamic MAC	Displays dynamic entries in the address table	181
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	182
Mirror	Mirrors traffic matching a specified source address from any port on the switch to a target port	183
Spanning Tree		185
Loopback Detection	Configures Loopback Detection parameters	187
STA	Spanning Tree Algorithm	
Configure Global		
Configure	Configures global bridge settings for STP, RSTP and MSTP	189
Show Information	Displays STA values used for the bridge	194
Configure Interface		
Configure	Configures interface settings for STA	195
Show Inform at on	Displays interface settings for STA	199
MSTP	Multiple Spanning Tree Algorithm	201
Configure Global		201
Add	Configures initial VLAN and priority for an MST instance	201
Show	Configures global settings for an MST instance	201
Add Member	Adds VLAN members for an MST instance	201
Show Member	Adds or deletes VLAN members for an MST instance	201
Configure Interface		204
Configure	Configures interface settings for an MST instance	204
Show Inform at on	Displays interface settings for an MST instance	204
Traffic		
Rate Limit	Sets the input and output rate limits for a port	207
Storm Control	Sets the broadcast storm threshold for each interface	209
Priority		
Default Priority	Sets the default priority for each port or trunk	211
Queue	Sets queue mode for the switch; sets the service weight for each queue that will use a weighted or hybrid mode	212
Trust Mode	Selects IP Precedence, DSCP or CoS priority processing	218

Table 4: Switch Main Menu (Continued)

Menu	Description	Page
DSCP to DSCP		219
Add	Maps DSCP values in incoming packets to per-hop behavior and drop precedence values for internal priority processing	219
Show	Shows the DSCP to DSCP mapping list	219
CoS to DSCP		222
Add	Maps CoS/CFI values in incoming packets to per-hop behavior and drop precedence values for priority processing	222
Show	Shows the CoS to DSCP mapping list	222
PHB to Queue		215
Add	Maps internal per-hop behavior values to hardware queues	215
Show	Shows the PHB to Queue mapping list	215
DiffServ		225
Configure Class		226
Add	Creates a class map for a type of traffic	226
Show	Shows configured class maps	226
Modify	Modifies the name of a class map	226
Add Rule	Configures the criteria used to classify ingress traffic	226
Show Rule	Shows the traffic classification rules for a class map	226
Configure Policy		229
Add	Creates a policy map to apply to multiple interfaces	229
Show	Shows configured policy maps	229
Modify	Modifies the name of a policy map	229
Add Rule	Sets the boundary parameters used for monitoring inbound traffic, and the action to take for conforming and non-conforming traffic	229
Show Rule	Shows the rules used to enforce bandwidth policing for a policy map	229
Configure Interface	Applies a policy map to an ingress port	239
VoIP	Voice over IP	241
Configure Global	Configures auto-detection of VoIP traffic, sets the Voice VLAN, and VLAN aging time	241
Configure OUI		242
Add	Maps the OUI in the source MAC address of ingress packets to the VoIP device manufacturer	242
Show	Shows the OUI telephony list	242
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	244
Security		247
AAA	Authentication, Authorization and Accounting	248
System Authentication	Configures authentication sequence – local, RADIUS, and TACACS	249

Table 4: Switch Main Menu (Continued)

Menu	Description	Page
Server		250
Configure Server	Configures RADIUS and TACACS server message exchange settings	250
Configure Group		250
Add	Specifies a group of authentication servers and sets the priority sequence	250
Show	Shows the authentication server groups and priority sequence	250
Accounting	Enables accounting of requested services for billing or security purposes	255
Configure Global	Specifies the interval at which the local accounting service updates information to the accounting server	255
Configure Method		255
Add	Configures accounting for various service types	255
Show	Shows the accounting settings used for various service types	255
Configure Service	Sets the accounting method applied to specific interfaces for 802.1X, CLI command privilege levels for the console port, and for Telnet	255
Show Information		255
Summary	Shows the configured accounting methods, and the methods applied to specific interfaces	255
Statistics	Shows basic accounting information recorded for user sessions	255
Authorization	Enables authorization of requested services	260
Configure Method		260
Add	Configures authorization for various service types	260
Show	Shows the authorization settings used for various service types	260
Configure Service	Sets the authorization method applied used for the console port, and for Telnet	260
Show Information	Shows the configured authorization methods, and the methods applied to specific interfaces	260
User Accounts		263
Add	Configures user names, passwords, and access levels	263
Show	Shows authorized users	263
Modify	Modifies user attributes	263
Web Authentication	Allows authentication and access to the network when 802.1X or Network Access authentication are infeasible or impractical	264
Configure Global	Configures general protocol settings	265
Configure Interface	Enables Web Authentication for individual ports	266
Network Access	MAC address-based network access authentication	267
Configure Global	Enables aging for authenticated MAC addresses, and sets the time period after which a connected MAC address must be reauthenticated	269

Table 4: Switch Main Menu (Continued)

Menu	Description	Page
Configure Interface		270
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	270
Link Detection	Configures detection of changes in link status, and the response (i.e., send trap or shut down port)	272
Configure MAC Filter		273
Add	Specifies MAC addresses exempt from authentication	273
Show	Shows the list of exempt MAC addresses	273
Show Information	Shows the authenticated MAC address list	275
HTTPS	Secure HTTP	277
Configure Global	Enables HTTPs, and specifies the UDP port to use	277
Copy Certificate	Replaces the default secure-site certificate	278
SSH	Secure Shell	280
Configure Global	Configures SSH server settings	283
Configure Host Key		284
Generate	Generates the host key pair (public and private)	284
Clear	Displays RSA and DSA host keys; deletes host keys	284
Configure User Key		286
Copy	Imports user public keys from TFTP server	286
Show	Displays RSA and DSA user keys; deletes user keys	286
ACL	Access Control Lists	288
Configure Time Range	Configures the time to apply an ACL	289
Add	Specifies the name of a time range	289
Show	Shows the name of configured time ranges	289
Add Rule		289
Absolute	Sets exact time or time range	289
Periodic	Sets a recurrent time	289
Show Rule	Shows the time specified by a rule	289
Configure ACL		292
Show TCAM	Shows utilization parameters for TCAM	291
Add	Adds an ACL based on IP or MAC address filtering	292
Show	Shows the name and type of configured ACLs	292
Add Rule	Configures packet filtering based on IP or MAC addresses and other packet attributes	292
Show Rule	Shows the rules specified for an ACL	292
Configure Interface	Binds a port to the specified ACL and time range	301

Table 4: Switch Main Menu (Continued)

Menu	Description	Page
ARP Inspection		302
Configure General	Enables inspection globally, configures validation of additional address components, and sets the log rate for packet inspection	303
Configure VLAN	Enables ARP inspection on specified VLANs	305
Configure Interface	Sets the trust mode for ports, and sets the rate limit for packet inspection	307
Show Information		
Show Statistics	Displays statistics on the inspection process	308
Show Log	Shows the inspection log list	309
IP Filter		310
Add	Sets IP addresses of clients allowed management access via the web, SNMP, and Telnet	310
Show	Shows the addresses to be allowed management access	310
Port Security	Configures per port security, including status, response for security breach, and maximum allowed MAC addresses	312
Port Authentication	IEEE 802.1X	314
Configure Global	Enables authentication and EAPOL pass-through	315
Configure Interface	Sets authentication parameters for individual ports	317
Show Statistics	Displays protocol statistics for the selected port	323
IP Source Guard	Filters IP traffic based on static entries in the IP Source Guard table, or dynamic entries in the DHCP Snooping table	325
Port Configuration	Enables IP source guard and selects filter type per port	325
Static Binding		327
Add	Adds a static addresses to the source-guard binding table	327
Show	Shows static addresses in the source-guard binding table	327
Dynamic Binding	Displays the source-guard binding table for a selected interface	329
Administration		339
Log		339
System		339
Configure Global	Stores error messages in local memory	339
Show System Logs	Shows logged error messages	339
Remote	Configures the logging of messages to a remote logging process	342
SMTP	Sends an SMTP client message to a participating server	343
LLDP		344
Configure Global	Configures global LLDP timing parameters	345
Configure Interface	Sets the message transmission mode; enables SNMP notification; and sets the LLDP attributes to advertise	347
Show Local Device Information		350
General	Displays general information about the local device	350

Table 4: Switch Main Menu (Continued)

Menu	Description	Page
Port/Trunk	Displays information about each interface	350
Show Remote Device Information		352
Port/Trunk	Displays information about a remote device connected to a port on this switch	352
Port/Trunk Details	Displays detailed information about a remote device connected to this switch	352
Show Device Statistics		354
General	Displays statistics for all connected remote devices	354
Port/Trunk	Displays statistics for remote devices on a selected port or trunk	354
PoE	Power over Ethernet	356
Configure Global	Displays the power budget for the switch	357
Configure Interface	Configures port power parameters	358
SNMP	Simple Network Management Protocol	360
Configure Global	Enables SNMP agent status, and sets related trap functions	362
Configure Engine		363
Set Engine ID	Sets the SNMP v3 engine ID on this switch	363
Add Remote Engine	Sets the SNMP v3 engine ID for a remote device	364
Show Remote Engine	Shows configured engine ID for remote devices	364
Configure View		365
Add View	Adds an SNMP v3 view of the OID MIB	365
Show View	Shows configured SNMP v3 views	365
Add OID Subtree	Specifies a part of the subtree for the selected view	365
Show OID Subtree	Shows the subtrees assigned to each view	365
Configure Group		368
Add	Adds a group with access policies for assigned users	368
Show	Shows configured groups and access policies	368
Configure User		
Add Community	Configures community strings and access mode	372
Show Community	Shows community strings and access mode	372
Add SNMPv3 Local User	Configures SNMPv3 users on this switch	373
Show SNMPv3 Local User	Shows SNMPv3 users configured on this switch	373
Change SNMPv3 Local User Group	Assign a local user to a new group	373
Add SNMPv3 Remote User	Configures SNMPv3 users from a remote device	375
Show SNMPv3 Remote User	Shows SNMPv3 users set from a remote device	373
Configure Trap		378
Add	Configures trap managers to receive messages on key events that occur this switch	378
Show	Shows configured trap managers	378

Table 4: Switch Main Menu (Continued)

Menu	Description	Page
RMON	Remote Monitoring	383
Configure Global		
Add		
Alarm	Sets threshold bounds for a monitored variable	383
Event	Creates a response event for an alarm	386
Show		
Alarm	Shows all configured alarms	383
Event	Shows all configured events	386
Configure Interface		
Add		
History	Periodically samples statistics on a physical interface	388
Statistics	Enables collection of statistics on a physical interface	391
Show		
History	Shows sampling parameters for each entry in the history group	388
Statistics	Shows sampling parameters for each entry in the statistics group	391
Show Details		
History	Shows sampled data for each entry in the history group	388
Statistics	Shows sampled data for each entry in the history group	391
Cluster		393
Configure Global	Globally enables clustering for the switch; sets Commander status	394
Configure Member	Adds switch Members to the cluster	395
Show Member	Shows cluster switch member; managed switch members	397
IP		399
General		
Ping	Sends ICMP echo request packets to another node on the network	399
ARP	Address Resolution Protocol	400
Configure General	Sets the aging time for dynamic entries in the ARP cache	401
Show Information	Shows entries in the Address Resolution Protocol (ARP) cache	402
IPv6 Configuration		405
Configure Global	Sets an IPv6 default gateway for traffic with no known next hop	405
Configure Interface	Configures IPv6 interface address using auto-configuration or link-local address, and sets related protocol settings	406
Add IPv6 Address	Adds an global unicast, EUI-64, or link-local IPv6 address to an interface	409
Show IPv6 Address	Show the IPv6 addresses assigned to an interface	412
Show IPv6 Neighbor Cache	Displays information in the IPv6 neighbor discovery cache	413
Show Statistics		415

Table 4: Switch Main Menu (Continued)

Menu	Description	Page
IPv6	Shows statistics about IPv6 traffic	415
ICMPv6	Shows statistics about ICMPv6 messages	415
UDP	Shows statistics about UDP messages	415
Show MTU	Shows the maximum transmission unit (MTU) cache for destinations that have returned an ICMP packet-too-big message along with an acceptable MTU to this switch	420
IP Service		423
DNS	Domain Name Service	
General		423
Configure Global	Enables DNS lookup; defines the default domain name appended to incomplete host names	423
Add Domain Name	Defines a list of domain names that can be appended to incomplete host names	424
Show Domain Names	Shows the configured domain name list	424
Add Name Server	Specifies IP address of name servers for dynamic lookup	426
Show Name Servers	Shows the name server address list	426
Static Host Table		427
Add	Configures static entries for domain name to address mapping	427
Show	Shows the list of static mapping entries	427
Modify	Modifies the static address mapped to the selected host name	427
Cache	Displays cache entries discovered by designated name servers	429
DHCP	Dynamic Host Configuration Protocol	
Snooping		330
Configure Global	Enables DHCP snooping globally, MAC-address verification, information option; and sets the information policy	333
Configure VLAN	Enables DHCP snooping on a VLAN	334
Configure Interface	Sets the trust mode for an interface	335
Show Information	Displays the DHCP Snooping binding information	336
Multicast		431
IGMP Snooping		432
General	Enables multicast filtering; configures parameters for multicast snooping	433
Multicast Router		437
Add Static Multicast Router	Assigns ports that are attached to a neighboring multicast router	437
Show Static Multicast Router	Displays ports statically configured as attached to a neighboring multicast router	437
Show Current Multicast Router	Displays ports attached to a neighboring multicast router, either through static or dynamic configuration	437
IGMP Member		439
Add Static Member	Statically assigns multicast addresses to the selected VLAN	439

Table 4: Switch Main Menu (Continued)

Menu	Description	Page
Show Static Member	Shows multicast addresses statically configured on the selected VLAN	439
Show Current Member	Shows multicast addresses associated with the selected VLAN, either through static or dynamic configuration	439
Interface		441
Configure	Configures IGMP snooping per VLAN interface	441
Show	Shows IGMP snooping settings per VLAN interface	441
Forwarding Entry	Displays the current multicast groups learned through IGMP Snooping	446
Filter		447
Configure General	Enables IGMP filtering for the switch	447
Configure Profile		448
Add	Adds IGMP filter profile; and sets access mode	448
Show	Shows configured IGMP filter profiles	448
Add Multicast Group Range	Assigns multicast groups to selected profile	448
Show Multicast Group Range	Shows multicast groups assigned to a profile	448
Configure Interface	Assigns IGMP filter profiles to port interfaces and sets throttling action	451
MVR	Multicast VLAN Registration	452
Configure General	Globally enables MVR, sets the MVR VLAN, adds multicast stream addresses	454
Configure Interface	Configures MVR interface type and immediate leave mode; also displays MVR operational and active status	455
Configure Static Group Member		457
Add	Statically assigns MVR multicast streams to an interface	457
Show	Shows MVR multicast streams assigned to an interface	457

4 BASIC MANAGEMENT TASKS

This chapter describes the basic functions required to set up management access to the switch, display or upgrade operating software, or reset the system.

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 481
- "SNMP Commands" on page 533

PARAMETERS

These parameters are displayed in the web interface:

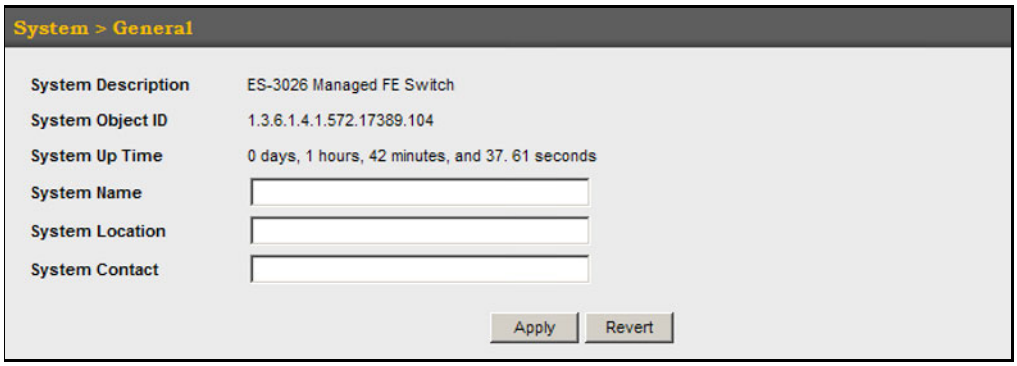
- **System Description** – Brief description of device type.
- **System Object ID** – MIB II object ID for switch's network management subsystem.
- **System Up Time** – Length of time the management agent has been up.
- **System Name** – Name assigned to the switch system.
- **System Location** – Specifies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

WEB INTERFACE

To configure general system information in the web interface:

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

Figure 3: System Information



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 481

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.

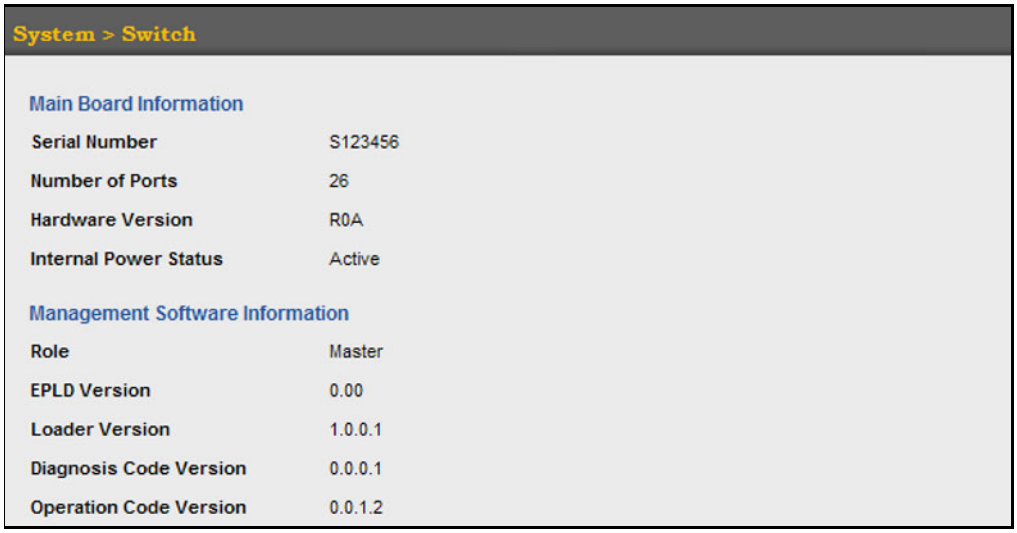
Management Software Information

- **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 in the web interface, Click System, then Switch.

Figure 4: General Switch Information



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 481

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:

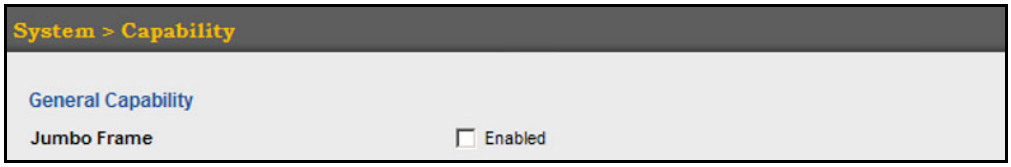
- **Jumbo Frame** – Configures support for jumbo frames. (Default: Disabled)

WEB INTERFACE

To configure support for jumbo frames in the web interface:

1. Click System, then Capability.
2. Enable or disable support for jumbo frames.
3. Click Apply.

Figure 5: Configuring Support for Jumbo Frames



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 766

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 211.)
- **Static Entry Individual Port** – This switch allows static filtering for unicast and multicast addresses. (Refer to "Setting Static Addresses" on page 178.)
- **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 147.)

- **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.

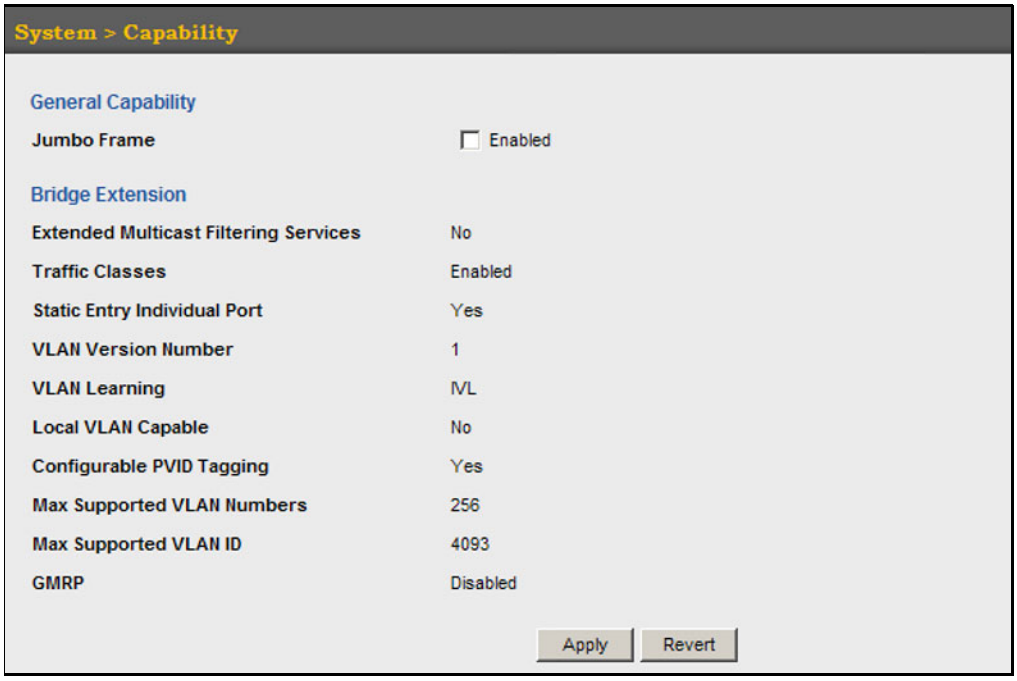
- **GMRP** – GARP Multicast Registration Protocol (GMRP) allows network devices to register end stations with multicast groups. This switch does not support GMRP; it uses the Internet Group Management Protocol (IGMP) to provide automatic multicast filtering.

WEB INTERFACE

To view Bridge Extension information in the web interface:

1. Click System, then Capability.

Figure 6: Displaying Bridge Extension Configuration



MANAGING SYSTEM FILES

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

COPYING FILES VIA FTP/TFTP OR HTTP

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

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

CLI REFERENCES

- "copy" on page 491

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.
  - TFTP Upgrade – Copies a file from a TFTP server to the switch.
  - TFTP Download – Copies a file from the switch to a TFTP 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
- **FTP/TFTP Server IP Address** – The IP address of an FTP/TFTP server.
- **User Name** – The user name for FTP server access.
- **Password** – The password for FTP server access.
- **File Type** – Specify Operation Code to copy firmware.
- **File Name** – The file name should not contain slashes (\ or /), the leading letter of the file name should not be a period (.), and the maximum length for file names is 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.

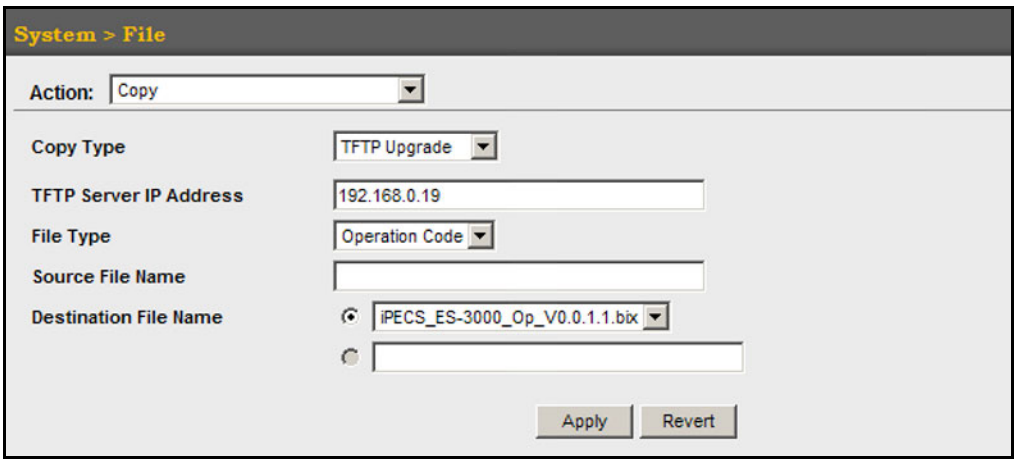
NOTE: The file "Factory_Default_Config.cfg" can be copied to a TFTP server or management station, but cannot be used as the destination file name on the switch.

WEB INTERFACE

To copy firmware files in the web interface:

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



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 491

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, ".", "-", "_")

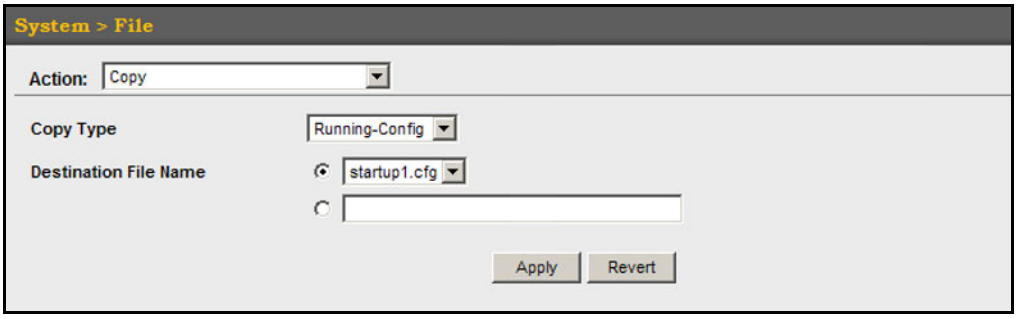
NOTE: The maximum number of user-defined configuration files is limited only by available flash memory space.

WEB INTERFACE

To save the running configuration file in the web interface:

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



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

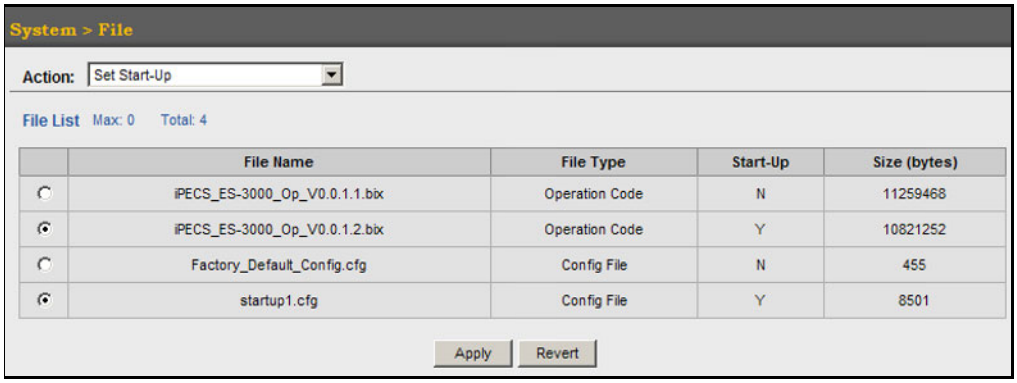
- "whichboot" on page 495
- "boot system" on page 490

WEB INTERFACE

To set a file to use for system initialization in the web interface:

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



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

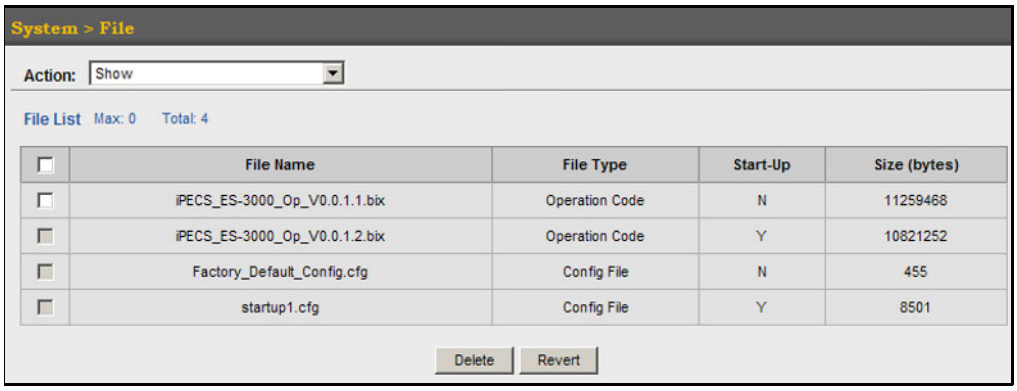
- "dir" on page 494
- "delete" on page 494

WEB INTERFACE

To show the system files in the web interface:

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



AUTOMATIC OPERATION CODE UPGRADE

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

CLI REFERENCES

- "upgrade opcode auto" on page 496
- "upgrade opcode path" on page 497

USAGE GUIDELINES

- If this feature is enabled, the switch searches the defined URL once during the bootup sequence.
- FTP (port 21) and TFTP (port 69) are both supported. Note that the TCP/UDP port bindings cannot be modified to support servers listening on non-standard ports.
- The host portion of the upgrade file location URL must be a valid IPv4 IP address. DNS host names are not recognized. Valid IP addresses consist of four numbers, 0 to 255, separated by periods.
- The path to the directory must also be defined. If the file is stored in the root directory for the FTP/TFTP service, then use the “/” to indicate this (e.g., ftp://192.168.0.1/).
- The file name must not be included in the upgrade file location URL. The file name of the code stored on the remote server must be

IPECS_ES-3000_Op.bix (using upper case and lower case letters exactly as indicated here). Enter the file name for other switches described in this manual exactly as shown on the web interface.

- The FTP connection is made with PASV mode enabled. PASV mode is needed to traverse some fire walls, even if FTP traffic is not blocked. PASV mode cannot be disabled.

- The switch-based search function is case-insensitive in that it will accept a file name in upper or lower case (i.e., the switch will accept *IPECS_ES-3000_OP.BIX* from the server even though *IPECS_ES-3000_Op.bix* was requested). However, keep in mind that the file systems of many operating systems such as Unix and most Unix-like systems (FreeBSD, NetBSD, OpenBSD, and most Linux distributions, etc.) are case-sensitive, meaning that two files in the same directory, *ipecs_es-3000_op.bix* and *IPECS_ES-3000_Op.bix* are considered to be unique files. Thus, if the upgrade file is stored as *IPECS_ES-3000_Op.bix* (or even *IPECS_es-3000_op.bix*) on a case-sensitive server, then the switch (requesting *ipecs_es-3000_op.bix*) will not be upgraded because the server does not recognize the requested file name and the stored file name as being equal. A notable exception in the list of case-sensitive Unix-like operating systems is Mac OS X, which by default is case-insensitive. Please check the documentation for your server's operating system if you are unsure of its file system's behavior.

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

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

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

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

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

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

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

PARAMETERS

The following parameters are displayed in the web interface:

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

- **Automatic Upgrade Location URL** – Defines where the switch should search for the operation code upgrade file. The last character of this URL must be a forward slash ("/"). The *IPECS_ES-3000_Op.bix* filename must not be included since it is automatically appended by the switch. (Options: ftp, tftp)

  The following syntax must be observed:

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

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

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

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

Examples

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

- tftp://192.168.0.1/

  The image file is in the TFTP root directory.

- tftp://192.168.0.1/switch-opcode/

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

- tftp://192.168.0.1/switches/opcode/

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

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

- ftp://192.168.0.1/

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

- ftp://switches:upgrade@192.168.0.1/

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

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

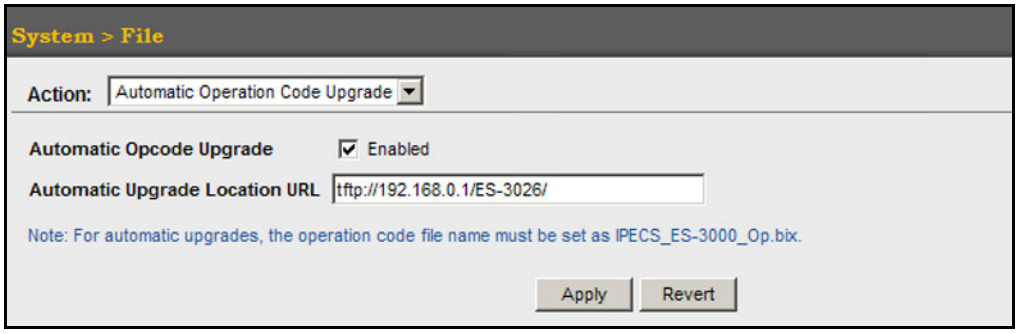
  The user name is “switches” and the password is “upgrade”. The image file is in the “opcode” directory, which is within the “switches” parent directory, relative to the FTP root.

WEB INTERFACE

To configure automatic code upgrade in the web interface:

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

Figure 11: Configuring Automatic Code Upgrade



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

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

SETTING THE SYSTEM CLOCK

Simple Network Time Protocol (SNTP) allows the switch to set its internal clock based on periodic updates from a time server (SNTP or NTP). Maintaining an accurate time on the switch enables the system log to record meaningful dates and times for event entries. You can also manually set the clock. If the clock is not set manually or via SNTP, the switch will only record the time from the factory default set at the last bootup.

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

SETTING THE TIME MANUALLY

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

CLI REFERENCES

- "calendar set" on page 523
- "show calendar" on page 523

PARAMETERS

The following parameters are displayed in the web interface:

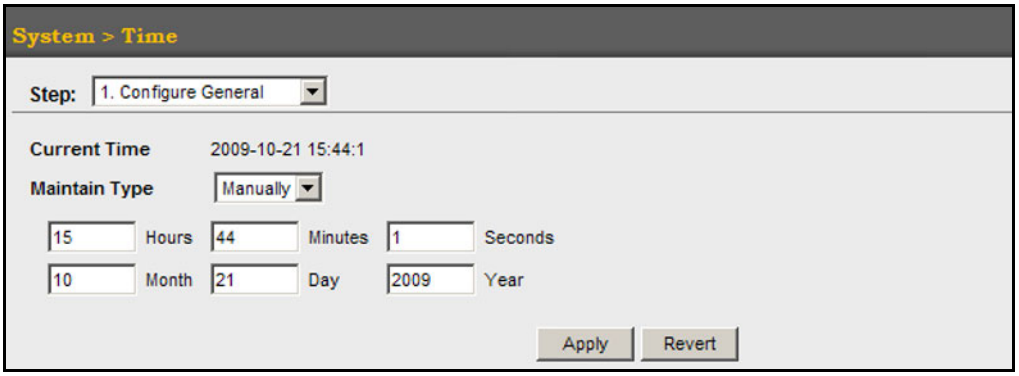
- **Current Time** – Shows the current time set on the switch.
- **Hours** – Sets the hour. (Range: 0-23; Default: 0)
- **Minutes** – Sets the minute value. (Range: 0-59; Default: 0)
- **Seconds** – Sets the second value. (Range: 0-59; Default: 0)
- **Month** – Sets the month. (Range: 1-12; Default: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

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

Figure 12: Manually Setting the System Clock



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 519

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:

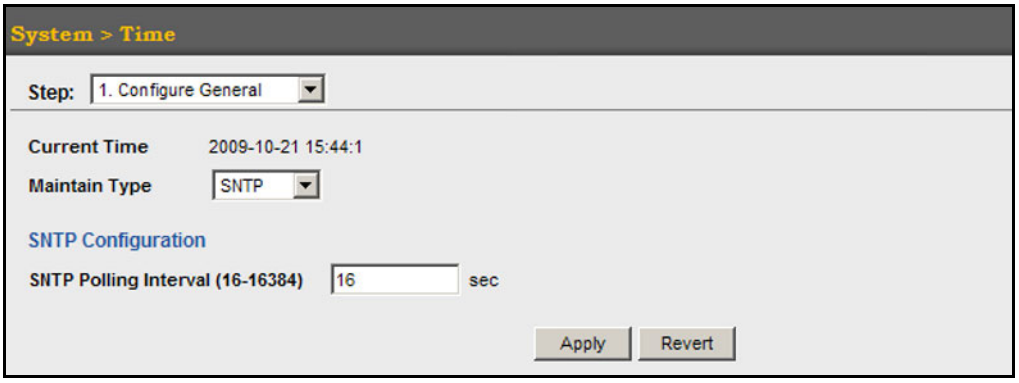
- **Current Time** – Shows the current time set on the switch.
- **SNTP Polling Interval** – Sets the interval between sending requests for a time update from a time server. (Range: 16-16384 seconds; Default: 16 seconds)

WEB INTERFACE

To set the polling interval for SNTP in the web interface:

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 13: Setting the Polling Interval for SNTP



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 521

PARAMETERS

The following parameters are displayed in the web interface:

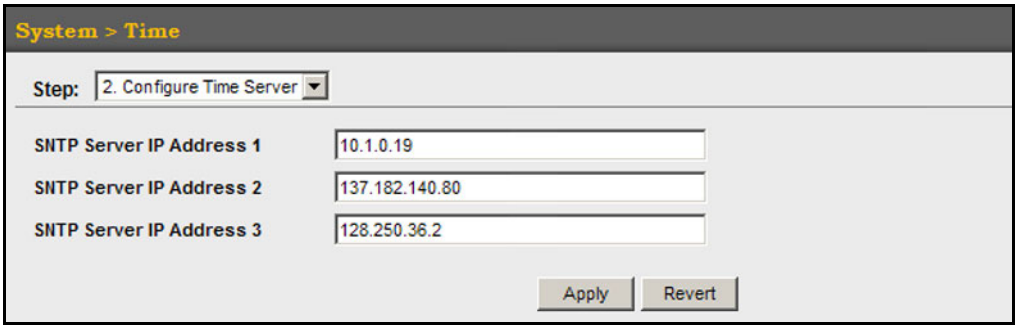
- **SNTP Server IP Address** – Sets the IP address for up to three time servers. The switch attempts to update the time from the first server, if this fails it attempts an update from the next server in the sequence.

WEB INTERFACE

To set the SNTP time servers in the web interface:

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 14: Specifying SNTP Time Servers



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:

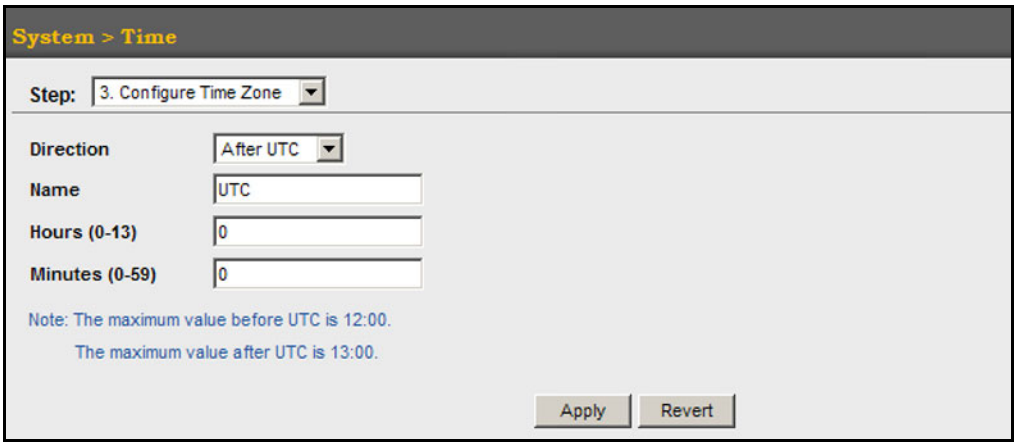
- **Direction**: Configures the time zone to be before (east of) or after (west of) UTC.
- **Name** – Assigns a name to the time zone. (Range: 1-29 characters)
- **Hours** (0-13) – The number of hours before/after UTC. The maximum value before UTC is 12. The maximum value after UTC is 13.
- **Minutes** (0-59) – The number of minutes before/after UTC.

WEB INTERFACE

To set your local time zone in the web interface:

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 15: Setting the Time Zone



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 499

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: 30 seconds)

- **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 503).

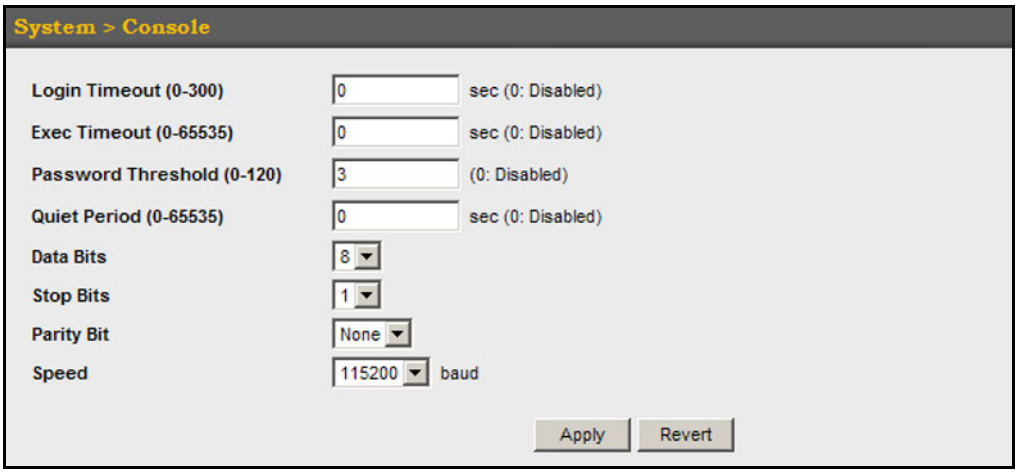
NOTE: Password checking can be enabled or disabled for logging in to the console connection (see "login" on page 501). You can select authentication by a single global password as configured for the password command, or by passwords set up for specific user-name accounts. The default is for local passwords configured on the switch.

WEB INTERFACE

To configure parameters for the console port in the web interface:

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

Figure 16: Console Port Settings



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 499

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)

NOTE: The password for the Telnet connection can only be configured through the CLI (see "password" on page 503).

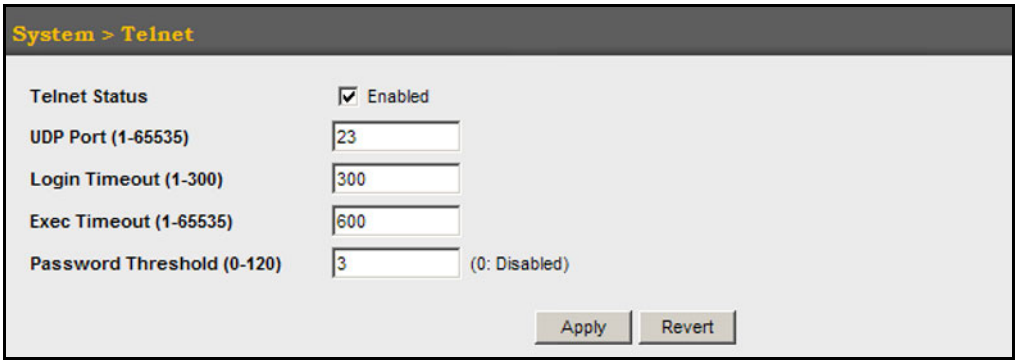
NOTE: Password checking can be enabled or disabled for login to the console connection (see "login" on page 501). You can select authentication by a single global password as configured for the password command, or by passwords set up for specific user-name accounts. The default is for local passwords configured on the switch.

WEB INTERFACE

To configure parameters for the console port in the web interface:

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

Figure 17: Telnet Connection Settings



DISPLAYING CPU UTILIZATION

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

CLI REFERENCES

- "show process cpu" on page 483

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)

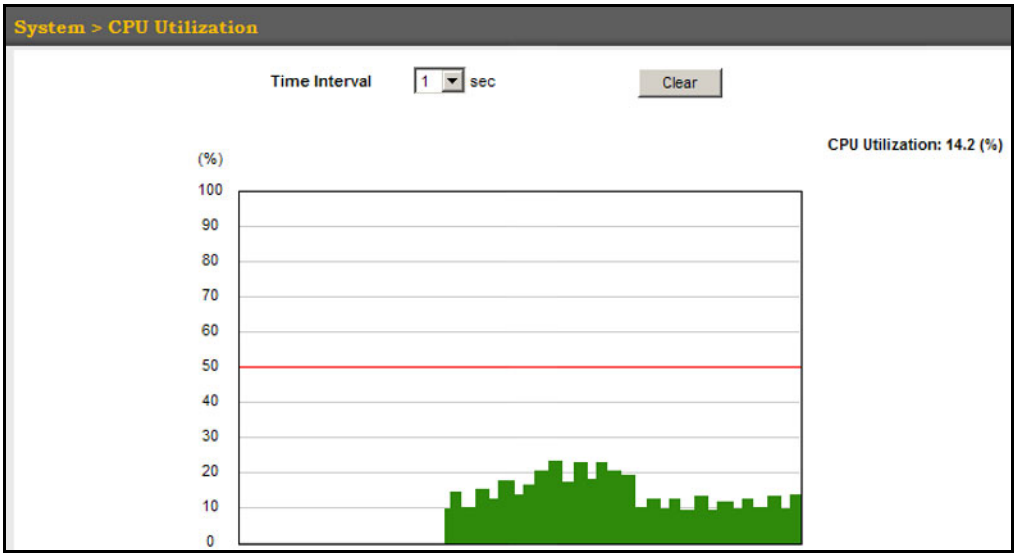
- **CPU Utilization** – CPU utilization over specified interval.

WEB INTERFACE

To display CPU utilization in the web interface:

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 18: Displaying CPU Utilization



DISPLAYING MEMORY UTILIZATION

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

CLI REFERENCES

- "show memory" on page 483

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 in the web interface:

1. Click System, then Memory Status.

Figure 19: Displaying Memory Utilization

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 478
- "reload (Global Configuration)" on page 474
- "show reload" on page 479

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 491).

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 in the web interface:

1. Click System, then Restart.
2. Select the required reset mode.
3. For any option other than to reset immediately, fill in the required parameters
4. Click Apply.
5. When prompted, confirm that you want reset the switch.

Figure 20: Restarting the Switch (Immediately)

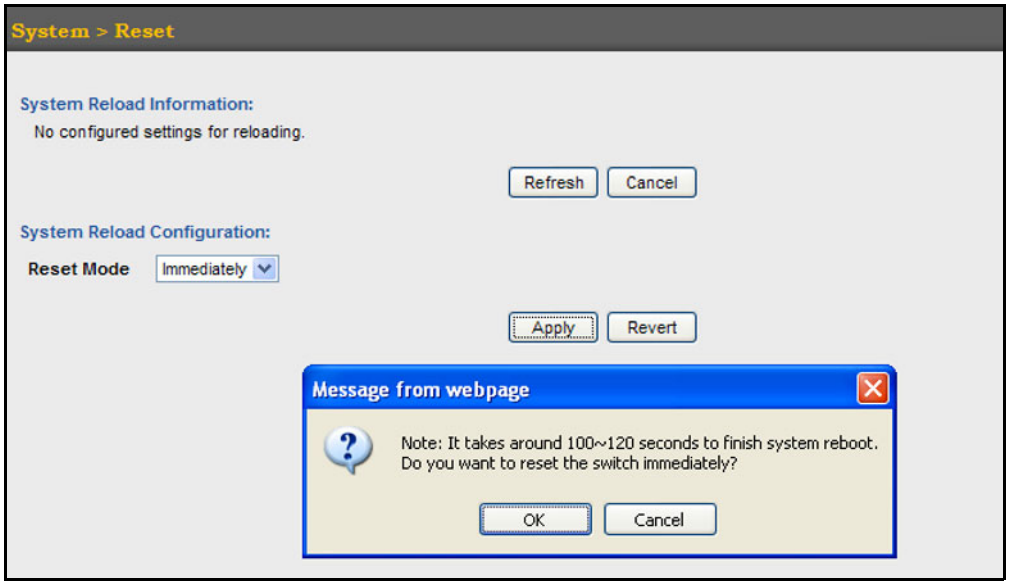


Figure 21: Restarting the Switch (In)

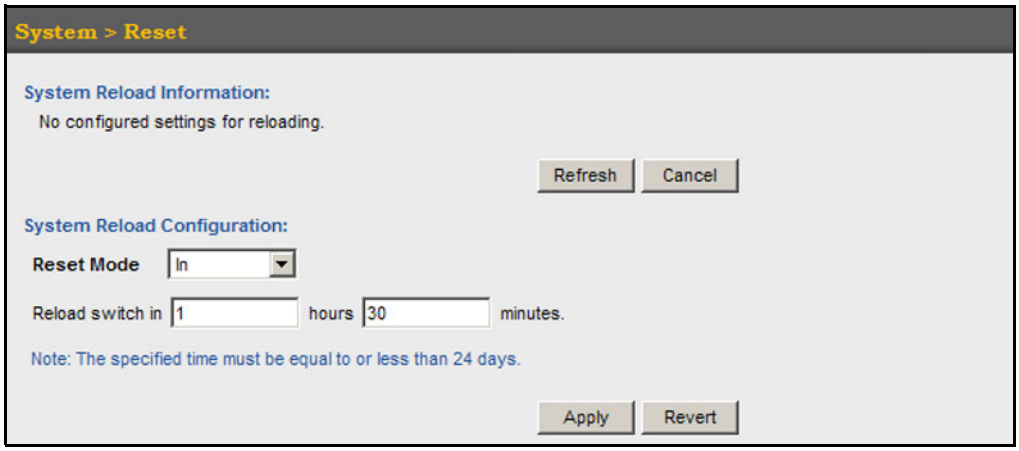


Figure 22: Restarting the Switch (At)

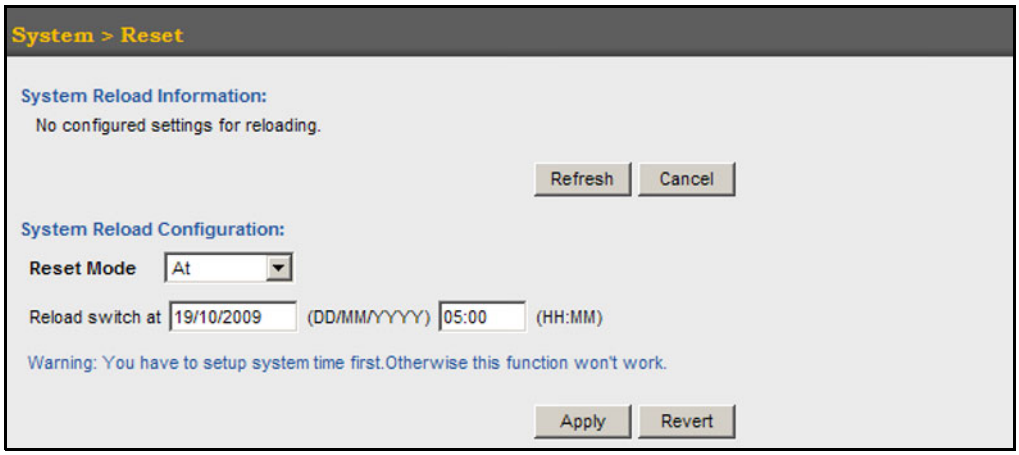
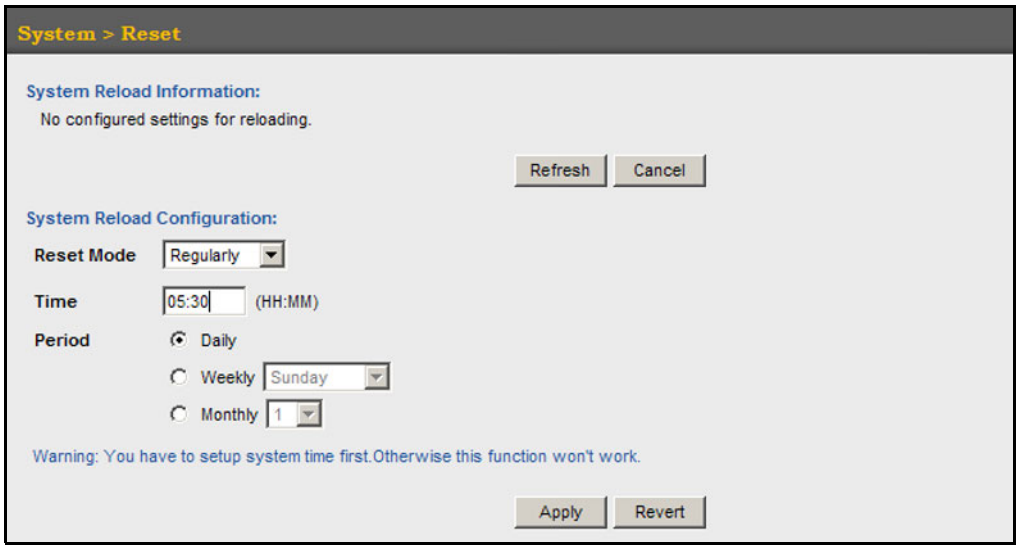


Figure 23: Restarting the Switch (Regularly)



5 INTERFACE CONFIGURATION

This chapter describes how to configure port and trunk connections, set up traffic segmentation, and configure VLAN pass-through trunking.

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 677

COMMAND USAGE

- Auto-negotiation must be disabled before you can configure or force the 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. (100Base-TX, 1000Base-T, 100Base SFP, 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 (25-26 on the ES-3026/P and 21-24 on ES-3024G/P).
  - **Copper-Forced** - Always uses the built-in RJ-45 port.
  - **SFP-Forced** - Always uses the SFP port (even if a module is not installed).
  - **SFP-Preferred-Auto** - Uses SFP port if both combination types are functioning and the SFP port has a valid link. (This is the default.)
- **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** (Gigabit only) - 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.

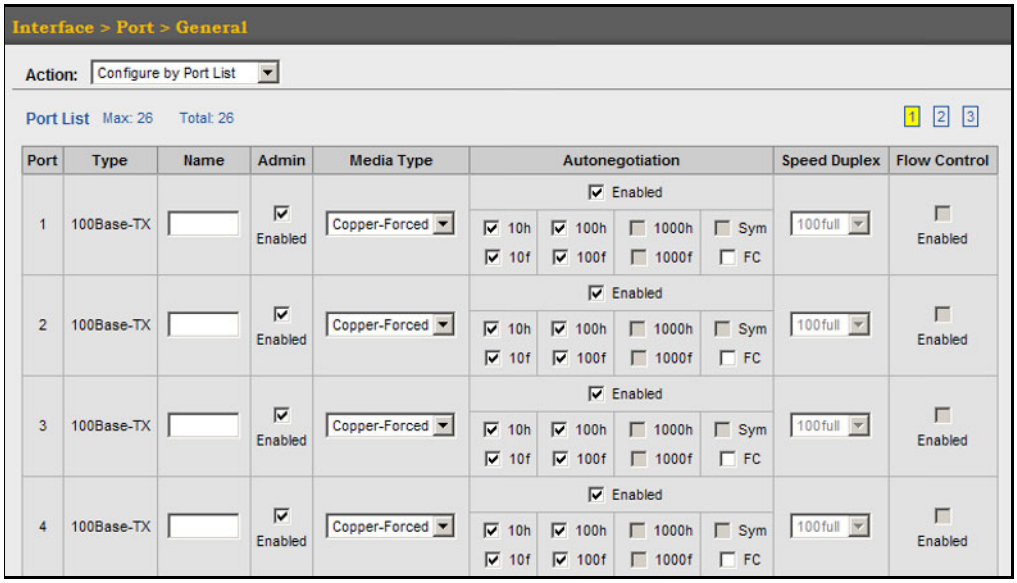
    (Default: Autonegotiation enabled; Advertised capabilities for 100Base-TX – 10half, 10full, 100half, 100full;
    1000BASE-T – 10half, 10full, 100half, 100full, 1000full;
    1000Base-SX/LX/LH – 1000full)
- **Speed/Duplex** – Allows you to manually set the port speed and duplex mode. (i.e., with auto-negotiation disabled)
- **Flow Control** – Allows automatic or manual selection of flow control.

WEB INTERFACE

To configure port connection parameters in the web interface:

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 24: Configuring Connections by Port List



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 113.

CLI REFERENCES

- "Interface Commands" on page 677

WEB INTERFACE

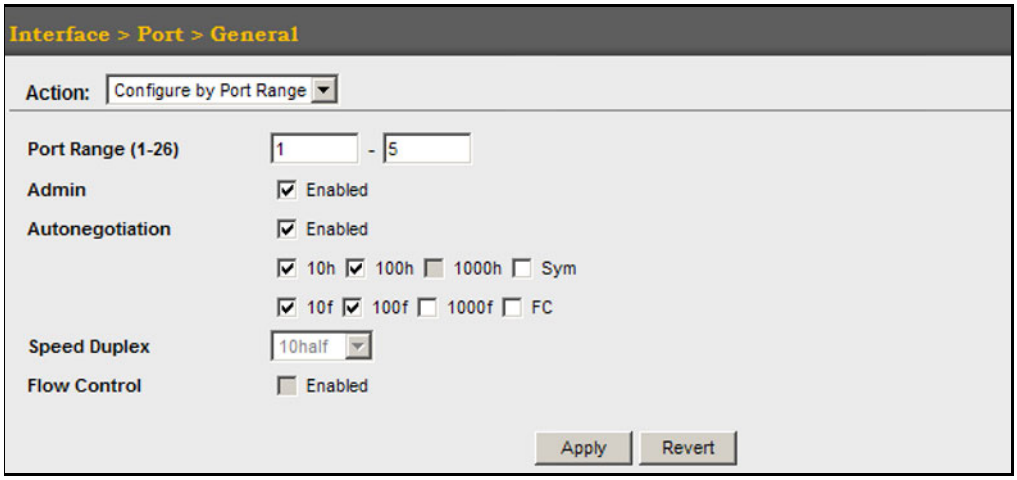
To configure port connection parameters in the web interface:

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 25: Configuring Connections by Port Range



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 688

PARAMETERS

These parameters are displayed in the web interface:

- **Port** – Port identifier.
- **Type** – Indicates the port type. (100Base-TX, 1000Base-T, 100Base SFP or 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: RJ-45 – Copper-Forced;
  SFP – Copper-Forced, SFP-Forced, or SFP-Preferred-Auto;
  Default: RJ-45 – Copper-Forced; SFP – SFP-Preferred-Auto)
- **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 in the web interface:

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

Figure 26: Displaying Port Information

Interface > Port > General

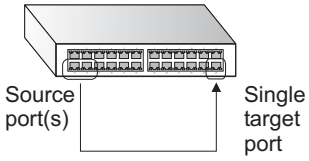
Action: Show Information

Port List Max: 26 Total: 26 1 2 3

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

CONFIGURING LOCAL PORT MIRRORING

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



CLI REFERENCES

- "Local Port Mirroring Commands" on page 711

COMMAND USAGE

- Traffic can be mirrored from one or more source ports to a destination port on the same switch (local port mirroring as described in this section), or from one or more source ports on remote switches to a destination port on this switch (remote port mirroring as described in "Configuring Remote Port Mirroring" on page 119).
- 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 185).

- When mirroring VLAN traffic (see "Configuring VLAN Mirroring" on page 174) or packets based on a source MAC address (see "Configuring MAC Address Mirroring" on page 183), the target port cannot be set to the same target ports as that used for port mirroring by this command.

- When traffic matches the rules for both port mirroring, and for mirroring of VLAN traffic or packets based on a MAC address, the matching packets will not be sent to target port specified for port mirroring.

PARAMETERS

These parameters are displayed in the web interface:

- **Source Port** – The port whose traffic will be monitored. (ES-3026/P: 1-26, ES-3024G/P: 1-24)

- **Target Port** – The port that will mirror the traffic on the source port. (ES-3026/P: 1-26, ES-3024G/P: 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 in the web interface:

1. Click Interface, Port, Mirror.

2. Select Add from the Action List.

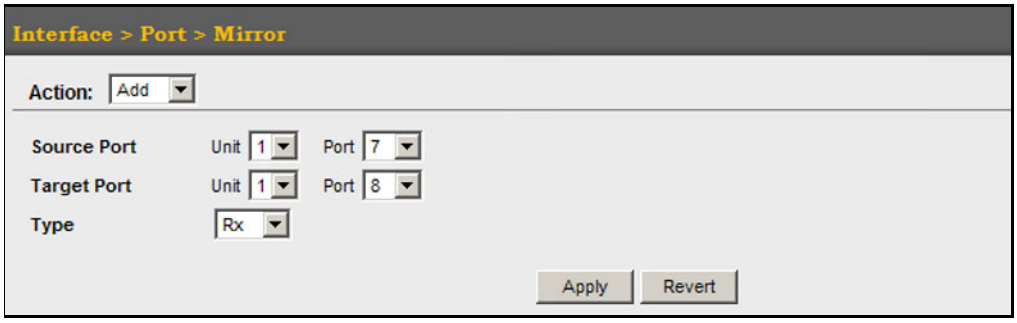
3. Specify the source port.

4. Specify the monitor port.

5. Specify the traffic type to be mirrored.

6. Click Apply.

Figure 27: Configuring Local Port Mirroring

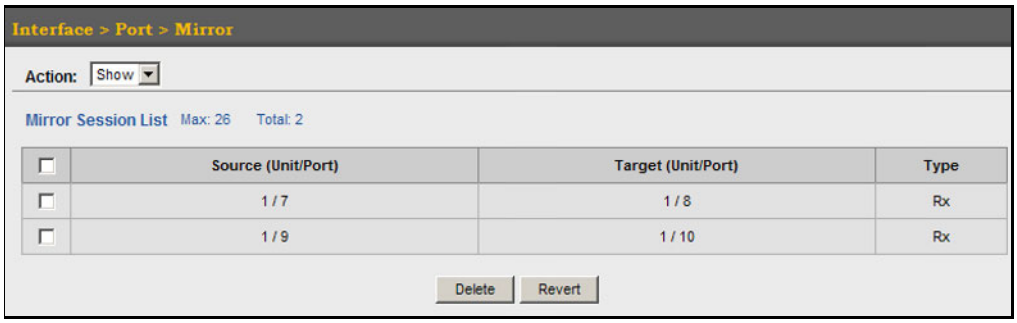


To display the configured mirror sessions in the web interface:

1. Click Interface, Port, Mirror.

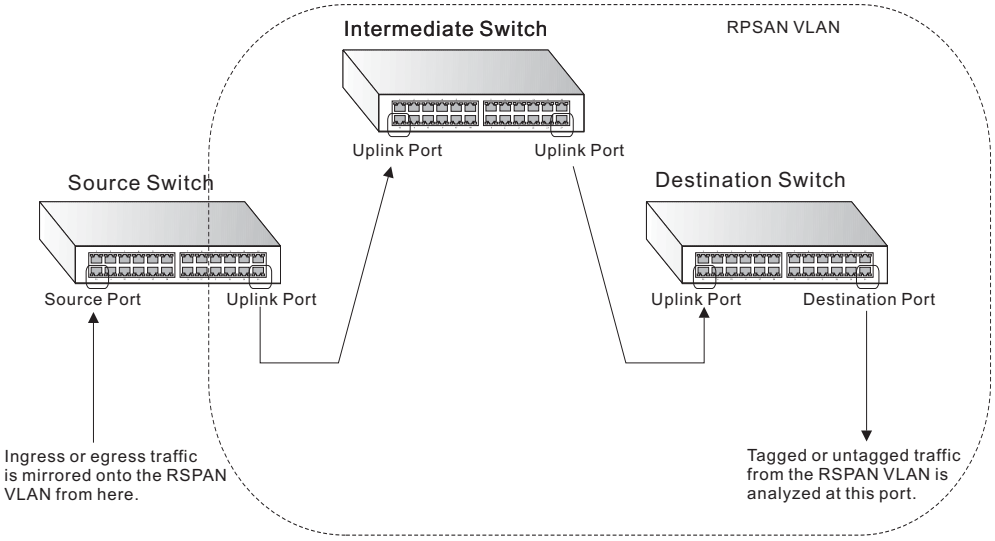
2. Select Show from the Action List.

Figure 28: Displaying Local Port Mirror Sessions



CONFIGURING REMOTE PORT MIRRORING

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



CLI REFERENCES

- "RSPAN Mirroring Commands" on page 713

COMMAND USAGE

- Traffic can be mirrored from one or more source ports to a destination port on the same switch (local port mirroring as described in "Configuring Local Port Mirroring" on page 117), or from one or more source ports on remote switches to a destination port on this switch (remote port mirroring as described in this section).

- *Configuration Guidelines*

  Take the following step to configure an RSPAN session:

  1. Use the VLAN Static List (see "Configuring VLAN Groups" on page 150) to reserve a VLAN for use by RSPAN (marking the "Remote VLAN" field on this page. (Default VLAN 1 is prohibited.)

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

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

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

- *RSPAN Limitations*

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

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

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

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

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

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

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

port is configured as an RSPAN uplink port, port security cannot be enabled on that port.

PARAMETERS

These parameters are displayed in the web interface:

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

  Only two mirror sessions are allowed, including both local and remote mirroring. If local mirroring is enabled (see page 117), then there is only one session available for RSPAN.

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

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

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

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

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

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

- **Remote VLAN** – The VLAN to which traffic mirrored from the source port will be flooded. The VLAN specified in this field must first be reserved for the RSPAN application using the VLAN > Static page (see page 150).

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

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

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

- **Type** – Specifies the traffic type to be mirrored remotely. (Options: Rx, Tx, Both)

- **Destination Port** – Specifies the destination port to monitor the traffic mirrored from the source ports. Only one destination port can be

configured on the same switch per session, but a destination port can be configured on more than one switch for the same session. Also note that a destination port can still send and receive switched traffic, and participate in any Layer 2 protocols to which it has been assigned.

- **Tag** – Specifies whether or not the traffic exiting the destination port to the monitoring device carries the RSPAN VLAN tag.

WEB INTERFACE

To configure a remote mirror session in the web interface:

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

Figure 29: Configuring Remote Port Mirroring (Source)

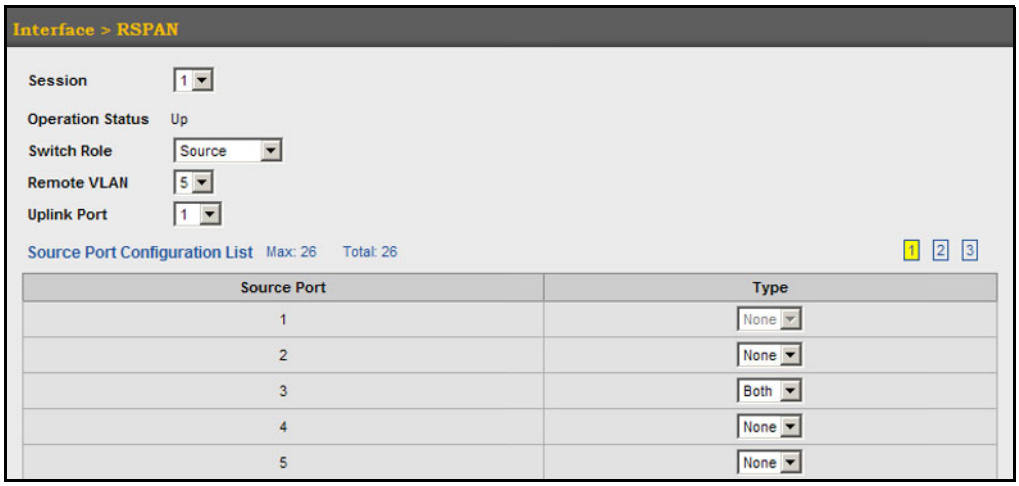


Figure 30: Configuring Remote Port Mirroring (Intermediate)

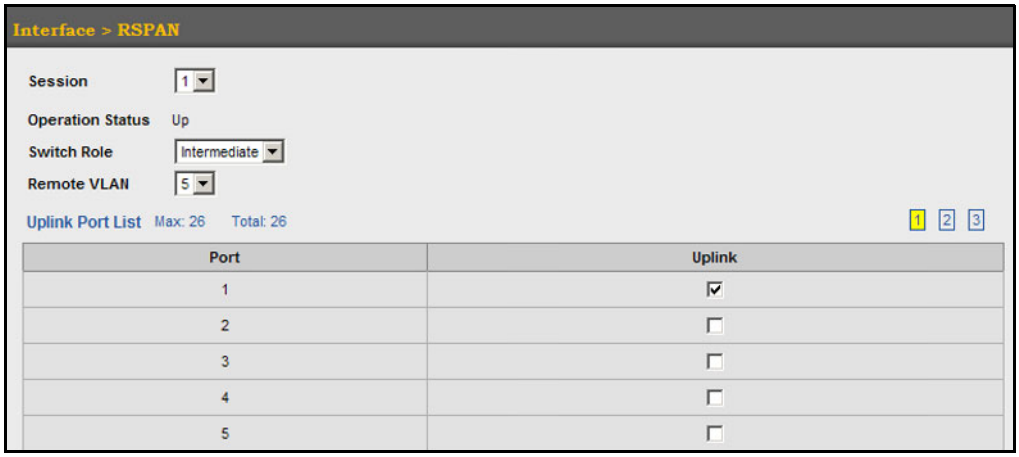
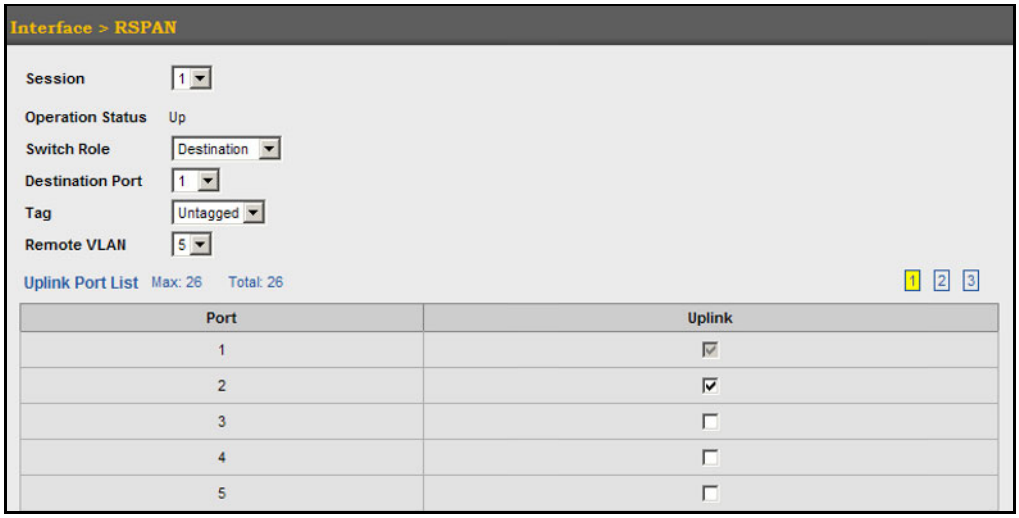


Figure 31: Configuring Remote Port Mirroring (Destination)



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 687

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.

Table 5: Port Statistics (Continued)

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

Table 5: Port Statistics (Continued)

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

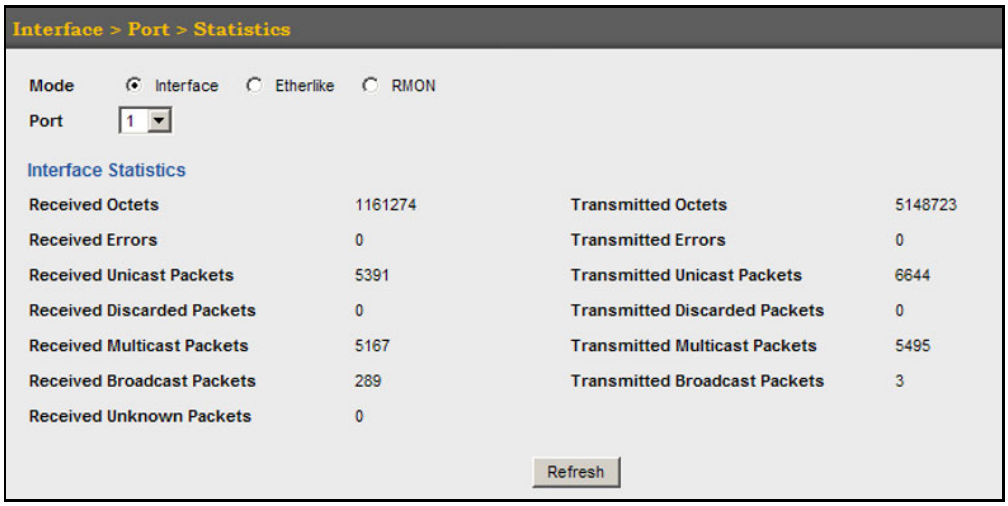
WEB INTERFACE

To show a list of port statistics in the web interface:

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 32: Showing Port Statistics (Table)



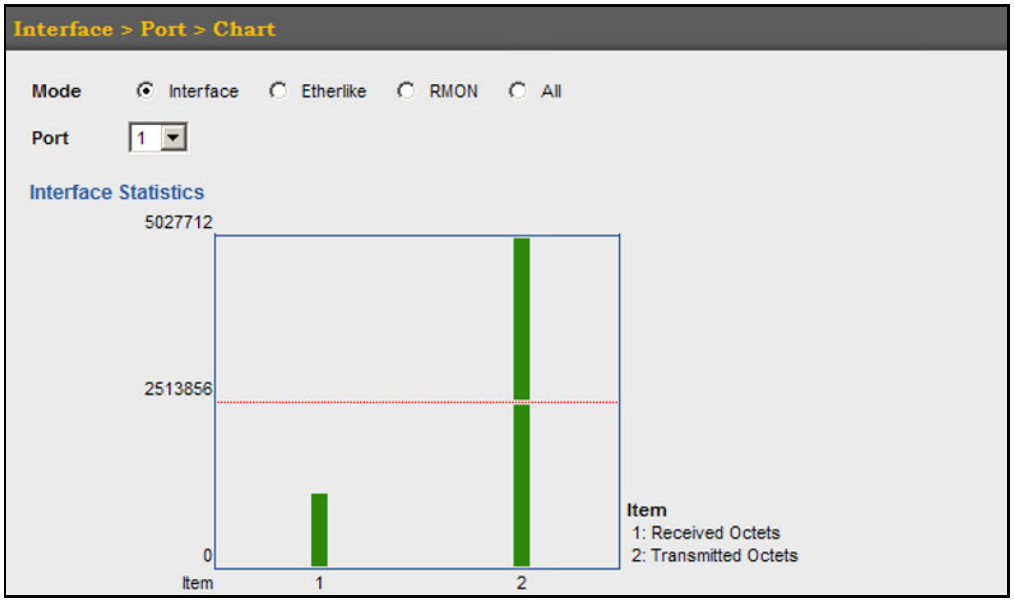
To show a chart of port statistics in the web interface:

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 33: Showing Port Statistics (Chart)



PERFORMING CABLE DIAGNOSTICS

Use the Interface > Port > Cable Test page to test the cable attached to a port. The cable test will check for any cable faults (short, open, etc.). If a fault is found, the switch reports the length to the fault. Otherwise, it reports the cable length. It can be used to determine the quality of the cable, connectors, and terminations. Problems such as opens, shorts, and cable impedance mismatch can be diagnosed with this test.

CLI REFERENCES

- "Interface Commands" on page 677

COMMAND USAGE

- Cable diagnostics are performed using Time Domain Reflectometry (TDR) test methods. TDR analyses the cable by sending a pulsed signal into the cable, and then examining the reflection of that pulse.
- 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 to a fault.
- 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.

PARAMETERS

These parameters are displayed in the web interface:

- **Port** – Switch port identifier. (ES-3026/P: 1-26, ES-3024G/P: 1-24)
- **Type** – Displays media type. (FE – Fast Ethernet, GE – Gigabit Ethernet)
- **Link Status** – Shows if the port link is up or down.
- **Test Result** – The results include common cable failures, as well as the status and approximate distance to a fault, or the approximate cable length if no fault is found.
- **Last Updated** – Shows the last time this port was tested.

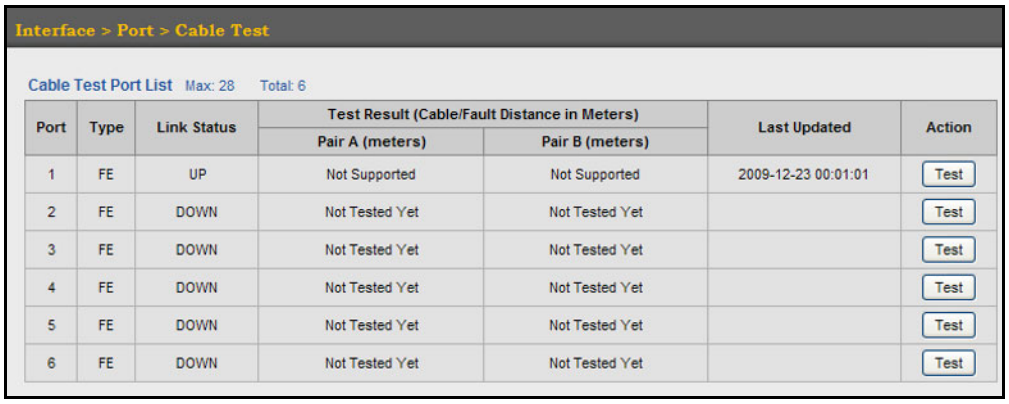
WEB INTERFACE

To show a list of port statistics in the web interface:

1. Click Interface, Port, Cable Test.

2. Click Test for any port to start the cable test.

Figure 34: Performing Cable Tests



Port	Type	Link Status	Test Result (Cable/Fault Distance in Meters)		Last Updated	Action
			Pair A (meters)	Pair B (meters)		
1	FE	UP	Not Supported	Not Supported	2009-12-23 00:01:01	Test
2	FE	DOWN	Not Tested Yet	Not Tested Yet		Test
3	FE	DOWN	Not Tested Yet	Not Tested Yet		Test
4	FE	DOWN	Not Tested Yet	Not Tested Yet		Test
5	FE	DOWN	Not Tested Yet	Not Tested Yet		Test
6	FE	DOWN	Not Tested Yet	Not Tested Yet		Test

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

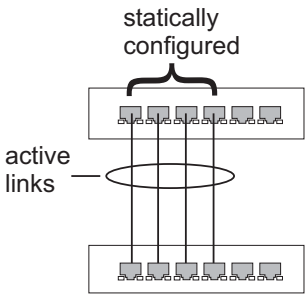
Use the Interface > Trunk > Static page to create a trunk, assign member ports, and configure the connection parameters.

CLI REFERENCES

- "Link Aggregation Commands" on page 695
- "Interface Commands" on page 677

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:

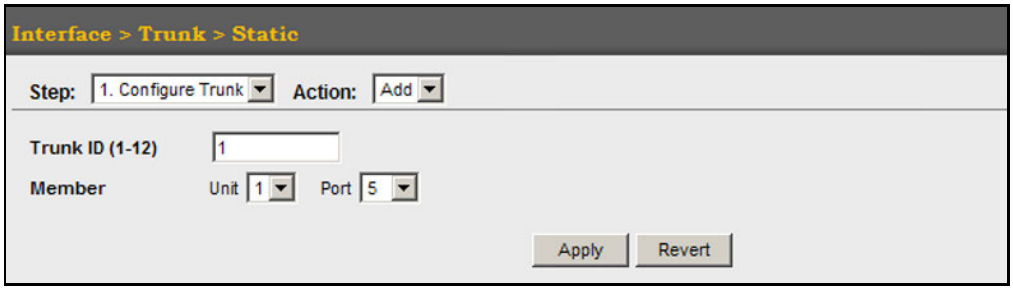
- **Trunk ID** – Trunk identifier. (Range: 1-12)
- **Member** – The initial trunk member. Use the Add Member page to configure additional members.
  - **Unit** – Unit identifier. (Range: 1)
  - **Port** – Port identifier. (ES-3026/P: 1-26, ES-3024G/P: 1-24)

WEB INTERFACE

To create a static trunk in the web interface:

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.

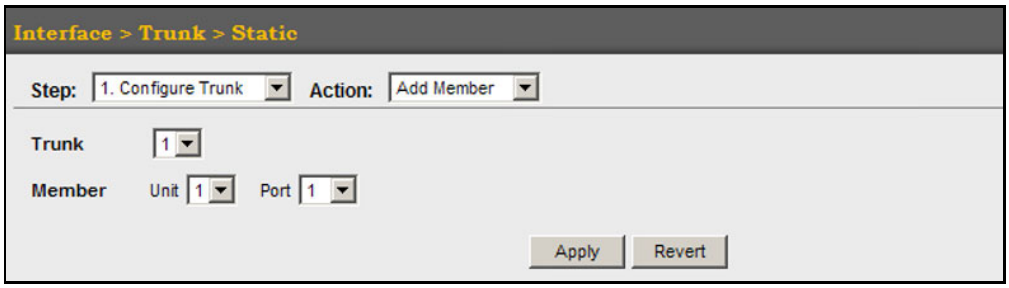
Figure 35: Creating Static Trunks



To add member ports to a static trunk in the web interface:

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.

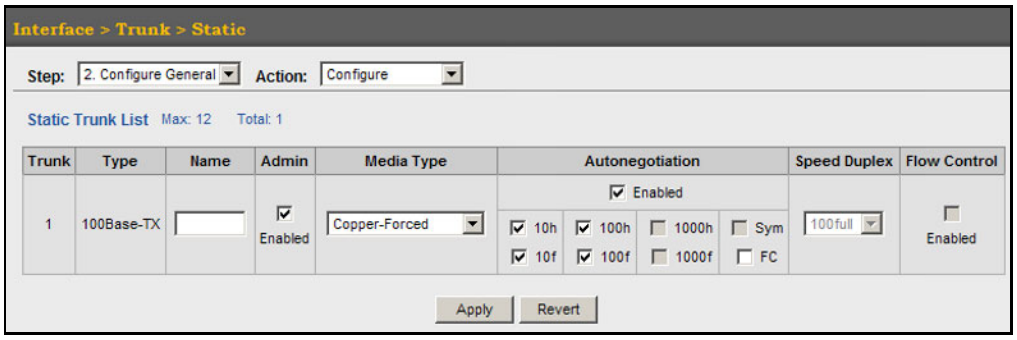
Figure 36: Adding Static Trunks Members



To configure connection parameters for a static trunk in the web interface:

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 113 for a description of the parameters.)
5. Click Apply.

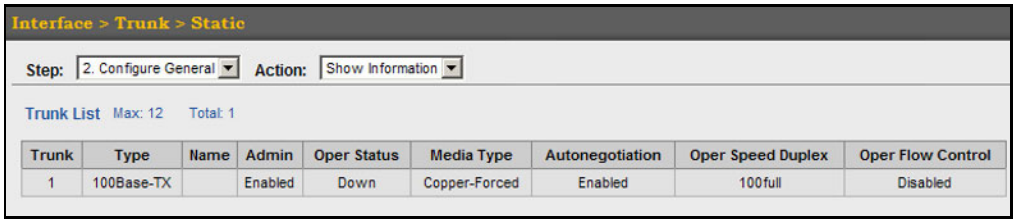
Figure 37: Configuring Connection Parameters for a Static Trunk



To show the static trunks configured on the switch in the web interface:

1. Click Interface, Trunk, Static.
2. Select Configure General from the Step list.
3. Select Show Information from the Action list.

Figure 38: Showing Information for Static Trunks



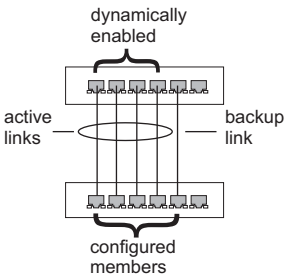
CONFIGURING A DYNAMIC TRUNK

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.

CLI REFERENCES

- "Link Aggregation Commands" on page 695

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 701).

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. (ES-3026/P: 1-26, ES-3024G/P: 1-24)
- **LACP Status** – Enables or disables LACP on a port.

Configure Aggregation Port - Actor/Partner

- **Port** – Port number. (ES-3026/P: 1-26, ES-3024G/P: 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.

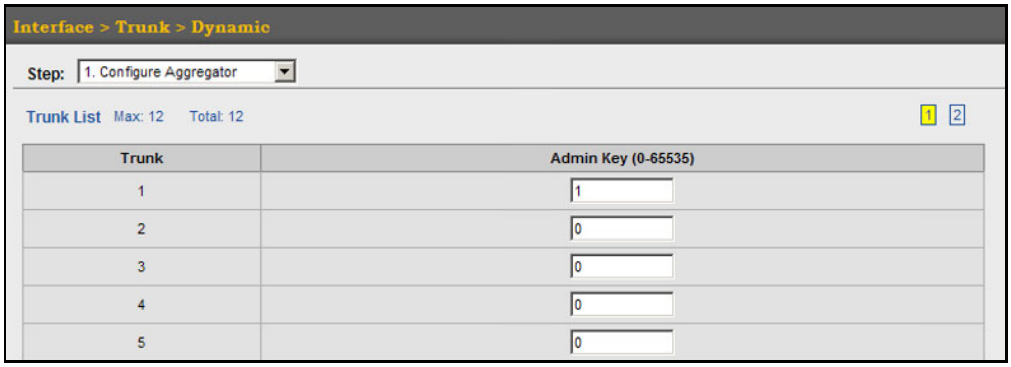
NOTE: Configuring the port partner sets the remote side of an aggregate link; i.e., the ports on the attached device. The command attributes have the same meaning as those used for the port actor.

WEB INTERFACE

To configure the admin key for a dynamic trunk in the web interface:

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.

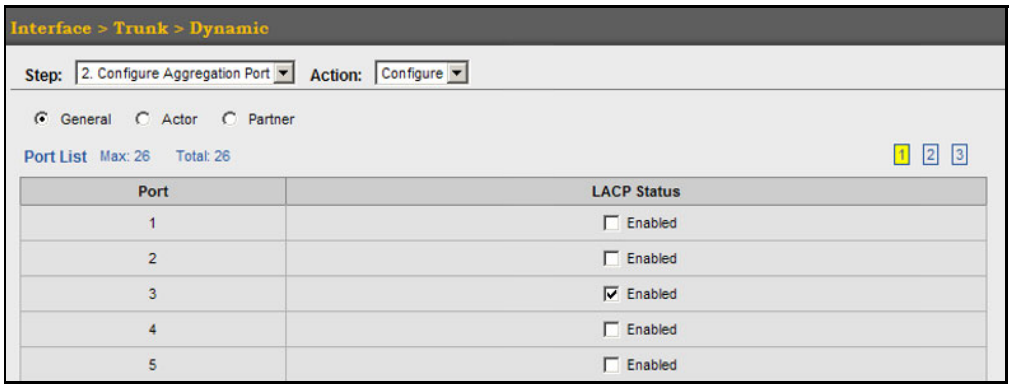
Figure 39: Configuring the LACP Aggregator Admin Key



To enable LACP for a port in the web interface:

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.

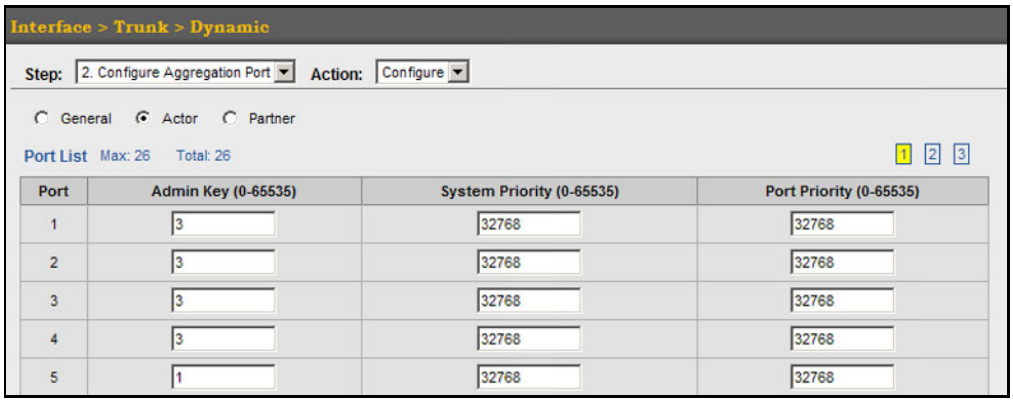
Figure 40: Enabling LACP on a Port



To configure LACP parameters for group members in the web interface:

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 41: Configuring LACP Parameters on a Port



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 701

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.

Table 6: LACP Port Counters (Continued)

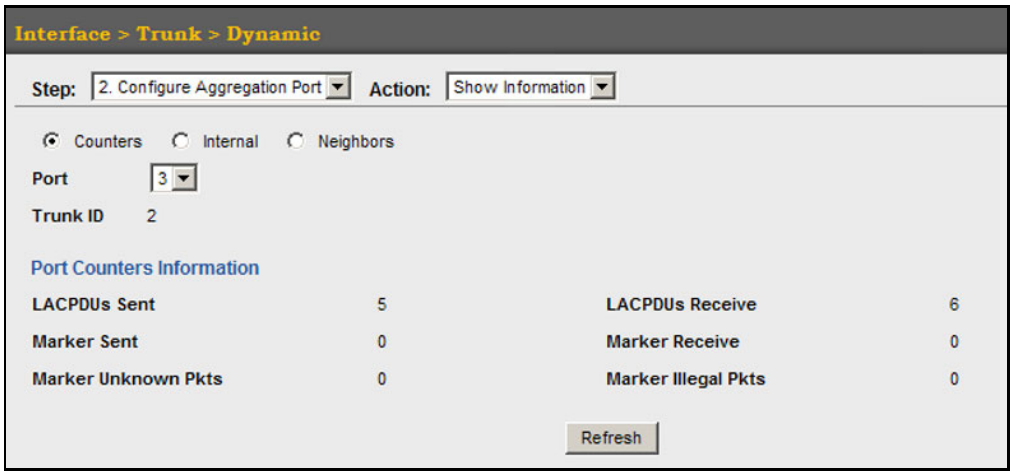
Parameter	Description
Marker Unknown Pkts	Number of frames received that either (1) Carry the Slow Protocols Ethernet Type value, but contain an unknown PDU, or (2) are addressed to the Slow Protocols group MAC Address, but do not carry the Slow Protocols Ethernet Type.
Marker Illegal Pkts	Number of 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 in the web interface:

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 42: Displaying LACP Port Counters



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 701

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.
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)

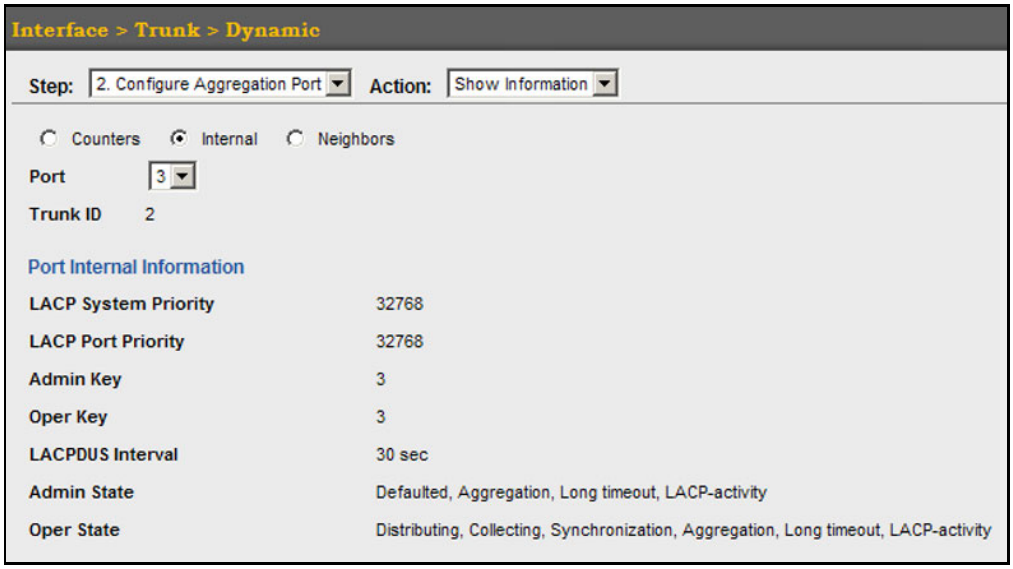
WEB INTERFACE

To display LACP settings and status for the local side in the web interface:

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 43: Displaying LACP Port Internal Information



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 701

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.

Table 8: LACP Internal Configuration Information (Continued)

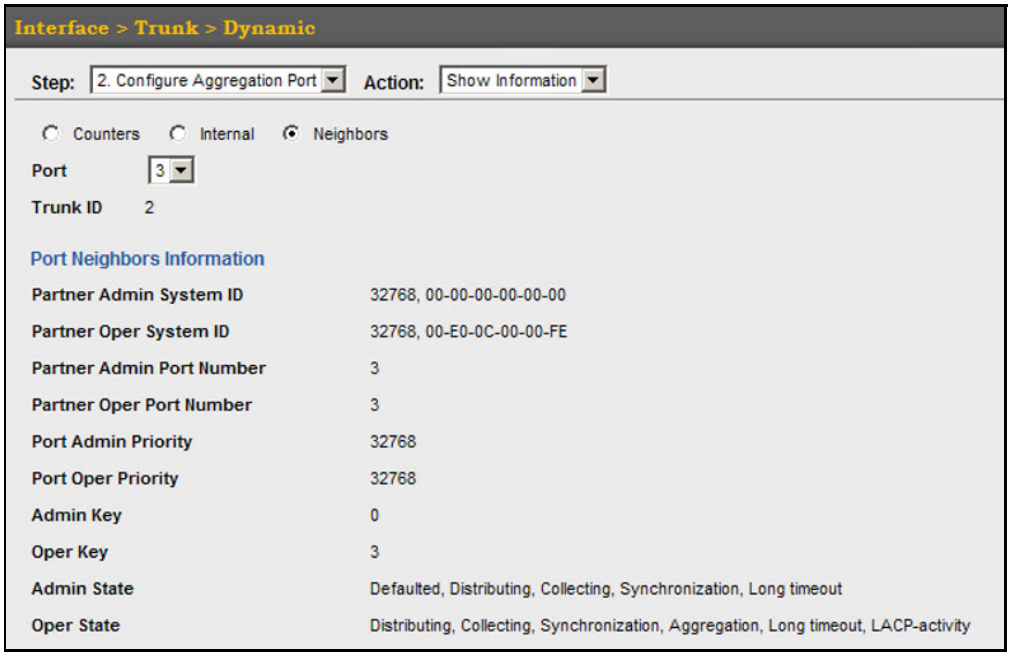
Parameter	Description
Admin State	Administrative values of the partner's state parameters. (See preceding table.)
Oper State	Operational values of the partner's state parameters. (See preceding table.)

WEB INTERFACE

To display LACP settings and status for the remote side in the web interface:

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 Remote Information



SAVING POWER

Use the Interface > Green Ethernet page to enable power savings mode on the selected port.

CLI REFERENCES

- "power-save" on page 692
- "show power-save" on page 693

COMMAND USAGE

- IEEE 802.3 defines the Ethernet standard and subsequent power requirements based on cable connections operating at 100 meters. Enabling power saving mode can reduce power used for cable lengths of 60 meters or less, with more significant reduction for cables of 20 meters or less, and continue to ensure signal integrity.

- The power-saving methods provided by this switch include:

  - Power saving when there is no link partner:

    Under normal operation, the switch continuously auto-negotiates to find a link partner, keeping the MAC interface powered up even if no link connection exists. When using power-savings mode, the switch checks for energy on the circuit to determine if there is a link partner. If none is detected, the switch automatically turns off the transmitter, and most of the receive circuitry (entering Sleep Mode). In this mode, the low-power energy-detection circuit continuously checks for energy on the cable. If none is detected, the MAC interface is also powered down to save additional energy. If energy is detected, the switch immediately turns on both the transmitter and receiver functions, and powers up the MAC interface.

  - Power saving when there is a link partner:

    Traditional Ethernet connections typically operate with enough power to support at least 100 meters of cable even though average network cable length is shorter. When cable length is shorter, power consumption can be reduced since signal attenuation is proportional to cable length. When power-savings mode is enabled, the switch analyzes cable length to determine whether or not it can reduce the signal amplitude used on a particular link.

NOTE: Power savings can only be implemented on Gigabit Ethernet ports when using twisted-pair cabling. Power-savings mode on a active link only works when connection speed is 1 Gbps, and line length is less than 60 meters.

PARAMETERS

These parameters are displayed in the web interface:

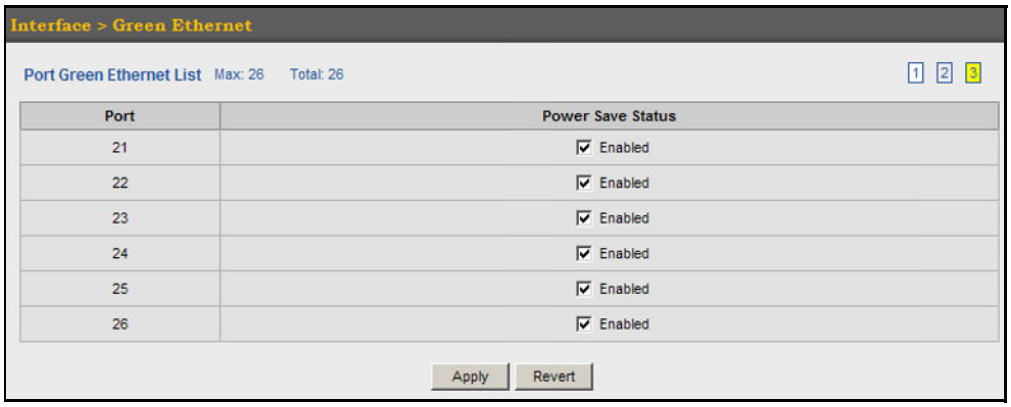
- **Port** – Power saving mode only applies to the Gigabit Ethernet ports using copper media.
- **Power Saving Status** – Adjusts the power provided to ports based on the length of the cable used to connect to other devices. Only sufficient power is used to maintain connection requirements. (Default: Enabled on Gigabit Ethernet RJ-45 ports)

WEB INTERFACE

To enable power savings in the web interface:

1. Click Interface, Green Ethernet.
2. Mark the Enabled check box for a port.
3. Click Apply.

Figure 45: Enabling Power Savings



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 784

PARAMETERS

These parameters are displayed in the web interface:

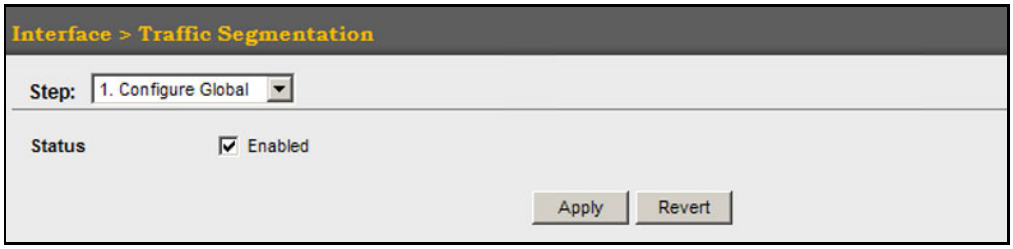
- **Status** – Enables port-based traffic segmentation. (Default: Disabled)

WEB INTERFACE

To enable traffic segmentation in the web interface:

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



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 784

PARAMETERS

These parameters are displayed in the web interface:

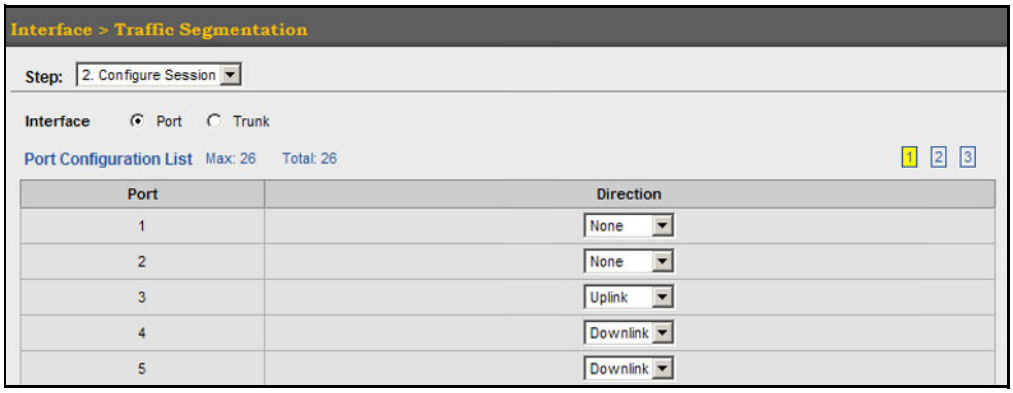
- **Interface** – Displays a list of ports or trunks.
- **Port** – Port Identifier. (ES-3026/P: 1-26, ES-3024G/P: 1-24)
- **Trunk** – Trunk Identifier. (Range: 1-12)
- **Direction** – Adds an interface to the segmented group by setting the direction to uplink or downlink. (Default: None)

WEB INTERFACE

To configure the members of the traffic segmentation group in the web interface:

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



VLAN TRUNKING

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

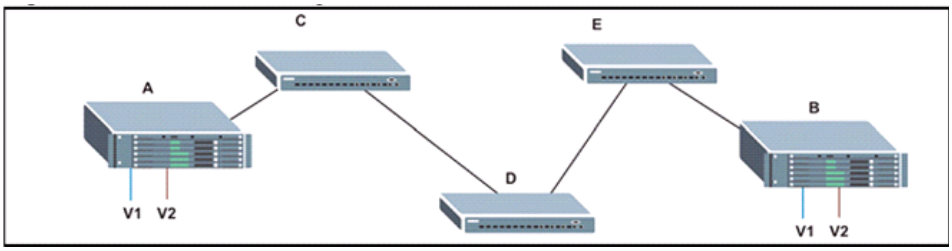
CLI REFERENCES

- "vlan-trunking" on page 778

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.



  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.

- VLAN trunking is mutually exclusive with the “access” switchport mode (see "Adding Static Members to VLANs" on page 152). If VLAN trunking is enabled on an interface, then that interface cannot be set to access mode, and vice versa.

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

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

PARAMETERS

These parameters are displayed in the web interface:

- **Interface** – Displays a list of ports or trunks.
- **Port** – Port Identifier. (ES-3026/P: 25-26, ES-3024G/P: 1-24)

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

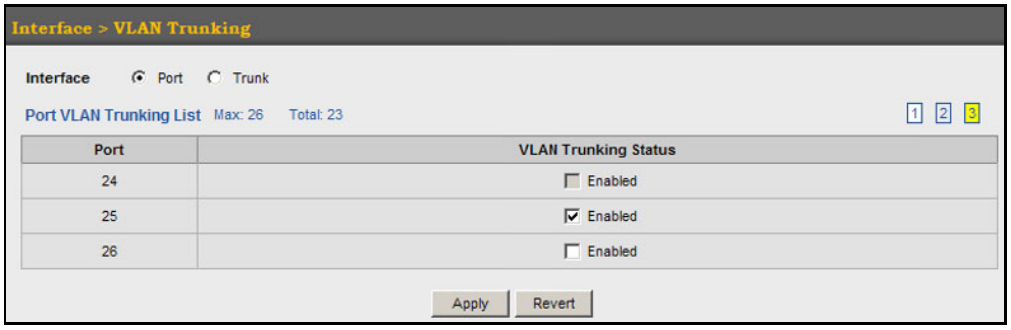
- **Trunk** – Trunk Identifier. (Range: 1-12)
- **VLAN Trunking Status** – Enables VLAN trunking on the selected interface.

WEB INTERFACE

To enable VLAN trunking on a port or trunk in the web interface:

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 48: Configuring VLAN Trunking



6 VLAN CONFIGURATION

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:

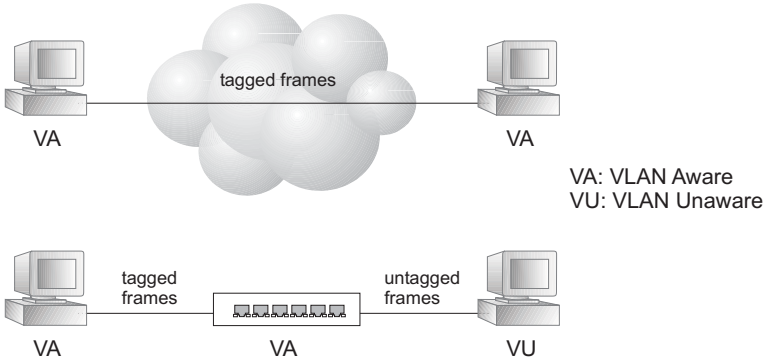
- Up to 256 VLANs based on the IEEE 802.1Q standard
- Distributed VLAN learning across multiple switches using explicit or implicit tagging and GVRP protocol
- Port overlapping, allowing a port to participate in multiple VLANs
- End stations can belong to multiple VLANs
- Passing traffic between VLAN-aware 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.



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.

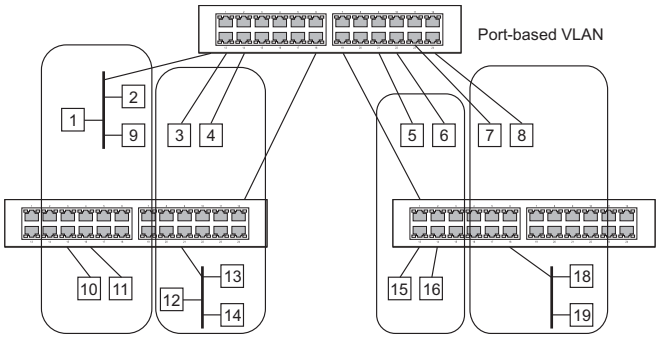
Untagged VLANs – Untagged VLANs are typically used to reduce broadcast traffic and to increase security. A group of network users assigned to a VLAN form a broadcast domain that is separate from other VLANs configured on the switch. Packets are forwarded only between ports that are designated for the 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 152). But you can still enable GVRP on these edge switches, as well as on the core switches in the network.



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 770

PARAMETERS

These parameters are displayed in the web interface:

Add

- **VLAN ID** – ID of VLAN or range of VLANs (1-4093).

  Up to 256 VLAN groups can be defined. VLAN 1 is the default untagged VLAN.

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

- **Remote VLAN** – Reserves this VLAN for RSPAN (see "Configuring Remote Port Mirroring" on page 119).

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.

- **Remote VLAN** – Shows if RSPAN is enabled on this VLAN (see "Configuring Remote Port Mirroring" on page 119).

