NETGEAR®

M4200 and M4300 Series ProSAFE Managed Switches

Software Administration Manual

Software Version 12.0.2

July 2016
202-11586-03

350 East Plumeria Drive
San Jose, CA 95134
USA

Support

Thank you for purchasing this NETGEAR product. You can visit *www.netgear.com/support* to register your product, get help, access the latest downloads and user manuals, and join our community. We recommend that you use only official NETGEAR support resources.

Conformity

For the current EU Declaration of Conformity, visit *http://kb.netgear.com/app/answers/detail/a_id/11621*.

Compliance

For regulatory compliance information, visit *http://www.netgear.com/about/regulatory*.

See the regulatory compliance document before connecting the power supply.

Trademarks

© NETGEAR, Inc., NETGEAR and the NETGEAR Logo are trademarks of NETGEAR, Inc. Any non-NETGEAR trademarks are used for reference purposes only.

Revision History

Publication Part Number	Publication Date	Comments
202-11586-03	July 2016	Added or changed the following sections: • *Add ACL Remarks* • *Change the Sequence of an ACL Rule* • *Command Authorization* • *Privileged Exec Command Mode Authorization* • *Error Disablement and Automatic Error Recovery* • *Loop Protection* • *Nondisruptive Configuration Management* • *DHCP L3 Relay* Made minor changes to other sections.
202-11586-02	May 2016	Updated *Compatible Switch Models*.
202-11586-01	December 2015	Initial publication.

Table of Contents

Chapter 1 Documentation Resources

Chapter 2 VLANs

VLAN Concepts 19
Create Two VLANs. 20
CLI: Create Two VLANs 20
Web Interface: Create Two VLANs 20
Assign Ports to VLAN 2 21
CLI: Assign Ports to VLAN 2 21
Web Interface: Assign Ports to VLAN 2 22
Create Three VLANs 23
CLI: Create Three VLANs 23
Web Interface: Create Three VLANs 23
Assign Ports to VLAN 3 25
CLI: Assign Ports to VLAN 3 25
Web Interface: Assign Ports to VLAN 3 25
Assign VLAN 3 as the Default VLAN for Port 1/0/2 26
CLI: Assign VLAN 3 as the Default VLAN for Port 1/0/2 26
Web Interface: Assign VLAN 3 as the Default VLAN for Port 1/0/2 27
Create a MAC-Based VLAN 27
CLI: Create a MAC-Based VLAN 28
Web Interface: Assign a MAC-Based VLAN 29
Create a Protocol-Based VLAN 31
CLI: Create a Protocol-Based VLAN 31
Web Interface: Create a Protocol-Based VLAN 32
Virtual VLANs: Create an IP Subnet–Based VLAN 35
CLI: Create an IP Subnet–Based VLAN 36
Web Interface: Create an IP Subnet–Based VLAN 37
Voice VLANs 38
CLI: Configure Voice VLAN and Prioritize Voice Traffic 39
Web Interface: Configure Voice VLAN and Prioritize Voice Traffic 41
Configure GARP VLAN Registration Protocol 46
CLI: Enable GVRP 47
Web Interface: Configure GVRP on switch A 49
Web Interface: Configure GVRP on Switch B 51
Private VLANs 52
Assign Private-VLAN Types (Primary, Isolated, Community) 54
CLI: Assign Private-VLAN Type (Primary, Isolated, Community) 54
Web Interface: Assign Private-VLAN Type (Primary, Isolated, Community) 54

Configure Private-VLAN Association 56
CLI: Configure Private-VLAN Association 56
Web Interface: Configure Private-VLAN Association 56
Configure Private-VLAN Port Mode (Promiscuous, Host) 57
CLI: Configure Private-VLAN Port Mode (Promiscuous, Host) 57
Web Interface: Configure Private-VLAN Port Mode (Promiscuous, Host) 57
Configure Private-VLAN Host Ports 58
CLI: Configure Private-VLAN Host Ports 58
Web Interface: Assign Private-VLAN Port Host Ports 59
Map Private-VLAN Promiscuous Port 60
CLI: Map Private-VLAN Promiscuous Port 60
Web Interface: Map Private-VLAN Promiscuous Port 60
VLAN Access Ports and Trunk Ports 61
CLI: Configure a VLAN Trunk 62
Web Interface: Configure a VLAN Trunk 63