WEB INTERFACE

To create VLAN groups in the web interface:

1. Click VLAN, Static.

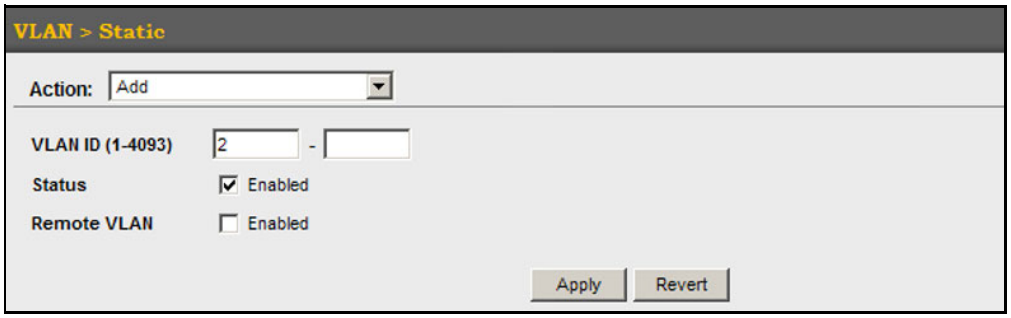
2. Select Add from the Action list.

3. Enter a VLAN ID or range of IDs.

4. Mark Enable to configure the VLAN as operational.

5. Click Apply.

Figure 49: Creating Static VLANs



To modify the configuration settings for VLAN groups in the web interface:

1. Click VLAN, Static.

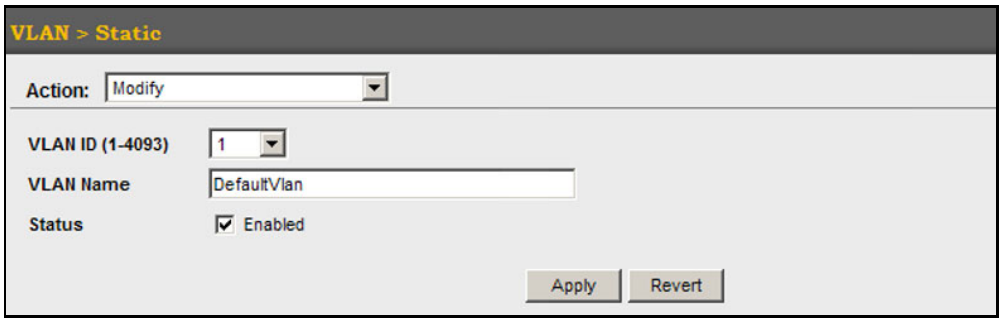
2. Select Modify from the Action list.

3. Select the identifier of a configured VLAN.

4. Modify the VLAN name or operational status as required.

5. Click Apply.

Figure 50: Modifying Settings for Static VLANs

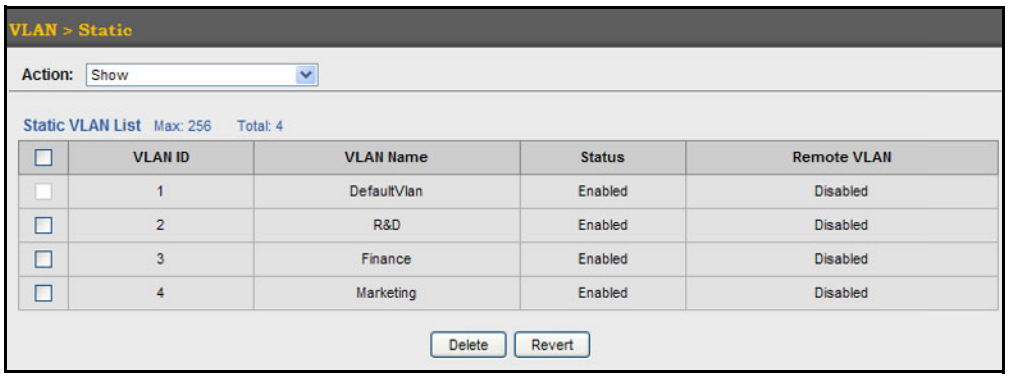


To show the configuration settings for VLAN groups in the web interface:

1. Click VLAN, Static.

2. Select Show from the Action list.

Figure 51: Showing Static VLANs



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 772
- "Displaying VLAN Information" on page 779

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. (ES-3026/P: 1-26, ES-3024G/P: 1-24)
- **Trunk** – Trunk Identifier. (Range: 1-12)

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

  - **Access** - Sets the port to operate as an untagged interface. The port transmits and receives untagged frames on a single VLAN only.

    Access mode is mutually exclusive with VLAN trunking (see "VLAN Trunking" on page 144). If VLAN trunking is enabled on an interface, then that interface cannot be set to access mode, and vice versa.

  - **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)

  When using Access mode, and an interface is assigned to a new VLAN, its PVID is automatically set to the identifier for that VLAN. When using Hybrid mode, the PVID for an interface can be set to any VLAN for which it is an untagged member.

- **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 148.
  - **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 using Access mode.

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. (ES-3026/P: 1-26, ES-3024G/P: 1-24)
- **Trunk Range** – Displays a list of ports. (Range: 1-12)

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 in the web interface:

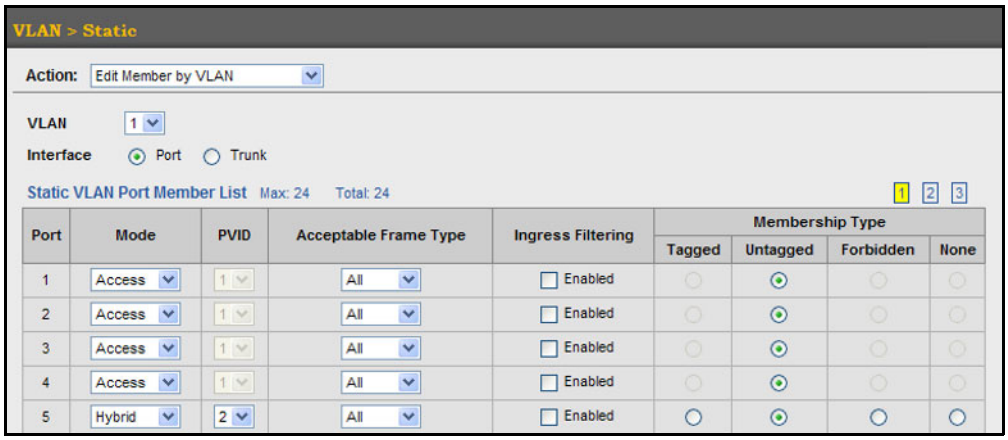
1. Click VLAN, Static.
2. Select Edit Member by VLAN from the Step list.

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 52: Configuring Static Members by VLAN Index



To configure static members by interface in the web interface:

1. Click VLAN, Static.

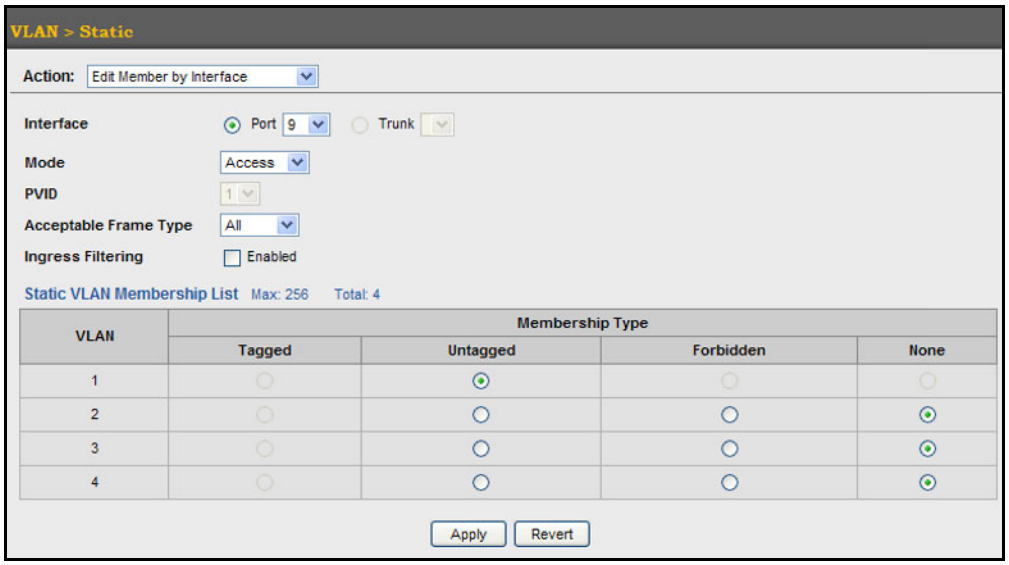
2. Select Edit Member by Interface from the Step list.

3. Select a port or trunk configure.

4. Modify the settings for any interface as required.

5. Click Apply.

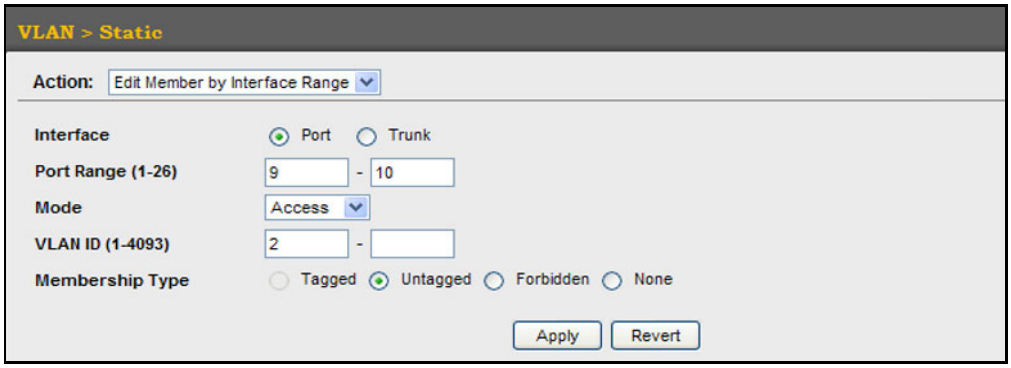
Figure 53: Configuring Static VLAN Members by Interface



To configure static members by interface range in the web interface:

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 54: Configuring Static VLAN Members by Interface Range



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 766
- "Configuring VLAN Interfaces" on page 772

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. (ES-3026/P: 1-26, ES-3024G/P: 1-24)
- **Trunk** – Trunk Identifier. (Range: 1-12)
- **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

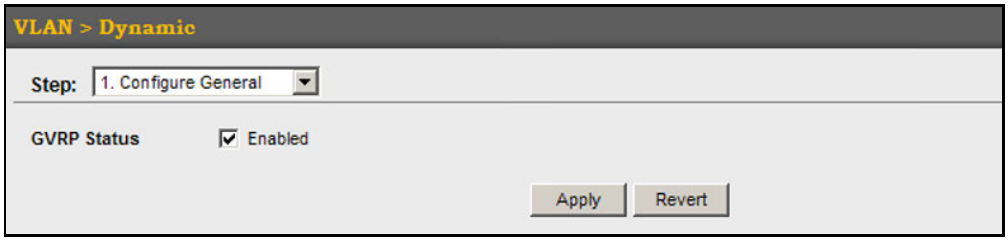
- **VLAN** – Identifier of a VLAN this switch has joined through GVRP.
- **Interface** – Displays a list of ports or trunks which have joined the selected VLAN through GVRP.

WEB INTERFACE

To configure GVRP on the switch in the web interface:

1. Click VLAN, Dynamic.
2. Select Configure General from the Step list.
3. Enable or disable GVRP.
4. Click Apply.

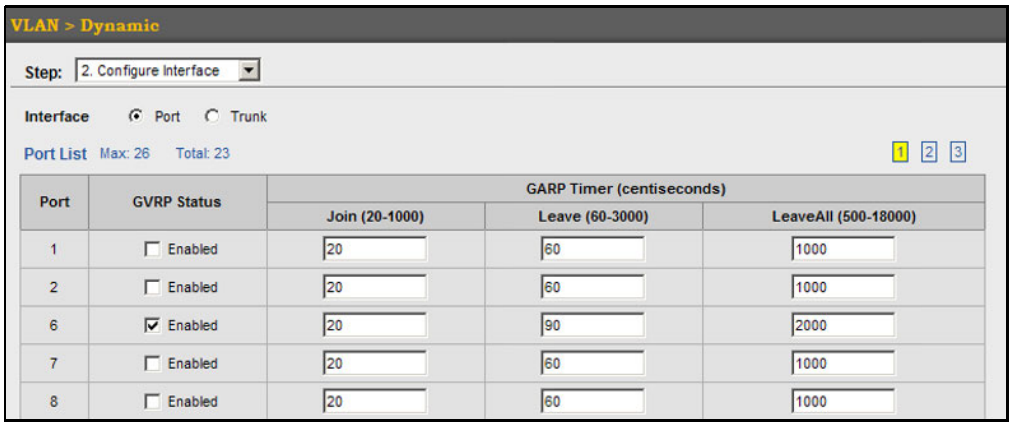
Figure 55: Configuring Global Status of GVRP



To configure GVRP status and timers on a port or trunk in the web interface:

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.

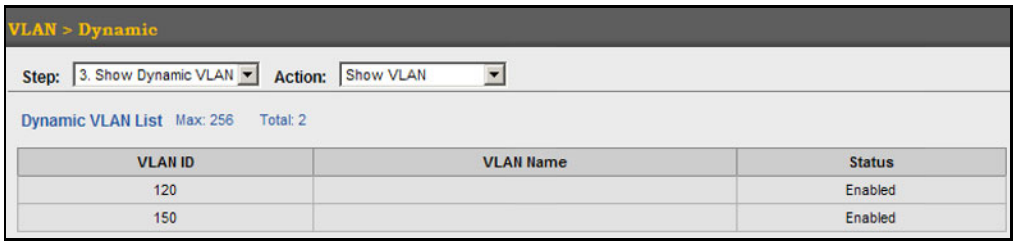
Figure 56: Configuring GVRP for an Interface



To show the dynamic VLAN joined by this switch in the web interface:

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

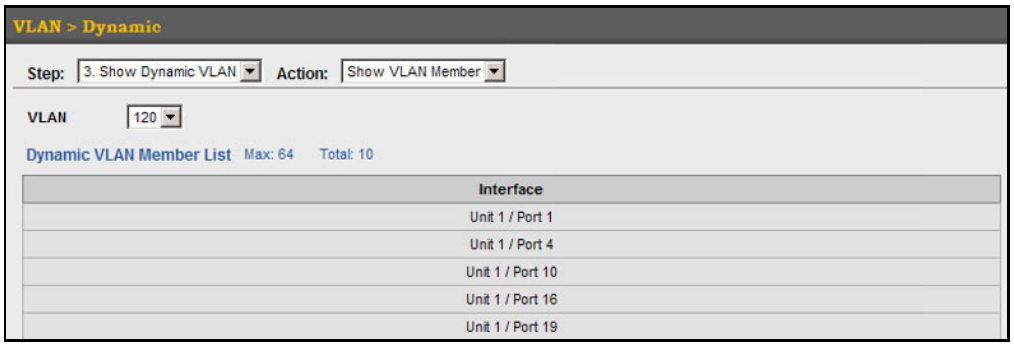
Figure 57: Showing Dynamic VLANs Registered on the Switch



To show the members of a dynamic VLAN in the web interface:

1. Click VLAN, Dynamic.
2. Select Show Dynamic VLAN from the Step list.
3. Select Show VLAN Members from the Action list.

Figure 58: Showing the Members of a Dynamic VLAN



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.

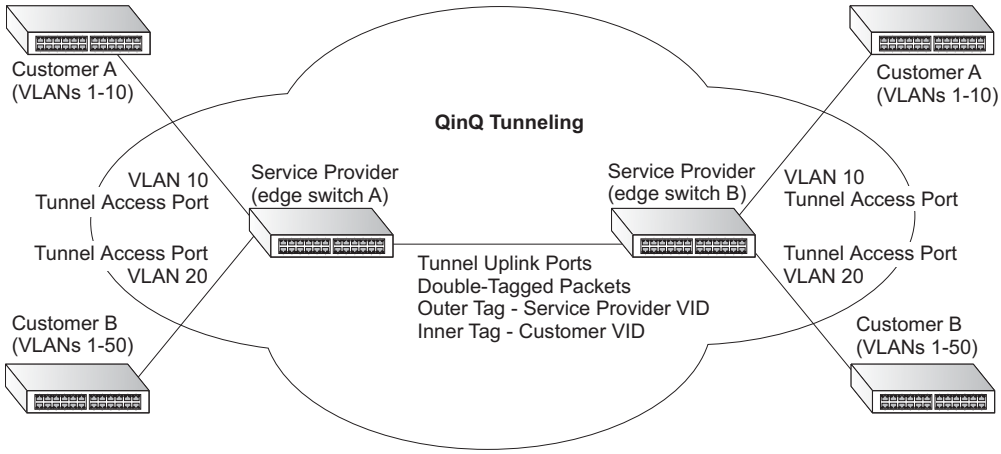
A service provider's customers may have specific requirements for their internal VLAN IDs and number of VLANs supported. VLAN ranges required by different customers in the same service-provider network might easily overlap, and traffic passing through the infrastructure might be mixed. Assigning a unique 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.



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 164.)

2. Create a Service Provider VLAN, also referred to as an SPVLAN (see "Configuring VLAN Groups" on page 150).

3. Configure the QinQ tunnel access port to Tunnel mode (see "Adding an Interface to a QinQ Tunnel" on page 165).

4. Configure the QinQ tunnel access port to join the SPVLAN as an untagged member (see "Adding Static Members to VLANs" on page 152).

5. Configure the SPVLAN ID as the native VID on the QinQ tunnel access port (see "Adding Static Members to VLANs" on page 152).

6. Configure the QinQ tunnel uplink port to Tunnel Uplink mode (see "Adding an Interface to a QinQ Tunnel" on page 165).

7. Configure the QinQ tunnel uplink port to join the SPVLAN as a tagged member (see "Adding Static Members to VLANs" on page 152).

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 780

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 in the web interface:

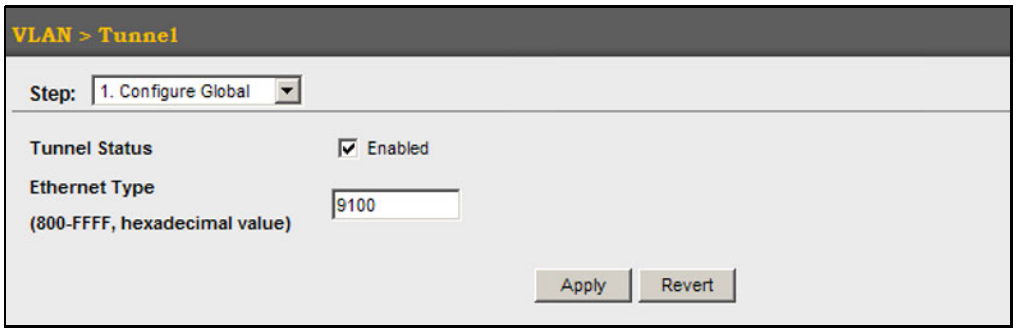
1. Click VLAN, Tunnel.

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 59: Enabling QinQ Tunneling



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 780

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 164). 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. (ES-3026/P: 1-26, ES-3024G/P: 1-24)

- **Trunk** – Trunk Identifier. (Range: 1-12)

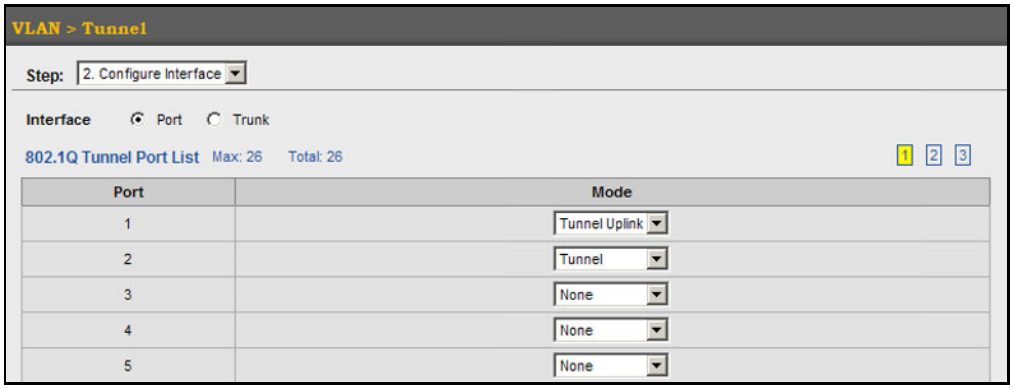
- **Mode** – Sets the VLAN membership mode of the port.
  - **None** – The port operates in its normal VLAN mode. (This is the default.)
  - **Tunnel** – Configures QinQ tunneling for a client access port to segregate and preserve customer VLAN IDs for traffic crossing the service provider network.
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

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 60: Adding an Interface to a QinQ Tunnel



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 770). 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 787

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 in the web interface:

1. Click VLAN, Protocol.

2. Select Configure Protocol from the Step list.

3. Select Add from the Action list.

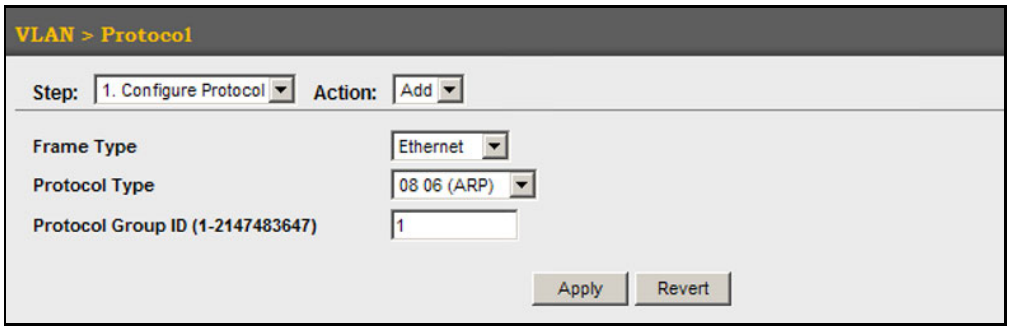
4. Select an entry from the Frame Type list.

5. Select an entry from the Protocol Type list.

6. Enter an identifier for the protocol group.]

7. Click Apply.

Figure 61: Configuring Protocol VLANs



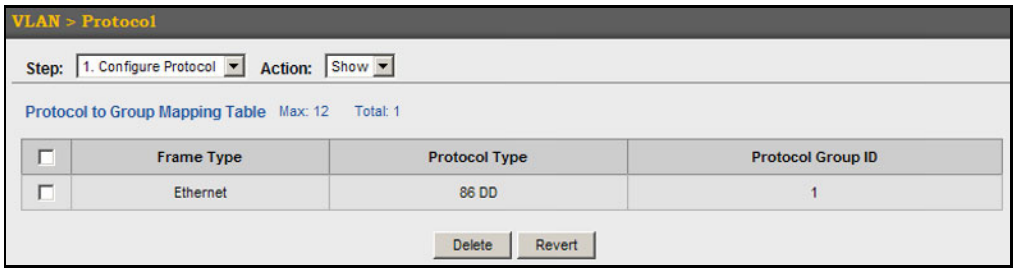
To configure a protocol group in the web interface:

1. Click VLAN, Protocol.

2. Select Configure Protocol from the Step list.

3. Select Show from the Action list.

Figure 62: Displaying Protocol VLANs



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 787

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 152), 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:

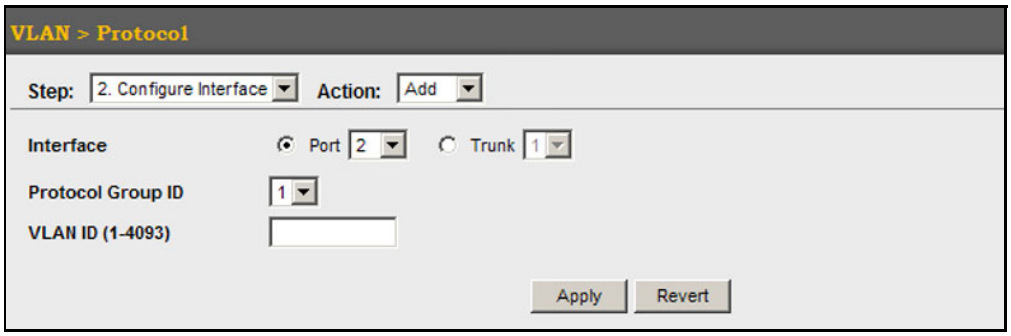
- **Interface** – Displays a list of ports or trunks.
- **Port** – Port Identifier. (ES-3026/P: 1-26, ES-3024G/P: 1-24)
- **Trunk** – Trunk Identifier. (Range: 1-12)
- **Protocol Group ID** – Protocol Group ID assigned to the Protocol VLAN Group. (Range: 1-2147483647)
- **VLAN ID** – VLAN to which matching protocol traffic is forwarded. (Range: 1-4093)

WEB INTERFACE

To map a protocol group to a VLAN for a port or trunk in the web interface:

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.

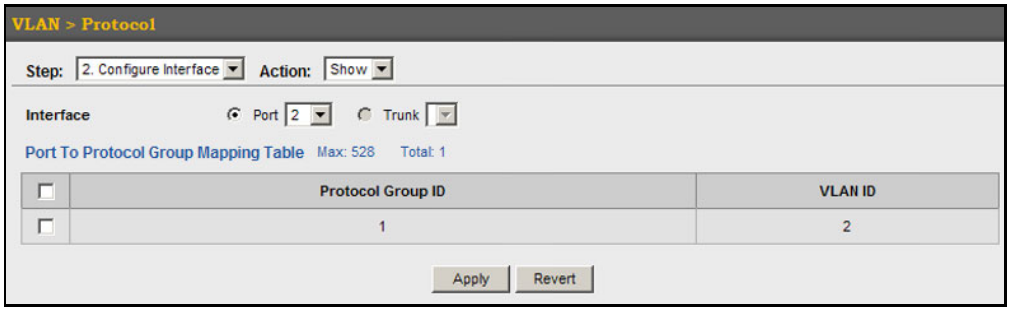
Figure 63: Assigning Interfaces to Protocol VLANs



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

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

Figure 64: Showing the Interface to Protocol Group Mapping



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 790

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:

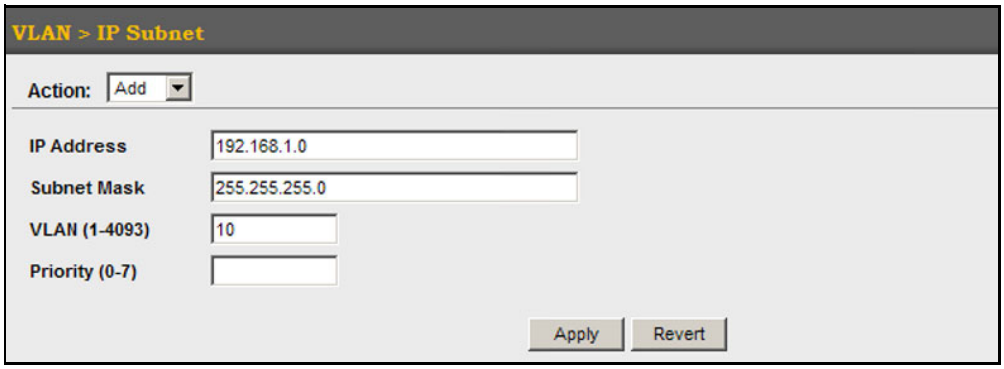
- **IP Address** – The IP address for a subnet. Valid IP addresses consist of four decimal numbers, 0 to 255, separated by periods.
- **Subnet Mask** – This mask identifies the host address bits of the IP subnet.
- **VLAN** – VLAN to which matching IP subnet traffic is forwarded. (Range: 1-4093)
- **Priority**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

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.

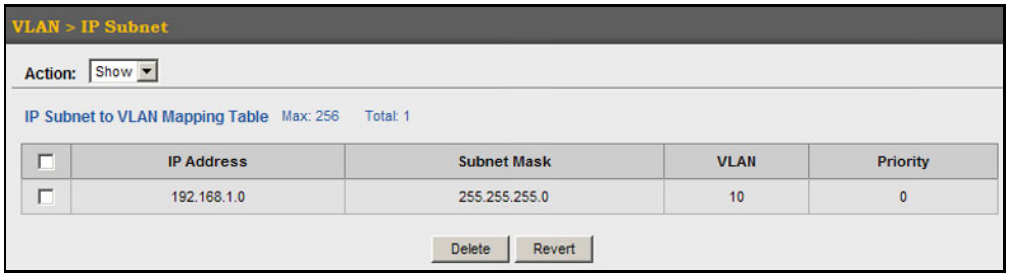
Figure 65: Configuring IP Subnet VLANs



To show the configured IP subnet VLANs in the web interface:

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

Figure 66: Showing IP Subnet VLANs



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 792

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)

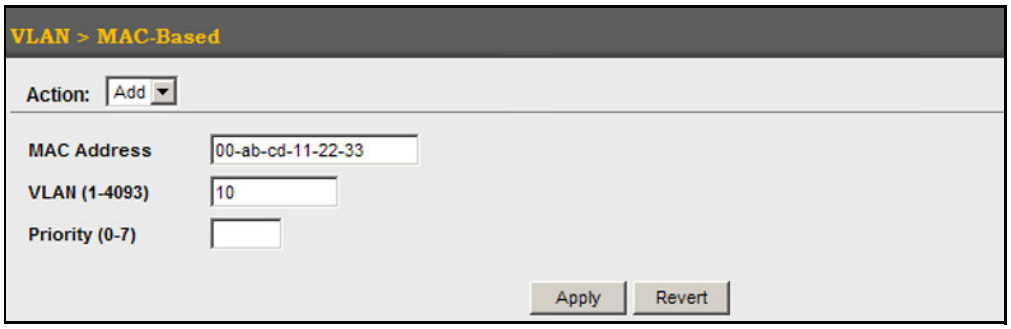
WEB INTERFACE

To map a MAC address to a VLAN in the web interface:

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 67: Configuring MAC-Based VLANs

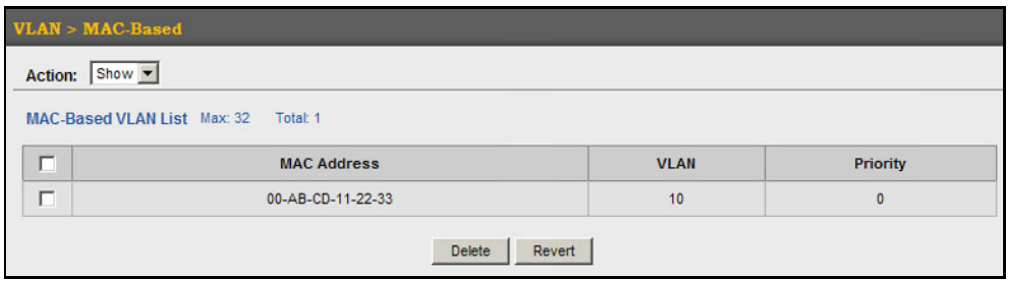


To show the MAC addresses mapped to a VLAN in the web interface:

1. Click VLAN, MAC-Based.

2. Select Show from the Action list.

Figure 68: Showing MAC-Based VLANs



CONFIGURING VLAN MIRRORING

Use the VLAN > Mirror (Add) page to mirror traffic from one or more source VLANs 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 VLAN(s) in a completely unobtrusive manner.

CLI REFERENCES

- "Port Mirroring Commands" on page 711

COMMAND USAGE

- All active ports in a source VLAN are monitored for ingress traffic only.
- All VLAN mirror sessions must share the same target port, preferably one that is not a member of the source VLAN.
- When VLAN mirroring and port mirroring are both enabled, they must use the same target port.

- When VLAN mirroring and port mirroring are both enabled, the target port can receive a mirrored packet twice; once from the source mirror port and again from the source mirrored VLAN.
- The target port receives traffic from all monitored source VLANs and can become congested. Some mirror traffic may therefore be dropped from the target port.
- When mirroring VLAN traffic or packets based on a source MAC address (see "Configuring MAC Address Mirroring" on page 183), the target port cannot be set to the same target ports as that used for port mirroring (see "Configuring Local Port Mirroring" on page 117).
- When traffic matches the rules for both port mirroring, and for mirroring of VLAN traffic or packets based on a MAC address, the matching packets will not be sent to target port specified for port mirroring.

PARAMETERS

These parameters are displayed in the web interface:

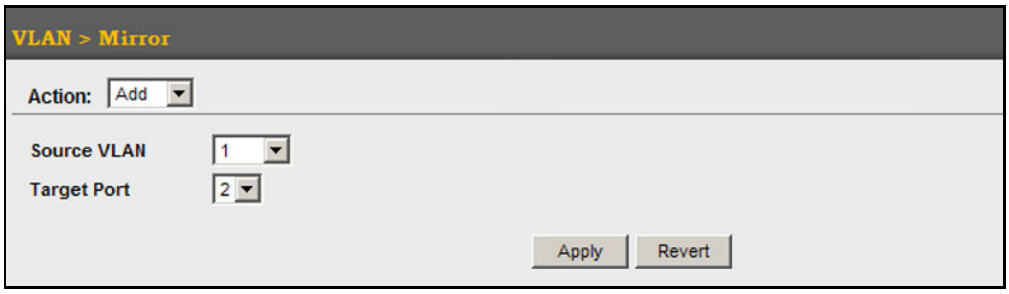
- **Source VLAN** – A VLAN whose traffic will be monitored. (Range: 1-4093)
- **Target Port** – The destination port that receives the mirrored traffic from the source VLAN. (ES-3026/P: 1-26, ES-3024G/P: 1-24)

WEB INTERFACE

To configure VLAN mirroring in the web interface:

1. Click VLAN, Mirror.
2. Select Add from the Action list.
3. Select the source VLAN, and select a target port.
4. Click Apply.

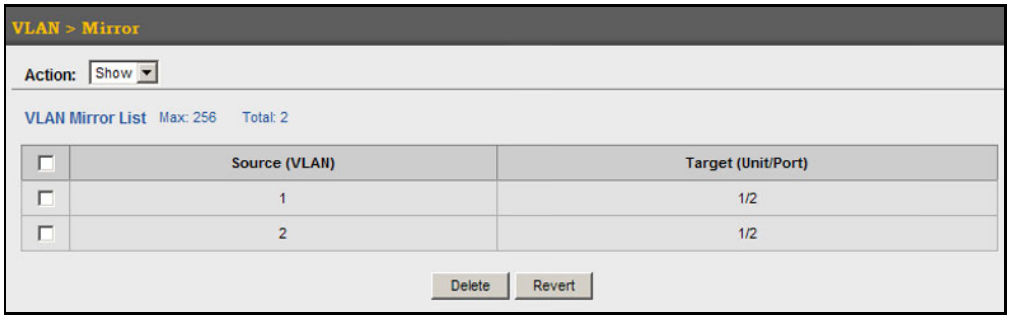
Figure 69: Configuring VLAN Mirroring



To show the VLANs to be mirrored in the web interface:

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

Figure 70: Showing the VLANs to Mirror



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.

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 616

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 178) 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 315).

  - Security Status (see "Configuring Port Security" on page 312) 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. (ES-3026/P: 1-26, ES-3024G/P: 1-24)

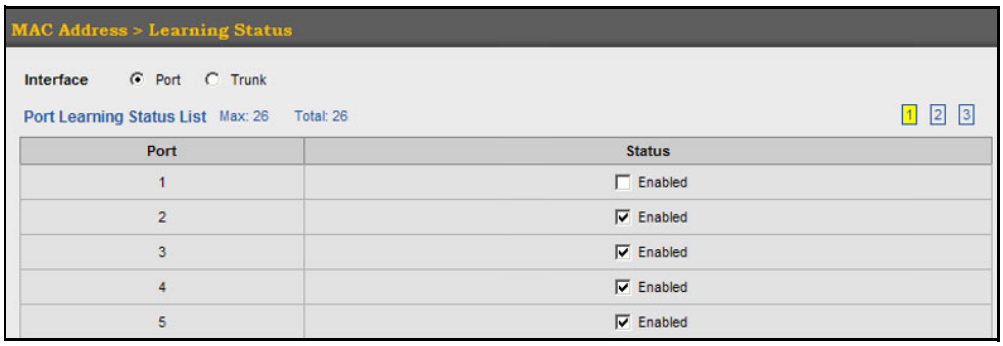
- **Trunk** – Trunk Identifier. (Range: 1-12)
- **Status** – The status of MAC address learning. (Default: Enabled)

WEB INTERFACE

To enable or disable MAC address learning in the web interface:

1. Click MAC Address, Learning Status.
2. Set the learning status for any interface.
3. Click Apply.

Figure 71: Configuring MAC Address Learning



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 738

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:

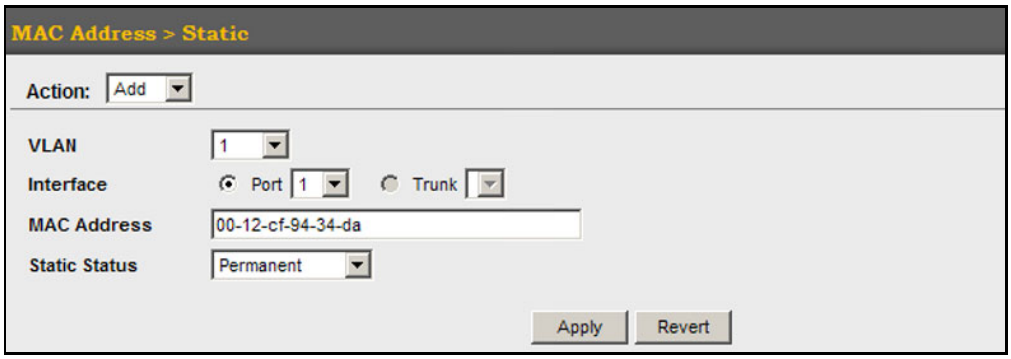
- **VLAN** – ID of configured VLAN. (Range: 1-4093)
- **Interface** – Port or trunk associated with the device assigned a static address.
- **MAC Address** – Physical address of a device mapped to this interface. Enter an address in the form of xx-xx-xx-xx-xx-xx or xxxxxxxxxxxx.
- **Static Status** – 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 in the web interface:

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.

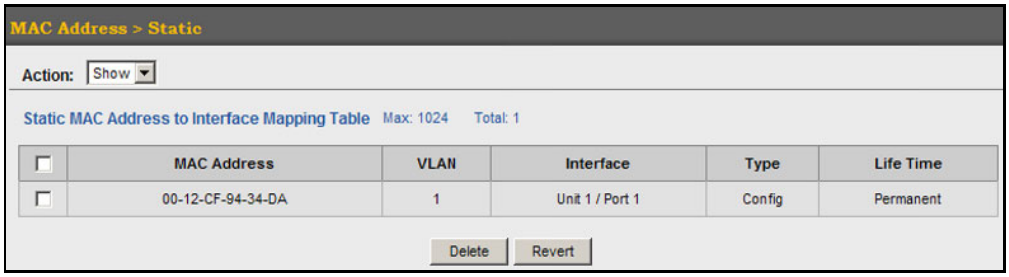
Figure 72: Configuring Static MAC Addresses



To show the static addresses in MAC address table in the web interface:

1. Click MAC Address, Static.
2. Select Show from the Action list.

Figure 73: Displaying Static MAC Addresses



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 737

PARAMETERS

These parameters are displayed in the web interface:

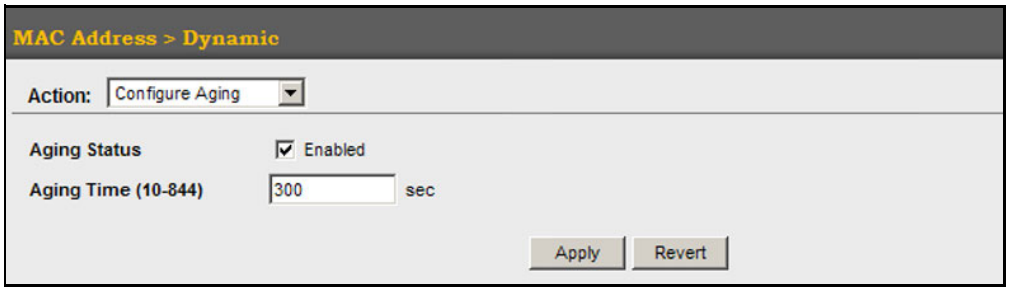
- **Aging Status** – Enables/disables the function.
- **Aging Time** – The time after which a learned entry is discarded. (Range: 10-1000000 seconds; Default: 300 seconds)

WEB INTERFACE

To set the aging time for entries in the dynamic address table in the web interface:

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 74: Setting the Address Aging Time



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 739

PARAMETERS

These parameters are displayed in the web interface:

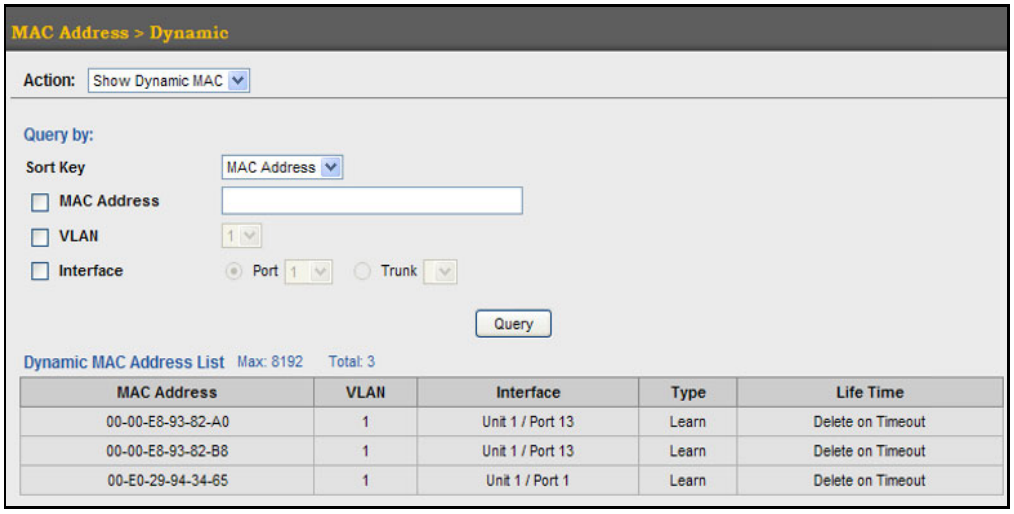
- **Sort Key** - You can sort the information displayed based on MAC address, VLAN or interface (port or trunk).
- **MAC Address** – Physical address associated with this interface.
- **VLAN** – ID of configured VLAN (1-4093).
- **Interface** – Indicates a port or trunk.
- **Type** – Shows that the entries in this table are learned.
- **Life Time** – Shows the time to retain the specified address.

WEB INTERFACE

To show the dynamic address table in the web interface:

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 75: Displaying the Dynamic MAC Address Table



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 739

PARAMETERS

These parameters are displayed in the web interface:

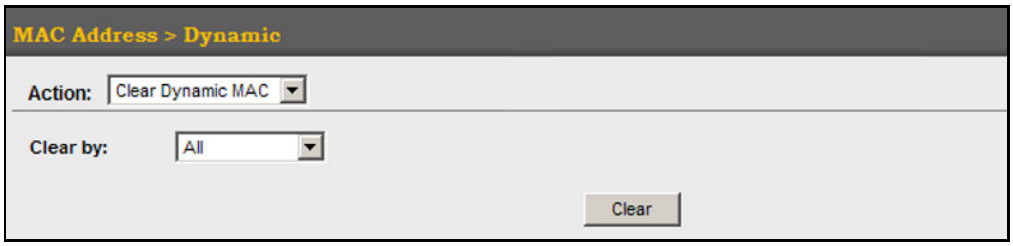
- **Clear by** – All entries can be cleared; or you can clear the entries for a specific MAC address, all the entries in a VLAN, or all the entries associated with a port or trunk.

WEB INTERFACE

To clear the entries in the dynamic address table in the web interface:

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 76: Clearing Entries in the Dynamic MAC Address Table



CONFIGURING MAC ADDRESS MIRRORING

Use the MAC Address > Mirror (Add) page to mirror traffic matching a specified source address from any port on the switch 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.

CLI REFERENCES

- "Local Port Mirroring Commands" on page 711

COMMAND USAGE

- When mirroring traffic from a MAC address, ingress traffic with the specified source address entering any port in the switch, other than the target port, will be mirrored to the destination port.
- All mirror sessions must share the same destination port.
- Spanning Tree BPDU packets are not mirrored to the target 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 185).
- When mirroring VLAN traffic (see "Configuring VLAN Mirroring" on page 174) or packets based on a source MAC address, the target port cannot be set to the same target ports as that used for port mirroring (see "Configuring Local Port Mirroring" on page 117).
- When traffic matches the rules for both port mirroring, and for mirroring of VLAN traffic or packets based on a MAC address, the matching packets will not be sent to target port specified for port mirroring.

PARAMETERS

These parameters are displayed in the web interface:

- **Source MAC** – MAC address in the form of xx-xx-xx-xx-xx-xx or xxxxxxxxxxxx.

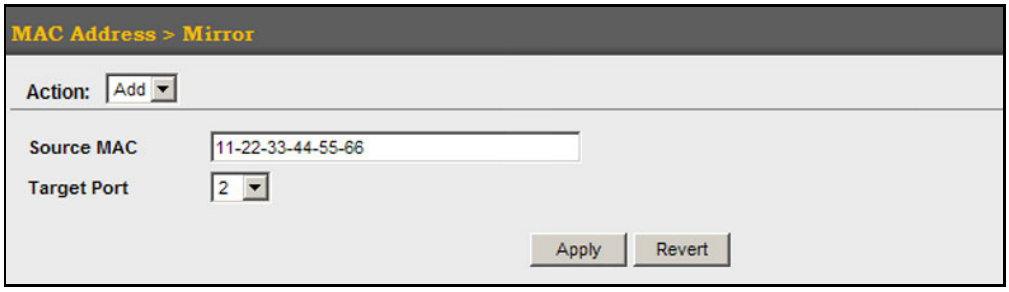
- **Target Port** – The port that will mirror the traffic from the source port. (ES-3026/P: 1-26, ES-3024G/P: 1-24)

WEB INTERFACE

To mirror packets based on a MAC address in the web interface:

1. Click MAC Address, Mirror.
2. Select Add from the Action list.
3. Specify the source MAC address and destination port.
4. Click Apply.

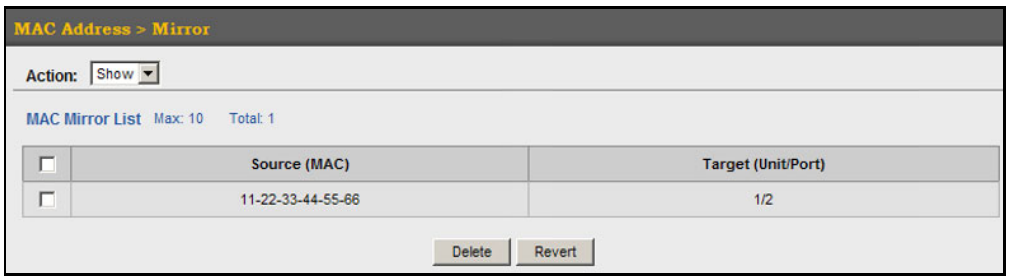
Figure 77: Mirroring Packets Based on the Source MAC Address



To show the MAC addresses to be mirrored in the web interface:

1. Click MAC Address, Mirror.
2. Select Show from the Action list.

Figure 78: Showing the Source MAC Addresses to Mirror



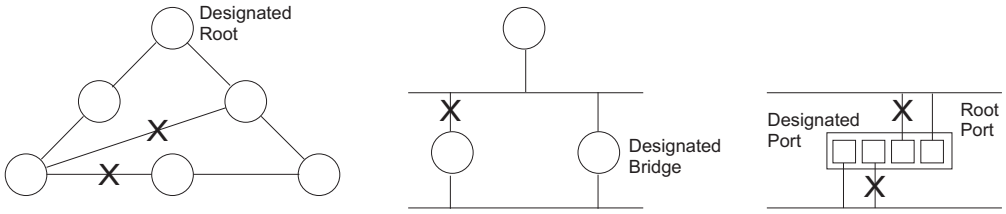
8 SPANNING TREE ALGORITHM

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)

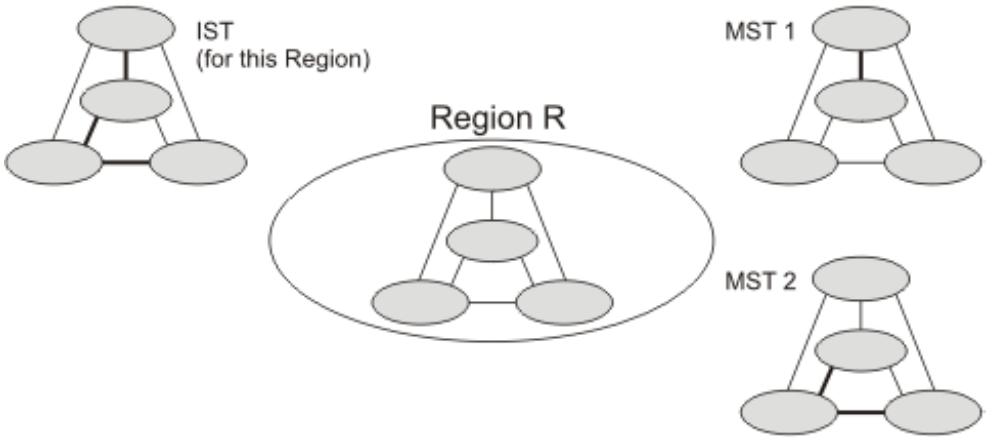
STP – STP uses a distributed algorithm to select a bridging device (STP-compliant switch, bridge or router) that serves as the root of the spanning tree network. It selects a root port on each bridging device (except for the root device) which incurs the lowest path cost when forwarding a packet from 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.



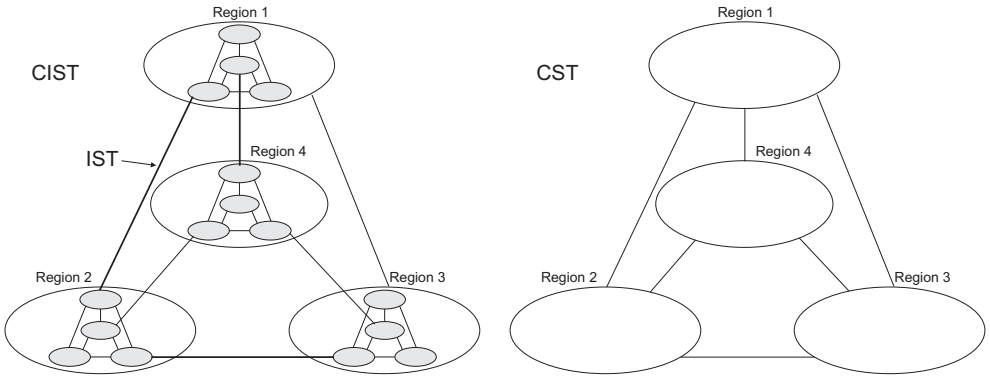
Once a stable network topology has been established, all bridges listen for Hello BPDUs (Bridge Protocol Data Units) transmitted from the Root Bridge. If a bridge does not get a Hello BPDU after a predefined interval (Maximum Age), the bridge assumes that the link to the Root Bridge is down. This bridge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



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 201). 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.



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 770

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)

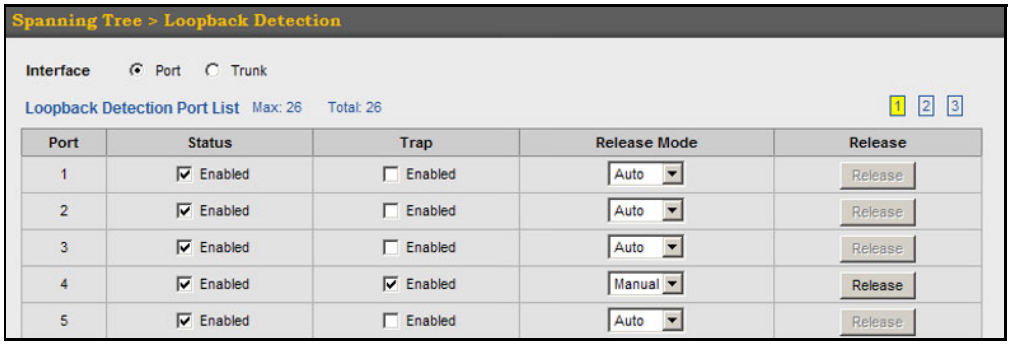
- **Trap** – Enables SNMP trap notification for loopback events on this interface. (Default: Disabled)
- **Release Mode** – Configures the interface for automatic or manual loopback release. (Default: Auto)
- **Release** – Allows an interface to be manually released from discard mode. This is only available if the interface is configured for manual release mode.

WEB INTERFACE

To configure loopback detection in the web interface:

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 79: Configuring Port Loopback Detection



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 741

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:

  - STP Mode – If the switch receives an 802.1D BPDU (i.e., STP BPDU) after a port's migration delay timer expires, the switch assumes it is connected to an 802.1D bridge and starts using only 802.1D BPDUs.

  - RSTP Mode – If RSTP is using 802.1D BPDUs on a port and receives an RSTP BPDU after the migration delay expires, RSTP restarts the migration delay timer and begins using RSTP BPDUs on that port.

- Multiple Spanning Tree Protocol

  MSTP generates a unique spanning tree for each instance. This provides multiple pathways across the network, thereby balancing the traffic load, preventing wide-scale disruption when a bridge node in a single instance fails, and allowing for faster convergence of a new topology for the failed instance.

  - To allow multiple spanning trees to operate over the network, you must configure a related set of bridges with the same MSTP configuration, allowing them to participate in a specific set of spanning tree instances.

  - A spanning tree instance can exist only on bridges that have compatible VLAN instance assignments.

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

- Be careful when switching between spanning tree modes. Changing modes stops all spanning-tree instances for the previous mode and restarts the system in the new mode, temporarily disrupting user traffic.

PARAMETERS

These parameters are displayed 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

- **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 RSTP

The following attributes apply to both RSTP and MSTP:

- **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)

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)
- **Maximum Hop Count** – The maximum number of hops allowed in the MST region before a BPDU is discarded. (Range: 1-40; Default: 20)

2. The MST name and revision number are both required to uniquely identify an MST region.

WEB INTERFACE

To configure global STA settings in the web interface:

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

Figure 80: Configuring Global Settings for STA (STP)

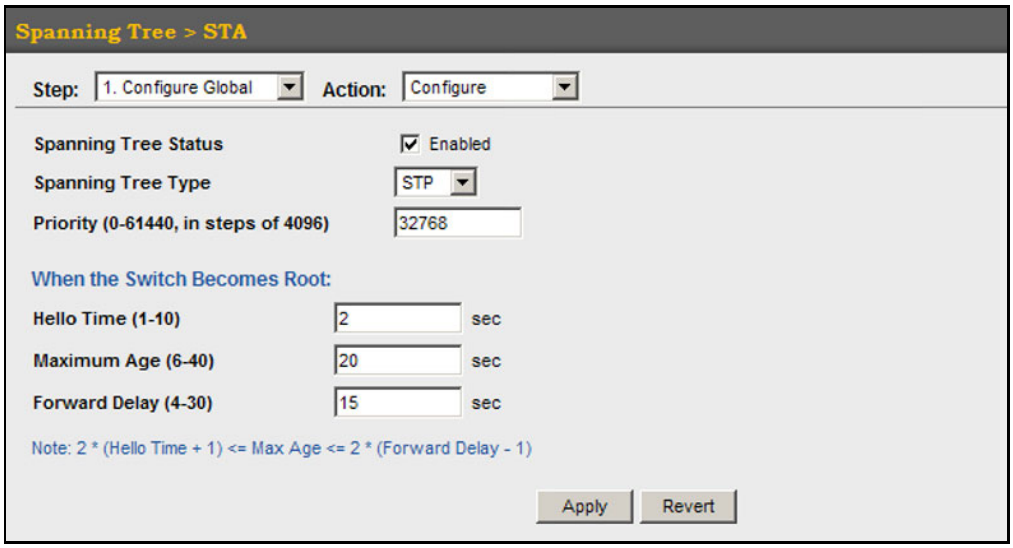


Figure 81: Configuring Global Settings for STA (RSTP)

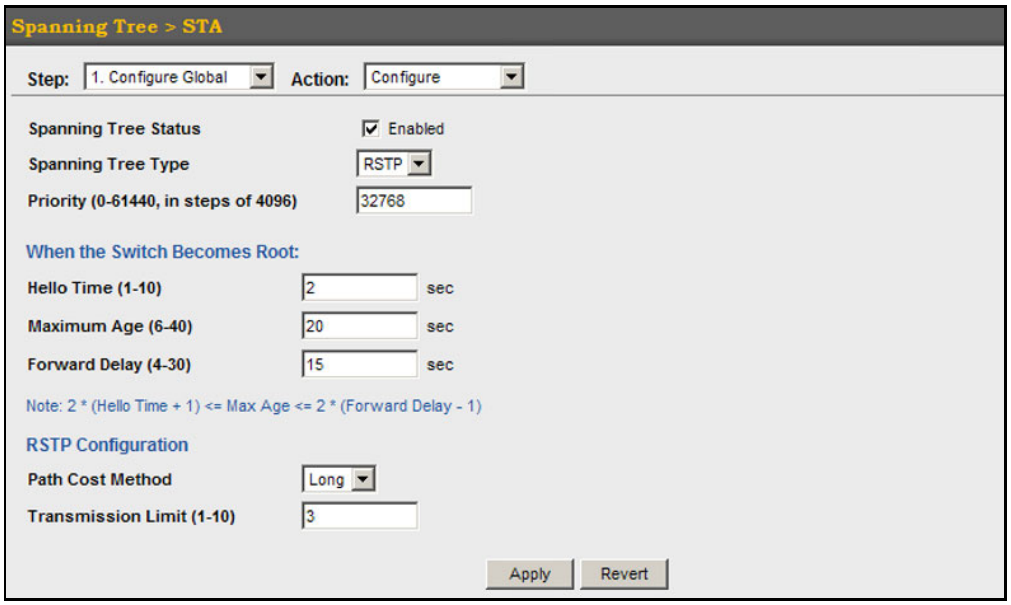
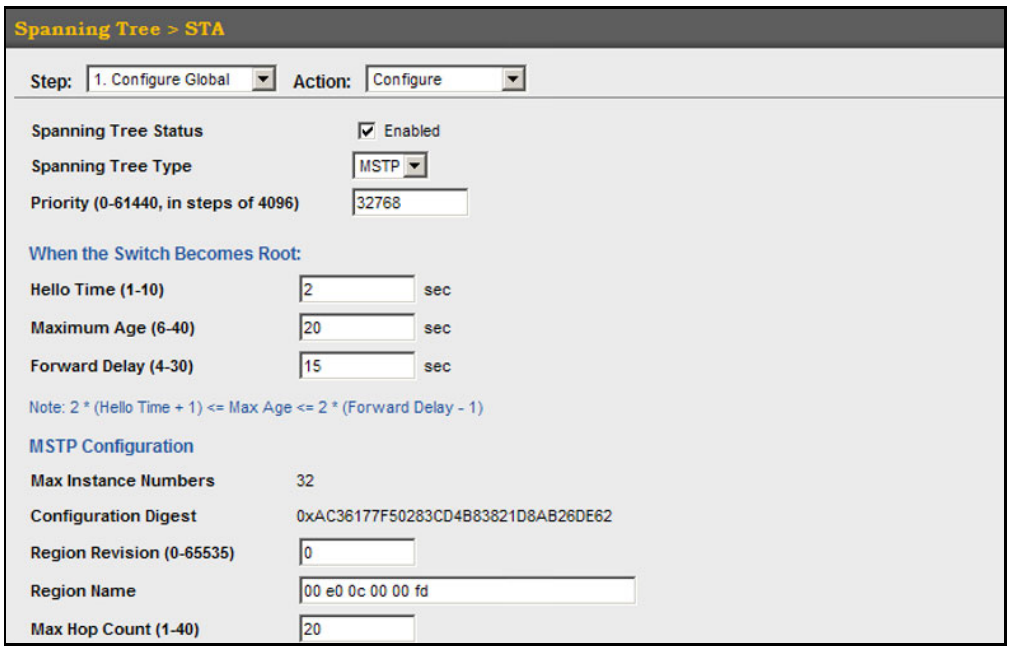


Figure 82: Configuring Global Settings for STA (MSTP)



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 763
- "show spanning-tree mst configuration" on page 764

PARAMETERS

The parameters displayed in the web interface are described in the preceding section, except for the following items:

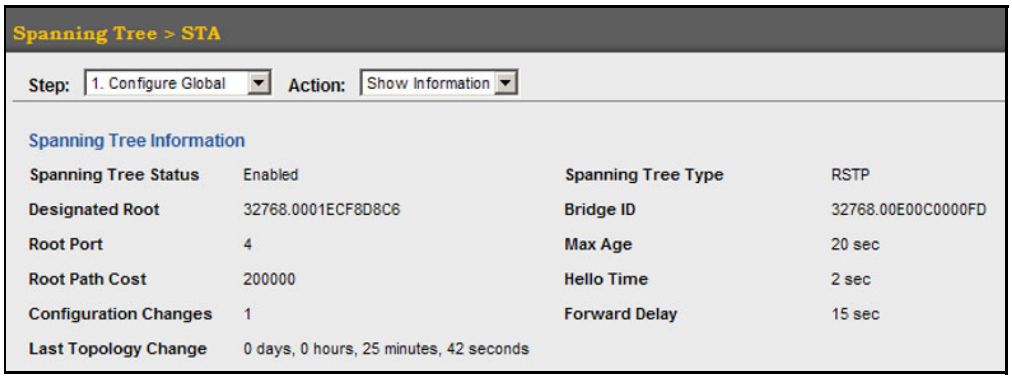
- **Bridge ID** – A unique identifier for this bridge, consisting of the bridge priority, the MST Instance ID 0 for the Common Spanning Tree when spanning tree type is set to MSTP, and MAC address (where the address is taken from the switch system).
- **Designated Root** – The priority and MAC address 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 in the web interface:

1. Click Spanning Tree, STA.
2. Select Configure Global from the Step list.
3. Select Show Information from the Action list.

Figure 83: Displaying Global Settings for STA



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 741

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. Note that path cost takes precedence over

port priority. (Range: 0 for auto-configuration, 1-65535 for the short path cost method[3], 1-200,000,000 for the long path cost method)

By default, the system automatically detects the speed and duplex mode used on each port, and configures the path cost according to the values shown below. Path cost "0" is used to indicate auto-configuration mode. When the short path cost method is selected and the default path cost recommended by the IEEE 8021w standard exceeds 65,535, the default is set to 65,535.

Table 9: Recommended STA Path Cost Range

Port Type	IEEE 802.1D-1998	IEEE 802.1w-2001
Ethernet	50-600	200,000-20,000,000
Fast Ethernet	10-60	20,000-2,000,000
Gigabit Ethernet	3-10	2,000-200,000

Table 10: Recommended STA Path Costs

Port Type	Link Type	IEEE 802.1D-1998	IEEE 802.1w-2001
Ethernet	Half Duplex	100	2,000,000
	Full Duplex	95	1,999,999
	Trunk	90	1,000,000
Fast Ethernet	Half Duplex	19	200,000
	Full Duplex	18	100,000
	Trunk	15	50,000
Gigabit Ethernet	Full Duplex	4	10,000
	Trunk	3	5,000

Table 11: Default STA Path Costs

Port Type	IEEE 802.1D-1998	IEEE 802.1w-2001
Ethernet	Half Duplex	2,000,000
	Full Duplex	1,000,000
	Trunk	500,000
Fast Ethernet	Half Duplex	200,000
	Full Duplex	100,000
	Trunk	50,000
Gigabit Ethernet	Full Duplex	10,000
	Trunk	5,000

- **Admin Link Type** – The link type attached to this interface.
  - Point-to-Point – A connection to exactly one other bridge.
  - Shared – A connection to two or more bridges.
  - Auto – The switch automatically determines if the interface is attached to a point-to-point link or to shared media. (This is the default setting.)

3. Refer to "Configuring Global Settings for STA" on page 189 for information on setting the path cost method.

- **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 189).

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

  - If spanning tree mode is set to STP (page 189), edge-port mode can be manually enabled or set to auto, but will have no effect.

  - If loopback detection is enabled (page 187) 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 199).

- **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)

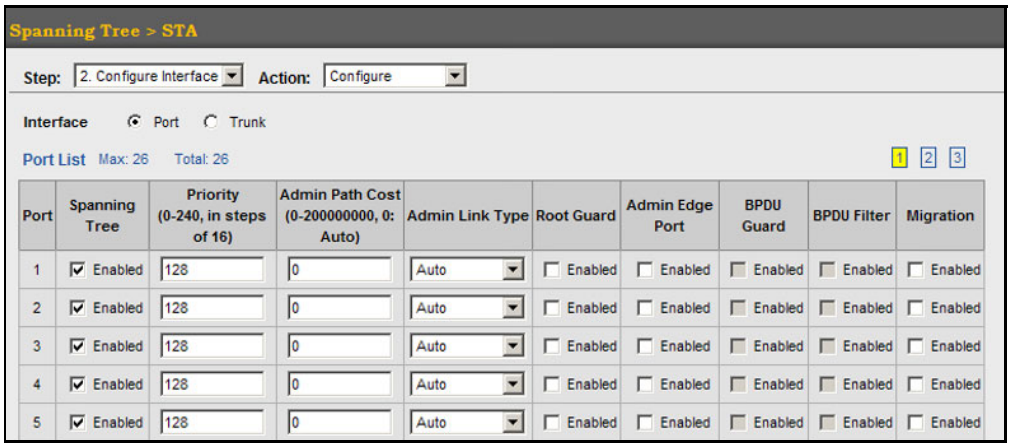
- **Migration** – If at any time the switch detects STP BPDUs, including Configuration or Topology Change Notification BPDUs, it will automatically set the selected interface to forced STP-compatible mode. However, you can also use the Protocol Migration button to manually re-check the appropriate BPDU format (RSTP or STP-compatible) to send on the selected interfaces. (Default: Disabled)

WEB INTERFACE

To configure interface settings for STA in the web interface:

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 84: Configuring Interface Settings for STA



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 763

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:

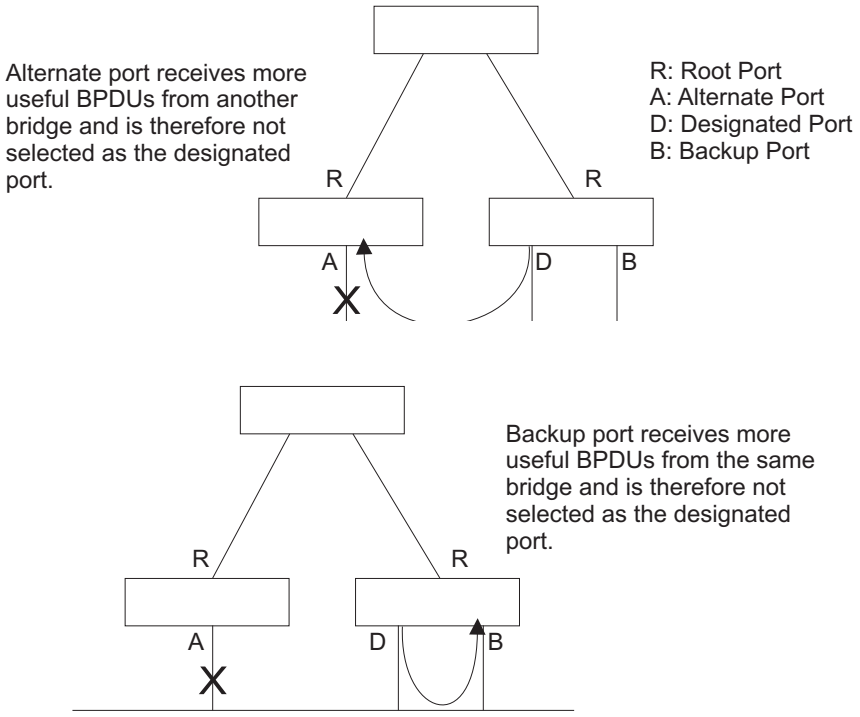
  - A port on a network segment with no other STA compliant bridging device is always forwarding.
  - If two ports of a switch are connected to the same segment and there is no other STA device attached to this segment, the port with the smaller ID forwards packets and the other is discarding.
  - All 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 195.

- **Oper Edge Port** – This parameter is initialized to the setting for Admin Edge Port in STA Port Configuration on page 195 (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.



WEB INTERFACE

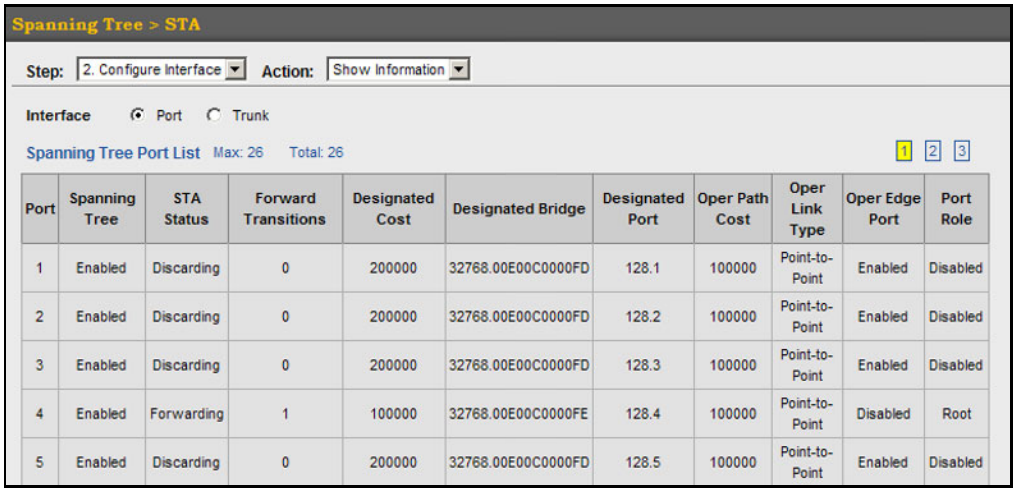
To display interface settings for STA in the web interface:

1. Click Spanning Tree, STA.

2. Select Configure Interface from the Step list.

3. Select Show Information from the Action list.

Figure 85: Displaying Interface Settings for STA



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	Discarding	0	200000	32768.00E00C0000FD	128.1	100000	Point-to-Point	Enabled	Disabled
2	Enabled	Discarding	0	200000	32768.00E00C0000FD	128.2	100000	Point-to-Point	Enabled	Disabled
3	Enabled	Discarding	0	200000	32768.00E00C0000FD	128.3	100000	Point-to-Point	Enabled	Disabled
4	Enabled	Forwarding	1	100000	32768.00E00C0000FE	128.4	100000	Point-to-Point	Disabled	Root
5	Enabled	Discarding	0	200000	32768.00E00C0000FD	128.5	100000	Point-to-Point	Enabled	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 741

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 189) 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 189).
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:

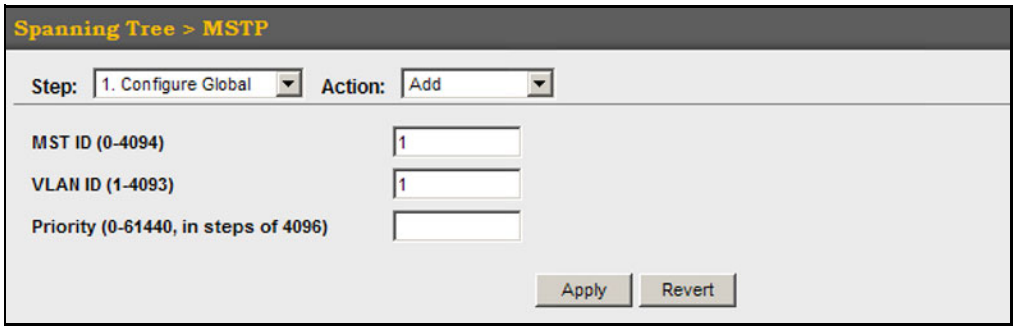
- **MST ID** – Instance identifier to configure. (Range: 0-4094)
- **VLAN ID** – VLAN to assign to this MST instance. (Range: 1-4093)
- **Priority** – The priority of a spanning tree instance. (Range: 0-61440 in steps of 4096; Options: 0, 4096, 8192, 12288, 16384, 20480, 24576, 28672, 32768, 36864, 40960, 45056, 49152, 53248, 57344, 61440; Default: 32768)

WEB INTERFACE

To create instances for MSTP in the web interface:

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.

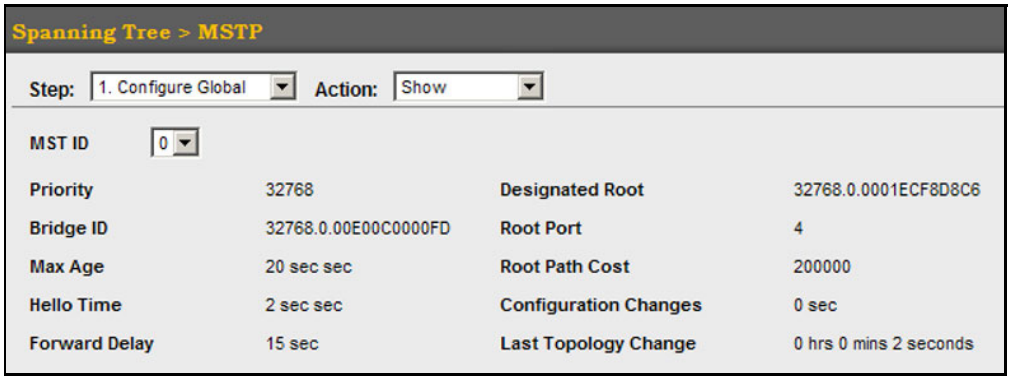
Figure 86: Creating an MST Instance



To show the MSTP instances in the web interface:

1. Click Spanning Tree, MSTP.
2. Select Configure Global from the Step list.
3. Select Show from the Action list. The attributes displayed on this page are described under "Displaying Global Settings for STA" on page 194.

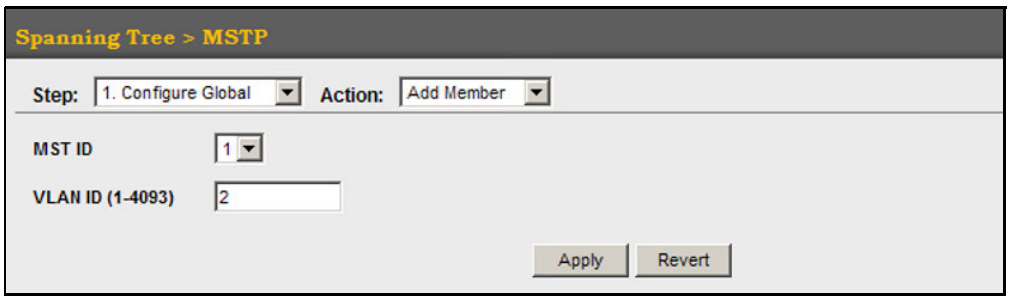
Figure 87: Displaying STA Settings for an MST Instance



To add additional VLAN groups to an MSTP instance in the web interface:

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

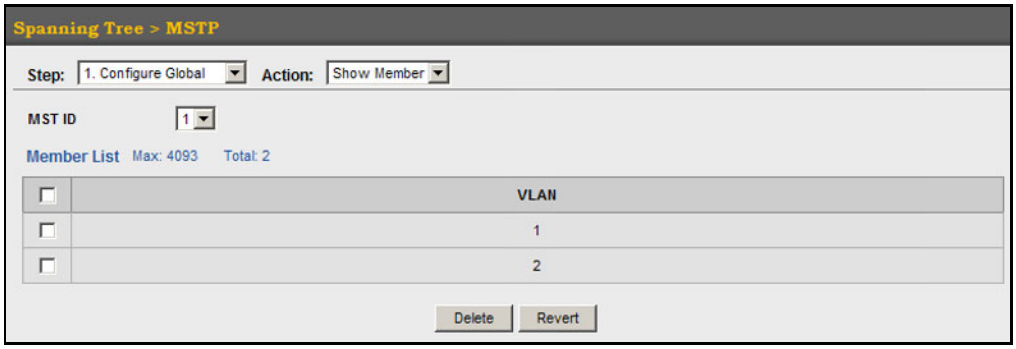
Figure 88: Adding a VLAN to an MST Instance



To show the VLAN member of an MSTP instance in the web interface:

1. Click Spanning Tree, MSTP.
2. Select Configure Global from the Step list.
3. Select Show Member from the Action list.

Figure 89: Displaying Members of an MST Instance



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 741

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 199 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

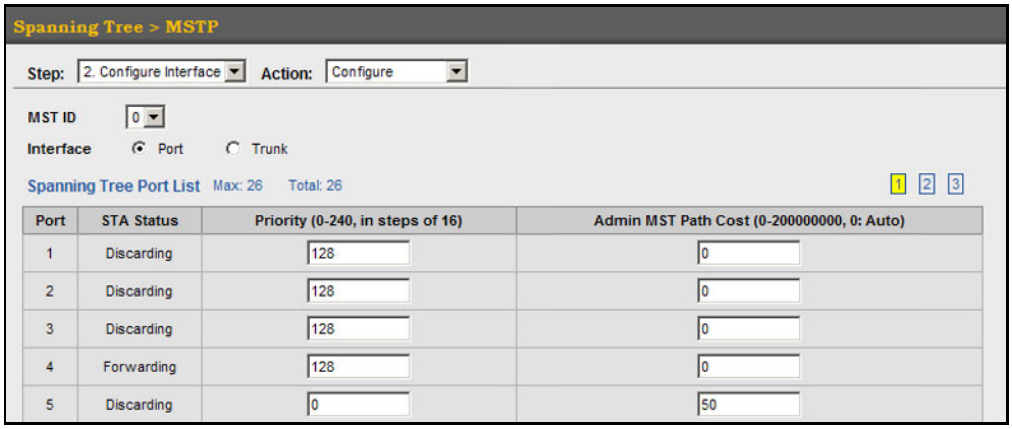
  The recommended range is listed in Table 9 on page 196.
  The recommended path cost is listed in Table 10 on page 196.
  The default path costs are listed in Table 11 on page 196.

WEB INTERFACE

To configure MSTP parameters for a port or trunk in the web interface:

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.

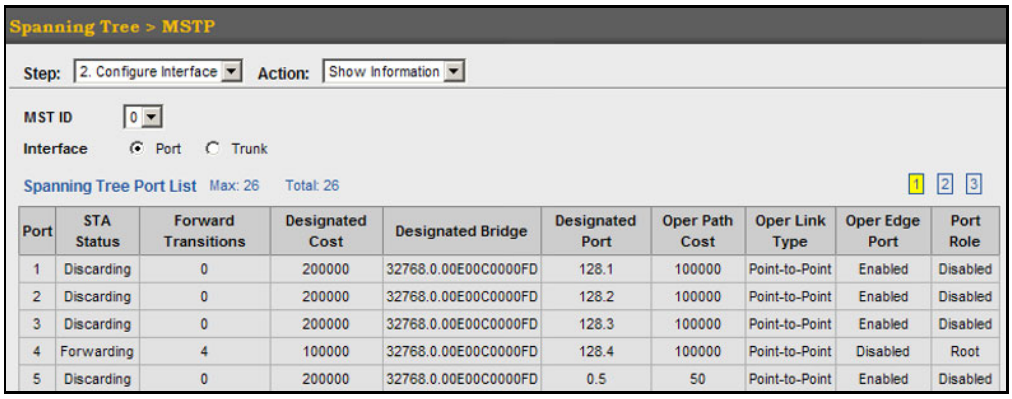
Figure 90: Configuring MSTP Interface Settings



To display MSTP parameters for a port or trunk in the web interface:

1. Click Spanning Tree, MSTP.
2. Select Configure Interface from the Step list.
3. Select Show Information from the Action list.

Figure 91: Displaying MSTP Interface Settings



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. 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 721

PARAMETERS

These parameters are displayed in the web interface:

- **Port** – Displays the port number.
- **Type** – Indicates the port type. (100Base-TX, 1000Base-T, or SFP)
- **Status** – Enables or disables the rate limit. (Default: Disabled)
- **Rate** – Sets the rate limit level. (Range: 64 - 100,000 kbits per second for Fast Ethernet ports; 64 - 1,000,000 kbits per second for Gigabit Ethernet ports)

WEB INTERFACE

To configure rate limits in the web interface:

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 92: Configuring Rate Limits

Traffic > Rate Limit

Port Rate Limit List Max: 26 Total: 26 1 2 3

Port	Type	Input		Output	
		Status	Rate (kbits/sec)	Status	Rate (kbits/sec)
1	100Base-TX	☐ Enabled	64 (64-100000)	☐ Enabled	100000 (64-100000)
2	100Base-TX	☐ Enabled	64 (64-100000)	☐ Enabled	100000 (64-100000)
3	100Base-TX	☑ Enabled	50 (64-100000)	☑ Enabled	50 (64-100000)
4	100Base-TX	☐ Enabled	64 (64-100000)	☐ Enabled	100000 (64-100000)
5	100Base-TX	☐ Enabled	64 (64-100000)	☐ Enabled	100000 (64-100000)

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 685

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-TX, 100Base-T, or SFP)
- **Unknown Unicast** – Specifies storm control for unknown unicast traffic.
- **Multicast** – Specifies storm control for multicast traffic.
- **Broadcast** – Specifies storm control for broadcast traffic.
- **Status** – Enables or disables storm control. (Default: Enabled for broadcast storm control, disabled for multicast and unknown unicast storm control)
- **Rate** – Threshold level as a rate; i.e., packets per second. (Range: 64-1,000,000 kbits per second; Default: 64 kbits per second)

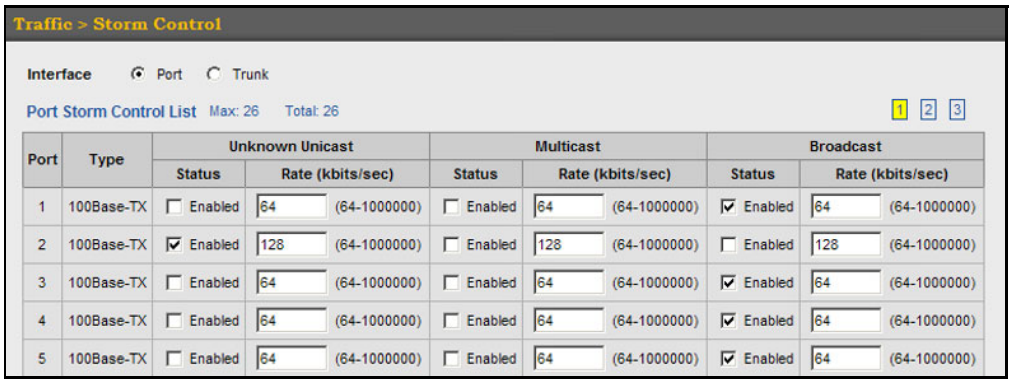
NOTE: Only one rate is supported for all traffic types on an interface.

WEB INTERFACE

To configure broadcast storm control in the web interface:

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 93: Configuring Broadcast Storm Control



Port	Type	Unknown Unicast		Multicast		Broadcast	
		Status	Rate (kbits/sec)	Status	Rate (kbits/sec)	Status	Rate (kbits/sec)
1	100Base-TX	☐ Enabled	64 (64-1000000)	☐ Enabled	64 (64-1000000)	☑ Enabled	64 (64-1000000)
2	100Base-TX	☑ Enabled	128 (64-1000000)	☐ Enabled	128 (64-1000000)	☐ Enabled	128 (64-1000000)
3	100Base-TX	☐ Enabled	64 (64-1000000)	☐ Enabled	64 (64-1000000)	☑ Enabled	64 (64-1000000)
4	100Base-TX	☐ Enabled	64 (64-1000000)	☐ Enabled	64 (64-1000000)	☑ Enabled	64 (64-1000000)
5	100Base-TX	☐ Enabled	64 (64-1000000)	☐ Enabled	64 (64-1000000)	☑ Enabled	64 (64-1000000)

11 CLASS OF SERVICE

Class of Service (CoS) allows you to specify which data packets have greater precedence when traffic is buffered in the switch due to congestion. This switch supports CoS with four priority queues for each port. Data packets in a port's high-priority queue will be transmitted before those in the lower-priority queues. You can set the default priority for each interface, and configure the mapping of frame priority tags to the switch's priority queues.

LAYER 2 QUEUE SETTINGS

This section describes how to configure the default priority for untagged frames, set the queue mode, set the weights assigned to each queue, and map class of service tags to queues.

SETTING THE DEFAULT PRIORITY FOR INTERFACES

Use the Traffic > Priority > Default Priority page to specify the default port priority for each interface on the switch. All untagged packets entering the switch are tagged with the specified default port priority, and then sorted into the appropriate priority queue at the output port.

CLI REFERENCES

- "switchport priority default" on page 804

COMMAND USAGE

- This switch provides four priority queues for each port. It uses Weighted Round Robin to prevent head-of-queue blockage.
- The default priority applies for an untagged frame received on a port set to accept all frame types (i.e, receives both untagged and tagged frames). This priority does not apply to IEEE 802.1Q VLAN tagged frames. If the incoming frame is an IEEE 802.1Q VLAN tagged frame, the IEEE 802.1p User Priority bits will be used.
- If the output port is an untagged member of the associated VLAN, these frames are stripped of all VLAN tags prior to transmission.

PARAMETERS

These parameters are displayed in the web interface:

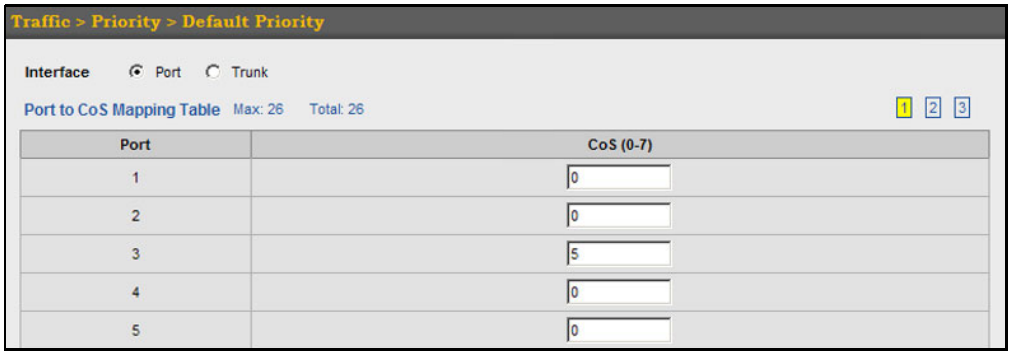
- **Interface** – Displays a list of ports or trunks.
- **CoS** – The priority that is assigned to untagged frames received on the specified interface. (Range: 0-7; Default: 0)

WEB INTERFACE

To configure the queue mode in the web interface:

1. Click Traffic, Priority, Default Priority.
2. Select the interface type to display (Port or Trunk).
3. Modify the default priority for any interface.
4. Click Apply.

Figure 94: Setting the Default Port Priority



SELECTING THE QUEUE MODE

Use the Traffic > Priority > Queue page to set the queue mode for the egress queues on any interface. The switch can be set to service the queues based on a strict rule that requires all traffic in a higher priority queue to be processed before the lower priority queues are serviced, Shaped Deficit Weighted Round-Robin (SDWRR) queuing that specifies a scheduling weight for each queue. SDWRR is labelled WRR in the menu. It can also be configured to use a combination of strict and weighted queuing.

CLI REFERENCES

- "queue mode" on page 802
- "show queue mode" on page 805

COMMAND USAGE

- Strict priority requires all traffic in a higher priority queue to be processed before lower priority queues are serviced.

- The WRR algorithm used by this switch is known as Shaped Deficit Weighted Round Robin (SDWRR).

  The basic WRR algorithm uses a 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.

  Deficit Weighted Round-Robin (DWRR) services the queues in a manner similar to WRR, but the next queue is serviced only when the queue's

Deficit Counter becomes smaller than the packet size to be transmitted. As a result, traffic on queues with large weights cause increased latency and jitter for traffic waiting for scheduling other queues. In SDWRR, if two or more queues have traffic eligible for transmission (i.e. the Deficit Counter is greater than the packet size to be transmitted), then a round-robin scheme among those queues is used, while still preserving the overall weight ratios between the queues. This produces less jitter and lower maximum latency for traffic on all of the serviced 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 SWDRR, or the queuing mode that uses a combination of strict and weighted queuing. Service time is allocated to each queue by calculating a precise number of bytes per second that will be serviced on each round.

- The specified queue mode applies to all interfaces.

PARAMETERS

These parameters are displayed in the web interface:

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

- **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** (SWDRR) – Shares bandwidth at the egress ports by using scheduling weights, servicing each queue in a round-robin fashion.

  - **Strict and WRR** – Uses strict priority on the high-priority queues and SDWRR for the rest of the queues. (This is the default setting.)

- **Queue ID** – The ID of the priority queue. (Range: 0-7)

- **Strict Mode** – If “Strict and WRR” mode is selected, then a combination of strict service is used for the high priority queues and weighted service for the remaining queues. Use this parameter to specify the queues assigned to use strict priority when using the strict-weighted queuing mode. (Default: Strict and WRR mode, with Queue 3 using strict mode)

- **Weight** – Sets a weight for each queue which is used by the SDWRR scheduler. (Range: 1-255; Default: Weights 1, 2, 4, 6 are assigned to queues 0 - 3 respectively)

WEB INTERFACE

To configure the queue mode in the web interface:

1. Click Traffic, Priority, Queue.
2. Set the queue mode.
3. If the weighted queue mode is selected, the queue weight can be modified if required.
4. If the queue modes that uses a combination of strict and weighted queueing is selected, the queues which are serviced first must be specified by enabling strict mode parameter in the table.
5. Click Apply.

Figure 95: Setting the Queue Mode (Strict)

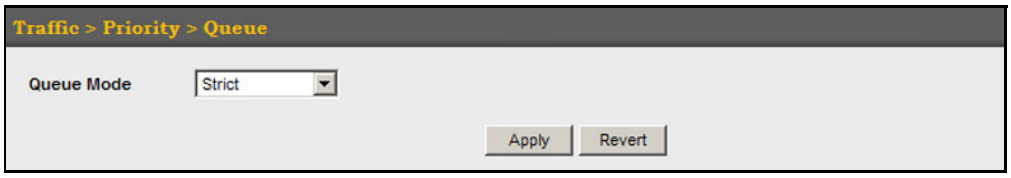


Figure 96: Setting the Queue Mode (WRR)

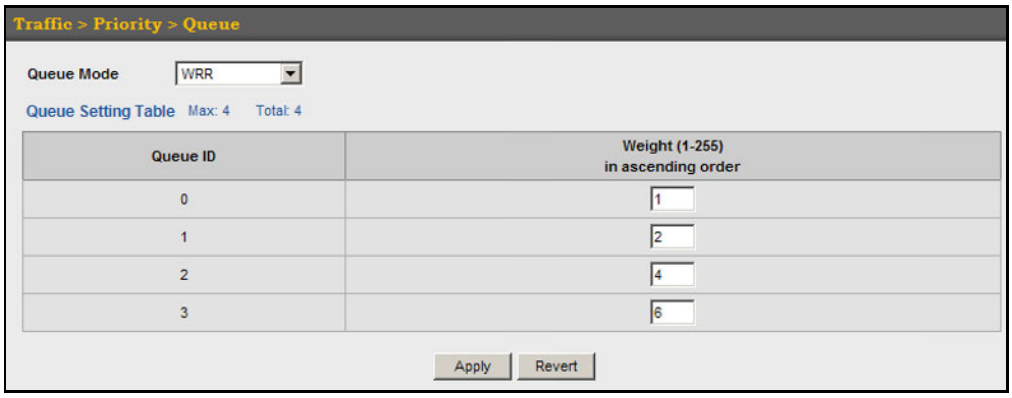
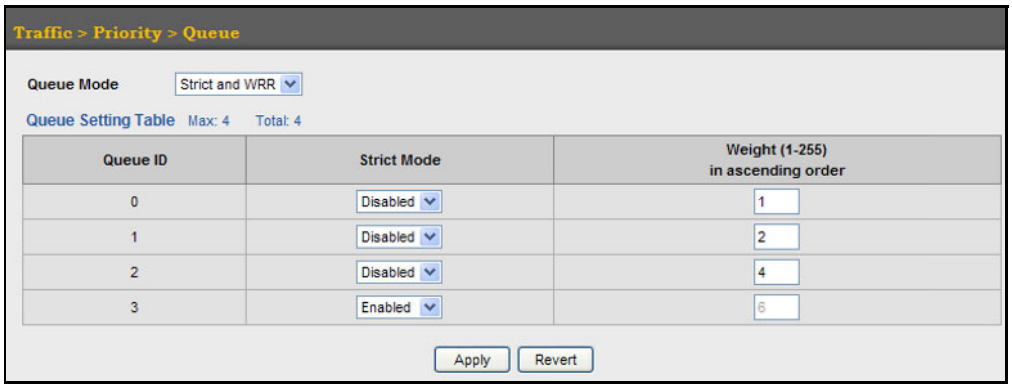


Figure 97: Setting the Queue Mode (Strict and WRR)



MAPPING COS VALUES TO EGRESS QUEUES

Use the Traffic > Priority > PHB to Queue page to specify the hardware output queues to use based on the internal per-hop behavior value. (For more information on exact manner in which the ingress priority tags are mapped to egress queues for internal processing, see "Mapping CoS Priorities to Internal DSCP Values" on page 222).

The switch processes Class of Service (CoS) priority tagged traffic by using four priority queues for each port, with service schedules based on strict priority, Shaped Deficit Weighted Round-Robin (SDWRR), or a combination of strict and weighted queuing. Up to eight separate traffic priorities are defined in IEEE 802.1p. Default priority levels are assigned according to recommendations in the IEEE 802.1p standard as shown in Table 12. The following table indicates the default mapping of internal per-hop behavior to the hardware queues. The actual mapping may differ if the CoS priorities to internal DSCP values have been modified (page 222).

Table 12: IEEE 802.1p Egress Queue Priority Mapping

Priority	0	1	2	3	4	5	6	7
Queue	1	0	0	1	2	2	3	3

The priority levels recommended in the IEEE 802.1p standard for various network applications are shown in Table 13. However, priority levels can be mapped to the switch's output queues in any way that benefits application traffic for the network.

Table 13: CoS Priority Levels

Priority Level	Traffic Type
1	Background
2	(Spare)
0 (default)	Best Effort
3	Excellent Effort
4	Controlled Load
5	Video, less than 100 milliseconds latency and jitter

Table 13: CoS Priority Levels (Continued)

Priority Level	Traffic Type
6	Voice, less than 10 milliseconds latency and jitter
7	Network Control

CLI REFERENCES

- "qos map phb-queue" on page 809

COMMAND USAGE

- Egress packets are placed into the hardware queues according to the mapping defined by this command.
- The default internal PHB to output queue mapping is shown below.

Table 14: Mapping Internal Per-hop Behavior to Hardware Queues

Per-hop Behavior	0	1	2	3	4	5	6	7
Hardware Queues	1	0	0	1	2	2	3	3

- The specified mapping applies to all interfaces.

PARAMETERS

These parameters are displayed in the web interface:

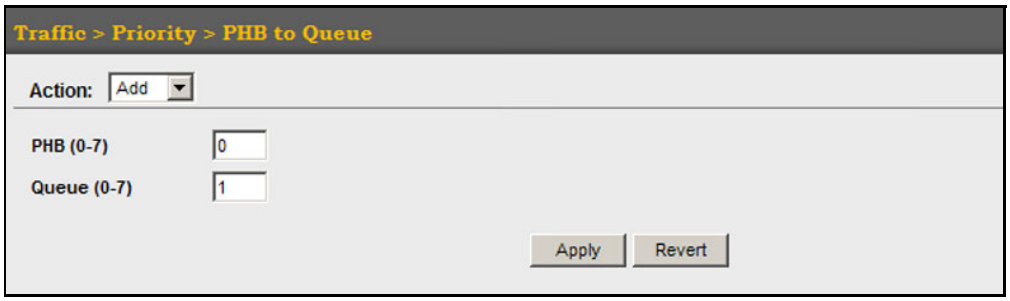
- **PHB** – Per-hop behavior, or the priority used for this router hop. (Range: 0-7, where 7 is the highest priority)
- **Queue** – Output queue buffer. (Range: 0-3, where 3 is the highest CoS priority queue)

WEB INTERFACE

To map internal PHB to hardware queues in the web interface:

1. Click Traffic, Priority, PHB to Queue.
2. Select Add from the Action list.
3. Select an interface.
4. Set the queue mode.
5. Map an internal PHB to a hardware queue. Depending on how an ingress packet is processed internally based on its CoS value, and the assigned output queue, the mapping done on this page can effectively determine the service priority for different traffic classes.
6. Click Apply.

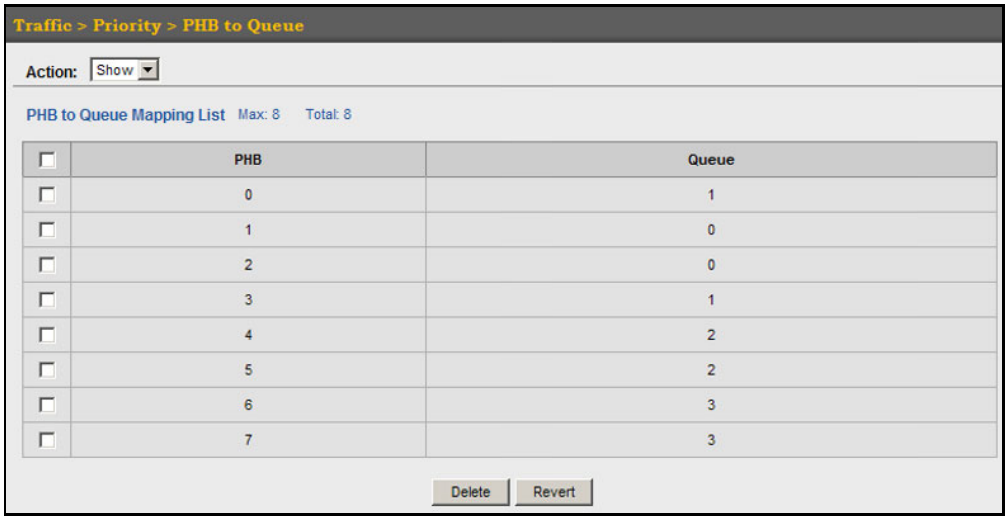
Figure 98: Mapping CoS Values to Egress Queues



To show the internal PHB to hardware queue map in the web interface:

1. Click Traffic, Priority, PHB to Queue.
2. Select Show from the Action list.
3. Select an interface.

Figure 99: Showing CoS Values to Egress Queues



PHB	Queue
0	1
1	0
2	0
3	1
4	2
5	2
6	3
7	3

LAYER 3/4 PRIORITY SETTINGS

Mapping Layer 3 / 4 Priorities to CoS Values

The switch supports several common methods of prioritizing layer 3/4 traffic to meet application requirements. Traffic priorities can be specified in the IP header of a frame, using the priority bits in the Type of Service (ToS) octet, or the number of the TCP/UDP port. If priority bits are used, the ToS octet may contain three bits for IP Precedence or six bits for Differentiated Services Code Point (DSCP) service. When these services are enabled, the priorities are mapped to a Class of Service value by the switch, and the traffic then sent to the corresponding output queue.

Because different priority information may be contained in the traffic, this switch maps priority values to the output queues in the following manner – The precedence for priority mapping is DSCP Priority and then Default Port Priority.

NOTE: The default settings used for mapping priority values from ingress traffic to internal DSCP values are used to determine the hardware queues used for egress traffic, not to replace the priority values. These defaults are designed to optimize priority services for the majority of network applications. It should not be necessary to modify any of the default settings, unless a queuing problem occurs with a particular application.

SETTING PRIORITY PROCESSING TO DSCP OR COS

The switch allows a choice between using DSCP or CoS priority processing methods. Use the Priority > Trust Mode page to select the required processing method.

CLI REFERENCES

- "qos map trust-mode" on page 810

COMMAND USAGE

- If the QoS mapping mode is set to DSCP, and the ingress packet type is IPv4, then priority processing will be based on the DSCP value in the ingress packet.

- If the QoS mapping mode is set to DSCP, and a non-IP packet is received, the packet's CoS and CFI (Canonical Format Indicator) values are used for priority processing if the packet is tagged. For an untagged packet, the default port priority (see page 211) is used for priority processing.

- If the QoS mapping mode is set to CoS, and the ingress packet type is IPv4, then priority processing will be based on the CoS and CFI values in the ingress packet.

  For an untagged packet, the default port priority (see page 211) is used for priority processing.

PARAMETERS

These parameters are displayed in the web interface:

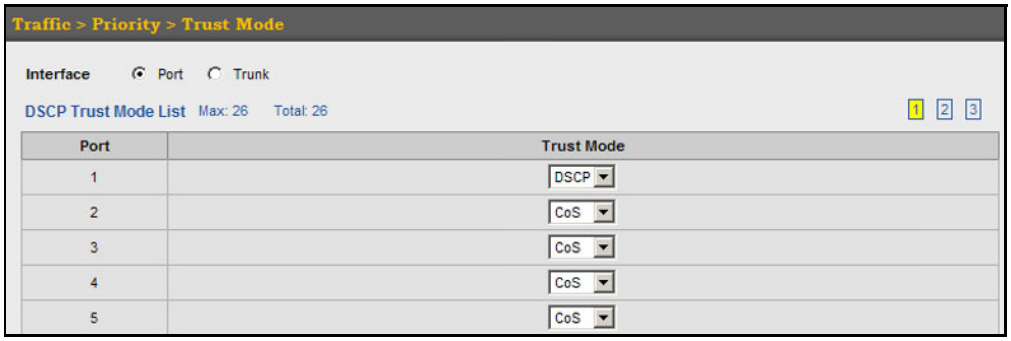
- **Interface** – Specifies a port or trunk.
- **Trust Mode**
  - **DSCP** – Maps layer 3/4 priorities using Differentiated Services Code Point values.
  - **CoS** – Maps layer 3/4 priorities using Class of Service values. (This is the default setting.)

WEB INTERFACE

To configure the trust mode in the web interface:

1. Click Traffic, Priority, Trust Mode.
2. Select the interface type to display (Port or Trunk).
3. Set the trust mode.
4. Click Apply.

Figure 100: Setting the Trust Mode



MAPPING INGRESS DSCP VALUES TO INTERNAL DSCP VALUES

Use the Traffic > Priority > DSCP to DSCP page to map DSCP values in incoming packets to per-hop behavior and drop precedence values for internal priority processing.

The DSCP is six bits wide, allowing coding for up to 64 different forwarding behaviors. The DSCP replaces the ToS bits, but it retains backward compatibility with the three precedence bits so that non-DSCP compliant, ToS-enabled devices, will not conflict with the DSCP mapping. Based on network policies, different kinds of traffic can be marked for different kinds of forwarding.

CLI REFERENCES

- "qos map dscp-mutation" on page 808

COMMAND USAGE

- Enter per-hop behavior and drop precedence for any of the DSCP values 0 - 63.
- This map is only used when the priority mapping mode is set to DSCP (see page 218), and the ingress packet type is IPv4.
- Two QoS domains can have different DSCP definitions, so the DSCP-to-PHB/Drop Precedence mutation map can be used to modify one set of DSCP values to match the definition of another domain. The mutation map should be applied at the receiving port (ingress mutation) at the boundary of a QoS administrative domain.
- Random Early Detection starts dropping yellow and red packets when the buffer fills up to 0x60 packets, and then starts dropping any packets regardless of color when the buffer fills up to 0x80 packets.
- The specified mapping applies to all interfaces.

PARAMETERS

These parameters are displayed in the web interface:

- **DSCP** – DSCP value in ingress packets. (Range: 0-63)
- **PHB** – Per-hop behavior, or the priority used for this router hop. (Range: 0-7)
- **Drop Precedence** – Drop precedence used for Random Early Detection in controlling traffic congestion. (Range: 0 - Green, 3 - Yellow, 1 - Red)

Table 15: Default Mapping of DSCP Values to Internal PHB/Drop Values

ingress-dscp10 \ ingress-dscp1	0	1	2	3	4	5	6	7	8	9
0	0,0	0,1	0,0	0,3	0,0	0,1	0,0	0,3	1,0	1,1
1	1,0	1,3	1,0	1,1	1,0	1,3	2,0	2,1	2,0	2,3
2	2,0	2,1	2,0	2,3	3,0	3,1	3,0	3,3	3.0	3,1
3	3,0	3,3	4,0	4,1	4,0	4,3	4,0	4,1	4.0	4,3
4	5,0	5,1	5,0	5,3	5,0	5,1	6,0	5,3	6,0	6,1
5	6,0	6,3	6,0	6,1	6,0	6,3	7,0	7,1	7.0	7,3
6	7,0	7,1	7,0	7,3						

The ingress DSCP is composed of ingress-dscp10 (most significant digit in the left column) and ingress-dscp1 (least significant digit in the top row (in other words, ingress-dscp = ingress-dscp10 * 10 + ingress-dscp1); and the corresponding internal-dscp is shown at the intersecting cell in the table.

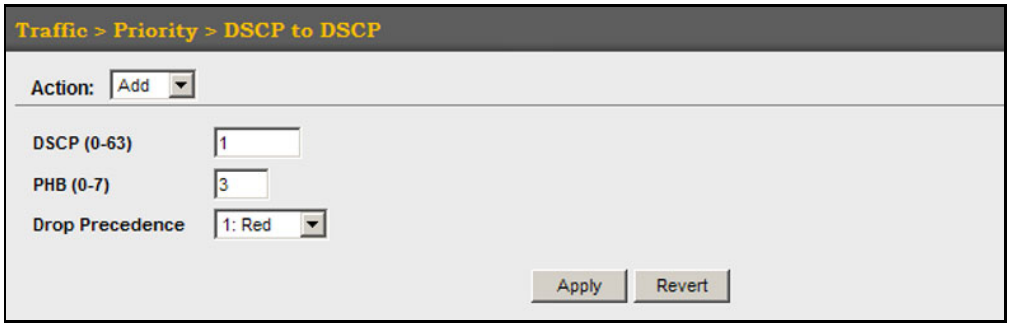
The ingress DSCP is bitwise ANDed with the binary value 11 to determine the drop precedence. If the resulting value is 10 binary, then the drop precedence is set to 0.

WEB INTERFACE

To map DSCP values to internal PHB/drop precedence in the web interface:

1. Click Traffic, Priority, DSCP to DSCP.
2. Select Add from the Action list.
3. Set the PHB and drop precedence for any DSCP value.
4. Click Apply.

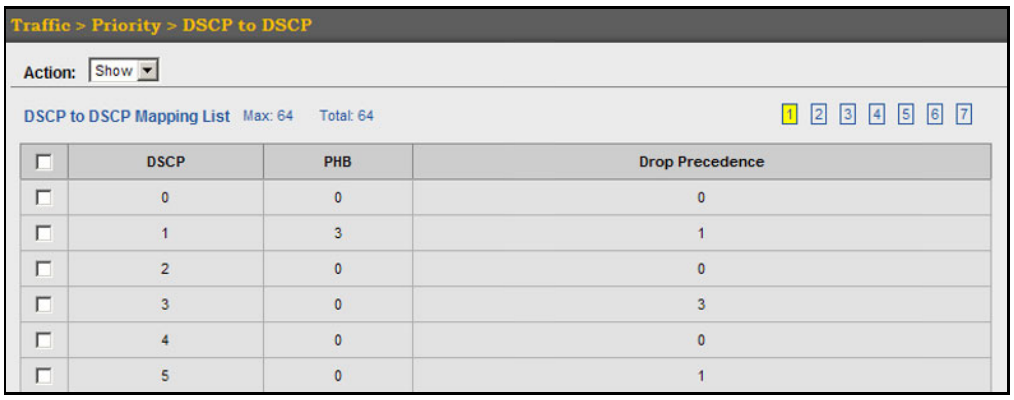
Figure 101: Configuring DSCP to DSCP Internal Mapping



To show the DSCP to internal PHB/drop precedence map in the web interface:

1. Click Traffic, Priority, DSCP to DSCP.
2. Select Show from the Action list.

Figure 102: Showing DSCP to DSCP Internal Mapping



DSCP	PHB	Drop Precedence
0	0	0
1	3	1
2	0	0
3	0	3
4	0	0
5	0	1

MAPPING COS PRIORITIES TO INTERNAL DSCP VALUES

Use the Traffic > Priority > CoS to DSCP page to maps CoS/CFI values in incoming packets to per-hop behavior and drop precedence values for priority processing.

CLI REFERENCES

- "qos map cos-dscp" on page 806

COMMAND USAGE

- The default mapping of CoS to PHB values is shown in Table 16 on page 223.
- Enter up to eight CoS/CFI paired values, per-hop behavior and drop precedence.
- If a packet arrives with a 802.1Q header but it is not an IP packet, then the CoS/CFI-to-PHB/Drop Precedence mapping table is used to generate priority and drop precedence values for internal processing. Note that priority tags in the original packet are not modified by this command.
- The internal DSCP consists of three bits for per-hop behavior (PHB) which determines the queue to which a packet is sent; and two bits for drop precedence (namely color) which is used by Random Early Detection (RED) to control traffic congestion.
- RED starts dropping yellow and red packets when the buffer fills up to 16 packets on Fast Ethernet ports and 72 packets on Gigabit Ethernet ports, and then starts dropping any packets regardless of color when the buffer fills up to 58 packets on Fast Ethernet ports and 80 packets on Gigabit Ethernet ports.
- The specified mapping applies to all interfaces.

PARAMETERS

These parameters are displayed in the web interface:

- **CoS** – CoS value in ingress packets. (Range: 0-7)
- **CFI** – Canonical Format Indicator. Set to this parameter to “0” to indicate that the MAC address information carried in the frame is in canonical format. (Range: 0-1)
- **PHB** – Per-hop behavior, or the priority used for this router hop. (Range: 0-7)
- **Drop Precedence** – Drop precedence used for Random Early Detection in controlling traffic congestion. (Range: 0 - Green, 3 - Yellow, 1 - Red)

Table 16: Default Mapping of CoS/CFI to Internal PHB/Drop Precedence

CoS \ CFI	0	1
0	(0,0)	(0,0)
1	(1,0)	(1,0)
2	(2,0)	(2,0)
3	(3,0)	(3,0)
4	(4,0)	(4,0)
5	(5,0)	(5,0)
6	(6,0)	(6,0)
7	(7,0)	(7,0)

WEB INTERFACE

To map CoS/CFI values to internal PHB/drop precedence in the web interface:

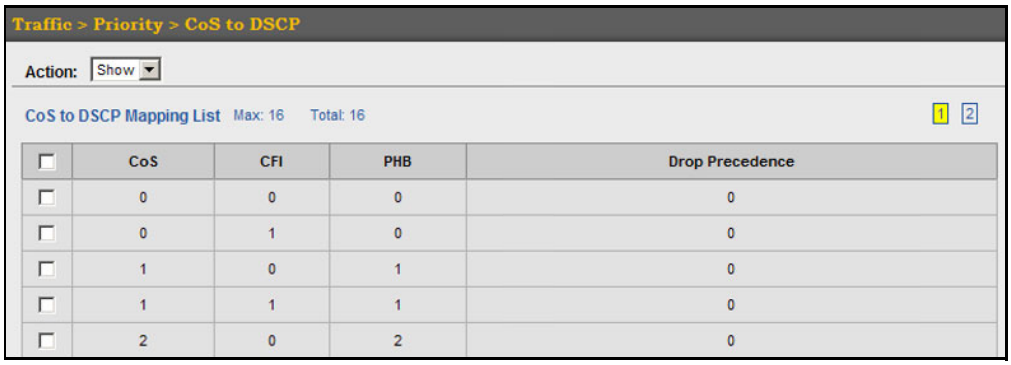
1. Click Traffic, Priority, CoS to DSCP.
2. Select Add from the Action list.
3. Set the PHB and drop precedence for any of the CoS/CFI combinations.
4. Click Apply.

Figure 103: Configuring CoS to DSCP Internal Mapping

To show the CoS/CFI to internal PHB/drop precedence map in the web interface:

1. Click Traffic, Priority, CoS to DSCP.
2. Select Show from the Action list.
3. Select an interface.

Figure 104: Showing CoS to DSCP Internal Mapping



	CoS	CFI	PHB	Drop Precedence
☐	0	0	0	0
☐	0	1	0	0
☐	1	0	1	0
☐	1	1	1	0
☐	2	0	2	0

12 QUALITY OF SERVICE

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 229).

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 815

COMMAND USAGE

- The class map is used with a policy map (page 229) to create a service policy (page 239) 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.

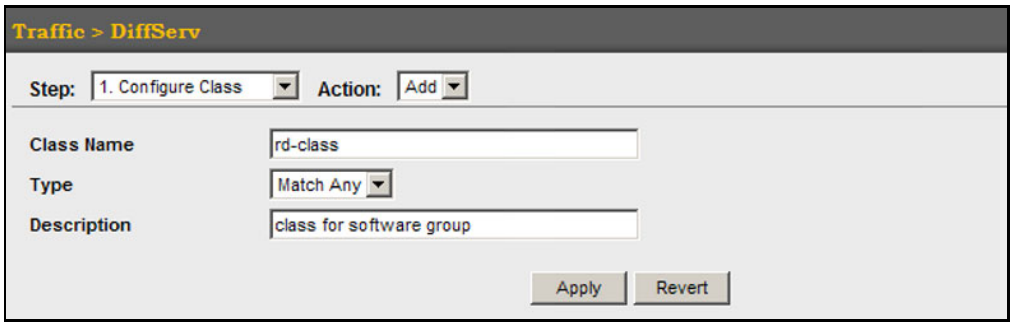
- **ACL List** – Name of an access control list. Any type of ACL can be specified, including standard or extended IP ACLs and MAC ACLs.
- **IP DSCP** – A DSCP value. (Range: 0-63)
- **IP Precedence** – An IP Precedence value. (Range: 0-7)
- **VLAN ID** – A VLAN. (Range:1-4093)

WEB INTERFACE

To configure a class map in the web interface:

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.

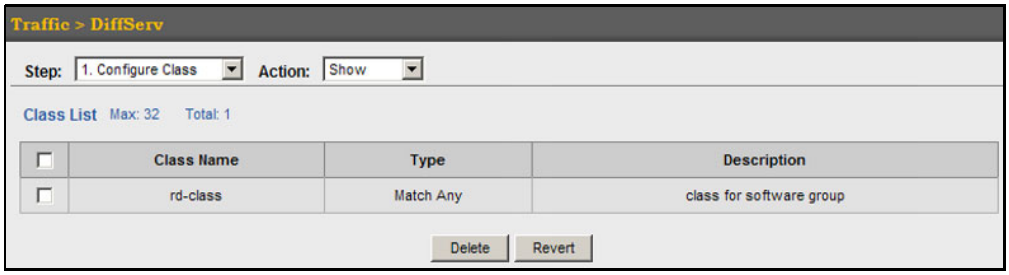
Figure 105: Configuring a Class Map



To show the configured class maps in the web interface:

1. Click Traffic, DiffServ.
2. Select Configure Class from the Step list.
3. Select Show from the Action list.

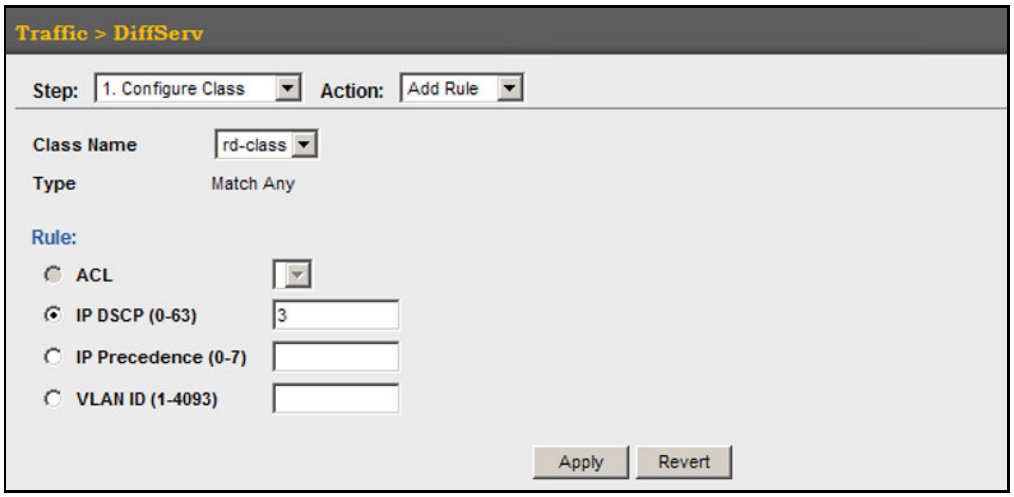
Figure 106: Showing Class Maps



To edit the rules for a class map in the web interface:

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.

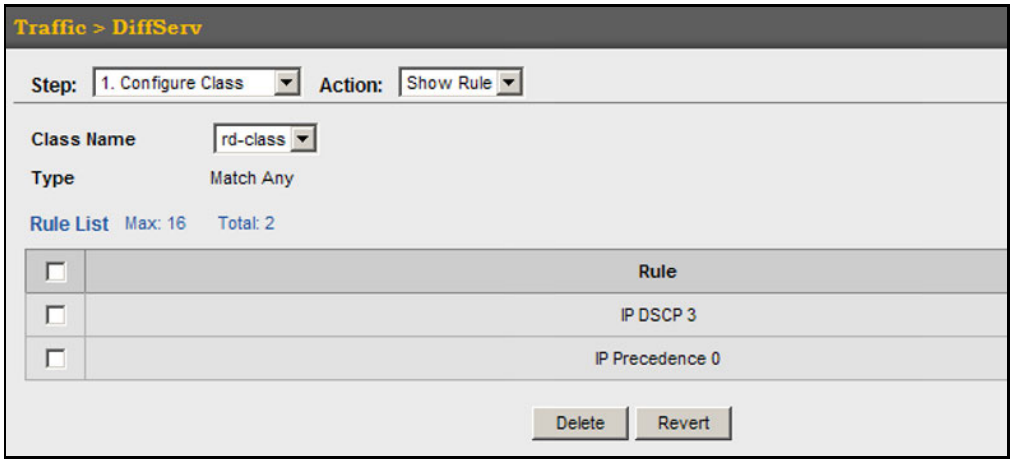
Figure 107: Adding Rules to a Class Map



To show the rules for a class map in the web interface:

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



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 226), modify service tagging, and enforce bandwidth policing. A policy map can then be bound by a service policy to one or more interfaces (page 239).

Configuring QoS policies requires several steps. A class map must first be configured which indicates how to match the inbound packets according to an access list, a DSCP or IP Precedence value, or a member of specific VLAN. A policy map is then configured which indicates the boundary parameters used for monitoring inbound traffic, and the action to take for conforming and non-conforming traffic. A policy map may contain one or more classes based on previously defined class maps.

The class of service or per-hop behavior (i.e., the priority used for internal queue processing) can be assigned to matching packets. In addition, the flow rate of inbound traffic can be monitored and the response to conforming and non-conforming traffic based by one of three distinct policing methods as described below.

Police Flow Meter – Defines the committed information rate (maximum throughput), committed burst size (burst rate), and the action to take for conforming and non-conforming traffic.

Policing is based on a token bucket, where bucket depth (that is, the maximum burst before the bucket overflows) is specified by the “burst” field (BC), and the average rate tokens are removed from the bucket is specified by the “rate” option (CIR). Action may be taken for traffic conforming to the maximum throughput, or exceeding the maximum throughput.

srTCM Police Meter – Defines an enforcer for classified traffic based on a single rate three color meter scheme defined in RFC 2697. This metering policy monitors a traffic stream and processes its packets according to the committed information rate (CIR, or maximum throughput), committed burst size (BC, or burst rate), and excess burst size (BE). Action may taken for traffic conforming to the maximum throughput, exceeding the maximum throughput, or exceeding the excess burst size.

- The PHB label is composed of five bits, three bits for per-hop behavior, and two bits for the color scheme used to control queue congestion. In addition to the actions defined by this command to transmit, remark the DSCP service value, or drop a packet, the switch will also mark the two color bits used to set the drop precedence of a packet for Random Early Detection. 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 ≥ 0, the packets is yellow and Te is decremented by B down to the minimum value of 0,
- else the packet is red and neither Tc nor Te is decremented.

When a packet of size B bytes arrives at time t, the following happens if srTCM is configured to operate in Color-Aware mode:

- If the packet has been precolored as green and Tc(t)-B ≥ 0, the packet is green and Tc is decremented by B down to the minimum value of 0, else
- If the packet has been precolored as yellow or green and if Te(t)-B ≥ 0, the packets is yellow and Te is decremented by B down to the minimum value of 0, else
- the packet is red and neither Tc nor Te is decremented.

The metering policy guarantees a deterministic behavior where the volume of green packets is never smaller than what has been determined by the CIR and BC, that is, tokens of a given color are always spent on packets of that color. Refer to RFC 2697 for more information on other aspects of srTCM.

trTCM Police Meter – Defines an enforcer for classified traffic based on a two rate three color meter scheme defined in RFC 2698. This metering policy monitors a traffic stream and processes its packets according to the committed information rate (CIR, or maximum throughput), peak information rate (PIR), and their associated burst sizes – committed burst size (BC, or burst rate), and peak burst size (BP). Action may taken for traffic conforming to the maximum throughput, exceeding the maximum throughput, or exceeding the peak burst size.

- The PHB label is composed of five bits, three bits for per-hop behavior, and two bits for the color scheme used to control queue congestion. In addition to the actions defined by this command to transmit, remark the DSCP service value, or drop a packet, the switch will also mark the two color bits used to set the drop precedence of a packet for Random Early Detection. 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.

Random Early Detection – RED starts dropping yellow and red packets when the buffer fills up to 0x60 packets, and then starts dropping any packets regardless of color when the buffer fills up to 0x80 packets.

CLI REFERENCES

- "Quality of Service Commands" on page 815

COMMAND USAGE

- A policy map can contain 16 class statements that can be applied to the same interface (page 239). Up to 32 policy maps can be configured for ingress ports.
- After using the policy map to define packet classification, service tagging, and bandwidth policing, it must be assigned to a specific interface by a service policy (page 239) 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 –** This attribute is used to set an internal QoS value in hardware for matching packets. The PHB label is composed of five bits, three bits for per-hop behavior, and two bits for the color scheme used to control queue congestion with the srTCM and trTCM metering functions.
  - **Set CoS** – Configures the service provided to ingress traffic by setting an internal CoS value for a matching packet (as specified in rule settings for a class map). (Range: 0-7)

    See Table 16, "Default Mapping of CoS/CFI to Internal PHB/Drop Precedence," on page 223).
  - **Set PHB** – Configures the service provided to ingress traffic by setting the internal per-hop behavior for a matching packet (as specified in rule settings for a class map). (Range: 0-7)

    See Table 15, "Default Mapping of DSCP Values to Internal PHB/ Drop Values," on page 220).
  - **Set IP DSCP** – Configures the service provided to ingress traffic by setting an IP DSCP value for a matching packet (as specified in rule settings for a class map). (Range: 0-63)
- **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: 64-10000000 kbps at a granularity of 64 kbps or maximum port speed, whichever is lower)

  The rate cannot exceed the configured interface speed.

- **Committed Burst Size** (BC) – Burst in bytes. (Range: 4000-16000000 at a granularity of 4k bytes)

  The burst size cannot exceed 16 Mbytes.

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

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

- **Violate** – Specifies whether the traffic that exceeds the maximum rate (CIR) will be dropped or the DSCP service level will be reduced.

  - **Set IP DSCP** – Decreases DSCP priority for out of conformance traffic. (Range: 0-63)

  - **Drop** – Drops out of conformance traffic.

- **srTCM** (Police Meter) – Defines the committed information rate (CIR, or maximum throughput), committed burst size (BC, or burst rate) and excess burst size (BE), and the action to take for traffic conforming to the maximum throughput, exceeding the maximum throughput but within the excess burst size, or exceeding the excess burst size. In addition to the actions defined by this command to transmit, remark the DSCP service value, or drop a packet, the switch will also mark the two color bits used to set the drop precedence of a packet for Random Early Detection.

  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: 64-10000000 kbps at a granularity of 64 kbps or maximum port speed, whichever is lower)

    The rate cannot exceed the configured interface speed.

  - **Committed Burst Size** (BC) – Burst in bytes. (Range: 4000-16000000 at a granularity of 4k bytes)

    The burst size cannot exceed 16 Mbytes.

- **Excess Burst Size** (BE) – Burst in excess of committed burst size. (Range: 4000-16000000 at a granularity of 4k bytes)

  The burst size cannot exceed 16 Mbytes.

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

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

- **Exceed** – Specifies whether traffic that exceeds the maximum rate (CIR) but is within the excess burst size (BE) will be dropped or the DSCP service level will be reduced.

  - **Set IP DSCP** – Decreases DSCP priority for out of conformance traffic. (Range: 0-63)

  - **Drop** – Drops out of conformance traffic.

- **Violate** – Specifies whether the traffic that exceeds the excess burst size (BE) will be dropped or the DSCP service level will be reduced.

  - **Set IP DSCP** – Decreases DSCP priority for out of conformance traffic. (Range: 0-63)

  - **Drop** – Drops out of conformance traffic.

- **trTCM** (Police Meter) – Defines the committed information rate (CIR, or maximum throughput), peak information rate (PIR), and their associated burst sizes – committed burst size (BC, or burst rate) and peak burst size (BP), and the action to take for traffic conforming to the maximum throughput, exceeding the maximum throughput but within the peak information rate, or exceeding the peak information rate. In addition to the actions defined by this command to transmit, remark the DSCP service value, or drop a packet, the switch will also mark the two color bits used to set the drop precedence of a packet for Random Early Detection.

  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: 64-10000000 kbps at a granularity of 64 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: 64-1000000 kbps at a granularity of 64 kbps or maximum port speed, whichever is lower)

  The rate cannot exceed the configured interface speed.

- **Committed Burst Size** (BC) – Burst in bytes. (Range: 4000-16000000 at a granularity of 4k bytes)

  The burst size cannot exceed 16 Mbytes.

- **Peak Burst Size** (BP) – Burst size in bytes. (Range: 4000-16000000 at a granularity of 4k bytes)

  The burst size cannot exceed 16 Mbytes.

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

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

- **Exceed** – Specifies whether traffic that exceeds the maximum rate (CIR) but is within the peak information rate (PIR) will be dropped or the DSCP service level will be reduced.

  - **Set IP DSCP** – Decreases DSCP priority for out of conformance traffic. (Range: 0-63).

  - **Drop** – Drops out of conformance traffic.

- **Violate** – Specifies whether the traffic that exceeds the peak information rate (PIR) will be dropped or the DSCP service level will be reduced.

  - **Set IP DSCP** – Decreases DSCP priority for out of conformance traffic. (Range: 0-63).

  - **Drop** – Drops out of conformance traffic.

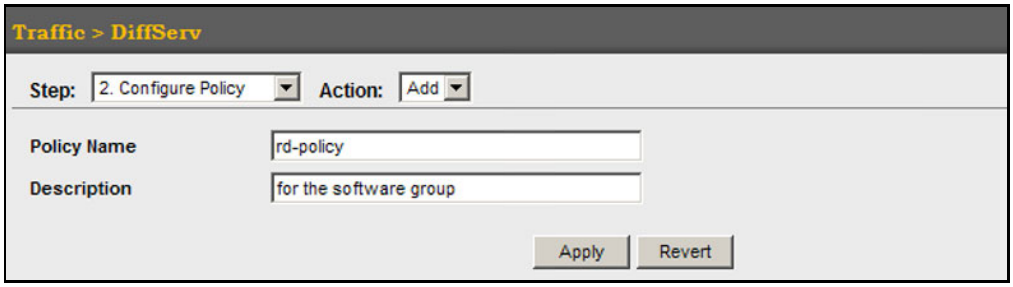
WEB INTERFACE

To configure a policy map in the web interface:

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.

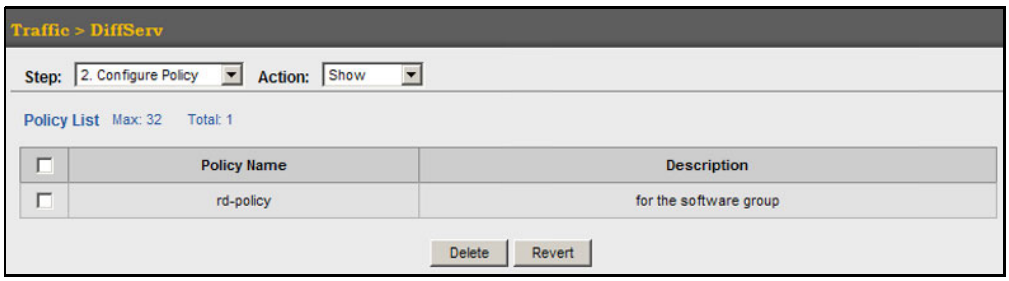
Figure 109: Configuring a Policy Map



To show the configured policy maps in the web interface:

1. Click Traffic, DiffServ.
2. Select Configure Policy from the Step list.
3. Select Show from the Action list.

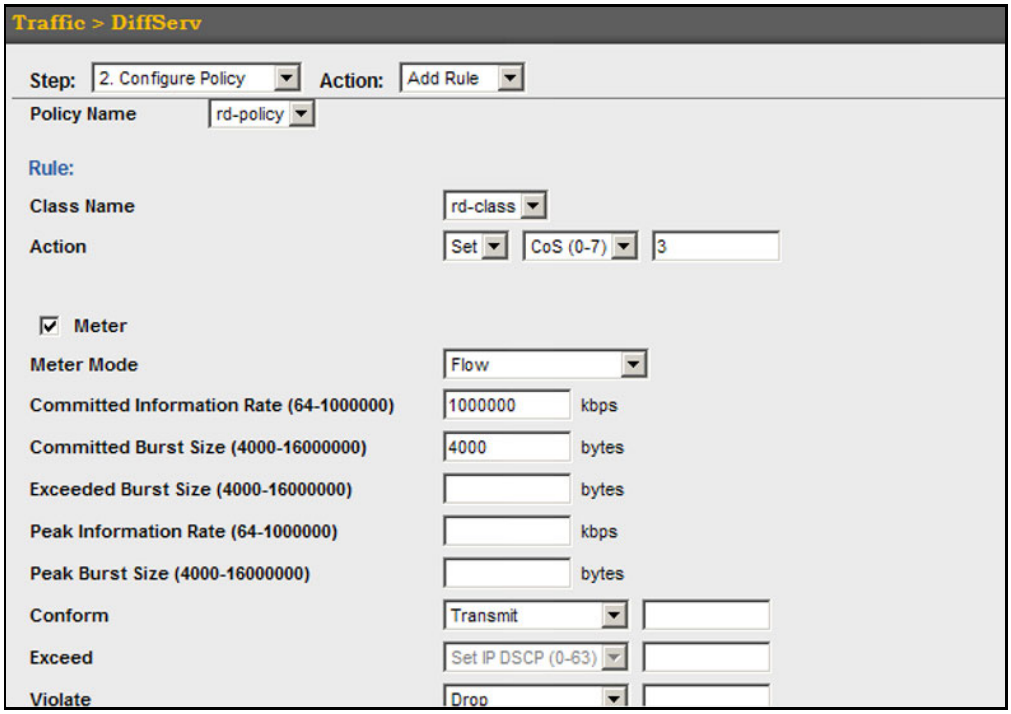
Figure 110: Showing Policy Maps



To edit the rules for a policy map in the web interface:

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.

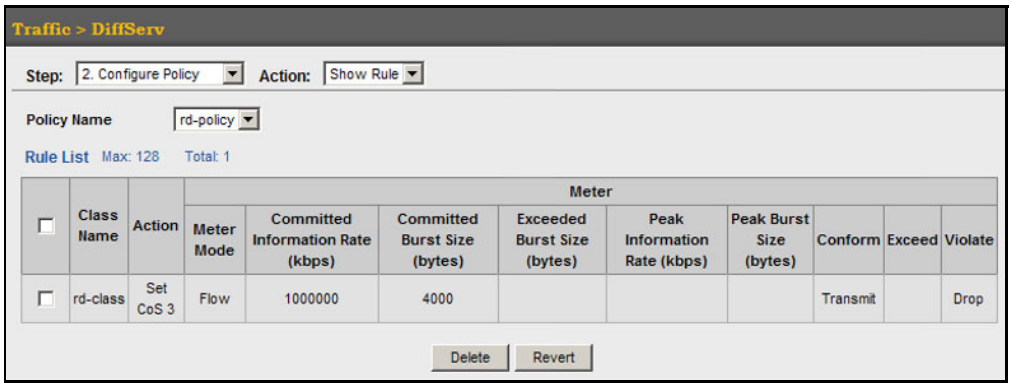
Figure 111: Adding Rules to a Policy Map



To show the rules for a policy map in the web interface:

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



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 815

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:

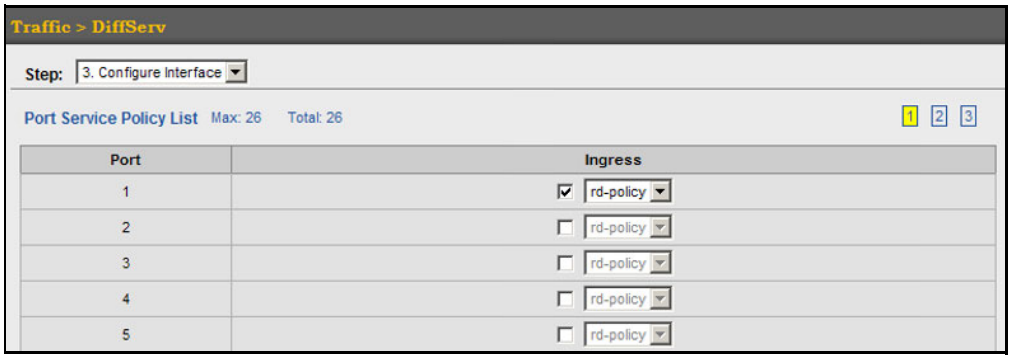
- **Port** – Specifies a port.
- **Ingress** – Applies the selected rule to ingress traffic.

WEB INTERFACE

To bind a policy map to a port in the web interface:

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



13 VoIP Traffic Configuration

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 793

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)

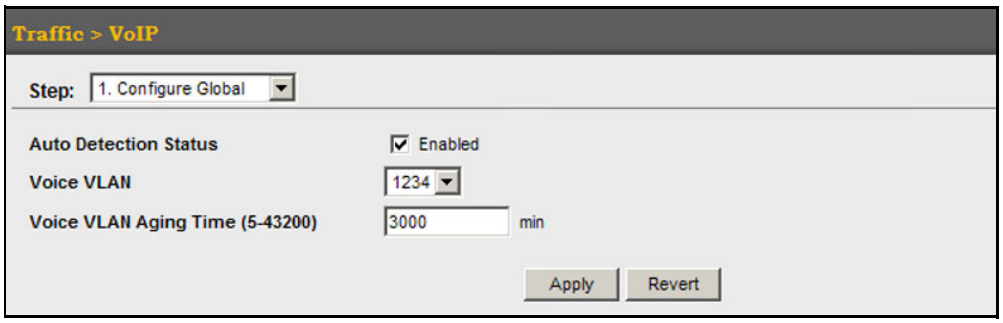
NOTE: The Voice VLAN ID cannot be modified when the global Auto Detection Status is enabled.

WEB INTERFACE

To configure global settings for a Voice VLAN in the web interface:

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



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 793

PARAMETERS

These parameters are displayed in the web interface:

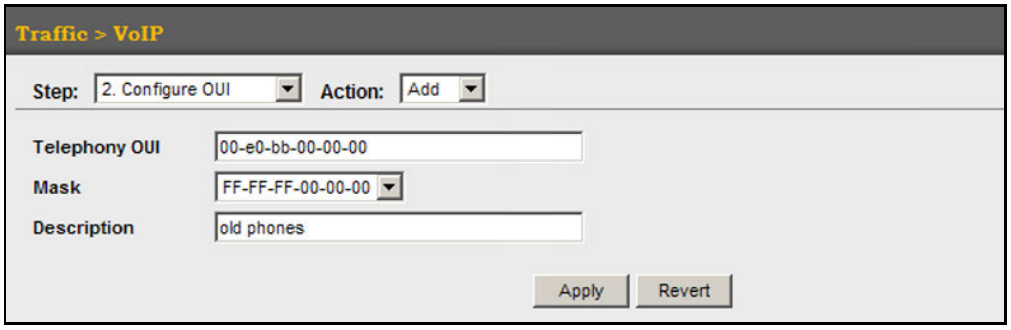
- **Telephony OUI** – Specifies a MAC address range to add to the list. Enter the MAC address in format 01-23-45-67-89-AB.
- **Mask** – Identifies a range of MAC addresses. Selecting a mask of FF-FF-FF-00-00-00 identifies all devices with the same OUI (the first three octets). Other masks restrict the 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 in the web interface:

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.

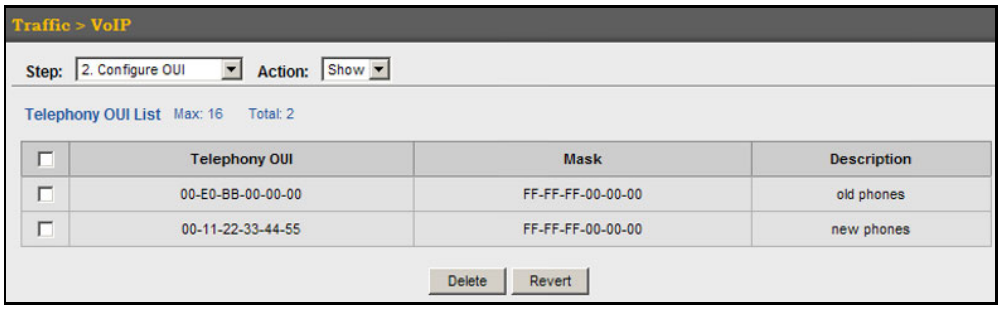
Figure 115: Configuring an OUI Telephony List



To show the MAC OUI numbers used for VoIP equipment in the web interface:

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



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 793

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)

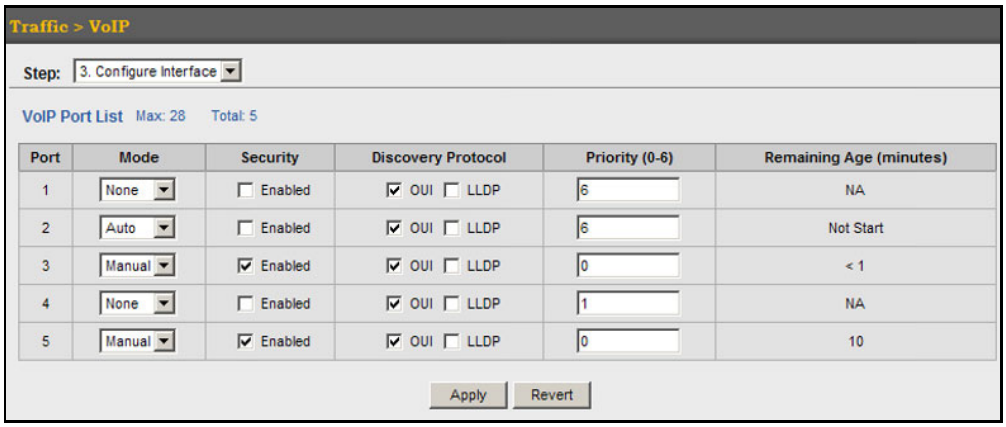
- **Discovery Protocol** – Selects a method to use for detecting VoIP traffic on the port. (Default: OUI)
  - **OUI** – Traffic from VoIP devices is detected by the Organizationally Unique Identifier (OUI) of the source MAC address. OUI numbers are assigned to manufacturers and form the first three octets 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.
  - **802.1ab** – Uses LLDP 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 344 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 in the web interface:

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



14 SECURITY MEASURES

You can configure this switch to authenticate users logging into the system for management access using local or remote authentication methods. Port-based authentication using IEEE 802.1X can also be configured to control either management access to the uplink ports or client access to the data ports. This switch provides secure network management access using the following options:

- AAA – Use local or remote authentication to configure access rights, specify authentication servers, configure remote authentication and accounting.
- User Accounts – Manually configure access rights on the switch for specified users.
- Web Authentication – Allows stations to authenticate and access the network in situations where 802.1X or Network Access authentication methods are infeasible or impractical.
- Network Access - Configure MAC authentication, intrusion response, dynamic VLAN assignment, and dynamic QoS assignment.
- HTTPS – Provide a secure web connection.
- SSH – Provide a secure shell (for secure Telnet access).
- ACL – Access Control Lists provide packet filtering for IP frames (based on address, protocol, Layer 4 protocol port number or TCP control code).
- ARP Inspection – Security feature that validates the MAC Address bindings for Address Resolution Protocol packets. Provides protection against ARP traffic with invalid MAC to IP Address bindings, which forms the basis for certain “man-in-the-middle” attacks.
- IP Filter – Filters management access to the web, SNMP or Telnet interface.
- Port Security – Configure secure addresses for individual ports.
- Port Authentication – Use IEEE 802.1X port authentication to control access to specific ports.
- 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, Web Authentication, Access Control Lists, IP Source Guard, and then DHCP Snooping.

AAA AUTHORIZATION AND ACCOUNTING

The Authentication, authorization, and accounting (AAA) feature provides the main framework for configuring access control on the switch. The three security functions can be summarized as follows:

- Authentication — Identifies users that request access to the network.
- Authorization — Determines if users can access specific services.
- Accounting — Provides reports, auditing, and billing for services that users have accessed on the network.

The AAA functions require the use of configured RADIUS or TACACS+ servers in the network. The security servers can be defined as sequential groups that are applied as a method for controlling user access to specified services. For example, when the switch attempts to authenticate a user, a request is sent to the first server in the defined group, if there is no response the second server will be tried, and so on. If at any point a pass or fail is returned, the process stops.

The switch supports the following AAA features:

- Accounting for IEEE 802.1X authenticated users that access the network through the switch.
- Accounting for users that access management interfaces on the switch through the console and Telnet.
- Accounting for commands that users enter at specific CLI privilege levels.
- Authorization of users that access management interfaces on the switch through the console and Telnet.

To configure AAA on the switch, you need to follow this general process:

1. Configure RADIUS and TACACS+ server access parameters. See "Configuring Local/Remote Logon Authentication" on page 249.
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 564

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.

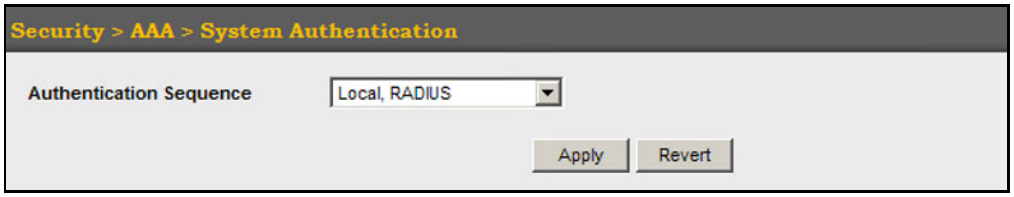
- [authentication sequence] – User authentication is performed by up to three authentication methods in the indicated sequence.

WEB INTERFACE

To configure the method(s) of controlling management access in the web interface:

1. Click Security, AAA, System Authentication.
2. Specify the authentication sequence (i.e., one to three methods).
3. Click Apply.

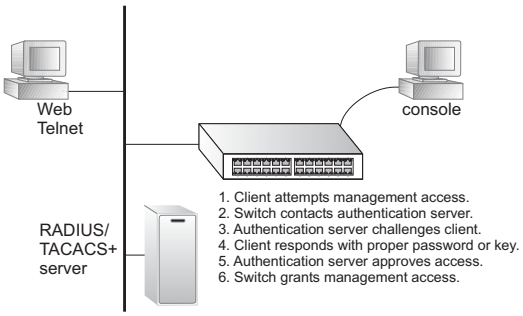
Figure 118: Configuring the Authentication Sequence



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.



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 566
- "TACACS+ Client" on page 570
- "AAA" on page 573

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 249).

WEB INTERFACE

To configure the parameters for RADIUS or TACACS+ authentication in the web interface:

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 119: Configuring Remote Authentication Server (RADIUS)

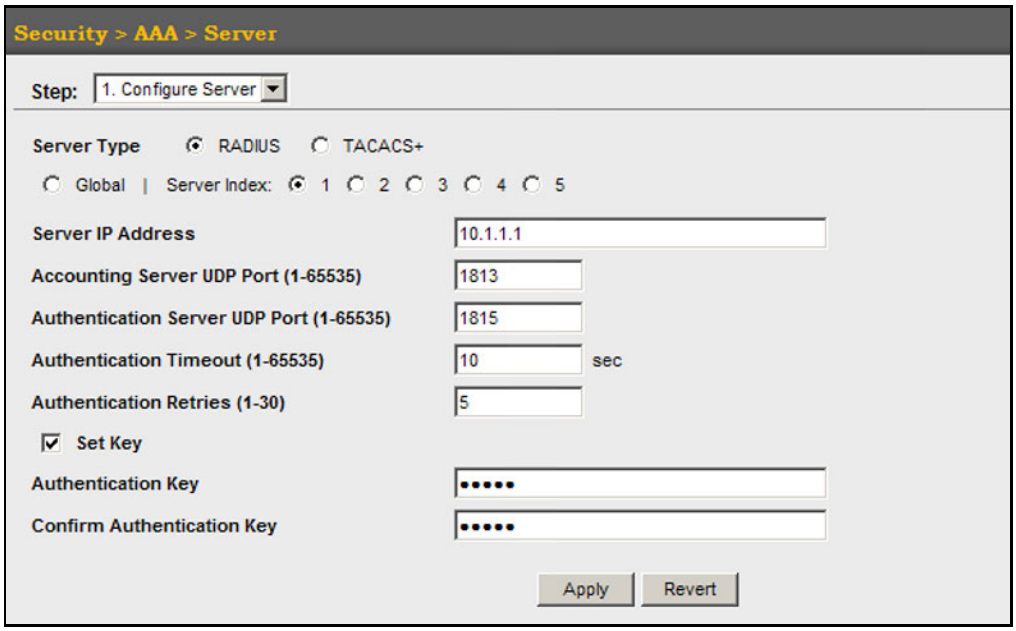
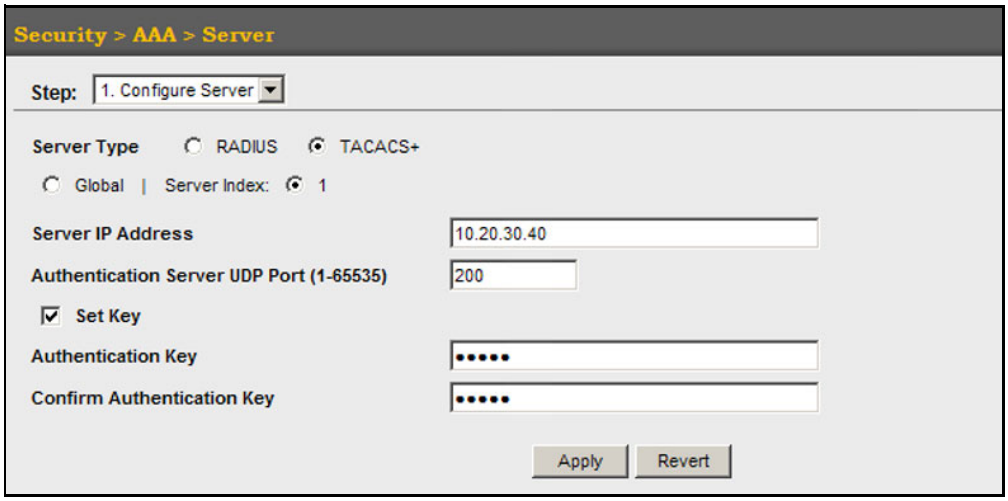


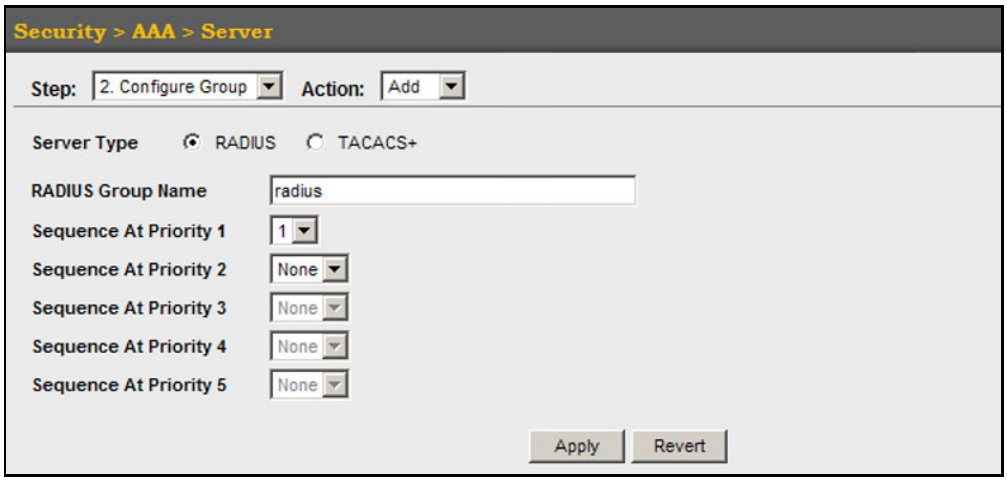
Figure 120: Configuring Remote Authentication Server (TACACS+)



To configure the RADIUS or TACACS+ server groups to use for accounting and authorization in the web interface:

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.

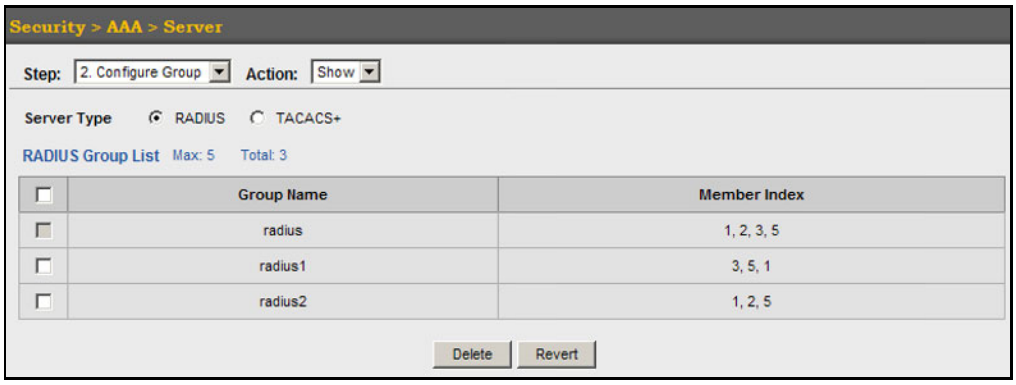
Figure 121: Configuring AAA Server Groups



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

1. Click Security, AAA, Server.
2. Select Configure Group from the Step list.
3. Select Show from the Action list.

Figure 122: Showing AAA Server Groups



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 573

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 249). 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

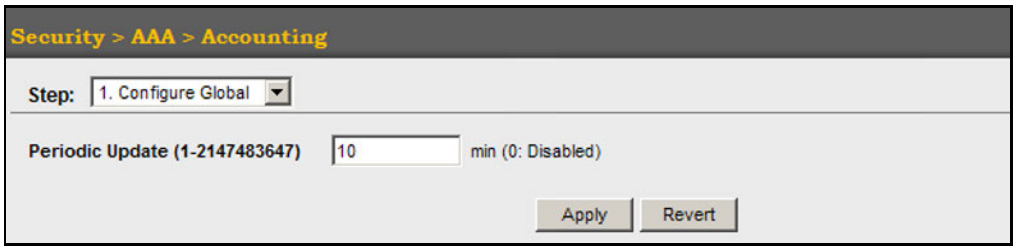
- **User Name** - Displays a registered user name.
- **Accounting Type** - Displays the accounting service.
- **Interface** - Displays the receive port number through which this user accessed the switch.
- **Time Elapsed** - Displays the length of time this entry has been active.

WEB INTERFACE

To configure global settings for AAA accounting in the web interface:

1. Click Security, AAA, Accounting.
2. Select Configure Global from the Step list.
3. Enter the required update interval.
4. Click Apply.

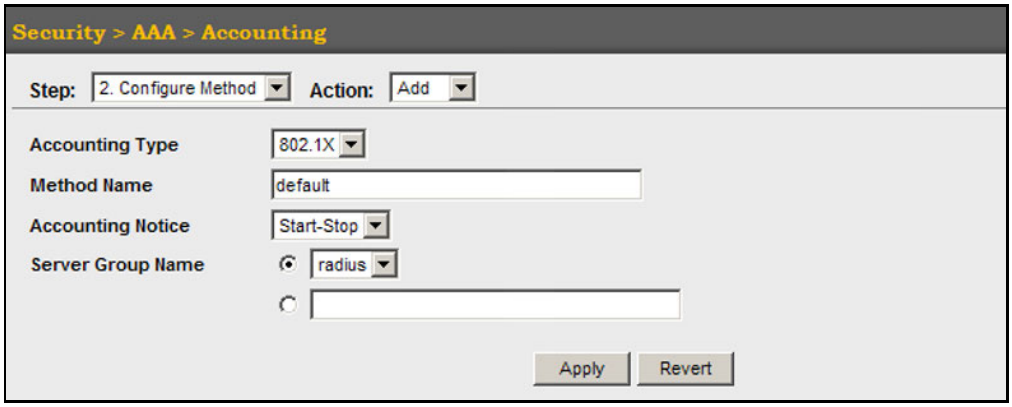
Figure 123: Configuring Global Settings for AAA Accounting



To configure the accounting method applied to various service types and the assigned server group in the web interface:

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.

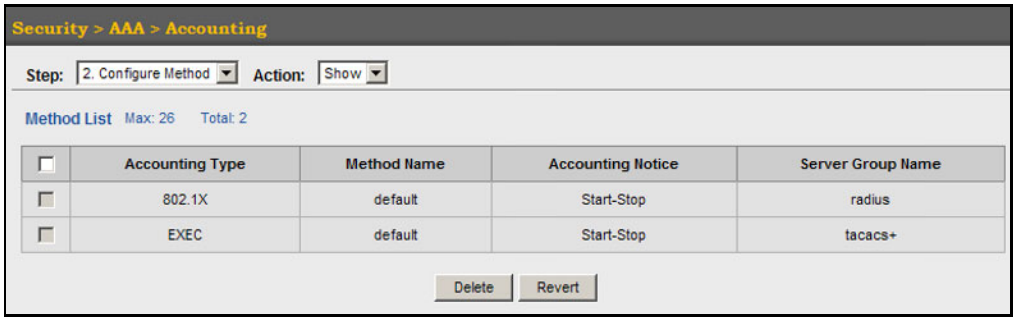
Figure 124: Configuring AAA Accounting Methods



To show the accounting method applied to various service types and the assigned server group in the web interface:

1. Click Security, AAA, Accounting.
2. Select Configure Method from the Step list.
3. Select Show from the Action list.

Figure 125: Showing AAA Accounting Methods



To configure the accounting method applied to specific interfaces, console commands entered at specific privilege levels, and local console, Telnet, or SSH connections in the web interface:

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 126: Configuring AAA Accounting Service for 802.1X Service

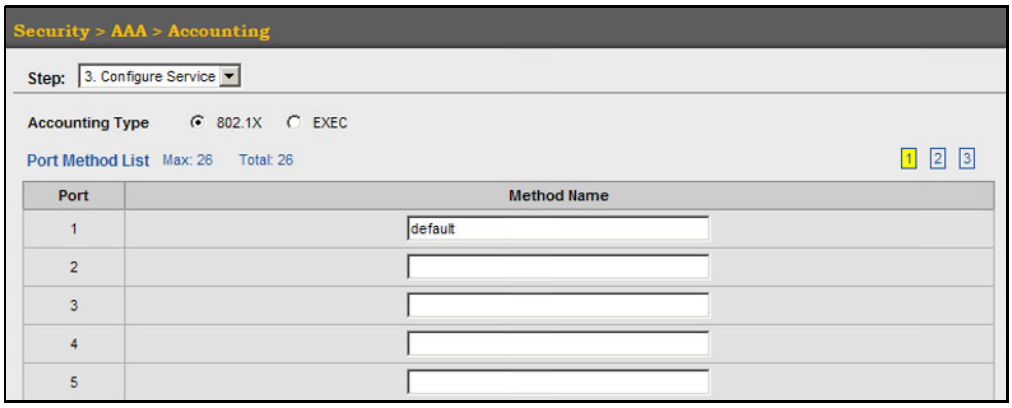
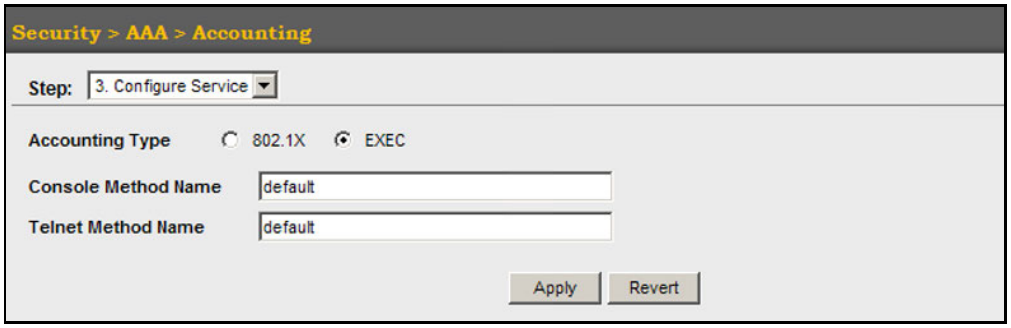


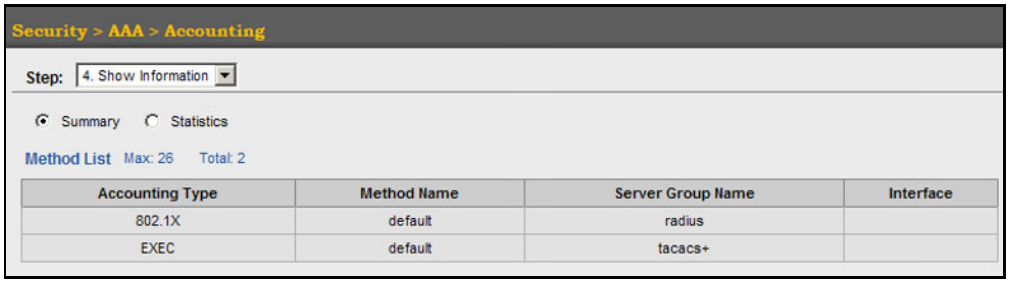
Figure 127: Configuring AAA Accounting Service for Exec Service



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

1. Click Security, AAA, Accounting.
2. Select Show Information from the Step list.
3. Click Summary.

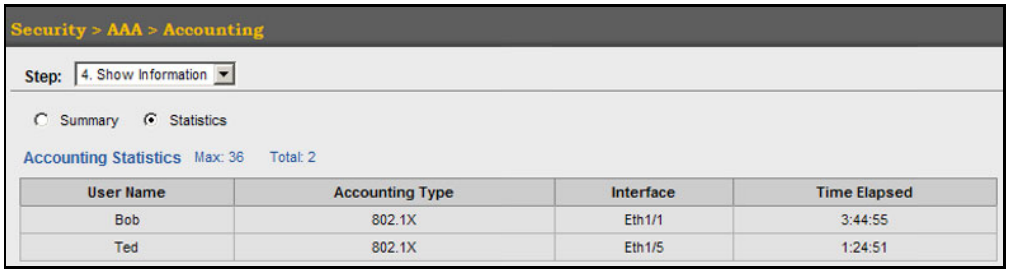
Figure 128: Displaying a Summary of Applied AAA Accounting Methods



To display basic accounting information and statistics recorded for user sessions in the web interface:

1. Click Security, AAA, Accounting.
2. Select Show Information from the Step list.
3. Click Statistics.

Figure 129: Displaying Statistics for AAA Accounting Sessions



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 573

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 249). 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.

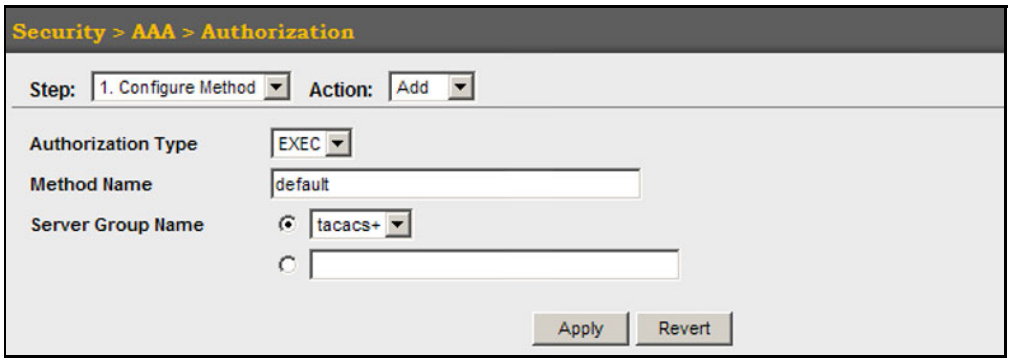
- **Interface** - Displays the console or Telnet interface to which these rules apply. (This field is null if the authorization method and associated server group has not been assigned to an interface.)

WEB INTERFACE

To configure the authorization method applied to the Exec service type and the assigned server group in the web interface:

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.

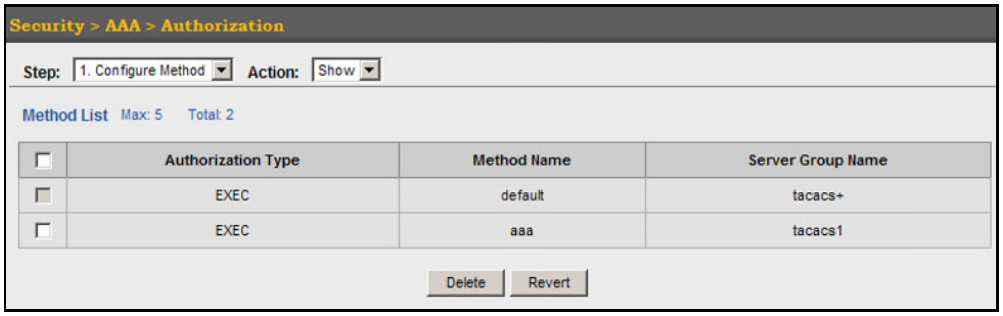
Figure 130: Configuring AAA Authorization Methods



To show the authorization method applied to the EXEC service type and the assigned server group in the web interface:

1. Click Security, AAA, Authorization.
2. Select Configure Method from the Step list.
3. Select Show from the Action list.

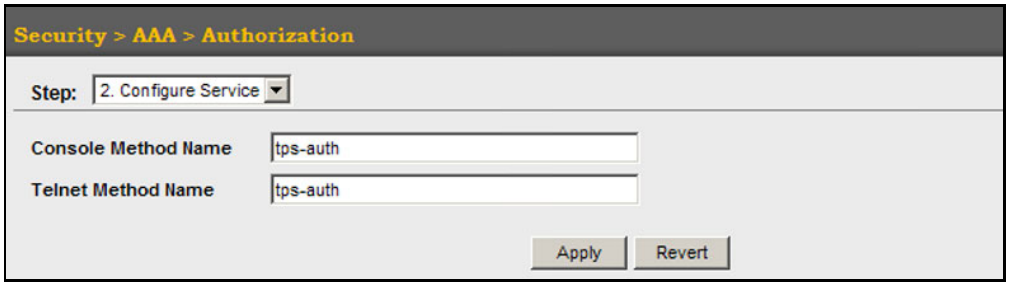
Figure 131: Showing AAA Authorization Methods



To configure the authorization method applied to local console, Telnet, or SSH connections in the web interface:

1. Click Security, AAA, Authorization.
2. Select Configure Service from the Step list.
3. Enter the required authorization method.
4. Click Apply.

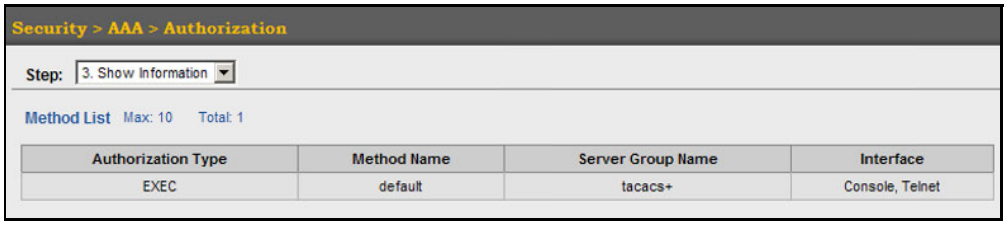
Figure 132: Configuring AAA Authorization Methods for Exec Service



To display a the configured authorization method and assigned server groups for The Exec service type in the web interface:

1. Click Security, AAA, Authorization.
2. Select Show Information from the Step list.

Figure 133: Displaying the Applied AAA Authorization Method



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 561

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)

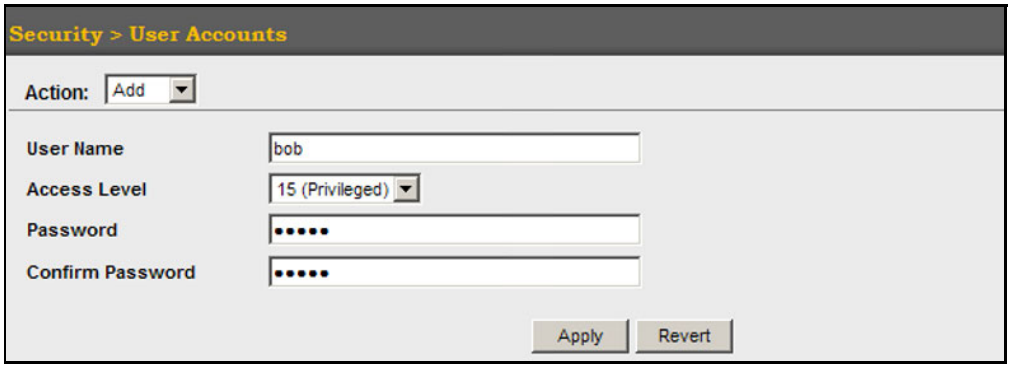
  Normal privilege level provides access to a limited number of the commands which display the current status of the switch, as well as several database clear and reset functions. Privileged level provides full access to all commands.
- **Password** – Specifies the user password.
  (Range: 0-8 characters 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 in the web interface:

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.

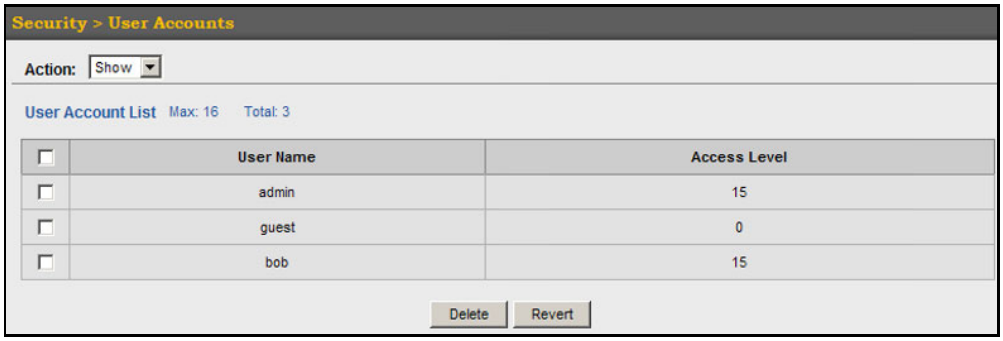
Figure 134: Configuring User Accounts



To show user accounts in the web interface:

1. Click Security, User Accounts.
2. Select Show from the Action list.

Figure 135: Showing User Accounts



WEB AUTHENTICATION

Web authentication allows stations to authenticate and access the network in situations where 802.1X or Network Access authentication are infeasible or impractical. The web authentication feature allows unauthenticated hosts to request and receive a DHCP assigned IP address and perform DNS queries. All other traffic, except for HTTP protocol traffic, is blocked. The switch intercepts HTTP protocol traffic and redirects it to a switch-generated web page that facilitates user name and password authentication via RADIUS. Once authentication is successful, the web browser is forwarded on to the originally requested web page. Successful authentication is valid for all hosts connected to the port.

NOTE: RADIUS authentication must be activated and configured properly for the web authentication feature to work properly. (See "Configuring Local/Remote Logon Authentication" on page 249.)

NOTE: Web authentication cannot be configured on trunk ports.

CONFIGURING GLOBAL SETTINGS FOR WEB AUTHENTICATION

Use the Security > Web Authentication (Configure Global) page to edit the global parameters for web authentication.

CLI REFERENCES

- "Web Authentication" on page 632

PARAMETERS

These parameters are displayed in the web interface:

- **Web Authentication Status** – Enables web authentication for the switch. (Default: Disabled)

  Note that this feature must also be enabled for any port where required under the Configure Interface menu.

- **Session Timeout** – Configures how long an authenticated session stays active before it must re-authenticate itself. (Range: 300-3600 seconds; Default: 3600 seconds)

- **Quiet Period** – Configures how long a host must wait to attempt authentication again after it has exceeded the maximum allowable failed login attempts. (Range: 1-180 seconds; Default: 60 seconds)

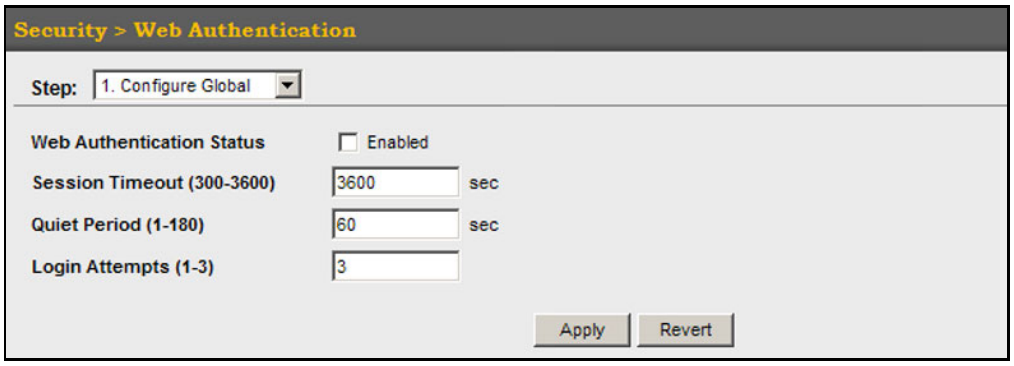
- **Login Attempts** – Configures the amount of times a supplicant may attempt and fail authentication before it must wait the configured quiet period. (Range: 1-3 attempts; Default: 3 attempts)

WEB INTERFACE

To configure global parameters for web authentication in the web interface:

1. Click Security, Web Authentication.
2. Select Configure Global from the Step list.
3. Enable web authentication globally on the switch, and adjust any of the protocol parameters as required.
4. Click Apply.

Figure 136: Configuring Global Settings for Web Authentication



CONFIGURING INTERFACE SETTINGS FOR WEB AUTHENTICATION

Use the Security > Web Authentication (Configure Interface) page to enable web authentication on a port, and display information for any connected hosts.

CLI REFERENCES

- "Web Authentication" on page 632

PARAMETERS

These parameters are displayed in the web interface:

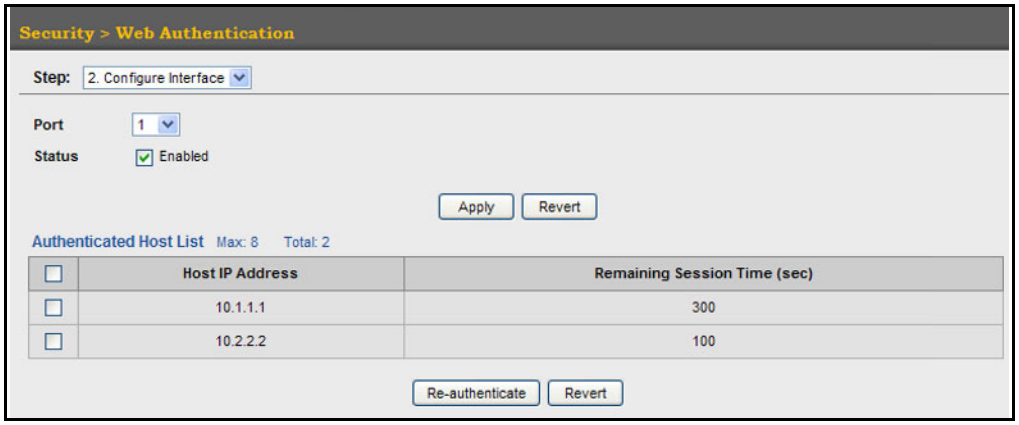
- **Port** – Indicates the port being configured.
- **Status** – Configures the web authentication status for the port.
- **Host IP Address** – Indicates the IP address of each connected host.
- **Remaining Session Time** – Indicates the remaining time until the current authorization session for the host expires.
- **Apply** – Enables web authentication if the Status box is checked.
- **Re-authenticate** – Ends all authenticated web sessions for selected host IP addresses in the Authenticated Host List, and forces the users to re-authenticate.

WEB INTERFACE

To enable web authentication for a port in the web interface:

1. Click Security, Web Authentication.
2. Select Configure Interface from the Step list.
3. Set the status box to enabled for any port that requires web authentication, and click Apply
4. Mark the check box for any host addresses that need to be re-authenticated, and click Re-authenticate.

Figure 137: Configuring Interface Settings for Web Authentication



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 250.)

NOTE: MAC authentication cannot be configured on trunk ports.

CLI REFERENCES

- "Network Access (MAC Address Authentication)" on page 619

COMMAND USAGE

- MAC address authentication controls access to the network by authenticating the MAC address of each host that attempts to connect to a switch port. Traffic received from a specific MAC address is forwarded by the switch only if the source MAC address is successfully authenticated by a central RADIUS server. While authentication for a MAC address is in progress, all traffic is blocked until authentication is completed. On successful authentication, the RADIUS server may optionally assign VLAN and quality of service settings for the switch port.

- When enabled on a port, the authentication process sends a Password Authentication Protocol (PAP) request to a configured RADIUS server. The user name and password are both equal to the MAC address being authenticated. On the RADIUS server, PAP user name and passwords must be configured in the MAC address format XX-XX-XX-XX-XX-XX (all in upper case).

- Authenticated MAC addresses are stored as dynamic entries in the switch secure MAC address table and are removed when the aging time expires. The maximum number of secure MAC addresses supported for the switch system is 1024.

- Configured static MAC addresses are added to the secure address table when seen on a switch port. Static addresses are treated as authenticated without sending a request to a RADIUS server.

- When port status changes to down, all MAC addresses mapped to that port are cleared from the secure MAC address table. Static VLAN assignments are not restored.

- The RADIUS server may optionally return a VLAN identifier list to be applied to the switch port. The following attributes need to be configured on the RADIUS server.
  - **Tunnel-Type** = VLAN
  - **Tunnel-Medium-Type** = 802
  - **Tunnel-Private-Group-ID** = 1u,2t [*VLAN ID list*]

  The VLAN identifier list is carried in the RADIUS "Tunnel-Private-Group-ID" attribute. The VLAN list can contain multiple VLAN identifiers in the format "1u,2t,3u" where "u" indicates an untagged VLAN and "t" a tagged VLAN.

- The RADIUS server may optionally return dynamic QoS assignments to be applied to a switch port for an authenticated user. The "Filter-ID" attribute (attribute 11) can be configured on the RADIUS server to pass the following QoS information:

Table 17: 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 619

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 317).

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.

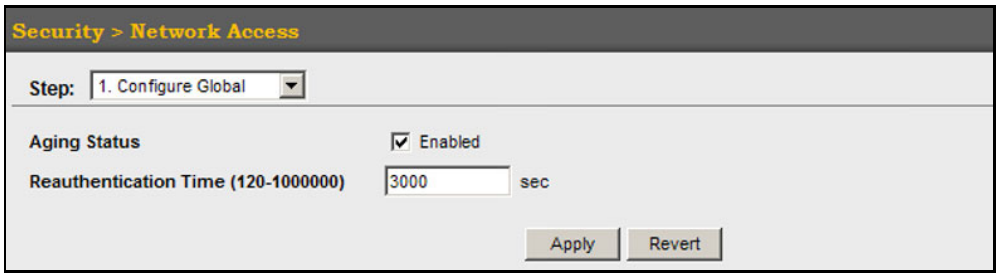
- **Reauthentication Time** – Sets the time period after which a connected host must be reauthenticated. When the reauthentication time expires for a secure MAC address, it is reauthenticated with the RADIUS server. During the reauthentication process traffic through the port remains unaffected. (Default: 1800 seconds; Range: 120-1000000 seconds)

WEB INTERFACE

To configure aging status and reauthentication time for MAC address authentication in the web interface:

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 138: Configuring Global Settings for Network Access



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 619

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 MAC Authentication or 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 150). Also, when used with 802.1X authentication, intrusion action must be set for “Guest VLAN” (see "Configuring Port Authenticator Settings for 802.1X" on page 317).

- **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 in the web interface:

1. Click Security, Network Access.

2. Select Configure Interface from the Step list.

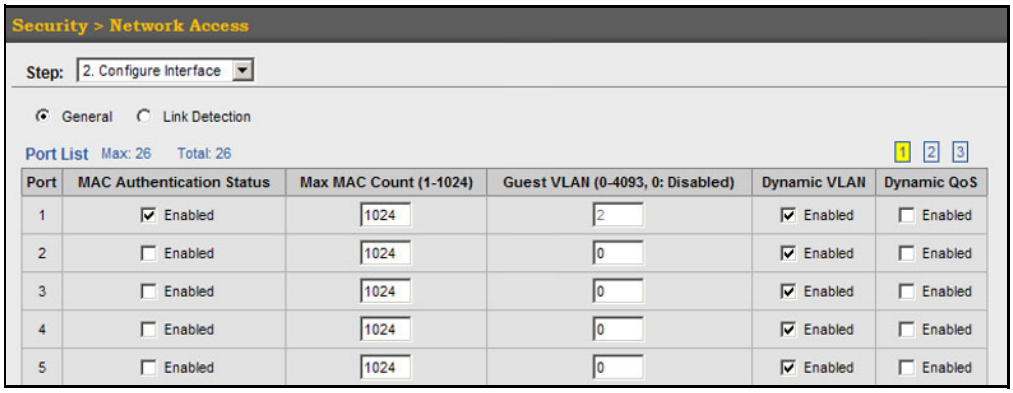
3. Click the General button.

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.

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 139: Configuring Interface Settings for Network Access



Port	MAC Authentication Status	Max MAC Count (1-1024)	Guest VLAN (0-4093, 0: Disabled)	Dynamic VLAN	Dynamic QoS
1	☑ Enabled	1024	2	☑ Enabled	☐ Enabled
2	☐ Enabled	1024	0	☑ Enabled	☐ Enabled
3	☐ Enabled	1024	0	☑ Enabled	☐ Enabled
4	☐ Enabled	1024	0	☑ Enabled	☐ Enabled
5	☐ Enabled	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 619

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.

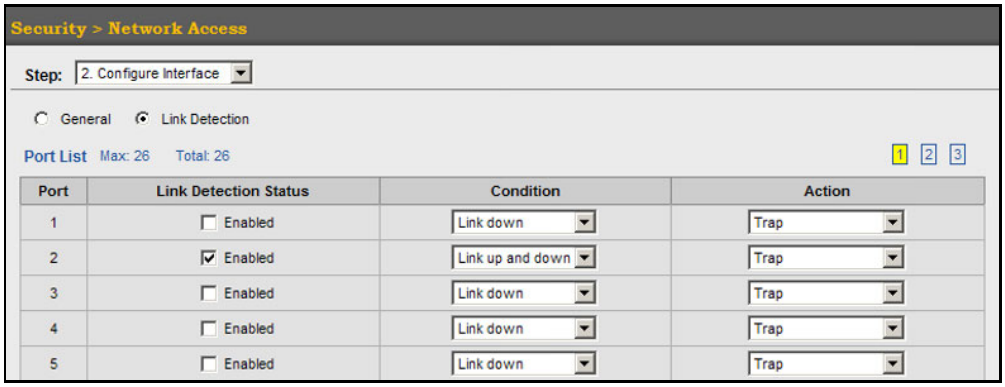
- **Shutdown** – The port is shut down.

WEB INTERFACE

To configure link detection on switch ports in the web interface:

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 140: Configuring Link Detection for Network Access



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 619

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).

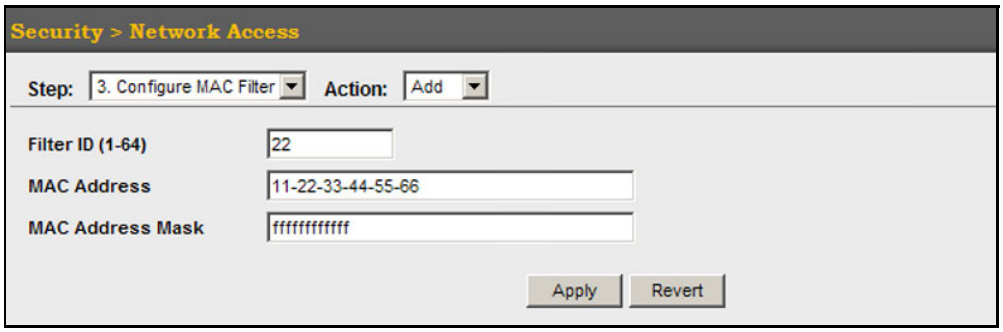
- **MAC Address Mask** – The filter rule will check for the range of MAC addresses defined by the MAC bit mask. If you omit the mask, the system will assign the default mask of an exact match.
(Range: 000000000000 - FFFFFFFFFFFF; Default: FFFFFFFFFFFF)

WEB INTERFACE

To add a MAC address filter for MAC authentication in the web interface:

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.

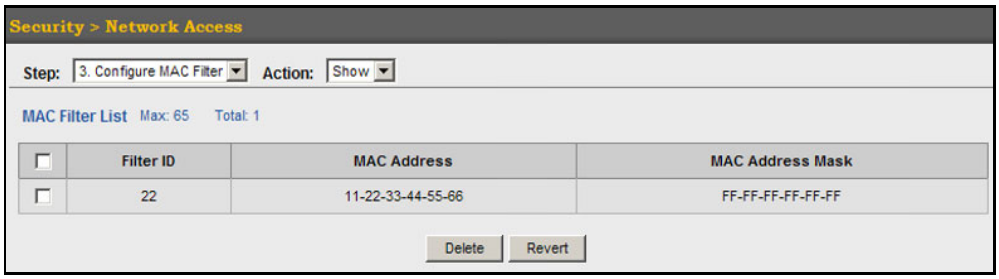
Figure 141: Configuring a MAC Address Filter for Network Access



To show the MAC address filter table for MAC authentication in the web interface:

1. Click Security, Network Access.
2. Select Configure MAC Filter from the Step list.
3. Select Show from the Action list.

Figure 142: Showing the MAC Address Filter Table for Network Access



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 619

PARAMETERS

These parameters are displayed in the web interface:

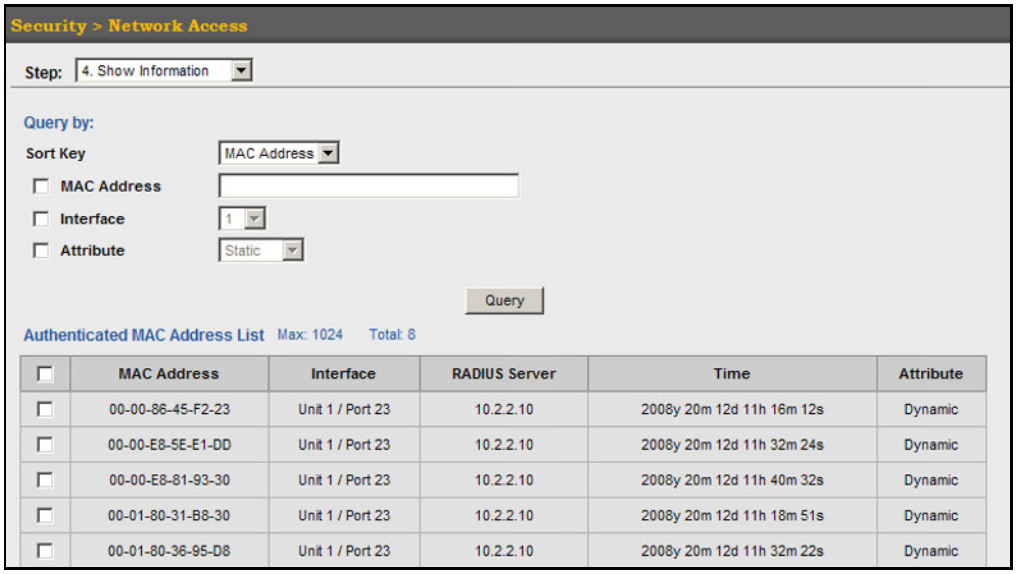
- **Query By** – Specifies parameters to use in the MAC address query.
  - **Sort Key** – Sorts the information displayed based on MAC address, port interface, or attribute.
  - **MAC Address** – Specifies a specific MAC address.
  - **Interface** – Specifies a port interface.
  - **Attribute** – Displays 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 in the web interface:

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 143: Showing Addresses Authenticated for Network Access



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 582

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 583.)
- 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 18: 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, Window 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 278.

PARAMETERS

These parameters are displayed in the web interface:

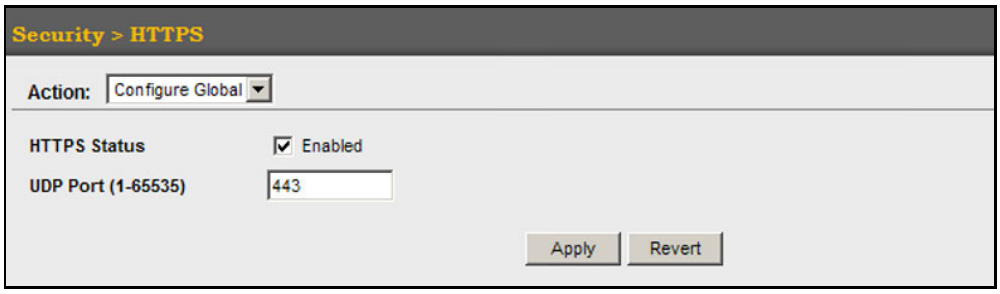
- **HTTPS Status** – Allows you to enable/disable the HTTPS server feature on the switch. (Default: Enabled)
- **HTTPS Port** – Specifies the UDP port number used for HTTPS connection to the switch's web interface. (Default: Port 443)

WEB INTERFACE

To configure HTTPS in the web interface:

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 144: Configuring HTTPS



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 109 or type “reload” at the commad prompt: ES-3026#`reload`

CLI REFERENCES

- "Web Server" on page 582

PARAMETERS

These parameters are displayed in the web interface:

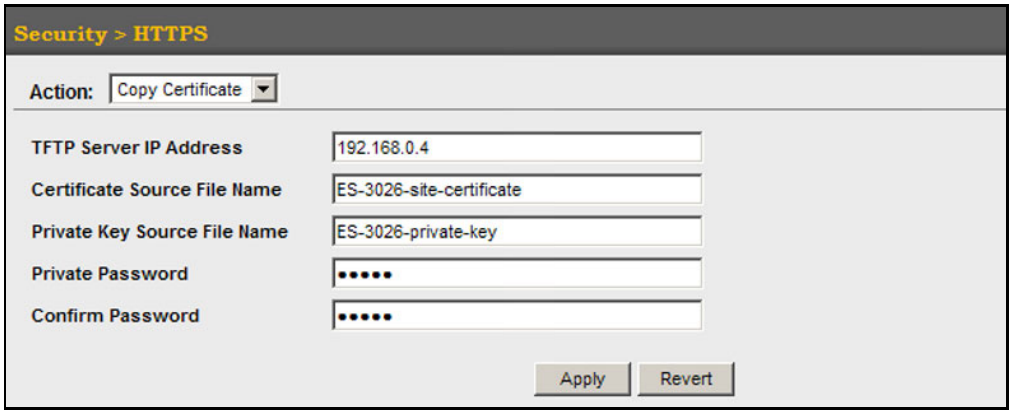
- **TFTP Server IP Address** – IP address of TFTP server which contains the certificate file.
- **Certificate Source File Name** – Name of certificate file stored on the TFTP server.
- **Private Key Source File Name** – Name of private key file stored on the TFTP server.
- **Private Password** – Password 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 in the web interface:

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 145: Downloading the Secure-Site Certificate



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 249). 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
   156849954018676692593339467750546173253136748908365472541502024559319986854435836165199992332978176606583095610825913212890233 76546801726272571413428762941301196195566782595664104869574278881462065194174677298486546861571773939016477935594230357741309802273708779454524083971752646358058176716709574804776117

3. *Import Client's Public Key to the Switch* – See "Importing User Public Keys" on page 286, or use the copy tftp public-key command (page 491) 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 263.) 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
   134108168560989392104094492015542534763164192187295892114317388005553616163105177594083868631109291232226828519254374603100937187721199696317813662774141689851320491172048303392543241016379975923714490119380060902539484084827178194372288402533115952134861022902978982721353267131629432532818915045306393916643 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.

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 284.

CLI REFERENCES

- "Secure Shell" on page 588

PARAMETERS

These parameters are displayed in the web interface:

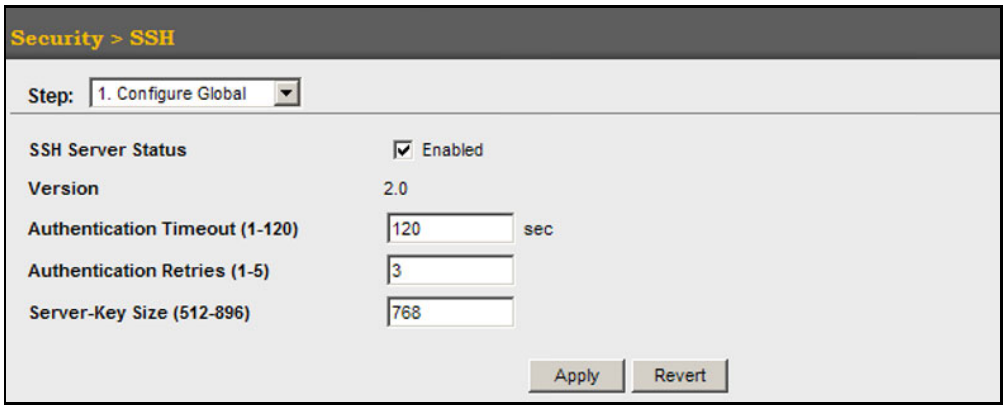
- **SSH Server Status** – Allows you to enable/disable the SSH server on the switch. (Default: Disabled)
- **Version** – The Secure Shell version number. Version 2.0 is displayed, but the switch supports management access via either SSH Version 1.5 or 2.0 clients.
- **Authentication Timeout** – Specifies 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 in the web interface:

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 146: Configuring the SSH Server



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 286.

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 283.

CLI REFERENCES

- "Secure Shell" on page 588

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.

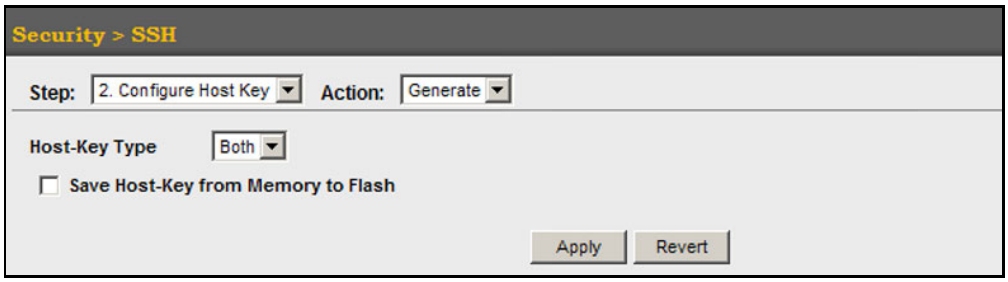
- **Save Host-Key from Memory to Flash** – Saves the host key from RAM (i.e., volatile memory) to flash memory. Otherwise, the host key pair is stored to RAM by default. Note that you must select this item prior to generating the host-key pair. (Default: Disabled)

WEB INTERFACE

To generate the SSH host key pair in the web interface:

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.

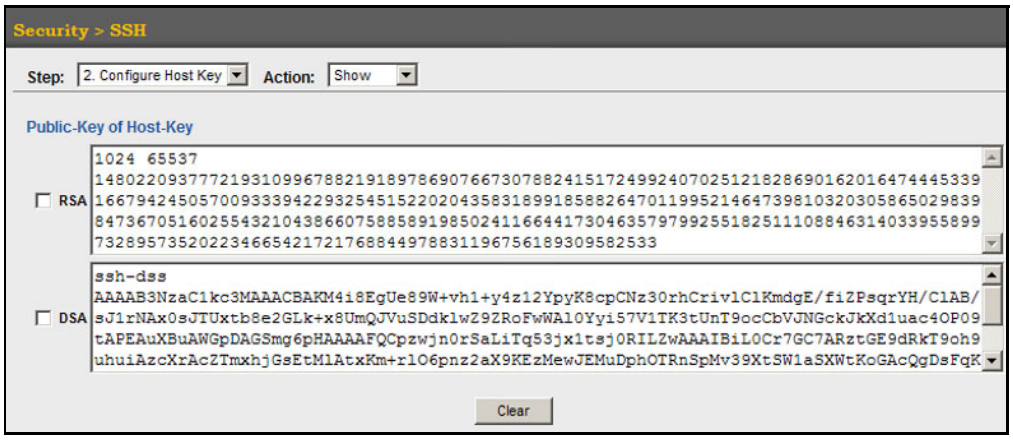
Figure 147: Generating the SSH Host Key Pair



To display or clear the SSH host key pair in the web interface:

1. Click Security, SSH.
2. Select Configure Host Key from the Step list.
3. Select Show from the Action list.
4. Select the host-key type to clear.
5. Click Clear.

Figure 148: Showing the SSH Host Key Pair



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 588

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 263).

- **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.

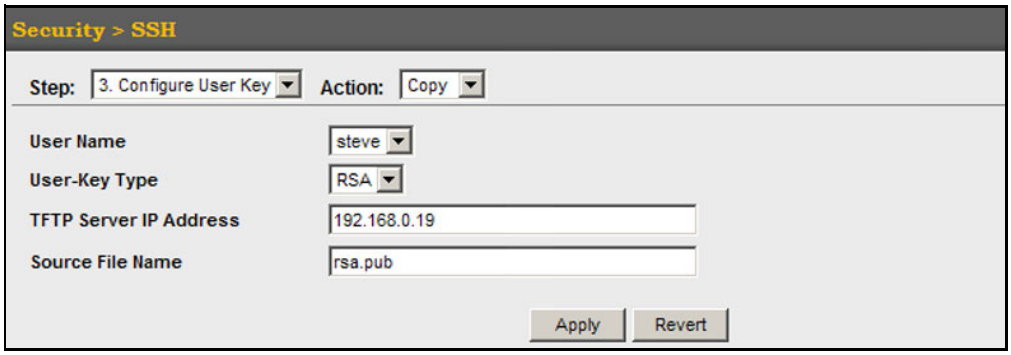
- **Source File Name** – The public key file to upload.

WEB INTERFACE

To copy the SSH user's public key in the web interface:

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.

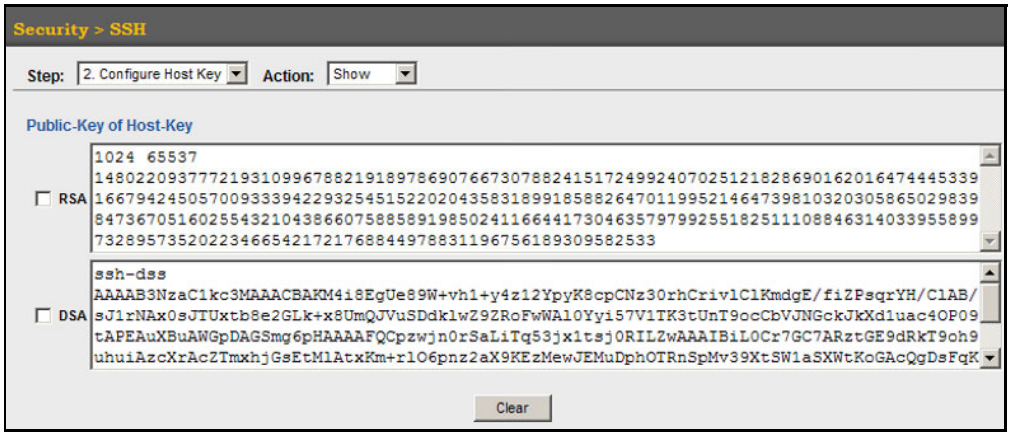
Figure 149: Copying the SSH User's Public Key



To display or clear the SSH user's public key in the web interface:

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 150: Showing the SSH User's Public Key



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), or any frames (based on MAC address or Ethernet type). To filter incoming packets, first create an access list, add the required rules, and then bind the list to a specific port.

Configuring Access Control Lists –

An ACL is a sequential list of permit or deny conditions that apply to IP addresses, MAC addresses, or other more specific criteria. This switch tests ingress packets against the conditions in an ACL one by one. A packet will be accepted as soon as it matches a permit rule, or dropped as soon as it matches a deny rule. If no rules match, the packet is accepted.

COMMAND USAGE

The following restrictions apply to ACLs:

- The maximum number of ACLs is 64.
- The maximum number of rules per system is 512 rules.
- An ACL can have up to 32 rules. However, due to resource restrictions, the average number of rules bound to the ports should not exceed 20.

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 524

PARAMETERS

These parameters are displayed in the web interface:

Add

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

Add Rule

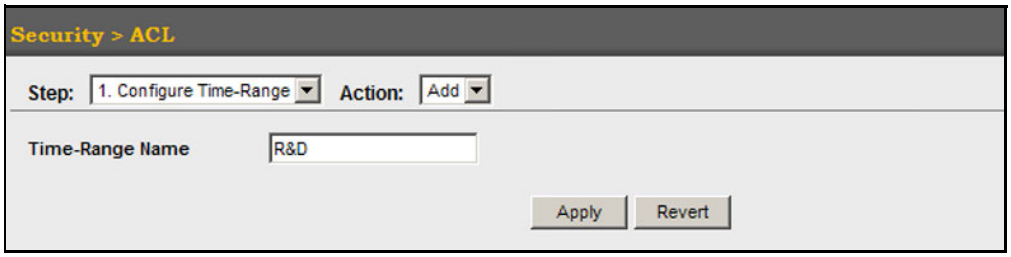
- **Time-Range** – Name of a time range.
- **Mode**
  - **Absolute** – Specifies a specific time or time range.
    - **Start/End** – Specifies the hours, minutes, month, day, and year at which to start or end.
  - **Periodic** – Specifies a periodic interval.
    - **Start/End** – Specifies the days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

WEB INTERFACE

To configure a time range in the web interface:

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.

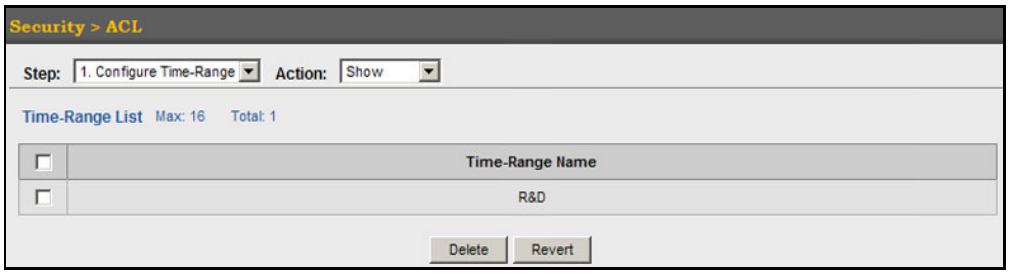
Figure 151: Setting the Name of a Time Range



To show a list of time ranges in the web interface:

1. Click Security, ACL.
2. Select Configure Time Range from the Step list.
3. Select Show from the Action list.

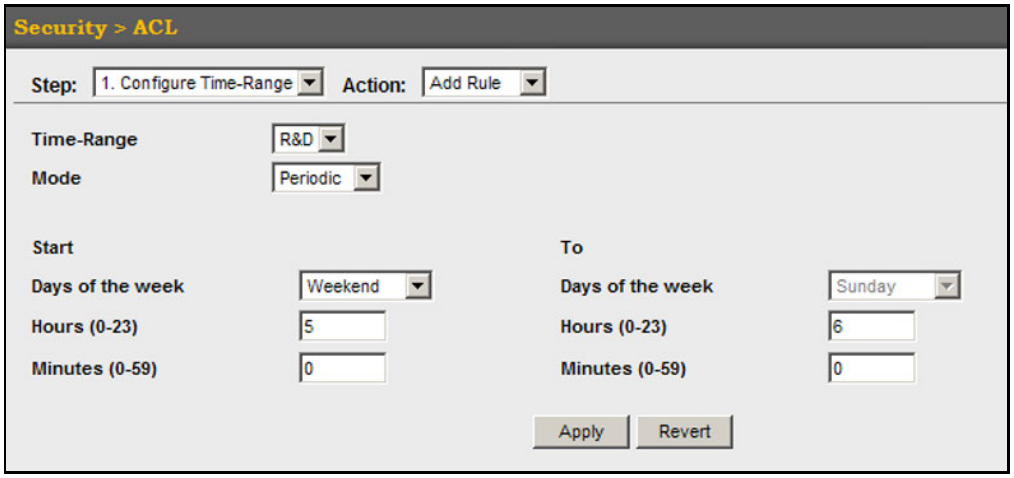
Figure 152: Showing a List of Time Ranges



To configure a rule for a time range in the web interface:

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.

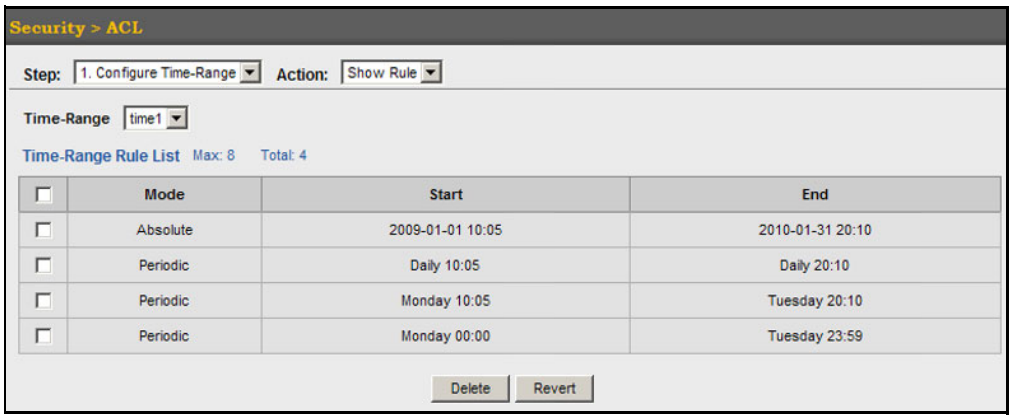
Figure 153: Add a Rule to a Time Range



To show the rules configured for a time range in the web interface:

1. Click Security, ACL.
2. Select Configure Time Range from the Step list.
3. Select Show Rule from the Action list.

Figure 154: Showing the Rules Configured for a Time Range



SHOWING TCAM UTILIZAITON

Use the Security > ACL (Configure ACL - Show TCAM) page to show utilization parameters for TCAM (Ternary Content Addressable Memory), including the number policy control entries in use, the number of free entries, and the overall percentage of TCAM in use.

CLI REFERENCES

- "show access-list tcam-utilization" on page 482

COMMAND USAGE

Policy control entires (PCEs) are used by various system functions which rely on rule-based searches, including Access Control Lists (ACLs), IP Source Guard filter rules, Quality of Service (QoS) processes, or traps.

For example, when binding an ACL to a port, each rule in an ACL will use two PCEs; and when setting an IP Source Guard filter rule for a port, the system will also use two PCEs.

PARAMETERS

These parameters are displayed in the web interface:

- **Total Policy Control Entries** – The number policy control entries in use.
- **Free Policy Control Entries** – The number of policy control entires available for use.
- **Entries Used by System** – The number of policy control entries used by the operating system.

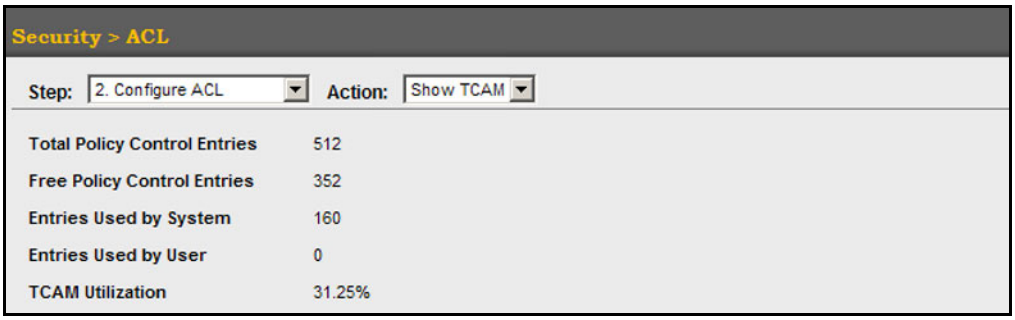
- **Entries Used by User** – The number of policy control entries used by configuration settings, such as access control lists.
- **TCAM Utilization** – The overall percentage of TCAM in use.

WEB INTERFACE

To show information on TCAM utilization in the web interface:

1. Click Security, ACL.
2. Select Configure ACL from the Step list.
3. Select Show TCM from the Action list.

Figure 155: Showing TCAM Utilization



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 662
- "show ip access-list" on page 667

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.
  - **MAC** – MAC ACL mode filters packets based on the source or destination MAC address and the Ethernet frame type (RFC 1060).

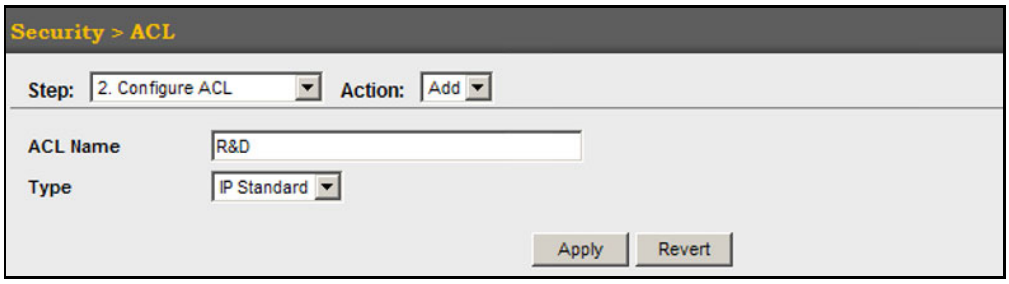
- **ARP** – ARP ACL specifies static IP-to-MAC address bindings used for ARP inspection (see "ARP Inspection" on page 302).

WEB INTERFACE

To configure the name and type of an ACL in the web interface:

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.

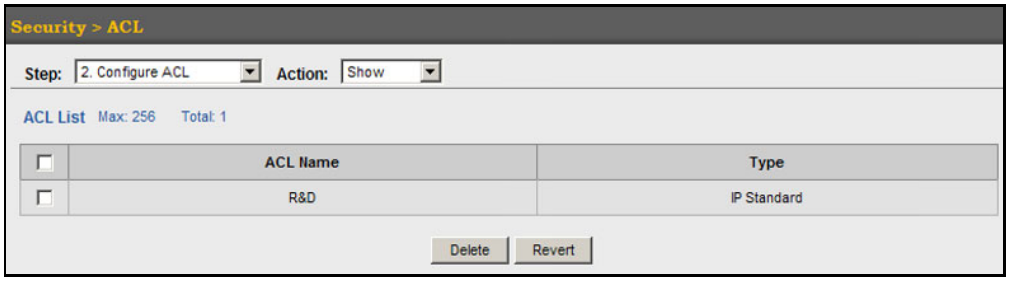
Figure 156: Creating an ACL



To show a list of ACLs in the web interface:

1. Click Security, ACL.
2. Select Configure ACL from the Step list.
3. Select Show from the Action list.

Figure 157: Showing a List of ACLs



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 663
- "show ip access-list" on page 667
- "Time Range" on page 524

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.

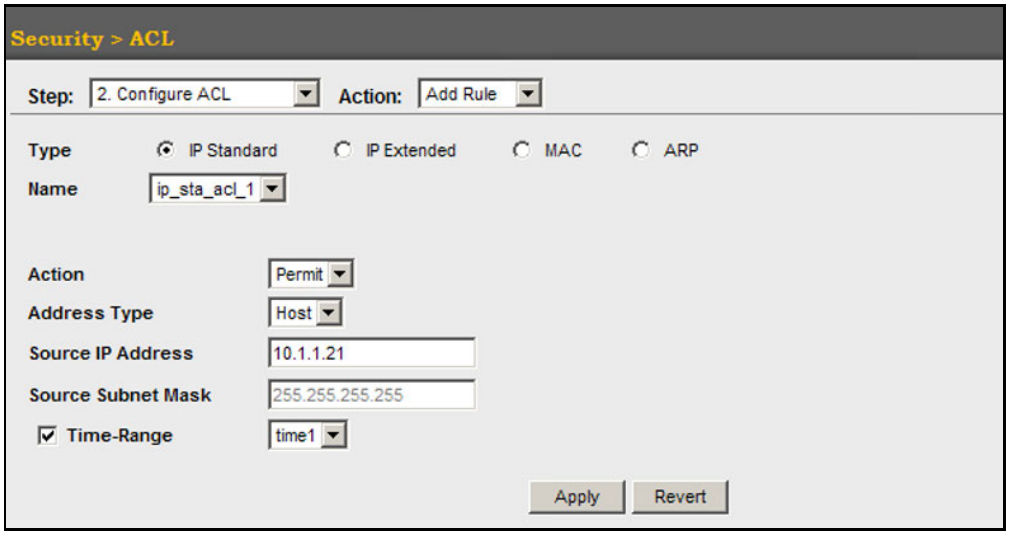
WEB INTERFACE

To add rules to a Standard IP ACL in the web interface:

1. Click Security, ACL.
2. Select Configure ACL from the Step list.
3. Select Add Rule from the Action list.
4. Select Standard IP 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 158: Configuring a Standard IPv4 ACL



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 664
- "show ip access-list" on page 667
- "Time Range" on page 524

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 294.)
- **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 IP ACL in the web interface:

1. Click Security, ACL.
2. Select Configure ACL from the Step list.
3. Select Add Rule from the Action list.
4. Select Extended IP from the Type list.

5. Select the name of an ACL from the Name list.

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

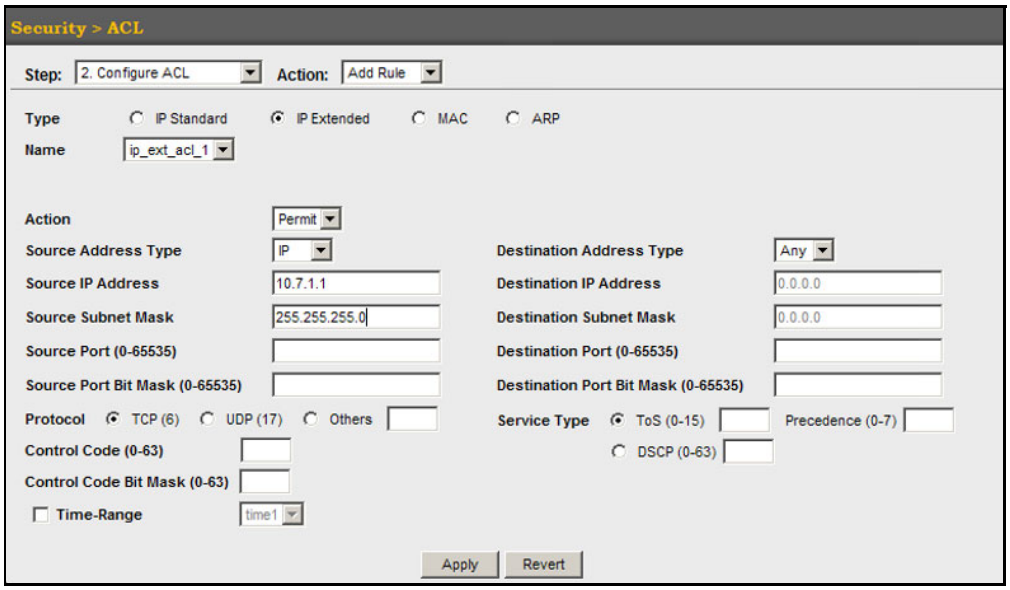
7. Select the address type (Any, Host, or IP).