Chapter 3 LAGs

Link Aggregation Concepts 68
Add Ports to LAGs 69
CLI: Add Ports to the LAGs 69
Web Interface: Add Ports to LAGs 69

Chapter 4 Port Routing

Port Routing Concepts 72
Port Routing Configuration 72
Enable Routing for the Switch 73
CLI: Enable Routing for the Switch 73
Web Interface: Enable Routing for the Switch 74
Enable Routing for Ports on the Switch 74
CLI: Enable Routing for Ports on the Switch 75
Web Interface: Enable Routing for Ports on the Switch 75
Add a Default Route 77
CLI: Add a Default Route 77
Web Interface: Add a Default Route 78
Add a Static Route 78
CLI: Add a Static Route 79
Web Interface: Add a Static Route 79

Chapter 5 VLAN Routing

VLAN Routing Concepts 81
Create Two VLANs 81
CLI: Create Two VLANs 82
Web Interface: Create Two VLANs 83
Set Up VLAN Routing for the VLANs and the Switch 86
CLI: Set Up VLAN Routing for the VLANs and the Switch 86

Web Interface: Set Up VLAN Routing for the VLANs and the Switch 87

Chapter 6 RIP

Routing Information Protocol Concepts 89
Enable Routing for the Switch 90
CLI: Enable Routing for the Switch 90
Web Interface: Enable Routing for the Switch 90
Enable Routing for Ports 91
CLI: Enable Routing and Assigning IP Addresses for Ports 1/0/2 and 1/0/3 91
Web Interface: Enable Routing for the Ports 91
Enable RIP on the Switch 93
CLI: Enable RIP on the Switch 93
Web Interface: Enable RIP on the Switch 93
Enable RIP for Ports 1/0/2 and 1/0/3 94
CLI: Enable RIP for Ports 1/0/2 and 1/0/3 94
Web Interface: Enable RIP for Ports 1/0/2 and 1/0/3 94
Configure VLAN Routing with RIP Support 95
CLI: Configure VLAN Routing with RIP Support 95
Web Interface: Configure VLAN Routing with RIP Support 97

Chapter 7 OSPF

Open Shortest Path First Concepts 101
Inter-area Router 101
CLI: Configure an Inter-area Router 102
Web Interface: Configure an Inter-area Router 104
OSPF on a Border Router 108
CLI: Configure OSPF on a Border Router 108
Web Interface: Configure OSPF on a Border Router 109
Stub Areas 114
CLI: Configure Area 1 as a Stub Area on A1 114
Web Interface: Configure Area 1 as a Stub Area on A1 116
CLI: Configure Area 1 as a Stub Area on A2 120
Web Interface: Configure Area 1 as a Stub Area on A2 121
NSSA Areas 123
CLI: Configure Area 1 as an NSSA Area 123
Web Interface: Configure Area 1 as an NSSA Area on A1 125
CLI: Configure Area 1 as an NSSA Area on A2 128
Web Interface: Configure Area 1 as an NSSA Area on A2 130
VLAN Routing OSPF 134
CLI: Configure VLAN Routing OSPF 135
Web Interface: Configure VLAN Routing OSPF 137
OSPFv3 139
CLI: Configure OSPFv3 140
Web Interface: Configure OSPFv3 142

Chapter 8 PBR

Policy-Based Routing Concepts 146
Route-Map Statements 146
PBR Processing Logic 147
PBR Configurations 148
PBR Example 149

Chapter 9 ARP

Proxy ARP Concepts 153
Proxy ARP Examples 153
CLI: show ip interface 153
CLI: ip proxy-arp 153
Web Interface: Configure Proxy ARP on a Port 154