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 159: Configuring an Extended IPv4 ACL



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 669
- "show ip access-list" on page 667
- "Time Range" on page 524

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 in the web interface:

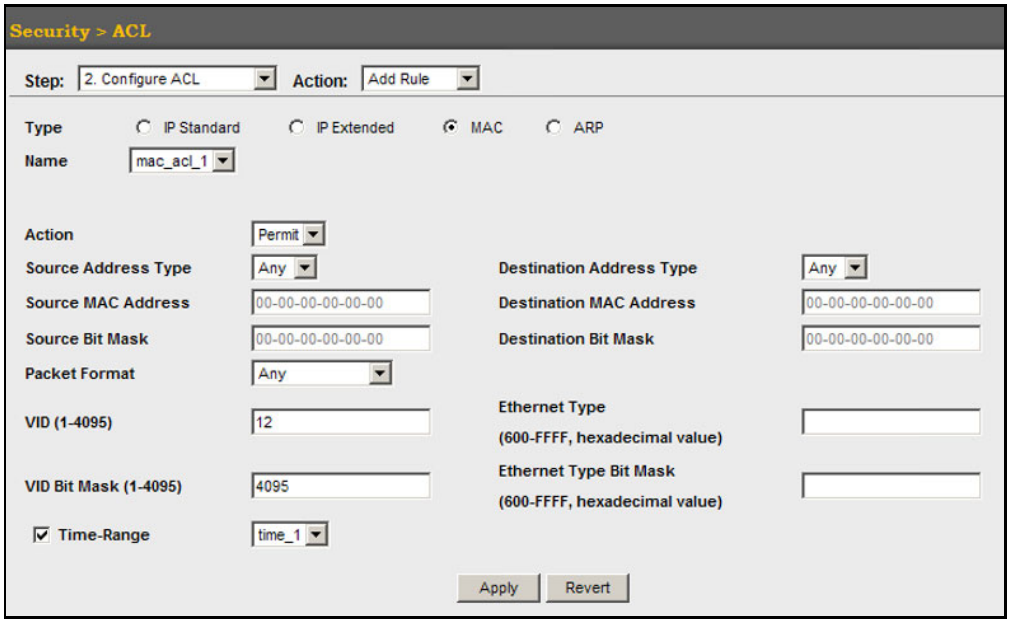
1. Click Security, ACL.
2. Select Configure ACL from the Step list.
3. Select Add Rule from the Action list.
4. Select MAC from the Type list.
5. Select the name of an ACL from the Name list.
6. Specify the action (i.e., Permit or Deny).
7. Select the address type (Any, Host, or MAC).

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



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 303).

CLI REFERENCES

- "permit, deny (ARP ACL)" on page 674
- "show ip access-list" on page 667
- "Time Range" on page 524

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 294.)

- **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.

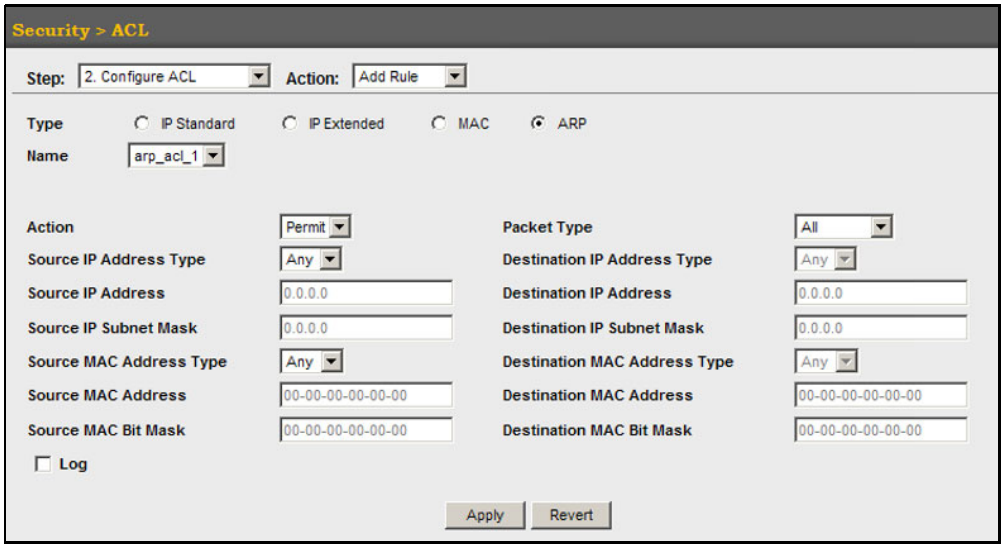
- **Log** – Logs a packet when it matches the access control entry.

WEB INTERFACE

To add rules to an ARP ACL in the web interface:

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



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 666
- "show ip access-group" on page 667
- "mac access-group" on page 671
- "show mac access-group" on page 672
- "Time Range" on page 524

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** – Fixed port or SFP module. (ES-3026/P: 1-26, ES-3024G/P: 1-24)
- **ACL** – ACL used for ingress packets.
- **Time Range** – Name of a time range.

WEB INTERFACE

To bind an ACL to a port in the web interface:

1. Click Security, ACL.

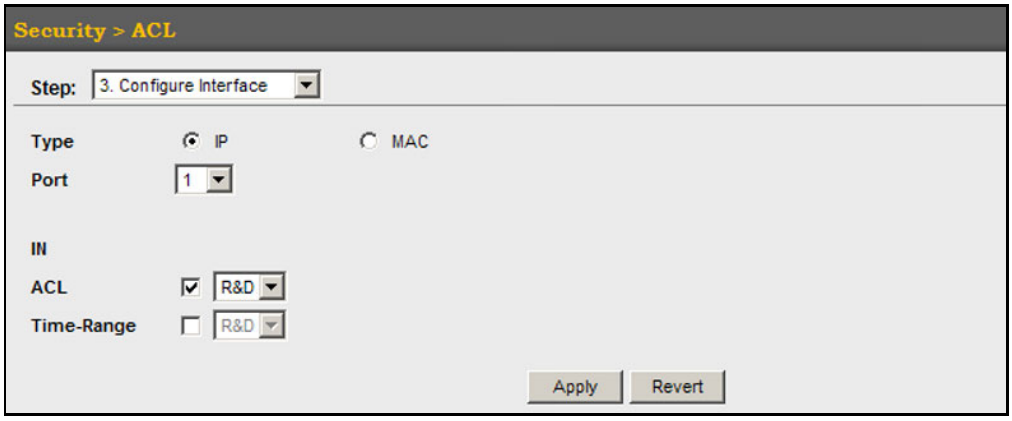
2. Select Configure Interface from the Step list.

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



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 333). 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 299).

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 651

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:

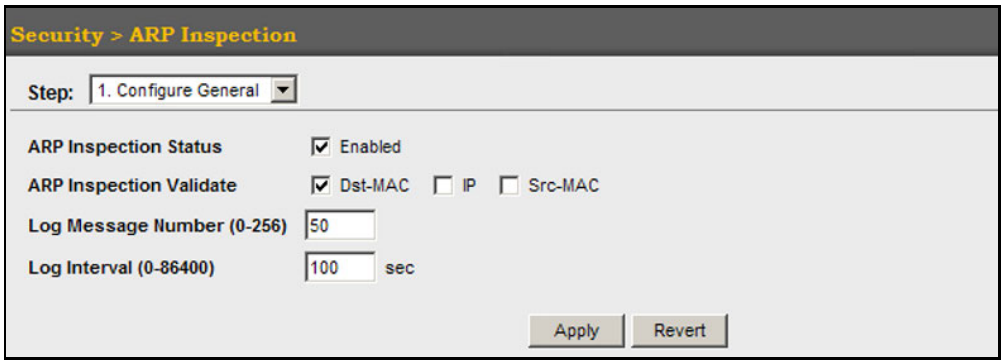
- **ARP Inspection Status** – Enables ARP Inspection globally. (Default: Disabled)
- **ARP Inspection Validation** – Enables extended ARP Inspection Validation if any of the following options are enabled. (Default: Disabled)
  - **Dst-MAC** – Validates the destination MAC address in the Ethernet header 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 in the web interface:

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



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 651

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 299).
- 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:

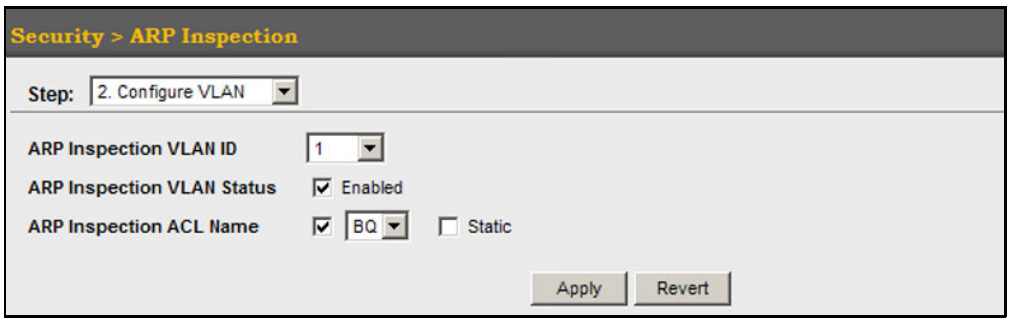
- **ARP Inspection VLAN ID** – Selects any configured VLAN. (Default: 1)
- **ARP Inspection VLAN Status** – Enables ARP Inspection for the selected VLAN. (Default: Disabled)
- **ARP Inspection ACL Name**
  - *ARP ACL* – Allows selection of any configured ARP ACLs. (Default: None)
  - **Static** – When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

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



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 651

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 in the web interface:

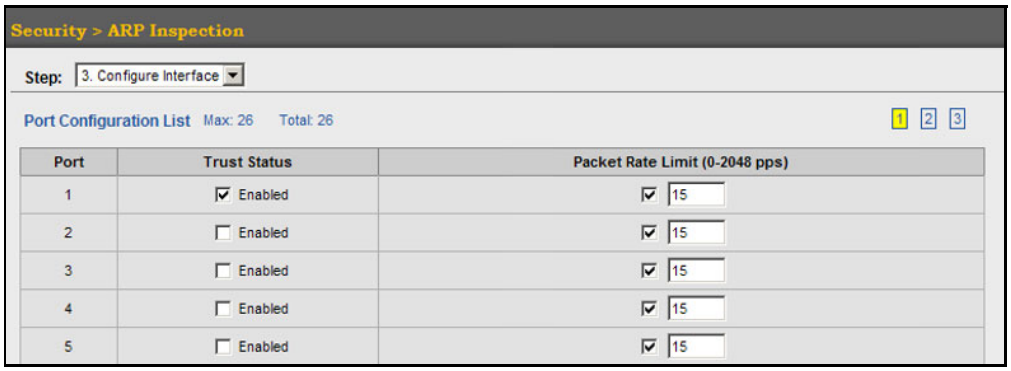
1. Click Security, ARP Inspection.

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



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 659

PARAMETERS

These parameters are displayed in the web interface:

Table 19: ARP Inspection Statistics

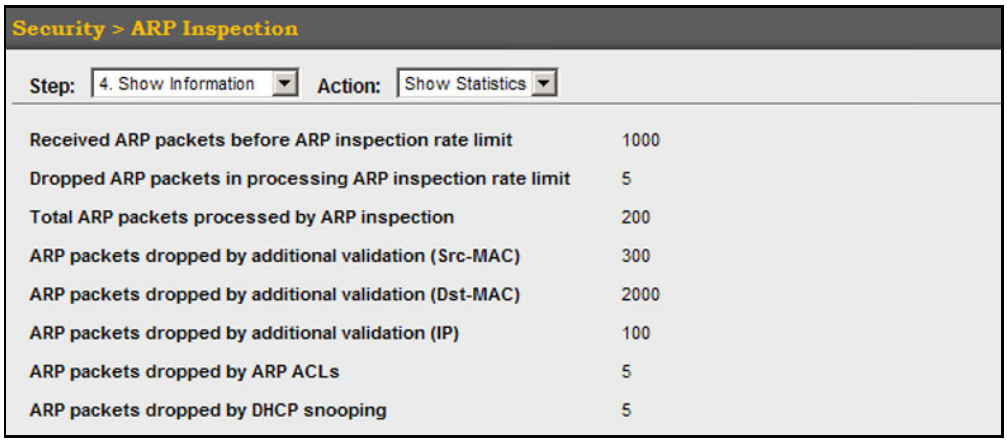
Parameter	Description
Received ARP packets before ARP inspection rate limit	Count of ARP packets received but not exceeding the ARP Inspection rate limit.
Dropped ARP packets in the process of ARP inspection rate limit	Count of ARP packets exceeding (and dropped by) ARP rate limiting.
ARP packets dropped 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 in the web interface:

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



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 659

PARAMETERS

These parameters are displayed in the web interface:

Table 20: ARP Inspection Log

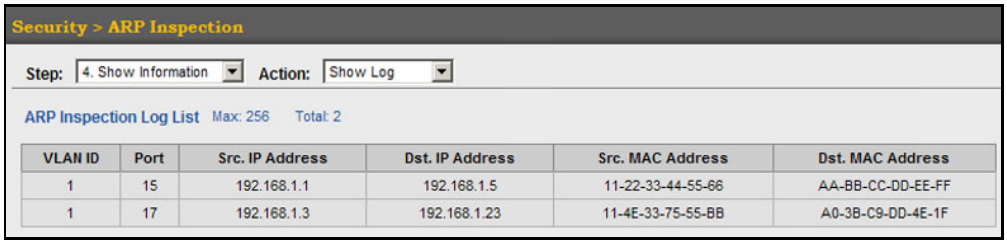
Parameter	Description
VLAN ID	The VLAN where this packet was seen.
Port	The port where this packet was seen.
Src. IP Address	The source IP address in the packet.
Dst. IP Address	The destination IP address in the packet.
Src. MAC Address	The source MAC address in the packet.
Dst. MAC Address	The destination MAC address in the packet.

WEB INTERFACE

To display the ARP Inspection log in the web interface:

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



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 612

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:

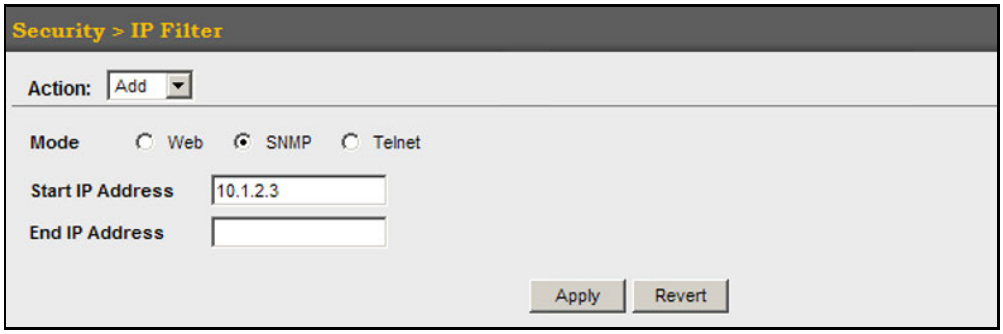
- **Mode**
  - **Web** – Configures IP address(es) for the web group.
  - **SNMP** – Configures IP address(es) for the SNMP group.
  - **Telnet** – Configures IP address(es) for the Telnet group.
- **Start IP Address** – A single IP address, or the starting address of a range.
- **End IP Address** – The end address of a range.

WEB INTERFACE

To create a list of IP addresses authorized for management access in the web interface:

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

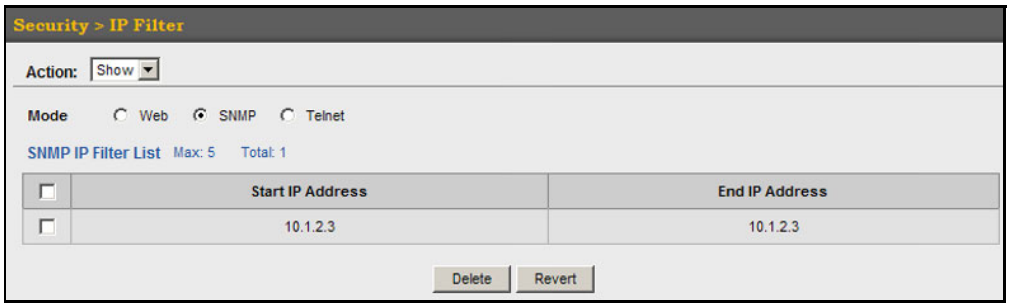


To show a list of IP addresses authorized for management access in the web interface:

1. Click Security, IP Filter.

2. Select Show from the Action list.

Figure 169: Showing IP Addresses Authorized for Management Access



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 178). 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 616

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 113).

PARAMETERS

These parameters are displayed in the web interface:

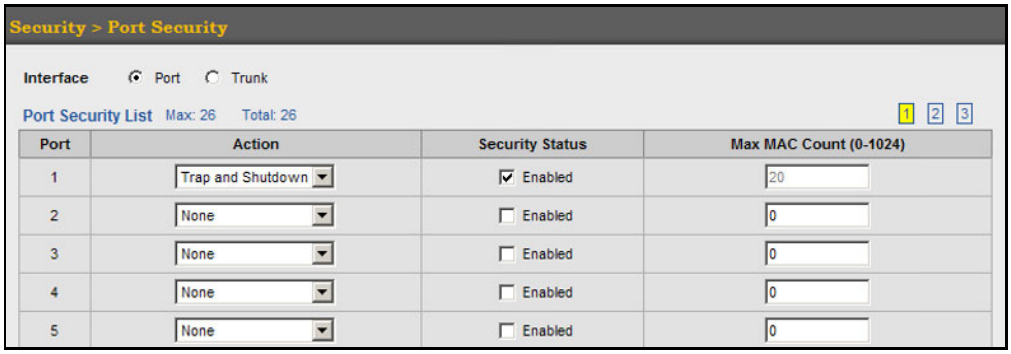
- **Port** – Port number.
- **Action** – Indicates the action to be taken when a port security violation is detected:
  - **None**: No action should be taken. (This is the default.)
  - **Trap**: Send an SNMP trap message.
  - **Shutdown**: Disable the port.
  - **Trap and Shutdown**: Send an SNMP trap 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)

WEB INTERFACE

To configure port security in the web interface:

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

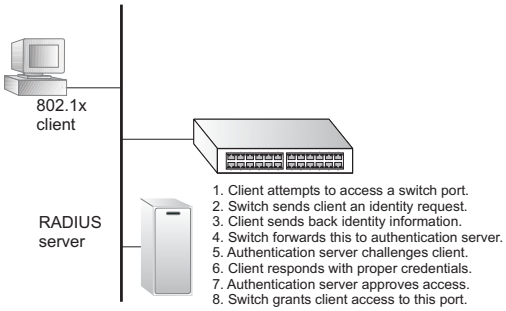
Figure 170: Configuring Port Security



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.

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 597

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.

- **Identity Profile User Name** – The dot1x supplicant user name. (Range: 1-8 characters)

  The global supplicant user name and password are used to identify this switch as a supplicant when responding to an MD5 challenge from the authenticator. These parameters must be set when this switch passes client authentication requests to another authenticator on the network (see "Configuring Port Supplicant Settings for 802.1X" on page 321).

- **Set Password** – Allows the dot1x supplicant password to be entered.

- **Indentity Profile Password** – The dot1x supplicant password used to identify this switch as a supplicant when responding to an MD5 challenge from the authenticator. (Range: 1-8 characters)

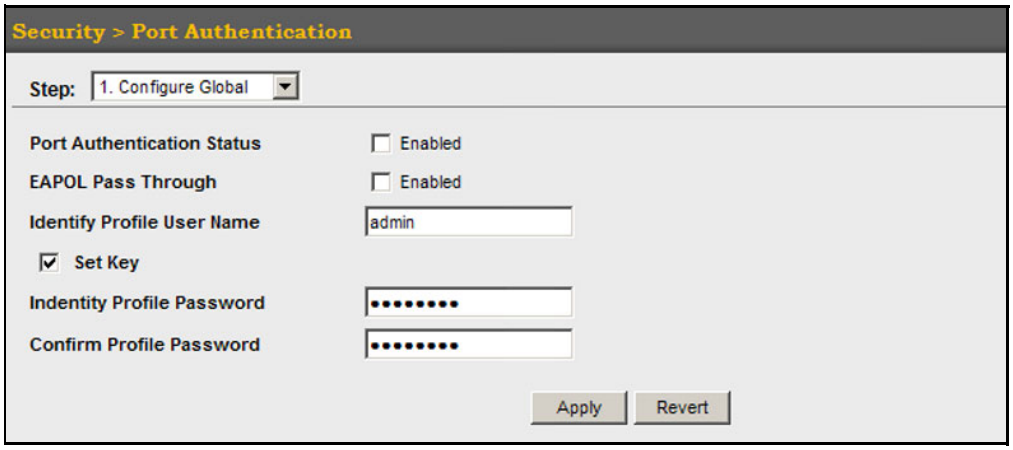
- **Confirm Profile Password** – This field is used to confirm the dot1x supplicant password.

WEB INTERFACE

To configure global settings for 802.1X in the web interface:

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 171: Configuring Global Settings for 802.1X Port Authentication



CONFIGURING PORT AUTHENTICATOR SETTINGS FOR 802.1X

Use the Security > Port Authentication (Configure Interface – Authenticator) 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 597

COMMAND USAGE

- When the switch functions as a local authenticator between supplicant devices attached to the switch and the authentication server, configure the parameters for the exchange of EAP messages between the authenticator and clients on the Authenticator configuration page.

- When devices attached to a port must submit requests to another authenticator on the network, configure the Identity Profile parameters on the Configure Global page (see "Configuring 802.1X Global Settings" on page 315) which identify this switch as a supplicant, and configure the supplicant parameters for those ports which must authenticate clients through the remote authenticator (see "Configuring Port Supplicant Settings for 802.1X" on page 321).

- This switch can be configured to serve as the authenticator on selected ports by setting the Control Mode to Auto on this configuration page, and as a supplicant on other ports by the setting the control mode to Force-Authorized on this page and enabling the PAE supplicant on the Supplicant configuation page.

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 150) and mapped on each port (See "Configuring Network Access for Ports" on page 270).

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

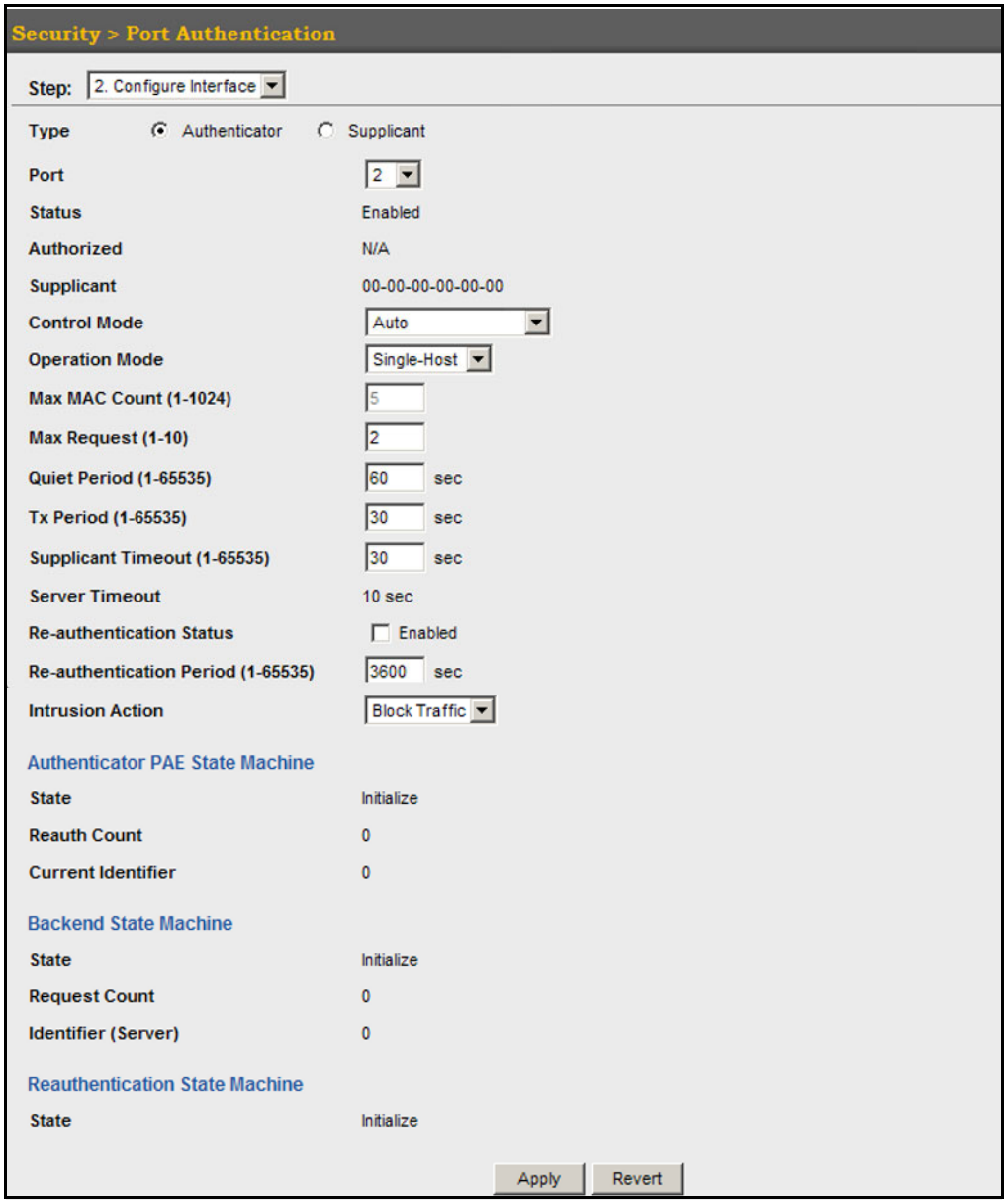
- **State** – Current state (including initialize, reauthenticate).

WEB INTERFACE

To configure port authenticator settings for 802.1X in the web interface:

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 172: Configuring Interface Settings for 802.1X Port Authenticator



CONFIGURING PORT SUPPLICANT SETTINGS FOR 802.1X

Use the Security > Port Authentication (Configure Interface – Supplicant) page to configure 802.1X port settings for supplicant requests issued from a port to an authenticator on another device. When 802.1X is enabled and the control mode is set to Force-Authorized (see "Configuring Port Authenticator Settings for 802.1X" on page 317), you need to configure the parameters for the client supplicant process if the client must be authenticated through another device in the network.

CLI REFERENCES

- "802.1X Port Authentication" on page 597

COMMAND USAGE

- When devices attached to a port must submit requests to another authenticator on the network, configure the Identity Profile parameters on the Configure Global page (see "Configuring 802.1X Global Settings" on page 315) which identify this switch as a supplicant, and configure the supplicant parameters for those ports which must authenticate clients through the remote authenticator on this configuration page. When PAE supplicant mode is enabled on a port, it will not respond to dot1x messages meant for an authenticator.

- This switch can be configured to serve as the authenticator on selected ports by setting the Control Mode to Auto on the Authenticator configuration page, and as a supplicant on other ports by the setting the control mode to Force-Authorized on that configuration page and enabling the PAE supplicant on the Supplicant configuation page.

PARAMETERS

These parameters are displayed in the web interface:

- **Port** – Port number.

- **PAE Supplicant** – Enables PAE supplicant mode. (Default: Disabled)

  If the attached client must be authenticated through another device in the network, supplicant status must be enabled.

  Supplicant status can only be enabled if PAE Control Mode is set to “Force-Authorized” on this port (see "Configuring Port Authenticator Settings for 802.1X" on page 317).

  PAE supplicant status cannot be enabled if a port is a member of trunk or LACP is enabled on the port.

- **Authentication Period** – The time that a supplicant port waits for a response from the authenticator. (Range: 1-65535 seconds; Default: 30 seconds)

- **Hold Period** – The time that a supplicant port waits before resending its credentials to find a new an authenticator. (Range: 1-65535 seconds; Default: 30 seconds)

- **Start Period** – The time that a supplicant port waits before resending an EAPOL start frame to the authenticator.. (Range: 1-65535 seconds; Default: 30 seconds)

- **Maximum Start** – The maximum number of times that a port supplicant will send an EAP start frame to the client before assuming that the client is 802.1X unaware. (Range: 1-65535; Default: 3)

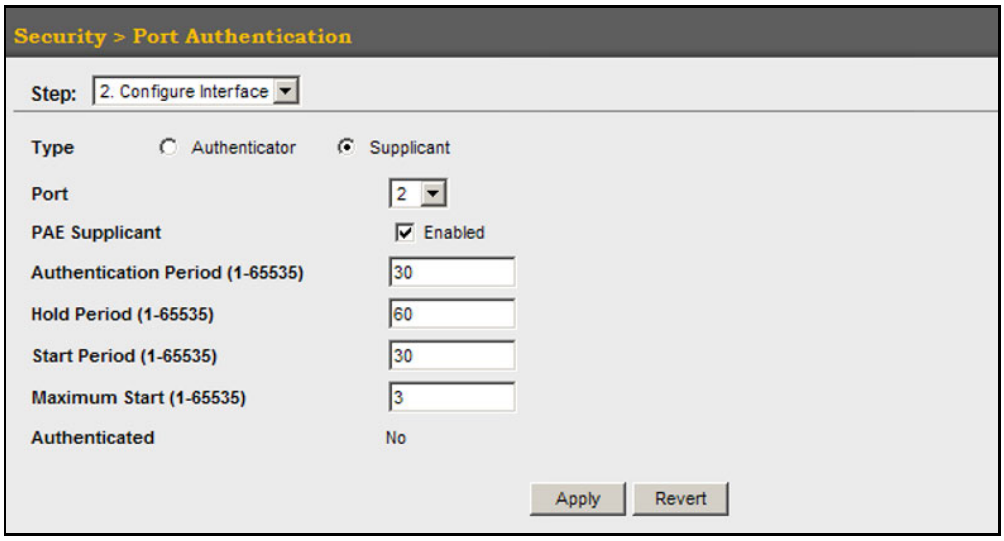
- **Authenticated** – Shows whether or not the supplicant has been authenticated.

WEB INTERFACE

To configure port authenticator settings for 802.1X in the web interface:

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

Figure 173: Configuring Interface Settings for 802.1X Port Supplicant



DISPLAYING 802.1X STATISTICS

Use the Security > Port Authentication (Configure Interface) page to display statistics for dot1x protocol exchanges for any port.

CLI REFERENCES

- "show dot1x" on page 609

PARAMETERS

These parameters are displayed in the web interface:

Table 21: 802.1X Statistics

Parameter	Description
Authenticator	
Rx EAPOL Start	The number of EAPOL Start frames that have been received by this Authenticator.
Rx EAPOL Logoff	The number of EAPOL Logoff frames that have been received by this Authenticator.
Rx EAPOL Invalid	The number of EAPOL frames that have been received by this Authenticator in which the frame type is not recognized.
Rx EAPOL Total	The number of valid EAPOL frames of any type that have been received by this Authenticator.
Rx Last EAPOLVer	The protocol version number carried in the most recent EAPOL frame received by this Authenticator.
Rx Last EAPOLSrc	The source MAC address carried in the most recent EAPOL frame received by this Authenticator.
Rx EAP Resp/Id	The number of EAP Resp/Id frames that have been received by this Authenticator.
Rx EAP Resp/Oth	The number of valid EAP Response frames (other than Resp/Id frames) that have been received by this Authenticator.
Rx EAP LenError	The number of EAPOL frames that have been received by this Authenticator in which the Packet Body Length field is invalid.
Tx EAP Req/Id	The number of EAP Req/Id frames that have been transmitted by this Authenticator.
Tx EAP Req/Oth	The number of EAP Request frames (other than Rq/Id frames) that have been transmitted by this Authenticator.
Tx EAPOL Total	The number of EAPOL frames of any type that have been transmitted by this Authenticator.
Supplicant	
Rx EAPOL Invalid	The number of EAPOL frames that have been received by this Supplicant in which the frame type is not recognized.
Rx EAPOL Total	The number of valid EAPOL frames of any type that have been received by this Supplicant.
Rx Last EAPOLVer	The protocol version number carried in the most recent EAPOL frame received by this Supplicant.
Rx Last EAPOLSrc	The source MAC address carried in the most recent EAPOL frame received by this Supplicant.
Rx EAP Resp/Id	The number of EAP Resp/Id frames that have been received by this Supplicant.
Rx EAP Resp/Oth	The number of valid EAP Response frames (other than Resp/Id frames) that have been received by this Supplicant.
Rx EAP LenError	The number of EAPOL frames that have been received by this Supplicant in which the Packet Body Length field is invalid.

Table 21: 802.1X Statistics (Continued)

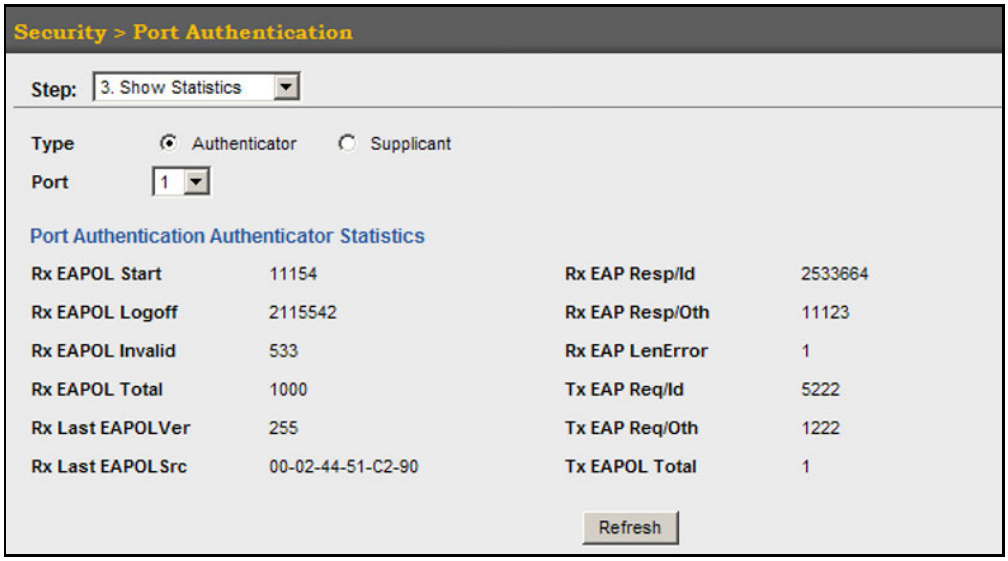
Parameter	Description
Tx EAPOL Total	The number of EAPOL frames of any type that have been transmitted by this Supplicant.
Tx EAPOL Start	The number of EAPOL Start frames that have been transmitted by this Supplicant.
Tx EAPOL Logoff	The number of EAPOL Logoff frames that have been transmitted by this Supplicant.
Tx EAP Req/Id	The number of EAP Req/Id frames that have been transmitted by this Supplicant.
Tx EAP Req/Oth	The number of EAP Request frames (other than Rq/Id frames) that have been transmitted by this Supplicant.

WEB INTERFACE

To display port authenticator statistics for 802.1X in the web interface:

1. Click Security, Port Authentication.
2. Select Show Statistics from the Step list.
3. Click Authenticator.

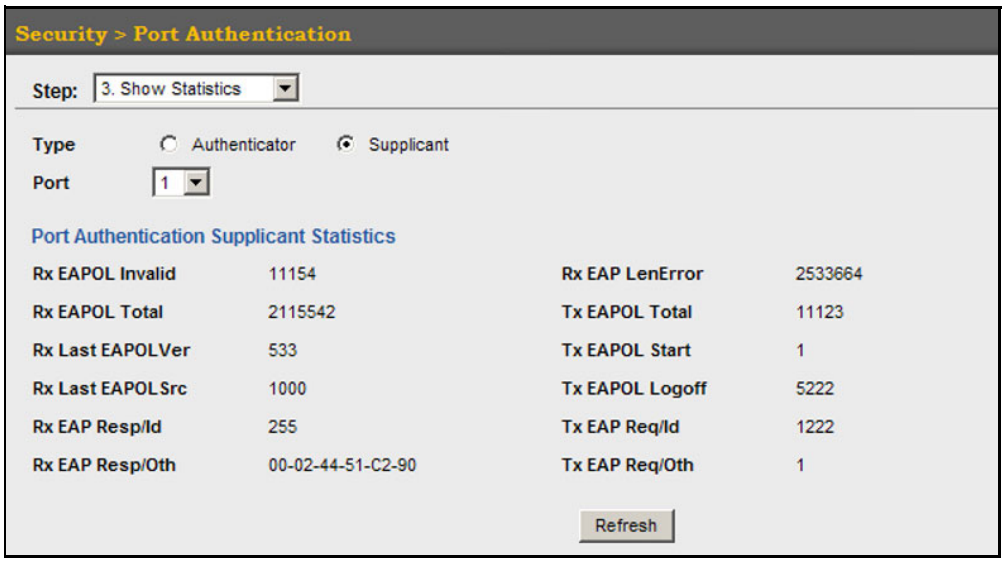
Figure 174: Showing Statistics for 802.1X Port Authenticator



To display port supplicant statistics for 802.1X in the web interface:

1. Click Security, Port Authentication.
2. Select Show Statistics from the Step list.
3. Click Supplicant.

Figure 175: Showing Statistics for 802.1X Port Supplicant



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 330). 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 648

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 330), 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 333), 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.

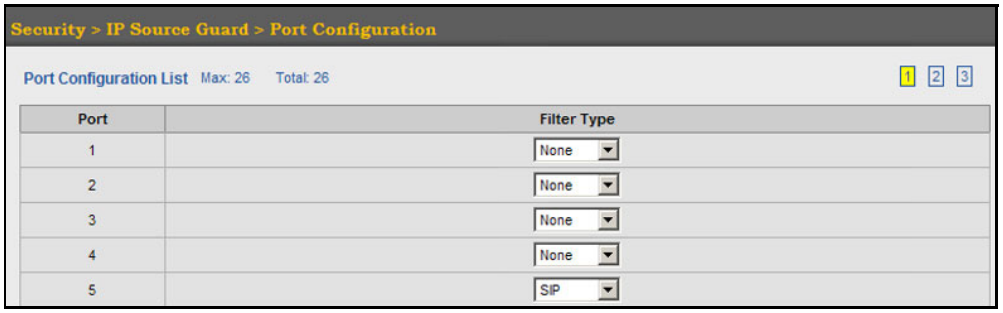
- **SIP-MAC** – Enables traffic filtering based on IP addresses and corresponding MAC addresses stored in the binding table.

WEB INTERFACE

To set the IP Source Guard filter for ports in the web interface:

1. Click Security, IP Source Guard, Port Configuration.
2. Set the required filtering type for each port.
3. Click Apply

Figure 176: Setting the Filter Type for IP Source Guard



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 647

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:

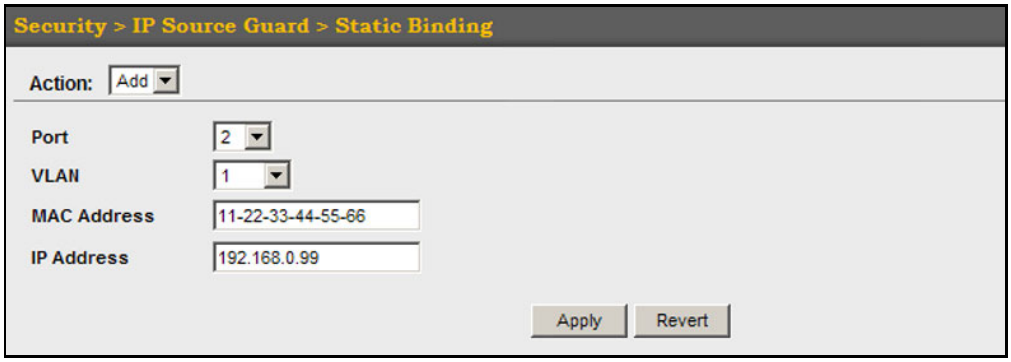
- **Port** – The port to which a static entry is bound.
- **VLAN** – ID of a configured VLAN (Range: 1-4093)
- **MAC Address** – A valid unicast MAC address.
- **IP Address** – A valid unicast IP address, including classful types A, B or C.

WEB INTERFACE

To configure static bindings for IP Source Guard in the web interface:

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

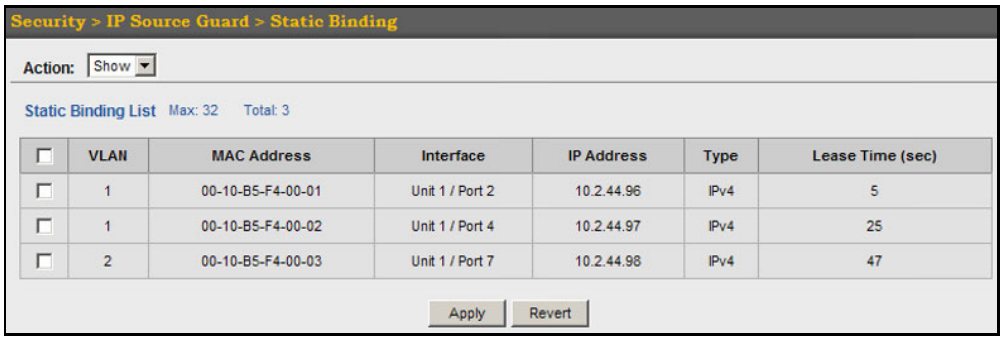
Figure 177: Configuring Static Bindings for IP Source Guard



To display static bindings for IP Source Guard in the web interface:

1. Click Security, IP Source Guard, Static Configuration.
2. Select Show from the Action list.

Figure 178: Displaying Static Bindings for IP Source Guard



	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

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 646

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

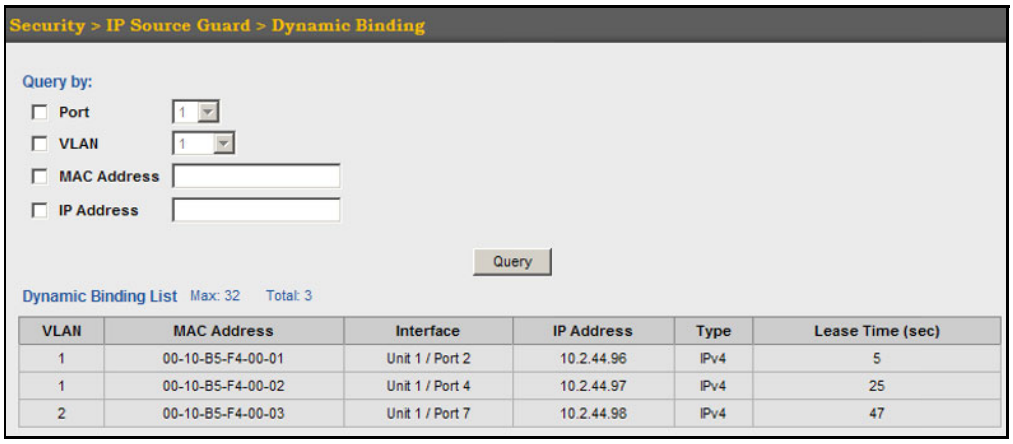
- **VLAN** – VLAN to which this entry is bound.
- **MAC Address** – Physical address associated with the entry.
- **Interface** – Port to which this entry is bound.
- **IP Address** – IP address corresponding to the client.
- **Type** – Static or dynamic binding.
- **Lease Time** – The time for which this IP address is leased to the client.

WEB INTERFACE

To display the binding table for IP Source Guard in the web interface:

1. Click Security, IP Source Guard, Dynamic Binding.
2. Mark the search criteria, and enter the required values.
3. Click Query

Figure 179: Showing the IP Source Guard Binding Table



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 638

PARAMETERS

These parameters are displayed in the web interface:

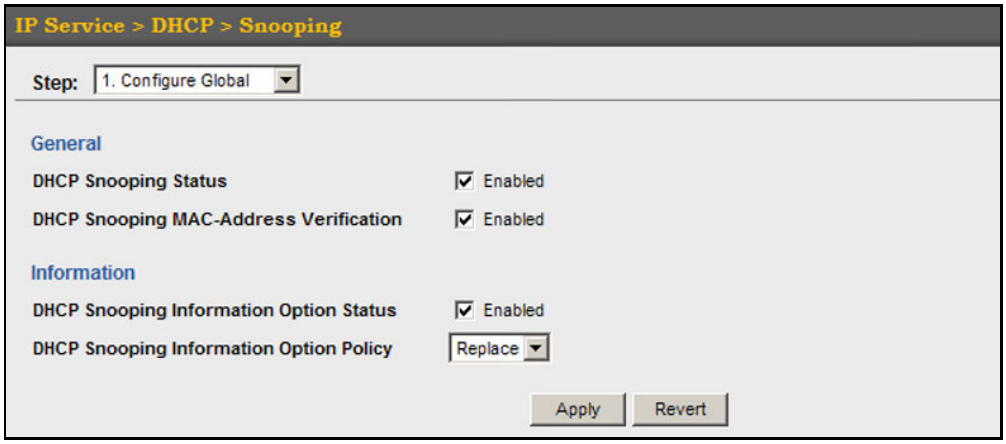
- **DHCP Snooping Status –** Enables DHCP snooping globally. (Default: Disabled)
- **DHCP Snooping MAC-Address Verification** – Enables or disables MAC address verification. If the source MAC address in the Ethernet header of the packet is not same as the client's hardware address in the DHCP packet, 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 in the web interface:

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 180: Configuring Global Settings for DHCP Snooping



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 643

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

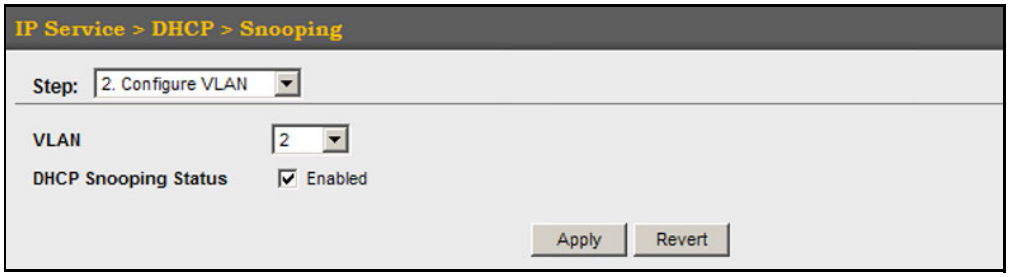
To configure global settings for DHCP Snooping in the web interface:

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 181: Configuring DHCP Snooping on a VLAN



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 644

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

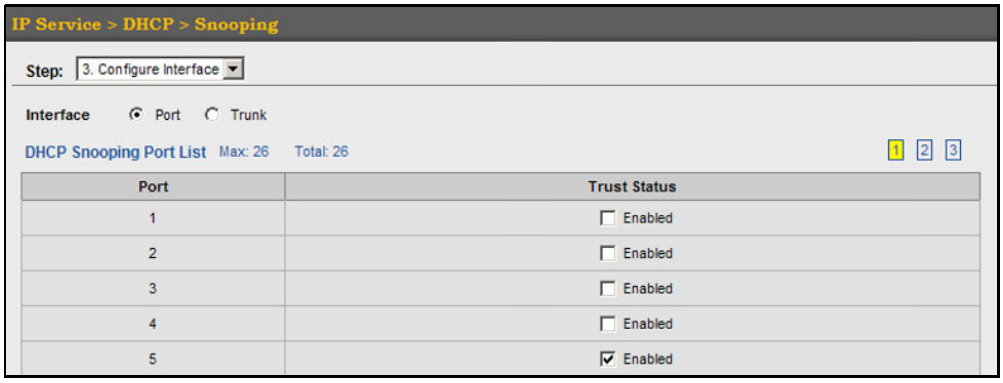
To configure global settings for DHCP Snooping in the web interface:

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 182: Configuring the Port Mode for DHCP Snooping



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 646

PARAMETERS

These parameters are displayed in the web interface:

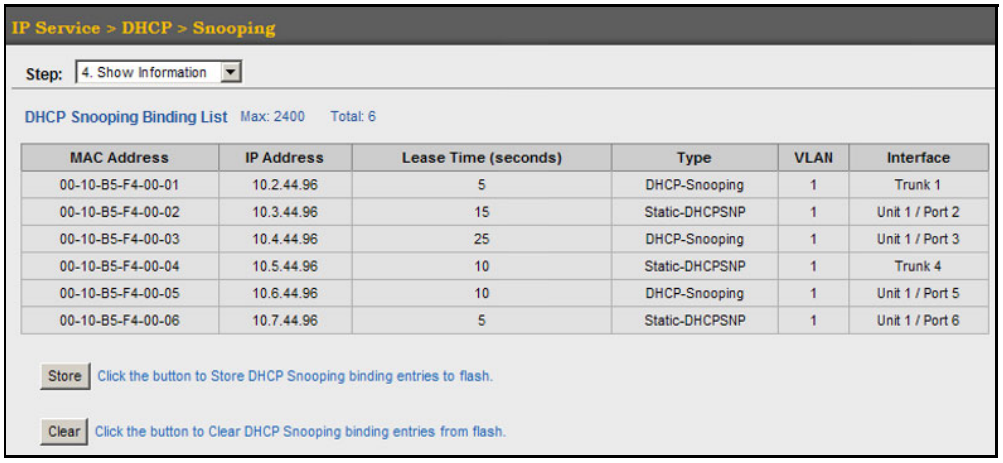
- **MAC Address** – Physical address associated with the entry.
- **IP Address** – IP address corresponding to the client.
- **Lease Time** (Seconds) – The time for which this IP address is leased to the client.
- **Type** – Entry types include:
  - **DHCP-Snooping** – Dynamically snooped.
  - **Static-DHCPSNP** – 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 in the web interface:

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 183: Displaying the Binding Table for DHCP Snooping



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

15 BASIC ADMINISTRATION PROTOCOLS

This chapter describes basic administration tasks including configuring logging of error messages, Link Layer Discovery Protocol (LLDP), and Simple Network Management Protocol (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 508

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 22: 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)

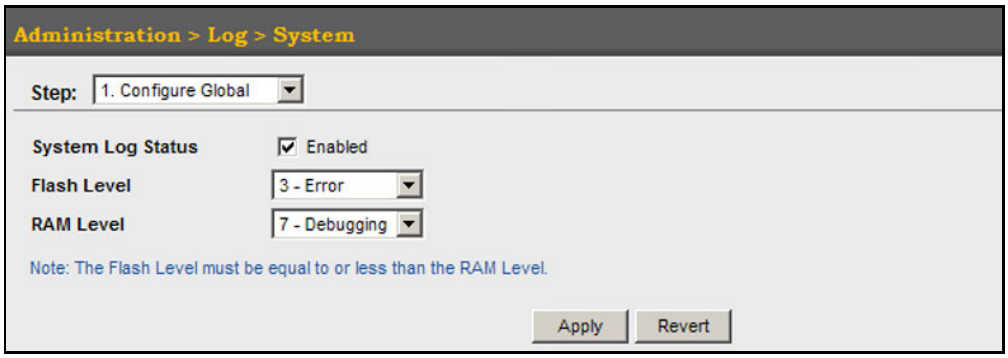
NOTE: The Flash Level must be equal to or less than the RAM Level.

WEB INTERFACE

To configure the logging of error messages to system memory in the web interface:

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 184: Configuring Settings for System Memory Logs



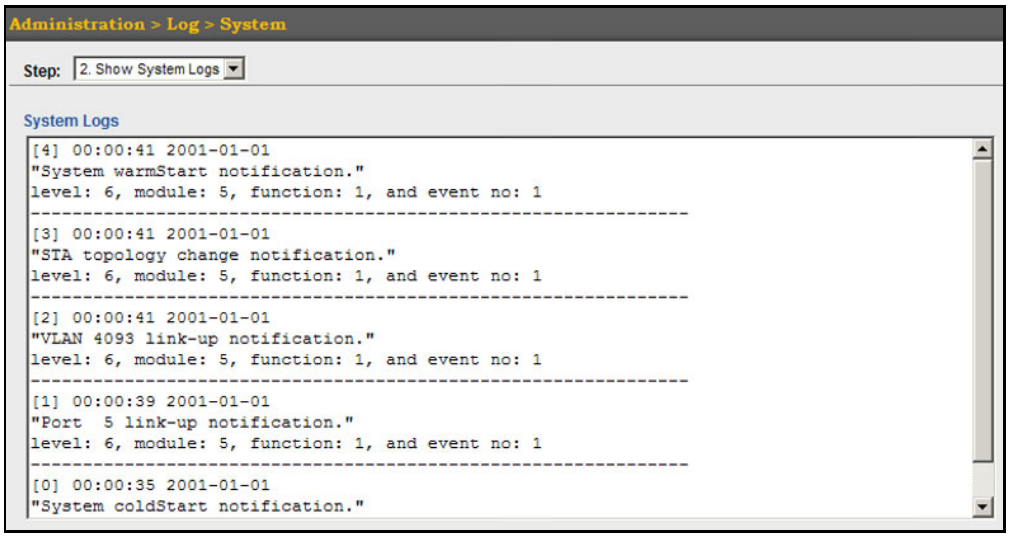
To show the error messages logged to system memory in the web interface:

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 185: Showing Error Messages Looged to System Memory



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 508

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 IP address of a remote server which will be sent syslog messages.

WEB INTERFACE

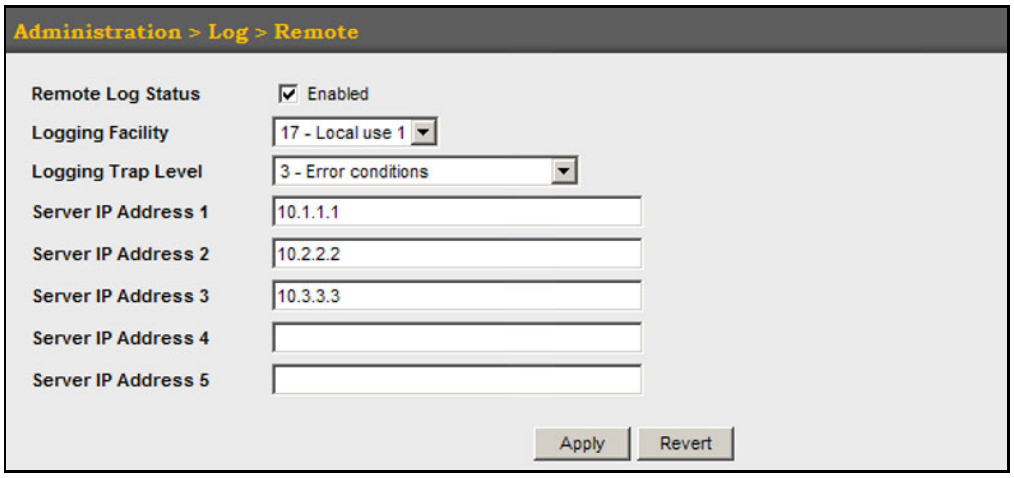
To configure the logging of error messages to remote servers in the web interface:

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 186: Configuring Settings for Remote Logging of Error Messages



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 515

PARAMETERS

These parameters are displayed in the web interface:

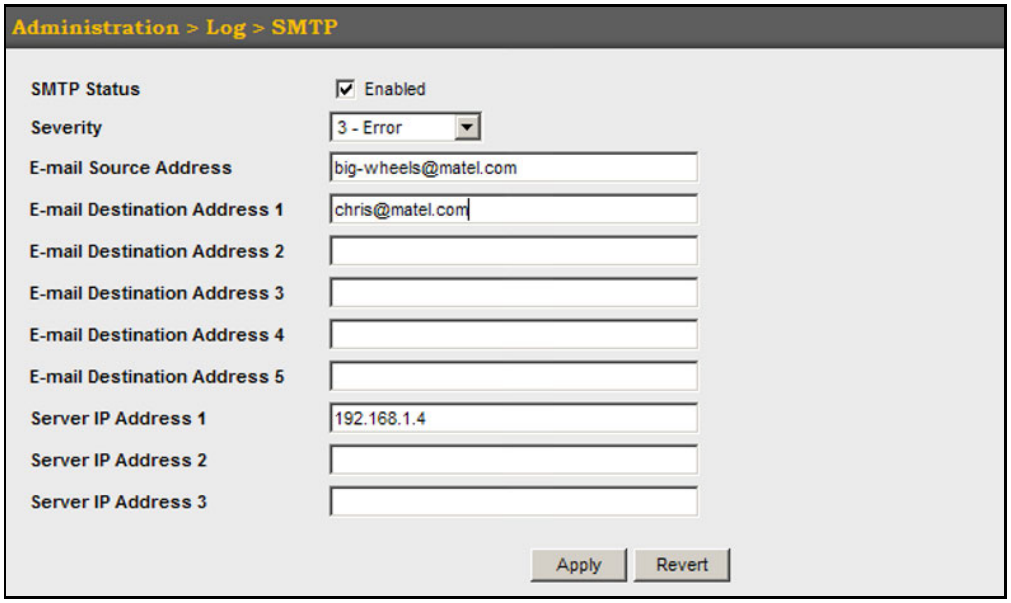
- **SMTP Status** – Enables/disables the SMTP function. (Default: Enabled)
- **Severity** – Sets the syslog severity threshold level (see table on page 340) used to trigger alert messages. All events at this level or higher will be sent to the configured email recipients. For example, using Level 7 will 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 in the web interface:

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 187: Configuring SMTP Alert Messages



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 867

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.

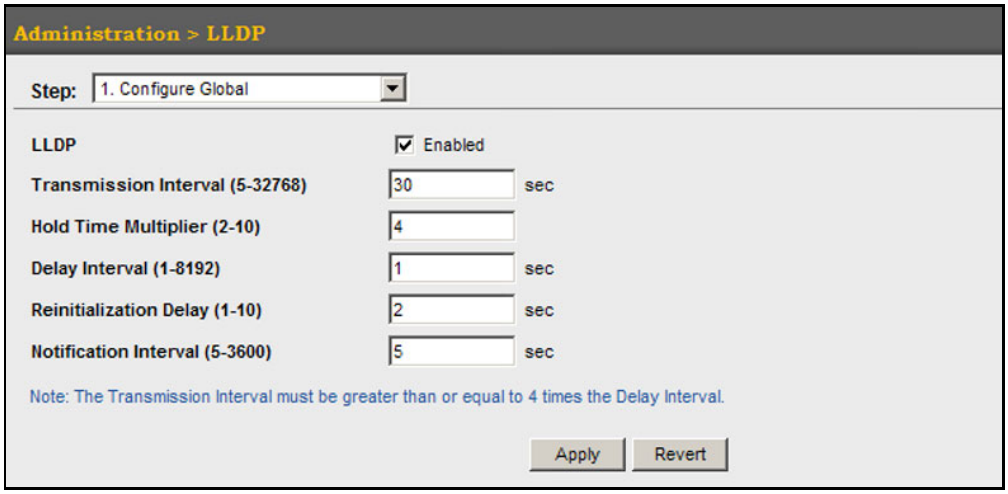
Information about changes in LLDP neighbors that occur between SNMP notifications is not transmitted. Only state changes that exist at the time of a notification are included in the transmission. An SNMP agent should therefore periodically check the value of lldpStatsRemTableLastChangeTime to detect any lldpRemTablesChange notification-events missed due to throttling or transmission loss.

WEB INTERFACE

To configure LLDP timing attributes in the web interface:

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 188: Configuring LLDP Timing Attributes



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 867

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 378.

  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 87.

◆ **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 166).

- **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 147).

- **VLAN Name** – The name of all VLANs to which this interface has been assigned(see "IEEE 802.1Q VLANs" on page 147 and "Protocol VLANs" on page 166).

- **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 147 and "Protocol VLANs" on page 166).

◆ **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 89 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.

- **PoE** – Power-over-Ethernet capabilities, including whether or not PoE is supported, currently enabled, if the port pins through which power is delivered can be controlled, the port pins selected to deliver power, and the power class.

WEB INTERFACE

To configure LLDP interface attributes in the web interface:

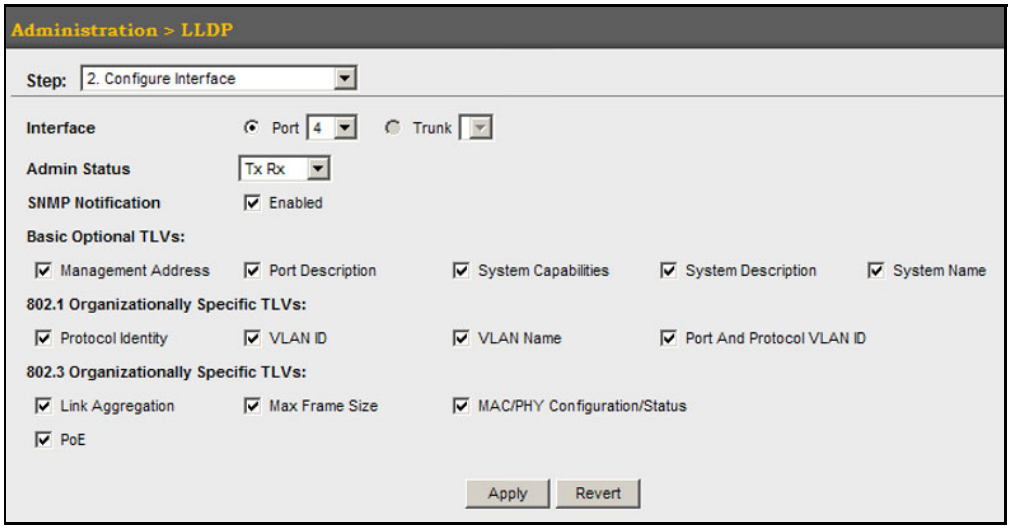
1. Click Administration, LLDP.

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 189: Configuring LLDP Interface Attributes



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 880

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 23: 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 87).
- **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 24: System Capabilities

ID Basis	Reference
Other	—
Repeater	IETF RFC 2108
Bridge	IETF RFC 2674

Table 24: System Capabilities (Continued)

ID Basis	Reference
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 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.

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 in the web interface:

1. Click Administration, LLDP.
2. Select Show Local Device Information from the Step list.
3. Select General, Port, or Trunk.

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

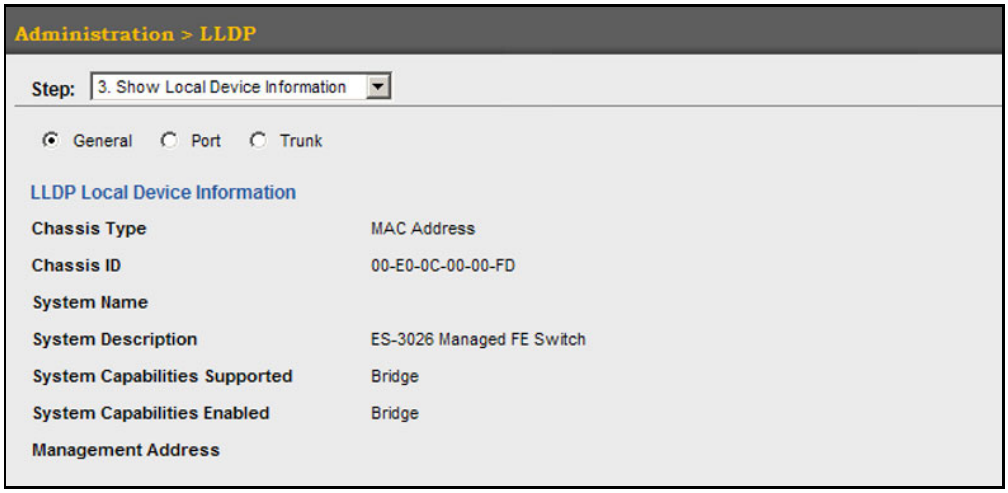
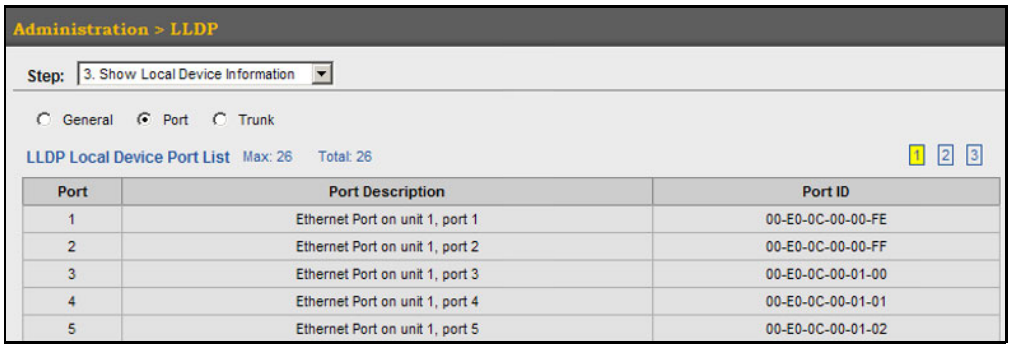


Figure 191: Displaying Local Device Information for LLDP (Port)



Port	Port Description	Port ID
1	Ethernet Port on unit 1, port 1	00-E0-0C-00-00-FE
2	Ethernet Port on unit 1, port 2	00-E0-0C-00-00-FF
3	Ethernet Port on unit 1, port 3	00-E0-0C-00-01-00
4	Ethernet Port on unit 1, port 4	00-E0-0C-00-01-01
5	Ethernet Port on unit 1, port 5	00-E0-0C-00-01-02

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 881

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 23, "Chassis ID Subtype," on page 350.)
- **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 25: 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 24, "System Capabilities," on page 350.)

- **System Capabilities Enabled** – The primary function(s) of the system which are currently enabled. (See Table 24, "System Capabilities," on page 350.)

WEB INTERFACE

To display LLDP information for a remote port in the web interface:

1. Click Administration, LLDP.
2. Select Show Remote Device Information from the Step list.
3. Select Port, Port Details, Trunk, or Trunk Details.

Figure 192: Displaying Remote Device Information for LLDP (Port)

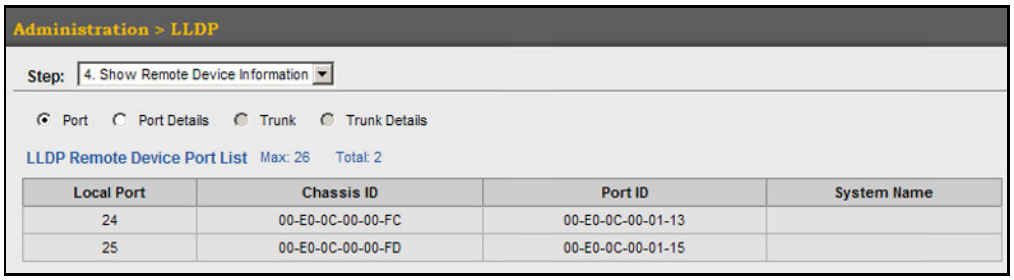
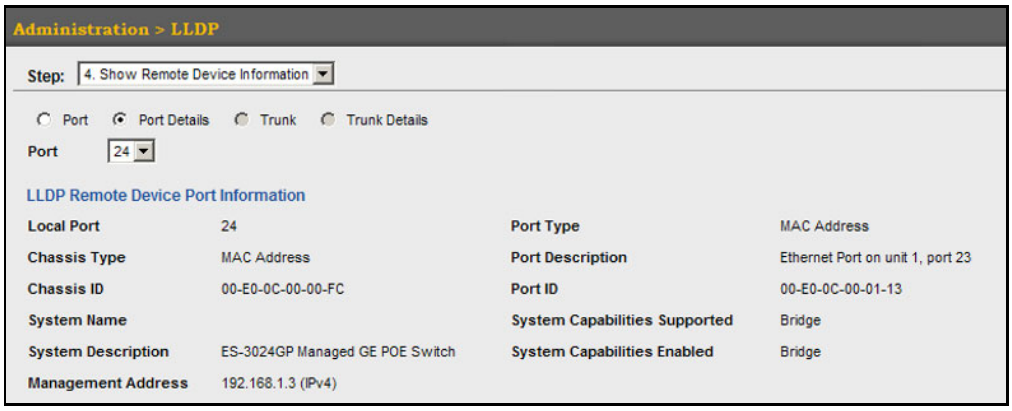


Figure 193: Displaying Remote Device Information for LLDP (Port Details)



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 882

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 in the web interface:

1. Click Administration, LLDP.
2. Select Show Device Statistics from the Step list.

3. Select General, Port, or Trunk.

Figure 194: Displaying LLDP Device Statistics (General)

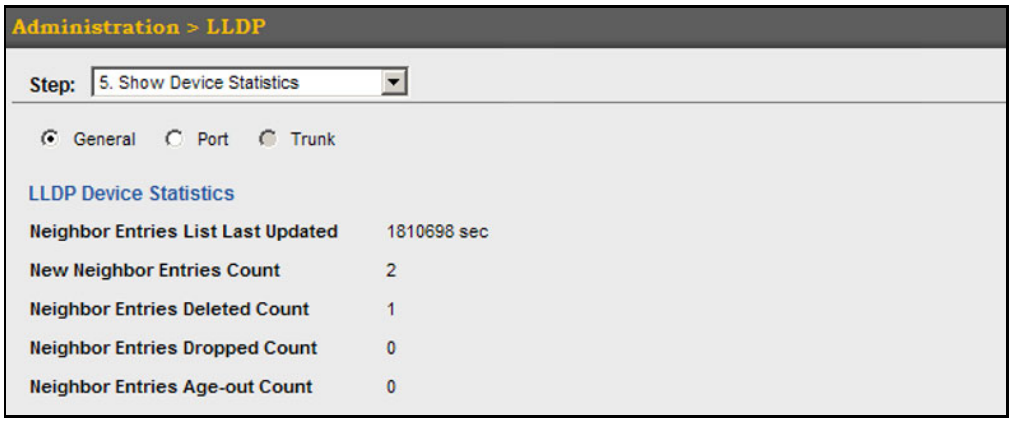
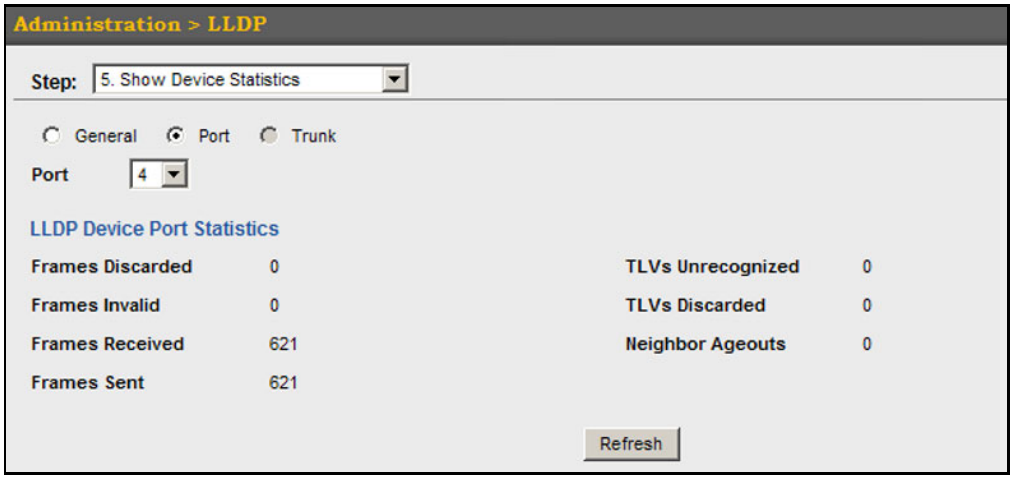


Figure 195: Displaying LLDP Device Statistics (Port)



POWER OVER ETHERNET

The switch can provide DC power to a wide range of connected devices, eliminating the need for an additional power source and cutting down on the amount of cables attached to each device. Once configured to supply power, an automatic detection process is initialized by the switch that is authenticated by a PoE signature from the connected device. Detection and authentication prevent damage to non-compliant devices (IEEE 802.3af or 802.3at).

The switch's power management enables individual port power to be controlled within the switch's power budget. Port power can be automatically turned on and off for connected devices, and a per-port power priority can be set so that the switch never exceeds its power budget. When a device is connected to a switch port, its power requirements are detected by the switch before power is supplied. If the

power required by a device exceeds the power budget of the port or the whole switch, power is not supplied.

Ports can be set to one of four power priority levels, critical, high, medium, or low. To control the power supply within the switch's budget, ports set at critical to medium priority have power enabled in preference to those ports set at low priority. For example, when a device connected to a port is set to critical priority, the switch supplies the required power, if necessary by denying power to ports set for a lower priority during bootup. If a device is connected to a switch port and the switch detects that it requires more than the power budget of the port, no power is supplied to the device (i.e., port power remains off).

If the power demand from devices connected to switch ports exceeds the power budget set for the switch, the port power priority settings are used to control the supplied power. For example:

- If a device is connected to a low-priority port and causes the switch to exceed its budget, port power is not turned on.
- If a device is connected to a critical or high-priority port and would cause the switch to exceed its power budget as determined during booting up, power is provided to the port only if the switch can drop power to one or more lower-priority ports and thereby remain within its overall budget.
- If a device is connected to a port after the switch has finished booting up and would cause the switch to exceed its budget, power will not be provided to that port.

NOTE: Power is dropped from low-priority ports in sequence starting from port number 1.

NOTE: For more information on using the PoE provided by this switch refer to the Installation Guide.

DISPLAYING THE SWITCH'S OVERALL POE POWER BUDGET

Use the Administration > PoE (Configure Global) page to display the maximum PoE power budget for the switch (power available to all Fast Ethernet ports). The maximum power budget is fixed at the maximum available setting, which prevents overload conditions at the power source. If the power demand from devices connected to the switch exceeds the power budget, the switch uses port power priority settings to limit the supplied power.

CLI REFERENCES

- "Power over Ethernet Commands" on page 705

PARAMETERS

These parameters are displayed in the web interface:

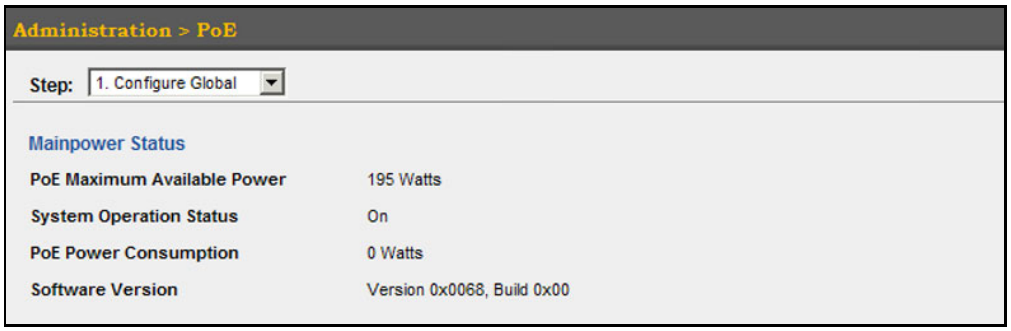
- **PoE Maximum Available Power** – The power budget for the switch. If devices connected to the switch require more power than the switch budget, the port power priority settings are used to control the supplied power. (Fixed: 195 Watts)
- **System Operation Status** – Status of the PoE power service provided to the switch ports.
- **PoE Power Consumption** – The amount of power being consumed by PoE devices connected to the switch.
- **Software Version** – The version of software running on the PoE controller subsystem in the switch.

WEB INTERFACE

To set the overall PoE power budget for switch in the web interface:

1. Click Administration, PoE.
2. Select Configure Global from the Step list.

Figure 196: Showing the Switch's PoE Budget



SETTING THE PORT POE POWER BUDGET

Use the Administration > PoE (Configure Interface) page to set the maximum power provided to a port.

CLI REFERENCES

- "Power over Ethernet Commands" on page 705

COMMAND USAGE

- The switch only provides power to the Fast Ethernet ports. It can supply up to 30W of power to the first six ports (based on the IEEE 802.3at draft), up to 15.4W to 12 ports (based on IEEE 802.3af). or up to 7.5 to 24 ports (based on IEEE 802.3af).
- If a device is connected to a switch port and the switch detects that it requires more than the power budget set for the port or to the overall

switch, no power is supplied to the device (i.e., port power remains off).

- If the power demand from devices connected to all switch ports exceeds the power budget set for the switch, the port power priority settings are used to control the supplied power. For example:
  - If a device is connected to a low-priority port and causes the switch to exceed its budget, power to this port is not turned on.
  - If a device is connected to a critical or high-priority port and causes the switch to exceed its budget, port power is turned on, but the switch drops power to one or more lower-priority ports.

NOTE: Power is dropped from low-priority ports in sequence starting from port number 1.

- If a device is connected to a port after the switch has finished booting up and would cause the switch to exceed its budget, power will not be provided to that port regardless of its priority setting.

PARAMETERS

These parameters are displayed in the web interface:

- **Port** – The port number on the switch.
- **Admin Status** – Enables PoE power on a port. Power is automatically supplied when a device is detected on a port, providing that the power demanded does not exceed the switch or port power budget. (Default: Enabled)
- **Mode** – Shows whether or not PoE power is being supplied to a port.
- **Priority** – Sets the power priority for a port. (Options: Low, High, or Critical; Default: Low)
- **Power Allocation** – Sets the power budget for a port.
  (Range: 3000-30000 milliwatts on ports 1-6, 3000-15400 milliwatts on ports 7-24; Default: 15400 milliwatts)
- **Power Consumption** – Current power consumption on a port.

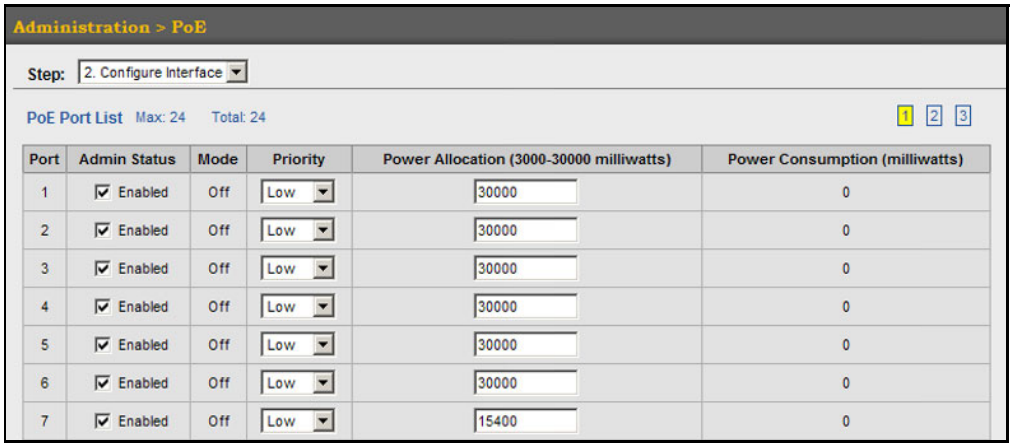
WEB INTERFACE

To set the PoE power budget for a port in the web interface:

1. Click Administration, PoE.
2. Select Configure Interface from the Step list.
3. Enable PoE power on selected ports. Set the priority and the power budget.

4. Click Apply.

Figure 197: Setting a Port's PoE Budget



Port	Admin Status	Mode	Priority	Power Allocation (3000-30000 milliwatts)	Power Consumption (milliwatts)
1	Enabled	Off	Low	30000	0
2	Enabled	Off	Low	30000	0
3	Enabled	Off	Low	30000	0
4	Enabled	Off	Low	30000	0
5	Enabled	Off	Low	30000	0
6	Enabled	Off	Low	30000	0
7	Enabled	Off	Low	15400	0

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 26: 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 534
- "snmp-server enable traps" on page 537

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 in the web interface:

1. Click Administration, SNMP.

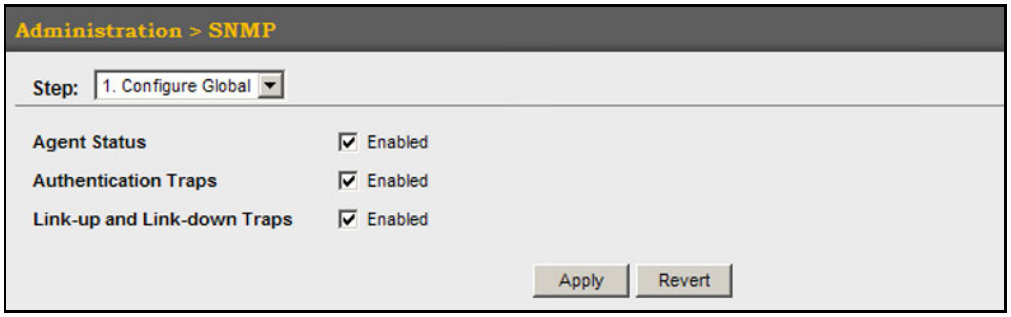
2. Select Configure Global from the Step list.

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 365).

3. Enable SNMP and the required trap types.

4. Click Apply

Figure 198: Configuring Global Settings for SNMP



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 541

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 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 in the web interface:

1. Click Administration, SNMP.

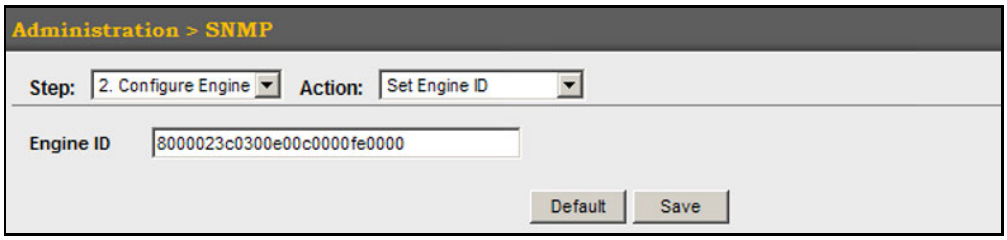
2. Select Configure Engine from the Step list.

3. Select Set Engine ID from the Action list.

4. Enter an ID of a least 9 hexadecimal characters.

5. Click Apply

Figure 199: Configuring the Local Engine ID for SNMP



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 541

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 375.)

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 in the web interface:

1. Click Administration, SNMP.

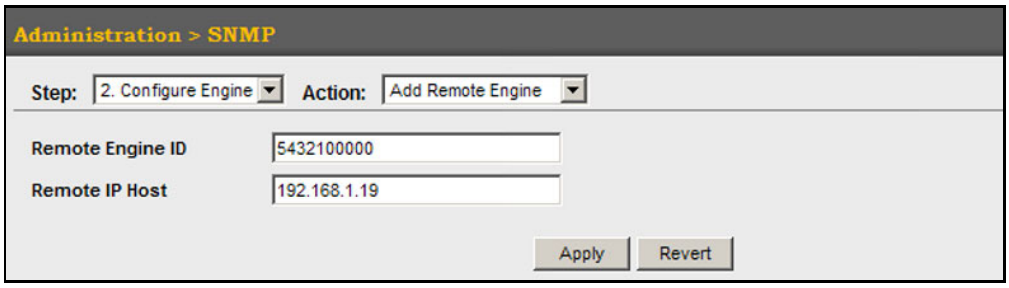
2. Select Configure Engine from the Step list.

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 200: Configuring a Remote Engine ID for SNMP



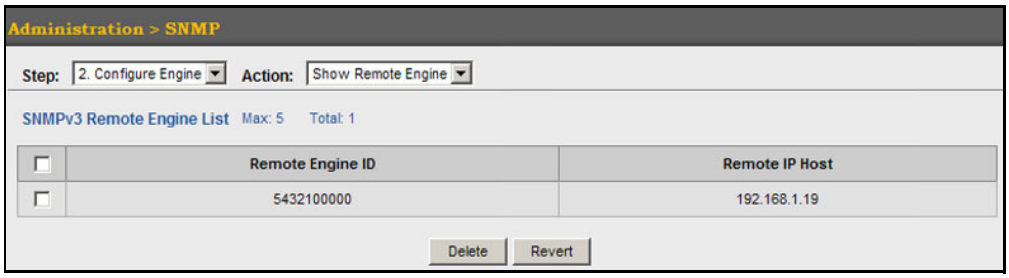
To show the remote SNMP engine IDs in the web interface:

1. Click Administration, SNMP.

2. Select Configure Engine from the Step list.

3. Select Show Remote Engine from the Action list.

Figure 201: Showing Remote Engine IDs for SNMP



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 544

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

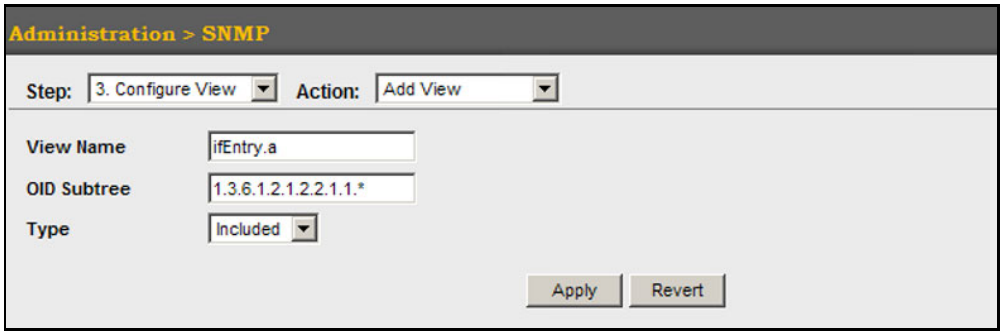
- **View Name** – Lists the SNMP views configured in the Add View page.
- **OID Subtree** – Adds an additional object identifier of a branch within the MIB tree to the selected View. Wild cards can be used to mask a specific portion of the OID string.
- **Type** – Indicates if the object identifier of 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 in the web interface:

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

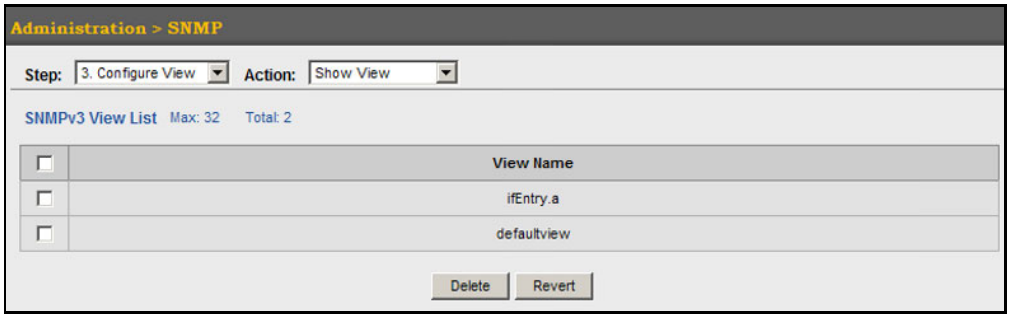
Figure 202: Creating an SNMP View



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

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

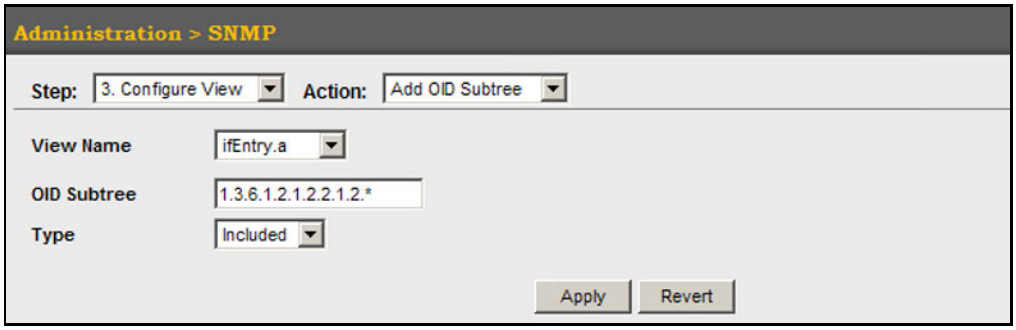
Figure 203: Showing SNMP Views



To add an object identifier to an existing SNMP view of the switch's MIB database in the web interface:

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

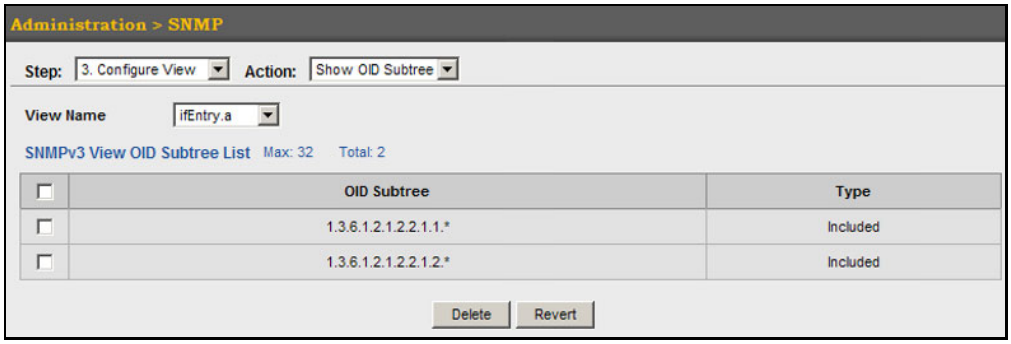
Figure 204: Adding an OID Subtree to an SNMP View



To show the OID branches configured for the SNMP views of the switch's MIB database in the web interface:

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 205: Showing the OID Subtree Configured for SNMP Views



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 546

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 27: Supported Notification Messages

Model	Level	Group
RFC 1493 Traps		
newRoot	1.3.6.1.2.1.17.0.1	The newRoot trap indicates that the sending agent has become the new root of the Spanning Tree; the trap is sent by a bridge soon after its election as the new root, e.g., upon expiration of the Topology Change Timer immediately subsequent to its election.
topologyChange	1.3.6.1.2.1.17.0.2	A topologyChange trap is sent by a bridge when any of its configured ports transitions from the Learning state to the Forwarding state, or from the Forwarding state to the Discarding state. The trap is not sent if a newRoot trap is sent for the same transition.
SNMPv2 Traps		
coldStart	1.3.6.1.6.3.1.1.5.1	A coldStart trap signifies that the SNMPv2 entity, acting in an agent role, is reinitializing itself and that its configuration may have been altered.
warmStart	1.3.6.1.6.3.1.1.5.2	A warmStart trap signifies that the SNMPv2 entity, acting in an agent role, is reinitializing itself such that its configuration is unaltered.
linkDown*	1.3.6.1.6.3.1.1.5.3	A linkDown trap signifies that the SNMP entity, acting in an agent role, has detected that the ifOperStatus object for one of its communication links is about to enter the down state from some other state (but not from the notPresent state). This other state is indicated by the included value of ifOperStatus.
linkUp*	1.3.6.1.6.3.1.1.5.4	A linkUp trap signifies that the SNMP entity, acting in an agent role, has detected that the ifOperStatus object for one of its communication links left the down state and transitioned into some other state (but not into the notPresent state). This other state is indicated by the included value of ifOperStatus.
authenticationFailure*	1.3.6.1.6.3.1.1.5.5	An authenticationFailure trap signifies that the SNMPv2 entity, acting in an agent role, has received a protocol message that is not properly authenticated. While all implementations of the SNMPv2 must be capable of generating this trap, the snmpEnableAuthenTraps object indicates whether this trap will be generated.
RMON Events (V2)		
risingAlarm	1.3.6.1.2.1.16.0.1	The SNMP trap that is generated when an alarm entry crosses its rising threshold and generates an event that is configured for sending SNMP traps.
fallingAlarm	1.3.6.1.2.1.16.0.2	The SNMP trap that is generated when an alarm entry crosses its falling threshold and generates an event that is configured for sending SNMP traps.

Table 27: Supported Notification Messages (Continued)

Model	Level	Group
Private Traps		
swPowerStatus ChangeTrap	1.3.6.1.4.1.572.17389.13000.2.1.0.1	This trap is sent when the power state changes.
swPortSecurityTrap	1.3.6.1.4.1.572.17389.13000.2.1.0.36	This trap is sent when the port is being intruded. This trap will only be sent when the portSecActionTrap is enabled.
swIpFilterRejectTrap	1.3.6.1.4.1.572.17389.13000.2.1.0.40	This trap is sent when an incorrect IP address is rejected by the IP Filter.
swAuthenticationFailure	1.3.6.1.4.1.572.17389.13000.2.1.0.66	This trap will be triggered if authentication fails.
swAuthenticationSuccess	1.3.6.1.4.1.572.17389.13000.2.1.0.67	This trap will be triggered if authentication is successful.
swAtcBcastStormAlarmFireTrap	1.3.6.1.4.1.572.17389.13000.2.1.0.70	When broadcast traffic is detected as a storm, this trap is fired.
swAtcBcastStormAlarmClearTrap	1.3.6.1.4.1.572.17389.13000.2.1.0.71	When a broadcast storm is detected as normal traffic, this trap is fired.
swAtcBcastStormTcApplyTrap	1.3.6.1.4.1.572.17389.13000.2.1.0.72	When ATC is activated, this trap is fired.
swAtcBcastStormTcReleaseTrap	1.3.6.1.4.1.572.17389.13000.2.1.0.73	When ATC is released, this trap is fired.
swAtcMcastStormAlarmFireTrap	1.3.6.1.4.1.572.17389.13000.2.1.0.74	When multicast traffic is detected as the storm, this trap is fired.
swAtcMcastStormAlarmClearTrap	1.3.6.1.4.1.572.17389.13000.2.1.0.75	When multicast storm is detected as normal traffic, this trap is fired.
swAtcMcastStormTcApplyTrap	1.3.6.1.4.1.572.17389.13000.2.1.0.76	When ATC is activated, this trap is fired.
swAtcMcastStormTcReleaseTrap	1.3.6.1.4.1.572.17389.13000.2.1.0.77	When ATC is released, this trap is fired.
swLoopbackDetectionTrap	1.3.6.1.4.1.572.17389.13000.2.1.0.92	This trap is sent when loopback BPDUs have been detected.
networkAccessPortLinkDetectionTrap	1.3.6.1.4.1.572.17389.13000.2.1.0.96	This trap is sent when a networkAccessPortLinkDetection event is triggered.
autoUpgradeTrap	1.3.6.1.4.1.572.17389.13000.2.1.0.104	This trap is sent when auto upgrade is executed.
swCpuUtiRisingNotification	1.3.6.1.4.1.572.17389.13000.2.1.0.107	This notification indicates that the CPU utilization has risen from cpuUtiFallingThreshold to cpuUtiRisingThreshold.
swCpuUtiFallingNotification	1.3.6.1.4.1.572.17389.13000.2.1.0.108	This notification indicates that the CPU utilization has fallen from cpuUtiRisingThreshold to cpuUtiFallingThreshold.
swMemoryUtiRisingThresholdNotification	1.3.6.1.4.1.572.17389.13000.2.1.0.109	This notification indicates that the memory utilization has risen from memoryUtiFallingThreshold to memoryUtiRisingThreshold.
swMemoryUtiFallingThresholdNotification	1.3.6.1.4.1.572.17389.13000.2.1.0.110	This notification indicates that the memory utilization has fallen from memoryUtiRisingThreshold to memoryUtiFallingThreshold.
dhcpRougeServerAttackTrap	1.3.6.1.4.1.572.17389.13000.2.1.0.114	This trap is sent when receiving a DHCP packet from a rouge server.

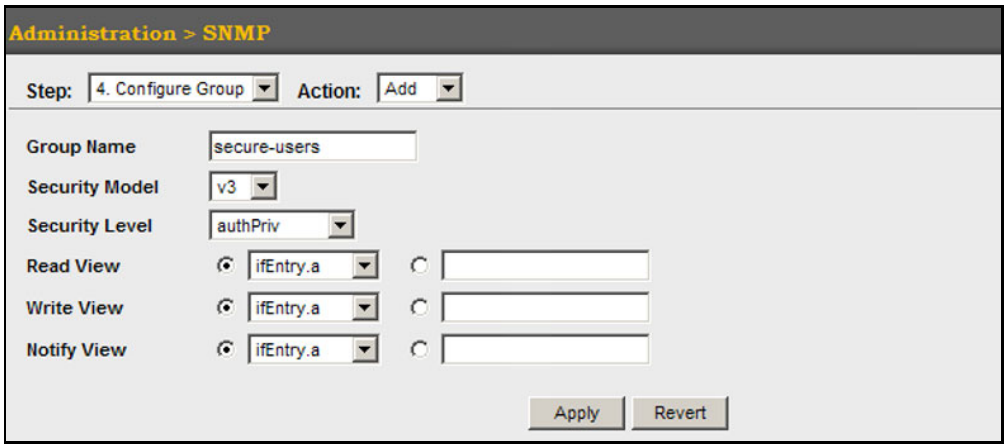
* These are legacy notifications and therefore must be enabled in conjunction with the corresponding traps on the SNMP Configuration menu.

WEB INTERFACE

To configure an SNMP group in the web interface:

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 206: Creating an SNMP Group



To show SNMP groups in the web interface:

1. Click Administration, SNMP.
2. Select Configure Group from the Step list.
3. Select Show from the Action list.

Figure 207: Showing SNMP Groups

Group Name	Model	Level	Read View	Write View	Notify View
public	v1	noAuthNoPriv	defaultview	No writeview specified	No notifyview specified
public	v2c	noAuthNoPriv	defaultview	No writeview specified	No notifyview specified
private	v1	noAuthNoPriv	defaultview	defaultview	No notifyview specified
private	v2c	noAuthNoPriv	defaultview	defaultview	No notifyview specified
secure-users	v3	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 535

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 in the web interface:

1. Click Administration, SNMP.

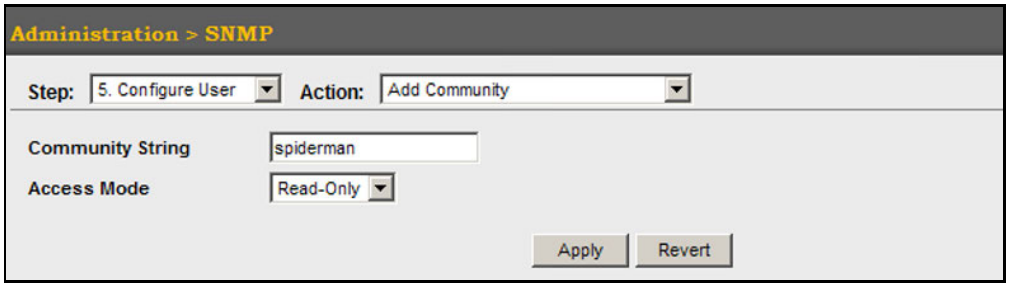
2. Select Configure User from the Step list.

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

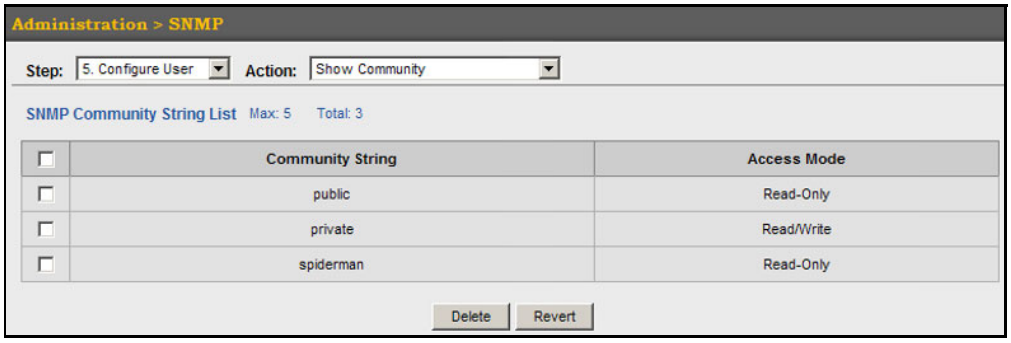
Figure 208: Setting Community Access Strings



To show the community access strings in the web interface:

1. Click Administration, SNMP.
2. Select Configure User from the Step list.
3. Select Show Community from the Action list.

Figure 209: Showing Community Access Strings



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 543

PARAMETERS

These parameters are displayed in the web interface:

- **User Name** – The name of user connecting to the SNMP agent. (Range: 1-32 characters)

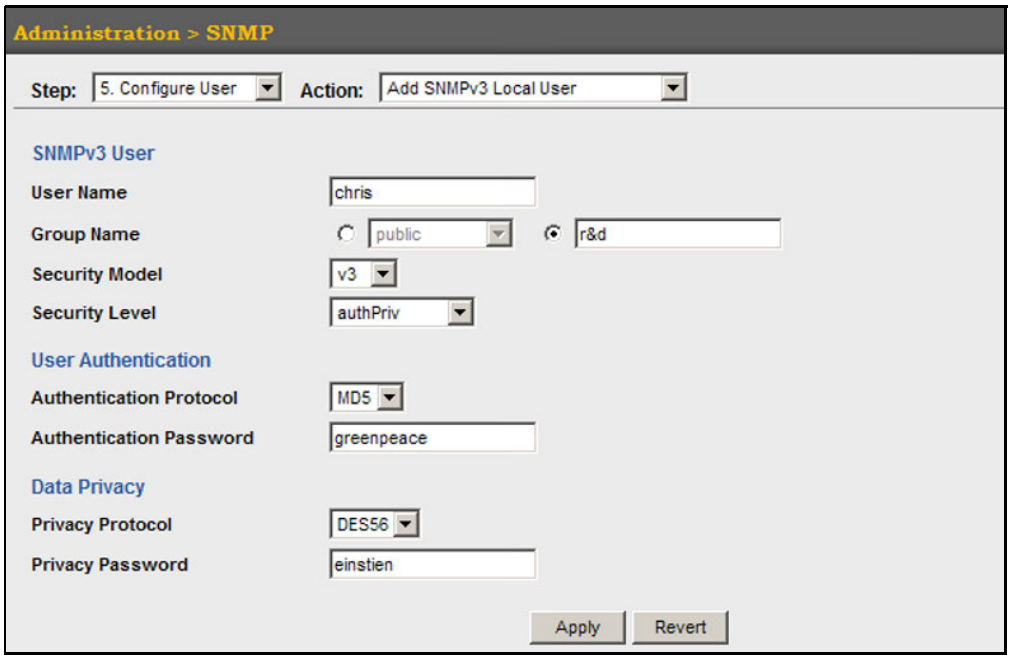
- **Group Name** – The name of the SNMP group to which the user is assigned. (Range: 1-32 characters)
- **Security Model** – The user security model; SNMP v1, v2c or v3.
- **Security Level** – The following security levels are only used for the groups assigned to the SNMP security model:
  - **noAuthNoPriv** – 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 in the web interface:

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

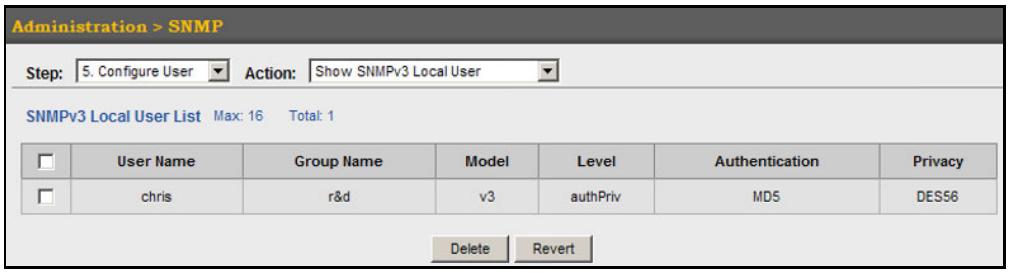
Figure 210: Configuring Local SNMPv3 Users



To show local SNMPv3 users in the web interface:

1. Click Administration, SNMP.
2. Select Configure User from the Step list.
3. Select Show SNMPv3 Local User from the Action list.

Figure 211: Showing Local SNMPv3 Users



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 543

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 378 and "Specifying a Remote Engine ID" on page 364.)

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 in the web interface:

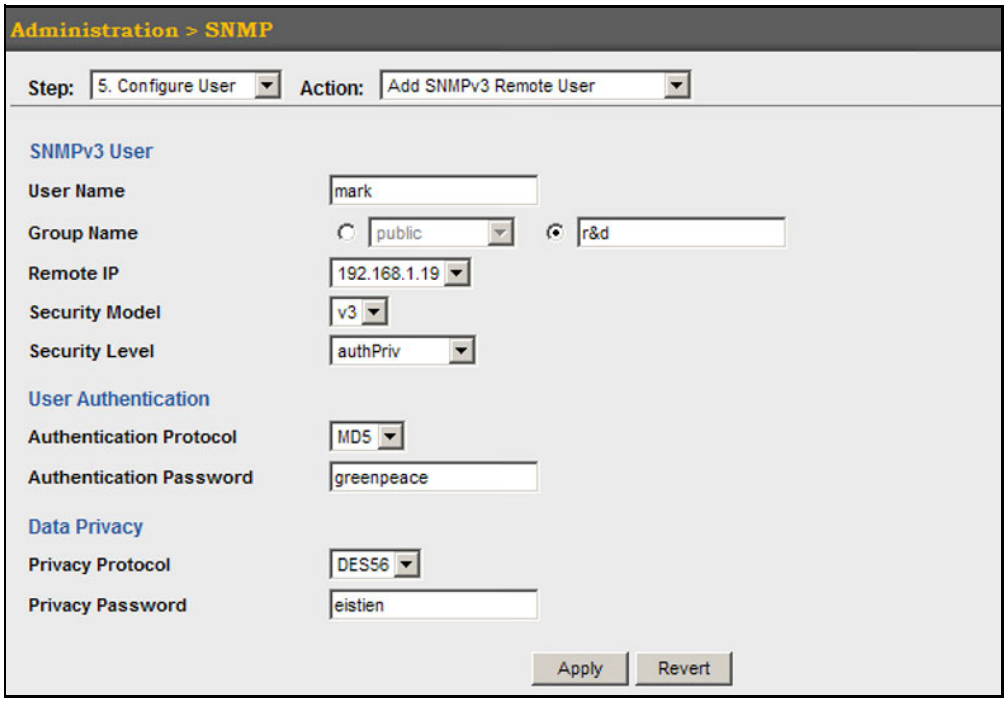
1. Click Administration, SNMP.
2. Select Configure User from the Step list.

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 212: Configuring Remote SNMPv3 Users



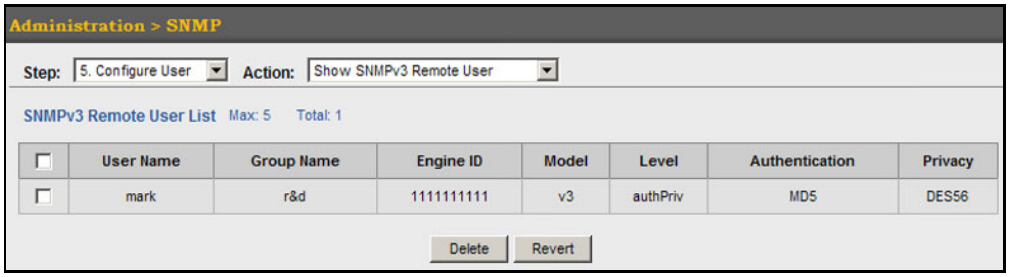
To show remote SNMPv3 users in the web interface:

1. Click Administration, SNMP.

2. Select Configure User from the Step list.

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

Figure 213: Showing Remote SNMPv3 Users



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 538
- "snmp-server enable traps" on page 537

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 362).
  2. Create a view with the required notification messages (page 365).
  3. Configure the group (matching the community string specified on the Configure Trap - Add page) to include the required notify view (page 368).
  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 362).
  2. Create a local SNMPv3 user to use in the message exchange process (page 373). 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 365).
  4. Create a group that includes the required notify view (page 368).
  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 373), 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 375), 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 in the web interface:

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 214: Configuring Trap Managers (SNMPv1)

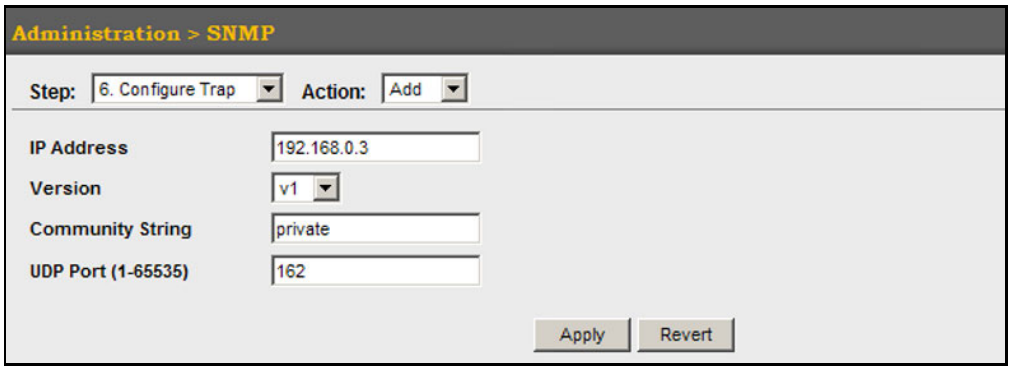


Figure 215: Configuring Trap Managers (SNMPv2c)

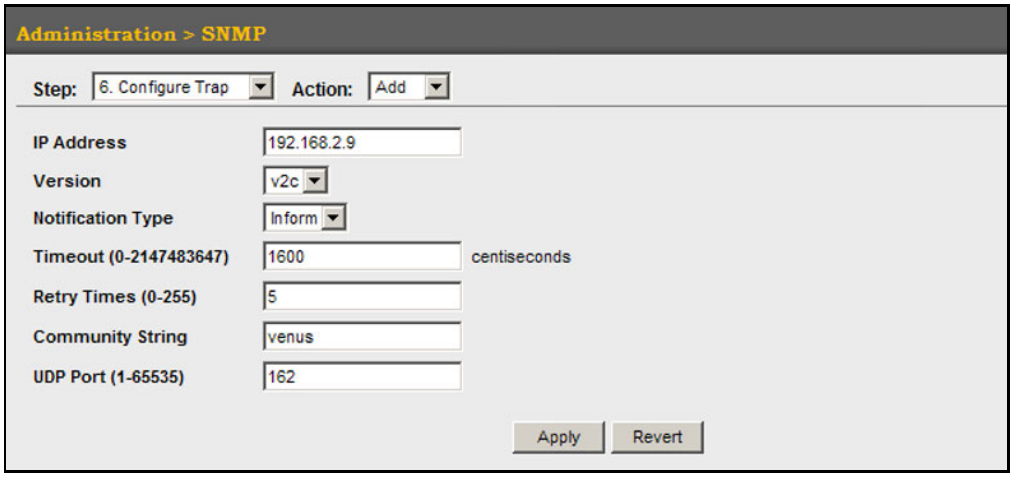
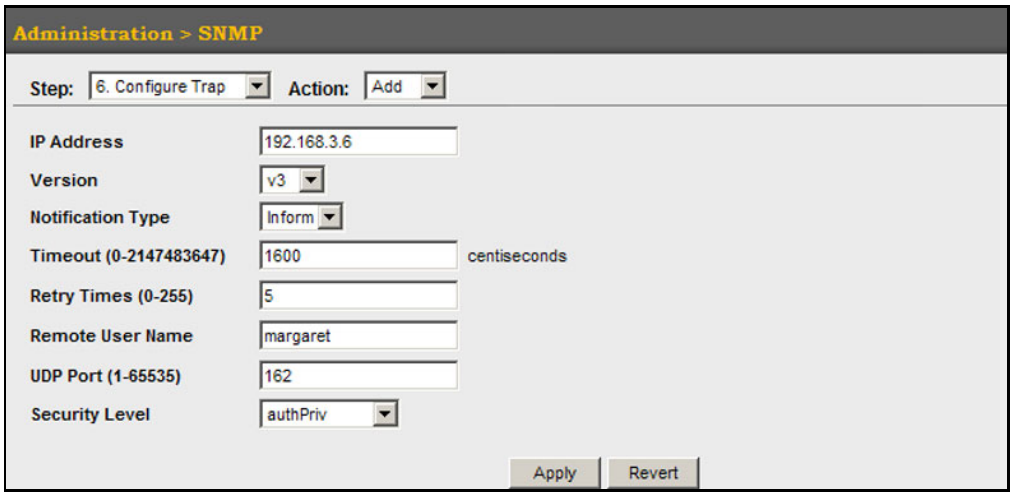


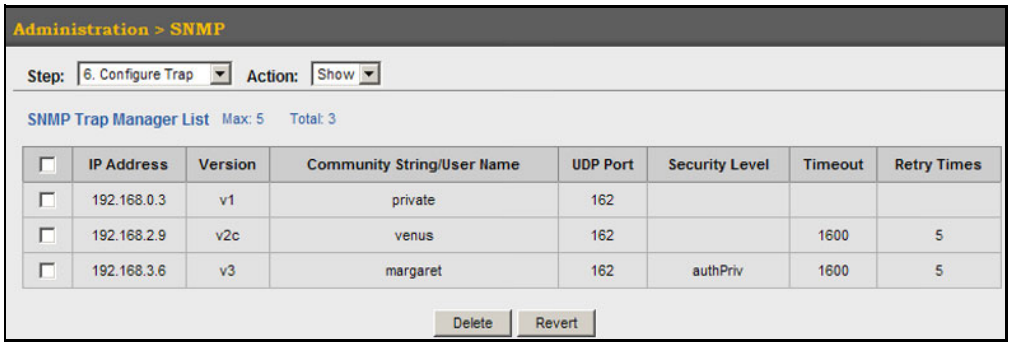
Figure 216: Configuring Trap Managers (SNMPv3)



To show configured trap managers in the web interface:

1. Click Administration, SNMP.
2. Select Configure Trap from the Step list.
3. Select Show from the Action list.

Figure 217: Showing Trap Managers



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 553

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)

- **Variable** – The object identifier of the MIB variable to be sampled. Only variables of the type etherStatsEntry.n.n may be sampled.

  Note that etherStatsEntry.n uniquely defines the MIB variable, and etherStatsEntry.n.n defines the MIB variable, plus the etherStatsIndex. For example, 1.3.6.1.2.1.16.1.1.1.6.1 denotes etherStatsBroadcastPkts, plus the etherStatsIndex of 1.

- **Interval** – The polling interval. (Range: 1-31622400 seconds)
- **Sample Type** – Tests for absolute or relative changes in the specified variable.
  - **Absolute** – The variable is compared directly to the thresholds at the end of the sampling period.
  - **Delta** – The last sample is subtracted from the current value and the difference is then compared to the thresholds.
- **Rising Threshold** – If the current value is greater than or equal to the rising threshold, and the last sample value was less than this threshold, then an alarm will be generated. After a rising event has been generated, another such event will not be generated until the sampled value has fallen below the rising threshold, reaches the falling threshold, and again moves back up to the rising threshold. (Range: 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)

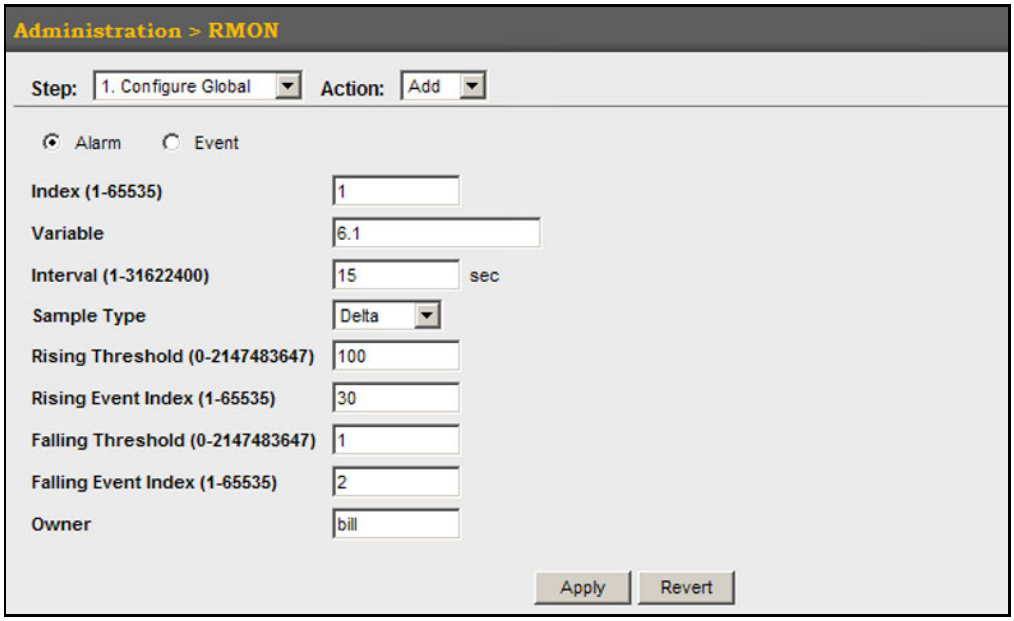
WEB INTERFACE

To configure an RMON alarm in the web interface:

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

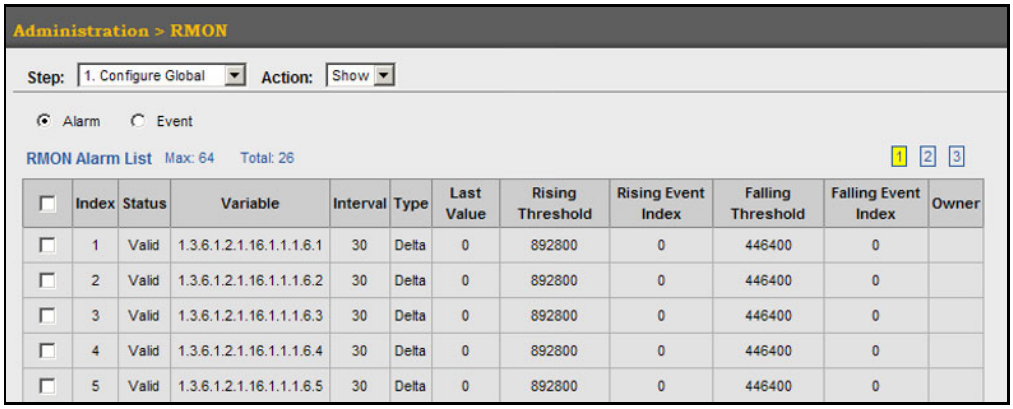
Figure 218: Configuring an RMON Alarm



To show configured RMON alarms in the web interface:

1. Click Administration, RMON.
2. Select Configure Global from the Step list.
3. Select Show from the Action list.
4. Click Alarm.

Figure 219: Showing Configured RMON Alarms



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 553

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 339).

  - **Trap** – Sends a trap message to all configured trap managers (see "Specifying Trap Managers" on page 378).

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

- **Description** – A comment that describes this event. (Range: 1-127 characters)

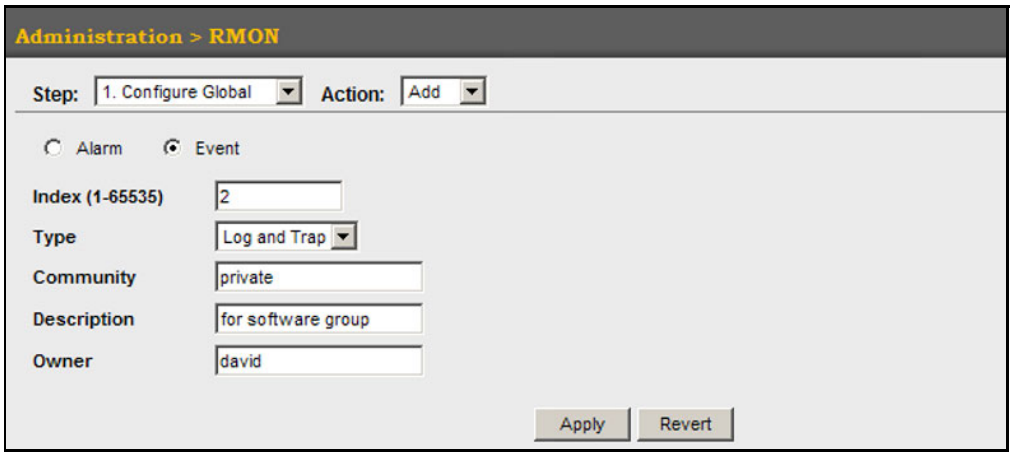
- **Owner** – Name of the person who created this entry. (Range: 1-127 characters)

WEB INTERFACE

To configure an RMON event in the web interface:

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 220: Configuring an RMON Event



To show configured RMON events in the web interface:

1. Click Administration, RMON.
2. Select Configure Global from the Step list.
3. Select Show from the Action list.
4. Click Event.

Figure 221: Showing Configured RMON Events

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 553

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 123.

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.

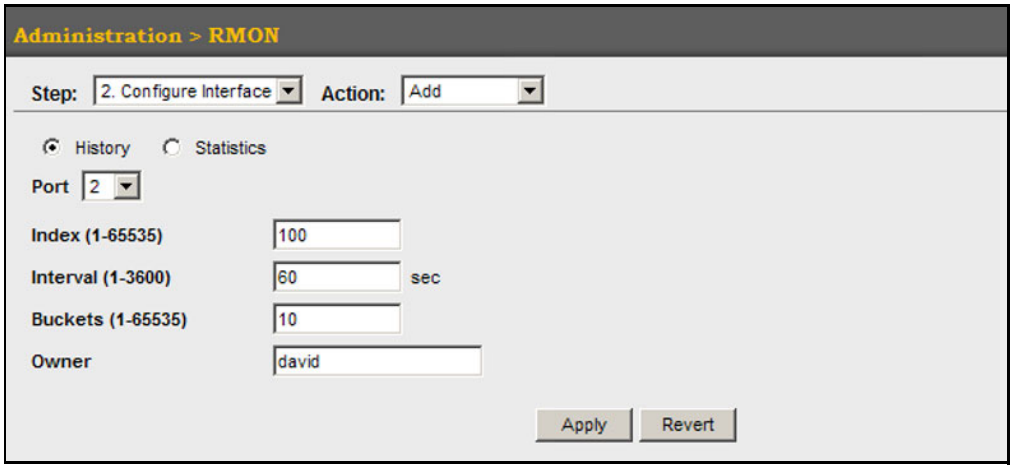
- **Owner** - Name of the person who created this entry. (Range: 1-127 characters)

WEB INTERFACE

To periodically sample statistics on a port in the web interface:

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

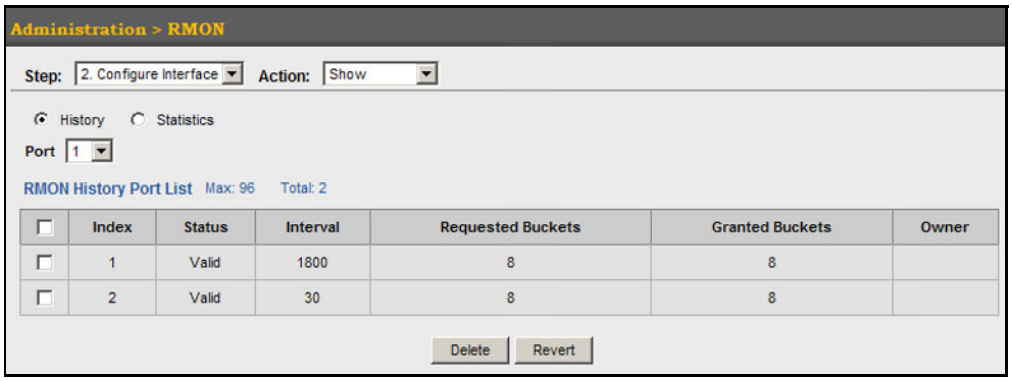
Figure 222: Configuring an RMON History Sample



To show configured RMON history samples in the web interface:

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.

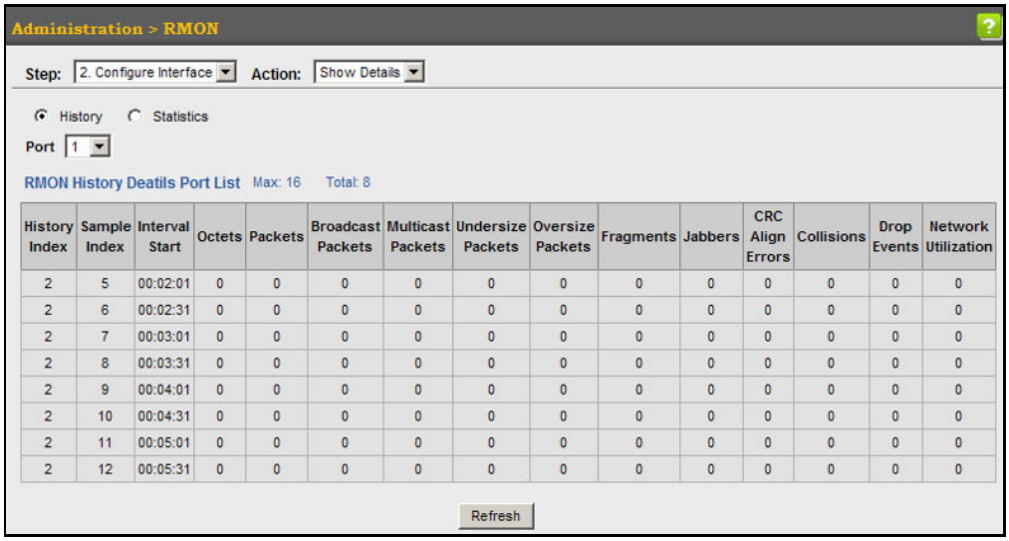
Figure 223: Showing Configured RMON History Samples



To show collected RMON history samples in the web interface:

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 224: Showing Collected RMON History Samples



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 553

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:

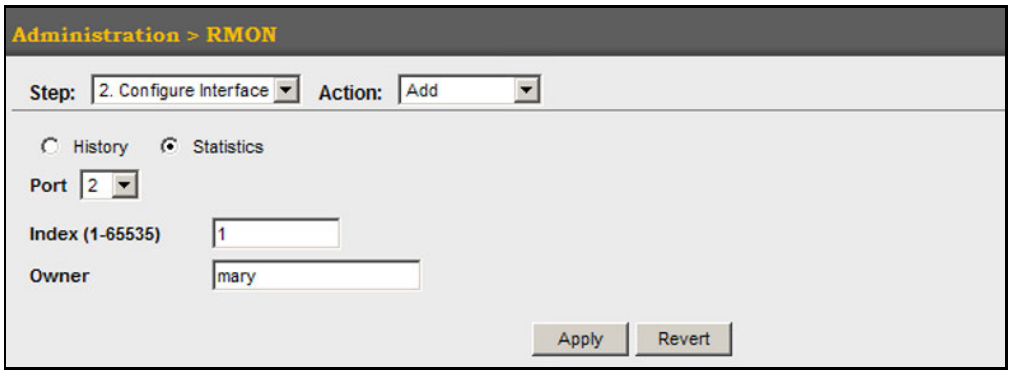
- **Port** – The port number on the switch.
- **Index** - Index to this entry. (Range: 1-65535)
- **Owner** - Name of the person who created this entry. (Range: 1-127 characters)

WEB INTERFACE

To enable regular sampling of statistics on a port in the web interface:

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

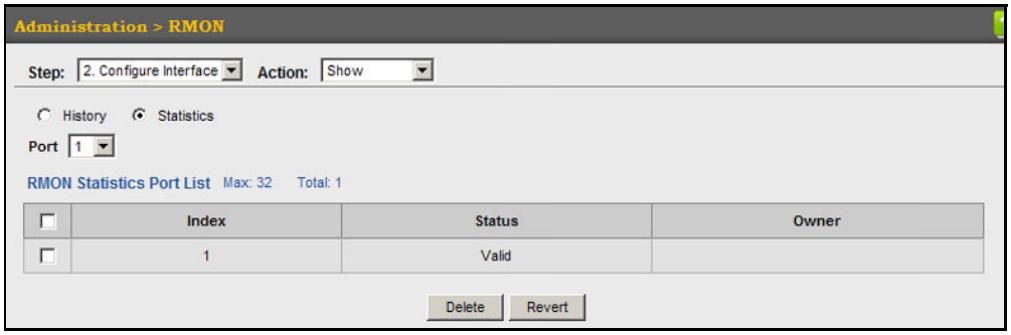
Figure 225: Configuring an RMON Statistical Sample



To show configured RMON statistical samples in the web interface:

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.

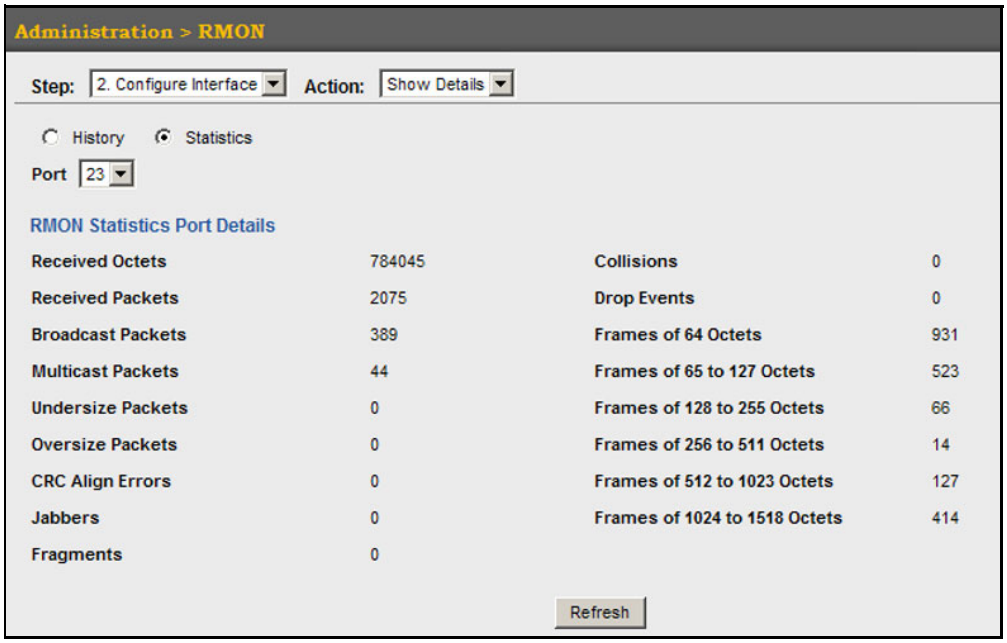
Figure 226: Showing Configured RMON Statistical Samples



To show collected RMON statistical samples in the web interface:

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 227: Showing Collected RMON Statistical Samples



SWITCH CLUSTERING

Switch clustering is a method of grouping switches together to enable centralized management through a single unit. Switches that support clustering can be grouped together regardless of physical location or switch type, as long as they are connected to the same local network.

COMMAND USAGE

- A switch cluster has a primary unit called the “Commander” which is used to manage all other “Member” switches in the cluster. The management station can use either Telnet or the web interface to communicate directly with the Commander through its IP address, and then use the Commander to manage Member switches through the cluster’s “internal” IP addresses.

- Clustered switches must be in the same Ethernet broadcast domain. In other words, clustering only functions for switches which can pass information between the Commander and potential Candidates or active Members through VLAN 4093.

- Once a switch has been configured to be a cluster Commander, it automatically discovers other cluster-enabled switches in the network. These “Candidate” switches only become cluster Members when manually selected by the administrator through the management station.

- There can be up to 100 candidates and 36 member switches in one cluster.

- A switch can only be a member of one cluster.
- The cluster VLAN 4093 is not configured by default. Before using clustering, take the following actions to set up this VLAN:
  1. Create VLAN 4093 (see "Configuring VLAN Groups" on page 150).
  2. Add the participating ports to this VLAN (see "Adding Static Members to VLANs" on page 152), and set them to hybrid mode, tagged members, PVID = 1, and acceptable frame type = all.
- After the Commander and Members have been configured, any switch in the cluster can be managed from the web agent by choosing the desired Member ID from the Show Member page.

CONFIGURING GENERAL SETTINGS FOR CLUSTERS

Use the Administration > Cluster (Configure Global) page to create a switch cluster.

CLI REFERENCES

- "Switch Clustering" on page 527

COMMAND USAGE

First be sure that clustering is enabled on the switch (the default is disabled), then set the switch as a Cluster Commander. Set a Cluster IP Pool that does not conflict with the network IP subnet. Cluster IP addresses are assigned to switches when they become Members and are used for communication between Member switches and the Commander.

PARAMETERS

These parameters are displayed in the web interface:

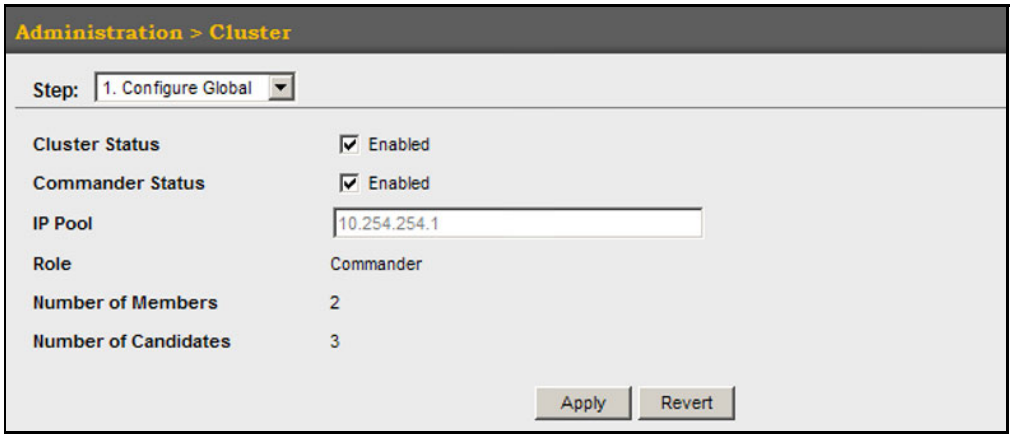
- **Cluster Status** – Enables or disables clustering on the switch. (Default: Disabled)
- **Commander Status** – Enables or disables the switch as a cluster Commander. (Default: Disabled)
- **IP Pool** – An “internal” IP address pool that is used to assign IP addresses to Member switches in the cluster. Internal cluster IP addresses are in the form 10.x.x.member-ID. Only the base IP address of the pool needs to be set since Member IDs can only be between 1 and 36. Note that you cannot change the cluster IP pool when the switch is currently in Commander mode. Commander mode must first be disabled. (Default: 10.254.254.1)
- **Role** – Indicates the current role of the switch in the cluster; either Commander, Member, or Candidate. (Default: Candidate)
- **Number of Members** – The current number of Member switches in the cluster.
- **Number of Candidates** – The current number of Candidate switches discovered in the network that are available to become Members.

WEB INTERFACE

To configure a switch cluster in the web interface:

1. Click Administration, Cluster.
2. Select Configure Global from the Step list.
3. Set the required attributes for a Commander or a managed candidate.
4. Click Apply

Figure 228: Configuring a Switch Cluster



CLUSTER MEMBER CONFIGURATION

Use the Administration > Cluster (Configure Member - Add) page to add Candidate switches to the cluster as Members.

CLI REFERENCES

- "Switch Clustering" on page 527

PARAMETERS

These parameters are displayed in the web interface:

- **Member ID** – Specify a Member ID number for the selected Candidate switch. (Range: 1-36)
- **MAC Address** – Select a discovered switch MAC address from the Candidate Table, or enter a specific MAC address of a known switch.

WEB INTERFACE

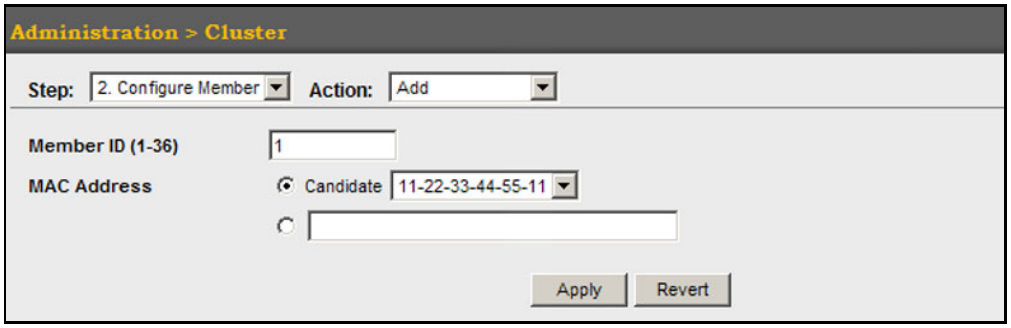
To configure cluster members in the web interface:

1. Click Administration, Cluster.
2. Select Configure Member from the Step list.
3. Select Add from the Action list.

4. Select one of the cluster candidates discovered by this switch, or enter the MAC address of a candidate.

5. Click Apply.

Figure 229: Configuring a Cluster Members



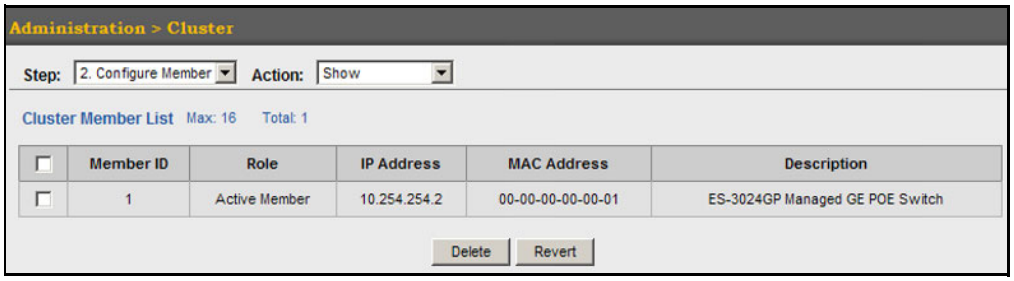
To show the cluster members in the web interface:

1. Click Administration, Cluster.

2. Select Configure Member from the Step list.

3. Select Show from the Action list.

Figure 230: Showing Cluster Members



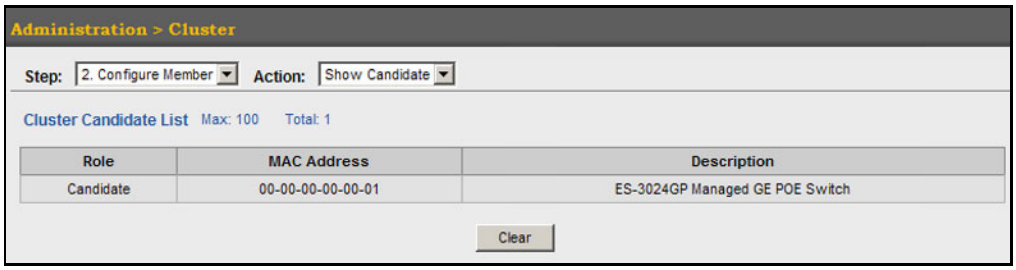
To show cluster candidates in the web interface:

1. Click Administration, Cluster.

2. Select Configure Member from the Step list.

3. Select Show Candidate from the Action list.

Figure 231: Showing Cluster Candidates



MANAGING CLUSTER MEMBERS

Use the Administration > Cluster (Show Member) page to manage another switch in the cluster.

CLI REFERENCES

- "Switch Clustering" on page 527

PARAMETERS

These parameters are displayed in the web interface:

Member ID – The ID number of the Member switch. (Range: 1-36)

Role – Indicates the current status of the switch in the cluster.

IP Address – The internal cluster IP address assigned to the Member switch.

MAC Address – The MAC address of the Member switch.

Description – The system description string of the Member switch.

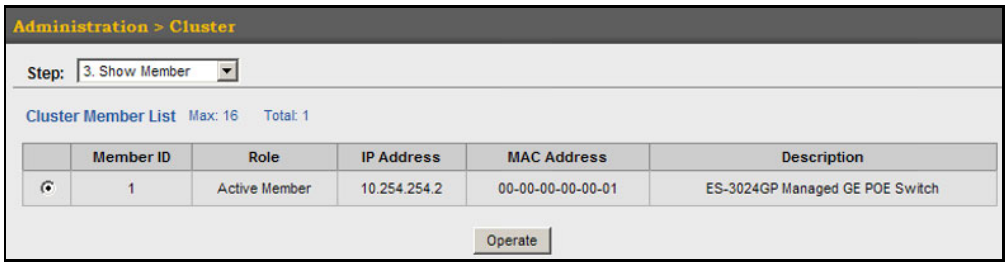
Operate – Remotely manage a cluster member.

WEB INTERFACE

To manage a cluster member in the web interface:

1. Click Administration, Cluster.
2. Select Show Member from the Step list.
3. Select an entry from the Cluster Member List.
4. Click Operate.

Figure 232: Managing a Cluster Member



16 IP CONFIGURATION

This chapter describes how to configure an IP interface for management access to the switch over the network. This switch supports both IP Version 4 and Version 6, and can be managed simultaneously through either of these address types. You can manually configure a specific IPv4 or IPv6 address or direct the switch to obtain an IPv4 address from a BOOTP or DHCP server when it is powered on. An IPv6 address can either be manually configured or dynamically generated.

For information on configuring the switch with an IPv4 address, see the following section. For information on configuring the switch with an IPv6 address, see "Setting the Switch's IP Address (IP Version 6)" on page 405.

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 905

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.

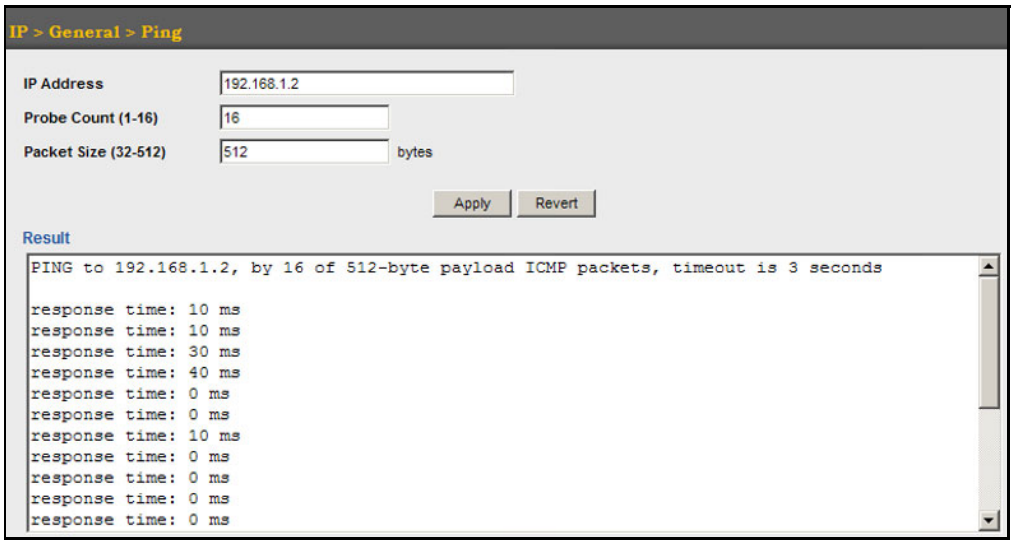
- *Destination unreachable* - The gateway for this destination indicates that the destination is unreachable.
- *Network or host unreachable* - The gateway found no corresponding entry in the route table.

WEB INTERFACE

To ping another device on the network in the web interface:

1. Click IP, General, Ping.
2. Specify the target device and ping parameters.
3. Click Apply.

Figure 233: Pnging a Network Device



ADDRESS RESOLUTION PROTOCOL

Address Resolution Protocol (ARP) is used to map an IP address to a physical layer (i.e., MAC) address. When a device sends or receives a packet with an IP header, it must first resolve the destination IP address into a MAC address. When an IP frame is received by this switch, it first looks up the MAC address corresponding to the destination IP address in the ARP cache. If the address is found, the switch writes the MAC address into the appropriate field in the frame header, and forwards the frame on to the destination.

If there is no entry for an IP address in the ARP cache, the switch 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 28: 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 destination. As long as this entry has not timed out, the switch will be able forward traffic directly to 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.

SETTING THE ARP TIMEOUT

Use the IP > ARP (Configure General) page to specify the timeout for ARP cache entries.

CLI REFERENCES

- "arp timeout" on page 907

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 only be set globally for all VLANs.

  The aging time determines how long dynamic entries remain in the cache. If the timeout is too short, the switch 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.

WEB INTERFACE

To configure the timeout for the ARP cache or to enable Proxy ARP for a VLAN (i.e., IP subnetwork):

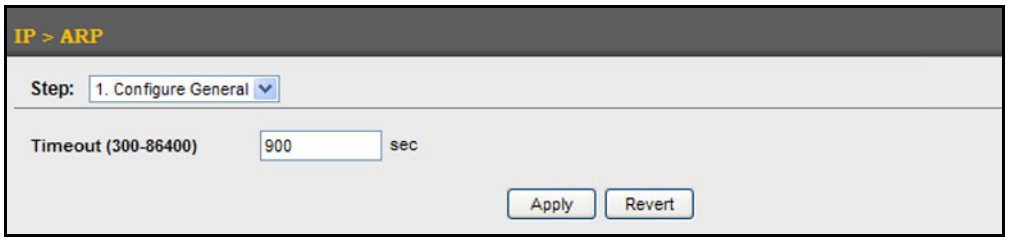
1. Click IP, ARP.

2. Select Configure General from the Step List.

3. Set the timeout to a suitable value for the ARP cache.

4. Click Apply.

Figure 234: Setting the ARP Timeout



DISPLAYING ARP ENTRIES

Use the IP > ARP (Show Information) page to display dynamic or local entries in the ARP cache. The ARP cache contains entries for local interfaces, including subnet, host, and broadcast addresses. However, most entries will be dynamically learned through replies to broadcast messages.

CLI REFERENCES

◆ "show arp" on page 908
◆ "clear arp-cache" on page 908

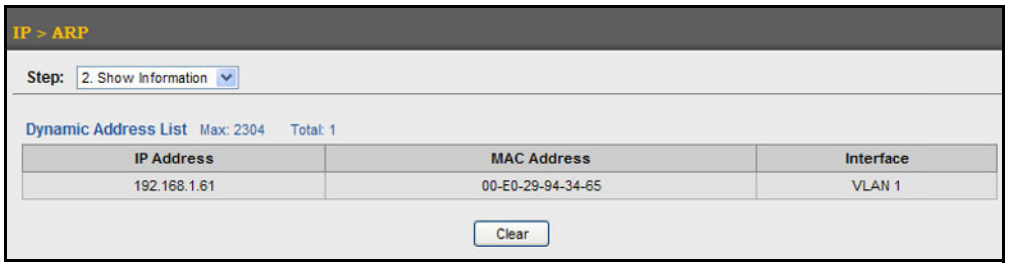
WEB INTERFACE

To display entries in the ARP cache:

1. Click IP, ARP.

2. Select Show Information from the Step List.

Figure 235: Displaying ARP Entries



SETTING THE SWITCH'S IP ADDRESS (IP VERSION 4)

Use the System > IP page to configure an IPv4 address for the switch. An IPv4 address is obtained via DHCP by default for VLAN 1. To configure a static address, you need to change the switch's default settings to values that are compatible with your network. You may also need to a establish a default gateway between the switch and management stations that exist on another network segment.

You can direct the device to obtain an address from a BOOTP or DHCP server, or manually configure a static IP address. Valid IP addresses consist of four decimal numbers, 0 to 255, separated by periods. Anything other than this format will not be accepted.

CLI REFERENCES

- "DHCP Client" on page 895
- "Basic IPv4 Configuration" on page 902

PARAMETERS

These parameters are displayed in the web interface:

- **Management 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: Static)

- **IP Address** – Address of the VLAN to which the management station is attached. Valid IP addresses consist of four numbers, 0 to 255, separated by periods. (Default: 192.168.1.10)

- **Subnet Mask** – This mask identifies the host address bits used for routing to specific subnets. (Default: 255.255.255.0)

- **Gateway IP Address** – IP address of the gateway router between the switch and management stations that exist on other network segments. (Default: 0.0.0.0)

- **MAC Address** – The physical layer address for this switch.

- **Restart DHCP** – Requests a new IP address from the DHCP server.

WEB INTERFACE

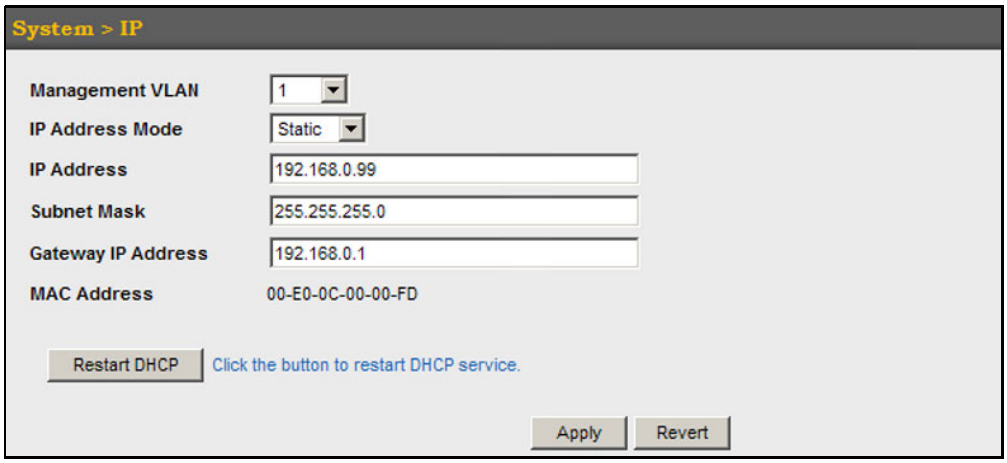
To set a static address for the switch in the web interface:

1. Click System, IP.

2. Select the VLAN through which the management station is attached, set the IP Address Mode to "Static," enter the IP address, subnet mask and gateway.

3. Click Apply.

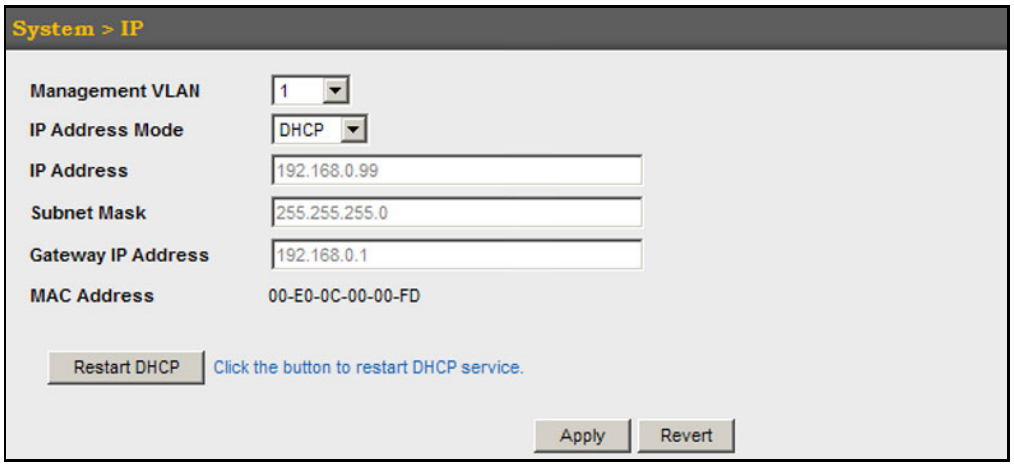
Figure 236: Configuring a Static IPv4 Address



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

1. Click System, IP.
2. Select the VLAN through which the management station is attached, set the IP Address Mode to "DHCP" or "BOOTP."
3. Click Apply to save your changes.
4. Then click Restart DHCP to immediately request a new address.

Figure 237: Configuring a Dynamic IPv4 Address



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.

SETTING THE SWITCH'S IP ADDRESS (IP VERSION 6)

This section describes how to configure an IPv6 interface for management access over the network. This switch supports both IPv4 and IPv6, and can be managed through either of these address types. For information on configuring the switch with an IPv4 address, see "Setting the Switch's IP Address (IP Version 4)" on page 402.

COMMAND USAGE

- IPv6 includes two distinct address types – link-local unicast and global unicast. A link-local address makes the switch accessible over IPv6 for all devices attached to the same local subnet. Management traffic using this kind of address cannot be passed by any router outside of the subnet. A link-local address is easy to set up, and may be useful for simple networks or basic troubleshooting tasks. However, to connect to a larger network with multiple segments, the switch must be configured with a global unicast address. Both link-local and global unicast address types can either be dynamically assigned (using the Configure Interface page) or manually configured (using the Add IPv6 Address page).

CONFIGURING THE IPV6 DEFAULT GATEWAY

Use the IP > IPv6 Configuration (Configure Global) page to configure an IPv6 default gateway for the switch.

CLI REFERENCES

- "ip default-gateway" on page 903

PARAMETERS

These parameters are displayed in the web interface:

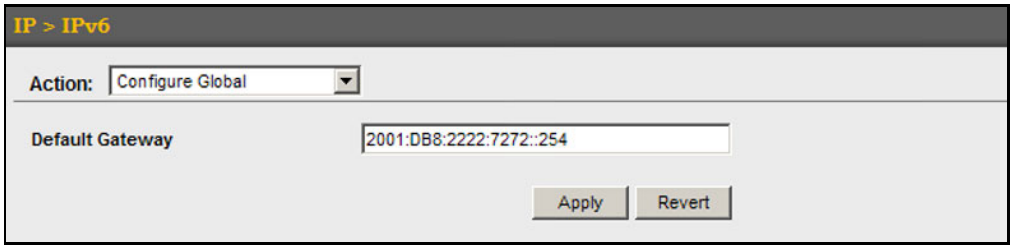
- **Default Gateway** – Sets the IPv6 address of the default next hop router.
  - An IPv6 default gateway must be defined if the management station is located in a different IPv6 segment.
  - An IPv6 default gateway can only be successfully set when a network interface that directly connects to the gateway has been configured on the switch.

WEB INTERFACE

To configure an IPv6 default gateway for the switch in the web interface:

1. Click IP, IPv6 Configuration.
2. Select Configure Global from the Action list.
3. Enter the IPv6 default gateway.
4. Click Apply.

Figure 238: Configuring the IPv6 Default Gateway



CONFIGURING IPV6 INTERFACE SETTINGS

Use the IP > IPv6 Configuration (Configure Interface) page to configure general IPv6 settings for the selected VLAN, including auto-configuration of a global unicast interface address, explicit configuration of a link local interface address, the MTU size, and neighbor discovery protocol settings for duplicate address detection and the neighbor solicitation interval.

CLI REFERENCES

- "IPv6 Interface" on page 909
- "DHCP Client" on page 895

COMMAND USAGE

- The switch must always be configured with a link-local address. The switch's address auto-configuration function will automatically create a link-local address, as well as an IPv6 global address if router advertisements are detected on the local interface.
- The option to explicitly enable IPv6 will also create a link-local address, but will not generate a global IPv6 address if auto-configuration is not enabled. In this case, you must manually configure an address (see "Configuring an IPv6 Address" on page 409).
- IPv6 Neighbor Discovery Protocol supersedes IPv4 Address Resolution Protocol in IPv6 networks. IPv6 nodes on the same network segment use Neighbor Discovery to discover each other's presence, to determine each other's link-layer addresses, to find routers and to maintain reachability information about the paths to active neighbors. The key parameters used to facilitate this process are the number of attempts made to verify whether or not a duplicate address exists on the same network segment, and the interval between neighbor solicitations used to verify reachability information.

PARAMETERS

These parameters are displayed in the web interface:

- **VLAN** – ID of a configured VLAN which is to be used for management access. By default, all ports on the switch are members of VLAN 1. However, the management station can be attached to a port belonging to any VLAN, as long as that VLAN has been assigned an IP address. (Range: 1-4093)

- **Address Autoconfig** – Enables stateless autoconfiguration of IPv6 addresses on an interface and enables IPv6 functionality on that interface. The network portion of the address is based on prefixes received in IPv6 router advertisement messages, and the host portion is automatically generated using the modified EUI-64 form of the interface identifier (i.e., the switch's MAC address).
  - If the router advertisements have the "other stateful configuration" flag set, the switch will attempt to acquire other non-address configuration information (such as a default gateway).
  - If auto-configuration is not selected, then an address must be manually configured using the Add Interface page described below.

- **Enable IPv6 Explicitly** – Enables IPv6 on an interface. Note that when an explicit address is assigned to an interface, IPv6 is automatically enabled, and cannot be disabled until all assigned addresses have been removed. (Default: Disabled)

  Disabling this parameter does not disable IPv6 for an interface that has been explicitly configured with an IPv6 address.

- **MTU** – Sets the size of the maximum transmission unit (MTU) for IPv6 packets sent on an interface. (Range: 1280-65535 bytes; Default: 1500 bytes)
  - IPv6 routers do not fragment IPv6 packets forwarded from other routers. However, traffic originating from an end-station connected to an IPv6 router may be fragmented.
  - All devices on the same physical medium must use the same MTU in order to operate correctly.
  - IPv6 must be enabled on an interface before the MTU can be set. If an IPv6 address has not been assigned to the switch, "N/A" is displayed in the MTU field.

- **ND DAD Attempts** – The number of consecutive neighbor solicitation messages sent on an interface during duplicate address detection. (Range: 0-600, Default: 1)
  - Configuring a value of 0 disables duplicate address detection.
  - Duplicate address detection determines if a new unicast IPv6 address already exists on the network before it is assigned to an interface.
  - Duplicate address detection is stopped on any interface that has been suspended (see "Configuring VLAN Groups" on page 150).

While an interface is suspended, all unicast IPv6 addresses assigned to that interface are placed in a "pending" state. Duplicate address detection is automatically restarted when the interface is administratively re-activated.

- An interface that is re-activated restarts duplicate address detection for all unicast IPv6 addresses on the interface. While duplicate address detection is performed on the interface's link-local address, the other IPv6 addresses remain in a "tentative" state. If no duplicate link-local address is found, duplicate address detection is started for the remaining IPv6 addresses.
- If a duplicate address is detected, it is set to "duplicate" state, and a warning message is sent to the console. If a duplicate link-local address is detected, IPv6 processes are disabled on the interface. If a duplicate global unicast address is detected, it is not used. All configuration commands associated with a duplicate address remain configured while the address is in "duplicate" state.
- If the link-local address for an interface is changed, duplicate address detection is performed on the new link-local address, but not for any of the IPv6 global unicast addresses already associated with the interface.

◆ **ND NS Interval** – The interval between transmitting IPv6 neighbor solicitation messages on an interface. (Range: 1000-3600000 milliseconds;

Default: 1000 milliseconds is used for neighbor discovery operations,
0 milliseconds is advertised in router advertisements.

This attribute specifies the interval between transmitting neighbor solicitation messages when resolving an address, or when probing the reachability of a neighbor. Therefore, avoid using very short intervals for normal IPv6 operations.

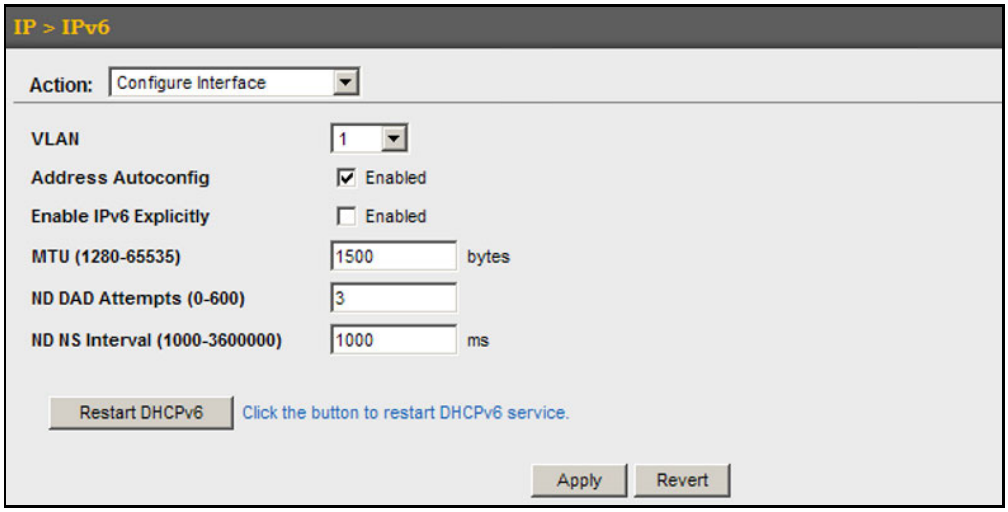
Restart DHCPv6 – DHCPv6 stateful configuration of IP address prefixes is not supported in the current software release. If the router advertisements have the "other stateful configuration" flag set, the switch will attempt to acquire other non-address configuration information (such as a default gateway) from a DHCPv6 server.

WEB INTERFACE

To general IPv6 settings for the switch in the web interface:

1. Click IP, IPv6 Configuration.
2. Select Configure Interface from the Action list.
3. Specify the VLAN to configure, enable address auto-configuration, or enable IPv6 explicitly to automatically configure a link-local address and enable IPv6 on the selected interface. Set the MTU size, the maximum number of duplicate address detection messages, and the neighbor solicitation message interval.
4. Click Apply.

Figure 239: Configuring General Settings for an IPv6 Interface



CONFIGURING AN IPV6 ADDRESS

Use the IP > IPv6 Configuration (Add IPv6 Address) page to configure an IPv6 interface for management access over the network.

CLI REFERENCES

- "IPv6 Interface" on page 909

COMMAND USAGE

- All IPv6 addresses must be formatted according to RFC 2373 "IPv6 Addressing Architecture," using 8 colon-separated 16-bit hexadecimal values. One double colon may be used in the address to indicate the appropriate number of zeros required to fill the undefined fields.

- The switch must always be configured with a link-local address. Therefore any configuration process that enables IPv6 functionality, or assigns a global unicast address to the switch, including address auto-configuration or explicitly enabling IPv6 (see "Configuring IPv6 Interface Settings" on page 406), will also automatically generate a link-local unicast address. The prefix length for a link-local address is fixed at 64 bits, and the host portion of the default address is based on the modified EUI-64 (Extended Universal Identifier) form of the interface identifier (i.e., the physical MAC address). Alternatively, you can manually configure the link-local address by entering the full address with the network prefix FE80.

- To connect to a larger network with multiple subnets, you must configure a global unicast address. There are several alternatives to configuring this address type:
  - The global unicast address can be automatically configured by taking the network prefix from router advertisements observed on the local interface, and using the modified EUI-64 form of the interface identifier to automatically create the host portion of the address (see "Configuring IPv6 Interface Settings" on page 406).

- It can be manually configured by specifying the entire network prefix and prefix length, and using the EUI-64 form of the interface identifier to automatically create the low-order 64 bits in the host portion of the address.
- You can also manually configure the global unicast address by entering the full address and prefix length.

- You can configure multiple IPv6 global unicast addresses per interface, but only one link-local address per interface.

- If a duplicate link-local address is detected on the local segment, this interface is disabled and a warning message displayed on the console. If a duplicate global unicast address is detected on the network, the address is disabled on this interface and a warning message displayed on the console.

- When an explicit address is assigned to an interface, IPv6 is automatically enabled, and cannot be disabled until all assigned addresses have been removed.

PARAMETERS

These parameters are displayed in the web interface:

- **VLAN** – ID of a configured VLAN which is to be used for management access. By default, all ports on the switch are members of VLAN 1. However, the management station can be attached to a port belonging to any VLAN, as long as that VLAN has been assigned an IP address. (Range: 1-4093)

- **Address Type** – Defines the address type configured for this interface.

  - **Global** – Configures an IPv6 global unicast address with a full IPv6 address including the network prefix and host address bits, followed by a forward slash, and a decimal value indicating how many contiguous bits (from the left) of the address comprise the prefix (i.e., the network portion of the address).

  - **EUI-64** (Extended Universal Identifier) – Configures an IPv6 address for an interface using an EUI-64 interface ID in the low order 64 bits.

    - When using EUI-64 format for the low-order 64 bits in the host portion of the address, the value entered in the IPv6 Address field includes the network portion of the address, and the prefix length indicates how many contiguous bits (starting at the left) of the address comprise the prefix (i.e., the network portion of the address). Note that the value specified in the IPv6 Address field may include some of the high-order host bits if the specified prefix length is less than 64 bits. If the specified prefix length exceeds 64 bits, then the bits used in the network portion of the address will take precedence over the interface identifier.

    - IPv6 addresses are 16 bytes long, of which the bottom 8 bytes typically form a unique host identifier based on the device's MAC

address. The EUI-64 specification is designed for devices that use an extended 8-byte MAC address. For devices that still use a 6-byte MAC address (also known as EUI-48 format), it must be converted into EUI-64 format by inverting the universal/local bit in the address and inserting the hexadecimal number FFFE between the upper and lower three bytes of the MAC address.

For example, if a device had an EUI-48 address of 28-9F-18-1C-82-35, the global/local bit must first be inverted to meet EUI-64 requirements (i.e., 1 for globally defined addresses and 0 for locally defined addresses), changing 28 to 2A. Then the two bytes FFFE are inserted between the OUI (i.e., organizationally unique identifier, or company identifier) and the rest of the address, resulting in a modified EUI-64 interface identifier of 2A-9F-18-FF-FE-1C-82-35.

- This host addressing method allows the same interface identifier to be used on multiple IP interfaces of a single device, as long as those interfaces are attached to different subnets.

- **Link Local** – Configures an IPv6 link-local address.
  - The address prefix must be FE80.
  - You can configure only one link-local address per interface.
  - The specified address replaces a link-local address that was automatically generated for the interface.

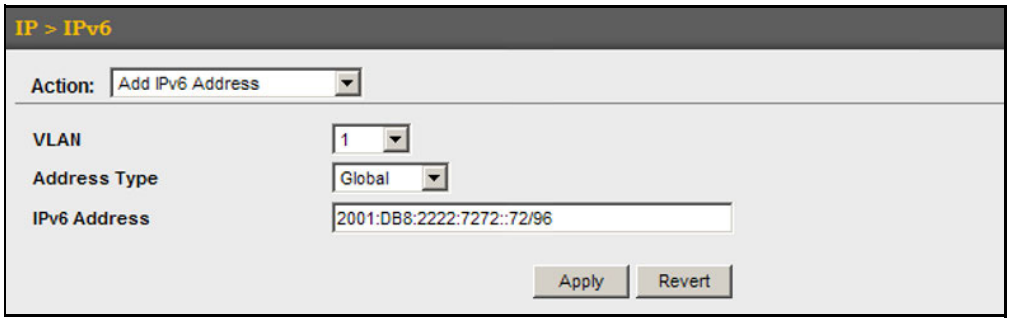
◆ **IPv6 Address** – IPv6 address assigned to this interface.

WEB INTERFACE

To configure an IPv6 address in the web interface:

1. Click IP, IPv6 Configuration.
2. Select Add IPv6 Address from the Action list.
3. Specify the VLAN to configure, select the address type, and then enter an IPv6 address and prefix length.
4. Click Apply.

Figure 240: Configuring an IPv6 Address



SHOWING IPV6 ADDRESSES

Use the IP > IPv6 Configuration (Show IPv6 Address) page to display the IPv6 addresses assigned to an interface.

CLI REFERENCES

- "show ipv6 interface" on page 919

PARAMETERS

These parameters are displayed in the web interface:

- **VLAN** – ID of a configured VLAN which is to be used for management access. By default, all ports on the switch are members of VLAN 1. However, the management station can be attached to a port belonging to any VLAN, as long as that VLAN has been assigned an IP address. (Range: 1-4093)

- **IP Address Type** – The address type (Global, EUI-64, Link Local).

- **IP Address** – An IPv6 address assigned to this interface.

  In addition to the unicast addresses assigned to an interface, a host is also required to listen to the all-nodes multicast addresses FF01::1 (interface-local scope) and FF02::1 (link-local scope).

  FF01::1/16 is the transient interface-local multicast address for all attached IPv6 nodes, and FF02::1/16 is the link-local multicast address for all attached IPv6 nodes. The interface-local multicast address is only used for loopback transmission of multicast traffic. Link-local multicast addresses cover the same types as used by link-local unicast addresses, including all nodes (FF02::1), all routers (FF02::2), and solicited nodes (FF02::1:FFXX:XXXX) as described below.

  A node is also required to compute and join the associated solicited-node multicast addresses for every unicast and anycast address it is assigned. IPv6 addresses that differ only in the high-order bits, e.g. due to multiple high-order prefixes associated with different aggregations, will map to the same solicited-node address, thereby reducing the number of multicast addresses a node must join. In this example, FF02::1:FF90:0/104 is the solicited-node multicast address which is formed by taking the low-order 24 bits of the address and appending those bits to the prefix.

  Note that the solicited-node multicast address (link-local scope FF02) is used to resolve the MAC addresses for neighbor nodes since IPv6 does not support the broadcast method used by the Address Resolution Protocol in IPv4.

  These additional addresses are displayed by the CLI (see "show ip interface" on page 904).

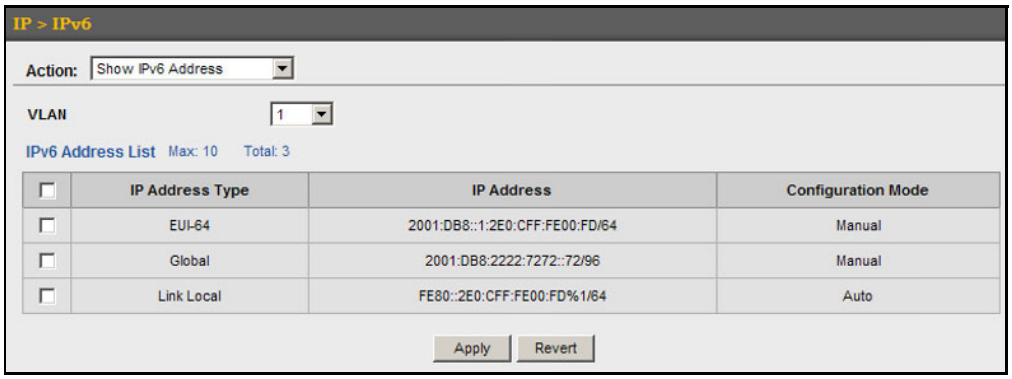
- **Configuration Mode** – Indicates if this address was automatically generated for manually configured.

WEB INTERFACE

To show the configured IPv6 addresses in the web interface:

1. Click IP, IPv6 Configuration.
2. Select Show IPv6 Address from the Action list.
3. Select a VLAN from the list.

Figure 241: Showing Configured IPv6 Addresses



SHOWING THE IPV6 NEIGHBOR CACHE

Use the IP > IPv6 Configuration (Show IPv6 Neighbor Cache) page to display the IPv6 addresses detected for neighbor devices.

CLI REFERENCES

- "show ipv6 neighbors" on page 930

PARAMETERS

These parameters are displayed in the web interface:

Table 29: Show IPv6 Neighbors - display description

Field	Description
IPv6 Address	IPv6 address of neighbor
Age	The time since the address was verified as reachable (in seconds). A static entry is indicated by the value "Permanent."
Link-layer Addr	Physical layer MAC address.

Table 29: Show IPv6 Neighbors - display description (Continued)

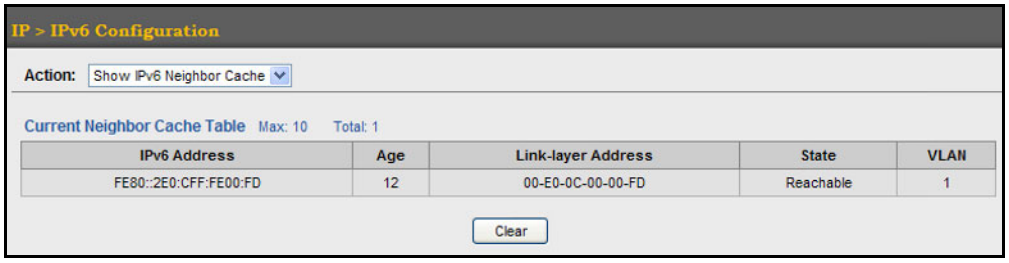
Field	Description
State	The following states are used for dynamic entries: ◆ INCMP (Incomplete) - Address resolution is being carried out on the entry. A neighbor solicitation message has been sent to the multicast address of the target, but it has not yet returned a neighbor advertisement message. ◆ REACH (Reachable) - Positive confirmation was received within the last ReachableTime interval that the forward path to the neighbor was functioning. While in REACH state, the device takes no special action when sending packets. ◆ STALE - More than the ReachableTime interval has elapsed since the last positive confirmation was received that the forward path was functioning. While in STALE state, the device takes no action until a packet is sent. ◆ DELAY - More than the ReachableTime interval has elapsed since the last positive confirmation was received that the forward path was functioning. A packet was sent within the last DELAY_FIRST_PROBE_TIME interval. If no reachability confirmation is received within this interval after entering the DELAY state, the switch will send a neighbor solicitation message and change the state to PROBE. ◆ PROBE - A reachability confirmation is actively sought by resending neighbor solicitation messages every RetransTimer interval until confirmation of reachability is received. ◆ UNKNO - Unknown state. The following states are used for static entries: ◆ INCMP (Incomplete)-The interface for this entry is down. ◆ REACH (Reachable) - The interface for this entry is up. Reachability detection is not applied to static entries in the IPv6 neighbor discovery cache.
VLAN	VLAN interface from which the address was reached.

WEB INTERFACE

To show neighboring IPv6 devices in the web interface:

1. Click IP, IPv6 Configuration.
2. Select Show IPv6 Neighbors from the Action list.

Figure 242: Showing IPv6 Neighbors



SHOWING IPV6 STATISTICS

Use the IP > IPv6 Configuration (Show Statistics) page to display statistics about IPv6 traffic passing through this switch.

CLI REFERENCES

- "show ipv6 traffic" on page 921

COMMAND USAGE

This switch provides statistics for the following traffic types:

- **IPv6** – The Internet Protocol for Version 6 addresses provides a mechanism for transmitting blocks of data (often called packets or frames) from a source to a destination, where these network devices (that is, hosts) are identified by fixed length addresses. The Internet Protocol also provides for fragmentation and reassembly of long packets, if necessary, for transmission through "small packet" networks.

- **ICMPv6** – Internet Control Message Protocol for Version 6 addresses is a network layer protocol that transmits message packets to report errors in processing IPv6 packets. ICMP is therefore an integral part of the Internet Protocol. ICMP messages may be used to report various situations, such as when a datagram cannot reach its destination, when the gateway does not have the buffering capacity to forward a datagram, and when the gateway can direct the host to send traffic on a shorter route. ICMP is also used by routers to feed back information about more suitable routes (that is, the next hop router) to use for a specific destination.

- **UDP** – User Datagram Protocol provides a datagram mode of packet switched communications. It uses IP as the underlying transport mechanism, providing access to IP-like services. UDP packets are delivered just like IP packets – connection-less datagrams that may be discarded before reaching their targets. UDP is useful when TCP would be too complex, too slow, or just unnecessary.

PARAMETERS

These parameters are displayed in the web interface:

Table 30: Show IPv6 Statistics - display description

Field	Description
IPv6 Statistics	
IPv6 Received	
Total	The total number of input datagrams received by the interface, including those received in error.
Header Errors	The number of input datagrams discarded due to errors in their IPv6 headers, including version number mismatch, other format errors, hop count exceeded, IPv6 options, etc.
Too Big Errors	The number of input datagrams that could not be forwarded because their size exceeded the link MTU of outgoing interface.
No Routes	The number of input datagrams discarded because no route could be found to transmit them to their destination.

Table 30: Show IPv6 Statistics - display description (Continued)

Field	Description
Address Errors	The number of input datagrams discarded because the IPv6 address in their IPv6 header's destination field was not a valid address to be received at this entity. This count includes invalid addresses (e.g., ::0) and unsupported addresses (e.g., addresses with unallocated prefixes). For entities which are not IPv6 routers and therefore do not forward datagrams, this counter includes datagrams discarded because the destination address was not a local address.
Unknown Protocols	The number of locally-addressed datagrams received successfully but discarded because of an unknown or unsupported protocol. This counter is incremented at the interface to which these datagrams were addressed which might not be necessarily the input interface for some of the datagrams.
Truncated Packets	The number of input datagrams discarded because datagram frame didn't carry enough data.
Discards	The number of input IPv6 datagrams for which no problems were encountered to prevent their continued processing, but which were discarded (e.g., for lack of buffer space). Note that this counter does not include any datagrams discarded while awaiting re-assembly.
Delivers	The total number of datagrams successfully delivered to IPv6 user-protocols (including ICMP). This counter is incremented at the interface to which these datagrams were addressed which might not be necessarily the input interface for some of the datagrams.
Reassembly Request Datagrams	The number of IPv6 fragments received which needed to be reassembled at this interface. Note that this counter is increment ed at the interface to which these fragments were addressed which might not be necessarily the input interface for some of the fragments.
Reassembled Succeeded	The number of IPv6 datagrams successfully reassembled. Note that this counter is incremented at the interface to which these datagrams were addressed which might not be necessarily the input interface for some of the fragments.
Reassembled Failed	The number of failures detected by the IPv6 re-assembly algorithm (for whatever reason: timed out, errors, etc.). Note that this is not necessarily a count of discarded IPv6 fragments since some algorithms (notably the algorithm in RFC 815) can lose track of the number of fragments by combining them as they are received. This counter is incremented at the interface to which these fragments were addressed which might not be necessarily the input interface for some of the fragments.
IPv6 Transmitted	
Forwards Datagrams	The number of output datagrams which this entity received and forwarded to their final destinations. In entities which do not act as IPv6 routers, this counter will include only those packets which were Source-Routed via this entity, and the Source-Route processing was successful. Note that for a successfully forwarded datagram the counter of the outgoing interface is incremented."
Requests	The total number of IPv6 datagrams which local IPv6 user-protocols (including ICMP) supplied to IPv6 in requests for transmission. Note that this counter does not include any datagrams counted in ipv6IfStatsOutForwDatagrams.
Discards	The number of output IPv6 datagrams for which no problem was encountered to prevent their transmission to their destination, but which were discarded (e.g., for lack of buffer space). Note that this counter would include datagrams counted in ipv6IfStatsOutForwDatagrams if any such packets met this (discretionary) discard criterion.
No Routes	The number of input datagrams discarded because no route could be found to transmit them to their destination.

Table 30: Show IPv6 Statistics - display description (Continued)

Field	Description
Generated Fragments	The number of output datagram fragments that have been generated as a result of fragmentation at this output interface.
Fragment Succeeded	The number of IPv6 datagrams that have been successfully fragmented at this output interface.
Fragment Failed	The number of IPv6 datagrams that have been discarded because they needed to be fragmented at this output interface but could not be.
ICMPv6 Statistics	
ICMPv6 received	
Input	The total number of ICMP messages received by the interface which includes all those counted by ipv6IfIcmpInErrors. Note that this interface is the interface to which the ICMP messages were addressed which may not be necessarily the input interface for the messages.
Errors	The number of ICMP messages which the interface received but determined as having ICMP-specific errors (bad ICMP checksums, bad length, etc.).
Destination Unreachable Messages	The number of ICMP Destination Unreachable messages received by the interface.
Packet Too Big Messages	The number of ICMP Packet Too Big messages received by the interface.
Time Exceeded Messages	The number of ICMP Time Exceeded messages received by the interface.
Parameter Problem Messages	The number of ICMP Parameter Problem messages received by the interface.
Echo Request Messages	The number of ICMP Echo (request) messages received by the interface.
Echo Reply Messages	The number of ICMP Echo Reply messages received by the interface.
Redirect Messages	The number of Redirect messages received by the interface.
Group Membership Query Messages	The number of ICMPv6 Group Membership Query messages received by the interface.
Group Membership Response Messages	The number of ICMPv6 Group Membership Response messages received by the interface.
Group Membership Reduction Messages	The number of ICMPv6 Group Membership Reduction messages received by the interface.
Router Solicit Messages	The number of ICMP Router Solicit messages received by the interface.
Router Advertisement Messages	The number of ICMP Router Advertisement messages received by the interface.
Neighbor Solicit Messages	The number of ICMP Neighbor Solicit messages received by the interface.
Neighbor Advertisement Messages	The number of ICMP Neighbor Advertisement messages received by the interface.
Redirect Messages	The number of Redirect messages received by the interface.
ICMPv6 Transmitted	
Output	The total number of ICMP messages which this interface attempted to send. Note that this counter includes all those counted by icmpOutErrors.

Table 30: Show IPv6 Statistics - display description (Continued)

Field	Description
Destination Unreachable Messages	The number of ICMP Destination Unreachable messages sent by the interface.
Packet Too Big Messages	The number of ICMP Packet Too Big messages sent by the interface.
Time Exceeded Messages	The number of ICMP Time Exceeded messages sent by the interface.
Parameter Problem Message	The number of ICMP Parameter Problem messages sent by the interface.
Echo Reply Messages	The number of ICMP Echo Reply messages sent by the interface.
Router Solicit Messages	The number of ICMP Router Solicitation messages sent by the interface.
Neighbor Advertisement Messages	The number of ICMP Router Advertisement messages sent by the interface.
Redirect Messages	The number of Redirect messages sent. For a host, this object will always be zero, since hosts do not send redirects.
Group Membership Response Messages	The number of ICMPv6 Group Membership Response messages sent.
Group Membership Reduction Messages	The number of ICMPv6 Group Membership Reduction messages sent.
UDP Statistics	
Input	The total number of UDP datagrams delivered to UDP users.
No Port Errors	The total number of received UDP datagrams for which there was no application at the destination port.
Other Errors	The number of received UDP datagrams that could not be delivered for reasons other than the lack of an application at the destination port.
Output	The total number of UDP datagrams sent from this entity.

WEB INTERFACE

To show the IPv6 statistics in the web interface:

1. Click IP, IPv6 Configuration.
2. Select Show Statistics from the Action list.
3. Click IPv6, ICMPv6 or UDP.

Figure 243: Showing IPv6 Statistics (IPv6)

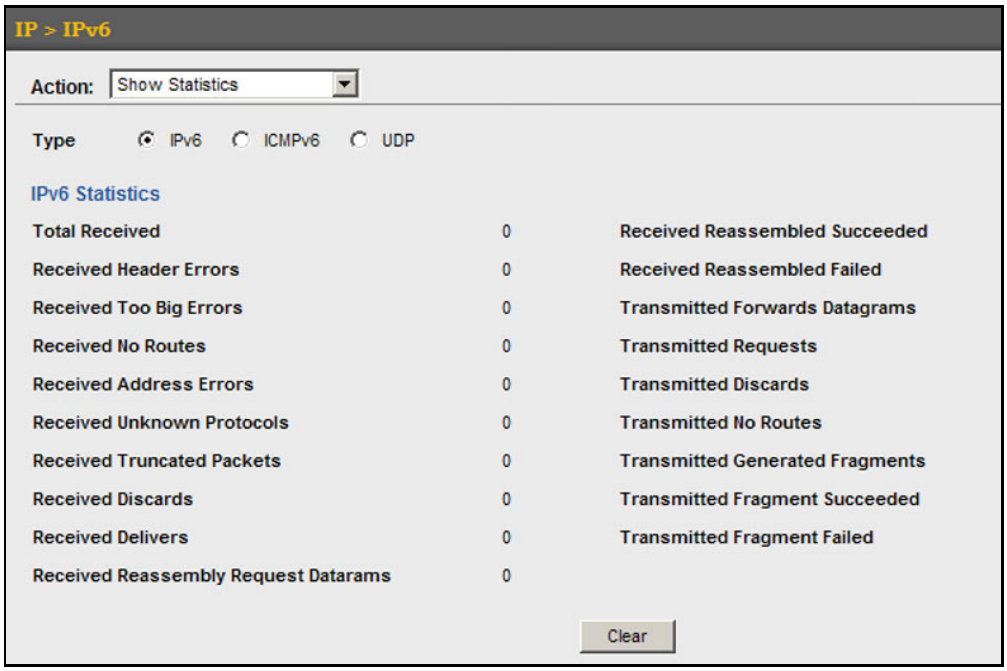


Figure 244: Showing IPv6 Statistics (ICMPv6)

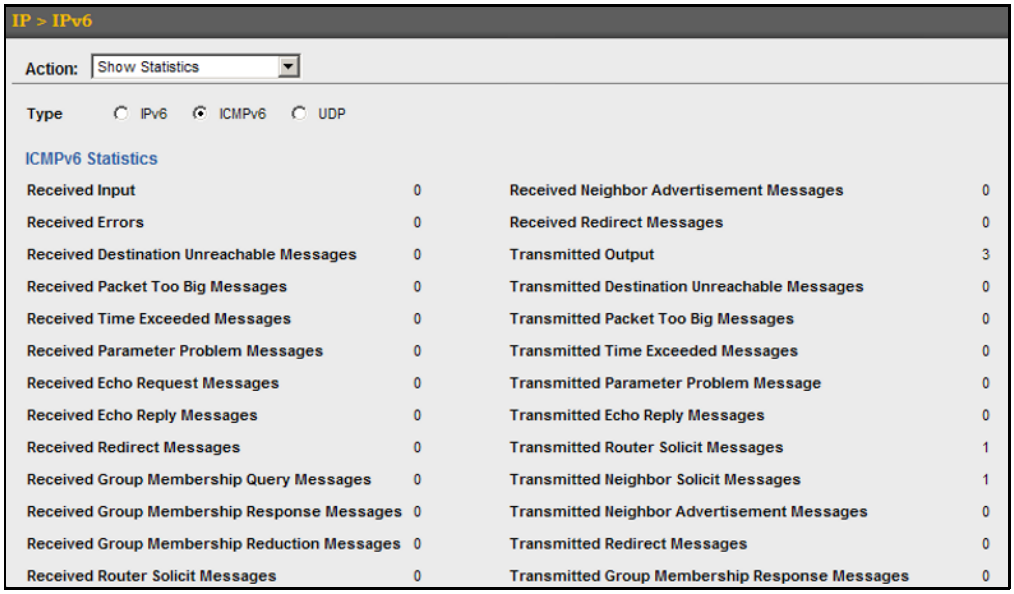
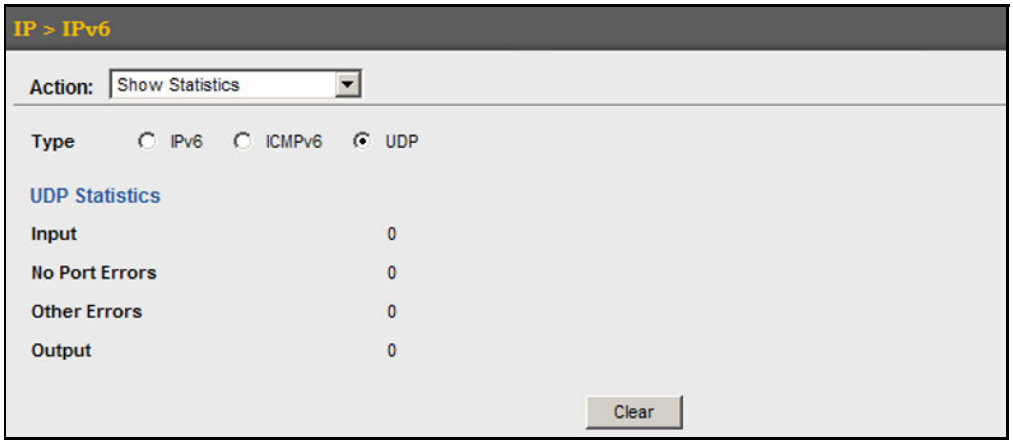


Figure 245: Showing IPv6 Statistics (UDP)



SHOWING THE MTU FOR RESPONDING DESTINATIONS

Use the IP > IPv6 Configuration (Show MTU) page to display the maximum transmission unit (MTU) cache for destinations that have returned an ICMP packet-too-big message along with an acceptable MTU to this switch.

CLI REFERENCES

- "show ipv6 mtu" on page 920

PARAMETERS

These parameters are displayed in the web interface:

Table 31: Show MTU - display description

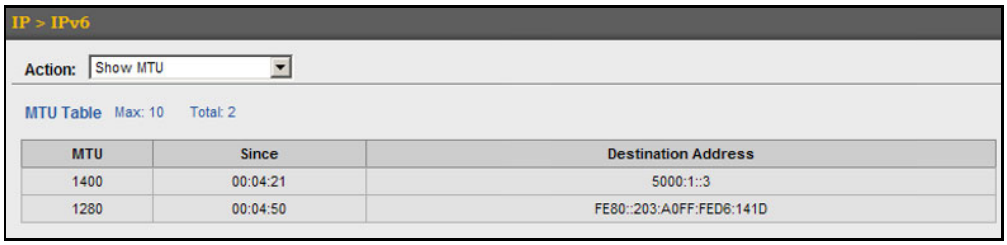
Field	Description
MTU	Adjusted MTU contained in the ICMP packet-too-big message returned from this destination, and now used for all traffic sent along this path.
Since	Time since an ICMP packet-too-big message was received from this destination.
Destination Address	Address which sent an ICMP packet-too-big message.

WEB INTERFACE

To show the MTU reported from other devices in the web interface:

1. Click IP, IPv6 Configuration.
2. Select Show MTU from the Action list.

Figure 246: Showing Reported MTU Values



MTU	Since	Destination Address
1400	00:04:21	5000:1::3
1280	00:04:50	FE80::203:A0FF:FED6:141D

17 IP SERVICES

This chapter describes how to configure Domain Name Service (DNS) on this switch. For information on DHCP snooping which is included in this folder, see "DHCP Snooping" on page 330.

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 886
- "ip domain-name" on page 887

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 426).

PARAMETERS

These parameters are displayed in the web interface:

- **Domain Lookup** – Enables DNS host name-to-address translation. (Default: Disabled)

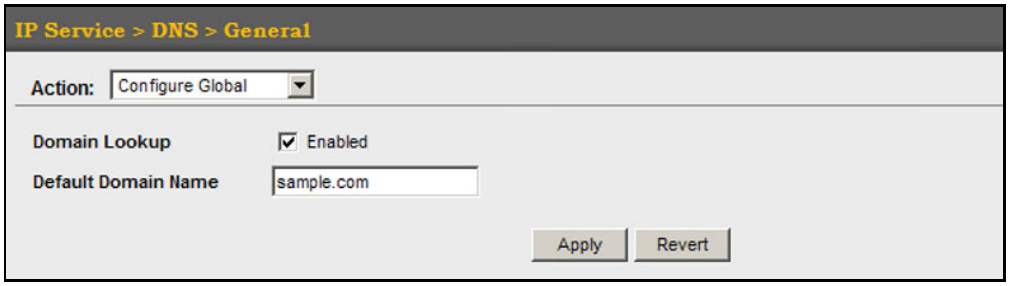
- **Default Domain Name** – Defines the default domain name appended to incomplete host names. Do not include the initial dot that separates the host name from the domain name.
  (Range: 1-127 alphanumeric characters)

WEB INTERFACE

To configure general settings for DNS in the web interface:

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 247: Configuring General Settings for DNS



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 885
- "show dns" on page 891

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 423). 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 426).

PARAMETERS

These parameters are displayed in the web interface:

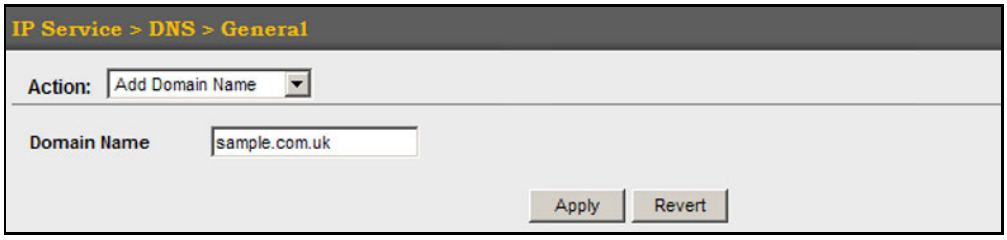
Domain Name – Name of the host. Do not include the initial dot that separates the host name from the domain name.
(Range: 1-68 characters)

WEB INTERFACE

To create a list domain names in the web interface:

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.

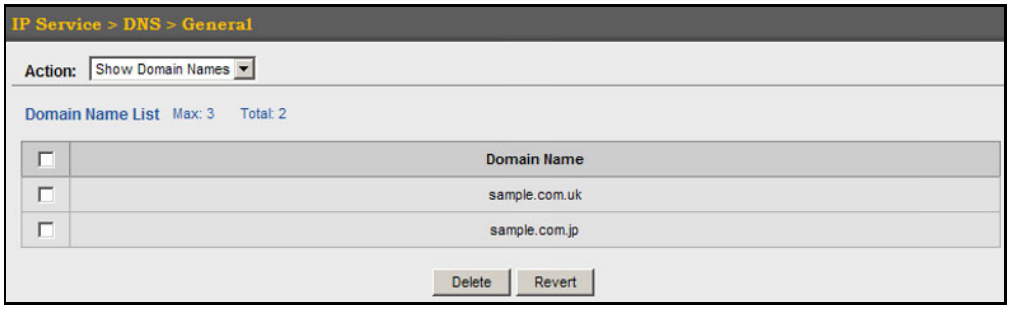
Figure 248: Configuring a List of Domain Names for DNS



To show the list domain names in the web interface:

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

Figure 249: Showing the List of Domain Names for DNS



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 889
- "show dns" on page 891

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 423).
- 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:

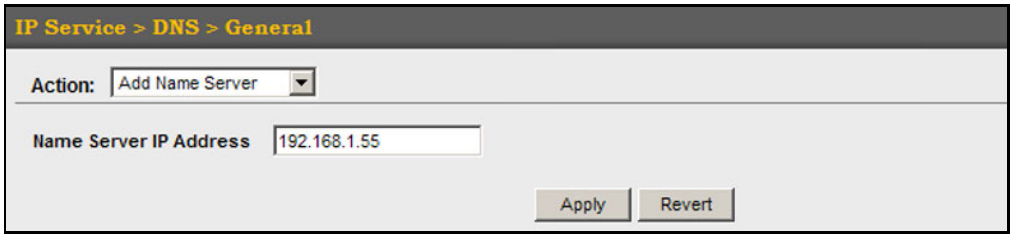
Name Server IP Address – Specifies the address of a domain name server to use for name-to-address resolution. Up to six IP addresses can be added to the name server list.

WEB INTERFACE

To create a list name servers in the web interface:

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 250: Configuring a List of Name Servers for DNS

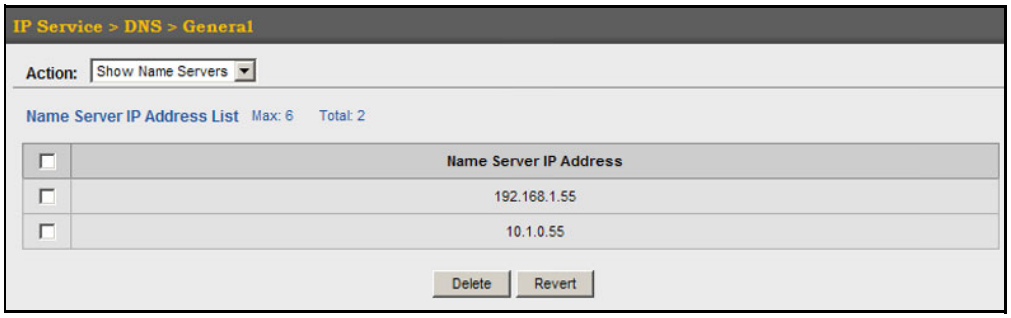


To show the list name servers in the web interface:

1. Click IP Service, DNS.

2. Select Show Name Servers from the Action list.

Figure 251: Showing the List of Name Servers for DNS



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 888
- "show hosts" on page 892

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 in the web interface:

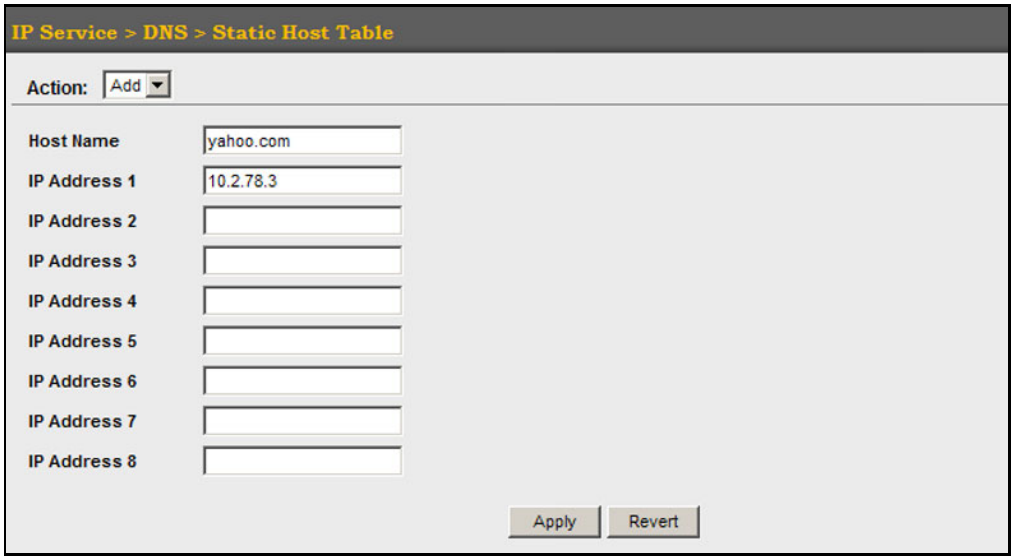
1. Click IP Service, DNS, Static Host Table.

2. Select Add from the Action list.

3. Enter a host name and the corresponding address.

4. Click Apply.

Figure 252: Configuring Static Entries in the DNS Table

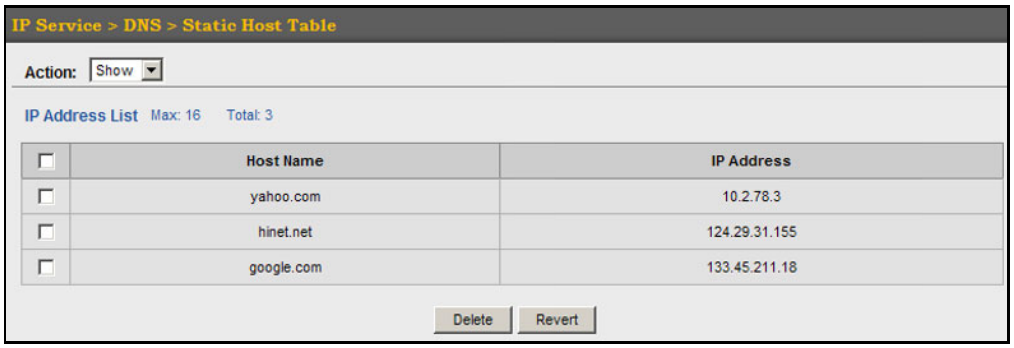


To show static entries in the DNS table in the web interface:

1. Click IP Service, DNS, Static Host Table.

2. Select Show from the Action list.

Figure 253: Showing Static Entries in the DNS Table



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 892

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:

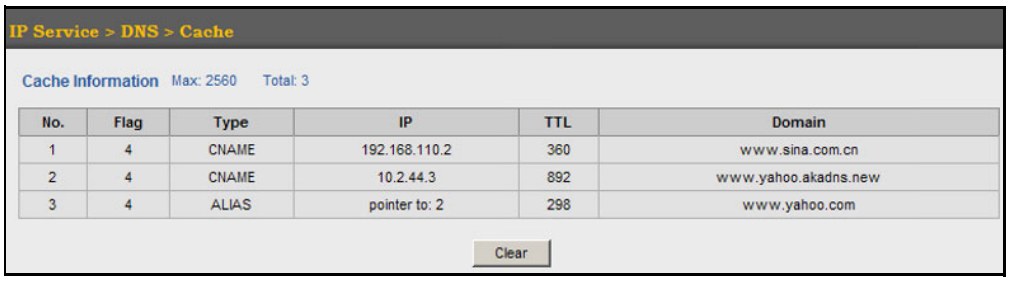
- **No.** – The entry number for each resource record.
- **Flag** – The flag is always “4” indicating a cache entry and therefore unreliable.
- **Type** – This field includes CNAME which specifies the host address for the owner, and ALIAS which specifies an alias.
- **IP** – The IP address associated 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 in the web interface:

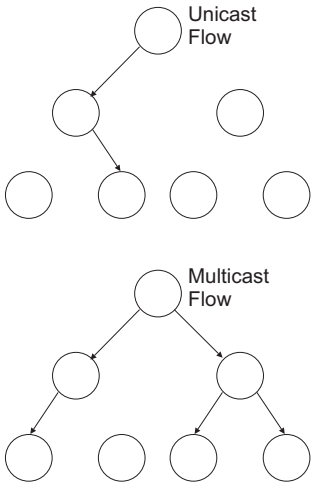
1. Click IP Service, DNS, Cache.

Figure 254: Showing Entries in the DNS Cache



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

18 MULTICAST FILTERING



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.

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 (Layer 2) 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).

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 452.

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 433) 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.

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 437). 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 256 multicast entries can be maintained for IGMP snooping. 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 433).

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 437). 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 439).

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

When proxy reporting is disabled, all IGMP reports received by the switch are forwarded natively to the upstream multicast routers.

- Last Leave: Intercepts, absorbs and summarizes IGMP leaves coming from IGMP hosts. IGMP leaves are relayed upstream only when necessary, that is, when the last user leaves a multicast group.
- Query Suppression: Intercepts and processes IGMP queries in such a way that IGMP specific queries are never sent to client ports.

The only deviation from TR-101 is that 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. 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 833

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 DVMRP or 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 441).

  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, an 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

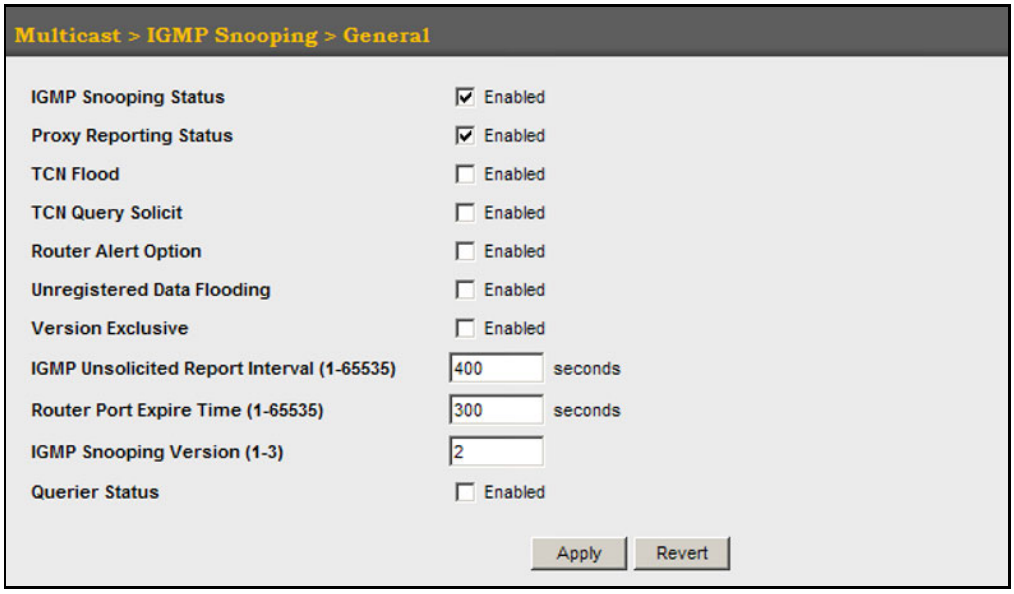
To configure general settings for IGMP Snooping and Query in the web interface:

1. Click Multicast, IGMP Snooping, General.

2. Adjust the IGMP settings as required.

3. Click Apply.

Figure 255: Configuring General Settings for IGMP Snooping



SPECIFYING STATIC INTERFACES FOR A MULTICAST ROUTER

Use the Multicast > IGMP Snooping > Multicast Router (Add) 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 851

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

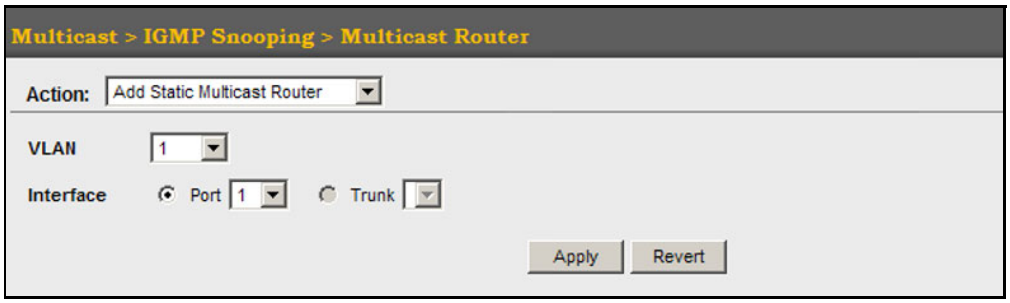
To specify a static interface attached to a multicast router in the web interface:

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 256: Configuring a Static Interface for a Multicast Router



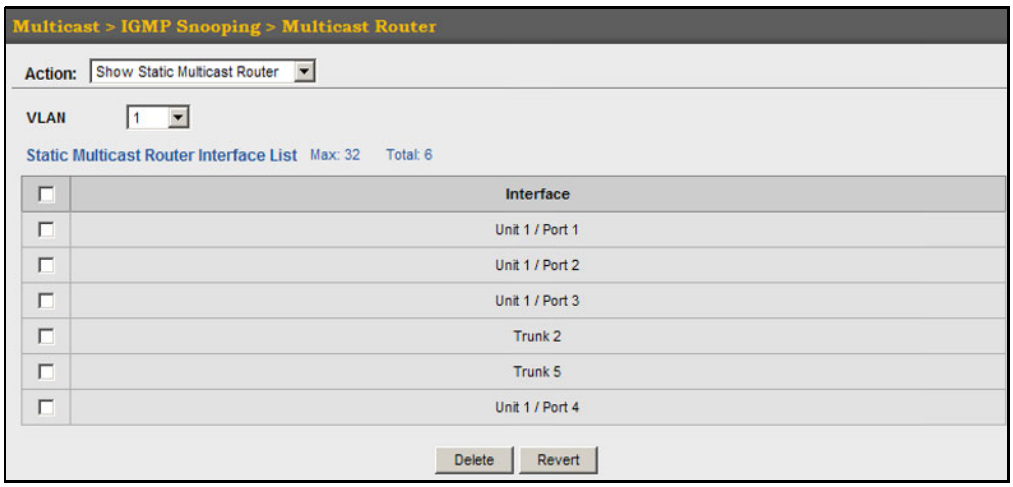
To show the static interfaces attached to a multicast router in the web interface:

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 257: Showing Static Interfaces Attached a Multicast Router



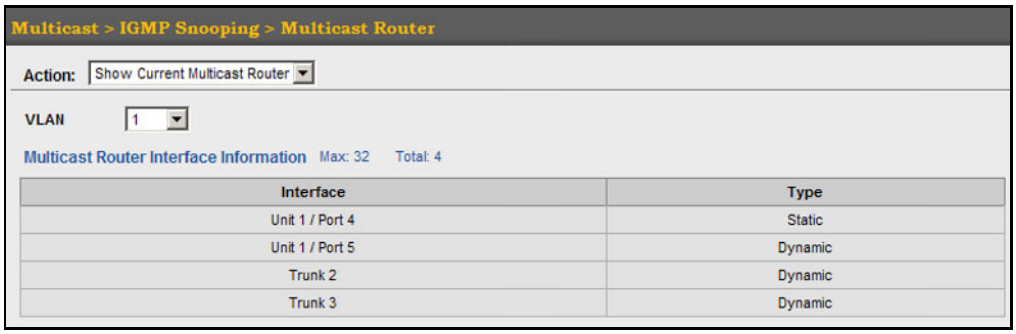
To show the all interfaces attached to a multicast router in the web interface:

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.

Figure 258: Showing Current Interfaces Attached a Multicast Router



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 433). 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 848

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

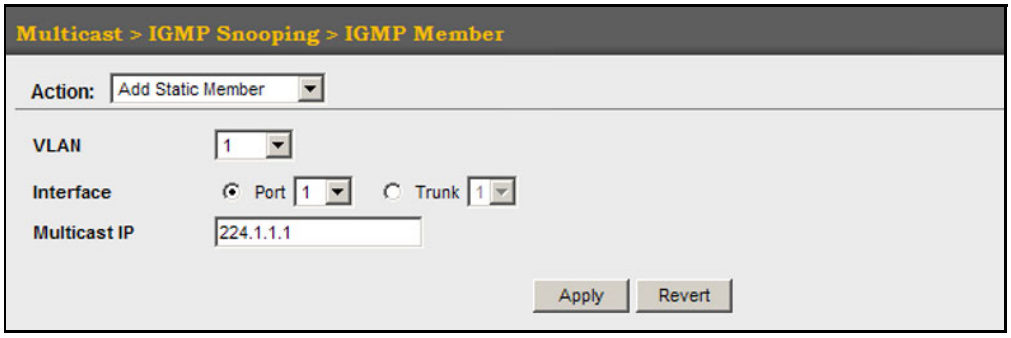
To statically assign an interface to a multicast service in the web interface:

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 259: Assigning an Interface to a Multicast Service



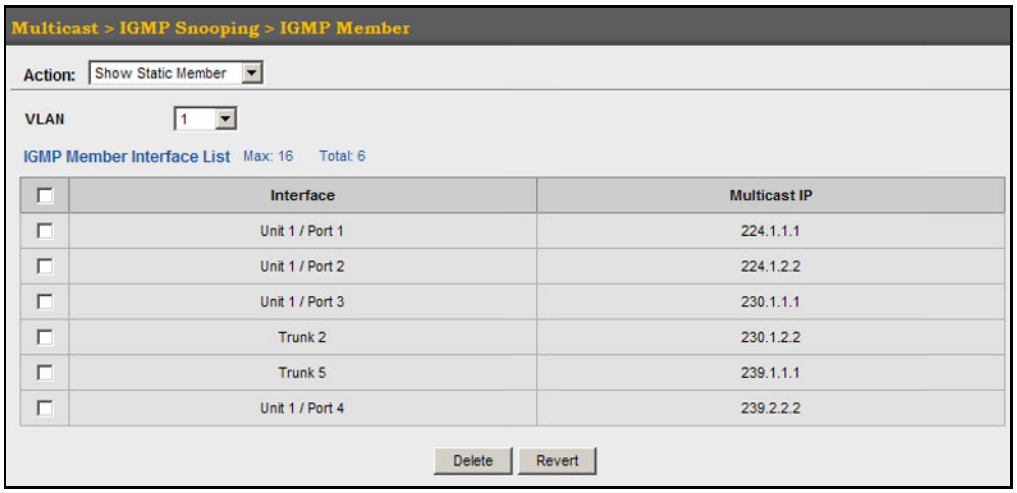
To show the static interfaces assigned to a multicast service in the web interface:

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 260: Showing Static Interfaces Assigned to a Multicast Service



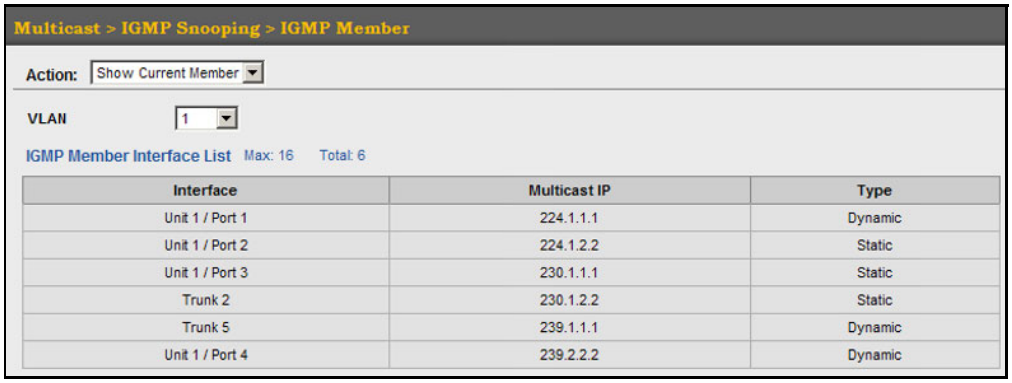
To show the all interfaces statically or dynamically assigned to a multicast service in the web interface:

1. Click Multicast, IGMP Snooping, Multicast Router.

2. Select Current Member from the Action list.

3. Select the VLAN for which to display this information.

Figure 261: Showing Current Interfaces Assigned to a Multicast Service



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 433.

CLI REFERENCES

- "IGMP Snooping" on page 833

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 433), the per VLAN interface settings for IGMP snooping take precedence.

When IGMP snooping is disabled globally, snooping can still be configured per VLAN interface, but the interface settings will not take effect until snooping is re-enabled globally.

- **Version Exclusive** – Discards any received IGMP messages (except for multicast protocol packets) which use a version different to that currently configured by the IGMP Version attribute. (Default: Disabled)

  If version exclusive is disabled on a VLAN, then this setting is based on the global setting configured on the Multicast > IGMP Snooping > General page. If it is enabled on a VLAN, then this setting takes precedence over the global setting.