Chapter 10 VRRP

Virtual Router Redundancy Protocol Concepts 156
VRRP on a Master Router 157
CLI: Configure VRRP on a Master Router 157
Web Interface: Configure VRRP on a Master Router 158
VRRP on a Backup Router 159
CLI: Configure VRRP on a Backup Router 159
Web Interface: Configure VRRP on a Backup Router 160

Chapter 11 ACLs

Access Control List Concepts 163
MAC ACLs 163
IP ACLs 164
ACL Configuration 164
Set Up an IP ACL with Two Rules 164
CLI: Set Up an IP ACL with Two Rules 165
Web Interface: Set Up an IP ACL with Two Rules 166
One-Way Access Using a TCP Flag in an ACL 169
CLI: Configure One-Way Access Using a TCP Flag in an ACL 169
Web Interface: Configure One-Way Access Using a TCP Flag in an ACL 173
Use ACLs to Configure Isolated VLANs on a Layer 3 Switch 184
CLI: Configure One-Way Access Using a TCP Flag in ACL Commands 185
Web Interface: Configure One-Way Access Using a TCP Flag in an ACL 187
Set up a MAC ACL with Two Rules 195
CLI: Set up a MAC ACL with Two Rules 195
Web Interface: Set up a MAC ACL with Two Rules 196
Configure ACL Mirroring 198
CLI: Configure ACL Mirroring 199

Web Interface: Configure ACL Mirroring 201
Configure ACL Redirection 204
CLI: Redirect a Traffic Stream 205
Web Interface: Redirect a Traffic Stream 206
Add ACL Remarks 209
Change the Sequence of an ACL Rule 210
Configure a Management ACL 212
Example 1: Permit Any Host to Access the Switch Through Telnet or HTTP: 213
Example 2: Permit a Specific Host to Access the Switch Through SSH Only 213
Configure IPv6 ACLs 213
CLI: Configure an IPv6 ACL 215
Web Interface: Configure an IPv6 ACL 216

Chapter 12 CoS Queuing

CoS Queuing Concepts 223
CoS Queue Mapping 223
Trusted Ports 223
Untrusted Ports 224
CoS Queue Configuration 224
Show classofservice Trust 225
CLI: Show classofservice Trust 225
Web Interface: Show classofservice Trust 225
Set classofservice Trust Mode 225
CLI: Set classofservice Trust Mode 225
Web Interface: Set classofservice Trust Mode 226
Configure Cos-queue Min-bandwidth and Strict Priority Scheduler Mode . . 226
CLI: Configure Cos-queue Min-bandwidth and Strict Priority Scheduler Mode 226
Web Interface: Configure CoS-queue Min-bandwidth and Strict Priority Scheduler Mode 226
Set CoS Trust Mode for an Interface 228
CLI: Set CoS Trust Mode for an Interface 228
Web Interface: Set CoS Trust Mode for an Interface 228
Configure Traffic Shaping 229
CLI: Configure traffic-shape 229
Web Interface: Configure Traffic Shaping 229

Chapter 13 DiffServ

Differentiated Services Concepts 231
DiffServ 232
CLI: Configure DiffServ 232
Web Interface: Configure DiffServ 235
DiffServ for VoIP 248
CLI: Configure DiffServ for VoIP 248
Web Interface: Diffserv for VoIP 250

Auto VoIP 255
Protocol-Based Auto VoIP 255
OUI-Based Auto VoIP 256
Example 1: Enable Protocol-Based Auto VoIP 257
Example 2: Change the Queue of Protocol-Based Auto VoIP 258
Example 3: Create an Auto VoIP VLAN 259
DiffServ for IPv6 260
CLI: Configure DiffServ for IPv6 261
Web Interface: Configure DiffServ for IPv6 262
Color Conform Policy 268
CLI: Configure a Color Conform Policy 269
Web Interface: Configure a Color Conform Policy 270
WRED Explicit Congestion Notification 275