- **Immediate Leave Status** – Immediately deletes a member port of a multicast service if a leave packet is received at that port and immediate leave is enabled for the parent VLAN. (Default: Disabled)

  If immediate leave is not used, a multicast router (or querier) will send a group-specific query message when an IGMPv2 group leave message is received. The router/querier stops forwarding traffic for that group only if no host replies to the query within the specified time out period. Note that this time out is set to Last Member Query Interval * Robustness Variable (fixed at 2) as defined in RFC 2236.

  If immediate leave is enabled, the switch assumes that only one host is connected to the interface. Therefore, immediate leave should only be enabled on an interface if it is connected to only one IGMP-enabled device, either a service host or a neighbor running IGMP snooping.

  This attribute is only effective if IGMP snooping is enabled, and IGMPv2 snooping is used.

- **Multicast Router Discovery** – MRD is used to discover which interfaces are attached to multicast routers. (Default: 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.

- **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.

- **Proxy 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 will take effect only if IGMP snooping proxy reporting is enabled (see page 433).

- **Proxy 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 will take effect only if IGMP snooping proxy reporting is enabled (see page 433).

- **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 433).

- **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.

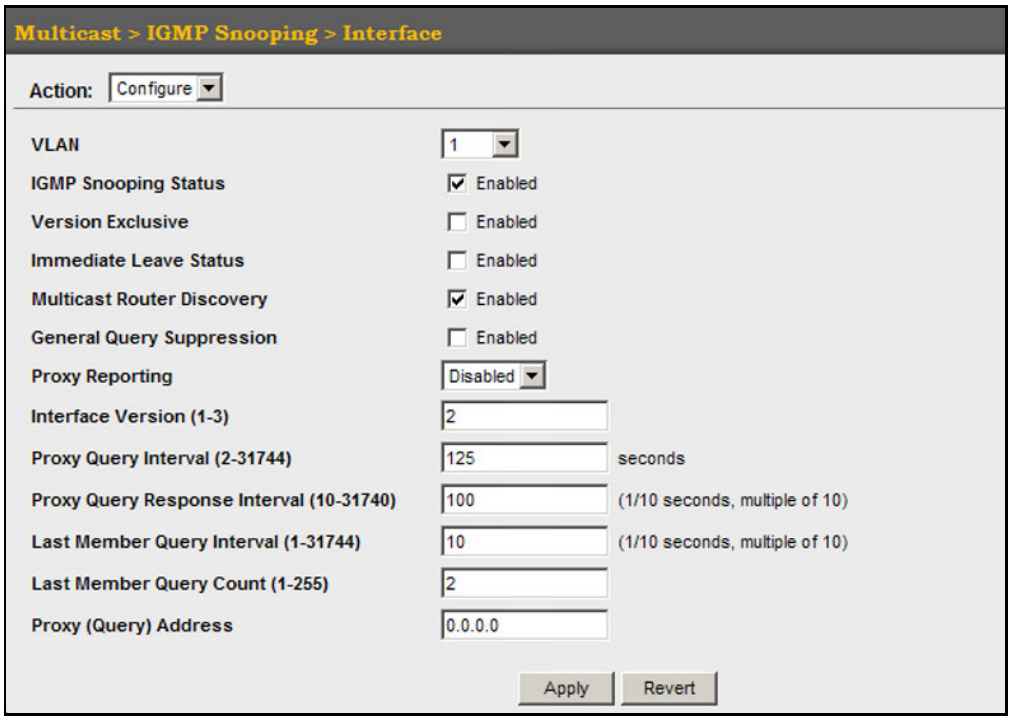
To resolve this problem, the source address in proxied IGMP query messages can be replaced with any valid unicast address (other than the router's own address).

WEB INTERFACE

To configure IGMP snooping on a VLAN in the web interface:

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 262: Configuring IGMP Snooping on an Interface



To show the interface settings for IGMP snooping in the web interface:

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

Figure 263: Showing Interface Settings for IGMP Snooping

Multicast > IGMP Snooping > Interface

Action: Show

IGMP Snooping VLAN List Max: 256 Total: 2

VLAN	IGMP Snooping Status	Immediate Leave Status	Proxy Query Interval	Proxy 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
4093	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 850

COMMAND USAGE

To display information about multicast groups, IGMP Snooping must first be enabled on the switch (see page 433).

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 in the web interface:

1. Click Multicast, IGMP Snooping, Forwarding Entry.
2. Select the VLAN for which to display this information.

Figure 264: Showing Multicast Groups Learned by IGMP Snooping

Multicast > IGMP Snooping > Forwarding Entry

VLAN 1

IGMP Snooping Forwarding Entry List Max: 32 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 853

PARAMETERS

These parameters are displayed in the web interface:

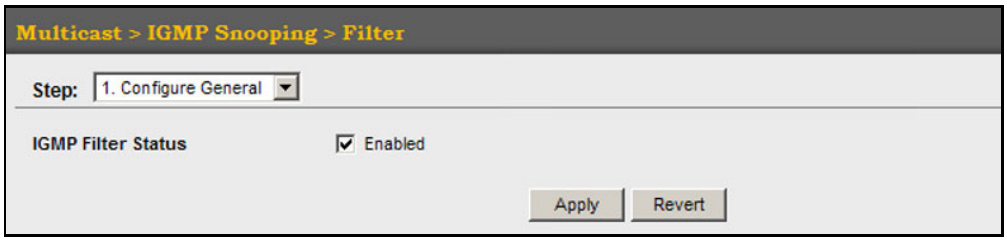
- **IGMP Filter Status** – Enables IGMP filtering and throttling globally for the switch. (Default: Disabled)

WEB INTERFACE

To enables IGMP filtering and throttling on the switch in the web interface:

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

Figure 265: Enabling IGMP Filtering and Throttling



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 852

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

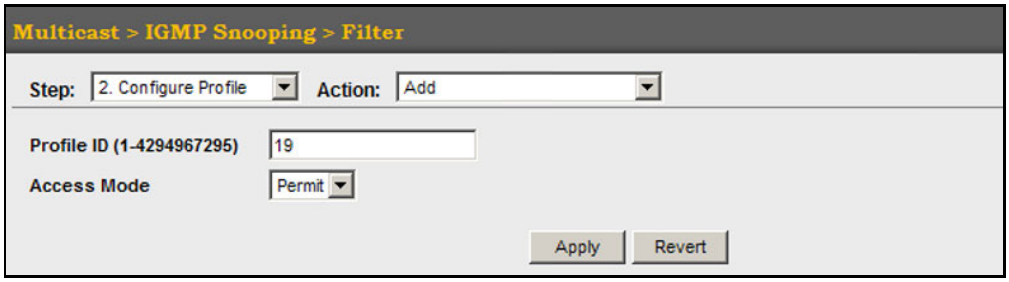
- **Profile ID** – Selects an IGMP profile to configure.
- **Start Multicast IP Address** – Specifies the starting address of a range of multicast groups.
- **End Multicast IP Address** – Specifies the ending address of a range of multicast groups.

WEB INTERFACE

To create an IGMP filter profile and set its access mode in the web interface:

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.

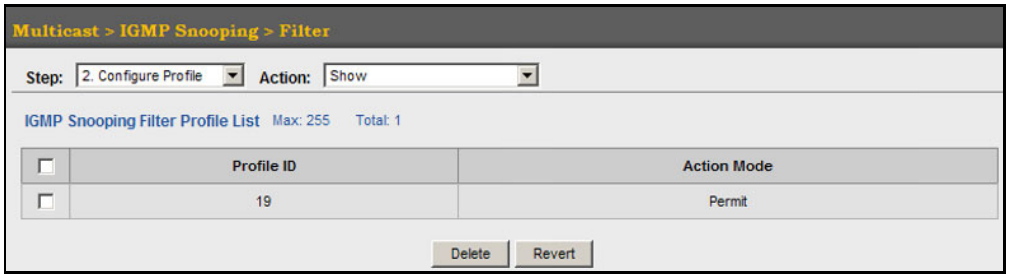
Figure 266: Creating an IGMP Filtering Profile



To show the IGMP filter profiles in the web interface:

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

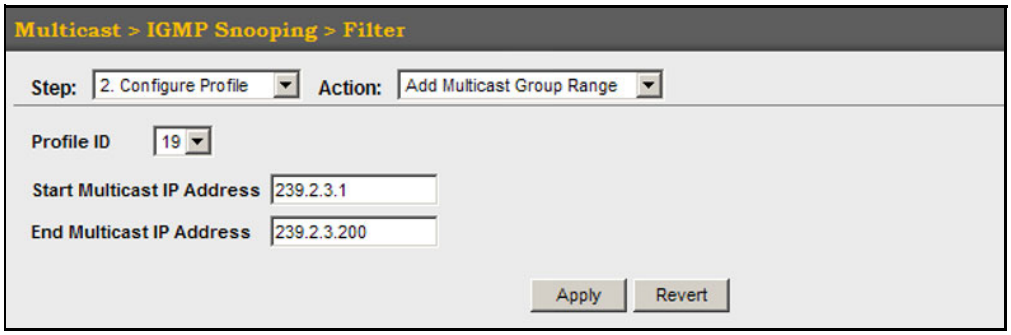
Figure 267: Showing the IGMP Filtering Profiles Created



To add a range of multicast groups to an IGMP filter profile in the web interface:

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.

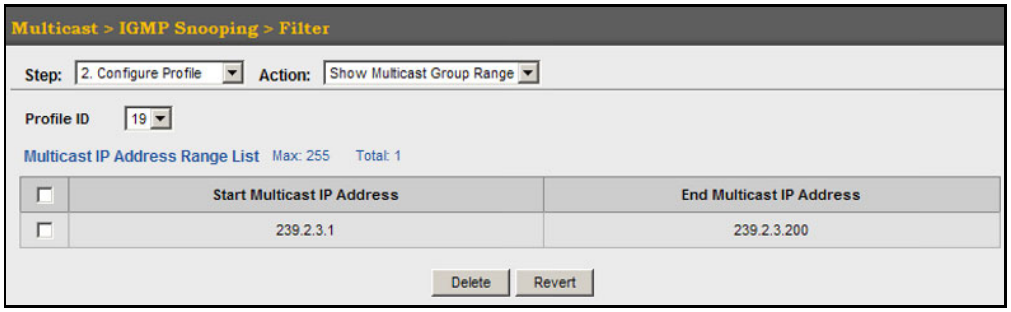
Figure 268: Adding Multicast Groups to an IGMP Filtering Profile



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

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 269: Showing the Groups Assigned to an IGMP Filtering Profile



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 852

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: 0-1024; Default: 256)

- **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.

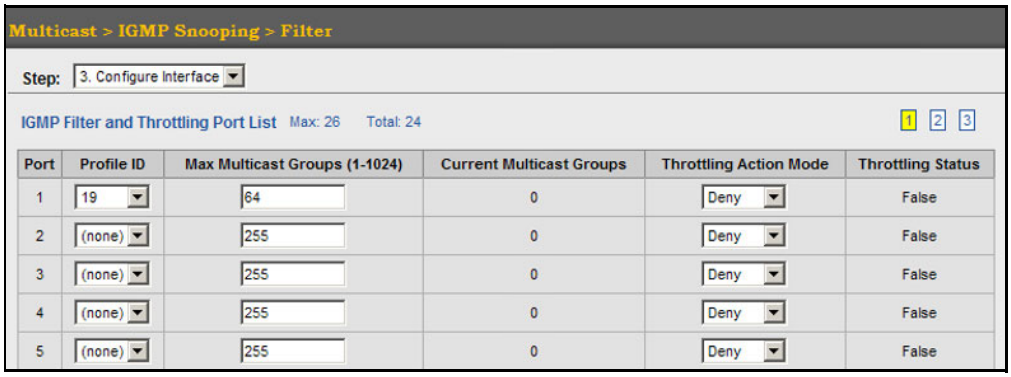
◆ **Throttling Status** – Indicates if the throttling action has been implemented on the interface. (Options: True or False)

WEB INTERFACE

To configure IGMP filtering or throttling for a port or trunk in the web interface:

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 270: Configuring IGMP Filtering and Throttling Interface Settings



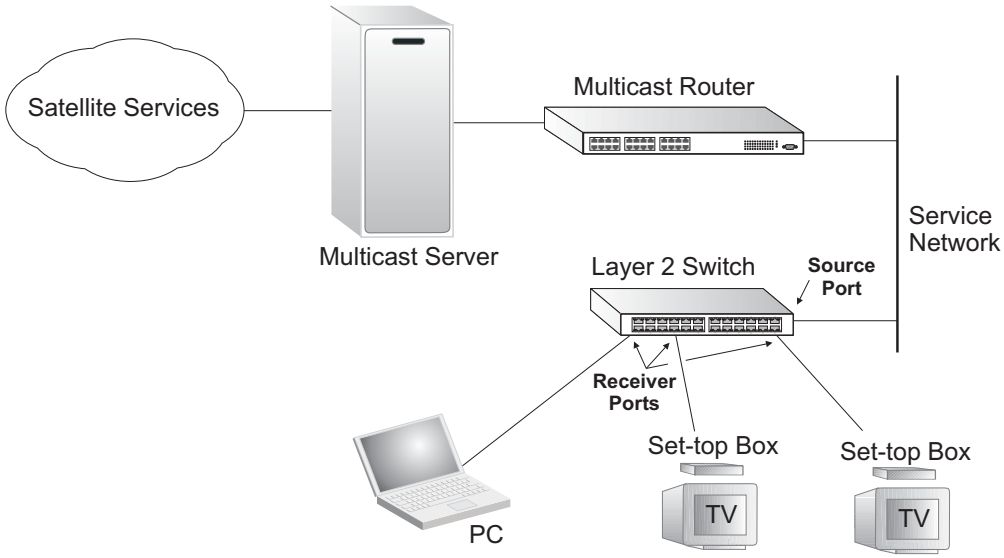
Port	Profile ID	Max Multicast Groups (1-1024)	Current Multicast Groups	Throttling Action Mode	Throttling Status
1	19	64	0	Deny	False
2	(none)	255	0	Deny	False
3	(none)	255	0	Deny	False
4	(none)	255	0	Deny	False
5	(none)	255	0	Deny	False

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).



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 454).
  2. Set the interfaces that will join the MVR as source ports or receiver ports (see "Configuring MVR Interface Status" on page 455).
  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 457).

- 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, select the VLAN that will serve as the sole channel for common multicast streams supported by the service provider, and assign the multicast group address for each of these services to the MVR VLAN.

CLI REFERENCES

- "Multicast VLAN Registration" on page 859

COMMAND USAGE

IGMP snooping and MVR share a maximum number of 256 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 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 152), 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 455).

- **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.

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

WEB INTERFACE

To configure global settings for MVR in the web interface:

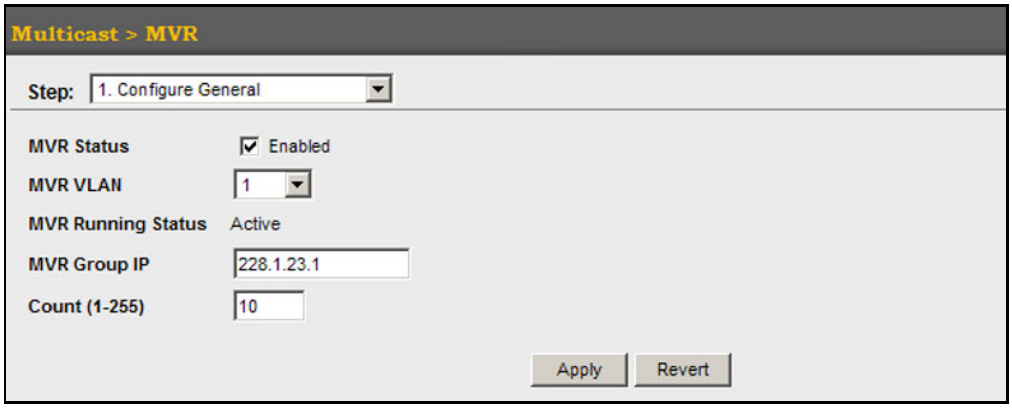
1. Click Multicast, MVR.

2. Select Configure General from the Action list.

3. Enable MVR globally on the switch, select the MVR VLAN, and add the multicast groups that will stream traffic to participating hosts.

4. Click Apply.

Figure 271: Configuring Global Settings for MVR



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 859

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 457).

  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 457).

  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:

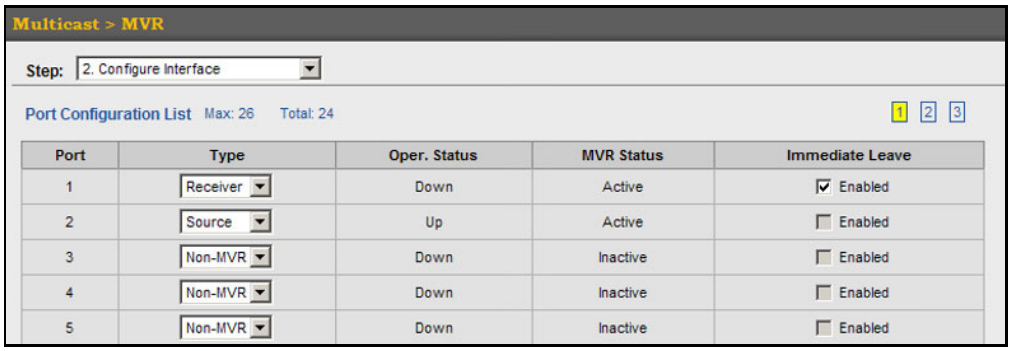
- **Port** – Port identifier.
- **Type** – The following interface types are supported:
  - **Source** – An uplink port that can send and receive multicast data for the groups assigned to the MVR VLAN. Note that the source port must be manually configured as a member of the MVR VLAN (see "Adding Static Members to VLANs" on page 152).
  - **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 457).
  - **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 in the web interface:

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 272: Configuring Interface Settings for MVR



Port	Type	Oper. Status	MVR Status	Immediate Leave
1	Receiver	Down	Active	☑ Enabled
2	Source	Up	Active	☐ 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 863

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 in the web interface:

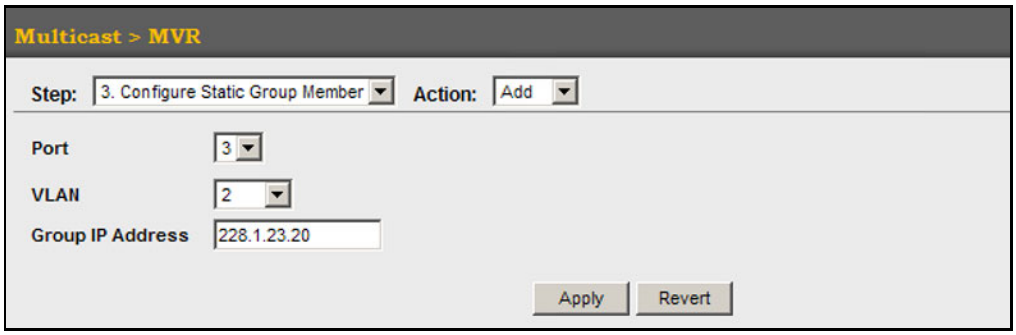
1. Click Multicast, MVR.
2. Select Configure Static Group Member from the Step list.

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 273: Assigning Static MVR Groups to a Port



To show the static MVR groups assigned to a port in the web interface:

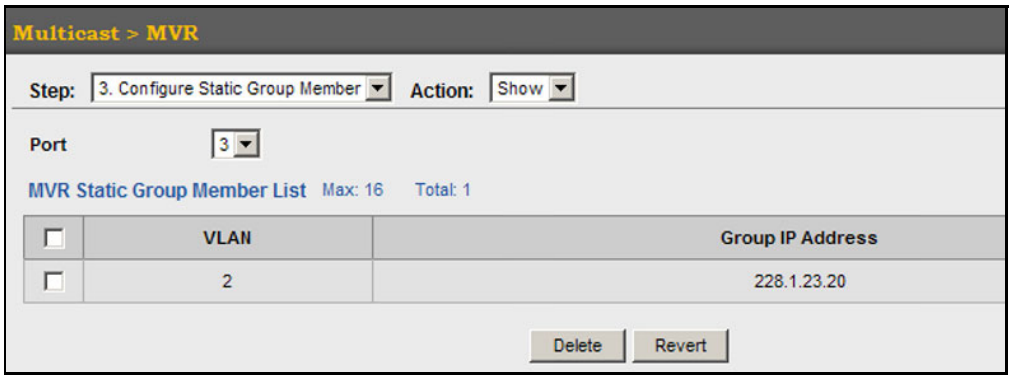
1. Click Multicast, MVR.

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 274: Showing the Static MVR Groups Assigned to a Port



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 473
- "System Management Commands" on page 481
- "SNMP Commands" on page 533
- "Remote Monitoring Commands" on page 553
- "Authentication Commands" on page 561
- "General Security Measures" on page 615
- "Access Control Lists" on page 661
- "Interface Commands" on page 677
- "Link Aggregation Commands" on page 695
- "Power over Ethernet Commands" on page 705
- "Port Mirroring Commands" on page 711
- "Rate Limit Commands" on page 721
- "Automatic Traffic Control Commands" on page 723
- "Address Table Commands" on page 737
- "Spanning Tree Commands" on page 741

- "VLAN Commands" on page 765
- "Class of Service Commands" on page 801
- "Quality of Service Commands" on page 815
- "Multicast Filtering Commands" on page 833
- "LLDP Commands" on page 867
- "Domain Name Service Commands" on page 885
- "DHCP Commands" on page 895
- "IP Interface Commands" on page 901

19 USING THE COMMAND LINE INTERFACE

iPECS ES-3000 Series

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 "ES-3026#" prompt and enters privileged access mode (i.e., Privileged Exec). But when the guest user name and password is entered, the CLI displays the "ES-3026>" prompt and enters normal access mode (i.e., Normal Exec).

NOTE: The displayed command prompt is based on the switch model (ES-3026, ES-3026P, ES3024G or ES-3024GP).

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 ES-3026 is opened.
  To end the CLI session, enter [Exit].
ES-3026#
```

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,

```
ES-3026(config)#interface vlan 1
ES-3026(config-if)#ip address 10.1.0.254 255.255.255.0
ES-3026(config-if)#exit
ES-3026(config)#ip default-gateway 10.1.0.254
ES-3026(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 ES-3026 is opened.
  To end the CLI session, enter [Exit].

Vty-0#
```

NOTE: You can open up to four sessions to the device via Telnet.

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:

```
ES-3026>enable
ES-3026#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:

```
ES-3026(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.

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 "**system ?**" displays a list of possible system commands:

```
ES-3026#show ?
  access-group          Access groups
  access-list           Access lists
  accounting            Uses an accounting list with this name
  arp                   Information of ARP cache
  authorization         Enables EXEC accounting
  auto-traffic-control  Auto traffic control information
  bridge-ext            Bridge extension information
  cable-diagnostics     Shows the information of cable diagnostics
  calendar              Date and time information
  class-map             Displays class maps
  cluster               Display cluster
  dns                   DNS information
  dot1q-tunnel          dot1q-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
  memory                Memory utilization
  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
  power                 Shows power
  power-save            Shows the power saving information
  protocol-vlan         Protocol-VLAN information
  public-key            Public key information
  qos                   Quality of Service
  queue                 Priority queue information
  radius-server         RADIUS server information
  reload                Shows the reload settings
  rmon                  Remote Monitoring Protocol
  rspan                 Display status of the current RSPAN configuration
  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
  time-range             Time range
  traffic-segmentation   Traffic segmentation information
  upgrade                Shows upgrade information
  users                  Information about users logged in
  version                System hardware and software versions
  vlan                   Shows virtual LAN settings
  voice                  Shows the voice VLAN information
  web-auth               Shows web authentication configuration
ES-3026#show
```

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

```
ES-3026#show interfaces ?
  counters       Interface counters information
  protocol-vlan  Protocol-VLAN information
  status         Shows interface status
  switchport     Shows interface switchport information
ES-3026#
```

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."

```
ES-3026#show s?
snmp            sntp            spanning-tree   ssh             startup-config
subnet-vlan     system
ES-3026#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 32: General Command Modes

Class	Mode	
Exec	Normal Privileged	
Configuration	Global*	Access Control List Class Map IGMP Profile DHCP Interface Line Multiple Spanning Tree Policy Map 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 "ES-3026>" 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 "ES-3026#" 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 ES-3026 is opened.
  To end the CLI session, enter [Exit].

ES-3026#
```

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

  CLI session with the ES-3026 is opened.
  To end the CLI session, enter [Exit].

ES-3026>enable
Password: [privileged level password]
ES-3026#
```

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.
- 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 "ES-3026(config)#" which gives you access privilege to all Global Configuration commands.

```
ES-3026#configure
ES-3026(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 33: Configuration Command Modes

Mode	Command	Prompt	Page
Line	line {console | vty}	ES-3026(config-line)	499
Access Control List	access-list ip standard access-list ip extended access-list mac	ES-3026(config-std-acl) ES-3026(config-ext-acl) ES-3026(config-mac-acl)	662 662 668
Class Map	class-map	ES-3026(config-cmap)	816
Interface	interface {ethernet *port* | port-channel *id*| vlan *id*}	ES-3026(config-if)	678
MSTP	spanning-tree mst-configuration	ES-3026(config-mstp)	747
Policy Map	policy-map	ES-3026(config-pmap)	819
Time Range	time-range	ES-3026(config-time-range)	524
VLAN	vlan database	ES-3026(config-vlan)	771

For example, you can use the following commands to enter interface configuration mode, and then return to Privileged Exec mode

```
ES-3026(config)#interface ethernet 1/5
.
.
.
ES-3026(config-if)#exit
ES-3026(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 34: 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 35: Command Group Index

Command Group	Description	Page
General	Basic commands for entering privileged access mode, restarting the system, or quitting the CLI	473
System Management	Display and setting of system information, basic modes of operation, maximum frame size, file management, console port and telnet settings, system logs, SMTP alerts, the system clock, and switch clustering	481
Simple Network Management Protocol	Activates authentication failure traps; configures community access strings, and trap receivers	533
Remote Monitoring	Supports statistics, history, alarm and event groups	553
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	561
General Security Measures	Segregates traffic for clients attached to common data ports; and prevents unauthorized access by configuring valid static or dynamic addresses, web authentication, MAC address authentication, filtering DHCP requests and replies, and discarding invalid ARP responses	615
Access Control List	Provides filtering for IPv4 frames (based on address, protocol, TCP/UDP port number or TCP control code), or non-IP frames (based on MAC address or Ethernet type)	661
Interface	Configures the connection parameters for all Ethernet ports, aggregated links, and VLANs	677
Link Aggregation	Statically groups multiple ports into a single logical trunk; configures Link Aggregation Control Protocol for port trunks	695
Power over Ethernet	Configures power output for connected devices	705
Mirror Port	Mirrors data to another port for analysis without affecting the data passing through or the performance of the monitored port	711
Rate Limit	Controls the maximum rate for traffic transmitted or received on a port	721
Automatic Traffic Control	Configures bounding thresholds for broadcast and multicast storms which can be used to trigger configured rate limits or to shut down a port	723
Address Table	Configures the address table for filtering specified addresses, displays current entries, clears the table, or sets the aging time	737
Spanning Tree	Configures Spanning Tree settings for the switch	741
VLANs	Configures VLAN settings, and defines port membership for VLAN groups; also enables or configures private VLANs, protocol VLANs, voice VLANs, and QinQ tunneling	765
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 DSCP	801

Table 35: Command Group Index (Continued)

Command Group	Description	Page
Quality of Service	Configures Differentiated Services	815
Multicast Filtering	Configures IGMP multicast filtering, query, profile, and proxy parameters; specifies ports attached to a multicast router; also configures multicast VLAN registration	833
Link Layer Discovery Protocol	Configures LLDP settings to enable information discovery about neighbor devices	867
Domain Name Service	Configures DNS services.	885
Dynamic Host Configuration Protocol	Configures DHCP client, relay and server functions	895
IP Interface	Configures IP address for the switch interfaces; also configures ARP parameters and static entries	901

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)
VC (VLAN Database Configuration)

20 GENERAL COMMANDS

These commands are used to control the command access mode, configuration mode, and other basic functions.

Table 36: 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

```
ES-3026(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 491).

EXAMPLE

This example shows how to reset the switch after 30 minutes:

```
ES-3026(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 466.

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

```
ES-3026>enable
Password: [privileged level password]
ES-3026#
```

RELATED COMMANDS

disable (478)
enable password (562)

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:

```
ES-3026#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:

```
ES-3026#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

ES-3026#
```

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**).

```
ES-3026#!2
ES-3026#config
ES-3026(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 466.

DEFAULT SETTING

None

COMMAND MODE

Privileged Exec

EXAMPLE

```
ES-3026#configure
ES-3026(config)#
```

RELATED COMMANDS

end (479)

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 466.

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

```
ES-3026#disable
ES-3026>
```

RELATED COMMANDS

enable (475)

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:

```
ES-3026#reload
Note: It takes around 100~120 seconds to finish system reboot.
Do you really want to reset the switch?
```

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

```
ES-3026#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.
ES-3026#
```

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:

```
ES-3026(config-if)#end
ES-3026#
```

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:

```
ES-3026(config)#exit
ES-3026#exit

Press ENTER to start session

User Access Verification

Username:
```

21 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 37: 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
Switch Clustering	Configures management of multiple devices via a single IP address

DEVICE DESIGNATION

This section describes commands used to configure information that uniquely identifies the switch.

Table 38: 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

```
ES-3026(config)#hostname RD#1
ES-3026(config)#
```

SYSTEM STATUS

This section describes commands used to display system information.

Table 39: System Status Commands

Command	Function	Mode
show access-list tcam-utilization	Shows utilization parameters for TCAM	PE
show memory	Shows memory utilization parameters	NE, PE
show process cpu	Shows CPU utilization parameters	NE, PE
show running-config	Displays the configuration data currently in use	PE
show startup-config	Displays the contents of the configuration file (stored in flash memory) that is used to start up the system	PE
show system	Displays system information	NE, PE
show 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 access-list tcam-utilization

This command shows utilization parameters for TCAM (Ternary Content Addressable Memory), including the number policy control entries in use, the number of free entries, and the overall percentage of TCAM in use.

COMMAND MODE

Privileged Exec

COMMAND USAGE

Policy control entires (PCEs) are used by various system functions which rely on rule-based searches, including Access Control Lists (ACLs), IP Source Guard filter rules, Quality of Service (QoS) processes, or traps.

For example, when binding an ACL to a port, each rule in an ACL will use two PCEs; and when setting an IP Source Guard filter rule for a port, the system will also use two PCEs.

EXAMPLE

```
ES-3026#show access-list tcam-utilization
  Total Policy Control Entries   : 512
  Free Policy Control Entries    : 352
  Entries Used by System         : 160
  Entries Used by User           : 0
  TCAM Utilization               : 31.25%
ES-3026#
```

show memory

This command shows memory utilization parameters.

COMMAND MODE

Normal Exec, Privileged Exec

COMMAND USAGE

This command shows the amount of memory currently free for use, and the amount of memory allocated to active processes.

EXAMPLE

```
ES-3026#show memory
 Status   Bytes
 ------ ----------
 Free     50917376
 Used     83300352
Total    134217728

ES-3026#
```

show process cpu

This command shows the CPU utilization parameters.

COMMAND MODE

Normal Exec, Privileged Exec

EXAMPLE

```
ES-3026#show process cpu
 CPU Utilization in the past 5 seconds : 3.98%
ES-3026#
```

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
  - SNTP server settings
  - SNMP community strings
  - Users (names, access levels, and encrypted passwords)
  - VLAN database (VLAN ID, name and state)
  - VLAN configuration settings for each interface
  - Multiple spanning tree instances (name and interfaces)
  - IP address configured for management VLAN
  - Layer 4 precedence settings
  - Spanning tree settings
  - Interface settings
  - Any configured settings for the console port and Telnet

EXAMPLE

```
ES-3026#show running-config
Building startup configuration. Please wait...
!<stackingDB>00</stackingDB>
!<stackingMac>01_00-e0-0c-00-00-fd_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

 qos map dscp-mutation 6 0 from 46
:

!
```

```
interface vlan 1
 ip address 192.168.1.10 255.255.255.0
!
 queue mode strict-wrr 0 0 0 1
!
line console
!
line vty
!
end
!
ES-3026#
```

RELATED COMMANDS

show startup-config (485)

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
  - SNMP trap authentication
  - RMON alarms settings
  - Users (names and access levels)
  - VLAN database (VLAN ID, name and state)
  - Multiple spanning tree instances (name and interfaces)
  - Interface settings and VLAN configuration settings for each interface
  - IP address for management VLAN
  - Any configured settings for the console port and Telnet

EXAMPLE

Refer to the example for the running configuration file.

RELATED COMMANDS

show running-config (484)

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 87.
- The POST results should all display “PASS.” If any POST test indicates “FAIL,” contact your distributor for assistance.

EXAMPLE

```
ES-3026#show system
System Description : ES-3026 Managed FE Switch
System OID String  : 1.3.6.1.4.1.572.17389.104
System Information
 System Up Time         : 0 days, 7 hours, 20 minutes, and 43.30 seconds
 System Name            :
 System Location        :
 System Contact         :
 MAC Address (Unit 1)   : 00-E0-0C-00-00-FD
 Web Server             : Enabled
 Web Server Port        : 80
 Web Secure Server      : Enabled
 Web Secure Server Port : 443
 Telnet Server          : Enabled
 Telnet Server Port     : 23
 Jumbo Frame            : Disabled

ES-3026#
```

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

```
ES-3026#show users
 User Name Accounts:
  User Name Privilege Public-Key
  --------- --------- ----------
      admin        15 None
      guest         0 None
      steve        15  RSA

 Online Users:
  Line        Username Idle time (h:m:s) Remote IP addr.
  ----------- -------- ----------------- ---------------
  0   console    admin           0:14:14
* 1     VTY 0    admin           0:00:00    192.168.1.19
  2     SSH 1    steve           0:00:06    192.168.1.19

 Web Online Users:
  Line        Remote IP Addr  User Name Idle time (h:m:s)
  ----------- --------------- --------- ------------------
  1      HTTP    192.168.1.19     admin            0:00:00

ES-3026#
```

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 88 for detailed information on the items displayed by this command.

EXAMPLE

```
ES-3026#show version
Unit 1
 Serial Number           : S123456
 Hardware Version        : R0A
 EPLD Version            : 0.00
 Number of Ports         : 26
 Main Power Status       : Up
 Redundant Power Status  : Not present
 Role                    : Master
 Loader Version          :  1.0.0.1
 Linux Kernel Version    : 2.6.22.18
 Boot ROM Version        : 0.0.0.1
 Operation Code Version  : IPECS_ES-3000.00

ES-3026#
```

FRAME SIZE

This section describes commands used to configure the Ethernet frame size on the switch.

Table 40: 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

```
ES-3026(config)#jumbo frame
ES-3026(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 41: 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
Automatic Code Upgrade Commands		
upgrade opcode auto	Automatically upgrades the current image when a new version is detected on the indicated server	GC
upgrade opcode path	Specifies an FTP/TFTP server and directory in which the new opcode is stored	GC

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

```
ES-3026(config)#boot system config: startup
ES-3026(config)#
```

RELATED COMMANDS

dir (494)
whichboot (495)

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 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 588.)

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 278. 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:

```
ES-3026#copy tftp file
TFTP server ip address: 10.1.0.19
Choose file type:
 1. config:  2. opcode: <1-2>: 2
Source file name: m360.bix
Destination file name: m360.bix
\Write to FLASH Programming.
-Write to FLASH finish.
Success.
ES-3026#
```

The following example shows how to upload the configuration settings to a file on the TFTP server:

```
ES-3026#copy file tftp
Choose file type:
 1. config:  2. opcode: <1-2>: 1
Source file name: startup
TFTP server ip address: 10.1.0.99
Destination file name: startup.01
TFTP completed.
Success.

ES-3026#
```

The following example shows how to copy the running configuration to a startup file.

```
ES-3026#copy running-config file
destination file name: startup
Write to FLASH Programming.
\Write to FLASH finish.
Success.

ES-3026#
```

The following example shows how to download a configuration file:

```
ES-3026#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.

ES-3026#
```

This example shows how to copy a secure-site certificate from an TFTP server. It then reboots the switch to activate the certificate:

```
ES-3026#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.
ES-3026#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.

```
ES-3026#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.

ES-3026#
```

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.

```
ES-3026#delete test2.cfg
ES-3026#
```

RELATED COMMANDS

dir (494)
delete public-key (593)

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 42: File Directory Information

Column Heading	Description
File Name	The name of the file.
File Type	File types: Boot-Rom, Operation Code, and Config file.
Startup	Shows if this file is used when the system is started.
Create Time	The date and time the file was created.
Size	The length of the file in bytes.

EXAMPLE

The following example shows how to display all file information:

```
ES-3026#dir
        File Name                  Type  Startup Modify Time         Size(bytes)
-------------------------- -------------- ------- ------------------- ---------
 Unit 1:
IPECS_ES-3000_Op_V0.0.1.0.bix    OpCode     N    2009-10-08 02:44:05   10735312
iPECS_ES-3000_Op_V0.0.1.1.bix    OpCode     Y    2009-10-11 11:29:21   11259468
Factory_Default_Config.cfg       Config     N    2009-10-08 02:23:36        455
startup1.cfg                     Config     Y    2009-09-28 21:07:09       8501
 ---------------------------------------------------------------------------
                         Free space for compressed user config files:    745472
ES-3026#
```

whichboot

This command displays which files were booted when the system powered up.

SYNTAX

whichboot

DEFAULT SETTING

None

COMMAND MODE

Privileged Exec

EXAMPLE

This example shows the information displayed by the **whichboot** command. See the table under the **dir** command for a description of the file information displayed by this command.

```
ES-3026#whichboot
        File Name                   Type  Startup Modify Time         Size(bytes)
------------------------------- ------- ------- ------------------- ----------
 Unit 1:
iPECS_ES-3000_Op_V0.0.1.1.bix    OpCode     Y    2009-10-11 11:29:21   11259468
startup1.cfg                     Config     Y    2009-09-28 21:07:09       8501

ES-3026#
```

upgrade opcode auto

This command automatically upgrades the current operational code when a new version is detected on the server indicated by the upgrade opcode path command. Use the **no** form of this command to restore the default setting.

SYNTAX

[**no**] **upgrade opcode auto**

DEFAULT SETTING

Disabled

COMMAND MODE

Global Configuration

COMMAND USAGE

- This command is used to enable or disable automatic upgrade of the operational code. When the switch starts up and automatic image upgrade is enabled by this command, the switch will follow these steps when it boots up:

  1. It will search for a new version of the image at the location specified by upgrade opcode path command (page 497). The name for the new image stored on the TFTP server must be IPECS_ES-3000_Op.bix. If the switch detects a code version newer than the one currently in use, it will download the new image. If two code images are already stored in the switch, the image not set to start up the system will be overwritten by the new version.

  2. After the image has been downloaded, the switch will send a trap message to log whether or not the upgrade operation was successful.

  3. It sets the new version as the startup image.

  4. It then restarts the system to start using the new image.

- Any changes made to the default setting can be displayed with the show running-config (page 484) or show startup-config (page 485) commands.

EXAMPLE

```
ES-3026(config)#upgrade opcode auto
ES-3026(config)#upgrade opcode path tftp://192.168.0.1/sm24/
ES-3026(config)#
```

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

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

upgrade opcode path

This command specifies an TFTP server and directory in which the new opcode is stored. Use the **no** form of this command to clear the current setting.

SYNTAX

upgrade opcode path *opcode-dir-url*

no upgrade opcode path

opcode-dir-url - The location of the new code.

DEFAULT SETTING

None

COMMAND MODE

Global Configuration

COMMAND USAGE

- This command is used in conjunction with the upgrade opcode auto command to facilitate automatic upgrade of new operational code stored at the location indicated by this command.

- The name for the new image stored on the TFTP server must be IPECS_ES-3000_Op.bix. However, note that file name is not to be included in this command.

- When specifying a TFTP server, the following syntax must be used, where *filedir* indicates the path to the directory containing the new image:

  `tftp://192.168.0.1[/filedir]/`

- When specifying an FTP server, the following syntax must be used, where *filedir* indicates the path to the directory containing the new image:

  `ftp://[username[:password@]]192.168.0.1[/filedir]/`

  If the user name is omitted, “Anonymous” will be used for the connection. If the password is omitted a null string (“”) will be used for the connection.

EXAMPLE

This shows how to specify a TFTP server where new code is stored.

```
ES-3026(config)#upgrade opcode path tftp://192.168.0.1/sm24/
ES-3026(config)#
```

This shows how to specify an FTP server where new code is stored.

```
ES-3026(config)#upgrade opcode path ftp://admin:billy@192.168.0.1/sm24/
ES-3026(config)#
```

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 43: 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:

```
ES-3026(config)#line console
ES-3026(config-line)#
```

RELATED COMMANDS
show line (508)
show users (486)

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:

```
ES-3026(config-line)#databits 7
ES-3026(config-line)#
```

RELATED COMMANDS
parity (502)

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:

```
ES-3026(config-line)#exec-timeout 120
ES-3026(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
```
ES-3026(config-line)#login local
ES-3026(config-line)#
```

RELATED COMMANDS
username (563)
password (503)

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:

```
ES-3026(config-line)#parity none
ES-3026(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

```
ES-3026(config-line)#password 0 secret
ES-3026(config-line)#
```

RELATED COMMANDS

login (501)
password-thresh (504)

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:

```
ES-3026(config-line)#password-thresh 5
ES-3026(config-line)#
```

RELATED COMMANDS

silent-time (505)

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:

```
ES-3026(config-line)#silent-time 60
ES-3026(config-line)#
```

RELATED COMMANDS

password-thresh (504)

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:

```
ES-3026(config-line)#speed 57600
ES-3026(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:

```
ES-3026(config-line)#stopbits 2
ES-3026(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:

```
ES-3026(config-line)#timeout login response 120
ES-3026(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

```
ES-3026#disconnect 1
ES-3026#
```

RELATED COMMANDS
show ssh (597)
show users (486)

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:

```
ES-3026#show line
 Console Configuration:
  Password Threshold : 3 times
  Inactive Timeout   : Disabled
  Login Timeout      : Disabled
  Silent Time        : Disabled
  Baud Rate          : Auto
  Data Bits          : 8
  Parity             : None
  Stop Bits          : 1

 VTY Configuration:
  Password Threshold : 3 times
  Inactive Timeout   : 600 sec.
  Login Timeout      : 300 sec.
ES-3026#
```

EVENT LOGGING

This section describes commands used to configure event logging on the switch.

Table 44: 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

Table 44: Event Logging Commands (Continued)

Command	Function	Mode
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

```
ES-3026(config)#logging facility 19
ES-3026(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 45: 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

```
ES-3026(config)#logging history ram 0
ES-3026(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 IP 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

```
ES-3026(config)#logging host 10.1.0.3
ES-3026(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

```
ES-3026(config)#logging on
ES-3026(config)#
```

RELATED COMMANDS

logging history (510)
logging trap (512)
clear log (512)

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 510. 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

```
ES-3026(config)#logging trap 4
ES-3026(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

```
ES-3026#clear log
ES-3026#
```

RELATED COMMANDS
show log (513)

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.

```
ES-3026#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
ES-3026#
```

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 518).

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).

```
ES-3026#show logging flash
Syslog logging:           Enabled
History logging in FLASH: level errors
ES-3026#show logging ram
Syslog logging:           Enabled
History logging in RAM: level debugging
ES-3026#
```

Table 46: 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.

```
ES-3026#show logging trap
Syslog logging: Enable
REMOTELOG Status: disable
REMOTELOG Facility Type: Local use 7
```

```
REMOTELOG Level Type:        Debugging messages
REMOTELOG server IP Address: 1.2.3.4
REMOTELOG server IP Address: 0.0.0.0
REMOTELOG server IP Address: 0.0.0.0
REMOTELOG server IP Address: 0.0.0.0
REMOTELOG server IP Address: 0.0.0.0
ES-3026#
```

Table 47: 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 (518)

SMTP ALERTS

These commands configure SMTP event handling, and forwarding of alert messages to the specified SMTP servers and email recipients.

Table 48: 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

```
ES-3026(config)#logging sendmail
ES-3026(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

```
ES-3026(config)#logging sendmail host 192.168.1.19
ES-3026(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 510). 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.

```
ES-3026(config)#logging sendmail level 3
ES-3026(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

```
ES-3026(config)#logging sendmail destination-email ted@this-company.com
ES-3026(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

```
ES-3026(config)#logging sendmail source-email bill@this-company.com
ES-3026(config)#
```

show logging sendmail

This command displays the settings for the SMTP event handler.

COMMAND MODE
Normal Exec, Privileged Exec

EXAMPLE

```
ES-3026#show logging sendmail
SMTP servers
---------------------------------------------
192.168.1.19
```

```
SMTP Minimum Severity Level: 7

SMTP destination email addresses
-----------------------------------------------
ted@this-company.com

SMTP Source Email Address: bill@this-company.com

SMTP Status: Enabled
ES-3026#
```

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 49: 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

```
ES-3026(config)#sntp server 10.1.0.19
ES-3026(config)#sntp poll 60
ES-3026(config)#sntp client
ES-3026(config)#end
ES-3026#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
ES-3026#
```

RELATED COMMANDS

sntp server (521)
sntp poll (520)
show sntp (521)

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

```
ES-3026(config)#sntp poll 60
ES-3026#
```

RELATED COMMANDS
sntp client (519)

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 - IP 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

```
ES-3026(config)#sntp server 10.1.0.19
ES-3026#
```

RELATED COMMANDS
sntp client (519)
sntp poll (520)
show sntp (521)

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

```
ES-3026#show sntp
Current Time   : Nov  5 18:51:22 2006
Poll Interval  : 16 seconds
Current Mode   : Unicast
SNTP Status    : Enabled
SNTP Server    : 137.92.140.80 0.0.0.0 0.0.0.0
Current Server : 137.92.140.80
ES-3026#
```

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

```
ES-3026(config)#clock timezone Japan hours 8 minute 0 after-UTC
ES-3026(config)#
```

RELATED COMMANDS

show sntp (521)

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.

```
ES-3026#calendar set 15:12:34 1 February 2002
ES-3026#
```

show calendar

This command displays the system clock.

DEFAULT SETTING

None

COMMAND MODE

Normal Exec, Privileged Exec

EXAMPLE

```
ES-3026#show calendar
 15:12:34 February 1 2002
ES-3026#
```

TIME RANGE

This section describes the commands used to sets a time range for use by other functions, such as Access Control Lists.

Table 50: Time Range Commands

Command	Function	Mode
time-range	Specifies the name of a time range, and enters time range configuration mode	GC
absolute	Sets the time range for the execution of a command	TR
periodic	Sets the time range for the periodic execution of a command	TR
show time-range	Shows configured time ranges.	PE

time-range

This command specifies the name of a time range, and enters time range configuration mode. Use the **no** form to remove a previously specified time range.

SYNTAX

[**no**] **time-range** *name*

name - Name of the time range. (Range: 1-30 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

```
ES-3026(config)#time-range r&d
ES-3026(config-time-range)#
```

RELATED COMMANDS

Access Control Lists (661)

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.

```
ES-3026(config)#time-range r&d
ES-3026(config-time-range)#absolute start 1 1 1 april 2009 end 2 1 1 april
  2009
ES-3026(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.

```
ES-3026(config)#time-range sales
ES-3026(config-time-range)#periodic daily 1 1 to 2 1
ES-3026(config-time-range)#
```

show time-range

This command shows configured time ranges.

SYNTAX

show time-range [*name*]

name - Name of the time range. (Range: 1-30 characters)

DEFAULT SETTING
None

COMMAND MODE
Privileged Exec

EXAMPLE

```
ES-3026#showtime-range r&d
 Time-range r&d:
   absolute start 01:01 01 April 2009
   periodic    Daily 01:01 to    Daily 02:01
   periodic    Daily 02:01 to    Daily 03:01
ES-3026#
```

SWITCH CLUSTERING

Switch Clustering is a method of grouping switches together to enable centralized management through a single unit. Switches that support clustering can be grouped together regardless of physical location or switch type, as long as they are connected to the same local network.

Table 51: Switch Cluster Commands

Command	Function	Mode
cluster	Configures clustering on the switch	GC
cluster commander	Configures the switch as a cluster Commander	GC
cluster ip-pool	Sets the cluster IP address pool for Members	GC
cluster member	Sets Candidate switches as cluster members	GC
rcommand	Provides configuration access to Member switches	GC
show cluster	Displays the switch clustering status	PE
show cluster members	Displays current cluster Members	PE
show cluster candidates	Displays current cluster Candidates in the network	PE

Using Switch Clustering

- A switch cluster has a primary unit called the “Commander” which is used to manage all other “Member” switches in the cluster. The management station can use either Telnet or the web interface to communicate directly with the Commander through its IP address, and then use the Commander to manage the Member switches through the cluster’s “internal” IP addresses.

- Clustered switches must be in the same Ethernet broadcast domain. In other words, clustering only functions for switches which can pass information between the Commander and potential Candidates or active Members through VLAN 4093.

- Once a switch has been configured to be a cluster Commander, it automatically discovers other cluster-enabled switches in the network. These “Candidate” switches only become cluster Members when manually selected by the administrator through the management station.

- The cluster VLAN 4093 is not configured by default. Before using clustering, take the following actions to set up this VLAN:

  1. Create VLAN 4093 (see "Editing VLAN Groups" on page 770).
  2. Add the participating ports to this VLAN (see "Configuring VLAN Interfaces" on page 772), and set them to hybrid mode, tagged members, PVID = 1, and acceptable frame type = all.

NOTE: Cluster Member switches can be managed either through a Telnet connection to the Commander, or through a web management connection

to the Commander. When using a console connection, from the Commander CLI prompt, use the rcommand to connect to the Member switch.

cluster

This command enables clustering on the switch. Use the **no** form to disable clustering.

SYNTAX

[**no**] **cluster**

DEFAULT SETTING

Disabled

COMMAND MODE

Global Configuration

COMMAND USAGE

- To create a switch cluster, first be sure that clustering is enabled on the switch (the default is enabled), then set the switch as a Cluster Commander. Set a Cluster IP Pool that does not conflict with any other IP subnets in the network. Cluster IP addresses are assigned to switches when they become Members and are used for communication between Member switches and the Commander.
- Switch clusters are limited to the same Ethernet broadcast domain.
- There can be up to 100 candidates and 36 member switches in one cluster.
- A switch can only be a Member of one cluster.
- Configured switch clusters are maintained across power resets and network changes.

EXAMPLE

```
ES-3026(config)#cluster
ES-3026(config)#
```

cluster commander

This command enables the switch as a cluster Commander. Use the **no** form to disable the switch as cluster Commander.

SYNTAX

[**no**] **cluster commander**

DEFAULT SETTING

Disabled

COMMAND MODE
Global Configuration

COMMAND USAGE
- Once a switch has been configured to be a cluster Commander, it automatically discovers other cluster-enabled switches in the network. These “Candidate” switches only become cluster Members when manually selected by the administrator through the management station.

- Cluster Member switches can be managed through a Telnet connection to the Commander. From the Commander CLI prompt, use the rcommand id command to connect to the Member switch.

EXAMPLE

```
ES-3026(config)#cluster commander
ES-3026(config)#
```

cluster ip-pool

This command sets the cluster IP address pool. Use the **no** form to reset to the default address.

SYNTAX

cluster ip-pool *ip-address*

no cluster ip-pool

ip-address - The base IP address for IP addresses assigned to cluster Members. The IP address must start 10.x.x.x.

DEFAULT SETTING
10.254.254.1

COMMAND MODE
Global Configuration

COMMAND USAGE
- An “internal” IP address pool is used to assign IP addresses to Member switches in the cluster. Internal cluster IP addresses are in the form 10.*x.x.member-ID*. Only the base IP address of the pool needs to be set since Member IDs can only be between 1 and 36.

- Set a Cluster IP Pool that does not conflict with addresses in the network IP subnet. Cluster IP addresses are assigned to switches when they become Members and are used for communication between Member switches and the Commander.

- You cannot change the cluster IP pool when the switch is currently in Commander mode. Commander mode must first be disabled.

EXAMPLE

```
ES-3026(config)#cluster ip-pool 10.2.3.4
ES-3026(config)#
```

cluster member

This command configures a Candidate switch as a cluster Member. Use the **no** form to remove a Member switch from the cluster.

SYNTAX

cluster member mac-address *mac-address* **id** *member-id*

no cluster member id *member-id*

mac-address - The MAC address of the Candidate switch.

member-id - The ID number to assign to the Member switch. (Range: 1-36)

DEFAULT SETTING

No Members

COMMAND MODE

Global Configuration

COMMAND USAGE

- The maximum number of cluster Members is 36.
- The maximum number of cluster Candidates is 100.

EXAMPLE

```
ES-3026(config)#cluster member mac-address 00-12-34-56-78-9a id 5
ES-3026(config)#
```

rcommand

This command provides access to a cluster Member CLI for configuration.

SYNTAX

rcommand id *member-id*

member-id - The ID number of the Member switch. (Range: 1-36)

COMMAND MODE

Privileged Exec

COMMAND USAGE

- This command only operates through a Telnet connection to the Commander switch. Managing cluster Members using the local console CLI on the Commander is not supported.

- There is no need to enter the username and password for access to the Member switch CLI.

EXAMPLE

```
ES-3026#rcommand id 1

      CLI session with the ES-3024GP is opened.
      To end the CLI session, enter [Exit].

Vty-0#
```

show cluster

This command shows the switch clustering configuration.

COMMAND MODE

Privileged Exec

EXAMPLE

```
ES-3026#show cluster
Role                  : commander
Interval Heartbeat    : 30
Heartbeat Loss Count  : 3 seconds
Number of Members     : 1
Number of Candidates  : 2
ES-3026#
```

show cluster members

This command shows the current switch cluster members.

COMMAND MODE

Privileged Exec

EXAMPLE

```
ES-3026#show cluster members
Cluster Members:
ID          : 1
Role        : Active member
IP Address  : 10.254.254.2
MAC Address : 00-E0-0C-00-00-FE
Description : ES-3024GP Managed GE POE Switch
ES-3026#
```

show cluster candidates

This command shows the discovered Candidate switches in the network.

COMMAND MODE

Privileged Exec

EXAMPLE

```
ES-3026#show cluster candidates
Cluster Candidates:
Role            MAC Address       Description
--------------- ----------------- ----------------------------------------
Active member   00-E0-0C-00-00-FE ES-3024GP Managed GE POE Switch
CANDIDATE       00-12-CF-0B-47-A0 ES-3024GP Managed GE POE Switch
ES-3026#
```

22 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 52: 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 52: 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
ATC Trap Commands		
snmp-server enable port-traps atc broadcast-alarm-clear	Sends a trap when broadcast traffic falls beneath the lower threshold after a storm control response has been triggered	IC (Port)
snmp-server enable port-traps atc broadcast-alarm-fire	Sends a trap when broadcast traffic exceeds the upper threshold for automatic storm control	IC (Port)
snmp-server enable port-traps atc broadcast-control-apply	Sends a trap when broadcast traffic exceeds the upper threshold for automatic storm control and the apply timer expires	IC (Port)
snmp-server enable port-traps atc broadcast-control-release	Sends a trap when broadcast traffic falls beneath the lower threshold after a storm control response has been triggered and the release timer expires	IC (Port)
snmp-server enable port-traps atc multicast-alarm-clear	Sends a trap when multicast traffic falls beneath the lower threshold after a storm control response has been triggered	IC (Port)
snmp-server enable port-traps atc multicast-alarm-fire	Sends a trap when multicast traffic exceeds the upper threshold for automatic storm control	IC (Port)
snmp-server enable port-traps atc multicast-control-apply	Sends a trap when multicast traffic exceeds the upper threshold for automatic storm control and the apply timer expires	IC (Port)
snmp-server enable port-traps atc multicast-control-release	Sends a trap when multicast traffic falls beneath the lower threshold after a storm control response has been triggered and the release timer expires	IC (Port)

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

```
ES-3026(config)#snmp-server
ES-3026(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

```
ES-3026(config)#snmp-server community alpha rw
ES-3026(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

```
ES-3026(config)#snmp-server contact Paul
ES-3026(config)#
```

RELATED COMMANDS
snmp-server location (536)

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

```
ES-3026(config)#snmp-server location WC-19
ES-3026(config)#
```

RELATED COMMANDS
snmp-server contact (535)

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

```
ES-3026#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
ES-3026#
```

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

```
ES-3026(config)#snmp-server enable traps link-up-down
ES-3026(config)#
```

RELATED COMMANDS

snmp-server host (538)

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 360 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 534).
2. Create a view with the required notification messages (page 544).
3. Create a group that includes the required notify view (page 542).
4. Allow the switch to send SNMP traps; i.e., notifications (page 537).
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 534).
2. Create a local SNMPv3 user to use in the message exchange process (page 543).
3. Create a view with the required notification messages (page 544).
4. Create a group that includes the required notify view (page 542).
5. Allow the switch to send SNMP traps; i.e., notifications (page 537).
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

```
ES-3026(config)#snmp-server host 10.1.19.23 batman
ES-3026(config)#
```

RELATED COMMANDS

snmp-server enable traps (537)

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 543).

EXAMPLE

```
ES-3026(config)#snmp-server engine-id local 1234567890
ES-3026(config)#snmp-server engineID remote 9876543210 192.168.1.19
ES-3026(config)#
```

RELATED COMMANDS

snmp-server host (538)

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 360 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[6] (read only), private[7] (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 27, "Supported Notification Messages," on page 369. 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.

6. No view is defined.
7. Maps to the defaultview.

EXAMPLE

```
ES-3026(config)#snmp-server group r&d v3 auth write daily
ES-3026(config)#
```

snmp-server user

This command adds a user to an SNMP group, restricting the user to a specific SNMP Read, Write, or Notify View. Use the **no** form to remove a user from an SNMP group.

SYNTAX

snmp-server user *username groupname* [**remote** *ip-address*] {**v1** | **v2c** | **v3** [**encrypted**] [**auth** {**md5** | **sha**} *auth-password* [**priv des56** *priv-password*]]

no snmp-server user *username* {**v1** | **v2c** | **v3** | **remote**}

username - Name of user connecting to the SNMP agent. (Range: 1-32 characters)

groupname - Name of an SNMP group to which the user is assigned. (Range: 1-32 characters)

remote - Specifies an SNMP engine on a remote device.

ip-address - The Internet address of the remote device.

v1 | **v2c** | **v3** - Use SNMP version 1, 2c or 3.

encrypted - Accepts the password as encrypted input.

auth - Uses SNMPv3 with authentication.

md5 | **sha** - Uses MD5 or SHA authentication.

auth-password - Authentication password. Enter as plain text if the **encrypted** option is not used. Otherwise, enter an encrypted password. (A minimum of eight characters is required.)

priv des56 - Uses SNMPv3 with privacy with DES56 encryption.

priv-password - Privacy password. Enter as plain text if the **encrypted** option is not used. Otherwise, enter an encrypted password.

DEFAULT SETTING

None

COMMAND MODE

Global Configuration

COMMAND USAGE

- Local users (i.e., the command does not specify a remote engine identifier) must be configured to authorize management access for SNMPv3 clients, or to identify the source of SNMPv3 trap messages sent from the local switch.

- Remote users (i.e., the command specifies a remote engine identifier) must be configured to identify the source of SNMPv3 inform messages sent from the local switch.
- The SNMP engine ID is used to compute the authentication/privacy digests from the password. You should therefore configure the engine ID with the snmp-server engine-id command before using this configuration command.
- Before you configure a remote user, use the snmp-server engine-id command to specify the engine ID for the remote device where the user resides. Then use the **snmp-server user** command to specify the user and the IP address for the remote device where the user resides. The remote agent's SNMP engine ID is used to compute authentication/privacy digests from the user's password. If the remote engine ID is not first configured, the **snmp-server user** command specifying a remote user will fail.
- SNMP passwords are localized using the engine ID of the authoritative agent. For informs, the authoritative SNMP agent is the remote agent. You therefore need to configure the remote agent's SNMP engine ID before you can send proxy requests or informs to it.

EXAMPLE

```
ES-3026(config)#snmp-server user steve group r&d v3 auth md5 greenpeace priv
  des56 einstien
ES-3026(config)#snmp-server user mark group r&d remote 192.168.1.19 v3 auth
  md5 greenpeace priv des56 einstien
ES-3026(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.

```
ES-3026(config)#snmp-server view mib-2 1.3.6.1.2.1 included
ES-3026(config)#
```

This view includes the MIB-2 interfaces table, ifDescr. The wild card is used to select all the index values in this table.

```
ES-3026(config)#snmp-server view ifEntry.2 1.3.6.1.2.1.2.2.1.*.2 included
ES-3026(config)#
```

This view includes the MIB-2 interfaces table, and the mask selects all index entries.

```
ES-3026(config)#snmp-server view ifEntry.a 1.3.6.1.2.1.2.2.1.1.* included
ES-3026(config)#
```

show snmp engine-id

This command shows the SNMP engine ID.

COMMAND MODE

Privileged Exec

EXAMPLE

This example shows the default engine ID.

```
ES-3026#show snmp engine-id
Local SNMP EngineID: 8000002a8000000000e8666672
Local SNMP EngineBoots: 1

Remote SNMP EngineID                                        IP address
80000000030004e2b316c54321                                  192.168.1.19
ES-3026#
```

Table 53: show snmp engine-id - display description

Field	Description
Local SNMP engineID	String identifying the engine ID.
Local SNMP engineBoots	The number of times that the engine has (re-)initialized since the snmp EngineID was last configured.

Table 53: show snmp engine-id - display description (Continued)

Field	Description
Remote SNMP engineID	String identifying an engine ID on a remote device.
IP address	IP address of the device containing the corresponding remote SNMP engine.

show snmp group

Four default groups are provided – SNMPv1 read-only access and read/write access, and SNMPv2c read-only access and read/write access.

COMMAND MODE

Privileged Exec

EXAMPLE

```
ES-3026#show snmp group
Group Name: r&d
Security Model: v3
Read View: defaultview
Write View: daily
Notify View: none
Storage Type: permanent
Row Status: active

Group Name: public
Security Model: v1
Read View: defaultview
Write View: none
Notify View: none
Storage Type: volatile
Row Status: active

Group Name: public
Security Model: v2c
Read View: defaultview
Write View: none
Notify View: none
Storage Type: volatile
Row Status: active

Group Name: private
Security Model: v1
Read View: defaultview
Write View: defaultview
Notify View: none
Storage Type: volatile
Row Status: active

Group Name: private
Security Model: v2c
Read View: defaultview
Write View: defaultview
Notify View: none
Storage Type: volatile
Row Status: active

ES-3026#
```

Table 54: show snmp group - display description

Field	Description
groupname	Name of an SNMP group.
security model	The SNMP version.
readview	The associated read view.
writeview	The associated write view.
notifyview	The associated notify view.
storage-type	The storage type for this entry.
Row Status	The row status of this entry.

show snmp user

This command shows information on SNMP users.

COMMAND MODE

Privileged Exec

EXAMPLE

```
ES-3026#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

ES-3026#
```

Table 55: 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

```
ES-3026#show snmp view
View Name: mib-2
Subtree OID: 1.2.2.3.6.2.1
View Type: included
Storage Type: permanent
Row Status: active

View Name: defaultview
Subtree OID: 1
View Type: included
Storage Type: volatile
Row Status: active

ES-3026#
```

Table 56: 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 logs A1 and A2.

```
ES-3026(config)#nlm A1
ES-3026(config)#nlm A2
ES-3026(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.

```
ES-3026(config)#snmp-server host 10.1.19.23 batman
ES-3026(config)#snmp-server notify-filter A1 remote 10.1.19.23
ES-3026#
```

show nlm oper-status

This command shows the operational status of configured notification logs.

COMMAND MODE

Privileged Exec

EXAMPLE

```
ES-3026#sh nlm oper-status
Filter Name: A1
Oper-Status: Operational
Filter Name: A2
Oper-Status: Operational
ES-3026#
```

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. Note that the last entry is a default filter created when a trap host is initially created.

```
ES-3026#show snmp notify-filter
Filter profile name            IP address
----------------------------  ----------------
A1                             10.1.19.23
A2                             10.1.19.22
traphost.1.1.1.1.private       1.1.1.1
ES-3026#
```

23 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 57: 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

```
ES-3026(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
ES-3026(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 508).

trap – Sends a trap message to all configured trap managers (see "snmp-server host" on page 538).

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 535) 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

```
ES-3026(config)#rmon event 2 log description urgent owner mike
ES-3026(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

```
ES-3026(config)#interface  ethenet 1/1
ES-3026(config-if)#rmon collection history 21 buckets 24 interval 60 owner
  mike
ES-3026(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

```
ES-3026(config)#interface ethernet 1/1
ES-3026(config-if)#rmon collection stats 1 owner mike
ES-3026(config-if)#
```

show rmon alarm

This command shows the settings for all configured alarms.

COMMAND MODE

Privileged Exec

EXAMPLE

```
ES-3026#show rmon alarm
alarm Index = 1
        alarm Interval = 30
        alarm Type is Delta
        alarm Value  = 0
        alarm Rising Threshold = 892800
        alarm Rising Event = 0
        alarm Falling Threshold = 446400
        alarm Falling Event = 0
        alarm Owner is RMON_SNMP
⋮
```

show rmon event

This command shows the settings for all configured events.

COMMAND MODE

Privileged Exec

EXAMPLE

```
ES-3026#show rmon event
 event Index = 1
       Description: RMON_TRAP_LOG
       Event type: log & trap
       Event community name is public
       Last Time Sent = 0
       Owner is RMON_SNMP

 ES-3026#
```

show rmon history

This command shows the sampling parameters configured for each entry in the history group.

COMMAND MODE

Privileged Exec

EXAMPLE

```
ES-3026#show rmon history
 history index = 1
        data source ifindex = 1
        buckets requested = 8
        buckets granted = 8
        Interval = 1800
        Owner RMON_SNMP

 history index = 2
        data source ifindex = 1
```

```
        buckets requested = 8
        buckets granted = 8
        Interval = 30
        Owner RMON_SNMP
⋮
```

show rmon statistics

This command shows the information collected for all configured entries in the statistics group.

COMMAND MODE

Privileged Exec

EXAMPLE

```
ES-3026#show rmon statistics
    rmon collection index 1
    stats->ifindex = 1
    input packets 00, bytes 00, dropped 00, multicast packets 00
    output packets 00, bytes 05, multicast packets 00 broadcast packets 00
    rmon collection index 2
    stats->ifindex = 2
    input packets 00, bytes 00, dropped 00, multicast packets 00
    output packets 00, bytes 05, multicast packets 00 broadcast packets 00
⋮
```

24 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[8] to the data ports.

Table 58: 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 499), user authentication via a remote authentication server (page 561), and host access authentication for specific ports (page 597).

Table 59: 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

8. For other methods of controlling client access, see "General Security Measures" on page 615.

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

```
ES-3026(config)#enable password level 15 0 admin
ES-3026(config)#
```

RELATED COMMANDS

enable (475)
authentication enable (564)

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 60: 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.

```
ES-3026(config)#username bob access-level 15
ES-3026(config)#username bob password 0 smith
ES-3026(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 61: 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

```
ES-3026(config)#authentication enable radius
ES-3026(config)#
```

RELATED COMMANDS

enable password - sets the password for changing command modes (562)

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

```
ES-3026(config)#authentication login radius
ES-3026(config)#
```

RELATED COMMANDS

username - for setting the local user names and passwords (563)

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 62: 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

```
ES-3026(config)#radius-server acct-port 181
ES-3026(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

```
ES-3026(config)#radius-server auth-port 181
ES-3026(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

```
ES-3026(config)#radius-server 1 host 192.168.1.20 port 181 timeout 10
  retransmit 5 key green
ES-3026(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

```
ES-3026(config)#radius-server key green
ES-3026(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

```
ES-3026(config)#radius-server retransmit 5
ES-3026(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

```
ES-3026(config)#radius-server timeout 10
ES-3026(config)#
```

show radius-server

This command displays the current settings for the RADIUS server.

DEFAULT SETTING

None

COMMAND MODE

Privileged Exec

EXAMPLE

```
ES-3026#show radius-server

Remote RADIUS Server Configuration:

Global Settings:
 Auth-port            : 1812
 Acct-port            : 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

ES-3026#
```

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 63: 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

```
ES-3026(config)#tacacs-server host 192.168.1.25
ES-3026(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

```
ES-3026(config)#tacacs-server host 192.168.1.25
ES-3026(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

```
ES-3026(config)#tacacs-server key green
ES-3026(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

```
ES-3026(config)#tacacs-server port 181
ES-3026(config)#
```

show tacacs-server

This command displays the current settings for the TACACS+ server.

DEFAULT SETTING

None

COMMAND MODE

Privileged Exec

EXAMPLE

```
ES-3026#show tacacs-server

Remote TACACS+ server configuration:

Global settings:
 Communication key with TACACS+ server:
 Server port number:                    49

Server 1:
 Server IP address: 10.11.12.13
 Communication key with TACACS+ server:
 Server port number: 49

ES-3026#
```

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 64: 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 64: 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

```
ES-3026(config)#aaa accounting commands 15 default start-stop group tacacs+
ES-3026(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

```
ES-3026(config)#aaa accounting dot1x default start-stop group radius
ES-3026(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

```
ES-3026(config)#aaa accounting exec default start-stop group tacacs+
ES-3026(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

```
ES-3026(config)#aaa accounting update periodic 30
ES-3026(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
```
ES-3026(config)#aaa authorization exec default group tacacs+
ES-3026(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
```
ES-3026(config)#aaa group server radius tps
ES-3026(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

```
ES-3026(config)#aaa group server radius tps
ES-3026(config-sg-radius)#server 10.2.68.120
ES-3026(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

```
ES-3026(config)#interface ethernet 1/2
ES-3026(config-if)#accounting dot1x tps
ES-3026(config-if)#
```

accounting exec

This command applies an accounting method to local console or Telnet 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

```
ES-3026(config)#line console
ES-3026(config-line)#accounting exec tps
ES-3026(config-line)#exit
ES-3026(config)#line vty
ES-3026(config-line)#accounting exec default
ES-3026(config-line)#
```

authorization exec

This command applies an authorization method to local console or Telnet 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

```
ES-3026(config)#line console
ES-3026(config-line)#authorization exec tps
ES-3026(config-line)#exit
ES-3026(config)#line vty
ES-3026(config-line)#authorization exec default
ES-3026(config-line)#
```

show accounting

This command displays the current accounting settings per function and per port.

SYNTAX

show accounting [**commands** [*level*]] | [[**dot1x** [**statistics** [**username** *user-name* | **interface** *interface*]] | **exec** [**statistics**] | **statistics**]

commands - Displays command accounting information.

level - Displays command accounting information for a specifiable command level.

dot1x - Displays dot1x accounting information.

exec - Displays Exec accounting records.

statistics - Displays accounting records.

user-name - Displays accounting records for a specifiable username.

interface

ethernet *unit/port*

unit - Unit identifier. (Range: 1)

port - Port number. (ES-3026/P: 1-26, ES-3024G/P: 1-24)

DEFAULT SETTING
None

COMMAND MODE
Privileged Exec

EXAMPLE

```
ES-3026#show accounting
Accounting type: dot1x
  Method list: default
  Group list: radius
  Interface:
```

```
    Method list: tps
    Group list: radius
    Interface: eth 1/2

  Accounting type: Exec
    Method list: default
    Group list: radius
    Interface: vty

  ES-3026#
```

WEB SERVER

This section describes commands used to configure web browser management access to the switch.

Table 65: 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

```
ES-3026(config)#ip http port 769
ES-3026(config)#
```

RELATED COMMANDS
ip http server (583)
show system (486)

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

```
ES-3026(config)#ip http server
ES-3026(config)#
```

RELATED COMMANDS
ip http port (582)
show system (486)

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 66: 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 278. Also refer to the copy tftp https-certificate command.

EXAMPLE

```
ES-3026(config)#ip http secure-server
ES-3026(config)#
```

RELATED COMMANDS

ip http secure-port (585)
copy tftp https-certificate (491)
show system (486)

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

```
ES-3026(config)#ip http secure-port 1000
ES-3026(config)#
```

RELATED COMMANDS

ip http secure-server (583)
show system (486)

TELNET SERVER

This section describes commands used to configure Telnet management access to the switch.

Table 67: 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

```
ES-3026(config)#ip telnet max-sessions 1
ES-3026(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

```
ES-3026(config)#ip telnet port 123
ES-3026(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

```
ES-3026(config)#ip telnet server
ES-3026(config)#
```

show ip telnet

This command displays the configuration settings for the Telnet server.

COMMAND MODE
Normal Exec, Privileged Exec

EXAMPLE

```
ES-3026#show ip telnet
IP Telnet Configuration:

Telnet Status: Enabled
Telnet Service Port: 23
Telnet Max Session: 4
ES-3026#
```

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 68: 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
   156849954018676692593339467750546173253136748908365472541502024559319986854435836165199992332978176606583095610825913212890233765468017262725714134287629413011961955667825956641048695742788814620651941746772984865468615717739390164779355942303577413098022737087794545240839717526463580581767167095748047761 17

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
   134108168560989392104094492015542534763164192187295892114317388005553616163105177594083868631109291232226828519254374603100937187721199696317813662774141689851320491172048303392543241016379975923714490119380060902539484084827178194372288402533115952134861022902978982721353267131629432532818915045306393916643 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.

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

```
ES-3026(config)#ip ssh authentication-retires 2
ES-3026(config)#
```

RELATED COMMANDS

show ip ssh (595)

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

```
ES-3026#ip ssh crypto host-key generate dsa
ES-3026#configure
ES-3026(config)#ip ssh server
ES-3026(config)#
```

RELATED COMMANDS

ip ssh crypto host-key generate (593)
show ssh (597)

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

```
ES-3026(config)#ip ssh server-key size 512
ES-3026(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

```
ES-3026(config)#ip ssh timeout 60
ES-3026(config)#
```

RELATED COMMANDS
exec-timeout (501)
show ip ssh (595)

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

```
ES-3026#delete public-key admin dsa
ES-3026#
```

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
```
ES-3026#ip ssh crypto host-key generate dsa
ES-3026#
```

RELATED COMMANDS
ip ssh crypto zeroize (594)
ip ssh save host-key (595)

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

```
ES-3026#ip ssh crypto zeroize dsa
ES-3026#
```

RELATED COMMANDS

ip ssh crypto host-key generate (593)
ip ssh save host-key (595)
no ip ssh server (591)

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

```
ES-3026#ip ssh save host-key dsa
ES-3026#
```

RELATED COMMANDS

ip ssh crypto host-key generate (593)

show ip ssh

This command displays the connection settings used when authenticating client access to the SSH server.

COMMAND MODE

Privileged Exec

EXAMPLE

```
ES-3026#show ip ssh
SSH Enabled - Version 2.0
Negotiation Timeout : 120 seconds; Authentication Retries : 3
Server Key Size     : 768 bits
ES-3026#
```

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

```
ES-3026#show public-key host
Host:
RSA:
1024 65537 132369406582547640313827955265363759278355253279726295211302 41
  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
ES-3026#
```

show ssh

This command displays the current SSH server connections.

COMMAND MODE

Privileged Exec

EXAMPLE

```
ES-3026#show ssh
Connection Version State                Username Encryption
  0          2.0   Session-Started      admin    ctos aes128-cbc-hmac-md5
                                                 stoc aes128-cbc-hmac-md5
ES-3026#
```

Table 69: 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 70: 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 70: 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
Supplicant Commands		
dot1x identity profile	Configures dot1x supplicant user name and password	GC
dot1x max-start	Sets the maximum number of times that a port supplicant will send an EAP start frame to the client	IC
dot1x pae supplicant	Enables dot1x supplicant mode on an interface	IC
dot1x timeout auth-period	Sets the time that a supplicant port waits for a response from the authenticator	IC
dot1x timeout held-period	Sets the time a port waits after the maximum start count has been exceeded before attempting to find another authenticator	IC
dot1x timeout start-period	Sets the time that a supplicant port waits before resending an EAPOL start frame to the authenticator	IC
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

```
ES-3026(config)#dot1x default
ES-3026(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.

```
ES-3026(config)#dot1x eapol-pass-through
ES-3026(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

```
ES-3026(config)#dot1x system-auth-control
ES-3026(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

```
ES-3026(config)#interface eth 1/2
ES-3026(config-if)#dot1x intrusion-action guest-vlan
ES-3026(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

```
ES-3026(config)#interface eth 1/2
ES-3026(config-if)#dot1x max-req 2
ES-3026(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

```
ES-3026(config)#interface eth 1/2
ES-3026(config-if)#dot1x operation-mode multi-host max-count 10
ES-3026(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

```
ES-3026(config)#interface eth 1/2
ES-3026(config-if)#dot1x port-control auto
ES-3026(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

```
ES-3026(config)#interface eth 1/2
ES-3026(config-if)#dot1x re-authentication
ES-3026(config-if)#
```

RELATED COMMANDS

dot1x timeout re-authperiod (603)

dot1x timeout quiet-period

This command sets the time that a switch port waits after the maximum request count (see page 600) 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

```
ES-3026(config)#interface eth 1/2
ES-3026(config-if)#dot1x timeout quiet-period 350
ES-3026(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

```
ES-3026(config)#interface eth 1/2
ES-3026(config-if)#dot1x timeout re-authperiod 300
ES-3026(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

```
ES-3026(config)#interface eth 1/2
ES-3026(config-if)#dot1x timeout supp-timeout 300
ES-3026(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

```
ES-3026(config)#interface eth 1/2
ES-3026(config-if)#dot1x timeout tx-period 300
ES-3026(config-if)#
```

dot1x re-authenticate

This command forces re-authentication on all ports or a specific interface.

SYNTAX

dot1x re-authenticate [*interface*]

interface

ethernet *unit*/*port*

unit - Unit identifier. (Range: 1)

port - Port number. (ES-3026/P: 1-26, ES-3024G/P: 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

```
ES-3026#dot1x re-authenticate
ES-3026#
```

dot1x identity profile

This command sets the dot1x supplicant user name and password. Use the **no** form to delete the identity settings.

SYNTAX

dot1x identity profile {**username** *username* | **password** *password*}

no dot1x identity profile {**username** | **password**}

username - Specifies the supplicant user name.
(Range: 1-8 characters)

password - Specifies the supplicant password.
(Range: 1-8 characters)

DEFAULT

No user name or password

COMMAND MODE

Global Configuration

COMMAND USAGE

The global supplicant user name and password are used to identify this switch as a supplicant when responding to an MD5 challenge from the authenticator. These parameters must be set when this switch passes client authentication requests to another authenticator on the network (see the dot1x pae supplicant command on page 607).

EXAMPLE

```
ES-3026(config)#dot1x identity profile username steve
ES-3026(config)#dot1x identity profile password excess
ES-3026(config)#
```

dot1x max-start

This command sets the maximum number of times that a port supplicant will send an EAP start frame to the client before assuming that the client is 802.1X unaware. Use the **no** form to restore the default value.

SYNTAX

dot1x max-start *count*

no dot1x max-start

count - Specifies the maximum number of EAP start frames.
(Range: 1-65535)

DEFAULT

3

COMMAND MODE

Interface Configuration

EXAMPLE

```
ES-3026(config)#interface eth 1/2
ES-3026(config-if)#dot1x max-start 10
ES-3026(config-if)#
```

dot1x pae supplicant

This command enables dot1x supplicant mode on a port. Use the **no** form to disable dot1x supplicant mode on a port.

SYNTAX

[**no**] **dot1x pae supplicant**

DEFAULT

Disabled

COMMAND MODE

Interface Configuration

COMMAND USAGE

- When devices attached to a port must submit requests to another authenticator on the network, configure the identity profile parameters (see dot1x identity profile command on page 606) which identify this switch as a supplicant, and enable dot1x supplicant mode for those ports which must authenticate clients through a remote authenticator using this command. In this mode the port will not respond to dot1x messages meant for an authenticator.

- This switch can be configured to serve as the authenticator on selected ports by setting the control mode to “auto” (see the dot1x port-control command on page 602), and as a supplicant on other ports by the setting the control mode to “force-authorized” and enabling dot1x supplicant mode with this command.

- A port cannot be configured as a dot1x supplicant if it is a member of a trunk or LACP is enabled on the port.

EXAMPLE

```
Console(config)#interface ethernet 1/2
Console(config-if)#dot1x pae supplicant
Console(config-if)#
```

dot1x timeout auth-period

This command sets the time that a supplicant port waits for a response from the authenticator. Use the **no** form to resstore the default setting.

SYNTAX

dot1x timeout auth-period *seconds*

no dot1x timeout auth-period

seconds - The number of seconds. (Range: 1-65535)

DEFAULT

30 seconds

COMMAND MODE

Interface Configuration

COMMAND USAGE

This command sets the time that the supplicant waits for a response from the authenticator for packets other than EAPOL-Start.

EXAMPLE

```
ES-3026(config)#interface eth 1/2
ES-3026(config-if)#dot1x timeout auth-period 60
ES-3026(config-if)#
```

dot1x timeout held-period

This command sets the time that a supplicant port waits before resending its credentials to find a new an authenticator. Use the **no** form to reset the default.

SYNTAX

dot1x timeout held-period *seconds*

no dot1x timeout held-period

seconds - The number of seconds. (Range: 1-65535)

DEFAULT

60 seconds

COMMAND MODE

Interface Configuration

EXAMPLE

```
ES-3026(config)#interface eth 1/2
ES-3026(config-if)#dot1x timeout held-period 120
ES-3026(config-if)#
```

dot1x timeout start-period

This command sets the time that a supplicant port waits before resending an EAPOL start frame to the authenticator. Use the **no** form to restore the default setting.

SYNTAX

dot1x timeout start-period *seconds*

no dot1x timeout start-period

seconds - The number of seconds. (Range: 1-65535)

DEFAULT

30 seconds

COMMAND MODE

Interface Configuration

EXAMPLE

```
ES-3026(config)#interface eth 1/2
ES-3026(config-if)#dot1x timeout start-period 60
ES-3026(config-if)#
```

show dot1x

This command shows general port authentication related settings on the switch or a specific interface.

SYNTAX

show dot1x [**statistics**] [**interface** *interface*]

statistics - Displays dot1x status for each port.

interface

ethernet *unit*/*port*

unit - Unit identifier. (Range: 1)

port - Port number. (ES-3026/P: 1-26, ES-3024G/P: 1-24)

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 599).
- *Authenticator Parameters* – Shows whether or not EAPOL pass-through is enabled (page 599).

- *Supplicant Parameters* – Shows the supplicant user name used when the switch responds to an MD5 challenge from an authenticator (page 606).

- *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 601).
  - Mode– Dot1x port control mode (page 602).
  - 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 602).
  - Reauth Period – Time after which a connected client must be re-authenticated (page 603).
  - Quiet Period – Time a port waits after Max Request Count is exceeded before attempting to acquire a new client (page 603).
  - TX Period – Time a port waits during authentication session before re-transmitting EAP packet (page 604).
  - 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 600).
  - 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 602).
  - Intrusion Action– Sets the port response to intrusion when authentication fails (page 600).
  - Supplicant– MAC address of authorized client.

- *Authenticator State Machine*

  - State – Current state (including initialize, disconnected, connecting, authenticating, authenticated, aborting, held, force_authorized, force_unauthorized).
  - Reauth Count– Number of times connecting state is re-entered.
  - Current Identifier– The integer (0-255) used by the Authenticator to identify the current authentication session.

- *Backend State Machine*

  - State – Current state (including request, response, success, fail, timeout, idle, initialize).
  - Request Count– Number of EAP Request packets sent to the Supplicant without receiving a response.

- Identifier (Server)– Identifier carried in the most recent EAP Success, Failure or Request packet received from the Authentication Server.

◆ *Reauthentication State Machine*

State – Current state (including initialize, reauthenticate).

EXAMPLE

```
ES-3026#show dot1x
Global 802.1X Parameters
  System-auth-control: Enabled

Authenticator Parameters:
 EAPOL Pass Through        : Disabled

Supplicant Parameters:
 Identity Profile Username : steve

802.1X Port Summary

Port Name  Status         Operation Mode   Mode                Authorized
1/1        Disabled      Single-Host      ForceAuthorized     N/A
1/2        Disabled      Single-Host      ForceAuthorized     N/A
.
.
.
1/27       Disabled      Single-Host      ForceAuthorized     Yes
1/28       Enabled       Single-Host      Auto                Yes

802.1X Port Details

802.1X Authenticator is enabled on port 1/1
802.1X Supplicant is disabled on port 1/1
.
.
.
802.1X Authenticator is enabled on port 26
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 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

ES-3026#
```

MANAGEMENT IP FILTER

This section describes commands used to configure IP management access to the switch.

Table 71: 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.

```
ES-3026(config)#management all-client 192.168.1.19
ES-3026(config)#management all-client 192.168.1.25 192.168.1.30
ES-3026#
```

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

```
ES-3026#show management all-client
Management Ip Filter
 HTTP-Client:
   Start IP address      End IP address
-----------------------------------------------
1. 192.168.1.19          192.168.1.19
2. 192.168.1.25          192.168.1.30

 SNMP-Client:
   Start IP address      End IP address
-----------------------------------------------
1. 192.168.1.19          192.168.1.19
2. 192.168.1.25          192.168.1.30
```

```
 TELNET-Client:
   Start IP address      End IP address
-----------------------------------------------
1. 192.168.1.19          192.168.1.19
2. 192.168.1.25          192.168.1.30

ES-3026#
```

25 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 72: General Security Commands

Command Group	Function
Port Security*	Configures secure addresses for a port
802.1X Port Authentication*	Configures host authentication on specific ports using 802.1X
Network Access*	Configures MAC authentication and dynamic VLAN assignment
Web Authentication*	Configures Web authentication
Access Control Lists*	Provides filtering for IP frames (based on address, protocol, TCP/UDP port number or TCP control code) or non-IP frames (based on MAC address or Ethernet type)
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, Web Authentication, Access Control Lists, DHCP Snooping, and then IP Source Guard.

PORT SECURITY

These commands can be used to enable port security on a port.

When MAC address learning is disabled on an interface, only incoming traffic with source addresses already stored in the dynamic or static address table for this port will be authorized to access the network.

When using port security, the switch stops learning new MAC addresses on the specified port when it has reached a configured maximum number. Only incoming traffic with source addresses already stored in the dynamic or static address table for this port will be authorized to access the network. The port will drop any incoming frames with a source MAC address that is unknown or has been previously learned from another port. If a device with an unauthorized MAC address attempts to use the switch port, the intrusion will be detected and the switch can automatically take action by disabling the port and sending a trap message.

Table 73: 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.

```
ES-3026(config)#interface ethernet 1/2
ES-3026(config-if)#no mac-learning
ES-3026(config-if)#
```

RELATED COMMANDS

show interfaces status (688)

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:

```
ES-3026(config)#interface ethernet 1/5
ES-3026(config-if)#port security action trap
```

RELATED COMMANDS

show interfaces status (688)
shutdown (683)
mac-address-table static (738)

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 74: 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 601).
- The maximum number of secure MAC addresses supported for the switch system is 1024.

EXAMPLE

```
ES-3026(config-if)#network-access aging
ES-3026(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
```
ES-3026(config)#network-access mac-filter 1 mac-address 11-22-33-44-55-66
ES-3026(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
```
ES-3026(config)#mac-authentication reauth-time 300
ES-3026(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 75: 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.

```
ES-3026(config)#interface ethernet 1/1
ES-3026(config-if)#network-access dynamic-qos
ES-3026(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.

```
ES-3026(config)#interface ethernet 1/1
ES-3026(config-if)#network-access dynamic-vlan
ES-3026(config-if)#
```

network-access guest-vlan

Use this command to assign all traffic on a port to a guest VLAN when network access (MAC authentication) or 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
```
ES-3026(config)#interface ethernet 1/1
ES-3026(config-if)#network-access guest-vlan 25
ES-3026(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
```
ES-3026(config)#interface ethernet 1/1
ES-3026(config-if)#network-access link-detection
ES-3026(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

```
ES-3026(config)#interface ethernet 1/1
ES-3026(config-if)#network-access link-detection link-down action trap
ES-3026(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

```
ES-3026(config)#interface ethernet 1/1
ES-3026(config-if)#network-access link-detection link-up action trap
ES-3026(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

```
ES-3026(config)#interface ethernet 1/1
ES-3026(config-if)#network-access link-detection link-up-down action trap
ES-3026(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 failed.

EXAMPLE

```
ES-3026(config-if)#network-access max-mac-count 5
ES-3026(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

```
ES-3026(config-if)#network-access mode mac-authentication
ES-3026(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

```
ES-3026(config)#interface ethernet 1/1
ES-3026(config-if)#network-access port-mac-filter 1
ES-3026(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

```
ES-3026(config-if)#mac-authentication intrusion-action block-traffic
ES-3026(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

```
ES-3026(config-if)#mac-authentication max-mac-count 32
ES-3026(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 - Unit identifier. (Range: 1)

port - Port number. (ES-3026/P: 1-26, ES-3024G/P: 1-24)

DEFAULT SETTING

Displays the settings for all interfaces.

COMMAND MODE

Privileged Exec

EXAMPLE

```
ES-3026#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
ES-3026#
```

show network-access mac-address-table

Use this command to display secure MAC address table entries.

SYNTAX

show network-access mac-address-table [**static** | **dynamic**] [**address** *mac-address* [*mask*]] [**interface** *interface*] [**sort** {**address** | **interface**}]

static - Specifies static address entries.

dynamic - Specifies dynamic address entries.

mac-address - Specifies a MAC address entry. (Format: xx-xx-xx-xx-xx-xx)

mask - Specifies a MAC address bit mask for filtering displayed addresses.

interface - Specifies a port interface.

ethernet *unit*/*port*

unit - Unit identifier. (Range: 1)

port - Port number. (ES-3026/P: 1-26, ES-3024G/P: 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

```
ES-3026#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

ES-3026#
```

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#
```

WEB AUTHENTICATION

Web authentication allows stations to authenticate and access the network in situations where 802.1X or Network Access authentication are infeasible or impractical. The web authentication feature allows unauthenticated hosts to request and receive a DHCP assigned IP address and perform DNS queries. All other traffic, except for HTTP protocol traffic, is blocked. The switch intercepts HTTP protocol traffic and redirects it to a switch-generated web page that facilitates user name and password authentication via RADIUS. Once authentication is successful, the web browser is forwarded on to the originally requested web page. Successful authentication is valid for all hosts connected to the port.

NOTE: RADIUS authentication must be activated and configured for the web authentication feature to work properly (see "Authentication Sequence" on page 564).

NOTE: Web authentication cannot be configured on trunk ports.

Table 76: Web Authentication

Command	Function	Mode
web-auth login-attempts	Defines the limit for failed web authentication login attempts	GC
web-auth quiet-period	Defines the amount of time to wait after the limit for failed login attempts is exceeded.	GC
web-auth session-timeout	Defines the amount of time a session remains valid	GC

Table 76: Web Authentication (Continued)

Command	Function	Mode
web-auth system-auth-control	Enables web authentication globally for the switch	GC
web-auth	Enables web authentication for an interface	IC
web-auth re-authenticate (Port)	Ends all web authentication sessions on the port and forces the users to re-authenticate	PE
web-auth re-authenticate (IP)	Ends the web authentication session associated with the designated IP address and forces the user to re-authenticate	PE
show web-auth	Displays global web authentication parameters	PE
show web-auth interface	Displays interface-specific web authentication parameters and statistics	PE
show web-auth summary	Displays a summary of web authentication port parameters and statistics	PE

web-auth login-attempts

This command defines the limit for failed web authentication login attempts. After the limit is reached, the switch refuses further login attempts until the quiet time expires. Use the **no** form to restore the default.

SYNTAX

web-auth login-attempts *count*

no web-auth login-attempts

count - The limit of allowed failed login attempts. (Range: 1-3)

DEFAULT SETTING

3 login attempts

COMMAND MODE

Global Configuration

EXAMPLE

```
ES-3026(config)#web-auth login-attempts 2
ES-3026(config)#
```

web-auth quiet-period

This command defines the amount of time a host must wait after exceeding the limit for failed login attempts, before it may attempt web authentication again. Use the **no** form to restore the default.

SYNTAX

web-auth quiet-period *time*

no web-auth quiet period

time - The amount of time the host must wait before attempting authentication again. (Range: 1-180 seconds)

DEFAULT SETTING

60 seconds

COMMAND MODE

Global Configuration

EXAMPLE

```
ES-3026(config)#web-auth quiet-period 120
ES-3026(config)#
```

web-auth session-timeout

This command defines the amount of time a web-authentication session remains valid. When the session timeout has been reached, the host is logged off and must re-authenticate itself the next time data transmission takes place. Use the **no** form to restore the default.

SYNTAX

web-auth session-timeout *timeout*

no web-auth session timeout

timeout - The amount of time that an authenticated session remains valid. (Range: 300-3600 seconds)

DEFAULT SETTING

3600 seconds

COMMAND MODE

Global Configuration

EXAMPLE

```
ES-3026(config)#web-auth session-timeout 1800
ES-3026(config)#
```

web-auth system-auth-control

This command globally enables web authentication for the switch. Use the **no** form to restore the default.

SYNTAX

[**no**] **web-auth system-auth-control**

DEFAULT SETTING

Disabled

COMMAND MODE

Global Configuration

COMMAND USAGE

Both **web-auth system-auth-control** for the switch and web-auth for an interface must be enabled for the web authentication feature to be active.

EXAMPLE

```
ES-3026(config)#web-auth system-auth-control
ES-3026(config)#
```

web-auth

This command enables web authentication for an interface. Use the no form to restore the default.

SYNTAX

[**no**] **web-auth**

DEFAULT SETTING

Disabled

COMMAND MODE

Interface Configuration

COMMAND USAGE

Both web-auth system-auth-control for the switch and **web-auth** for a port must be enabled for the web authentication feature to be active.

EXAMPLE

```
ES-3026(config-if)#web-auth
ES-3026(config-if)#
```

web-auth re-authenticate (Port)

This command ends all web authentication sessions connected to the port and forces the users to re-authenticate.

SYNTAX

web-auth re-authenticate interface *interface*

interface - Specifies a port interface.

ethernet *unit/port*

unit - This is unit 1.

port - Port number. (ES-3026/P: 1-26, ES-3024G/P: 1-24)

DEFAULT SETTING

None

COMMAND MODE

Privileged Exec

EXAMPLE

```
ES-3026#web-auth re-authenticate interface ethernet 1/2
Failed to reauth.
ES-3026#
```

web-auth re-authenticate (IP)

This command ends the web authentication session associated with the designated IP address and forces the user to re-authenticate.

SYNTAX

web-auth re-authenticate interface *interface ip*

interface - Specifies a port interface.

ethernet *unit/port*

unit - This is unit 1.

port - Port number. (ES-3026/P: 1-26, ES-3024G/P: 1-24)

ip - IPv4 formatted IP address

DEFAULT SETTING

None

COMMAND MODE

Privileged Exec

EXAMPLE

```
ES-3026#web-auth re-authenticate interface ethernet 1/2 192.168.1.5
Failed to reauth port.
ES-3026#
```

show web-auth

This command displays global web authentication parameters.

COMMAND MODE

Privileged Exec

EXAMPLE

```
ES-3026#show web-auth

Global Web-Auth Parameters

  System Auth Control      : Enabled
  Session Timeout          : 3600
  Quiet Period             : 60
  Max Login Attempts       : 3
ES-3026#
```

show web-auth interface

This command displays interface-specific web authentication parameters and statistics.

SYNTAX

show web-auth interface *interface*

interface - Specifies a port interface.

ethernet *unit*/*port*

unit - This is unit 1.

port - Port number. (ES-3026/P: 1-26, ES-3024G/P: 1-24)

COMMAND MODE

Privileged Exec

EXAMPLE

```
ES-3026#show web-auth interface ethernet 1/2
Web Auth Status      : Enabled

Host Summary

IP address      Web-Auth-State Remaining-Session-Time
--------------- -------------- ----------------------
1.1.1.1         Authenticated  295
1.1.1.2         Authenticated  111
ES-3026#
```

show web-auth summary

This command displays a summary of web authentication port parameters and statistics.

COMMAND MODE

Privileged Exec

EXAMPLE

```
ES-3026#show web-auth summary

Global Web-Auth Parameters

  System Auth Control      : Enabled
Port       Status         Authenticated Host Count
----       ------         ------------------------
1/ 1       Disabled       0
1/ 2       Enabled        8
1/ 3       Disabled       0
1/ 4       Disabled       0
1/ 5       Disabled       0
⋮
```

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 77: 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.

```
ES-3026(config)#ip dhcp snooping
ES-3026(config)#
```

RELATED COMMANDS

ip dhcp snooping vlan (643)
ip dhcp snooping trust (644)

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

```
ES-3026(config)#ip dhcp snooping database flash
ES-3026(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.

```
ES-3026(config)#ip dhcp snooping information option
ES-3026(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

```
ES-3026(config)#ip dhcp snooping information policy drop
ES-3026(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.

```
ES-3026(config)#ip dhcp snooping verify mac-address
ES-3026(config)#
```

RELATED COMMANDS

ip dhcp snooping (639)
ip dhcp snooping vlan (643)
ip dhcp snooping trust (644)

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.

```
ES-3026(config)#ip dhcp snooping vlan 1
ES-3026(config)#
```

RELATED COMMANDS

ip dhcp snooping (639)
ip dhcp snooping trust (644)

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.

```
ES-3026(config)#interface ethernet 1/5
ES-3026(config-if)#no ip dhcp snooping trust
ES-3026(config-if)#
```

RELATED COMMANDS

ip dhcp snooping (639)
ip dhcp snooping vlan (643)

clear ip dhcp snooping database flash

This command removes all dynamically learned snooping entries from flash memory.

COMMAND MODE

Privileged Exec

EXAMPLE

```
ES-3026(config)#ip dhcp snooping database flash
ES-3026(config)#
```

show ip dhcp snooping

This command shows the DHCP snooping configuration settings.

COMMAND MODE

Privileged Exec

EXAMPLE

```
ES-3026#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

```
ES-3026#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
ES-3026#
```

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 638). 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 78: 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
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 ethernet** *unit/port*

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.

unit - Unit identifier. (Range: 1)

port - Port number. (ES-3026/P: 1-26, ES-3024G/P: 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 650).
- 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.

```
ES-3026(config)#ip source-guard binding 11-22-33-44-55-66 vlan 1 192.168.0.99
  interface ethernet 1/5
ES-3026(config-if)#
```

RELATED COMMANDS

ip source-guard (648)
ip dhcp snooping (639)
ip dhcp snooping vlan (643)

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 647) 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 639), 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.

```
ES-3026(config)#interface ethernet 1/5
ES-3026(config-if)#ip source-guard sip
ES-3026(config-if)#
```

RELATED COMMANDS

ip source-guard binding (647)
ip dhcp snooping (639)
ip dhcp snooping vlan (643)

show ip source-guard

This command shows whether source guard is enabled or disabled on each interface.

COMMAND MODE

Privileged Exec

EXAMPLE

```
ES-3026#show ip source-guard
Interface   Filter-type
---------   -----------
Eth 1/1     DISABLED
Eth 1/2     DISABLED
Eth 1/3     DISABLED
Eth 1/4     DISABLED
Eth 1/5     SIP
Eth 1/6     DISABLED
⋮
```

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 638)

static - Shows static entries configured with the ip source-guard binding command (see page 647).

COMMAND MODE

Privileged Exec

EXAMPLE

```
ES-3026#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
ES-3026#
```

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 79: 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 79: 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

```
ES-3026(config)#ip arp inspection
ES-3026(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 299.
- 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

```
ES-3026(config)#ip arp inspection filter sales vlan 1
ES-3026(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

```
ES-3026(config)#ip arp inspection log-buffer logs 1 interval 10
ES-3026(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

```
ES-3026(config)#ip arp inspection validate dst-mac
ES-3026(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
```
ES-3026(config)#ip arp inspection vlan 1,2
ES-3026(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

```
ES-3026(config)#interface ethernet 1/1
ES-3026(config-if)#ip arp inspection limit 150
ES-3026(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

```
ES-3026(config)#interface ethernet 1/1
ES-3026(config-if)#ip arp inspection trust
ES-3026(config-if)#
```

show ip arp inspection configuration

This command displays the global configuration settings for ARP Inspection.

COMMAND MODE

Privileged Exec

EXAMPLE

```
ES-3026#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
ES-3026#
```

show ip arp inspection interface

This command shows the trust status and ARP Inspection rate limit for ports.

SYNTAX

show ip arp inspection interface [*interface*]

interface

ethernet *unit*/*port*

unit - Unit identifier. (Range: 1)

port - Port number. (ES-3026/P: 1-26, ES-3024G/P: 1-24)

COMMAND MODE

Privileged Exec

EXAMPLE

```
ES-3026#show ip arp inspection interface ethernet 1/1

Port Number        Trust Status             Limit Rate (pps)
-------------   --------------------    ------------------------------
Eth 1/1            trusted                    150
ES-3026#
```

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

```
ES-3026#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
ES-3026#
```

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

```
ES-3026#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
--- ---- ---- --------------  --------------  ---------------  -----------

ES-3026#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

ES-3026#
```

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

```
ES-3026#show ip arp inspection vlan 1

VLAN ID     DAI Status             ACL Name             ACL Status
--------   ---------------    ---------------------    ---------------------
1           disabled               sales                static
ES-3026#
```

26 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), 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 80: 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
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 81: 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

```
ES-3026(config)#access-list ip standard david
ES-3026(config-std-acl)#
```

RELATED COMMANDS

permit, deny (663)
ip access-group (666)
show ip access-list (667)

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.

```
ES-3026(config-std-acl)#permit host 10.1.1.21
ES-3026(config-std-acl)#permit 168.92.16.0 255.255.240.0
ES-3026(config-std-acl)#
```

RELATED COMMANDS

access-list ip (662)
Time Range (524)

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[9] source port number. (Range: 0-65535)

dport – Protocol[9] destination port number. (Range: 0-65535)

9. 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.

```
ES-3026(config-ext-acl)#permit 10.7.1.1 255.255.255.0 any
ES-3026(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).

```
ES-3026(config-ext-acl)#permit 192.168.1.0 255.255.255.0 any destination-port
  80
ES-3026(config-ext-acl)#
```

This permits all TCP packets from class C addresses 192.168.1.0 with the TCP control code set to “SYN.”

```
ES-3026(config-ext-acl)#permit tcp 192.168.1.0 255.255.255.0 any  control-
  flag 2 2
ES-3026(config-ext-acl)#
```

RELATED COMMANDS

access-list ip (662)
Time Range (524)

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

```
ES-3026(config)#int eth 1/2
ES-3026(config-if)#ip access-group david in
ES-3026(config-if)#
```

RELATED COMMANDS

show ip access-list (667)
Time Range (524)

show ip access-group

This command shows the ports assigned to IP ACLs.

COMMAND MODE

Privileged Exec

EXAMPLE

```
ES-3026#show ip access-group
Interface ethernet 1/2
 IP access-list david in
ES-3026#
```

RELATED COMMANDS

ip access-group (666)

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

```
ES-3026#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
ES-3026#
```

RELATED COMMANDS

permit, deny (663)
ip access-group (666)

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 82: 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

```
ES-3026(config)#access-list mac jerry
ES-3026(config-mac-acl)#
```

RELATED COMMANDS

permit, deny (669)
mac access-group (671)
show mac access-list (672)

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[10] – Bitmask for MAC address (in hexadecimal format).

vid – VLAN ID. (Range: 1-4093)

vid-bitmask[10] – VLAN bitmask. (Range: 1-4095)

protocol – A specific Ethernet protocol number. (Range: 600-ffff hex.)

protocol-bitmask[10] – 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

10. For all bitmasks, “1” means care and “0” means ignore.

COMMAND USAGE

- New rules are added to the end of the list.
- The **ethertype** option can only be used to filter Ethernet II formatted packets.
- 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.

```
ES-3026(config-mac-acl)#permit any host 00-e0-29-94-34-de ethertype 0800
ES-3026(config-mac-acl)#
```

RELATED COMMANDS

access-list mac (668)
Time Range (524)

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

```
ES-3026(config)#interface ethernet 1/2
ES-3026(config-if)#mac access-group jerry in
ES-3026(config-if)#
```

RELATED COMMANDS

show mac access-list (672)
Time Range (524)

show mac access-group

This command shows the ports assigned to MAC ACLs.

COMMAND MODE

Privileged Exec

EXAMPLE

```
ES-3026#show mac access-group
Interface ethernet 1/5
 MAC access-list M5 in
ES-3026#
```

RELATED COMMANDS

mac access-group (671)

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

```
ES-3026#show mac access-list
MAC access-list jerry:
  permit any 00-e0-29-94-34-de ethertype 0800
ES-3026#
```

RELATED COMMANDS

permit, deny (669)
mac access-group (671)

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 655).

Table 83: 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.
- An ACL can contain up to 128 rules.

EXAMPLE

```
ES-3026(config)#access-list arp factory
ES-3026(config-arp-acl)#
```

RELATED COMMANDS

permit, deny (674)
show arp access-list (675)

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[11] – IPv4 number representing the address bits to match.

source-mac – Source MAC address.

destination-mac – Destination MAC address range with bitmask.

mac-address-bitmask[11] – 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.

11. 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.

```
ES-3026(config-arp-acl)#$permit response ip any 192.168.0.0 255.255.0.0 mac
  any any
ES-3026(config-mac-acl)#
```

RELATED COMMANDS

access-list arp (673)

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

```
ES-3026#show arp access-list
ARP access-list factory:
  permit response ip any 192.168.0.0 255.255.0.0 mac any any
ES-3026#
```

RELATED COMMANDS

permit, deny (674)

ACL INFORMATION

This section describes commands used to display ACL information.

Table 84: 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

```
ES-3026#show access-group
Interface ethernet 1/2
 IP access-list david
 MAC access-list jerry
ES-3026#
```

show access-list

This command shows all ACLs and associated rules.