Chapter 14 IGMP Snooping and Querier

Internet Group Management Protocol Concepts 279
IGMP Snooping 279
CLI: EnaP Snooping 279
The following example shows how to enable IGble IGMMP snooping. 279
Web Interface: Enable IGMP Snooping 279
Show igmpsnooping 280
CLI: Show igmpsnooping 280
Web Interface: Show igmpsnooping 280
Show mac-address-table igmpsnooping 281
CLI for IGMPv1 and IGMPv2: Show mac-address-table igmpsnooping . . 281
CLI for IGMPv3: show igmpsnooping ssm entries 281
Web Interface: Show mac-address-table igmpsnooping 282
External Multicast Router 282
CLI: Configure the Switch with an External Multicast Router 282
Web Interface: Configure the Switch with an External Multicast Router . . 282
Multicast Router Using VLAN 283
CLI: Configure the Switch with a Multicast Router Using VLAN 283
Web Interface: Configure the Switch with a Multicast Router Using VLAN 283
IGMP Querier Concepts 284
Enable IGMP Querier 285
CLI: Enable IGMP Querier 285
Web Interface: Enable IGMP Querier 285
Show IGMP Querier Status 287
CLI: Show IGMP Querier Status 287
Web Interface: Show IGMP Querier Status 288

Chapter 15 MVR

Multicast VLAN Registration 290
Configure MVR in Compatible Mode 291
CLI: Configure MVR in Compatible Mode 292
Web Interface: Configure MVR in Compatible Mode 294

Configure MVR in Dynamic Mode 297
CLI: Configure MVR in Dynamic Mode 297
Web Interface: Configure MVR in Dynamic Mode 300

Chapter 16 Security Management

Port Security Concepts 305
Set the Dynamic and Static Limit on Port 1/0/1 306
CLI: Set the Dynamic and Static Limit on Port 1/0/1 306
Web Interface: Set the Dynamic and Static Limit on Port 1/0/1 306
Convert the Dynamic Address Learned from 1/0/1 to a Static Address 307
CLI: Convert the Dynamic Address Learned from 1/0/1 to the Static Address 307
Web Interface: Convert the Dynamic Address Learned from 1/0/1 to the Static Address 308
Create a Static Address 308
CLI: Create a Static Address 308
Web Interface: Create a Static Address 309
Protected Ports 309
CLI: Configure a Protected Port to Isolate Ports on the Switch 310
Web Interface: Configure a Protected Port to Isolate Ports on the Switch 312
802.1x Port Security 315
CLI: Authenticating dot1x Users by a RADIUS Server 316
Web Interface: Authenticating dot1x Users by a RADIUS Server 317
Create a Guest VLAN 321
CLI: Create a Guest VLAN 322
Web Interface: Create a Guest VLAN 323
Assign VLANs Using RADIUS 326
CLI: Assign VLANS Using RADIUS 327
Web Interface: Assign VLANS Using RADIUS 329
Dynamic ARP Inspection 332
CLI: Configure Dynamic ARP Inspection 333
Web Interface: Configure Dynamic ARP Inspection 334
Static Mapping 337
CLI: Configure Static Mapping 337
Web Interface: Configure Static Mapping 338
DHCP Snooping 339
CLI: Configure DHCP Snooping 340
Web Interface: Configure DHCP Snooping 341
Find a Rogue DHCP Server 343
CLI: Find a Rogue DHCP server 343
Web Interface: Find a Rogue DHCP server 344
Enter Static Binding into the Binding Database 346
CLI: Enter Static Binding into the Binding Database 346
Web Interface: Enter Static Binding into the Binding Database 346
Maximum Rate of DHCP Messages 347
CLI: Configure the Maximum Rate of DHCP Messages 347
Web Interface: Configure the Maximum Rate of DHCP Messages 347

IP Source Guard 348
CLI: Configure Dynamic ARP Inspection 349
Web Interface: Configure Dynamic ARP Inspection 350
Command Authorization 353
CLI Example 1: Configure Command Authorization by a TACACS+ Server 353
CLI Example 2: Configure Command Authorization by a RADIUS Server . 356
Privileged Exec Command Mode Authorization 359
CLI Example 1: Configure EXEC Authorization by a TACACS+ Server 359
CLI Example 2: Configure EXEC Authorization by a RADIUS Server 362
Accounting 364
CLI: Configure Telnet Command Accounting by a TACACS+ Server 364
Configure Telnet EXEC Accounting by RADIUS Server 365
Use the Authentication Manager to Set Up an Authentication Method List 366
Configure a Dot1x–MAB Authentication Method List with Dot1x–MAB Priority 367
Configure a Dot1x–MAB Authentication Method List with MAB–Dot1x Priority 368
Configure a Dot1x, MAB, and Captive Portal Authentication Method List with Default Priority 368
RADIUS Change of Authorization 370
IPv6 Stateless RA Guard 372

Chapter 17 MAB

MAC Authentication Bypass Concepts 375
Configure MAC Authentication Bypass on a Switch 377
Configure a Network Policy Server on a Microsoft Windows Server 2008 R2 or Later Server 381
Configure an Active Directory on a Microsoft Windows Server 2008 R2 or Later Server 389
Reduce the MAB Authentication Time 390
CLI: Reduce the Authentication Time for MAB 391
Web Interface: Reduce the Authentication Time for MAB 391

Chapter 18 SNTP

Simple Network Time Protocol Concepts 393
Show SNTP (CLI Only) 393
show sntp 393
show sntp client 393
show sntp server 394
Configure SNTP 394
CLI: Configure SNTP 394
Web Interface: Configure SNTP 396
Set the Time Zone (CLI Only) 397
Set the Named SNTP Server 397
CLI: Set the Named SNTP Server 397
Web Interface: Set the Named SNTP Server 398

Chapter 19 Tools

Traceroute . . . 401
CLI: Traceroute . . . 401
Web Interface: Traceroute . . . 402
Configuration Scripting . . . 402
script Command . . . 403
script list Command and script delete Command . . . 403
script apply running-config.scr Command . . . 404
Create a Configuration Script . . . 404
Upload a Configuration Script . . . 404
Pre-Login Banner . . . 405
Create a Pre-Login Banner . . . 405
Port Mirroring . . . 406
CLI: Specify the Source (Mirrored) Ports and Destination (Probe) . . . 406
Web Interface: Specify the Source (Mirrored) Ports and Destination (Probe) . . . 407
Remote SPAN . . . 407
CLI: Enable RSPAN on a Switch . . . 408
Dual Image . . . 410
CLI: Download a Backup Image and Make It Active . . . 411
Web Interface: Download a Backup Image and Make It Active . . . 412
Outbound Telnet . . . 413
CLI: show network . . . 414
CLI: show telnet . . . 414
CLI: transport output telnet . . . 415
Web Interface: Configure Telnet . . . 415
CLI: Configure the Session Limit and Session Time-out . . . 416
Web Interface: Configure the Session Time-out . . . 416
Error Disablement and Automatic Error Recovery . . . 417
Loop Protection . . . 419
Nondisruptive Configuration Management . . . 420
Full Memory Dump . . . 421

Chapter 20 Syslog

Syslog Concepts . . . 423
Show Logging . . . 423
CLI: Show Logging . . . 423
Web Interface: Show Logging . . . 424
Show Logging Buffered . . . 426
CLI: Show Logging Buffered . . . 426
Web Interface: Show Logging Buffered . . . 427
Show Logging Traplogs . . . 427
CLI: Show Logging Traplogs . . . 427
Web Interface: Show Logging Trap Logs . . . 428
Show Logging Hosts . . . 428
CLI: Show Logging Hosts . . . 428
Web Interface: Show Logging Hosts . . . 429

Configure Logging for a Port 429
CLI: Configure Logging for the Port 429
Web Interface: Configure Logging for the Port 430
Email Alerting 431
CLI: Send Log Messages to admin@switch.com Using Account aaaa@netgear.com 432