COMMAND MODE

Privileged Exec

EXAMPLE

```
ES-3026#show access-list
IP standard access-list david:
  permit host 10.1.1.21
  permit 168.92.0.0 255.255.15.0
IP extended access-list bob:
  permit 10.7.1.1 255.255.255.0 any
  permit 192.168.1.0 255.255.255.0 any destination-port 80 80
  permit 192.168.1.0 255.255.255.0 any protocol tcp control-code 2 2
MAC access-list jerry:
  permit any host 00-30-29-94-34-de ethertype 800 800
IP extended access-list A6:
  deny tcp any any control-flag 2 2
  permit any any
ES-3026#
```

27 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 85: 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 broadcast, multicast, and unknown unicast storm control thresholds	IC
clear counters	Clears statistics on an interface	PE
show interfaces brief	Displays a summary of key information, including operational status, native VLAN ID, default priority, speed/duplex mode, and port type	PE
show interfaces counters	Displays statistics for the specified interfaces	NE, PE
show interfaces 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	Performs cable diagnostics on the specified port	PE
show cable-diagnostics	Shows the results of a cable diagnostics test	PE
Power Savings		
power-save	Enables power savings mode on the specified port	IC
show power-save	Shows the configuration settings for power savings	PE

* Enabling hardware-level storm control with this command on a port will disable software-level automatic storm control on the same port if configured by the auto-traffic-control command (page 727).

interface

This command configures an interface type and enter 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 - Unit identifier. (Range: 1)

port - Port number. (ES-3026/P: 1-26, ES-3024G/P: 1-24)

port-channel *channel-id* (Range: 1-12)

vlan *vlan-id* (Range: 1-4093)

DEFAULT SETTING

None

COMMAND MODE

Global Configuration

EXAMPLE

To specify port 4, enter the following command:

```
ES-3026(config)#interface ethernet 1/4
ES-3026(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.

```
ES-3026(config)#interface ethernet 1/4
ES-3026(config-if)#alias finance
ES-3026(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

100BASE-TX: 10half, 10full, 100half, 100full
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.

```
ES-3026(config)#interface ethernet 1/5
ES-3026(config-if)#capabilities 100half
ES-3026(config-if)#capabilities 100full
ES-3026(config-if)#capabilities flowcontrol
ES-3026(config-if)#
```

RELATED COMMANDS

negotiation (682)
speed-duplex (684)
flowcontrol (681)

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.

```
ES-3026(config)#interface ethernet 1/4
ES-3026(config-if)#description RD-SW#3
ES-3026(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.

```
ES-3026(config)#interface ethernet 1/5
ES-3026(config-if)#flowcontrol
ES-3026(config-if)#no negotiation
ES-3026(config-if)#
```

RELATED COMMANDS

negotiation (682)
capabilities (flowcontrol, symmetric) (679)

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 25-26 on the ES-3026/P and 21-24 on ES-3024G/P)

EXAMPLE

This forces the switch to use the built-in RJ-45 port for the combination port 25.

```
ES-3026(config)#interface ethernet 1/25
ES-3026(config-if)#media-type copper-forced
ES-3026(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.

```
ES-3026(config)#interface ethernet 1/11
ES-3026(config-if)#negotiation
ES-3026(config-if)#
```

RELATED COMMANDS

capabilities (679)
speed-duplex (684)

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.

```
ES-3026(config)#interface ethernet 1/5
ES-3026(config-if)#shutdown
ES-3026(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 {**100full** | **100half** | **10full** | **10half**}

no speed-duplex

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.
- When auto-negotiation is disabled, the default speed-duplex setting is:
  - Fast Ethernet ports – **100full** for 100BASE-TX ports
  - Gigabit Ethernet ports – **100full** for 1000BASE-T ports

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.

```
ES-3026(config)#interface ethernet 1/5
ES-3026(config-if)#speed-duplex 100half
ES-3026(config-if)#no negotiation
ES-3026(config-if)#
```

RELATED COMMANDS

negotiation (682)
capabilities (679)

switchport packet-rate

This command configures broadcast, multicast and unknown unicast storm control. Use the **no** form to restore the default setting.

SYNTAX

switchport {**broadcast** | **multicast** | **unicast**} **packet-rate** *rate*

no switchport {**broadcast** | **multicast** | **unicast**}

broadcast - Specifies storm control for broadcast traffic.

multicast - Specifies storm control for multicast traffic.

unicast - Specifies storm control for unknown unicast traffic.

rate - Threshold level as a rate; i.e., packets per second. (Range: 500-262143)

DEFAULT SETTING

Broadcast Storm Control: Enabled, packet-rate limit: 500 pps
Multicast Storm Control: Disabled
Unknown Unicast Storm Control: Disabled

COMMAND MODE

Interface Configuration (Ethernet)

COMMAND USAGE

- When traffic exceeds the threshold specified for broadcast and multicast or unknown unicast traffic, packets exceeding the threshold are dropped until the rate falls back down beneath the threshold.

- 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 Fast Ethernet 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:

```
ES-3026(config)#interface ethernet 1/5
ES-3026(config-if)#switchport broadcast packet-rate 600
ES-3026(config-if)#
```

clear counters

This command clears statistics on an interface.

SYNTAX

clear counters *interface*

interface

ethernet *unit/port*

unit - Unit identifier. (Range: 1)

port - Port number. (ES-3026/P: 1-26, ES-3024G/P: 1-24)

port-channel *channel-id* (Range: 1-12)

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.

```
ES-3026#clear counters ethernet 1/5
ES-3026#
```

show interfaces brief

This command displays a summary of key information, including operational status, native VLAN ID, default priority, speed/duplex mode, and port type for all ports.

COMMAND MODE

Privileged Exec

EXAMPLE

```
Console#show interfaces brief
Interface Name               Status   PVID Pri Speed/Duplex  Type         Trunk
--------- ------------------ -------- ---- --- ------------- ------------ ---
Eth 1/ 1                     Up          1   0 Auto-100full  100TX        None
Eth 1/ 2                     Down        1   0 Auto          100TX        None
Eth 1/ 3                     Down        1   0 Auto          100TX        None
Eth 1/ 4                     Down        1   0 Auto          100TX        None
Eth 1/ 5                     Down        1   0 Auto          100TX        None
Eth 1/ 6                     Down        1   0 Auto          100TX        None
⋮
```

show interfaces counters

This command displays interface statistics.

SYNTAX

show interfaces counters [*interface*]

interface

ethernet *unit*/*port*

unit - Unit identifier. (Range: 1)

port - Port number. (ES-3026/P: 1-26, ES-3024G/P: 1-24)

port-channel *channel-id* (Range: 1-12)

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 123.

EXAMPLE

```
ES-3026#show interfaces counters ethernet 1/17
Ethernet 1/ 1
 ===== IF table Stats =====
                 2166458 Octets Input
                14734059 Octets Output
                   14707 Unicast Input
                   19806 Unicast Output
                       0 Discard Input
                       0 Discard Output
                       0 Error Input
                       0 Error Output
                       0 Unknown Protos Input
                       0 QLen Output
 ===== Extended Iftable Stats =====
                      23 Multi-cast Input
                    5525 Multi-cast Output
                     170 Broadcast Input
                      11 Broadcast Output
 ===== Ether-like Stats =====
                       0 Alignment Errors
                       0 FCS Errors
                       0 Single Collision Frames
                       0 Multiple Collision Frames
                       0 SQE Test Errors
                       0 Deferred Transmissions
                       0 Late Collisions
                       0 Excessive Collisions
                       0 Internal Mac Transmit Errors
                       0 Internal Mac Receive Errors
                       0 Frames Too Long
                       0 Carrier Sense Errors
                       0 Symbol Errors
```

```
 ===== RMON Stats =====
                        0 Drop Events
                 16900558 Octets
                    40243 Packets
                      170 Broadcast PKTS
                       23 Multi-cast PKTS
                        0 Undersize PKTS
                        0 Oversize PKTS
                        0 Fragments
                        0 Jabbers
                        0 CRC Align Errors
                        0 Collisions
                    21065 Packet Size <= 64 Octets
                     3805 Packet Size 65 to 127 Octets
                     2448 Packet Size 128 to 255 Octets
                      797 Packet Size 256 to 511 Octets
                     2941 Packet Size 512 to 1023 Octets
                     9187 Packet Size 1024 to 1518 Octets
ES-3026#
```

show interfaces status

This command displays the status for an interface.

SYNTAX

show interfaces status [*interface*]

interface

ethernet *unit*/*port*

unit - Unit identifier. (Range: 1)

port - Port number. (ES-3026/P: 1-26, ES-3024G/P: 1-24)

port-channel *channel-id* (Range: 1-12)

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 116.

EXAMPLE

```
ES-3026#show interfaces status ethernet 1/21
Information of Eth 1/21
 Basic Information:
  Port Type              : 100TX
  Mac Address            : 00-E0-0C-00-00-FE
 Configuration:
  Name                   :
  Port Admin             : Up
```

```
  Speed-duplex           : Auto
  Capabilities           : 10half, 10full, 100half, 100full
  Broadcast Storm        : Enabled
  Broadcast Storm Limit  : 500 packets/second
  Multicast Storm        : Disabled
  Multicast Storm Limit  : 64 Kbits/second
  Unknown Unicast Storm       : Disabled
  Unknown Unicast Storm Limit : 64 Kbits/second
  Flow Control           : Disabled
  LACP                   : Disabled
  Mac-Learning           : Yes
  Port Security          : Disabled
  Max MAC Count          : 0
  Port Security Action   : None
  Media Type             : Copper forced
 Current Status:
  Link Status            : Up
  Port Operation Status  : Up
  Operation Speed-duplex : 100full
  Flow Control Type      : None
ES-3026#
```

show interfaces switchport

This command displays the administrative and operational status of the specified interfaces.

SYNTAX

show interfaces switchport [*interface*]

interface

ethernet *unit*/*port*

unit - Unit identifier. (Range: 1)

port - Port number. (ES-3026/P: 1-26, ES-3024G/P: 1-24)

port-channel *channel-id* (Range: 1-12)

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.

```
ES-3026#show interfaces switchport ethernet 1/21
Information of Eth 1/21
 Broadcast Threshold           : Enabled, 500 packets/second
 Multicast Threshold           : Disabled
 Unknown Unicast Threshold     : Disabled
 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                 :
 802.1Q-tunnel Status           : Disable
 802.1Q-tunnel Mode             : NORMAL
 802.1Q-tunnel TPID             : 8100(Hex)
ES-3026#
```

Table 86: 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 685).
Multicast Threshold	Shows if multicast storm suppression is enabled or disabled; if enabled it also shows the threshold level (page 685).
Unknown-unicast Threshold	Shows if unknown unicast storm suppression is enabled or disabled; if enabled it also shows the threshold level (page 685).
LACP Status	Shows if Link Aggregation Control Protocol has been enabled or disabled (page 697).
Ingress/Egress Rate Limit	Shows if rate limiting is enabled, and the current rate limit (page 721).
VLAN Membership Mode	Indicates membership mode as Trunk or Hybrid (page 776).
Ingress Rule	Shows if ingress filtering is enabled or disabled (page 775).
Acceptable Frame Type	Shows if acceptable VLAN frames include all types or tagged frames only (page 774).
Native VLAN	Indicates the default Port VLAN ID (page 777).
Priority for Untagged Traffic	Indicates the default priority for untagged frames (page 804).
GVRP Status	Shows if GARP VLAN Registration Protocol is enabled or disabled (page 768).
Allowed VLAN	Shows the VLANs this interface has joined, where “(u)” indicates untagged and “(t)” indicates tagged (page 774).
Forbidden VLAN	Shows the VLANs this interface can not dynamically join via GVRP (page 768).
802.1Q-tunnel Status	Shows if 802.1Q tunnel is enabled on this interface (page 781).
802.1Q-tunnel Mode	Shows the tunnel mode as Normal, 802.1Q Tunnel or 802.1Q Tunnel Uplink (page 782).
802.1Q-tunnel TPID	Shows the Tag Protocol Identifier used for learning and switching packets (page 783).

test cable-diagnostics

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 interface *interface*

interface

ethernet *unit/port*

unit - Unit identifier. (Range: 1)

port - Port number. (ES-3026/P: 1-26, ES-3024G/P: 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

```
ES-3026#test cable-diagnostics interface ethernet 1/23
ES-3026#show cable-diagnostics interface e 1/23
Port     Type Link Status Pair A (meters)  Pair B (meters)  Last Update
-------- ---- ----------- ---------------- ---------------- -----------------
Eth 1/23   GE  Up         OK (21)          OK (21)          2009-11-13 09:44:19
ES-3026#
```

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. (ES-3026/P: 1-26, ES-3024G/P: 1-24)

COMMAND MODE

Privileged Exec

EXAMPLE

```
ES-3026#show cable-diagnostics interface ethernet 1/23
ES-3026#show cable-diagnostics interface e 1/23
Port     Type Link Status Pair A (meters)  Pair B (meters)  Last Update
-------- ---- ----------- ---------------- ---------------- -----------------
Eth 1/23   GE  Up         OK (21)          OK (21)          2009-11-13 09:44:19
ES-3026#
```

power-save

This command enables power savings mode on the specified port.

SYNTAX

[**no**] **power-save**

COMMAND MODE

Interface Configuration (Ethernet)

COMMAND USAGE

- IEEE 802.3 defines the Ethernet standard and subsequent power requirements based on cable connections operating at 100 meters. Enabling power saving mode can reduce power used for cable lengths of 60 meters or less, with more significant reduction for cables of 20 meters or less, and continue to ensure signal integrity.
- Power saving mode only applies to the Gigabit Ethernet ports using copper media.
- Power savings can be enabled on Gigabit Ethernet RJ-45 ports.
- The power-saving methods provided by this switch include:
  - Power saving when there is no link partner:

    Under normal operation, the switch continuously auto-negotiates to find a link partner, keeping the MAC interface powered up even if no link connection exists. When using power-savings mode, the switch checks for energy on the circuit to determine if there is a link

partner. If none is detected, the switch automatically turns off the transmitter, and most of the receive circuitry (entering Sleep Mode). In this mode, the low-power energy-detection circuit continuously checks for energy on the cable. If none is detected, the MAC interface is also powered down to save additional energy. If energy is detected, the switch immediately turns on both the transmitter and receiver functions, and powers up the MAC interface.

- Power saving when there is a link partner:

  Traditional Ethernet connections typically operate with enough power to support at least 100 meters of cable even though average network cable length is shorter. When cable length is shorter, power consumption can be reduced since signal attenuation is proportional to cable length. When power-savings mode is enabled, the switch analyzes cable length to determine whether or not it can reduce the signal amplitude used on a particular link.

NOTE: Power-savings mode on a active link only works when the connection speed is 100 Mbps or higher at linkup, and line length is less than 60 meters.

NOTE: Power savings can only be implemented on Gigabit Ethernet ports using twisted-pair cabling. Power-savings mode on a active link only works when connection speed is 1 Gbps, and line length is less than 60 meters.

EXAMPLE

```
ES-3026(config)#interface ethernet 1/1
ES-3026(config-if)#power-save
ES-3026(config-if)#
```

show power-save

This command shows the configuration settings for power savings.

SYNTAX

show power-save [**interface** *interface*]

interface

ethernet *unit*/*port*

unit - Unit identifier. (Range: 1)

port - Port number. (ES-3026/P: 1-26, ES-3024G/P: 1-24)

COMMAND MODE

Privileged Exec

EXAMPLE

```
ES-3026#sh power-save interface ethernet 1/4

   Power Saving Status      : Enabled
ES-3026#
```

28 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 87: 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: 1-12)

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:

```
ES-3026(config)#interface port-channel 1
ES-3026(config-if)#exit
ES-3026(config)#interface ethernet 1/11
ES-3026(config-if)#channel-group 1
ES-3026(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.

```
ES-3026(config)#interface ethernet 1/10
ES-3026(config-if)#lacp
ES-3026(config-if)#interface ethernet 1/11
ES-3026(config-if)#lacp
ES-3026(config-if)#interface ethernet 1/12
ES-3026(config-if)#lacp
ES-3026(config-if)#end
```

```
ES-3026#show interfaces status port-channel 1
Information of Trunk 1
 Basic Information:
  Port Type              : 100TX
  Mac Address            : 12-34-12-34-12-3F
Configuration:
  Name                   :
  Port Admin             : Up
  Speed-duplex           : Auto
  Capabilities           : 10half, 10full, 100half, 100full
  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,
ES-3026#
```

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

```
ES-3026(config)#interface ethernet 1/5
ES-3026(config-if)#lacp actor admin-key 120
ES-3026(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

```
ES-3026(config)#interface ethernet 1/5
ES-3026(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

```
ES-3026(config)#interface ethernet 1/5
ES-3026(config-if)#lacp actor system-priority 3
ES-3026(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

```
ES-3026(config)#interface port-channel 1
ES-3026(config-if)#lacp admin-key 3
ES-3026(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: 1-12)

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

```
ES-3026#show lacp 1 counters
Port Channel: 1
---------------------------------------------------------------------------
Eth 1/ 2
---------------------------------------------------------------------------
  LACPDUs Sent         : 12
  LACPDUs Receive      : 6
  Marker Sent          : 0
  Marker Receive       : 0
  LACPDUs Unknown Pkts : 0
  LACPDUs Illegal Pkts : 0
⋮
```

Table 88: 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.

```
ES-3026#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 89: 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 89: 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)

```
ES-3026#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 90: 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 90: 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.)

```
 ES-3026#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 91: 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.

29 POWER OVER ETHERNET COMMANDS

The commands in this group control the power that can be delivered to attached PoE devices through RJ-45 ports 1-24 on the switch.

The switch's power management enables total switch power and individual port power to be controlled within a configured power budget. Port power can be automatically turned on and off for connected devices, and a per-port power priority can be set so that the switch never exceeds its allocated power budget. When a device is connected to a switch port, its power requirements are detected by the switch before power is supplied. If the power required by a device exceeds the power budget of the port or the whole switch, power is not supplied.

Table 92: PoE Commands

Command	Function	Mode
power inline compatible	Provides power to pre-standard PoE devices	GC
power inline	Turns power on and off for specific ports	IC
power inline maximum allocation	Sets the maximum power available to specific switch ports	IC
power inline priority	Sets the priority for power supplied to specific ports	IC
show power inline status	Displays the current status of power management on specific ports or all ports	PE
show power mainpower	Displays the current status of power management for switch	PE

power inline compatible

This command allows the switch to detect and provide power to powered devices that were designed prior to the IEEE 802.3af PoE standard. Use the **no** form to disable this feature.

SYNTAX

[**no**] **power inline compatible**

DEFAULT SETTING

Enabled

COMMAND MODE

Global Configuration

COMMAND USAGE

- The switch automatically detects attached PoE devices by periodically transmitting test voltages that over the Fast Ethernet or Gigabit

Ethernet copper-media ports. When an IEEE 802.3af or 802.3at compatible device is plugged into one of these ports, the powered device reflects the test voltage back to the switch, which may then turn on the power to this device. When the **power inline compatible** command is used, this switch can detect IEEE 802.3af or 802.3at compliant devices and the more recent 802.3af non-compliant devices that also reflect the test voltages back to the switch. It cannot detect other legacy devices that do not reflect back the test voltages.

- For legacy devices to be supported by this switch, they must be able to accept power over the data pairs connected to the 10/100BASE-TX ports.

EXAMPLE

```
ES-3026(config)#power inline compatible
ES-3026(config)#end
ES-3026#show power inline status
Unit: 1
Compatible  mode : Enabled
                                Max        Used
Interface  Admin     Oper  Power      Power      Priority
---------  --------  ----  --------   --------   --------
Eth  1/ 1  Enabled   Off   30000 mW       0 mW   Low
Eth  1/ 2  Enabled   Off   30000 mW       0 mW   Low
Eth  1/ 3  Enabled   Off   30000 mW       0 mW   Low
Eth  1/ 4  Enabled   Off   30000 mW       0 mW   Low
Eth  1/ 5  Enabled   Off   30000 mW       0 mW   Low
Eth  1/ 6  Enabled   Off   30000 mW       0 mW   Low
Eth  1/ 7  Enabled   Off   15400 mW       0 mW   Low
Eth  1/ 8  Enabled   Off   15400 mW       0 mW   Low
Eth  1/ 9  Enabled   Off   15400 mW       0 mW   Low
Eth  1/10  Enabled   Off   15400 mW       0 mW   Low
Eth  1/11  Enabled   Off   15400 mW       0 mW   Low
Eth  1/12  Enabled   Off   15400 mW       0 mW   Low
⋮
```

power inline

This command instructs the switch to automatically detect if a PoE-compliant device is connected to the specified port, and turn power on or off accordingly. Use the **no** form to turn off power for a port.

SYNTAX

[**no**] **power inline**

DEFAULT SETTING

Detection is enabled for PoE-compliant devices.

COMMAND MODE

Interface Configuration (Ethernet ports 1-24)

COMMAND USAGE

- The switch only provides power to the Fast Ethernet ports.

- When detection is enabled for PoE-compliant devices, power is automatically supplied when a device is detected on the port, providing that the power demanded does not exceed the port's power budget or the switch's power budget.

EXAMPLE

```
ES-3026(config)#interface ethernet 1/1
ES-3026(config-if)#power inline auto
ES-3026(config-if)#exit
ES-3026(config)#interface ethernet 1/2
ES-3026(config-if)#no power inline
ES-3026(config-if)#
```

power inline maximum allocation

This command limits the power allocated to specific ports. Use the **no** form to restore the default setting.

SYNTAX

power inline maximum allocation *milliwatts*
no power inline maximum allocation

milliwatts - The maximum power budget for the port. (Range: 3000 - 30000 milliwatts on ports 1-6; 3000 - 15400 milliwatts on ports 7-24).

DEFAULT SETTING

30000 milliwatts on ports 1-6
15400 milliwatts on ports 7-24

COMMAND MODE

Interface Configuration (Ethernet ports 1-24)

COMMAND USAGE

- The switch can supply up to 30W of power to the first six ports (based on the IEEE 802.3at draft), up to 15.4W to 12 ports (based on IEEE 802.3af). or up to 7.5 to 24 ports (based on IEEE 802.3af).

- If a device is connected to a switch port and the switch detects that it requires more than the maximum power allocated to the port or to the overall switch, no power is supplied to the device (i.e., port power remains off).

EXAMPLE

```
ES-3026(config)#interface ethernet 1/1
ES-3026(config-if)#power inline maximum allocation 8000
ES-3026(config-if)#
```

power inline priority

This command sets the power priority for specific ports. Use the **no** form to restore the default setting.

SYNTAX

power inline priority *priority*
no power inline priority

priority - The power priority for the port.
Options: 1 (critical), 2 (high), or 3 (low)

DEFAULT SETTING

3 (low)

COMMAND MODE

Interface Configuration

COMMAND USAGE

- If the power demand from devices connected to the switch exceeds the power budget setting as determined during bootup, the switch uses port power priority settings to control the supplied power. For example:
  - A device connected to a low-priority port that causes the switch to exceed its budget is not supplied power.
  - If a device is connected to a critical or high-priority port and causes the switch to exceed its budget, port power is still be turned on if the switch can drop power to one or more lower-priority ports and keep within its budget.

    Power will be dropped from low-priority ports in sequence starting from port number 1.
  - If sufficient power cannot be freed up for a critical or high-priority port by turning off power to lower-priority ports, power will not be supplied to the newly connected device.
- If a device is connected to a port after the switch has finished booting up and would cause the switch to exceed its budget, power will not be provided to that port regardless of its priority setting.

EXAMPLE

```
ES-3026(config)#interface ethernet 1/1
ES-3026(config-if)#power inline priority 2
ES-3026(config-if)#
```

show power inline status

This command displays the current power status for all ports or for specific ports.

SYNTAX

show power inline status [*interface*]

interface

ethernet

unit - Unit identifier. (Range: 1)

port - Port number. (Range: 1-24)

COMMAND MODE

Privileged Exec

EXAMPLE

```
ES-3026#show power inline status
Unit: 1
Compatible  mode : Enabled
                            Max       Used
Interface  Admin     Oper  Power     Power     Priority
---------  --------  ----  --------  --------  --------
Eth  1/ 1  Enabled   Off   30000 mW      0 mW  Low
Eth  1/ 2  Enabled   Off   30000 mW      0 mW  Low
Eth  1/ 3  Enabled   Off   30000 mW   7505 mW  Low
Eth  1/ 4  Enabled   Off   30000 mW      0 mW  Low
Eth  1/ 5  Enabled   Off   30000 mW      0 mW  Low
Eth  1/ 6  Enabled   Off   30000 mW      0 mW  Low
Eth  1/ 7  Enabled   Off   15400 mW   8597 mW  Low
Eth  1/ 8  Enabled   Off   15400 mW      0 mW  Low
Eth  1/ 9  Enabled   Off   15400 mW      0 mW  Low
Eth  1/10  Enabled   Off   15400 mW      0 mW  Low
Eth  1/11  Enabled   Off   15400 mW      0 mW  Low
Eth  1/12  Enabled   Off   15400 mW      0 mW  Low
⋮
```

Table 93: **show power inline status** - display description

Field	Description
Admin	The power mode set on the port (see power inline)
Oper	The current operating power status (displays on or off)
Power (mWatt)	The maximum power allocated to this port (see power inline maximum allocation)
Power (used)	The current power consumption on the port in milliwatts
Priority	The port's power priority setting (see power inline priority)

show power mainpower

Use this command to display the current power status for the switch.

COMMAND MODE

Privileged Exec

EXAMPLE

```
ES-3026#show power mainpower
Unit 1 Main Power Status
 Maximum Available Power : 195 watts
 System Operation Status : on
 PoE Power Consumption   : 0 watts
 Software Version        : Version 0x0068, Build 0x00
ES-3026#
```

Table 94: **show power mainpower** - display description

Field	Description
Maximum Available Power	The available power budget for the switch
System Operation Status	The current operating power status (displays on or off)
PoE Power Consumption	The current power consumption on the switch in watts
Software Version	The version of software running on the PoE controller subsystem in the switch.

30 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 95: Port Mirroring Commands

Command	Function
Local Port Mirroring	Mirrors data to another port for analysis without affecting the data passing through or the performance of the monitored port
RSPAN Mirroring	Mirrors data from remote switches over a dedicated VLAN

LOCAL PORT MIRRORING COMMANDS

This section describes how to mirror traffic from a source port to a target port.

Table 96: 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**] | **vlan** *vlan-id* | **mac-address** *mac-address*}

no port monitor *interface*

interface - **ethernet** *unit*/*port* (source port)

unit - Unit identifier. (Range: 1)

port - Port number. (ES-3026/P: 1-26, ES-3024G/P: 1-24)

rx - Mirror received packets.

tx - Mirror transmitted packets.

both - Mirror both received and transmitted packets.

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

mac-address - MAC address in the form of xx-xx-xx-xx-xx-xx or xxxxxxxxxxxx.

DEFAULT SETTING

- No mirror session is defined.
- When enabled for an interface, default mirroring is for both received and transmitted packets.
- When enabled for a VLAN or a MAC address, mirroring is restricted to received packets.

COMMAND MODE

Interface Configuration (Ethernet, destination port)

COMMAND USAGE

- You can mirror traffic from any source port to a destination port for real-time analysis. You can then attach a logic analyzer or RMON probe to the destination port and study the traffic crossing the source port in a completely unobtrusive manner.
- Set the destination port by specifying an Ethernet interface with the interface configuration command, and then use the **port monitor** command to specify the source of the traffic to mirror.
- When mirroring traffic from a port, the mirror port and monitor port speeds should match, otherwise traffic may be dropped from the monitor port. When mirroring traffic from a VLAN, traffic may also be dropped under heavy loads.
- When VLAN mirroring and port mirroring are both enabled, the target port can receive a mirrored packet twice; once from the source mirror port and again from the source mirror VLAN.
- When mirroring traffic from a MAC address, ingress traffic with the specified source address entering any port in the switch, other than the target port, will be mirrored to the destination 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:

```
ES-3026(config)#interface ethernet 1/11
ES-3026(config-if)#port monitor ethernet 1/6 both
ES-3026(config-if)#
```

show port monitor

This command displays mirror information.

SYNTAX

show port monitor [*interface*]

interface - **ethernet** *unit*/*port* (source port)

unit - Unit identifier. (Range: 1)

port - Port number. (ES-3026/P: 1-26, ES-3024G/P: 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:

```
ES-3026(config)#interface ethernet 1/11
ES-3026(config-if)#port monitor ethernet 1/6
ES-3026(config-if)#end
ES-3026#show port monitor
Port Mirroring
-------------------------------------
 Destination Port (listen port):Eth1/1
 Source Port (monitored port)  :Eth1/6
 Mode                          :RX/TX
ES-3026#
```

RSPAN MIRRORING COMMANDS

Remote Switched Port Analyzer (RSPAN) allows you to mirror traffic from remote switches for analysis on a local destination port.

Table 97: RSPAN Commands

Command	Function	Mode
vlan rspan	Creates a VLAN dedicated to carrying RSPAN traffic	VC
rspan source	Specifies the source port and traffic type to be mirrored	GC
rspan destination	Specifies the destination port to monitor the mirrored traffic	GC
rspan remote vlan	Specifies the RSPAN VLAN, switch role (source, intermediate or destination), and the uplink ports	GC

Table 97: RSPAN Commands (Continued)

Command	Function	Mode
no rspan session	Deletes a configured RSPAN session	GC
show rspan	Displays the configuration settings for an RSPAN session	PE

Configuration Guidelines

Take the following steps to configure an RSPAN session:

1. Use the vlan rspan command to configure a VLAN to use for RSPAN. (Default VLAN 1 and switch cluster VLAN 4093 are prohibited.)

2. Use the rspan source command to specify the interfaces and the traffic type (RX, TX or both) to be monitored.

3. Use the rspan destination command to specify the destination port for the traffic mirrored by an RSPAN session.

4. Use the rspan remote vlan command to specify the VLAN to be used for an RSPAN session, to specify the switch's role as a source, intermediate relay, or destination of the mirrored traffic, and to configure the uplink ports designated to carry this traffic.

RSPAN Limitations

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

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

- *Local/Remote Mirror* – The destination of a local mirror session (created with the port monitor command) cannot be used as the destination for RSPAN traffic.

  Only two mirror sessions are allowed. Both sessions can be allocated to remote mirroring, unless local mirroring is enabled (which is limited to a single session).

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

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

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

be configured. When RSPAN uplink ports are enabled on the switch, 802.1X cannot be enabled globally.

RSPAN uplink ports cannot be configured to use IEEE 802.1X Port Authentication, but RSPAN source ports and destination ports can be configured to use it

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

rspan source

Use this command to specify the source port and traffic type to be mirrored remotely. Use the **no** form to disable RSPAN on the specified port, or with a traffic type keyword to disable mirroring for the specified type.

SYNTAX

[**no**] **rspan session** *session-id* **source interface** *interface-list* [**rx** | **tx** | **both**]

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

Only two mirror sessions are allowed, including both local and remote mirroring. If local mirroring is enabled with the port monitor command, then there is only one session available for RSPAN.

interface-list – One or more source ports. Use a hyphen to indicate a consecutive list of ports or a comma between non-consecutive ports.

ethernet *unit*/*port*

unit - Unit identifier. (Range: 1)

port - Port number. (ES-3026/P: 1-26, ES-3024G/P: 1-24)

rx - Mirror received packets.

tx - Mirror transmitted packets.

both - Mirror both received and transmitted packets.

DEFAULT SETTING

Both TX and RX traffic is mirrored

COMMAND MODE

Global Configuration

COMMAND USAGE

- One or more source ports can be assigned to the same RSPAN session, either on the same switch or on different switches.
- Only ports can be configured as an RSPAN source – static and dynamic trunks are not allowed.

- The source port and destination port cannot be configured on the same switch.

EXAMPLE

The following example configures the switch to mirror received packets from port 2 and 3:

```
ES-3026(config)#rspan session 1 source interface ethernet 1/2
ES-3026(config)#rspan session 1 source interface ethernet 1/3
ES-3026(config)#
```

rspan destination

Use this command to specify the destination port to monitor the mirrored traffic. Use the **no** form to disable RSPAN on the specified port.

SYNTAX

rspan session *session-id* **destination interface** *interface* [**tagged** | **untagged**]

no rspan session *session-id* **destination interface** *interface*

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

Only two mirror sessions are allowed, including both local and remote mirroring. If local mirroring is enabled with the port monitor command, then there is only one session available for RSPAN.

interface - **ethernet** *unit/port*

unit - Unit identifier. (Range: 1)

port - Port number. (ES-3026/P: 1-26, ES-3024G/P: 1-24)

tagged - Traffic exiting the destination port carries the RSPAN VLAN tag.

untagged - Traffic exiting the destination port is untagged.

DEFAULT SETTING

Traffic exiting the destination port is untagged.

COMMAND MODE

Global Configuration

COMMAND USAGE

- Only one destination port can be configured on the same switch per session, but a destination port can be configured on more than one switch for the same session.
- Only ports can be configured as an RSPAN destination – static and dynamic trunks are not allowed.
- The source port and destination port cannot be configured on the same switch.

- A destination port can still send and receive switched traffic, and participate in any Layer 2 protocols to which it has been assigned.

EXAMPLE

The following example configures port 4 to receive mirrored RSPAN traffic:

```
ES-3026(config)#rspan session 1 destination interface ethernet 1/2
ES-3026(config)#
```

rspan remote vlan

Use this command to specify the RSPAN VLAN, switch role (source, intermediate or destination), and the uplink ports. Use the **no** form to disable the RSPAN on the specified VLAN.

SYNTAX

[**no**] **rspan session** *session-id* **remote vlan** *vlan-id* {**source** | **intermediate** | **destination**} **uplink** *interface*

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

Only two mirror sessions are allowed, including both local and remote mirroring. If local mirroring is enabled with the port monitor command, then there is only one session available for RSPAN.

vlan-id - ID of configured RSPAN VLAN. (Range: 2-4092, 4094) Use the vlan rspan command to reserve a VLAN for RSPAN mirroring before enabling RSPAN with this command.

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

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

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

uplink - A port configured to receive or transmit remotely mirrored traffic.

interface - **ethernet** *unit*/*port*

ethernet *unit*/*port*

unit - Unit identifier. (Range: 1)

port - Port number. (ES-3026/P: 1-26, ES-3024G/P: 1-24)

DEFAULT SETTING

None

COMMAND MODE

Global Configuration

COMMAND USAGE

- Only 802.1Q trunk or hybrid (i.e., general use) ports can be configured as an RSPAN uplink port – access ports are not allowed (see switchport mode).
- Only one uplink port can be configured on a source switch, but there is no limitation on the number of uplink ports configured on an intermediate or destination switch.
- Only destination and uplink ports will be assigned by the switch as members of this VLAN. Ports cannot be manually assigned to an RSPAN VLAN with the switchport allowed vlan command. Nor can GVRP dynamically add port members to an RSPAN VLAN. Also, note that the show vlan command will not display any members for an RSPAN VLAN, but will only show configured RSPAN VLAN identifiers.

EXAMPLE

The following example enables RSPAN on VLAN 2, specifies this device as an RSPAN destination switch, and the uplink interface as port 3:

```
ES-3026(config)#rspan session 1 remote vlan 2 destination uplink ethernet 1/3
ES-3026(config)#
```

no rspan session

Use this command to delete a configured RSPAN session.

SYNTAX

no rspan session *session-id*

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

Only two mirror sessions are allowed, including both local and remote mirroring. If local mirroring is enabled with the port monitor command, then there is only one session available for RSPAN.

COMMAND MODE

Global Configuration

COMMAND USAGE

The **no rspan session** command must be used to disable an RSPAN VLAN before it can be deleted from the VLAN database (see the vlan command).

EXAMPLE

```
ES-3026(config)#no rspan session 1
ES-3026(config)#
```

show rspan

Use this command to displays the configuration settings for an RSPAN session.

SYNTAX

show rspan session [*session-id*]

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

Only two mirror sessions are allowed, including both local and remote mirroring. If local mirroring is enabled with the port monitor command, then there is only one session available for RSPAN.

COMMAND MODE

Privileged Exec

EXAMPLE

```
ES-3026#show rspan session
RSPAN Session ID                 : 1
Source Ports (mirrored ports)    : None
  RX Only                        : None
  TX Only                        : None
  BOTH                           : None
Destination Port (monitor port) : Eth 1/2
Destination Tagged Mode          : Untagged
Switch Role                      : Destination
RSPAN VLAN                       : 2
RSPAN Uplink Ports               : Eth 1/3
Operation Status                 : Up
ES-3026#
```

31 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. 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 98: 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: 1-100 Mbps for Fast Ethernet ports,
1-1000 Mbps for Gigabit Ethernet ports)

DEFAULT SETTING

Fast Ethernet: 100 Mbps
Gigabit Ethernet: 1000 Mbps

COMMAND MODE

Interface Configuration (Ethernet)

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 Fast Ethernet 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

```
ES-3026(config)#interface ethernet 1/1
ES-3026(config-if)#rate-limit input 64
ES-3026(config-if)#
```

RELATED COMMAND

show interfaces switchport (689)

32 AUTOMATIC TRAFFIC CONTROL COMMANDS

Automatic Traffic Control (ATC) configures bounding thresholds for broadcast and multicast storms which can be used to trigger configured rate limits or to shut down a port.

Table 99: ATC Commands

Command	Function	Mode
Threshold Commands		
auto-traffic-control apply-timer	Sets the time at which to apply the control response after ingress traffic has exceeded the upper threshold	GC
auto-traffic-control release-timer	Sets the time at which to release the control response after ingress traffic has fallen beneath the lower threshold	GC
auto-traffic-control*	Enables automatic traffic control for broadcast or multicast storms	IC (Port)
auto-traffic-control action	Sets the control action to limit ingress traffic or shut down the offending port	IC (Port)
auto-traffic-control alarm-clear-threshold	Sets the lower threshold for ingress traffic beneath which a cleared storm control trap is sent	IC (Port)
auto-traffic-control alarm-fire-threshold	Sets the upper threshold for ingress traffic beyond which a storm control response is triggered after the apply timer expires	IC (Port)
auto-traffic-control control-release	Manually releases a control response	IC (Port)
auto-traffic-control auto-control-release	Automatically releases a control response	PE
SNMP Trap Commands		
snmp-server enable port-traps atc broadcast-alarm-clear	Sends a trap when broadcast traffic falls beneath the lower threshold after a storm control response has been triggered	IC (Port)
snmp-server enable port-traps atc broadcast-alarm-fire	Sends a trap when broadcast traffic exceeds the upper threshold for automatic storm control	IC (Port)
snmp-server enable port-traps atc broadcast-control-apply	Sends a trap when broadcast traffic exceeds the upper threshold for automatic storm control and the apply timer expires	IC (Port)
snmp-server enable port-traps atc broadcast-control-release	Sends a trap when broadcast traffic falls beneath the lower threshold after a storm control response has been triggered and the release timer expires	IC (Port)
snmp-server enable port-traps atc multicast-alarm-clear	Sends a trap when multicast traffic falls beneath the lower threshold after a storm control response has been triggered	IC (Port)
snmp-server enable port-traps atc multicast-alarm-fire	Sends a trap when multicast traffic exceeds the upper threshold for automatic storm control	IC (Port)

Table 99: ATC Commands (Continued)

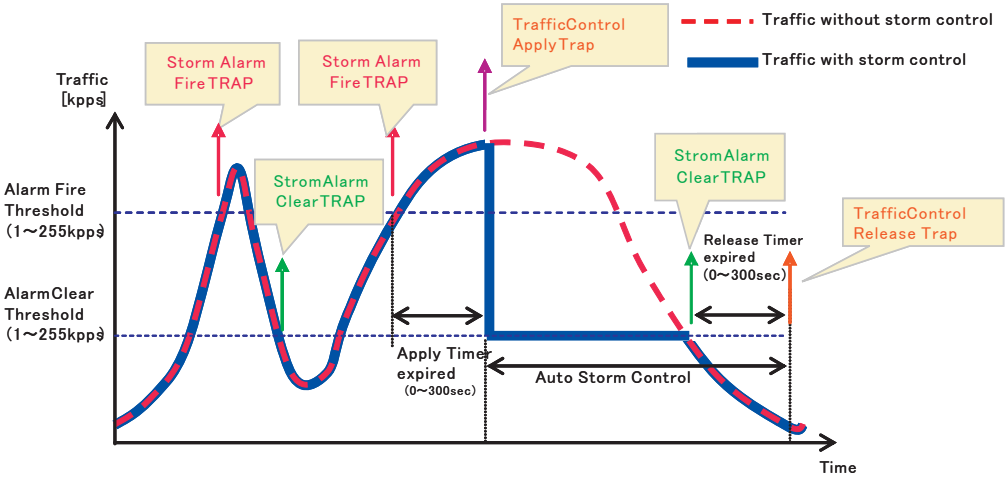
Command	Function	Mode
snmp-server enable port-traps atc multicast-control-apply	Sends a trap when multicast traffic exceeds the upper threshold for automatic storm control and the apply timer expires	IC (Port)
snmp-server enable port-traps atc multicast-control-release	Sends a trap when multicast traffic falls beneath the lower threshold after a storm control response has been triggered and the release timer expires	IC (Port)
ATC Display Commands		
show auto-traffic-control	Shows global configuration settings for automatic storm control	PE
show auto-traffic-control interface	Shows interface configuration settings and storm control status for the specified port	PE

* Enabling automatic storm control on a port will disable hardware-level storm control on the same port if configured by the switchport packet-rate command.

USAGE GUIDELINES

ATC includes storm control for broadcast or multicast traffic. The control response for either of these traffic types is the same, as shown in the following diagrams.

Storm control by limiting the traffic rate:



The key elements of this diagram are described below:

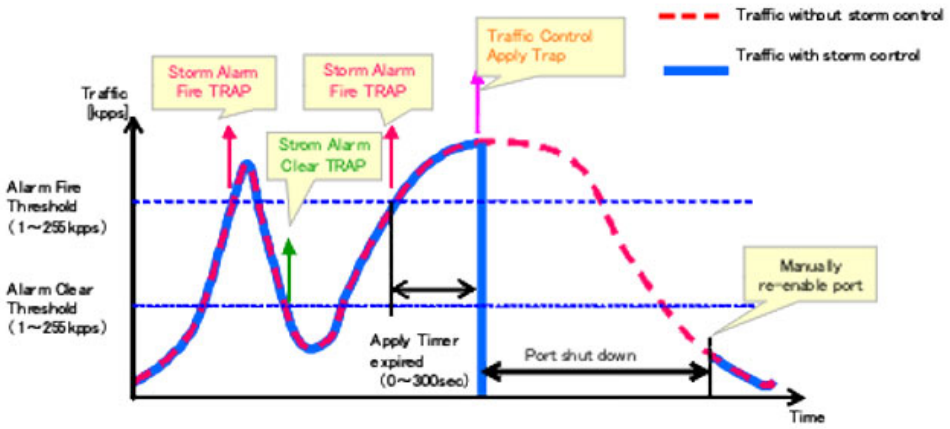
- Alarm Fire Threshold – The highest acceptable traffic rate. When ingress traffic exceeds the threshold, ATC sends a Storm Alarm Fire Trap and logs it.
- When traffic exceeds the alarm fire threshold and the apply timer expires, a traffic control response is applied, and a Traffic Control Apply Trap is sent and logged.
- Alarm Clear Threshold – The lower threshold beneath which an control response can be automatically terminated after the release timer

expires. When ingress traffic falls below this threshold, ATC sends a Storm Alarm Clear Trap and logs it.

- When traffic falls below the alarm clear threshold after the release timer expires, traffic control will be stopped and a Traffic Control Release Trap sent and logged.

- The traffic control response of rate limiting can be released automatically or manually. The control response of shutting down a port can only be released manually.

Storm control by shutting down a port:



The key elements of this diagram are the same as that described in the preceding diagram, except that automatic release of the control response is not provided. When traffic control is applied, you must manually re-enable the port.

FUNCTIONAL LIMITATIONS

Automatic storm control is a software level control function. Traffic storms can also be controlled at the hardware level using the switchport packet-rate command. However, only one of these control types can be applied to a port. Enabling automatic storm control on a port will disable hardware-level storm control on that port.

auto-traffic-control apply-timer

This command sets the time at which to apply the control response after ingress traffic has exceeded the upper threshold. Use the **no** form to restore the default setting.

SYNTAX

auto-traffic-control {**broadcast** | **multicast**} **apply-timer** *seconds*

no auto-traffic-control {**broadcast** | **multicast**} **apply-timer**

broadcast - Specifies automatic storm control for broadcast traffic.

multicast - Specifies automatic storm control for multicast traffic.

seconds - The interval after the upper threshold has been exceeded at which to apply the control response. (Range: 1-300 seconds)

DEFAULT SETTING

300 seconds

COMMAND MODE

Global Configuration

COMMAND USAGE

After the apply timer expires, a control action may be triggered as specified by the auto-traffic-control action command and a trap message sent as specified by the snmp-server enable port-traps atc broadcast-control-apply command or snmp-server enable port-traps atc multicast-control-apply command.

EXAMPLE

This example sets the apply timer to 200 seconds for all ports.

```
ES-3026(config)#auto-traffic-control broadcast apply-timer 200
ES-3026(config)#
```

auto-traffic-control release-timer

This command sets the time at which to release the control response after ingress traffic has fallen beneath the lower threshold. Use the **no** form to restore the default setting.

SYNTAX

auto-traffic-control {**broadcast** | **multicast**} **release-timer** *seconds*

no auto-traffic-control {**broadcast** | **multicast**} **release-timer**

broadcast - Specifies automatic storm control for broadcast traffic.

multicast - Specifies automatic storm control for multicast traffic.

seconds - The time at which to release the control response after ingress traffic has fallen beneath the lower threshold. (Range: 1-900 seconds)

DEFAULT SETTING
900 seconds

COMMAND MODE
Global Configuration

COMMAND USAGE
This command sets the delay after which the control response can be terminated. The auto-traffic-control auto-control-release command must be used to enable or disable the automatic release.

EXAMPLE
This example sets the release timer to 800 seconds for all ports.

```
ES-3026(config)#auto-traffic-control broadcast release-timer 800
ES-3026(config)#
```

auto-traffic-control

This command enables automatic traffic control for broadcast or multicast storms. Use the **no** form to disable this feature.

SYNTAX

[**no**] **auto-traffic-control** {**broadcast** | **multicast**}

broadcast - Specifies automatic storm control for broadcast traffic.

multicast - Specifies automatic storm control for multicast traffic.

DEFAULT SETTING
Disabled

COMMAND MODE
Interface Configuration (Ethernet)

COMMAND USAGE
- Automatic storm control can be enabled for either broadcast or multicast traffic. It cannot be enabled for both of these traffic types at the same time.
- Automatic storm control is a software level control function. Traffic storms can also be controlled at the hardware level using the switchport packet-rate command. However, only one of these control types can be applied to a port. Enabling automatic storm control on a port will disable hardware-level storm control on that port.

EXAMPLE

This example enables automatic storm control for broadcast traffic on port 1.

```
ES-3026(config)#interface ethernet 1/1
ES-3026(config-if)#auto-traffic-control broadcast
ES-3026(config-if)#
```

auto-traffic-control action

This command sets the control action to limit ingress traffic or shut down the offending port. Use the **no** form to restore the default setting.

SYNTAX

auto-traffic-control {**broadcast** | **multicast**}
action {**rate-control** | **shutdown**}

no auto-traffic-control {**broadcast** | **multicast**} **action**

broadcast - Specifies automatic storm control for broadcast traffic.

multicast - Specifies automatic storm control for multicast traffic.

rate-control - If a control response is triggered, the rate of ingress traffic is limited based on the threshold configured by the auto-traffic-control alarm-clear-threshold command.

shutdown - If a control response is triggered, the port is administratively disabled. A port disabled by automatic traffic control can only be manually re-enabled.

DEFAULT SETTING

rate-control

COMMAND MODE

Interface Configuration (Ethernet)

COMMAND USAGE

- When the upper threshold is exceeded and the apply timer expires, a control response will be triggered based on this command.
- When the control response is set to rate limiting by this command, the rate limits are determined by the auto-traffic-control alarm-clear-threshold command.
- If the control response is to limit the rate of ingress traffic, it can be automatically terminated once the traffic rate has fallen beneath the lower threshold and the release timer has expired.
- If a port has been shut down by a control response, it will not be re-enabled by automatic traffic control. It can only be manually re-enabled using the auto-traffic-control control-release command.

EXAMPLE

This example sets the control response for broadcast traffic on port 1.

```
ES-3026(config)#interface ethernet 1/1
ES-3026(config-if)#auto-traffic-control broadcast action shutdown
ES-3026(config-if)#
```

auto-traffic-control alarm-clear-threshold

This command sets the lower threshold for ingress traffic beneath which a cleared storm control trap is sent. Use the **no** form to restore the default setting.

SYNTAX

auto-traffic-control {**broadcast** | **multicast**} **alarm-clear-threshold** *threshold*

no auto-traffic-control {**broadcast** | **multicast**} **alarm-clear-threshold**

broadcast - Specifies automatic storm control for broadcast traffic.

multicast - Specifies automatic storm control for multicast traffic.

threshold - The lower threshold for ingress traffic beneath which a cleared storm control trap is sent. (Range: 1-255 kilo-packets per second seconds)

DEFAULT SETTING

128 kilo-packets per seconds

COMMAND MODE

Interface Configuration (Ethernet)

COMMAND USAGE

- Once the traffic rate falls beneath the lower threshold, a trap message may be sent if configured by the snmp-server enable port-traps atc broadcast-alarm-clear command or snmp-server enable port-traps atc multicast-alarm-clear command.

- If rate limiting has been configured as a control response, it will discontinued after the traffic rate has fallen beneath the lower threshold, and the release timer has expired. Note that if a port has been shut down by a control response, it will not be re-enabled by automatic traffic control. It can only be manually re-enabled using the auto-traffic-control control-release command.

EXAMPLE

This example sets the clear threshold for automatic storm control for broadcast traffic on port 1.

```
ES-3026(config)#interface ethernet 1/1
ES-3026(config-if)#auto-traffic-control broadcast alarm-clear-threshold 155
ES-3026(config-if)#
```

auto-traffic-control alarm-fire-threshold

This command sets the upper threshold for ingress traffic beyond which a storm control response is triggered after the apply timer expires. Use the **no** form to restore the default setting.

SYNTAX

auto-traffic-control {**broadcast** | **multicast**} **alarm-fire-threshold** *threshold*

no auto-traffic-control {**broadcast** | **multicast**} **alarm-fire-threshold**

broadcast - Specifies automatic storm control for broadcast traffic.

multicast - Specifies automatic storm control for multicast traffic.

threshold - The upper threshold for ingress traffic beyond which a storm control response is triggered after the apply timer expires. (Range: 1-255 kilo-packets per second seconds)

DEFAULT SETTING

128 kilo-packets per seconds

COMMAND MODE

Interface Configuration (Ethernet)

COMMAND USAGE

- Once the upper threshold is exceeded, a trap message may be sent if configured by the snmp-server enable port-traps atc broadcast-alarm-fire command or snmp-server enable port-traps atc multicast-alarm-fire command.
- After the upper threshold is exceeded, the control timer must first expire as configured by the auto-traffic-control apply-timer command before a control response is triggered if configured by the auto-traffic-control action command.

EXAMPLE

This example sets the trigger threshold for automatic storm control for broadcast traffic on port 1.

```
ES-3026(config)#interface ethernet 1/1
ES-3026(config-if)#auto-traffic-control broadcast alarm-fire-threshold 255
ES-3026(config-if)#
```

auto-traffic-control control-release

This command manually releases a control response.

SYNTAX

auto-traffic-control {**broadcast** | **multicast**} **control-release**

broadcast - Specifies automatic storm control for broadcast traffic.

multicast - Specifies automatic storm control for multicast traffic.

COMMAND MODE

Privileged Exec

COMMAND USAGE

This command can be used to manually stop a control response any time after the specified action has been triggered.

EXAMPLE

```
ES-3026#auto-traffic-control broadcast control-release interface ethernet 1/1
ES-3026#
```

auto-traffic-control auto-control-release

This command automatically releases a control response after the time specified in the auto-traffic-control release-timer command has expired.

SYNTAX

auto-traffic-control {**broadcast** | **multicast**} **auto-control-release**

broadcast - Specifies automatic storm control for broadcast traffic.

multicast - Specifies automatic storm control for multicast traffic.

COMMAND MODE

Interface Configuration (Ethernet)

COMMAND USAGE

This command can be used to automatically stop a control response after the specified action has been triggered and the release timer has expired.

EXAMPLE

```
ES-3026(config)#interface ethernet 1/1
ES-3026(config-if)#auto-traffic-control broadcast auto-control-release
ES-3026(config-if)#
```

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

This command sends a trap when broadcast traffic falls beneath the lower threshold after a storm control response has been triggered. Use the **no** form to disable this trap.

SYNTAX

[**no**] **snmp-server enable port-traps atc broadcast-alarm-clear**

DEFAULT SETTING

Disabled

COMMAND MODE

Interface Configuration (Ethernet)

EXAMPLE

```
ES-3026(config)#interface ethernet 1/1
ES-3026(config-if)#snmp-server enable port-traps atc broadcast-alarm-clear
ES-3026(config-if)#
```

RELATED COMMANDS

auto-traffic-control action (728)
auto-traffic-control alarm-clear-threshold (729)

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

This command sends a trap when broadcast traffic exceeds the upper threshold for automatic storm control. Use the **no** form to disable this trap.

SYNTAX

[**no**] **snmp-server enable port-traps atc broadcast-alarm-fire**

DEFAULT SETTING

Disabled

COMMAND MODE

Interface Configuration (Ethernet)

EXAMPLE

```
ES-3026(config)#interface ethernet 1/1
ES-3026(config-if)#snmp-server enable port-traps atc broadcast-alarm-fire
ES-3026(config-if)#
```

RELATED COMMANDS

auto-traffic-control alarm-fire-threshold (730)

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

This command sends a trap when broadcast traffic exceeds the upper threshold for automatic storm control and the apply timer expires. Use the **no** form to disable this trap.

SYNTAX

[**no**] **snmp-server enable port-traps atc broadcast-control-apply**

DEFAULT SETTING

Disabled

COMMAND MODE

Interface Configuration (Ethernet)

EXAMPLE

```
ES-3026(config)#interface ethernet 1/1
ES-3026(config-if)#snmp-server enable port-traps atc broadcast-control-apply
ES-3026(config-if)#
```

RELATED COMMANDS

auto-traffic-control alarm-fire-threshold (730)
auto-traffic-control apply-timer (726)

snmp-server enable port-traps atc broadcast-control-release

This command sends a trap when broadcast traffic falls beneath the lower threshold after a storm control response has been triggered and the release timer expires. Use the **no** form to disable this trap.

SYNTAX

[**no**] **snmp-server enable port-traps atc broadcast-control-release**

DEFAULT SETTING

Disabled

COMMAND MODE

Interface Configuration (Ethernet)

EXAMPLE

```
ES-3026(config)#interface ethernet 1/1
ES-3026(config-if)#snmp-server enable port-traps atc broadcast-control-
  release
ES-3026(config-if)#
```

RELATED COMMANDS

auto-traffic-control alarm-clear-threshold (729)
auto-traffic-control action (728)
auto-traffic-control release-timer (726)

snmp-server enable port-traps atc multicast-alarm-clear

This command sends a trap when multicast traffic falls beneath the lower threshold after a storm control response has been triggered. Use the **no** form to disable this trap.

SYNTAX

[**no**] **snmp-server enable port-traps atc multicast-alarm-clear**

DEFAULT SETTING

Disabled

COMMAND MODE

Interface Configuration (Ethernet)

EXAMPLE

```
ES-3026(config)#interface ethernet 1/1
ES-3026(config-if)#snmp-server enable port-traps atc multicast-alarm-clear
ES-3026(config-if)#
```

RELATED COMMANDS

auto-traffic-control action (728)
auto-traffic-control alarm-clear-threshold (729)

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

This command sends a trap when multicast traffic exceeds the upper threshold for automatic storm control. Use the **no** form to disable this trap.

SYNTAX

[**no**] **snmp-server enable port-traps atc multicast-alarm-fire**

DEFAULT SETTING

Disabled

COMMAND MODE

Interface Configuration (Ethernet)

EXAMPLE

```
ES-3026(config)#interface ethernet 1/1
ES-3026(config-if)#snmp-server enable port-traps atc multicast-alarm-fire
ES-3026(config-if)#
```

RELATED COMMANDS

auto-traffic-control alarm-fire-threshold (730)

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

This command sends a trap when multicast traffic exceeds the upper threshold for automatic storm control and the apply timer expires. Use the **no** form to disable this trap.

SYNTAX

[**no**] **snmp-server enable port-traps atc multicast-control-apply**

DEFAULT SETTING

Disabled

COMMAND MODE

Interface Configuration (Ethernet)

EXAMPLE

```
ES-3026(config)#interface ethernet 1/1
ES-3026(config-if)#snmp-server enable port-traps atc multicast-control-apply
ES-3026(config-if)#
```

RELATED COMMANDS

auto-traffic-control alarm-fire-threshold (730)
auto-traffic-control apply-timer (726)

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

This command sends a trap when multicast traffic falls beneath the lower threshold after a storm control response has been triggered and the release timer expires. Use the **no** form to disable this trap.

SYNTAX

[**no**] **snmp-server enable port-traps atc multicast-control-release**

DEFAULT SETTING

Disabled

COMMAND MODE

Interface Configuration (Ethernet)

EXAMPLE

```
ES-3026(config)#interface ethernet 1/1
ES-3026(config-if)#snmp-server enable port-traps atc multicast-control-
  release
ES-3026(config-if)#
```

RELATED COMMANDS

auto-traffic-control alarm-clear-threshold (729)
auto-traffic-control action (728)
auto-traffic-control release-timer (726)

show auto-traffic-control

This command shows global configuration settings for automatic storm control.

COMMAND MODE

Privileged Exec

EXAMPLE

```
ES-3026#show auto-traffic-control

Storm-control: Broadcast
 Apply-timer (sec)   : 300
 release-timer (sec) : 900

Storm-control: Multicast
 Apply-timer(sec)    : 300
 release-timer(sec)  : 900
ES-3026#
```

show auto-traffic-control interface

This command shows interface configuration settings and storm control status for the specified port.

SYNTAX

show auto-traffic-control interface [*interface*]

interface

ethernet *unit*/*port*

unit - Unit identifier. (Range: 1)

port - Port number. (ES-3026/P: 1-26, ES-3024G/P: 1-24)

COMMAND MODE

Privileged Exec

EXAMPLE

```
ES-3026#show auto-traffic-control interface ethernet 1/1
Eth 1/1 Information
----------------------------------------------------------------------
Storm Control:              Broadcast                    Multicast
State:                      Disabled                     Disabled
Action:                     rate-control                 rate-control
Auto Release Control:       Disabled                     Disabled
Alarm Fire Threshold(Kpps): 128                          128
Alarm Clear Threshold(Kpps):128                          128
Trap Storm Fire:            Disabled                     Disabled
Trap Storm Clear:           Disabled                     Disabled
Trap Traffic Apply:         Disabled                     Disabled
Trap Traffic Release:       Disabled                     Disabled
----------------------------------------------------------------------

ES-3026#
```

33 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 100: 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

```
ES-3026(config)#mac-address-table aging-time 100
ES-3026(config)#
```

mac-address-table static

This command maps a static address to a destination port in a VLAN. Use the **no** form to remove an address.

SYNTAX

mac-address-table static *mac-address* **interface** *interface* **vlan** *vlan-id* [*action*]

no mac-address-table static *mac-address* **vlan** *vlan-id*

mac-address - MAC address.

interface

ethernet *unit*/*port*

unit - Unit identifier. (Range: 1)

port - Port number. (ES-3026/P: 1-26, ES-3024G/P: 1-24)

port-channel *channel-id* (Range: 1-12)

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

```
ES-3026(config)#mac-address-table static 00-e0-29-94-34-de interface ethernet
  1/1 vlan 1 delete-on-reset
ES-3026(config)#
```

clear mac-address-table dynamic

This command removes any learned entries from the forwarding database.

DEFAULT SETTING

None

COMMAND MODE

Privileged Exec

EXAMPLE

```
ES-3026#clear mac-address-table dynamic
ES-3026#
```

show mac-address-table

This command shows classes of entries in the bridge-forwarding database.

SYNTAX

show mac-address-table [**address** *mac-address* [*mask*]]
[**interface** *interface*] [**vlan** *vlan-id*]
[**sort** {**address** | **vlan** | **interface**}]

mac-address - MAC address.

mask - Bits to match in the address.

interface

ethernet *unit*/*port*

unit - Unit identifier. (Range: 1)

port - Port number. (ES-3026/P: 1-26, ES-3024G/P: 1-24)

port-channel *channel-id* (Range: 1-12)

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 16K.

EXAMPLE

```
ES-3026#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
ES-3026#
```

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

```
ES-3026#show mac-address-table aging-time
 Aging Status : Enabled
 Aging Time: 300 sec.
ES-3026#
```

34 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 101: 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 101: 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:

```
ES-3026(config)#spanning-tree
ES-3026(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

```
ES-3026(config)#spanning-tree forward-time 20
ES-3026(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

```
ES-3026(config)#spanning-tree hello-time 5
ES-3026(config)#
```

RELATED COMMANDS

spanning-tree forward-time (743)
spanning-tree max-age (744)

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

```
ES-3026(config)#spanning-tree max-age 40
ES-3026(config)#
```

RELATED COMMANDS

spanning-tree forward-time (743)
spanning-tree hello-time (743)

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:

```
ES-3026(config)#spanning-tree mode rstp
ES-3026(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 753) takes precedence over port priority (page 759).

EXAMPLE

```
ES-3026(config)#spanning-tree pathcost method long
ES-3026(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

```
ES-3026(config)#spanning-tree priority 40000
ES-3026(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

```
ES-3026(config)#spanning-tree mst configuration
ES-3026(config-mstp)#
```

RELATED COMMANDS

mst vlan (750)
mst priority (749)
name (750)

revision (751)
max-hops (748)

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

```
ES-3026(config)#spanning-tree transmission-limit 4
ES-3026(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

```
ES-3026(config-mstp)#max-hops 30
ES-3026(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

```
ES-3026(config-mstp)#mst 1 priority 4096
ES-3026(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 58 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 750) 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

```
ES-3026(config-mstp)#mst 1 vlan 2-5
ES-3026(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 751) 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

```
ES-3026(config-mstp)#name R&D
ES-3026(config-mstp)#
```

RELATED COMMANDS
revision (751)

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 750) 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

```
ES-3026(config-mstp)#revision 1
ES-3026(config-mstp)#
```

RELATED COMMANDS
name (750)

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

```
ES-3026(config)#interface ethernet ethernet 1/5
ES-3026(config-if)#spanning-tree edge-port
ES-3026(config-if)#spanning-tree bpdu-filter
ES-3026(config-if)#
```

RELATED COMMANDS

spanning-tree edge-port (754)

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

```
ES-3026(config)#interface ethernet ethernet 1/5
ES-3026(config-if)#spanning-tree edge-port
ES-3026(config-if)#spanning-tree bpdu-guard
ES-3026(config-if)#
```

RELATED COMMANDS

spanning-tree edge-port (754)
spanning-tree spanning-disabled (761)

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[12], 1-200,000,000 for long path cost method)

Table 102: Recommended STA Path Cost Range

Port Type	IEEE 802.1D-1998	IEEE 802.1w-2001
Fast Ethernet	10-60	20,000-2,000,000
Gigabit Ethernet	3-10	2,000-200,000

Table 103: Recommended STA Path Cost

Port Type	Link Type	IEEE 802.1D-1998	IEEE 802.1w-2001
Fast Ethernet	Half Duplex	19	200,000
	Full Duplex	18	100,000
	Trunk	15	50,000
Gigabit Ethernet	Full Duplex	4	10,000
	Trunk	3	5,000

12. Use the spanning-tree pathcost method command on page 746 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 104: Default STA Path Costs

Port Type	Link Type	IEEE 802.1w-2001
Fast Ethernet	Half Duplex Full Duplex Trunk	200,000 100,000 50,000
Gigabit Ethernet	Full Duplex Trunk	10,000 5,000

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 746) is set to short, the maximum value for path cost is 65,535.

EXAMPLE

```
ES-3026(config)#interface ethernet 1/5
ES-3026(config-if)#spanning-tree cost 50
ES-3026(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

```
ES-3026(config)#interface ethernet 1/5
ES-3026(config-if)#spanning-tree edge-port
ES-3026(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

```
ES-3026(config)#interface ethernet 1/5
ES-3026(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

```
ES-3026(config)#interface ethernet 1/5
ES-3026(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.

EXAMPLE
```
ES-3026(config)#interface ethernet 1/5
ES-3026(config-if)#spanning-tree loopback-detection release-mode manual
```

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
```
ES-3026(config)#interface ethernet ethernet 1/5
ES-3026(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[13], 1-200,000,000 for long path cost method)

The recommended path cost range is listed in Table 102 on page 753. The recommended path cost is listed in Table 103 on page 753.

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 104 on page 754.

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

```
ES-3026(config)#interface Ethernet 1/5
ES-3026(config-if)#spanning-tree mst 1 cost 50
ES-3026(config-if)#
```

RELATED COMMANDS

spanning-tree mst port-priority (759)

13. 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

```
ES-3026(config)#interface Ethernet 1/5
ES-3026(config-if)#spanning-tree mst 1 port-priority 0
ES-3026(config-if)#
```

RELATED COMMANDS

spanning-tree mst cost (758)

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

```
ES-3026(config)#interface ethernet 1/5
ES-3026(config-if)#spanning-tree port-priority 0
```

RELATED COMMANDS

spanning-tree cost (753)

spanning-tree root-guard

This command prevents a designated port[14] 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.

14. See Port Role under "Displaying Interface Settings for STA" on page 199.

EXAMPLE

```
ES-3026(config)#interface ethernet ethernet 1/5
ES-3026(config-if)#spanning-tree edge-port
ES-3026(config-if)#spanning-tree root-guard
ES-3026(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.

```
ES-3026(config)#interface ethernet 1/5
ES-3026(config-if)#spanning-tree spanning-disabled
ES-3026(config-if)#
```

spanning-tree loopback-detection release

This command manually releases a port placed in discarding state by loopback-detection.

SYNTAX

spanning-tree loopback-detection release *interface*

interface

ethernet *unit*/*port*

unit - Unit identifier. (Range: 1)

port - Port number. (EC-S4626F: 1-26, EC-S4650F: 1-50)

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 - Unit identifier. (Range: 1)

port - Port number. (ES-3026/P: 1-26, ES-3024G/P: 1-24)

port-channel *channel-id* (Range: 1-12)

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

```
ES-3026#spanning-tree protocol-migration eth 1/5
ES-3026#
```

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 - Unit identifier. (Range: 1)

port - Port number. (ES-3026/P: 1-26, ES-3024G/P: 1-24)

port-channel *channel-id* (Range: 1-12)

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 189. For a description of the items displayed for specific interfaces, see "Displaying Interface Settings for STA" on page 199.

EXAMPLE

```
ES-3026#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
 Admin Root Guard         : Disabled
 Oper Root Guard          : Disabled
 Spanning-Tree Status     : Enabled
.
.
.
```

show spanning-tree mst configuration

This command shows the configuration of the multiple spanning tree.

COMMAND MODE

Privileged Exec

EXAMPLE

```
ES-3026#show spanning-tree mst configuration
Mstp Configuration Information
-------------------------------------------------------------
 Configuration Name : R&D
 Revision Level     :0

 Instance VLANs
-------------------------------------------------------------
     0    1-4093
ES-3026#
```

35 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 105: 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 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 106: 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

```
ES-3026(config)#bridge-ext gvrp
ES-3026(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

```
ES-3026(config)#interface ethernet 1/1
ES-3026(config-if)#garp timer join 100
ES-3026(config-if)#
```

RELATED COMMANDS

show garp timer (769)

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:

```
ES-3026(config)#interface ethernet 1/1
ES-3026(config-if)#switchport forbidden vlan add 3
ES-3026(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

```
ES-3026(config)#interface ethernet 1/1
ES-3026(config-if)#switchport gvrp
ES-3026(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 90 for a description of the displayed items.

EXAMPLE

```
ES-3026#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
ES-3026#
```

show garp timer

This command shows the GARP timers for the selected interface.

SYNTAX

show garp timer [*interface*]

interface

ethernet *unit*/*port*

unit - Unit identifier. (Range: 1)

port - Port number. (ES-3026/P: 1-26, ES-3024G/P: 1-24)

port-channel *channel-id* (Range: 1-12)

DEFAULT SETTING

Shows all GARP timers.

COMMAND MODE

Normal Exec, Privileged Exec

EXAMPLE

```
ES-3026#show garp timer ethernet 1/1
Eth 1/ 1 GARP timer status:
 Join Timer:     20 centiseconds
 Leave Timer:    60 centiseconds
 Leaveall Timer: 1000 centiseconds
ES-3026#
```

RELATED COMMANDS

garp timer (767)

show gvrp configuration

This command shows if GVRP is enabled.

SYNTAX

show gvrp configuration [*interface*]

interface

ethernet *unit*/*port*

unit - Unit identifier. (Range: 1)

port - Port number. (ES-3026/P: 1-26, ES-3024G/P: 1-24)

port-channel *channel-id* (Range: 1-12)

DEFAULT SETTING

Shows both global and interface-specific configuration.

COMMAND MODE

Normal Exec, Privileged Exec

EXAMPLE

```
ES-3026#show gvrp configuration ethernet 1/7
Eth 1/ 7:
 GVRP Configuration : Disabled
ES-3026#
```

EDITING VLAN GROUPS

Table 107: 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

```
ES-3026(config)#vlan database
ES-3026(config-vlan)#
```

RELATED COMMANDS

show vlan (779)

vlan

This command configures a VLAN. Use the **no** form to restore the default settings or delete a VLAN.

SYNTAX

vlan *vlan-id* [**name** *vlan-name*] **media ethernet** [**state** {**active** | **suspend**}] [**rspan**]

no vlan *vlan-id* [**name** | **state**]

vlan-id - VLAN ID, specified as a single number, a range of consecutive numbers separated by a hyphen, or multiple numbers separated by commas. (Range: 1-4093, 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.

rspan - Keyword to create a VLAN used for mirroring traffic from remote switches. The VLAN used for RSPN cannot include

VLAN 1 (the switch's default VLAN), nor VLAN 4093 (the VLAN used for switch clustering). For more information on configuring RSPAN through the CLI, see "RSPAN Mirroring Commands" on page 713.

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.

NOTE: The switch allows 256 user-manageable VLANs.

EXAMPLE

The following example adds a VLAN, using VLAN ID 105 and name RD5. The VLAN is activated by default.

```
ES-3026(config)#vlan database
ES-3026(config-vlan)#vlan 105 name RD5 media ethernet
ES-3026(config-vlan)#
```

RELATED COMMANDS

show vlan (779)

CONFIGURING VLAN INTERFACES

Table 108: Commands for Configuring VLAN Interfaces

Command	Function	Mode
interface vlan	Enters interface configuration mode for a specified VLAN	IC
switchport acceptable-frame-types	Configures frame types to be accepted by an interface	IC
switchport allowed vlan	Configures the VLANs associated with an interface	IC
switchport forbidden vlan	Configures forbidden VLANs for an interface	IC
switchport gvrp	Enables GVRP for an interface	IC

Table 108: Commands for Configuring VLAN Interfaces (Continued)

Command	Function	Mode
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:

```
ES-3026(config)#interface vlan 1
ES-3026(config-if)#ip address 192.168.1.254 255.255.255.0
ES-3026(config-if)#
```

RELATED COMMANDS

shutdown (683)
interface (678)
vlan (771)

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:

```
ES-3026(config)#interface ethernet 1/1
ES-3026(config-if)#switchport acceptable-frame-types tagged
ES-3026(config-if)#
```

RELATED COMMANDS

switchport mode (776)

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:

```
ES-3026(config)#interface ethernet 1/1
ES-3026(config-if)#switchport allowed vlan add 1,2,5,6 tagged
ES-3026(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:

```
ES-3026(config)#interface ethernet 1/1
ES-3026(config-if)#switchport ingress-filtering
ES-3026(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 {**access** | **hybrid** | **trunk**}

no switchport mode

access - Specifies an access VLAN interface. The port transmits and receives untagged frames on a single VLAN only.

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 access mode with the PVID set to VLAN 1.

COMMAND MODE

Interface Configuration (Ethernet, Port Channel)

COMMAND USAGE

Access mode is mutually exclusive with VLAN trunking (see the vlan-trunking command). If VLAN trunking is enabled on an interface, then that interface cannot be set to access mode, and vice versa.

EXAMPLE

The following shows how to set the configuration mode to port 1, and then set the switchport mode to hybrid:

```
ES-3026(config)#interface ethernet 1/1
ES-3026(config-if)#switchport mode hybrid
ES-3026(config-if)#
```

RELATED COMMANDS

switchport acceptable-frame-types (774)

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

- When using Access mode, and an interface is assigned to a new VLAN, its PVID is automatically set to the identifier for that VLAN. When using Hybrid mode, the PVID for an interface can be set to any VLAN for which it is an untagged member.
- If acceptable frame types is set to **all** or switchport mode is set to **hybrid**, the PVID will be inserted into all untagged frames entering the ingress port.

EXAMPLE

The following example shows how to set the PVID for port 1 to VLAN 3:

```
ES-3026(config)#interface ethernet 1/1
ES-3026(config-if)#switchport native vlan 3
ES-3026(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

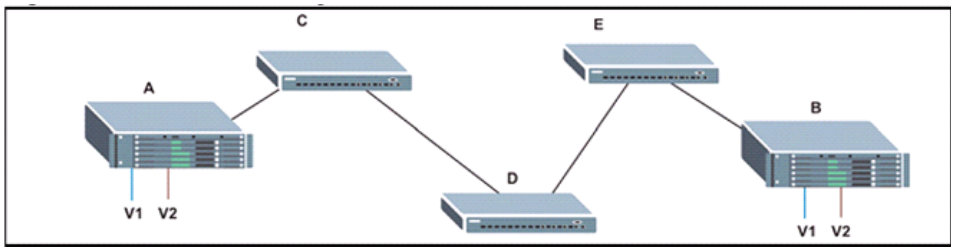
COMMAND MODE

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:

```
ES-3026(config)#interface ethernet 1/27
ES-3026(config-if)#vlan-trunking
ES-3026(config-if)#interface ethernet 1/28
ES-3026(config-if)#vlan-trunking
ES-3026(config-if)#
```

DISPLAYING VLAN INFORMATION

This section describes commands used to display VLAN information.

Table 109: 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:

```
ES-3026#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)
ES-3026#
```

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 110: 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

```
ES-3026(config)#dot1q-tunnel system-tunnel-control
ES-3026(config)#
```

RELATED COMMANDS

show dot1q-tunnel (783)
show interfaces switchport (689)

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

```
ES-3026(config)#interface ethernet 1/1
ES-3026(config-if)#switchport dot1q-tunnel mode access
ES-3026(config-if)#
```

RELATED COMMANDS

show dot1q-tunnel (783)
show interfaces switchport (689)

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

```
ES-3026(config)#interface ethernet 1/1
ES-3026(config-if)#switchport dot1q-tunnel tpid 9100
ES-3026(config-if)#
```

RELATED COMMANDS

show interfaces switchport (689)

show dot1q-tunnel

This command displays information about QinQ tunnel ports.

COMMAND MODE

Privileged Exec

EXAMPLE

```
ES-3026(config)#dot1q-tunnel system-tunnel-control
ES-3026(config)#interface ethernet 1/1
ES-3026(config-if)#switchport dot1q-tunnel mode access
```

```
ES-3026(config-if)#interface ethernet 1/2
ES-3026(config-if)#switchport dot1q-tunnel mode uplink
ES-3026(config-if)#end
ES-3026#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 (782)

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 111: 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.

```
ES-3026(config)#traffic-segmentation
ES-3026(config)#traffic-segmentation uplink ethernet 1/12
  downlink ethernet 1/5-8
ES-3026(config)#
```

show traffic-segmentation

This command displays the configured traffic segments.

COMMAND MODE

Privileged Exec

EXAMPLE

```
ES-3026#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
ES-3026#
```

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 112: 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 771). 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[15] - 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:

```
ES-3026(config)#protocol-vlan protocol-group 1 add frame-type ethernet
  protocol-type ip
ES-3026(config)#protocol-vlan protocol-group 1 add frame-type ethernet
  protocol-type arp
ES-3026(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.

15. 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.

```
ES-3026(config)#interface ethernet 1/1
ES-3026(config-if)#protocol-vlan protocol-group 1 vlan 2
ES-3026(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:

```
ES-3026#show protocol-vlan protocol-group

 Protocol Group ID   Frame Type    Protocol Type
------------------ ------------- ---------------
                 1      ethernet     08 00
ES-3026#
```

show interfaces protocol-vlan protocol-group

This command shows the mapping from protocol groups to VLANs for the selected interfaces.

SYNTAX

show interfaces protocol-vlan protocol-group [*interface*]

interface

ethernet *unit*/*port*

unit - Unit identifier. (Range: 1)

port - Port number. (ES-3026/P: 1-26, ES-3024G/P: 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:

```
ES-3026#show interfaces protocol-vlan protocol-group

   Port     ProtocolGroup ID    VLAN ID
---------- ------------------ -----------
   Eth 1/1                  1       vlan2
ES-3026#
```

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 113: 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.

```
ES-3026(config)#subnet-vlan subnet 192.168.12.192 255.255.255.224 vlan 4
ES-3026(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.

```
ES-3026#show subnet-vlan
    IP address           Mask        VLAN ID
---------------- ---------------- ---------
 192.168.12.0      255.255.255.128         2
 192.168.12.128    255.255.255.192         3
 192.168.12.192    255.255.255.224         4
 192.168.12.224    255.255.255.240         5
 192.168.12.240    255.255.255.248         6
 192.168.12.248    255.255.255.252         7
 192.168.12.252    255.255.255.254         8
 192.168.12.254    255.255.255.255         9
 192.168.12.255    255.255.255.255        10
ES-3026#
```

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 114: 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.

```
ES-3026(config)#mac-vlan mac-address 00-00-00-11-22-33 vlan 10
ES-3026(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.

```
ES-3026#show mac-vlan
    MAC address       VLAN ID
------------------- ---------
 00-00-00-11-22-33        10
ES-3026#
```

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 115: 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 115: 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.

```
ES-3026(config)#voice vlan 1234
ES-3026(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.

```
ES-3026(config)#voice vlan aging 3000
ES-3026(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.

```
ES-3026(config)#voice vlan mac-address 00-12-34-56-78-90 mask ff-ff-ff-00-00-
  00 description A new phone
ES-3026(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.

```
ES-3026(config)#interface ethernet 1/1
ES-3026(config-if)#switchport voice vlan auto
ES-3026(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.

```
ES-3026(config)#interface ethernet 1/1
ES-3026(config-if)#switchport voice vlan priority 5
ES-3026(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 867 for more information on LLDP.

EXAMPLE
The following example enables the OUI method on port 1 for detecting VoIP traffic.

```
ES-3026(config)#interface ethernet 1/1
ES-3026(config-if)#switchport voice vlan rule oui
ES-3026(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.

```
ES-3026(config)#interface ethernet 1/1
ES-3026(config-if)#switchport voice vlan security
ES-3026(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

```
ES-3026#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
-------- -------- -------- --------- --------
Eth 1/ 1 Auto     Enabled  OUI              6
Eth 1/ 2 Disabled Disabled OUI              6
Eth 1/ 3 Manual   Enabled  OUI              5
Eth 1/ 4 Auto     Enabled  OUI              6
Eth 1/ 5 Disabled Disabled OUI              6
Eth 1/ 6 Disabled Disabled OUI              6
Eth 1/ 7 Disabled Disabled OUI              6
Eth 1/ 8 Disabled Disabled OUI              6
Eth 1/ 9 Disabled Disabled OUI              6
Eth 1/10 Disabled Disabled OUI              6

ES-3026#show voice vlan oui
OUIAddress        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

ES-3026#
```

36 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 116: Priority Commands

Command Group	Function
Priority Commands (Layer 2)	Configures the queue mode, queue weights, and default priority for untagged frames
Priority Commands (Layer 3 and 4)	Sets the default priority processing method (CoS or DSCP), maps priority tags for internal processing, maps values from internal priority table to CoS values used in tagged egress packets for Layer 2 interfaces, maps internal per hop behavior to hardware queues

PRIORITY COMMANDS (LAYER 2)

This section describes commands used to configure Layer 2 traffic priority on the switch.

Table 117: Priority Commands (Layer 2)

Command	Function	Mode
queue mode	Sets the queue mode to Shaped Deficit Weighted Round-Robin (SDWRR), strict priority, or a combination of strict and weighted queuing	GC
queue weight	Assigns round-robin weights to the priority queues	GC
switchport priority default	Sets a port priority for incoming untagged frames	IC
show interfaces switchport	Displays the administrative and operational status of an interface	PE
show queue mode	Shows the current queue mode	PE
show queue weight	Shows weights assigned to the weighted queues	PE

queue mode

This command sets the scheduling mode used for processing each of the class of service (CoS) priority queues. The options include strict priority, Shaped Deficiit Weighted Round-Robin (SDWRR), 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 - Shaped Deficit 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 SDWRR 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

Strict and WRR, with Queue 3 using strict mode

COMMAND MODE

Global Configuration

COMMAND USAGE

- The switch can be set to service the port queues based on strict priority, SDWRR, 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.
- The SDWRR algorithm used by this switch is known as Shaped Deficit Weighted Round Robin (SDWRR).

  The basic WRR algorithm uses a 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.

  Deficit Weighted Round-Robin (DWRR) services the queues in a manner similar to WRR, but the next queue is serviced only when the queue's Deficit Counter becomes smaller than the packet size to be transmitted. As a result, traffic on queues with large weights cause increased latency and jitter for traffic waiting for scheduling on other queues. In SDWRR, if two or more queues have traffic eligible for transmission (i.e., the Deficit Counter is greater than the packet size to be transmitted), then a round-robin scheme among those queues is used, while still

preserving the overall weight ratios between the queues. This produces less jitter and lower maximum latency for traffic on all of the serviced queues.

- If Strict and SDWRR 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 SWDRR, 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:

```
ES-3026(config)#queue mode strict
ES-3026(config)#
```

RELATED COMMANDS

queue weight (803)
show queue mode (805)

queue weight

This command assigns weights to the four 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...weight3*

no queue weight

weight0...weight3 - The ratio of weights for queues 0 - 3 determines the weights used by the SWDRR scheduler. (Range: 1-15)

DEFAULT SETTING

Weights 1, 2, 4, 6 are assigned to queues 0 - 3 respectively.

COMMAND MODE

Global Configuration

COMMAND USAGE

- This command shares bandwidth at the egress port by defining scheduling weights for SWDRR, or for the queuing mode that uses a combination of strict and weighted queuing (page 802).

- 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 - 4 to the CoS priority queues 0 - 3.

```
ES-3026(config)#queue weight 1 2 3 4
ES-3026(config)#
```

RELATED COMMANDS

queue mode (802)
show queue weight (805)

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 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 four priority queues for each port. It can be configured to use strict priority queuing, SDWRR, 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:

```
ES-3026(config)#interface ethernet 1/3
ES-3026(config-if)#switchport priority default 5
ES-3026(config-if)#
```

RELATED COMMANDS

show interfaces switchport (689)

show queue mode

This command shows the current queue mode.

COMMAND MODE

Privileged Exec

EXAMPLE

```
ES-3026#show queue mode

Queue Mode : Weighted Round Robin Mode
ES-3026#
```

show queue weight

This command displays the weights used for the weighted queues.

COMMAND MODE

Privileged Exec

EXAMPLE

```
ES-3026#show queue weight
 Queue ID  Weight
 --------  ------
        0       1
        1       2
        2       4
        3       6
ES-3026#
```

PRIORITY COMMANDS (LAYER 3 AND 4)

This section describes commands used to configure Layer 3 and 4 traffic priority mapping on the switch.

Table 118: Priority Commands (Layer 3 and 4)

Command	Function	Mode
qos map cos-dscp	Maps CoS/CFI values in incoming packets to per-hop behavior and drop precedence values for internal priority processing	IC
qos map dscp-mutation	Maps DSCP values in incoming packets to per-hop behavior and drop precedence values for internal priority processing	IC
qos map phb-queue	Maps internal per-hop behavior values to hardware queues	IC
qos map trust-mode	Sets QoS mapping to DSCP or CoS	IC
show qos map dscp-mutation	Shows ingress DSCP to internal DSCP map	PE
show qos map phb-queue	Shows internal per-hop behavior to hardware queue map	PE
show qos map cos-dscp	Shows ingress CoS to internal DSCP map	PE
show qos map trust-mode	Shows the QoS mapping mode	PE

* The default settings used for mapping priority values to internal DSCP values and back to the hardware queues are designed to optimize priority services for the majority of network applications. It should not be necessary to modify any of the default settings unless a queuing problem occurs with a particular application.

qos map cos-dscp

This command maps CoS/CFI values in incoming packets to per-hop behavior and drop precedence values for priority processing. Use the **no** form to restore the default settings.

SYNTAX

qos map cos-dscp *phb drop-precedence* **from** *cos0 cfi0...cos7 cfi7*

no qos map cos-dscp *cos0 cfi0...cos7 cfi7*

phb - Per-hop behavior, or the priority used for this router hop. (Range: 0-7)

drop-precedence - Drop precedence used for Random Early Detection in controlling traffic congestion. (Range: 0 - Green, 3 - Yellow, 1 - Red)

cos - CoS value in ingress packets. (Range: 0-7)

cfi - Canonical Format Indicator. Set to this parameter to “0” to indicate that the MAC address information carried in the frame is in canonical format. (Range: 0-1)

DEFAULT SETTING.

Table 119: Default Mapping of CoS/CFI to Internal PHB/Drop Precedence

CoS \ CFI	0	1
0	(0,0)	(0,0)
1	(1,0)	(1,0)
2	(2,0)	(2,0)
3	(3,0)	(3,0)
4	(4,0)	(4,0)
5	(5,0)	(5,0)
6	(6,0)	(6,0)
7	(7,0)	(7,0)

COMMAND MODE

Interface Configuration (Port, Static Aggregation)

COMMAND USAGE

- The default mapping of CoS to PHB values shown in Table 119 is based on the recommended settings in IEEE 802.1p for mapping CoS values to output queues.
- Enter a value pair for the internal per-hop behavior and drop precedence, followed by the keyword “from” and then up to eight CoS/CFI paired values separated by spaces.
- If a packet arrives with a 802.1Q header but it is not an IP packet, then the CoS/CFI-to-PHB/Drop Precedence mapping table is used to generate priority and drop precedence values for internal processing. Note that priority tags in the original packet are not modified by this command.
- The internal DSCP consists of three bits for per-hop behavior (PHB) which determines the queue to which a packet is sent; and two bits for drop precedence (namely color) which is used by Random Early Detection (RED) to control traffic congestion.
- RED starts dropping yellow and red packets when the buffer fills up to 16 packets on ports 1-24 and 72 packets on ports 25-26, and then starts dropping any packets regardless of color when the buffer fills up to 58 packets on ports 1-24 and 80 packets on ports 25-26.
- The specified mapping applies to all interfaces.

EXAMPLE

```
ES-3026(config)#interface ethernet 1/5
ES-3026(config-if)#qos map cos-dscp 0 0 from 0 1
ES-3026(config-if)#
```

qos map dscp-mutation

This command maps DSCP values in incoming packets to per-hop behavior and drop precedence values for priority processing. Use the **no** form to restore the default settings.

SYNTAX

qos map dscp-mutation *phb drop-precedence* **from** *dscp0 ... dscp7*

no qos map dscp-mutation *dscp0 ... dscp7*

phb - Per-hop behavior, or the priority used for this router hop. (Range: 0-7)

drop-precedence - Drop precedence used for Random Early Detection in controlling traffic congestion.
(Range: 0 - Green, 3 - Yellow, 1 - Red)

dscp - DSCP value in ingress packets. (Range: 0-63)

DEFAULT SETTING.

Table 120: Default Mapping of DSCP Values to Internal PHB/Drop Values

ingress-dscp10 \ ingress-dscp1	0	1	2	3	4	5	6	7	8	9
0	0,0	0,1	0,0	0,3	0,0	0,1	0,0	0,3	1,0	1,1
1	1,0	1,3	1,0	1,1	1,0	1,3	2,0	2,1	2,0	2,3
2	2,0	2,1	2,0	2,3	3,0	3,1	3,0	3,3	3.0	3,1
3	3,0	3,3	4,0	4,1	4,0	4,3	4,0	4,1	4.0	4,3
4	5,0	5,1	5,0	5,3	5,0	5,1	6,0	5,3	6,0	6,1
5	6,0	6,3	6,0	6,1	6,0	6,3	7,0	7,1	7.0	7,3
6	7,0	7,1	7,0	7,3						

The ingress DSCP is composed of ingress-dscp10 (most significant digit in the left column) and ingress-dscp1 (least significant digit in the top row (in other words, ingress-dscp = ingress-dscp10 * 10 + ingress-dscp1); and the corresponding internal-dscp is shown at the intersecting cell in the table.

The ingress DSCP is bitwise ANDed with the binary value 11 to determine the drop precedence. If the resulting value is 10 binary, then the drop precedence is set to 0.

COMMAND MODE

Interface Configuration (Port, Static Aggregation)

COMMAND USAGE

- Enter a value pair for the internal per-hop behavior and drop precedence, followed by the keyword “from” and then up to eight DSCP values separated by spaces.
- This map is only used when the QoS mapping mode is set to “DSCP” by the qos map trust-mode command, and the ingress packet type is IPv4.
- Two QoS domains can have different DSCP definitions, so the DSCP-to-PHB/Drop Precedence mutation map can be used to modify one set of DSCP values to match the definition of another domain. The mutation

map should be applied at the receiving port (ingress mutation) at the boundary of a QoS administrative domain.

- Random Early Detection starts dropping yellow and red packets when the buffer fills up to 0x60 packets, and then starts dropping any packets regardless of color when the buffer fills up to 0x80 packets.
- The specified mapping applies to all interfaces.

EXAMPLE

This example changes the priority for all packets entering port 1 which contain a DSCP value of 1 to a per-hop behavior of 3 and a drop precedence of 1. Referring to Table 120, note that the DSCP value for these packets is now set to 25 ($3x2^3+1$) and passed on to the egress interface.

```
ES-3026(config)#interface ethernet 1/5
ES-3026(config-if)#qos map dscp-mutation 3 1 from 1
ES-3026(config-if)#
```

qos map phb-queue

This command determines the hardware output queues to use based on the internal per-hop behavior value. Use the **no** form to restore the default settings.

SYNTAX

qos map phb-queue *queue-id* **from** *phb0 ... phb7*

no map phb-queue *phb0 ... phb7*

phb - Per-hop behavior, or the priority used for this router hop. (Range: 0-7)

queue-id - The ID of the priority queue. (Range: 0-7, where 7 is the highest priority queue)

DEFAULT SETTING.

Table 121: Mapping Internal Per-hop Behavior to Hardware Queues

Per-hop Behavior	0	1	2	3	4	5	6	7
Hardware Queues	1	0	0	1	2	2	3	3

COMMAND MODE

Interface Configuration (Port, Static Aggregation)

COMMAND USAGE

- Enter a queue identifier, followed by the keyword “from” and then up to eight internal per-hop behavior values separated by spaces.
- Egress packets are placed into the hardware queues according to the mapping defined by this command.

EXAMPLE

```
ES-3026(config)#interface ethernet 1/5
ES-3026(config-if)#qos map phb-queue 0 from 1 2 3
ES-3026(config-if)#
```

qos map trust-mode

This command sets QoS mapping to DSCP or CoS. Use the **no** form to restore the default setting.

SYNTAX

qos map trust-mode {**dscp** | **cos**}

no qos map trust-mode

dscp - Sets the QoS mapping mode to DSCP.

cos - Sets the QoS mapping mode to CoS.

DEFAULT SETTING

CoS

COMMAND MODE

Interface Configuration (Port, Static Aggregation)

COMMAND USAGE

- If the QoS mapping mode is set to DSCP with this command, and the ingress packet type is IPv4, then priority processing will be based on the DSCP value in the ingress packet.
- If the QoS mapping mode is set to DSCP, and a non-IP packet is received, the packet's CoS and CFI (Canonical Format Indicator) values are used for priority processing if the packet is tagged. For an untagged packet, the default port priority (see page 804) is used for priority processing.
- If the QoS mapping mode is set to CoS with this command, and the ingress packet type is IPv4, then priority processing will be based on the CoS and CFI values in the ingress packet.

  For an untagged packet, the default port priority (see page 804) is used for priority processing.

EXAMPLE

This example sets the QoS priority mapping mode to use DSCP based on the conditions described in the Command Usage section.

```
ES-3026(config)#interface ge1/1
ES-3026(config-if)#qos map trust-mode dscp
ES-3026(config-if)#
```

show qos map dscp-mutation

This command shows the ingress DSCP to internal DSCP map.

SYNTAX

show qos map dscp-mutation interface *interface*

interface

ethernet *unit/port*

unit - Unit identifier. (Range: 1)

port - Port number. (ES-3026/P: 1-26, ES-3024G/P: 1-24)

port-channel *channel-id* (Range: 1-12)

COMMAND MODE

Privileged Exec

COMMAND USAGE

This map is only used when the QoS mapping mode is set to “DSCP” by the qos map trust-mode command, and the ingress packet type is IPv4.

EXAMPLE

The ingress DSCP is composed of “d1” (most significant digit in the left column) and “d2” (least significant digit in the top row (in other words, ingress DSCP = d1 * 10 + d2); and the corresponding Internal DSCP and drop precedence is shown at the intersecting cell in the table.

```
ES-3026#show qos map dscp-mutation interface ethernet 1/5
dscp mutation map.(x,y),x: phb,y: drop precedence:
 d1: d2 0     1     2     3     4     5     6     7     8     9
 ---------------------------------------------------------------
 0 :    (0,0) (0,1) (0,0) (0,3) (0,0) (0,1) (0,0) (0,3) (1,0) (1,1)
 1 :    (1,0) (1,3) (1,0) (1,1) (1,0) (1,3) (2,0) (2,1) (2,0) (2,3)
 2 :    (2,0) (2,1) (2,0) (2,3) (3,0) (3,1) (3,0) (3,3) (3,0) (3,1)
 3 :    (3,0) (3,3) (4,0) (4,1) (4,0) (4,3) (4,0) (4,1) (4,0) (4,3)
 4 :    (5,0) (5,1) (5,0) (5,3) (5,0) (5,1) (6,0) (5,3) (6,0) (6,1)
 5 :    (6,0) (6,3) (6,0) (6,1) (6,0) (6,3) (7,0) (7,1) (7,0) (7,3)
 6 :    (7,0) (7,1) (7,0) (7,3)
ES-3026#
```

show qos map phb-queue

This command shows internal per-hop behavior to hardware queue map.

SYNTAX

show qos map phb-queue interface *interface*

interface

ethernet *unit/port*

unit - Unit identifier. (Range: 1)

port - Port number. (ES-3026/P: 1-26, ES-3024G/P: 1-24)

port-channel *channel-id* (Range: 1-12)

COMMAND MODE
Privileged Exec

EXAMPLE

```
ES-3026#show qos map phb-queue interface ethernet 1/5
Information of Eth 1/5
 phb-queue map:
 phb:       0     1     2     3     4     5     6     7
 -----------------------------------------------------
 queue:     2     0     1     3     4     5     6     7
ES-3026#
```

show qos map cos-dscp

This command shows ingress CoS/CFI to internal DSCP map.

SYNTAX

show qos map cos-dscp interface *interface*

interface

ethernet *unit*/*port*

unit - Unit identifier. (Range: 1)

port - Port number. (ES-3026/P: 1-26, ES-3024G/P: 1-24)

port-channel *channel-id* (Range: 1-12)

COMMAND MODE
Privileged Exec

EXAMPLE

```
ES-3026#show qos map cos-dscp interface ethernet 1/5
 cos-dscp map.(x,y),x: phb,y: drop precedence:
 cos  : cfi  0          1
 --------------------------------
 0            (0,0)       (0,0)
 1            (1,0)       (1,0)
 2            (2,0)       (2,0)
 3            (3,0)       (3,0)
 4            (4,0)       (4,0)
 5            (5,0)       (5,0)
 6            (6,0)       (6,0)
 7            (7,0)       (7,0)
ES-3026#
```

show qos map trust-mode

This command shows the QoS mapping mode.

SYNTAX

show qos map trust-mode interface *interface*

interface

ethernet *unit*/*port*

unit - Unit identifier. (Range: 1)

port - Port number. (ES-3026/P: 1-26, ES-3024G/P: 1-24)

port-channel *channel-id* (Range: 1-12)

COMMAND MODE

Privileged Exec

EXAMPLE

The following shows that the trust mode is set to CoS:

```
ES-3026#show qos map trust-mode interface ethernet 1/5
Information of Eth 1/5
  COS Map mode:          cos mode
ES-3026#
```

37 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 122: Quality of Service Commands

Command	Function	Mode
class-map	Creates a class map for a type of traffic	GC
description	Specifies the description of a class map	CM
match	Defines the criteria used to classify traffic	CM
rename	Redefines the name of a class map	CM
policy-map	Creates a policy map for multiple interfaces	GC
description	Specifies the description of a policy map	PM
class	Defines a traffic classification for the policy to act on	PM
rename	Redefines the name of a policy map	PM
police flow	Defines an enforcer for classified traffic based on a metered flow rate	PM-C
police srtcm-color	Defines an enforcer for classified traffic based on a single rate three color meter	PM-C
police trtcm-color	Defines an enforcer for classified traffic based on a two rate three color meter	PM-C
set cos	Services IP traffic by setting a class of service value for matching packets for internal processing	PM-C
set ip dscp	Services IP traffic by setting an IP DSCP value for matching packets for internal processing	PM-C
set phb	Services IP traffic by setting a per-hop behavior value for matching packets for internal processing	PM-C
service-policy	Applies a policy map defined by the policy-map command to the input of a particular interface	IC
show class-map	Displays the QoS class maps which define matching criteria used for classifying traffic	PE
show policy-map	Displays the QoS policy maps which define classification criteria for incoming traffic, and may include policers for bandwidth limitations	PE
show policy-map interface	Displays the configuration of all classes configured for all service policies on the specified interface	PE

To create a service policy for a specific category of ingress traffic, follow these steps:

1. Use the class-map command to designate a class name for a specific category of traffic, and enter the Class Map configuration mode.

2. Use the match command to select a specific type of traffic based on an access list, 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, set cos or set ip dscp 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 819). The policy map is then bound by a service policy to an interface (page 830). 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:

```
ES-3026(config)#class-map rd-class match-any
ES-3026(config-cmap)#match ip dscp 3
ES-3026(config-cmap)#
```

RELATED COMMANDS

show class-map (831)

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

```
ES-3026(config)#class-map rd-class#1
ES-3026(config-cmap)#description matches packets marked for DSCP service
  value 3
ES-3026(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* | **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.

```
ES-3026(config)#class-map rd-class#1 match-any
ES-3026(config-cmap)#match ip dscp 3
ES-3026(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.

```
ES-3026(config)#class-map rd-class#2 match-any
ES-3026(config-cmap)#match ip precedence 5
ES-3026(config-cmap)#
```

This example creates a class map call “rd-class#3,” and sets it to match packets marked for VLAN 1.

```
ES-3026(config)#class-map rd-class#3 match-any
ES-3026(config-cmap)#match vlan 1
ES-3026(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

```
ES-3026(config)#class-map rd-class#1
ES-3026(config-cmap)#rename rd-class#9
ES-3026(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 819) 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.

```
ES-3026(config)#policy-map rd-policy
ES-3026(config-pmap)#class rd-class
ES-3026(config-pmap-c)#set ip dscp 3
ES-3026(config-pmap-c)#police flow 10000 4000 conform-action transmit
  violate-action drop
ES-3026(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.)

- set ip dscp sets the IP DSCP value in matching packets in the packet's ToS field.
- **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.

```
ES-3026(config)#policy-map rd-policy
ES-3026(config-pmap)#class rd-class
ES-3026(config-pmap-c)#set phb 3
ES-3026(config-pmap-c)#police flow 10000 4000 conform-action transmit
  violate-action drop
ES-3026(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
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.

```
ES-3026(config)#policy-map rd-policy
ES-3026(config-pmap)#class rd-class
ES-3026(config-pmap-c)#set phb 3
ES-3026(config-pmap-c)#police flow 100000 4000 conform-action transmit
  violate-action drop
ES-3026(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
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.

```
ES-3026(config)#policy-map rd-policy
ES-3026(config-pmap)#class rd-class
ES-3026(config-pmap-c)#set phb 3
ES-3026(config-pmap-c)#police srtcm-color-blind 100000 4000 6000 conform-
  action transmit exceed-action 0 violate-action drop
ES-3026(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
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 - Peak 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.)

drop - Drops packet as required by exceed-action or violate-action.

transmit - Transmits without taking any action.

new-dscp - Differentiated Service Code Point (DSCP) value. (Range: 0-63)

DEFAULT SETTING

None

COMMAND MODE

Policy Map Class Configuration

COMMAND USAGE

- You can configure up to 16 policers (i.e., class maps) for ingress ports.
- The *committed-rate* and *peak-rate* cannot exceed the configured interface speed, and the *committed-burst* and *peak-burst* cannot exceed 16 Mbytes.
- The trTCM as defined in RFC 2698 meters a traffic stream and processes its packets based on two rates – Committed Information Rate (CIR) and Peak Information Rate (PIR), and their associated burst sizes - Committed Burst Size (BC) and Peak Burst Size (BP).
- The PHB label is composed of five bits, three bits for per-hop behavior, and two bits for the color scheme used to control queue congestion. A packet is marked red if it exceeds the PIR. Otherwise it is marked either yellow or green depending on whether it exceeds or doesn't exceed the CIR.

  The trTCM is useful for ingress policing of a service, where a peak rate needs to be enforced separately from a committed rate.
- The meter operates in one of two modes. In the color-blind mode, the meter assumes that the packet stream is uncolored. In color-aware mode the meter assumes that some preceding entity has pre-colored the incoming packet stream so that each packet is either green, yellow, or red. The marker (re)colors an IP packet according to the results of the meter. The color is coded in the DS field [RFC 2474] of the packet.
- The behavior of the meter is specified in terms of its mode and two token buckets, P and C, which are based on the rates PIR and CIR, respectively. The maximum size of the token bucket P is BP and the maximum size of the token bucket C is BC.
- The token buckets P and C are initially (at time 0) full, that is, the token count Tp(0) = BP and the token count Tc(0) = BC. Thereafter, the token count Tp is incremented by one PIR times per second up to BP and the token count Tc is incremented by one CIR times per second up to BC.

When a packet of size B bytes arrives at time t, the following happens if trTCM is configured to operate in color-blind mode:

- If Tp(t)-B < 0, the packet is red, else
- if Tc(t)-B < 0, the packet is yellow and Tp is decremented by B, else
- the packet is green and both Tp and Tc are decremented by B.

When a packet of size B bytes arrives at time t, the following happens if trTCM is configured to operate in color-aware mode:

- If the packet has been precolored as red or if Tp(t)-B < 0, the packet is red, else
- if the packet has been precolored as yellow or if Tc(t)-B < 0, the packet is yellow and Tp is decremented by B, else
- the packet is green and both Tp and Tc are decremented by B.

◆ The trTCM can be used to mark a IP packet stream in a service, where different, decreasing levels of assurances (either absolute or relative) are given to packets which are green, yellow, or red. Refer to RFC 2698 for more information on other aspects of trTCM.

EXAMPLE

This example creates a policy called “rd-policy,” uses the class command to specify the previously defined “rd-class,” uses the set phb command to classify the service that incoming packets will receive, and then uses the **police trtcm-color-blind** command to limit the average bandwidth to 100,000 Kbps, the committed burst rate to 4000 bytes, the peak information rate to 1,000,000 kbps, the peak burst size to 6000, to remark any packets exceeding the committed burst size, and to drop any packets exceeding the peak information rate.

```
ES-3026(config)#policy-map rd-policy
ES-3026(config-pmap)#class rd-class
ES-3026(config-pmap-c)#set phb 3
ES-3026(config-pmap-c)#police trtcm-color-blind 100000 4000 100000 6000
  conform-action transmit exceed-action 0 violate-action drop
ES-3026(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.

```
ES-3026(config)#policy-map rd-policy
ES-3026(config-pmap)#class rd-class
ES-3026(config-pmap-c)#set cos 3
ES-3026(config-pmap-c)#police flow 10000 4000 conform-action transmit
  violate-action drop
ES-3026(config-pmap-c)#
```

set ip dscp

This command services IP traffic by setting an IP DSCP value for a matching packet (as specified by the match command) in the packet’s ToS field. Use the **no** form to remove this setting.

SYNTAX

[**no**] **set dscp** *dscp-value*

dscp-value - Differentiated Service Code Point value. (Range: 0-63)

DEFAULT SETTING

None

COMMAND MODE

Policy Map Class Configuration

EXAMPLE

This example creates a policy called “rd-policy,” uses the class command to specify the previously defined “rd-class,” uses the **set dscp** 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.

```
ES-3026(config)#policy-map rd-policy
ES-3026(config-pmap)#class rd-class
ES-3026(config-pmap-c)#set dscp 3
ES-3026(config-pmap-c)#police flow 10000 4000 conform-action transmit
  violate-action drop
ES-3026(config-pmap-c)#
```

set phb

This command services IP traffic by setting a per-hop behavior value for a matching packet (as specified by the match command) for internal processing. Use the **no** form to remove this setting.

SYNTAX

[**no**] **set phb** *phb-value*

phb-value - Per-hop behavior value. (Range: 0-7)

DEFAULT SETTING

None

COMMAND MODE

Policy Map Class Configuration

COMMAND USAGE

- The **set phb** command is used to set an internal QoS value in hardware for matching packets (see Table 120, "Default Mapping of DSCP Values to Internal PHB/Drop Values"). The QoS label is composed of five bits, three bits for per-hop behavior, and two bits for the color scheme used to control queue congestion by the police srtcm-color command and police trtcm-color command.

- The set cos and **set phb** command function at the same level of priority. Therefore setting either of these commands will overwrite any action already configured by the other command.

EXAMPLE

This example creates a policy called “rd-policy,” uses the class command to specify the previously defined “rd-class,” uses the **set phb** command to classify the service that incoming packets will receive, and then uses the police flow command to limit the average bandwidth to 100,000 Kbps, the burst rate to 4000 bytes, and configure the response to drop any violating packets.