Chapter 21 Switch Stacks

Switch Stack Management and Connectivity 434
Stack Master and Stack Members 434
Stack Master 435
Stack Members 436
Stack Member Numbers 436
Stack Member Priority Values 436
Install and Power-up a Stack 436
Compatible Switch Models 436
Install a Switch Stack 437
Switch Firmware and Firmware Mismatch 438
Upgrade the Firmware 438
Migrate Configuration with a Firmware Upgrade 439
Web Interface: Copy Master Firmware to a Stack Member 439
Stack Switches Using a 10G Copper Port 440
CLI: Configure the 10G Copper Ports as Stack Ports 441
Web Interface: Configure the 10G Copper Ports as Stack Ports 443
Add, Remove, or Replace a Stack Member 444
Add Switches to an Operating Stack 444
Remove a Switch from a Stack 445
Replace a Stack Member 446
Switch Stack Configuration Files 447
Preconfigure a Switch 448
Renumber Stack Members 449
CLI: Renumber Stack Members 449
Web Interface: Renumber Stack Members 450
Move the Stack Master to a Different Unit 451
CLI: Move the Stack Master to a Different Unit 451
Web Interface: Move the Stack Master to a Different Unit 451

Chapter 22 SNMP

Add a New Community 453
CLI: Add a New Community 453
Web Interface: Add a New Community 453
Enable SNMP Trap 454
CLI: Enable SNMP Trap 454
Web Interface: Enable SNMP Trap 454
SNMP Version 3 455
CLI: Configure SNMPv3 455
Web Interface: Configure SNMPv3 456

sFlow 457
CLI: Configure Statistical Packet-Based Sampling of Packet Flows with sFlow 458
Web Interface: Configure Statistical Packet-based Sampling with sFlow 459
Time-Based Sampling of Counters with sFlow 460
CLI: Configure Time-Based Sampling of Counters with sFlow 460
Web Interface: Configure Time-Based Sampling of Counters with sFlow 461

Chapter 23 DNS

Domain Name System Concepts 463
Specify Two DNS Servers 463
CLI: Specify Two DNS Servers 463
Web Interface: Specify Two DNS Servers 463
Manually Add a Host Name and an IP Address 464
CLI: Manually Add a Host Name and an IP Address 464
Web Interface: Manually Add a Host Name and an IP Address 464

Chapter 24 DHCP Server

Dynamic Host Configuration Protocol Concepts 466
Configure a DHCP Server in Dynamic Mode 466
CLI: Configure a DHCP Server in Dynamic Mode 466
Web Interface: Configure a DHCP Server in Dynamic Mode 467
Configure a DHCP Server that Assigns a Fixed IP Address 469
CLI: Configure a DHCP Server that Assigns a Fixed IP Address 469
Web Interface: Configure a DHCP Server that Assigns a Fixed IP Address 470

Chapter 25 DHCPv6 Server

Dynamic Host Configuration Protocol Version 6 Concepts 473
CLI: Configure DHCPv6 Prefix Delegation 474
Web Interface: Configure DHCPv6 Prefix Delegation 475
Configure a Stateless DHCPv6 Server 479
CLI: Configure a Stateless DHCPv6 Server 479
Web Interface: Configure a Stateless DHCPv6 Server 480
Configure a Stateful DHCPv6 Server 483
CLI: Configure a Stateful DHCPv6 Server 483
Web Interface: Configure a Stateful DHCPv6 Server 484
CLI: Set Up a Configuration With a DHCPv6 Server and DHCPv6 Relay 488
Configure the DHCPv6 Server 488
Configure the DHCPv6 Relay 489

Chapter 26 DVLANs and Private VLANs

Double VLANs 492
CLI: Enable a Double VLAN 493
Web Interface: Enable a Double VLAN 493

Private VLAN Groups 496
CLI: Create a Private VLAN Group 497
Web Interface: Create a Private VLAN Group 498

Chapter 27 STP

Spanning Tree Protocol Concepts 503
Configure Classic STP (802.1d) 503
CLI: Configure Classic STP (802.1d) 503
Web Interface: Configure Classic STP (802.1d) 503
Configure Rapid STP (802.1w) 504
CLI: Configure Rapid STP (802.1w) 504
Web Interface: Configure Rapid STP (802.1w) 505
Configure Multiple STP (802.1s) 506
CLI: Configure Multiple STP (802.1s) 506
Web Interface: Configure Multiple STP (802.1s) 507
Configure PVSTP and PVRSTP 508
CLI: Configure PVSTP 510
Web Interface: Configure PVSTP 513

Chapter 28 Tunnels for IPv6

Tunnel Concepts 518
Create a 6in4 Tunnel 518
CLI: Create a 6in4 Tunnel 519
Web Interface: Create a 6in4 Tunnel 520
Create a 6to4 Tunnel 524
CLI: Create a 6to4 Tunnel 525
Web Interface: Create a 6to4 Tunnel 530

Chapter 29 IPv6 Interface Configuration

Create an IPv6 Routing Interface 544
CLI: Create an IPv6 Routing Interface 544
Web Interface: Create an IPv6 Routing Interface 545
Create an IPv6 Routing VLAN 547
CLI: Create an IPv6 Routing VLAN 547
Web Interface: Create an IPv6 VLAN Routing Interface 549
Configure DHCPv6 Mode on the Routing Interface 551
CLI: Configure DHCPv6 mode on routing interface 551
Web Interface: Configure DHCPv6 mode on routing interface 552

Chapter 30 PIM

Protocol Independent Multicast Concepts 556
PIM-DM 556
CLI: Configure PIM-DM 558
Web Interface: Configure PIM-DM 562
PIM-SM 579

CLI: Configure PIM-SM 580
Web Interface: Configure PIM-SM 584

Chapter 31 DHCP L2 Relay and L3 Relay

DHCP L2 Relay 605
CLI: Enable DHCP L2 Relay 605
Web Interface: Enable DHCP L2 Relay 607
DHCP L3 Relay 609
Configure the DHCP L3 Server in a Windows Server Operating System . . 610
Configure a DHCP L3 Switch 618

Chapter 32 MLD

Multicast Listener Discovery Concepts 624
Configure MLD 624
CLI: Configure MLD 625
Web Interface: Configure MLD 627
MLD Snooping 636
CLI: Configure MLD Snooping 637
Web Interface: Configure MLD Snooping 638

Chapter 33 DVMRP

Distance Vector Multicast Routing Protocol Concepts 641
CLI: Configure DVMRP 642
Web Interface: Configure DVMRP 648

Chapter 34 Link Dependency

Link Dependency Concepts 659
CLI: Create a Link State Group 660
Web Interface: Create a Link State Group 660

Chapter 35 Captive Portals

Captive Portal Concepts 664
Captive Portal Configuration Concepts 665
Enable a Captive Portal 665
CLI: Enable a Captive Portal 665
Web Interface: Enable a Captive Portal 666
Client Access, Authentication, and Control 667
Block a Captive Portal Instance 667
CLI: Block a Captive Portal Instance 667
Web Interface: Block a Captive Portal Instance 668
Local Authorization, Create Users and Groups 668
CLI: Create Users and Groups 668
Web Interface: Create Users and Groups 669
Remote Authorization (RADIUS) User Configuration 670
CLI: Configure RADIUS as the Verification Mode 671

Web Interface: Configure RADIUS as the Verification Mode 672
SSL Certificates 672

Chapter 36 iSCSI

iSCSI Concepts 674
Enable iSCSI Awareness with VLAN Priority Tag 675
CLI: Enable iSCSI Awareness with VLAN Priority Tag 675
Web Interface: Enable iSCSI Awareness with VLAN Priority Tag 675
Enable iSCSI Awareness with DSCP 676
CLI: Enable iSCSI Awareness with DSCP 676
Web Interface: Enable iSCSI Awareness with DSCP 676
Set the iSCSI Target Port 677
CLI: Set iSCSI Target Port 677
Web Interface: Set iSCSI Target Port 677
Show iSCSI Sessions 678
CLI: Show iSCSI Sessions 678
Web Interface: Show iSCSI Sessions 679