```
ES-3026(config)#policy-map rd-policy
ES-3026(config-pmap)#class rd-class
ES-3026(config-pmap-c)#set phb 3
ES-3026(config-pmap-c)#police flow 10000 4000 conform-action transmit
  violate-action drop
ES-3026(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.

```
ES-3026(config)#interface ethernet 1/1
ES-3026(config-if)#service-policy input rd-policy
ES-3026(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

```
ES-3026#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

ES-3026#
```

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

```
ES-3026#show policy-map
Policy Map rd-policy
```

```
Description:
 class rd-class
 set phb 3
ES-3026#show policy-map rd-policy class rd-class
Policy Map rd-policy
 class rd-class
 set phb 3
ES-3026#
```

show policy-map interface

This command displays the service policy assigned to the specified interface.

SYNTAX

show policy-map interface *interface* **input**

interface

unit/port

unit - Unit identifier. (Range: 1)

port - Port number. (ES-3026/P: 1-26, ES-3024G/P: 1-24)

port-channel *channel-id* (Range: 1-12)

COMMAND MODE

Privileged Exec

EXAMPLE

```
ES-3026#show policy-map interface 1/5 input
Service-policy rd-policy
ES-3026#
```

38 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.

Table 123: 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 SNOOPING

This section describes commands used to configure IGMP snooping on the switch.

Table 124: 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

Table 124: IGMP Snooping Commands (Continued)

Command	Function	Mode
ip igmp snooping unregistered-data-flood	Floods unregistered multicast traffic into the attached VLAN	GC
ip igmp snooping unsolicited-report-interval	Specifies how often the upstream interface should transmit unsolicited IGMP reports (when proxy reporting is enabled)	GC
ip igmp snooping version	Configures the IGMP version for snooping	GC
ip igmp snooping version-exclusive	Discards received IGMP messages which use a version different to that currently configured	GC
ip igmp snooping vlan general-query-suppression	Suppresses general queries except for ports attached to downstream multicast hosts	GC
ip igmp snooping vlan immediate-leave	Immediately deletes a member port of a multicast service if a leave packet is received at that port and immediate-leave is enabled for the parent VLAN	GC
ip igmp snooping vlan last-memb-query-count	Configures the number of IGMP proxy query messages that are sent out before the system assumes there are no local members	GC
ip igmp snooping vlan last-memb-query-intvl	Configures the last-member-query interval	GC
ip igmp snooping vlan mrd	Sends multicast router solicitation messages	GC
ip igmp snooping vlan proxy-address	Configures a static address for proxy IGMP query and reporting	GC
ip igmp snooping vlan proxy-query-interval	Configures the interval between sending IGMP proxy general queries	GC
ip igmp snooping vlan proxy-query-resp-intvl	Configures the maximum time the system waits for a response to proxy general queries	GC
ip igmp snooping vlan proxy-reporting	Enables IGMP Snooping with Proxy Reporting	GC
ip igmp snooping vlan static	Adds an interface as a member of a multicast group	GC
ip igmp snooping vlan version	Configures the IGMP version for snooping	GC
ip igmp snooping vlan version-exclusive	Discards received IGMP messages which use a version different to that currently configured	GC
show ip igmp snooping	Shows the IGMP snooping, proxy, and query configuration	PE
show ip igmp snooping group	Shows known multicast group, source, and host port mapping	PE

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
Disabled

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.

```
ES-3026(config)#ip igmp snooping
ES-3026(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 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 the IGMP proxy reporting is configured on a VLAN, this setting takes precedence over the global configuration.

EXAMPLE

```
ES-3026(config)#ip igmp snooping proxy-reporting
ES-3026(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

```
ES-3026(config)#ip igmp snooping querier
ES-3026(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

```
ES-3026(config)#ip igmp snooping router-alert-option-check
ES-3026(config)#
```

ip igmp snooping router-port-expire-time

This command configures the querier time out. 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 time out to 400 seconds:

```
ES-3026(config)#ip igmp snooping router-port-expire-time 400
ES-3026(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 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 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.

```
ES-3026(config)#ip igmp snooping tcn-flood
ES-3026(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.

```
ES-3026(config)#ip igmp snooping tcn query-solicit
ES-3026(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

```
ES-3026(config)#ip igmp snooping unregistered-data-flood
ES-3026(config)#
```

ip igmp snooping unsolicited-report-interval

This command specifies how often the upstream interface should transmit unsolicited IGMP reports when proxy reporting is enabled. Use the **no** form to restore the default value.

SYNTAX

ip igmp snooping unsolicited-report-interval *seconds*

no ip igmp snooping version-exclusive

seconds - The interval at which to issue unsolicited reports. (Range: 1-65535 seconds)

DEFAULT SETTING
400 seconds

COMMAND MODE
Global Configuration

COMMAND USAGE
- When a new upstream interface (that is, uplink port) starts up, the switch sends unsolicited reports for all currently learned multicast channels out through the new upstream interface.
- This command only applies when proxy reporting is enabled (see page 835).

EXAMPLE

```
ES-3026(config)#ip igmp snooping unsolicited-report-interval 5
ES-3026(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.

```
ES-3026(config)#ip igmp snooping version 1
ES-3026(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
```
ES-3026(config)#ip igmp snooping version-exclusive
ES-3026(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
```
ES-3026(config)#ip igmp snooping vlan 1 general-query-suppression
ES-3026(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 time out period. (The time out for this release is currently defined by Last Member Query Interval (fixed at one second) * 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 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.

```
ES-3026(config)#ip igmp snooping vlan 1 immediate-leave
ES-3026(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 or IGMP querier is enabled (page 835).

EXAMPLE

```
ES-3026(config)#ip igmp snooping vlan 1 last-memb-query-count 7
ES-3026(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 835).

EXAMPLE

```
ES-3026(config)#ip igmp snooping vlan 1 last-memb-query-intvl 700
ES-3026(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.

```
ES-3026(config)#no ip igmp snooping vlan 1 mrd
ES-3026(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.

```
ES-3026(config)#ip igmp snooping vlan 1 proxy-address 10.0.1.8
ES-3026(config)#
```

ip igmp snooping vlan proxy-query-interval

This command configures the interval between sending IGMP proxy general queries. Use the **no** form to restore the default.

SYNTAX

ip igmp snooping vlan *vlan-id* **proxy-query-interval** *interval*

no ip igmp snooping vlan *vlan-id* **proxy-query-interval**

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

interval - The interval between sending IGMP proxy 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 will take effect only if IGMP snooping proxy reporting is enabled (page 835).

EXAMPLE

```
ES-3026(config)#ip igmp snooping vlan 1 proxy-query-interval 150
ES-3026(config)#
```

ip igmp snooping vlan proxy-query-resp-intvl

This command configures the maximum time the system waits for a response to proxy general queries. Use the **no** form to restore the default.

SYNTAX

ip igmp snooping vlan *vlan-id* **proxy-query-resp-intvl** *interval*

no ip igmp snooping vlan *vlan-id* **proxy-query-resp-intvl**

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

interval - The maximum time the system waits for a response to proxy general queries. (Range: 10-31744 tenths of a second)

DEFAULT SETTING

100 (10 seconds)

COMMAND MODE

Global Configuration

COMMAND USAGE

This command will take effect only if IGMP snooping proxy reporting is enabled (page 835).

EXAMPLE

```
ES-3026(config)#ip igmp snooping vlan 1 proxy-query-resp-intvl 20
ES-3026(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 - Unit identifier. (Range: 1)

port - Port number. (ES-3026/P: 1-26, ES-3024G/P: 1-24)

port-channel *channel-id* (Range: 1-12)

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.

```
ES-3026(config)#ip igmp snooping vlan 1 static 224.0.0.12 ethernet 1/5
ES-3026(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 433 for a description of the displayed items.

EXAMPLE

The following shows the current IGMP snooping configuration:

```
ES-3026#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

 Vlan 1:
 --------
 IGMP snooping                      : Enabled
 IGMP snooping running status       : Inactive
 Immediate leave                    : Disabled
 Last member query interval         : 10 (1/10s)
 Last member query count            : 2
 Proxy query address                : 0.0.0.0
 Version                            : Using global version (2)
 Proxy query interval               : 125 s
 Proxy query response interval      : 100 (1/10s)
 Version exclusive                  : Disabled
 General query suppression          : Disabled
 Proxy reporting                    : Using global status (Enabled)
 Multicast Router Discovery         : Enabled
```

:

show ip igmp snooping group

This command shows known multicast group, source, and host port mappings for the specified VLAN interface, or for all interfaces if none is specified.

SYNTAX

show ip igmp snooping group [**vlan** *vlan-id* [**user** | **igmpsnp**]] [**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
Bridge Multicast Forwarding Entry Count:0
VLAN     Group            Source           Port List
-------- ---------------- ---------------- ----------------------------------
   1 224.1.1.12      *               Eth 1/12(S)
   1 224.1.1.12      *               Eth 1/23(D)
Console#
```

STATIC MULTICAST ROUTING

This section describes commands used to configure static multicast routing on the switch.

Table 125: 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 - Unit identifier. (Range: 1)

port - Port number. (ES-3026/P: 1-26, ES-3024G/P: 1-24)

port-channel *channel-id* (Range: 1-12)

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.

```
ES-3026(config)#ip igmp snooping vlan 1 mrouter ethernet 1/11
ES-3026(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.

```
ES-3026#show ip igmp snooping mrouter vlan 1
 VLAN M'cast Router Ports Type
 ---- ------------------ -------
    1            Eth 1/11  Static
ES-3026#
```

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 126: 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 126: 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

```
ES-3026(config)#ip igmp filter
ES-3026(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

```
ES-3026(config)#ip igmp profile 19
ES-3026(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

```
ES-3026(config)#ip igmp profile 19
ES-3026(config-igmp-profile)#permit
ES-3026(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

```
ES-3026(config)#ip igmp profile 19
ES-3026(config-igmp-profile)#range 239.1.1.1
ES-3026(config-igmp-profile)#range 239.2.3.1 239.2.3.100
ES-3026(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

```
ES-3026(config)#interface ethernet 1/1
ES-3026(config-if)#ip igmp filter 19
ES-3026(config-if)#
```

ip igmp max-groups

This command sets the IGMP throttling number for an interface on the switch. Use the **no** form to restore the default setting.

SYNTAX

ip igmp max-groups *number*

no ip igmp max-groups

number - The maximum number of multicast groups an interface can join at the same time. (Range: 1.255)

DEFAULT SETTING

255

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

```
ES-3026(config)#interface ethernet 1/1
ES-3026(config-if)#ip igmp max-groups 10
ES-3026(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

```
ES-3026(config)#interface ethernet 1/1
ES-3026(config-if)#ip igmp max-groups action replace
ES-3026(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 - Unit identifier. (Range: 1)

port - Port number. (ES-3026/P: 1-26, ES-3024G/P: 1-24)

port-channel *channel-id* (Range: 1-12)

DEFAULT SETTING

None

COMMAND MODE

Privileged Exec

EXAMPLE

```
ES-3026#show ip igmp filter
IGMP filter enabled
ES-3026#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
ES-3026#
```

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

```
ES-3026#show ip igmp profile
IGMP Profile 19
IGMP Profile 50
ES-3026#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
ES-3026#
```

show ip igmp throttle interface

This command displays the interface settings for IGMP throttling.

SYNTAX

show ip igmp throttle interface [*interface*]

interface

ethernet *unit*/*port*

unit - Unit identifier. (Range: 1)

port - Port number. (ES-3026/P: 1-26, ES-3024G/P: 1-24)

port-channel *channel-id* (Range: 1-12)

DEFAULT SETTING
None

COMMAND MODE
Privileged Exec

COMMAND USAGE
Using this command without specifying an interface displays all interfaces.

EXAMPLE

```
ES-3026#show ip igmp throttle interface ethernet 1/1
Eth  1/1 Information
  Status : TRUE
  Action : Deny
  Max Multicast Groups : 32
  Current Multicast Groups : 0

ES-3026#
```

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 127: 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	Statically binds a multicast group to a port	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: 1-1024)

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:

```
ES-3026(config)#mvr
ES-3026(config)#mvr group 228.1.23.1 10
ES-3026(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.

```
ES-3026(config)#interface ethernet 1/5
ES-3026(config-if)#mvr immediate
ES-3026(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)

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.

```
ES-3026(config)#interface ethernet 1/5
ES-3026(config-if)#mvr type source
ES-3026(config-if)#exit
ES-3026(config)#interface ethernet 1/6
ES-3026(config-if)#mvr type receiver
ES-3026(config-if)#exit
ES-3026(config)#interface ethernet 1/7
ES-3026(config-if)#mvr type receiver
ES-3026(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:

```
ES-3026(config)#interface ethernet 1/7
ES-3026(config-if)#mvr type receiver
ES-3026(config-if)#mvr vlan 3 group 225.0.0.5
ES-3026(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 - Unit identifier. (Range: 1)

port - Port number. (ES-3026/P: 1-26, ES-3024G/P: 1-24)

port-channel *channel-id* (Range: 1-12)

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:

```
ES-3026#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
ES-3026#
```

Table 128: 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 128: 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:

```
ES-3026#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

ES-3026#
```

Table 129: 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:

```
ES-3026#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)
ES-3026#
```

Table 130: 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 130: 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.

39 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 131: 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 131: 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

```
ES-3026(config)#lldp
ES-3026(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
```
ES-3026(config)#lldp holdtime-multiplier 10
ES-3026(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
```
ES-3026(config)#lldp notification-interval 30
ES-3026(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

```
ES-3026(config)#lldp refresh-interval 60
ES-3026(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

```
ES-3026(config)#lldp reinit-delay 10
ES-3026(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

```
ES-3026(config)#lldp tx-delay 10
ES-3026(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

```
ES-3026(config)#interface ethernet 1/1
ES-3026(config-if)#lldp admin-status rx-only
ES-3026(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

```
ES-3026(config)#interface ethernet 1/1
ES-3026(config-if)#lldp basic-tlv management-ip-address
ES-3026(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

```
ES-3026(config)#interface ethernet 1/1
ES-3026(config-if)#lldp basic-tlv port-description
ES-3026(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

```
ES-3026(config)#interface ethernet 1/1
ES-3026(config-if)#lldp basic-tlv system-capabilities
ES-3026(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

```
ES-3026(config)#interface ethernet 1/1
ES-3026(config-if)#lldp basic-tlv system-description
ES-3026(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

```
ES-3026(config)#interface ethernet 1/1
ES-3026(config-if)#lldp basic-tlv system-name
ES-3026(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

```
ES-3026(config)#interface ethernet 1/1
ES-3026(config-if)#no lldp dot1-tlv proto-ident
ES-3026(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 772 and "Configuring Protocol-based VLANs" on page 786).

EXAMPLE

```
ES-3026(config)#interface ethernet 1/1
ES-3026(config-if)#no lldp dot1-tlv proto-vid
ES-3026(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

```
ES-3026(config)#interface ethernet 1/1
ES-3026(config-if)#no lldp dot1-tlv pvid
ES-3026(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 774 and "protocol-vlan protocol-group (Configuring Interfaces)" on page 787.

EXAMPLE

```
ES-3026(config)#interface ethernet 1/1
ES-3026(config-if)#no lldp dot1-tlv vlan-name
ES-3026(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

```
ES-3026(config)#interface ethernet 1/1
ES-3026(config-if)#no lldp dot3-tlv link-agg
ES-3026(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

```
ES-3026(config)#interface ethernet 1/1
ES-3026(config-if)#no lldp dot3-tlv mac-phy
ES-3026(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 488 for information on configuring the maximum frame size for this switch.

EXAMPLE

```
ES-3026(config)#interface ethernet 1/1
ES-3026(config-if)#lldp dot3-tlv max-frame
ES-3026(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

```
ES-3026(config)#interface ethernet 1/1
ES-3026(config-if)#lldp notification
ES-3026(config-if)#
```

show lldp config

This command shows LLDP configuration settings for all ports.

SYNTAX

show lldp config [**detail** *interface*]

detail - Shows configuration summary.

interface

ethernet *unit*/*port*

unit - Unit identifier. (Range: 1)

port - Port number. (ES-3026/P: 1-26, ES-3024G/P: 1-24)

port-channel *channel-id* (Range: 1-12)

COMMAND MODE

Privileged Exec

EXAMPLE

```
ES-3026#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
.
.
.
ES-3026#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
 MED Configuration:
 MED Notification Enabled : True MED Enabled TLVs Advertised:
  *med-cap
 *network-policy
 *location
 *extPoe
 *inventory

ES-3026#
```

show lldp info local-device

This command shows LLDP global and interface-specific configuration settings for this device.

SYNTAX

show lldp info local-device [**detail** *interface*]

detail - Shows configuration summary.

interface

ethernet *unit*/*port*

unit - Unit identifier. (Range: 1)

port - Port number. (ES-3026/P: 1-26, ES-3024G/P: 1-24)

port-channel *channel-id* (Range: 1-12)

COMMAND MODE

Privileged Exec

EXAMPLE

```
ES-3026#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 : 24 10/100 ports and 4 gigabit ports with PoE switch
  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
.
.
.
ES-3026#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

ES-3026#
```

show lldp info remote-device

This command shows LLDP global and interface-specific configuration settings for remote devices attached to an LLDP-enabled port.

SYNTAX

show lldp info remote-device [**detail** *interface*]

detail - Shows configuration summary.

interface

ethernet *unit*/*port*

unit - Unit identifier. (Range: 1)

port - Port number. (ES-3026/P: 1-26, ES-3024G/P: 1-24)

port-channel *channel-id* (Range: 1-12)

COMMAND MODE

Privileged Exec

EXAMPLE

```
ES-3026#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

ES-3026#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            :
  SysDescr           : 24 10/100 ports and 4 gigabit ports with PoE switch
  PortDescr          : Ethernet Port on unit 1, port 1
  SystemCapSupported : Bridge
  SystemCapEnabled   : Bridge
  Remote Management Address :
    00-01-02-03-04-05 (MAC Address)

ES-3026#
```

show lldp info statistics

This command shows statistics based on traffic received through all attached LLDP-enabled interfaces.

SYNTAX

show lldp info statistics [**detail** *interface*]

detail - Shows configuration summary.

interface

ethernet *unit*/*port*

unit - Unit identifier. (Range: 1)

port - Port number. (ES-3026/P: 1-26, ES-3024G/P: 1-24)

port-channel *channel-id* (Range: 1-12)

COMMAND MODE

Privileged Exec

EXAMPLE

```
switch#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
⋮
switch#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

switch#
```

40 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 132: 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.

```
ES-3026(config)#ip domain-list sample.com.jp
ES-3026(config)#ip domain-list sample.com.uk
ES-3026(config)#end
ES-3026#show dns
Domain Lookup Status:
    DNS disabled
Default Domain Name:
    sample.com
Domain Name List:
    sample.com.jp
    sample.com.uk
Name Server List:
ES-3026#
```

RELATED COMMANDS
ip domain-name (887)

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.

```
ES-3026(config)#ip domain-lookup
ES-3026(config)#end
ES-3026#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
ES-3026#
```

RELATED COMMANDS

ip domain-name (887)
ip name-server (889)

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

```
ES-3026(config)#ip domain-name sample.com
ES-3026(config)#end
ES-3026#show dns
Domain Lookup Status:
    DNS Disabled
```

```
Default Domain Name:
    sample.com
Domain Name List:
Name Server List:
ES-3026#
```

RELATED COMMANDS

ip domain-list (885)
ip name-server (889)
ip domain-lookup (886)

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.

```
ES-3026(config)#ip host rd5 192.168.1.55
ES-3026(config)#end
ES-3026#show hosts
No.  Flag Type    IP Address            TTL   Domain
---- ---- ------- --------------------  ----- ------------------------------
   0    2 Address 192.168.1.55                rd5
ES-3026#
```

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.

```
ES-3026(config)#ip name-server 192.168.1.55 10.1.0.55
ES-3026(config)#end
ES-3026#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
ES-3026#
```

RELATED COMMANDS

ip domain-name (887)
ip domain-lookup (886)

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.

```
ES-3026(config)#ipv6 host rd6 2001:0db8:1::12
ES-3026(config)#end
ES-3026#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
ES-3026#
```

clear dns cache

This command clears all entries in the DNS cache.

COMMAND MODE

Privileged Exec

EXAMPLE

```
ES-3026#clear dns cache
ES-3026#show dns cache
No.     Flag    Type    IP Address      TTL     Domain
------- ------- ------- --------------- ------- --------
ES-3026#
```

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.

```
ES-3026(config)#clear host *
ES-3026(config)#
```

show dns

This command displays the configuration of the DNS service.

COMMAND MODE

Privileged Exec

EXAMPLE

```
ES-3026#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
ES-3026#
```

show dns cache

This command displays entries in the DNS cache.

COMMAND MODE

Privileged Exec

EXAMPLE

```
ES-3026#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
ES-3026#
```

Table 133: 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.

```
ES-3026#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
ES-3026#
```

Table 134: 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.

41 DHCP COMMANDS

These commands are used to configure Dynamic Host Configuration Protocol (DHCP) client functions.

Table 135: DHCP Commands

Command Group	Function
DHCP Client	Allows interfaces to dynamically acquire IP address information

DHCP CLIENT

Use the commands in this section to allow the switch's VLAN interfaces to dynamically acquire IP address information.

NOTE: DHCPv6 stateful configuration of IP address prefixes is not supported in the current software release. If the router advertisements have the "other stateful configuration" flag set, the switch will attempt to acquire other non-address configuration information (such as a default gateway) from a DHCPv6 server.

Table 136: DHCP Client Commands

Command	Function	Mode
DHCP for IPv4		
ip dhcp client class-id	Specifies the DHCP client identifier for an interface	IC
ip dhcp restart client	Submits a BOOTP or DHCP client request	PE
DHCP for IPv6		
ipv6 dhcp restart client vlan	Submits a DHCPv6 client request	PE
show ipv6 dhcp duid	Shows the DHCP Unique Identifier for this switch	PE
show ipv6 dhcp vlan	Shows DHCPv6 information for specified interface	PE

ip dhcp client class-id

This command specifies the DCHP client vendor class identifier for the current interface. Use the **no** form to remove this identifier.

SYNTAX

ip dhcp client class-id {**text** *text* | **hex** *hex*}

no ip dhcp client class-id

text - A text string. (Range: 1-32 characters)

hex - A hexadecimal value.

DEFAULT SETTING

None

COMMAND MODE

Interface Configuration (VLAN)

COMMAND USAGE

- This command is used to identify the vendor class and configuration of the switch to the DHCP server, which then uses this information to decide on how to service the client or the type of information to return.
- The general framework for this DHCP option is set out in RFC 2132 (Opton 60). This information is used to convey configuration settings or other identification information about a client, but the specific string to use should be supplied by your service provider or network administrator.
- The server should reply with Option 43 information, which encapsulates Option 66 attributes including the TFTP server name and boot file name.

EXAMPLE

```
ES-3026(config)#interface vlan 2
ES-3026(config-if)#ip dhcp client class-id hex 0000e8666572
ES-3026(config-if)#
```

RELATED COMMANDS

ip dhcp restart client (896)

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.

```
ES-3026(config)#interface vlan 1
ES-3026(config-if)#ip address dhcp
ES-3026(config-if)#exit
ES-3026#ip dhcp restart client
ES-3026#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
ES-3026#
```

RELATED COMMANDS

ip address (902)

ipv6 dhcp restart client vlan

This command submits a DHCPv6 client request.

SYNTAX

ipv6 dhcp restart client vlan *vlan-id*

vlan-id - VLAN ID, specified as a single number, a range of consecutive numbers separated by a hyphen, or multiple numbers separated by commas. (Range: 1-4093, no leading zeroes)

DEFAULT SETTING

None

COMMAND MODE

Privileged Exec

COMMAND USAGE

- This command starts the DHCPv6 client process if it is not yet running by submitting requests for address prefix delegation through the specified interface(s).

- When the DHCP client process is enabled and a prefix is successfully acquired, the prefix is stored in the IPv6 general prefix pool. Other commands and applications (such as the ipv6 address command) can then refer to the prefixes in the general prefix pool.
- DHCPv6 clients can also request configuration parameters that do not require a server to maintain any dynamic state for individual clients, such as DNS server addresses.
- DHCPv6 clients builds a list of servers by sending a solicit message and collecting advertised message replies. These servers are then ranked based on their advertised preference value. If the client needs to acquire prefixes from servers, only servers that have advertised prefixes are considered.

EXAMPLE

The following command submits a client request on VLAN 1.

```
ES-3026#ipv6 dhcp restart client vlan 1
ES-3026#
```

RELATED COMMANDS

ipv6 address (911)

show ipv6 dhcp duid

This command shows the DHCP Unique Identifier for this switch.

COMMAND MODE

Privileged Exec

COMMAND USAGE

DHCPv6 clients and servers are identified by a DHCP Unique Identifier (DUID) included in the client identifier and server identifier options. Static or dynamic address prefixes may be assigned by a DHCPv6 server based on the client's DUID.

EXAMPLE

```
ES-3026#show ipv6 dhcp duid
DHCPv6 Unique Identifier (DUID): 0001-0001-4A8158B4-00E00C0000FD
ES-3026#
```

show ipv6 dhcp vlan

This command shows DHCPv6 information for the specified interface(s).

SYNTAX

show ipv6 dhcp vlan *vlan-id*

vlan-id - VLAN ID, specified as a single number, a range of consecutive numbers separated by a hyphen, or multiple numbers separated by commas. (Range: 1-4093, no leading zeroes)

COMMAND MODE

Privileged Exec

EXAMPLE

```
ES-3026#show ipv6 dhcp vlan 1
VLAN 1 is in DHCP client mode, Rapid-Commit
 List of known servers:
  Server address : FE80::250:FCFF:FEF9:A494
  DUID           : 0001-0001-48CFB0D5-F48F2A006801

  Server address : FE80::250:FCFF:FEF9:A405
  DUID           : 0001-0001-38CF5AB0-F48F2A003917
ES-3026#
```

42 IP INTERFACE COMMANDS

An IP Version 4 and Version 6 address may be used for management access to the switch over the network. Both IPv4 or IPv6 addresses can be used simultaneously to access the switch. You can manually configure a specific IPv4 or IPv6 address or direct the switch to obtain an IPv4 address from a BOOTP or DHCP server when it is powered on. An IPv6 address can either be manually configured or dynamically generated.

An IPv4 address for this switch is obtained via DHCP by default for VLAN 1. You may also need to a establish an IPv4 or IPv6 default gateway between this device and management stations that exist on another network segment.

Table 137: IP Interface Commands

Command Group	Function
IPv4 Interface	Configures an IPv4 address for the switch
IPv6 Interface	Configures an IPv6 address for the switch

IPV4 INTERFACE

There are no IP addresses assigned to this switch by default. You must manually configure a new address to manage the switch over your network or to connect the switch to existing IP subnets. You may also need to a establish a default gateway between this device and management stations or other devices that exist on another network segment

This section includes commands for configuring IP interfaces, the Address Resolution Protocol (ARP) and Proxy ARP.

Table 138: IPv4 Interface Commands

Command Group	Function
Basic IPv4 Configuration	Configures the IP address for interfaces and the gateway router
ARP Configuration	Configures static, dynamic and proxy ARP service

BASIC IPV4 CONFIGURATION

This section describes commands used to configure IP addresses for VLAN interfaces on the switch.

Table 139: 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 default-gateway	Displays the default gateway configured for this device	PE
show ip interface	Displays the IP settings for this device	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**}

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.

DEFAULT SETTING

IP Address: 192.168.1.10
Subnet Mask: 255.255.255.0

COMMAND MODE

Interface Configuration (VLAN)

COMMAND USAGE

- An IP address must be assigned to this device to gain management access over the network or to connect the switch to existing IP subnets. A specific IP address can be manually configured, or the switch 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.

- 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 switch.

EXAMPLE

In the following example, the device is assigned an address in VLAN 1.

```
ES-3026(config)#interface vlan 1
ES-3026(config-if)#ip address 192.168.1.5 255.255.255.0
ES-3026(config-if)#
```

RELATED COMMANDS

ip dhcp restart client (896)
ipv6 address (911)

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

- A default gateway can only be successfully set when a network interface that directly connects to the gateway has been configured on the switch.
- A gateway must be defined if the management station is located in a different IP segment.

EXAMPLE

The following example defines a default gateway for this device:

```
ES-3026(config)#ip default-gateway 10.1.1.254
ES-3026(config)#
```

RELATED COMMANDS

ipv6 default-gateway (910)

show ip default-gateway

This command shows the IPv4 default gateway configured for this device.

DEFAULT SETTING

None

COMMAND MODE

Privileged Exec

EXAMPLE

```
Console#show ip redirects
ip default gateway 10.1.0.254
Console#
```

RELATED COMMANDS

ip default-gateway (903)
show ipv6 default-gateway (918)

show ip interface

This command displays the settings of an IPv4 interface.

COMMAND MODE

Privileged Exec

EXAMPLE

```
ES-3026#show ip interface
Vlan 1 is Administrative Up - Link Up
  Address is 00-E0-0C-00-00-FD (via 00-E0-0C-00-00-FD)
  Index: 1001, MTU: 1500, Bandwidth: 1g
  Address Mode is DHCP
  IP Address: 192.168.0.3 Mask: 255.255.255.0
  Proxy ARP is disabled
ES-3026#
```

RELATED COMMANDS

ip address (902)
show ipv6 interface (919)

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 time out (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 time out has been reached, may indicate this problem with the target device.

EXAMPLE

```
ES-3026#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.
ES-3026#
```

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 886). If necessary, local devices can also be specified in the DNS static host table (see page 888).

EXAMPLE
```
ES-3026#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
ES-3026#
```

RELATED COMMANDS
interface (678)

ARP CONFIGURATION
This section describes commands used to configure the Address Resolution Protocol (ARP) on the switch.

Table 140: Address Resolution Protocol Commands

Command	Function	Mode
arp timeout	Sets the time a dynamic entry remains in the ARP cache	GC

Table 140: Address Resolution Protocol Commands

Command	Function	Mode
clear arp-cache	Deletes all dynamic entries from the ARP cache	PE
show arp	Displays entries in the ARP cache	NE, PE

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).

```
ES-3026(config)#arp timeout 900
ES-3026(config)#
```

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.

```
ES-3026#clear arp-cache
This operation will delete all the dynamic entries in ARP Cache.
Are you sure to continue this operation (y/n)?y
ES-3026#
```

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.

```
ES-3026#show arp
ARP Cache Timeout: 1200 (seconds)

IP Address      MAC Address       Type      Interface
--------------- ----------------- --------- -----------
10.1.0.0        FF-FF-FF-FF-FF-FF other     VLAN1
10.1.0.254      00-00-AB-CD-00-00 other     VLAN1
10.1.0.255      FF-FF-FF-FF-FF-FF other     VLAN1
123.20.10.123   02-10-20-30-40-50 static    VLAN2
145.30.20.23    09-50-40-30-20-10 dynamic   VLAN3

Total entry : 5
ES-3026#
```

IPv6 INTERFACE

This switch supports the following IPv6 interface commands.

Table 141: IPv6 Configuration Commands

Command	Function	Mode
Interface Address Configuration and Utilities		
ipv6 default-gateway	Sets an IPv6 default gateway for traffic	GC
ipv6 address	Configures an IPv6 global unicast address, and enables IPv6 on an interface	IC
ipv6 address autoconfig	Enables automatic configuration of IPv6 global unicast addresses on an interface and enables IPv6 on the interface	IC
ipv6 address eui-64	Configures an IPv6 global unicast address for an interface using an EUI-64 interface ID in the low order 64 bits, and enables IPv6 on the interface	IC
ipv6 address link-local	Configures an IPv6 link-local address for an interface and enables IPv6 on the interface	IC
ipv6 enable	Enables IPv6 on an interface that has not been configured with an explicit IPv6 address	IC
ipv6 mtu	Sets the size of the maximum transmission unit (MTU) for IPv6 packets sent on an interface	IC
show ipv6 default-gateway	Displays the current IPv6 default gateway	NE, PE
show ipv6 interface	Displays the usability and configured settings for IPv6 interfaces	NE, PE
show ipv6 mtu	Displays maximum transmission unit (MTU) information for IPv6 interfaces	NE, PE
show ipv6 traffic	Displays statistics about IPv6 traffic	NE, PE
clear ipv6 traffic	Resets IPv6 traffic counters	PE
ping6	Sends IPv6 ICMP echo request packets to another node on the network	PE
Neighbor Discovery		
ipv6 nd dad attempts	Configures the number of consecutive neighbor solicitation messages sent on an interface during duplicate address detection	IC
ipv6 nd ns-interval	Configures the interval between IPv6 neighbor solicitation retransmissions on an interface	IC
ipv6 nd reachable-time	Configures the amount of time that a remote IPv6 node is considered reachable after some reachability confirmation event has occurred	IC
clear ipv6 neighbors	Deletes all dynamic entries in the IPv6 neighbor discovery cache	PE
show ipv6 neighbors	Displays information in the IPv6 neighbor discovery cache	PE

ipv6 default-gateway

This command sets an IPv6 default gateway to use when the destination is located in a different network segment. Use the **no** form to remove a previously configured default gateway.

SYNTAX

ipv6 default-gateway *ipv6-address*

no ipv6 address

ipv6-address - The IPv6 address of the default next hop router to use when the destination is located in a different network segment.

DEFAULT SETTING

No default gateway is defined

COMMAND MODE

Global Configuration

COMMAND USAGE

- All IPv6 addresses must be according to RFC 2373 “IPv6 Addressing Architecture,” using 8 colon-separated 16-bit hexadecimal values. One double colon may be used in the address to indicate the appropriate number of zeros required to fill the undefined fields.
- The same link-local address may be used by different interfaces/nodes in different zones (RFC 4007). Therefore, when specifying a link-local address, include zone-id information indicating the VLAN identifier after the % delimiter. For example, FE80::7272%1 identifies VLAN 1 as the interface from which the ping is sent.
- An IPv6 default gateway must be defined if the destination has been assigned an IPv6 address and is located in a different IP segment.
- An IPv6 default gateway can only be successfully set when a network interface that directly connects to the gateway has been configured on the switch.

EXAMPLE

The following example defines a default gateway for this device:

```
ES-3026(config)#ipv6 default-gateway FE80::269:3EF9:FE19:6780
ES-3026(config)#
```

RELATED COMMANDS

show ipv6 default-gateway (918)
ip default-gateway (903)

ipv6 address

This command configures an IPv6 global unicast address and enables IPv6 on an interface. Use the **no** form without any arguments to remove all IPv6 addresses from the interface, or use the **no** form with a specific IPv6 address to remove that address from the interface.

SYNTAX

[**no**] **ipv6 address** *ipv6-address/prefix-length*

ipv6-address - A full IPv6 address including the network prefix and host address bits.

prefix-length - A decimal value indicating how many contiguous bits (from the left) of the address comprise the prefix (i.e., the network portion of the address).

DEFAULT SETTING

No IPv6 addresses are defined

COMMAND MODE

Interface Configuration (VLAN)

COMMAND USAGE

- All IPv6 addresses must be according to RFC 2373 “IPv6 Addressing Architecture,” using 8 colon-separated 16-bit hexadecimal values. One double colon may be used in the address to indicate the appropriate number of zeros required to fill the undefined fields.
- To connect to a larger network with multiple subnets, you must configure a global unicast address. This address can be manually configured with this command, or it can be automatically configured using the ip ipv6 address autoconfig command.
- If a link-local address has not yet been assigned to this interface, this command will assign the specified static global unicast address and also dynamically generate a link-local unicast address for the interface. (The link-local address is made with an address prefix of FE80 and a host portion based the switch’s MAC address in modified EUI-64 format.)
- If a duplicate address is detected, a warning message is sent to the console.

EXAMPLE

This example specifies a full IPv6 address and prefix length.

```
ES-3026(config)#interface vlan 1
ES-3026(config-if)#ipv6 address 2001:DB8:2222:7272::72/96
ES-3026(config-if)#end
ES-3026#show ipv6 interface
Vlan 1 is up
IPv6 is enable.
Link-local address:
  FE80::2E0:CFF:FE00:FD/64
Global unicast address(es):
  2001:DB8:2222:7272::72/96, subnet is 2001:DB8:2222:7272::/96
```

```
Joined group address(es):
FF02::1:FF00:72
FF02::1:FF00:FD
FF02::1
IPv6 link MTU is 1500 bytes
ND DAD is enabled, number of DAD attempts: 3.
ND retransmit interval is 1000 milliseconds

ES-3026#
```

RELATED COMMANDS

ipv6 address eui-64 (913)
ipv6 address autoconfig (912)
show ipv6 interface (919)
ip address (902)

ipv6 address autoconfig

This command enables stateless autoconfiguration of IPv6 addresses on an interface and enables IPv6 on the interface. The network portion of the address is based on prefixes received in IPv6 router advertisement messages; the host portion in based on the modified EUI-64 form of the interface identifier (i.e., the switch's MAC address). Use the **no** form to remove the address generated by this command.

SYNTAX

[**no**] **ipv6 address autoconfig**

DEFAULT SETTING

No IPv6 addresses are defined

COMMAND MODE

Interface Configuration (VLAN)

COMMAND USAGE

- If a link local address has not yet been assigned to this interface, this command will dynamically generate a global unicast address and a link local address for the interface. (The link-local address is made with an address prefix of FE80 and a host portion based the switch's MAC address in modified EUI-64 format.)
- If a duplicate address is detected, a warning message is sent to the console.
- If the router advertisements have the "other stateful configuration" flag set, the switch will attempt to acquire other non-address configuration information (such as a default gateway).

EXAMPLE

This example assigns two dynamic global unicast address of 2005::212:CFFF:FE0B:4600 and 3FFE:501:FFFF:100:212:CFFF:FE0B:4600 to the switch.

```
ES-3026(config-if)#ipv6 address autoconfig
ES-3026(config-if)#end
ES-3026#show ipv6 interface
Vlan 1 is up
IPv6 is enable.
Link-local address:
  FE80::212:CFFF:FE0B:4600/64
Global unicast address(es):
  2005::212:CFFF:FE0B:4600, subnet is 2005:0:0:0::/64
  3FFE:501:FFFF:100:212:CFFF:FE0B:4600, subnet is 3FFE:501:FFFF:100::/64
Joined group address(es):
  FF01::1/16
  FF02::1/16
  FF02::1:FF0B:4600/104
MTU is 1500 bytes.
ND DAD is enabled, number of DAD attempts: 1.
ND retransmit interval is 1000 milliseconds

ES-3026#
```

RELATED COMMANDS

ipv6 address (911)
show ipv6 interface (919)

ipv6 address eui-64

This command configures an IPv6 address for an interface using an EUI-64 interface ID in the low order 64 bits and enables IPv6 on the interface. Use the **no** form without any arguments to remove all manually configured IPv6 addresses from the interface. Use the **no** form with a specific address to remove it from the interface.

SYNTAX

ipv6 address *ipv6-prefix/prefix-length eui*-**64**

no ipv6 address [*ipv6-prefix/prefix-length* **eui-64**]

ipv6-prefix - The IPv6 network portion of the address assigned to the interface.

prefix-length - A decimal value indicating how many contiguous bits (from the left) of the address comprise the prefix (i.e., the network portion of the address).

DEFAULT SETTING

No IPv6 addresses are defined

COMMAND MODE

Interface Configuration (VLAN)

COMMAND USAGE

- The prefix must be formatted according to RFC 2373 “IPv6 Addressing Architecture,” using 8 colon-separated 16-bit hexadecimal values. One double colon may be used in the address to indicate the appropriate number of zeros required to fill the undefined fields.

- If a link local address has not yet been assigned to this interface, this command will dynamically generate a global unicast address and a link-local address for this interface. (The link-local address is made with an address prefix of FE80 and a host portion based the switch’s MAC address in modified EUI-64 format.)

- Note that the value specified in the ipv6-prefix may include some of the high-order host bits if the specified prefix length is less than 64 bits. If the specified prefix length exceeds 64 bits, then the network portion of the address will take precedence over the interface identifier.

- If a duplicate address is detected, a warning message is sent to the console.

- IPv6 addresses are 16 bytes long, of which the bottom 8 bytes typically form a unique host identifier based on the device’s MAC address. The EUI-64 specification is designed for devices that use an extended 8-byte MAC address. For devices that still use a 6-byte MAC address (also known as EUI-48 format), it must be converted into EUI-64 format by inverting the universal/local bit in the address and inserting the hexadecimal number FFFE between the upper and lower three bytes of the MAC address.

- For example, if a device had an EUI-48 address of 28-9F-18-1C-82-35, the global/local bit must first be inverted to meet EUI-64 requirements (i.e., 1 for globally defined addresses and 0 for locally defined addresses), changing 28 to 2A. Then the two bytes FFFE are inserted between the OUI (i.e., company id) and the rest of the address, resulting in a modified EUI-64 interface identifier of 2A-9F-18-FF-FE-1C-82-35.

- This host addressing method allows the same interface identifier to be used on multiple IP interfaces of a single device, as long as those interfaces are attached to different subnets.

EXAMPLE

This example uses the network prefix of 2001:0DB8:0:1::/64, and specifies that the EUI-64 interface identifier be used in the lower 64 bits of the address.

```
ES-3026(config)#interface vlan 1
ES-3026(config-if)#ipv6 address 2001:0DB8:0:1::/64 eui-64
ES-3026(config-if)#end
ES-3026#show ipv6 interface
Vlan 1 is up
IPv6 is enable.
Link-local address:
  FE80::2E0:CFF:FE00:FD/64
```

```
Global unicast address(es):
  2001:DB8::1:2E0:CFF:FE00:FD/64, subnet is 2001:DB8::1:0:0:0:0/64[EUI]
  2001:DB8:2222:7272::72/96, subnet is 2001:DB8:2222:7272::/96[EUI]
Joined group address(es):
FF02::1:FF00:72
FF02::1:FF00:FD
FF02::1
IPv6 link MTU is 1500 bytes
ND DAD is enabled, number of DAD attempts: 3.
ND retransmit interval is 1000 milliseconds

ES-3026#
```

RELATED COMMANDS

ipv6 address autoconfig (912)
show ipv6 interface (919)

ipv6 address link-local

This command configures an IPv6 link-local address for an interface and enables IPv6 on the interface. Use the **no** form without any arguments to remove all manually configured IPv6 addresses from the interface. Use the **no** form with a specific address to remove it from the interface.

SYNTAX

ipv6 address *ipv6-address* **link-local**

no ipv6 address [*ipv6-address* **link-local**]

ipv6-address - The IPv6 address assigned to the interface.

DEFAULT SETTING

No IPv6 addresses are defined

COMMAND MODE

Interface Configuration (VLAN)

COMMAND USAGE

- The specified address must be formatted according to RFC 2373 “IPv6 Addressing Architecture,” using 8 colon-separated 16-bit hexadecimal values. One double colon may be used in the address to indicate the appropriate number of zeros required to fill the undefined fields. And the address prefix must be FE80.
- The address specified with this command replaces a link-local address that was automatically generated for the interface.
- You can configure multiple IPv6 global unicast addresses per interface, but only one link-local address per interface.
- If a duplicate address is detected, a warning message is sent to the console.

EXAMPLE

This example assigns a link-local address of FE80::269:3EF9:FE19:6779 to VLAN 1. Note that the prefix FE80 is required for link-local addresses, and the first 16-bit group in the host address is padded with a zero in the form 0269.

```
ES-3026(config)#interface vlan 1
ES-3026(config-if)#ipv6 address FE80::269:3EF9:FE19:6779 link-local
ES-3026(config-if)#end
ES-3026#show ipv6 interface
Vlan 1 is up
IPv6 is enable.
Link-local address:
  FE80::269:3EF9:FE19:6779/64
Global unicast address(es):
  2001:DB8::1:2E0:CFF:FE00:FD/64, subnet is 2001:DB8::1:0:0:0:0/64[EUI]
  2001:DB8:2222:7272::72/96, subnet is 2001:DB8:2222:7272::/96[EUI]
Joined group address(es):
FF02::1:FF19:6779
FF02::1:FF00:72
FF02::1:FF00:FD
FF02::1
IPv6 link MTU is 1500 bytes
ND DAD is enabled, number of DAD attempts: 3.
ND retransmit interval is 1000 milliseconds

ES-3026#
```

RELATED COMMANDS

ipv6 enable (916)
show ipv6 interface (919)

ipv6 enable

This command enables IPv6 on an interface that has not been configured with an explicit IPv6 address. Use the **no** form to disable IPv6 on an interface that has not been configured with an explicit IPv6 address.

SYNTAX

[no] ipv6 enable

DEFAULT SETTING

IPv6 is disabled

COMMAND MODE

Interface Configuration (VLAN)

COMMAND USAGE

- This command enables IPv6 on the current VLAN interface and automatically generates a link-local unicast address. The address prefix uses FE80, and the host portion of the address is generated by converting the switch's MAC address to modified EUI-64 format (see page 913). This address type makes the switch accessible over IPv6 for all devices attached to the same local subnet.

- If a duplicate address is detected on the local segment, this interface will be disabled and a warning message displayed on the console.
- The **no ipv6 enable** command does not disable IPv6 for an interface that has been explicitly configured with an IPv6 address.

EXAMPLE

In this example, IPv6 is enabled on VLAN 1, and the link-local address FE80::2E0:CFF:FE00:FD/64 is automatically generated by the switch.

```
ES-3026(config)#interface vlan 1
ES-3026(config-if)#ipv6 enable
ES-3026(config-if)#end
ES-3026#show ipv6 interface
Vlan 1 is up
IPv6 is enable.
Link-local address:
  FE80::2E0:CFF:FE00:FD/64
Global unicast address(es):
  2001:DB8:2222:7273::72/96, subnet is 2001:DB8:2222:7273::/96
Joined group address(es):
FF02::1:FF00:72
FF02::1:FF00:FD
FF02::1
IPv6 link MTU is 1280 bytes
ND DAD is enabled, number of DAD attempts: 3.
ND retransmit interval is 1000 milliseconds

ES-3026#
```

RELATED COMMANDS

ipv6 address link-local (915)
show ipv6 interface (919)

ipv6 mtu

This command sets the size of the maximum transmission unit (MTU) for IPv6 packets sent on an interface. Use the **no** form to restore the default setting.

SYNTAX

ipv6 mtu *size*

no ipv6 mtu

size - Specifies the MTU size. (Range: 1280-65535 bytes)

DEFAULT SETTING

1500 bytes

COMMAND MODE

Interface Configuration (VLAN)

COMMAND USAGE

- IPv6 routers do not fragment IPv6 packets forwarded from other routers. However, traffic originating from an end-station connected to an IPv6 router may be fragmented.
- All devices on the same physical medium must use the same MTU in order to operate correctly.
- IPv6 must be enabled on an interface before the MTU can be set.

EXAMPLE

The following example sets the MTU for VLAN 1 to 1280 bytes:

```
ES-3026(config)#interface vlan 1
ES-3026(config-if)#ipv6 mtu 1280
ES-3026(config-if)#
```

RELATED COMMANDS

show ipv6 mtu (920)
jumbo frame (488)

show ipv6 default-gateway

This command displays the current IPv6 default gateway.

COMMAND MODE

Normal Exec, Privileged Exec

EXAMPLE

The following shows the default gateway configured for this device:

```
ES-3026#show ipv6 default-gateway
IPv6 default gateway 2001:DB8:2222:7272::254

ES-3026#
```

show ipv6 interface

This command displays the usability and configured settings for IPv6 interfaces.

SYNTAX

show ipv6 interface [**brief** [**vlan** *vlan-id* [*ipv6-prefix*/*prefix-length*]]]

brief - Displays a brief summary of IPv6 operational status and the addresses configured for each interface.

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

ipv6-prefix - The IPv6 network portion of the address assigned to the interface. The prefix must be formatted according to RFC 2373 “IPv6 Addressing Architecture,” using 8 colon-separated 16-bit hexadecimal values. One double colon may be used in the address to indicate the appropriate number of zeros required to fill the undefined fields.

prefix-length - A decimal value indicating how many of the contiguous bits (from the left) of the address comprise the prefix (i.e., the network portion of the address).

COMMAND MODE

Normal Exec, Privileged Exec

EXAMPLE

This example displays all the IPv6 addresses configured for the switch.

```
ES-3026#show ipv6 interface
Vlan 1 is up
IPv6 is enable.
Link-local address:
  FE80::2E0:CFF:FE00:FD/64
Global unicast address(es):
  2001:DB8:2222:7273::72/96, subnet is 2001:DB8:2222:7273::/96
Joined group address(es):
FF02::1:FF00:72
FF02::1:FF00:FD
FF02::1
IPv6 link MTU is 1280 bytes
ND DAD is enabled, number of DAD attempts: 3.
ND retransmit interval is 1000 milliseconds

ES-3026#
```

Table 142: show ipv6 interface - display description

Field	Description
VLAN	A VLAN is marked “up” if the switch can send and receive packets on this interface, “down” if a line signal is not present, or “administratively down” if the interface has been disabled by the administrator.
IPv6	IPv6 is marked “enable” if the switch can send and receive IP traffic on this interface, “disable” if the switch cannot send and receive IP traffic on this interface, or “stalled” if a duplicate link-local address is detected on the interface.

Table 142: show ipv6 interface - display description (Continued)

Field	Description
Link-local address	Shows the link-local address assigned to this interface
Global unicast address(es)	Shows the global unicast address(es) assigned to this interface
Joined group address(es)	In addition to the unicast addresses assigned to an interface, a host is also required to listen to all-nodes multicast addresses FF01::1 (interface-local scope) and FF02::1 (link-local scope). FF01::1/16 is the transient interface-local multicast address for all attached IPv6 nodes, and FF02::1/16 is the link-local multicast address for all attached IPv6 nodes. The interface-local multicast address is only used for loopback transmission of multicast traffic. Link-local multicast addresses cover the same types as used by link-local unicast addresses, including all nodes (FF02::1), all routers (FF02::2), and solicited nodes (FF02::1:FFXX:XXXX) as described below. A node is also required to compute and join the associated solicited-node multicast addresses for every unicast and anycast address it is assigned. IPv6 addresses that differ only in the high-order bits, e.g. due to multiple high-order prefixes associated with different aggregations, will map to the same solicited-node address, thereby reducing the number of multicast addresses a node must join. In this example, FF02::1:FF90:0/104 is the solicited-node multicast address which is formed by taking the low-order 24 bits of the address and appending those bits to the prefix.
ND DAD	Indicates whether (neighbor discovery) duplicate address detection is enabled.
number of DAD attempts	The number of consecutive neighbor solicitation messages sent on the interface during duplicate address detection.
ND retransmit interval	The interval between IPv6 neighbor solicitation retransmissions sent on an interface during duplicate address detection.

This example displays a brief summary of IPv6 addresses configured on the switch.

```
ES-3026#show ipv6 interface brief
Interface       VLAN       IPv6       IPv6 Address
--------------- ---------- ---------- ------------------------------------
VLAN 1          Up         Up         2001:DB8:2222:7273::72/96
VLAN 1          Up         Up         FE80::2E0:CFF:FE00:FD%1/64
ES-3026#
```

RELATED COMMANDS

show ip interface (904)

show ipv6 mtu

This command displays the maximum transmission unit (MTU) cache for destinations that have returned an ICMP packet-too-big message along with an acceptable MTU to this switch.

COMMAND MODE

Normal Exec, Privileged Exec

EXAMPLE

The following example shows the MTU cache for this device:

```
ES-3026#show ipv6 mtu
MTU     Since   Destination Address
1400    00:04:21  5000:1::3
1280    00:04:50  FE80::203:A0FF:FED6:141D
ES-3026#
```

Table 143: show ipv6 mtu - display description*

Field	Description
MTU	Adjusted MTU contained in the ICMP packet-too-big message returned from this destination, and now used for all traffic sent along this path.
Since	Time since an ICMP packet-too-big message was received from this destination.
Destination Address	Address which sent an ICMP packet-too-big message.

* No information is displayed if an IPv6 address has not been assigned to the switch.

show ipv6 traffic

This command displays statistics about IPv6 traffic passing through this switch.

COMMAND MODE

Normal Exec, Privileged Exec

EXAMPLE

The following example shows statistics for all IPv6 unicast and multicast traffic, as well as ICMP, UDP and TCP statistics:

```
ES-3026#show ipv6 traffic
IPv6 Statistics:
IPv6 recived
                     total received
                     header errors
                     too big errors
                     no routes
                     address errors
                     unknown protocols
                     truncated packets
                     discards
                     delivers
                     reassembly request datarams
                     reassembled succeeded
                     reassembled failed
IPv6 sent
                     forwards datagrams
                  15 requests
                     discards
                     no routes
                     generated fragments
                     fragment succeeded
                     fragment failed
```

```
ICMPv6 Statistics:
ICMPv6 received
                     input
                     errors
                     destination unreachable messages
                     packet too big messages
                     time exceeded messages
                     parameter problem message
                     echo request messages
                     echo reply messages
                     redirect messages
                     group membership query messages
                     group membership response messages
                     group membership reduction messages
                     router solicit messages
                     router advertisement messages
                     neighbor solicit messages
                     neighbor advertisement messages
                     redirect messages
ICMPv6 sent
                  15 output
                     destination unreachable messages
                     packet too big messages
                     time exceeded messages
                     parameter problem message
                     echo reply messages
                   7 router solicit messages
                   3 neighbor solicit messages
                     neighbor advertisement messages
                     redirect messages
                     group membership response messages
                     group membership reduction messages
UDP Statistics:
                     input
                     no port errors
                     other errors
                     output
ES-3026#
```

Table 144: show ipv6 traffic - display description

Field	Description
IPv6 Statistics	
IPv6 recived	
total received	The total number of input datagrams received by the interface, including those received in error.
header errors	The number of input datagrams discarded due to errors in their IPv6 headers, including version number mismatch, other format errors, hop count exceeded, IPv6 options, etc.
too big errors	The number of input datagrams that could not be forwarded because their size exceeded the link MTU of outgoing interface.
no routes	The number of input datagrams discarded because no route could be found to transmit them to their destination.
address errors	The number of input datagrams discarded because the IPv6 address in their IPv6 header's destination field was not a valid address to be received at this entity. This count includes invalid addresses (e.g., ::0) and unsupported addresses (e.g., addresses with unallocated prefixes). For entities which are not IPv6 routers and therefore do not forward datagrams, this counter includes datagrams discarded because the destination address was not a local address.

Table 144: show ipv6 traffic - display description (Continued)

Field	Description
unknown protocols	The number of locally-addressed datagrams received successfully but discarded because of an unknown or unsupported protocol. This counter is incremented at the interface to which these datagrams were addressed which might not be necessarily the input interface for some of the datagrams.
truncated packets	The number of input datagrams discarded because datagram frame didn't carry enough data.
discards	The number of input IPv6 datagrams for which no problems were encountered to prevent their continued processing, but which were discarded (e.g., for lack of buffer space). Note that this counter does not include any datagrams discarded while awaiting re-assembly.
delivers	The total number of datagrams successfully delivered to IPv6 user-protocols (including ICMP). This counter is incremented at the interface to which these datagrams were addressed which might not be necessarily the input interface for some of the datagrams.
reassembly request datagrams	The number of IPv6 fragments received which needed to be reassembled at this interface. Note that this counter is incremented at the interface to which these fragments were addressed which might not be necessarily the input interface for some of the fragments.
reassembled succeeded	The number of IPv6 datagrams successfully reassembled. Note that this counter is incremented at the interface to which these datagrams were addressed which might not be necessarily the input interface for some of the fragments.
reassembled failed	The number of failures detected by the IPv6 re-assembly algorithm (for whatever reason: timed out, errors, etc.). Note that this is not necessarily a count of discarded IPv6 fragments since some algorithms (notably the algorithm in RFC 815) can lose track of the number of fragments by combining them as they are received. This counter is incremented at the interface to which these fragments were addressed which might not be necessarily the input interface for some of the fragments.
IPv6 sent	
forwards datagrams	The number of output datagrams which this entity received and forwarded to their final destinations. In entities which do not act as IPv6 routers, this counter will include only those packets which were Source-Routed via this entity, and the Source-Route processing was successful. Note that for a successfully forwarded datagram the counter of the outgoing interface is incremented.
requests	The total number of IPv6 datagrams which local IPv6 user-protocols (including ICMP) supplied to IPv6 in requests for transmission. Note that this counter does not include any datagrams counted in ipv6IfStatsOutForwDatagrams.
discards	The number of output IPv6 datagrams for which no problem was encountered to prevent their transmission to their destination, but which were discarded (e.g., for lack of buffer space). Note that this counter would include datagrams counted in ipv6IfStatsOutForwDatagrams if any such packets met this (discretionary) discard criterion.
no routes	The number of input datagrams discarded because no route could be found to transmit them to their destination.
generated fragments	The number of output datagram fragments that have been generated as a result of fragmentation at this output interface.
fragment succeeded	The number of IPv6 datagrams that have been successfully fragmented at this output interface.

Table 144: show ipv6 traffic - display description (Continued)

Field	Description
fragment failed	The number of IPv6 datagrams that have been discarded because they needed to be fragmented at this output interface but could not be.
ICMPv6 Statistics	
ICMPv6 received	
input	The total number of ICMP messages received by the interface which includes all those counted by ipv6IfIcmpInErrors. Note that this interface is the interface to which the ICMP messages were addressed which may not be necessarily the input interface for the messages.
errors	The number of ICMP messages which the interface received but determined as having ICMP-specific errors (bad ICMP checksums, bad length, etc.).
destination unreachable messages	The number of ICMP Destination Unreachable messages received by the interface.
packet too big messages	The number of ICMP Packet Too Big messages received by the interface.
time exceeded messages	The number of ICMP Time Exceeded messages received by the interface.
parameter problem message	The number of ICMP Parameter Problem messages received by the interface.
echo request messages	The number of ICMP Echo (request) messages received by the interface.
echo reply messages	The number of ICMP Echo Reply messages received by the interface.
redirect messages	The number of Redirect messages received by the interface.
group membership query messages	The number of ICMPv6 Group Membership Query messages received by the interface.
group membership response messages	The number of ICMPv6 Group Membership Response messages received by the interface.
group membership reduction messages	The number of ICMPv6 Group Membership Reduction messages received by the interface.
router solicit messages	The number of ICMP Router Solicit messages received by the interface.
router advertisement messages	The number of ICMP Router Advertisement messages received by the interface.
neighbor solicit messages	The number of ICMP Neighbor Solicit messages received by the interface.
neighbor advertisement messages	The number of ICMP Neighbor Advertisement messages received by the interface.
redirect messages	The number of Redirect messages received by the interface.
ICMPv6 sent	
output	The total number of ICMP messages which this interface attempted to send. Note that this counter includes all those counted by icmpOutErrors.
destination unreachable messages	The number of ICMP Destination Unreachable messages sent by the interface.
packet too big messages	The number of ICMP Packet Too Big messages sent by the interface.

Table 144: show ipv6 traffic - display description (Continued)

Field	Description
time exceeded messages	The number of ICMP Time Exceeded messages sent by the interface.
parameter problem message	The number of ICMP Parameter Problem messages sent by the interface.
echo reply messages	The number of ICMP Echo Reply messages sent by the interface.
router solicit messages	The number of ICMP Router Solicitation messages sent by the interface.
neighbor advertisement messages	The number of ICMP Router Advertisement messages sent by the interface.
redirect messages	The number of Redirect messages sent. For a host, this object will always be zero, since hosts do not send redirects.
group membership response messages	The number of ICMPv6 Group Membership Response messages sent.
group membership reduction messages	The number of ICMPv6 Group Membership Reduction messages sent.
UDP Statistics	
input	The total number of UDP datagrams delivered to UDP users.
no port errors	The total number of received UDP datagrams for which there was no application at the destination port.
other errors	The number of received UDP datagrams that could not be delivered for reasons other than the lack of an application at the destination port.
output	The total number of UDP datagrams sent from this entity.

clear ipv6 traffic

This command resets IPv6 traffic counters.

COMMAND MODE

Privileged Exec

COMMAND USAGE

This command resets all of the counters displayed by the show ipv6 traffic command.

EXAMPLE

```
ES-3026#clear ipv6 traffic
ES-3026#
```

ping6

This command sends (IPv6) ICMP echo request packets to another node on the network.

SYNTAX

ping6 {*ipv6-address* | *host-name*} [**count** *count*] [**size** *size*]

ipv6-address - The IPv6 address of a neighbor device. You can specify either a link-local or global unicast address formatted according to RFC 2373 "IPv6 Addressing Architecture," using 8 colon-separated 16-bit hexadecimal values. One double colon may be used in the address to indicate the appropriate number of zeros required to fill the undefined fields.

host-name - A host name string which can be resolved into an IPv6 address through a domain name server.

count - Number of packets to send. (Range: 1-16)

size - Number of bytes in a packet. (Range: 48-18024 bytes) The actual packet size will be eight bytes larger than the size specified because the router adds header information.

DEFAULT SETTING

count: 5
size: 100 bytes

COMMAND MODE

Privileged Exec

COMMAND USAGE

- Use the **ping6** command to see if another site on the network can be reached, or to evaluate delays over the path.
- The same link-local address may be used by different interfaces/nodes in different zones (RFC 4007). Therefore, when specifying a link-local address, include zone-id information indicating the VLAN identifier after the % delimiter. For example, FE80::7272%1 identifies VLAN 1 as the interface from which the ping is sent.
- When pinging a host name, be sure the DNS server has been enabled (see page 886). If necessary, local devices can also be specified in the DNS static host table (see page 888).
- When using ping6 with a host name, the switch first attempts to resolve the alias into an IPv6 address before trying to resolve it into an IPv4 address.

EXAMPLE

```
ES-3026#ping6 FE80::2E0:CFF:FE00:FC%1/64
Type ESC to abort.
PING to FE80::2E0:CFF:FE00:FC%1/64, by 5 32-byte payload ICMP packets,
  timeout is 3 seconds
response time: 20 ms    [FE80::2E0:CFF:FE00:FC] seq_no: 1
response time: 0 ms     [FE80::2E0:CFF:FE00:FC] seq_no: 2
response time: 0 ms     [FE80::2E0:CFF:FE00:FC] seq_no: 3
```

```
response time: 0 ms     [FE80::2E0:CFF:FE00:FC] seq_no: 4
response time: 0 ms     [FE80::2E0:CFF:FE00:FC] seq_no: 5
Ping statistics for FE80::2E0:CFF:FE00:FC%1/64:
 5 packets transmitted, 5 packets received (100%), 0 packets lost (0%)
Approximate round trip times:
 Minimum = 0 ms, Maximum = 20 ms, Average = 4 ms
ES-3026#
```

ipv6 nd dad attempts

This command configures the number of consecutive neighbor solicitation messages sent on an interface during duplicate address detection. Use the **no** form to restore the default setting.

SYNTAX

ipv6 nd dad attempts *count*

no ipv6 nd dad attempts

count - The number of neighbor solicitation messages sent to determine whether or not a duplicate address exists on this interface. (Range: 0-600)

DEFAULT SETTING

1

COMMAND MODE

Interface Configuration (VLAN)

COMMAND USAGE

- Configuring a value of 0 disables duplicate address detection.
- Duplicate address detection determines if a new unicast IPv6 address already exists on the network before it is assigned to an interface.
- Duplicate address detection is stopped on any interface that has been suspended (see the vlan command). While an interface is suspended, all unicast IPv6 addresses assigned to that interface are placed in a “pending” state. Duplicate address detection is automatically restarted when the interface is administratively re-activated.
- An interface that is re-activated restarts duplicate address detection for all unicast IPv6 addresses on the interface. While duplicate address detection is performed on the interface’s link-local address, the other IPv6 addresses remain in a “tentative” state. If no duplicate link-local address is found, duplicate address detection is started for the remaining IPv6 addresses.
- If a duplicate address is detected, it is set to “duplicate” state, and a warning message is sent to the console. If a duplicate link-local address is detected, IPv6 processes are disabled on the interface. If a duplicate global unicast address is detected, it is not used. All configuration commands associated with a duplicate address remain configured while the address is in “duplicate” state.

- If the link-local address for an interface is changed, duplicate address detection is performed on the new link-local address, but not for any of the IPv6 global unicast addresses already associated with the interface.

EXAMPLE

The following configures five neighbor solicitation attempts for addresses configured on VLAN 1. The show ipv6 interface command indicates that the duplicate address detection process is still on-going.

```
ES-3026(config)#interface vlan 1
ES-3026(config-if)#ipv6 nd dad attempts 5
ES-3026(config-if)#end
ES-3026#show ipv6 interface
Vlan 1 is up
IPv6 is stalled.
Link-local address:
  FE80::200:E8FF:FE90:0/64 [TENTATIVE]
Global unicast address(es):
  2009:DB9:2229::79, subnet is 2009:DB9:2229:0::/64 [TENTATIVE]
Joined group address(es):
  FF01::1/16
  FF02::1/16
  FF02::1:FF00:79/104
  FF02::1:FF90:0/104
MTU is 1500 bytes.
ND DAD is enabled, number of DAD attempts: 5.
ND retransmit interval is 1000 milliseconds
ES-3026#
```

RELATED COMMANDS

ipv6 nd ns-interval (928)
show ipv6 neighbors (930)

ipv6 nd ns-interval

This command configures the interval between transmitting IPv6 neighbor solicitation messages on an interface. Use the **no** form to restore the default value.

SYNTAX

ipv6 nd ns-interval *milliseconds*

no ipv6 nd ns-interval

milliseconds - The interval between transmitting IPv6 neighbor solicitation messages. (Range: 1000-3600000)

DEFAULT SETTING

1000 milliseconds is used for neighbor discovery operations

COMMAND MODE

Interface Configuration (VLAN)

COMMAND USAGE

- This command specifies the interval between transmitting neighbor solicitation messages when resolving an address, or when probing the reachability of a neighbor. Therefore, avoid using very short intervals for normal IPv6 operations.

EXAMPLE

The following sets the interval between sending neighbor solicitation messages to 30000 milliseconds:

```
ES-3026(config)#interface vlan 1
ES-3026(config)#pv6 nd ns-interval 30000
ES-3026(config)#end
ES-3026#show ipv6 interface
Vlan 1 is up
IPv6 is enable.
Link-local address:
  FE80::200:E8FF:FE90:0/64
Global unicast address(es):
  2009:DB9:2229::79, subnet is 2009:DB9:2229:0::/64
Joined group address(es):
  FF01::1/16
  FF02::1/16
  FF02::1:FF00:79/104
  FF02::1:FF90:0/104
MTU is 1500 bytes.
ND DAD is enabled, number of DAD attempts: 5.
ND retransmit interval is 30000 milliseconds
ES-3026#
```

RELATED COMMANDS

show running-config (484)

ipv6 nd reachable-time

This command configures the amount of time that a remote IPv6 node is considered reachable after some reachability confirmation event has occurred.

SYNTAX

ipv6 nd reachable-time *milliseconds*

no ipv6 nd reachable-time

milliseconds - The time that a node can be considered reachable after receiving confirmation of reachability.
(Range: 1000-3600000)

DEFAULT SETTING

30000 milliseconds is used for neighbor discovery operations

COMMAND MODE

Interface Configuration (VLAN)

COMMAND USAGE

- The time limit configured by this command allows the switch to detect unavailable neighbors.

EXAMPLE

The following sets the reachable time for a remote node to 1000 milliseconds:

```
ES-3026(config)#interface vlan 1
ES-3026(config)#pv6 nd reachable-time 1000
ES-3026(config)#
```

clear ipv6 neighbors

This command deletes all dynamic entries in the IPv6 neighbor discovery cache.

COMMAND MODE

Privileged Exec

EXAMPLE

The following deletes all dynamic entries in the IPv6 neighbor cache:

```
ES-3026#clear ipv6 neighbors
ES-3026#
```

show ipv6 neighbors

This command displays information in the IPv6 neighbor discovery cache.

SYNTAX

show ipv6 neighbors [**vlan** *vlan-id* | *ipv6-address*]

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

ipv6-address - The IPv6 address of a neighbor device. You can specify either a link-local or global unicast address formatted according to RFC 2373 “IPv6 Addressing Architecture,” using 8 colon-separated 16-bit hexadecimal values. One double colon may be used in the address to indicate the appropriate number of zeros required to fill the undefined fields.

DEFAULT SETTING

All IPv6 neighbor discovery cache entries are displayed.

COMMAND MODE

Privileged Exec

EXAMPLE

The following shows all known IPv6 neighbors for this switch:

```
ES-3026#show ipv6 neighbors
IPv6 Address                Age         Link-layer Addr    State       VLAN
2009:DB9:2229::79           666         00-00-E8-90-00-00  REACH       1
FE80::200:E8FF:FE90:0       671         00-00-E8-90-00-00  REACH       1
ES-3026#
```

Table 145: show ipv6 neighbors - display description

Field	Description
IPv6 Address	IPv6 address of neighbor
Age	The time since the address was verified as reachable (in seconds). A static entry is indicated by the value “Permanent.”
Link-layer Addr	Physical layer MAC address.
State	The following states are used for dynamic entries: INCMP (Incomplete) - Address resolution is being carried out on the entry. A neighbor solicitation message has been sent to the multicast address of the target, but it has not yet returned a neighbor advertisement message. REACH (Reachable) - Positive confirmation was received within the last ReachableTime interval that the forward path to the neighbor was functioning. While in REACH state, the device takes no special action when sending packets. STALE - More than the ReachableTime interval has elapsed since the last positive confirmation was received that the forward path was functioning. While in STALE state, the device takes no action until a packet is sent. DELAY - More than the ReachableTime interval has elapsed since the last positive confirmation was received that the forward path was functioning. A packet was sent within the last DELAY_FIRST_PROBE_TIME interval. If no reachability confirmation is received within this interval after entering the DELAY state, the switch will send a neighbor solicitation message and change the state to PROBE. PROBE - A reachability confirmation is actively sought by resending neighbor solicitation messages every RetransTimer interval until confirmation of reachability is received. UNKNO - Unknown state. The following states are used for static entries: INCMP (Incomplete)-The interface for this entry is down. REACH (Reachable) - The interface for this entry is up. Reachability detection is not applied to static entries in the IPv6 neighbor discovery cache.
VLAN	VLAN interface from which the address was reached.

RELATED COMMANDS

show mac-address-table (739)

SECTION IV

APPENDICES

This section provides additional information and includes these items:

- "Software Specifications" on page 935
- "Troubleshooting" on page 939

A SOFTWARE SPECIFICATIONS

iPECS ES-3000 Series

SOFTWARE FEATURES

MANAGEMENT AUTHENTICATION	Local, RADIUS, TACACS+, Port Authentication (802.1X), HTTPS, SSH, Port Security, IP Filter, DHCP Snooping
CLIENT ACCESS CONTROL	Access Control Lists (512 rules), Port Authentication (802.1X), MAC Authentication, Port Security, DHCP Snooping, IP Source Guard
PORT CONFIGURATION	100BASE-TX: 10/100 Mbps, half/full duplex 100BASE-FX: 100 Mbps at full duplex (SFP) 1000BASE-T: 10/100 Mbps at half/full duplex, 1000 Mbps at full duplex 1000BASE-SX/LX/LH - 1000 Mbps at full duplex (SFP)
FLOW CONTROL	Full Duplex: IEEE 802.3-2005 Half Duplex: Back pressure
STORM CONTROL	Broadcast, multicast, or unicast traffic throttled above a critical threshold
PORT MIRRORING	26 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 256 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 four levels of priority
Strict, Shaped Deficit Weighted Round Robin, or strict-WRR queuing
Layer 3/4 priority mapping: IP DSCP

QUALITY OF SERVICE DiffServ[16] supports class maps, policy maps, and service policies

MULTICAST FILTERING IGMP Snooping (Layer 2)
Multicast VLAN Registration

ADDITIONAL FEATURES BOOTP Client
DHCP Client
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)

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)

16. Currently only supported for IPv4. Will be supported for IPv6 in future release.

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
Link Aggregation Control Protocol (LACP)
Full-duplex flow control (ISO/IEC 8802-3)
IEEE 802.3ac VLAN tagging
DHCP Client (RFC 2131)
HTTPS
ICMP (RFC 792)
IGMP (RFC 1112)
IGMPv2 (RFC 2236)
IGMPv3 (RFC 3376) - partial support
IPv4 IGMP (RFC 3228)
RADIUS+ (RFC 2618)
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)

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 Multicasting related MIBs
IPV6-MIB (RFC 2065)
IPV6-ICMP-MIB (RFC 2066)
IPV6-TCP-MIB (RFC 2052)
IPV6-UDP-MIB (RFC2054)
Link Aggregation MIB (IEEE 802.3ad)
MAU MIB (RFC 3636)
MIB II (RFC 1213)
P-Bridge MIB (RFC 2674P)
Port Access Entity MIB (IEEE 802.1X)
Port Access Entity Equipment MIB
Power Ethernet MIB (RFC 3621)
Private MIB
Q-Bridge MIB (RFC 2674Q)
Quality of Service MIB
RADIUS Authentication Client MIB (RFC 2621)
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)

B TROUBLESHOOTING

PROBLEMS ACCESSING THE MANAGEMENT INTERFACE

Table 146: 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:

```
ES-3026(config)#logging on
ES-3026(config)#logging history flash 7
ES-3026(config)#snmp-server host 192.168.1.23
⋮
```

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.

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 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)

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.

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.

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.

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.

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.

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 574
aaa accounting dot1x 575
aaa accounting exec 576
aaa accounting update 577
aaa authorization exec 577
aaa group server 578
absolute 525
access-list arp 673
access-list ip 662
access-list mac 668
accounting dot1x 579
accounting exec 580
alias 678
arp timeout 907
authentication enable 564
authentication login 565
authorization exec 580
auto-traffic-control 727
auto-traffic-control action 728
auto-traffic-control alarm-clear-threshold 729
auto-traffic-controlalarm-fire-threshold 730
auto-traffic-control apply-timer 726
auto-traffic-controlauto-control-release 731
auto-traffic-control control-release 731
auto-traffic-control release-timer 726

B

boot system 490
bridge-ext gvrp 766

C

calendar set 523
capabilities 679
channel-group 696
class 820
class-map 816
clear arp-cache 908
clear counters 686
clear dns cache 890
clear host 891
clear ip dhcp snooping database flash 645
clear ipv6 neighbors 930
clear ipv6 traffic 925
clear log 512
clear mac-address-table dynamic 739
clock timezone 522
cluster 528
cluster commander 528
cluster ip-pool 529
cluster member 530
configure 477
copy 491

D

databits 500
delete 494
delete public-key 593
description 817
description 680
dir 494
disable 478
disconnect 507
dot1q-tunnel system-tunnel-control 781
dot1x default 598
dot1x eapol-pass-through 599
dot1x identity profile 606
dot1x intrusion-action 600
dot1x max-req 600
dot1x max-start 606
dot1x operation-mode 601
dot1x pae supplicant 607
dot1x port-control 602
dot1x re-authenticate 605
dot1x re-authentication 602
dot1x system-auth-control 599
dot1x timeout auth-period 608
dot1x timeout held-period 608
dot1x timeout quiet-period 603
dot1x timeout re-authperiod 603
dot1x timeout start-period 609
dot1x timeout supp-timeout 604
dot1x timeout tx-period 604

E

enable 475
enable password 562
end 479
exec-timeout 501
exit 479

F

flowcontrol 681

G

garp timer 767

H

hostname 482

I

nterface 678
interface vlan 773
ip access-group 666
ip address 902
ip arp inspection 652
ip arp inspection filter 653
ip arp inspection limit 656
ip arp inspection log-buffer logs 654
ip arp inspection trust 657
ip arp inspection validate 655
ip arp inspection vlan 655
ip default-gateway 903
ip dhcp client class-id 896
ip dhcp restart client 896
ip dhcp snooping 639
ip dhcp snooping database flash 641
ip dhcp snooping information option 641
ip dhcp snooping information policy 642
ip dhcp snooping trust 644
ip dhcp snooping verify mac-address 643
ip dhcp snooping vlan 643
ip domain-list 885
ip domain-lookup 886
ip domain-name 887
ip host 888
ip http port 582
ip http secure-port 585
ip http secure-server 583
ip http server 583
ip igmp filter (Global Configuration) 853
ip igmp filter (Interface Configuration) 855
ip igmp max-groups 856
ip igmp max-groups action 857
ip igmp profile 854
ip igmp snooping 834
ip igmp snooping proxy-reporting 835
ip igmp snooping querier 836
ip igmp snooping router-alert-option-check 836
ip igmp snooping router-port-expire-time 837
ip igmp snooping tcn-flood 838
ip igmp snooping tcn-query-solicit 839
ip igmp snooping unregistered-data-flood 839
ip igmp snooping unsolicited-report-interval 840
ip igmp snooping version 841
ip igmp snooping version-exclusive 841
ip igmp snooping vlan general-query-suppression 842
ip igmp snooping vlan immediate-leave 843
ip igmp snooping vlan last-memb-query-count 844
ip igmp snooping vlan last-memb-query-intvl 844
ip igmp snooping vlan mrd 845
ip igmp snooping vlan mrouter 851
ip igmp snooping vlan proxy-address 846
ip igmp snooping vlan proxy-query-interval 847
ip igmp snooping vlan proxy-query-resp-intvl 848
ip igmp snooping vlan static 848
ip name-server 889
ip source-guard 648
ip source-guard binding 647
ip ssh authentication-retries 591
ip ssh crypto host-key generate 593
ip ssh crypto zeroize 594
ip ssh save host-key 595
ip ssh server 591
ip ssh server-key size 592
ip ssh timeout 592
ip telnet max-sessions 586
ip telnet port 586
ip telnet server 587
ipv6 address 911
ipv6 address autoconfig 912
ipv6 address eui-64 913
ipv6 address link-local 915
ipv6 default-gateway 910
ipv6 dhcp restart client vlan 897
ipv6 enable 916
ipv6 host 890
ipv6 mtu 917
ipv6 nd dad attempts 927
ipv6 nd ns-interval 928
ipv6 nd reachable-time 929

J

jumbo frame 488

L

lacp 697
lacp admin-key (Ethernet Interface) 698
lacp admin-key (Port Channel) 700
lacp port-priority 699
lacp system-priority 700
line 499
lldp 868
lldp admin-status 871
lldp basic-tlv management-ip-address 872
lldp basic-tlv port-description 873
lldp basic-tlv system-capabilities 873
lldp basic-tlv system-description 874
lldp basic-tlv system-name 874
lldp dot1-tlv proto-ident 875
lldp dot1-tlv proto-vid 875
lldp dot1-tlv pvid 876
lldp dot1-tlv vlan-name 876
lldp dot3-tlv link-agg 877
lldp dot3-tlv mac-phy 877
lldp dot3-tlv max-frame 878
lldp holdtime-multiplier 868
lldp notification 878
lldp notification-interval 869
lldp refresh-interval 870
lldp reinit-delay 870
lldp tx-delay 871
logging facility 509
logging history 510
logging host 511
logging on 511
logging sendmail 516
logging sendmail destination-email 517
logging sendmail host 516
logging sendmail level 517
logging sendmail source-email 518
logging trap 512
login 501

M

mac access-group 671
mac-address-table aging-time 737
mac-address-table static 738
mac-authentication intrusion-action 629
mac-authentication max-mac-count 629
mac-authentication reauth-time 621
mac-learning 616
mac-vlan 792
management 612
match 818
max-hops 748
media-type 682
mst priority 749
mst vlan 750
mvr 860
mvr immediate-leave 861
mvr type 862
mvr vlan group 863

N

name 750
negotiation 682
network-access aging 620
network-access dynamic-qos 622
network-access dynamic-vlan 623
network-access guest-vlan 623
network-access link-detection 624
network-access link-detection link-down 625
network-access link-detection link-up 625
network-access link-detection link-up-down 626
network-access mac-filter 620
network-access max-mac-count 626
network-access mode mac-authentication 627
network-access port-mac-filter 628
nlm 548
no rspan session 718

P

parity 502
password 503
password-thresh 504
periodic 525
permit, deny 854
permit, deny (ARP ACL) 674
permit, deny (Extended IPv4 ACL) 664
permit, deny (MAC ACL) 669
permit, deny (Standard IP ACL) 663
ping 905
ping6 926
police flow 821
police srtcm-color 823
police trtcm-color 825
policy-map 819
port monitor 711
port security 617
power inline 706
power inline compatible 705
power inline maximum allocation 707
power inline priority 708
power-save 692
prompt 473
protocol-vlan protocol-group (Configuring Groups) 787

protocol-vlan protocol-group (Configuring Interfaces) 787

Q

qos map cos-dscp 806
qos map dscp-mutation 808
qos map phb-queue 809
qos map trust-mode 810
queue mode 802
queue weight 803
quit 476

R

radius-server acct-port 566
radius-server auth-port 567
radius-server host 567
radius-server key 568
radius-server retransmit 569
radius-server timeout 569
range 855
rate-limit 721
rcommand 530
reload (Global Configuration) 474
reload (Privileged Exec) 478
rename 819
revision 751
rmon alarm 554
rmon collection history 556
rmon collection stats 557
rmon event 555
rspan destination 716
rspan remote vlan 717
rspan source 715

S

server 579
service-policy 830
set cos 827
set ip dscp 828
set phb 829
show access-group 676
show access-list 676
show access-list tcam-utilization 482
show accounting 581
show arp 908
show arp access-list 675
show auto-traffic-control 736
show auto-traffic-control interface 736
show bridge-ext 769
show cable-diagnostics 692
show calendar 523
show class-map 831
show cluster 531
show cluster candidates 532
show cluster members 531
show dns 891
show dns cache 892
show dot1q-tunnel 783
show dot1x 609
show garp timer 769
show gvrp configuration 770
show history 476
show hosts 892
show interfaces brief 686
show interfaces counters 687
show interfaces protocol-vlan protocol-group 789
show interfaces status 688
show interfaces switchport 689
show ip access-group 667
show ip access-list 667
show ip arp inspection configuration 658
show ip arp inspection interface 658
show ip arp inspection log 659
show ip arp inspection statistics 659
show ip arp inspection vlan 659
show ip default-gateway 904
show ip dhcp snooping 646
show ip dhcp snooping binding 646
show ip igmp filter 857
show ip igmp profile 858
show ip igmp snooping 849
show ip igmp snooping group 850
show ip igmp snooping mrouter 852
show ip igmp throttle interface 858
show ip interface 904
show ip source-guard 650
show ip source-guard binding 650
show ip ssh 595
show ip telnet 587
show ipv6 default-gateway 918
show ipv6 dhcp duid 898
show ipv6 dhcp vlan 899
show ipv6 interface 919
show ipv6 mtu 920
show ipv6 neighbors 930
show ipv6 traffic 921
show lacp 701
show line 508
show lldp config 879
show lldp info local-device 880
show lldp info remote-device 881
show lldp info statistics 882
show log 513
show logging 514
show logging sendmail 518
show mac access-group 672
show mac access-list 672
show mac-address-table 739
show mac-address-table aging-time 740
show mac-vlan 793
show management 613

show memory 483
show mvr 864
show network-access 630
show network-access mac-address-table 631
show network-access mac-filter 632
show nlm oper-status 550
show policy-map 831
show policy-map interface 832
show port monitor 713
show power inline status 709
show power mainpower 710
show power-save 693
show process cpu 483
show protocol-vlan protocol-group 788
show public-key 596
show qos map cos-dscp 812
show qos map dscp-mutation 811
show qos map phb-queue 811
show qos map trust-mode 813
show queue mode 805
show queue weight 805
show radius-server 570
show reload 479
show rmon alarm 558
show rmon event 558
show rmon history 558
show rmon statistics 559
show rspan 719
show running-config 484
show snmp 536
show snmp engine-id 545
show snmp group 546
show snmp notify-filter 551
show snmp user 547
show snmp view 548
show sntp 521
show spanning-tree 763
show spanning-tree mst configuration 764
show ssh 597
show startup-config 485
show subnet-vlan 791
show system 486
show tacacs-server 573
show time-range 526
show traffic-segmentation 785
show users 486
show version 487
show vlan 779
show voice vlan 799
show web-auth 637
show web-auth interface 637
show web-auth summary 638
shutdown 683
silent-time 505
snmp-server 534
snmp-server community 535
snmp-server contact 535
snmp-server enable port-traps atc broadcast-alarm-clear 732
snmp-server enable port-traps atc broadcast-alarm-fire 732
snmp-server enable port-traps atc broadcast-control-apply 733
snmp-server enable port-traps atc broadcast-control-release 733
snmp-server enable port-traps atc multicast-alarm-clear 734
snmp-server enable port-traps atc multicast-alarm-fire 734
snmp-server enable port-traps atc multicast-control-apply 735
snmp-server enable port-traps atc multicast-control-release 735
snmp-server enable traps 537
snmp-server engine-id 541
snmp-server group 542
snmp-server host 538
snmp-server location 536
snmp-server notify-filter 549
snmp-server user 543
snmp-server view 544
sntp client 519
sntp poll 520
sntp server 521
spanning-tree 742
spanning-tree bpdu-filter 752
spanning-tree bpdu-guard 752
spanning-tree cost 753
spanning-tree edge-port 754
spanning-tree forward-time 743
spanning-tree hello-time 743
spanning-tree link-type 755
spanning-tree loopback-detection 756
spanning-tree loopback-detection release 761
spanning-tree loopback-detection release-mode 756
spanning-tree loopback-detection trap 757
spanning-tree max-age 744
spanning-tree mode 745
spanning-tree mst configuration 747
spanning-tree mst cost 758
spanning-tree mst port-priority 759
spanning-tree pathcost method 746
spanning-tree port-priority 759
spanning-tree priority 747
spanning-tree protocol-migration 762
spanning-tree root-guard 760
spanning-tree spanning-disabled 761
spanning-tree transmission-limit 748
speed 505
speed-duplex 684
stopbits 506
subnet-vlan 790

switchport acceptable-frame-types 774
switchport allowed vlan 774
switchport dot1q-tunnel mode 782
switchport dot1q-tunnel tpid 783
switchport forbidden vlan 768
switchport gvrp 768
switchport ingress-filtering 775
switchport mode 776
switchport native vlan 777
switchport packet-rate 685
switchport priority default 804
switchport voice vlan 796
switchport voice vlan priority 797
switchport voice vlan rule 797
switchport voice vlan security 798

T

tacacs-server 571
tacacs-server host 571
tacacs-server key 572
tacacs-server port 572
test cable-diagnostics 691
timeout login response 506
time-range 524
traceroute 904
traffic-segmentation 784

U

upgrade opcode auto 496
upgrade opcode path 497
username 563

V

vlan 771
vlan database 771
vlan-trunking 778
voice vlan 794
voice vlan aging 795
voice vlan mac-address 795

W

web-auth 635
web-auth login-attempts 633
web-auth quiet-period 634
web-auth re-authenticate (IP) 636
web-auth re-authenticate (Port) 636
web-auth session-timeout 634
web-auth system-auth-control 635
whichboot 495

INDEX

NUMERICS

802.1Q tunnel 160, 780
- access 165, 782
- configuration, guidelines 163
- configuration, limitations 163
- description 160
- ethernet type 164, 783
- interface configuration 165, 782–783
- mode selection 165, 782
- status, configuring 164, 781
- TPID 164, 783
- uplink 165, 782

802.1X
- authenticator, configuring 317
- global settings 315
- port authentication 314, 597, 599
- port authentication accounting 255, 256, 579
- supplicant, configuring 321

A

AAA
- accounting 802.1X port settings 255, 256, 579
- accounting exec command privileges 256
- accounting exec settings 255, 580
- accounting summary 256, 581
- accounting update 255, 577
- accounting, configuring 255, 573
- authorization & accounting 248, 573
- authorization exec settings 260, 577
- authorization method 260
- authorization settings 260, 577
- authorization summary 581
- RADIUS group settings 256, 578
- TACACS+ group settings 256, 578

acceptable frame type 153, 774

Access Control List *See* ACL

ACL 288, 661
- ARP 293, 299, 673
- binding to a port 301, 666
- IPv4 Extended 292, 295, 661, 664
- IPv4 Standard 292, 294, 661, 663
- MAC 292, 297, 668
- time range 289, 524

Address Resolution Protocol *See* ARP

address table 177, 737
- aging time 180, 737
- aging time, displaying 180, 740
- aging time, setting 180, 737

administrative users, displaying 486

ARP ACL 299, 653

ARP configuration 906

ARP description 400

ARP inspection 302, 651
- ACL filter 305, 653
- additional validation criteria 304, 655
- ARP ACL 306, 673
- enabling globally 304, 652
- enabling per VLAN 306, 655
- trusted ports 307, 657

ATC 723
- functional limitations 725
- limiting traffic rates 724
- shutting down a port 725
- usage 724

authentication
- MAC address authentication 267, 619, 627
- MAC, configuring ports 270, 619
- network access 267, 619, 627
- public key 282, 590
- web 264, 635
- web authentication for ports, configuring 266, 635
- web authentication port information, displaying 266, 637
- web authentication, re-authenticating address 636
- web authentication, re-authenticating ports 266, 636
- web, configuring 265, 635

Automatic Traffic Control *See* ATC

B

BOOTP 403, 902

BPDU 185
- filter 198, 752
- ignoring superior BPDUs 197, 760
- selecting protocol based on message format 198, 762
- shut down port on receipt 198, 752

bridge extension capabilities, displaying 90, 769

broadcast storm, threshold 209, 685

C

cable diagnostics 127, 691

canonical format indicator 222

class map
- description 817

DiffServ 816
Class of Service *See* CoS
CLI
command modes 466
showing commands 464
clustering switches, management access 393, 528
command line interface *See* CLI
committed burst size, QoS policy 233, 234, 235, 821, 823, 825
committed information rate, QoS policy 233, 234, 235, 821, 823, 825
community string 65, 372, 535
configuration files, restoring defaults 92, 489
configuration settings
restoring 67, 94, 95, 489, 491
saving 67, 94, 489, 491
console port, required connections 56
CoS 211, 810
configuring 211, 801
default mapping to internal values 222, 807
enabling 218, 810
layer 3/4 priorities 218, 806
priorities, mapping to internal values 222, 806
queue mapping 215, 809
queue mode 212, 802
queue weights, assigning 214, 803
CoS/CFI to PHB/drop precedence 222, 806
CPU
status 107, 483
utilization, showing 107, 483

D

default IPv4 gateway, configuration 403, 903
default IPv6 gateway, configuration 405, 910
default priority, ingress port 211, 804
default settings, system 52
DHCP 403, 902
class identifier 896
client 403, 895, 902
dynamic configuration 62
DHCP snooping 330, 638
enabling 333, 639
global configuration 333, 639
information option 333, 641
information option policy 333, 642
information option, enabling 333, 641
policy selection 333, 642
specifying trusted interfaces 335, 644
verifying MAC addresses 333, 643
VLAN configuration 334, 643
Differentiated Code Point Service *See* DSCP
Differentiated Services *See* DiffServ
DiffServ 225, 815
binding policy to interface 239, 830
class map 226, 816, 820
class map, description 817
classifying QoS traffic 226, 818
color aware, srTCM 234, 823
color aware, trTCM 235, 825
color blind, srTCM 234, 823
color blind, trTCM 235, 825
committed burst size 234, 236, 821, 823, 825
committed information rate 234, 235, 821, 823, 825
configuring 815
conforming traffic, configuring response 821, 823, 825
description 817
excess burst size 235, 823
metering, configuring 229, 230, 231, 821
peak burst size 236, 825
peak information rate 236, 825
policy map 229, 819
policy map, description 226, 817
QoS policy 229, 819
service policy 239, 830
setting CoS for matching packets 233, 827
setting PHB for matching packets 233, 829
single-rate, three-color meter 230, 234, 823
srTCM metering 230, 234, 823
traffic between CIR and BE, configuring response 234, 823
traffic between CIR and PIR, configuring response 235, 825
trTCM metering 235, 825
two-rate, three-color meter 231, 825
violating traffic, configuring response 236, 821, 823, 825
DNS
default domain name 423, 887
displaying the cache 429, 892
domain name list 423, 888, 890
enabling lookup 423, 886
name server list 423, 889
static entries, IPv4 427, 888
static entries, IPv6 890
Domain Name Service *See* DNS
downloading software 92, 491
automatically 96, 496
using FTP or TFTP 96
drop precedence
CoS priority mapping 222, 806
DSCP ingress map 220, 808
DSA encryption 284, 286, 593
DSCP 218, 810
enabling 218, 810
mapping to internal values 219, 808
DSCP ingress map
drop precedence 220, 808
DSCP to PHB/drop precedence 220, 808
dynamic addresses, clearing 182
dynamic addresses, displaying 181, 739
Dynamic Host Configuration Protocol *See* DHCP
dynamic QoS assignment 268, 271, 622
dynamic VLAN assignment 267, 271, 623

E

edge port, STA 197, 200, 754
encryption
  DSA 284, 286, 593
  RSA 284, 286, 593
engine ID 363, 364, 541
event logging 339, 508
excess burst size, QoS policy 234, 825
exec command privileges, accounting 256, 576
exec settings
  accounting 255, 580
  authorization 260, 577

F

firmware
  displaying version 88, 487
  upgrading 92, 491
  upgrading automatically 96, 496
  upgrading with FTP or TFP 96
  version, displaying 88, 487

G

GARP VLAN Registration Protocol *See* GVRP
gateway, IPv4 default 403, 903
gateway, IPv6 default 405, 910
general security measures 247, 615
GVRP
  enabling 157, 766
  global setting 157, 766
  interface configuration 157, 768

H

hardware version, displaying 88, 487
HTTP, web server 583
HTTPS 277, 278, 583
  configuring 277, 583, 585
  replacing SSL certificate 278, 491
  secure-site certificate 278, 491
HTTPS, secure server 277, 583

I

IEEE 802.1D 185, 745
IEEE 802.1s 185, 745
IEEE 802.1w 185, 745
IEEE 802.1X 314, 597, 599
IGMP
  filter profiles, configuration 448, 451, 854
  filter, parameters 448, 451
  filtering & throttling 447, 852
  filtering & throttling, configuring profile 854, 855
  filtering & throttling, creating profile 448, 449, 854
  filtering & throttling, enabling 448, 853
  filtering & throttling, interface configuration 451, 855
  filtering & throttling, interface settings 855–857
  filtering & throttling, status 447, 853
  groups, displaying 440, 850
  Layer 2 432, 833
  query 432, 434, 836
  snooping 432, 834
  snooping & query, parameters 433
  snooping, configuring 433, 833
  snooping, immediate leave 443, 843
IGMP services, displaying 446
IGMP snooping
  configuring 441, 833
  enabling per interface 441, 442, 834
  forwarding entries 446
  immediate leave, status 443, 843
  interface attached to multicast router 438, 851, 852
  last leave 433
  last member query interval 444, 844
  proxy query address 444, 846
  proxy query interval 444, 847
  proxy query response interval 444, 848
  proxy reporting 443, 835
  querier timeout 436, 837
  query suppression 433
  router port expire time 436
  static host interface 433, 848
  static multicast routing 437, 851
  static port assignment 439, 848
  static router interface 433, 851
  static router port, configuring 437, 851
  TCN flood 434, 838
  unregistered data flooding 435, 839
  versioin for interface, setting 444, 841
  version exclusive 436, 841
  version, setting 436, 841
  with proxy reporting 433, 835
immediate leave, IGMP snooping 443, 843
importing user public keys 286, 491
ingress filtering 153, 775
IP address, BOOTP/DHCP 403, 896
IP address, setting 399, 901
IP filter, for management access 310, 612
IP source guard
  configuring static entries 327, 647
  setting filter criteria 326, 648
IPv4 address
  BOOTP/DHCP 403, 902
  dynamic configuration 62
  manual configuration 59
  setting 59, 402, 902
IPv6
  displaying neighbors 413
  duplicate address detection 413, 927
  enabling 407, 916
  MTU 407, 917
IPv6 address
  dynamic configuration (global unicast) 63, 912
  dynamic configuration (link-local) 63

EUI format 410, 914
EUI-64 setting 410, 913, 914
explicit configuration 407, 916
global unicast 410, 911
link-local 411, 912
manual configuration (global unicast) 60, 410, 911
manual configuration (link-local) 60, 411, 915
setting 59, 405, 911

J

jumbo frame 89, 488

K

key
private 280, 588
public 280, 588
user public, importing 286, 491
key pair
host 280, 588
host, generating 284, 593

L

LACP
configuration 695
group attributes, configuring 135, 700
group members, configuring 133
local parameters 137, 701
partner parameters 138, 701
protocol message statistics 135, 701
protocol parameters 695
last member query interval, IGMP snooping 444, 844
Link Layer Discovery Protocol *See* LLDP
link type, STA 196, 200, 755
LLDP 344, 867
device statistics details, displaying 356, 882
device statistics, displaying 354, 882
display device information 350, 352, 881
displaying remote information 352, 881
interface attributes, configuring 347
local device information, displaying 350, 880
message attributes 347, 867
message statistics 354, 882
remote information, displaying 354, 881
remote port information, displaying 352, 881
timing attributes, configuring 345, 868–871
TLV 344, 347
TLV, management address 347, 872
TLV, port description 348, 873
TLV, system capabilities 348, 873
TLV, system description 348, 874
TLV, system name 348, 874
local engine ID 541
logging
messages, displaying 341, 513
syslog traps 342, 512
to syslog servers 342, 511
log-in, web interface 72
logon authentication 263, 561
encryption keys 252, 568, 572
RADIUS client 251, 566
RADIUS server 251, 566
sequence 249, 564, 565
settings 250, 565
TACACS+ client 250, 570
TACACS+ server 250, 570
logon authentication, settings 252
loopback detection, STA 187, 756

M

MAC address authentication 267, 619
ports, configuring 270, 619, 627
reauthentication 270, 621
MAC address, mirroring 183, 711
main menu, web interface 74
management access, filtering per address 310, 612
management access, IP filter 310, 612
Management Information Bases (MIBs) 937
matching class settings, classifying QoS traffic 226, 818
media-type 114, 682
memory
status 108
utilization, showing 108
mirror port
configuring 117, 711
configuring local traffic 117, 711
configuring remote traffic 119, 713
MSTP 201, 745
global settings, configuring 189, 201, 741
global settings, displaying 194, 763
interface settings, configuring 195, 204, 741
interface settings, displaying 206, 763
path cost 205, 758
MTU for IPv6 407, 917
multicast filtering 431, 833
enabling IGMP snooping 442, 834
enabling IGMP snooping per interface 441, 834
router configuration 437, 851
multicast groups 440, 446, 850
displaying 440, 446
static 439, 440, 848, 850
multicast router discovery 441, 845
multicast router port, displaying 438, 852
multicast services
configuring 439, 848
displaying 440, 850
multicast static router port 437, 851
configuring 437, 851
multicast storm, threshold 209, 685
Multicast VLAN Registration *See* MVR
multicast, filtering and throttling 447, 853

MVR
assigning static multicast groups 457, 863
configuring 454, 859
description 452
interface status, configuring 455, 861, 862
interface status, displaying 457, 864
setting interface type 456, 862
setting multicast groups 454, 860
specifying a VLAN 454, 860
static binding 457, 863
using immediate leave 456, 861

N

network access
authentication 267, 619
dynamic QoS assignment 271, 622
dynamic VLAN assignment 271, 623
port configuration 270, 627
reauthentication 270, 621
secure MAC information 275, 631, 632

P

password, line 503
passwords 58, 561
administrator setting 263, 563
path cost 200
method 191, 746
STA 200, 746
peak burst size, QoS policy 235, 825
peak information rate, QoS policy 235, 825
per-hop behavior, DSCP ingress map 220, 808
policing traffic, QoS policy 229, 233
policy map
description 817
DiffServ 229, 819
port authentication 314, 597, 599
port power
displaying status 360, 709
inline 358, 706
inline status 360, 709
maximum allocation 358, 707
priority 359, 708
showing main power 360, 710
port priority
configuring 211, 801
default ingress 211, 804
STA 195, 759
port security, configuring 312, 616
port, statistics 123, 687
ports
autonegotiation 114, 682
broadcast storm threshold 209, 685
capabilities 114, 679
configuring 113, 677
duplex mode 114, 684
flow control 114, 681
forced selection on combo ports 114, 682
mirroring 117, 711
mirroring local traffic 117, 711
mirroring remote traffic 119, 713
multicast storm threshold 209, 685
speed 114, 684
statistics 687
unknown unicast storm threshold 209, 685
power budgets
port 358, 707
port priority 359, 708
power savings
configuring 140
power savings, configuring 692
power savings, enabling per port 140, 692
priority, default port ingress 211, 804
private key 280, 588
problems, troubleshooting 939
protocol migration 198, 762
protocol VLANs 166, 786
configuring 167, 787
interface configuration 168, 787
system configuration 167, 787
proxy query address, IGMP snooping 444, 846
proxy query interval, IGMP snooping 444, 847
proxy query response interval, IGMP snooping 444, 848
proxy reporting, IGMP snooping 443, 835
public key 280, 588
PVID, port native VLAN 153, 777

Q

QinQ Tunneling *See* 802.1Q tunnel
QoS 225, 815
configuration guidelines 816
configuring 225, 815
CoS/CFI to PHB/drop precedence 222, 806
DSCP to PHB/drop precedence 219, 808
dynamic assignment 271, 622
matching class settings 226, 818
PHB to queue 215, 809
selecting DSCP, CoS 218, 810
QoS policy
committed burst size 233, 234, 235, 821, 823, 825
excess burst size 234, 823
peak burst size 235, 825
policing flow 229, 233
srTCM 230, 823
srTCM police meter 234, 823
trTCM 231, 825
trTCM police meter 235
QoS policy, committed information rate 233, 234, 235, 821, 823, 825
QoS policy, peak information rate 235, 825
Quality of Service *See* QoS
queue weight, assigning to CoS 214, 803

R

RADIUS
logon authentication 251, 566
settings 251, 566
rate limit
port 207, 721
setting 207, 721
remote engine ID 541
remote logging 342, 512
Remote Monitoriing *See* RMON
rename, DiffServ 819
restarting the system 109, 474, 478, 479
at scheduled times 109, 474
RMON 383, 553
alarm, displaying settings 385, 558
alarm, setting thresholds 383, 554
commands 553
event settings, displaying 387, 558
response to alarm setting 386, 555
statistics history, collection 388, 556
statistics history, displaying 389, 558
statistics, collection 391, 557
statistics, displaying 392, 559
RSA encryption 284, 286, 593
RSTP 185, 745
global settings, configuring 189, 745
global settings, displaying 194, 763
interface settings, configuring 195
interface settings, displaying 199, 763
running configuration files, displaying 484

S

secure shell 280, 588
configuration 280, 588
security, general measures 247, 615
serial port, configuring 104, 499
Simple Mail Transfer Protocol *See* SMTP
Simple Network Management Protocol *See* SNMP
single rate three color meter *See* srTCM
SMTP
event handling 343, 515
sending log events 343, 515
SNMP 360, 533
community string 372, 535
enabling traps 378, 537
filtering IP addresses 310, 612
global settings, configuring 362
trap manager 378, 538
users, configuring 373, 375
SNMPv3 541–543
engine ID 363, 364, 541
engine identifier, local 363, 541
engine identifier, remote 364, 541
groups 368, 542
local users, configuring 373, 543
remote users, configuring 375, 543
user configuration 373, 375, 543
views 365, 544
SNTP
setting the system clock 101, 519–521
specifying servers 102, 521
software
displaying version 88, 487
downloading 92, 491
version, displaying 88, 487
Spanning Tree Protocol *See* STA
specifications, software 935
srTCM
police meter 234, 823
QoS policy 230, 823
SSH 280, 588
authentication retries 283, 591
configuring 280, 588
downloading public keys for clients 286, 491
generating host key pair 284, 593
server, configuring 283, 591
timeout 283, 592
SSL, replacing certificate 278
STA 185, 741
BPDU filter 198, 752
BPDU shutdown 198, 752
detecting loopbacks 187, 756
edge port 197, 200, 754
global settings, configuring 189
global settings, displaying 194, 763
interface settings, configuring 195
interface settings, displaying 199, 763
link type 196, 200, 755
loopback detection 187, 756
MSTP interface settings, configuring 204
MSTP path cost 205, 758
path cost 200, 746
path cost method 191, 746
port priority 195, 759
port/trunk loopback detection 187, 756
protocol migration 198, 762
transmission limit 191, 748
standards, IEEE 937
startup files
creating 92, 491
displaying 92, 485, 495
setting 92, 490
static addresses, setting 178, 738
statistics, port 123, 687
STP 189, 745
Also see STA
summary, accounting 256, 581
switch clustering, for management 393, 527
switch settings
restoring 94, 489
saving 94, 489
system clock
setting 100, 519
setting manually 100, 523
setting the time zone 103, 522
setting with SNTP 101, 519–521

system logs 339, 511
system software, downloading from server 92, 491

T

TACACS+
  logon authentication 250, 570
  settings 252, 570
TCN
  flood 434, 838
  general query solitication 435, 839
Telnet
  configuring 106, 585
  server, enabling 106, 587
time range, ACL 289, 524
time zone, setting 103, 522
time, setting 100, 519
TPID 164, 783
traffic segmentation 142, 784
  assigning ports 142, 784
  enabling 142, 784
  sessions, assigning ports 143, 784
  sessions, creating 143, 784
trap manager 65, 378, 538
troubleshooting 939
trTCM
  police meter 235, 825
  QoS policy 231, 825
trunk
  configuration 128, 695
  LACP 132, 695, 697
  static 129, 696
tunneling unknown VLANs, VLAN trunking 144, 778
two rate three color meter *See* trTCM
Type Length Value
  See LLDP TLV

U

unknown unicast storm, threshold 209, 685
unregistered data flooding, IGMP snooping 435, 839
upgrading software 92, 491, 496
user account 561, 563
user password 263, 562, 563

V

VLAN trunking 144, 778
VLANs 147–174, 765–799
  802.1Q tunnel mode 165, 782
  acceptable frame type 153, 774
  adding static members 152, 774
  basic information, displaying 769
  creating 150, 771
  description 147
  displaying port members 779
  displaying port members by interface 156
  displaying port members by interface range 156
  displaying port members by VLAN index 155
  dynamic assignment 271, 623
  egress mode 153, 776
  ingress filtering 153, 775
  interface configuration 152, 774–778
  IP subnet-based 171, 790
  MAC-based 173, 792
  mirroring 174, 711
  port members, displaying 779
  protocol 166, 786
  protocol, configuring 167, 787
  protocol, configuring groups 167, 787
  protocol, interface configuration 168, 787
  protocol, system configuration 167, 787
  PVID 153, 777
  tunneling unknown groups 144, 778
  voice 241, 793
voice VLANs 241, 793
  detecting VoIP devices 241, 794
  enabling for ports 244, 796–797
  identifying client devices 242, 795
VoIP traffic 241, 793
  ports, configuring 244, 796–797
  telephony OUI, configuring 242, 795
  voice VLAN, configuring 241, 793
VoIP, detecting devices 245, 797

W

web authentication 264, 635
  address, re-authenticating 636
  configuring 265, 635
  port information, displaying 266, 637
  ports, configuring 266, 635
  ports, re-authenticating 266, 636
web interface
  access requirements 71
  configuration buttons 73
  home page 72
  menu list 74
  panel display 73

LG-NORTEL

CE

JAN/2010/ISSUE 1.0