Chapter 37 Override Factory Defaults

Override the Factory Default Configuration File 681
CLI: Install Another Factory Defaults Configuration File 681
CLI: Erase the Old Factory Default Configuration File 682

Chapter 38 NETGEAR SFP

Connect with NETGEAR SFP AGM731F 684

Index

Documentation Resources

1

Before installation, read the release notes for your switch. The release notes detail the platform-specific functionality of the switching, routing, SNMP, configuration, management, and other packages. In addition, see the following publications:

- The installation guide for your switch:
  - *Installation NETGEAR ProSAFE Managed Switches, M4200 Series*
  - *Installation NETGEAR ProSAFE Managed Switches, M4300 Series*
- The hardware installation guide for your switch:
  - *ProSAFE Managed Switch Series M4200 Hardware Installation Guide*
  - *ProSAFE Managed Switch Series M4200 Hardware Installation Guide*
- *M4200 and M4300 Series ProSAFE Managed Switches Software Setup Manual*
- *M4200 and M4300 Series ProSAFE Managed Switches CLI Command Reference Manual*
- *M4200 and M4300 Web Management User Guide*

Note: For more information about the topics covered in this manual, visit the support website at *netgear.com/support*.

Note: Firmware updates with new features and bug fixes are made available from time to time on *downloadcenter.netgear.com*. Some products can regularly check the site and download new firmware, or you can check for and download new firmware manually. If the features or behavior of your product do not match what is described in this guide, you might need to update your firmware.

VLANs

2

Virtual LANs

This chapter includes the following sections:

- *VLAN Concepts*
- *Create Two VLANs*
- *Assign Ports to VLAN 2*
- *Create Three VLANs*
- *Assign Ports to VLAN 3*
- *Assign VLAN 3 as the Default VLAN for Port 1/0/2*
- *Create a MAC-Based VLAN*
- *Create a Protocol-Based VLAN*
- *Virtual VLANs: Create an IP Subnet–Based VLAN*
- *Voice VLANs*
- *Configure GARP VLAN Registration Protocol*
- *Private VLANs*
- *Assign Private-VLAN Types (Primary, Isolated, Community)*
- *Configure Private-VLAN Association*
- *Configure Private-VLAN Port Mode (Promiscuous, Host)*
- *Configure Private-VLAN Host Ports*
- *Map Private-VLAN Promiscuous Port*
- *VLAN Access Ports and Trunk Ports*

VLAN Concepts

Adding virtual LAN (VLAN) support to a Layer 2 switch offers some of the benefits of both bridging and routing. Like a bridge, a VLAN switch forwards traffic based on the Layer 2 header, which is fast. Like a router, it partitions the network into logical segments, which provides better administration, security, and management of multicast traffic.

A VLAN is a set of end stations and the switch ports that connect them. You can have different reasons for the logical division, such as department or project membership. The only physical requirement is that the end station and the port to which it is connected both belong to the same VLAN.

Each VLAN in a network has an associated VLAN ID, which appears in the IEEE 802.1Q tag in the Layer 2 header of packets transmitted on a VLAN. An end station might omit the tag, or the VLAN portion of the tag, in which case the first switch port to receive the packet can either reject it or insert a tag using its default VLAN ID. A given port can handle traffic for more than one VLAN, but it can support only one default VLAN ID.

The Private Edge VLAN feature lets you set protection between ports located on the switch. This means that a protected port cannot forward traffic to another protected port on the same switch. The feature does not provide protection between ports located on different switches.

The diagram in this section shows a switch with four ports configured to handle the traffic for two VLANs. Port 1/0/2 handles traffic for both VLANs, while port 1/0/1 is a member of VLAN 2 only, and ports 1/0/3 and 1/0/4 are members of VLAN 3 only. The script following the diagram shows the commands you would use to configure the switch as shown in the diagram.

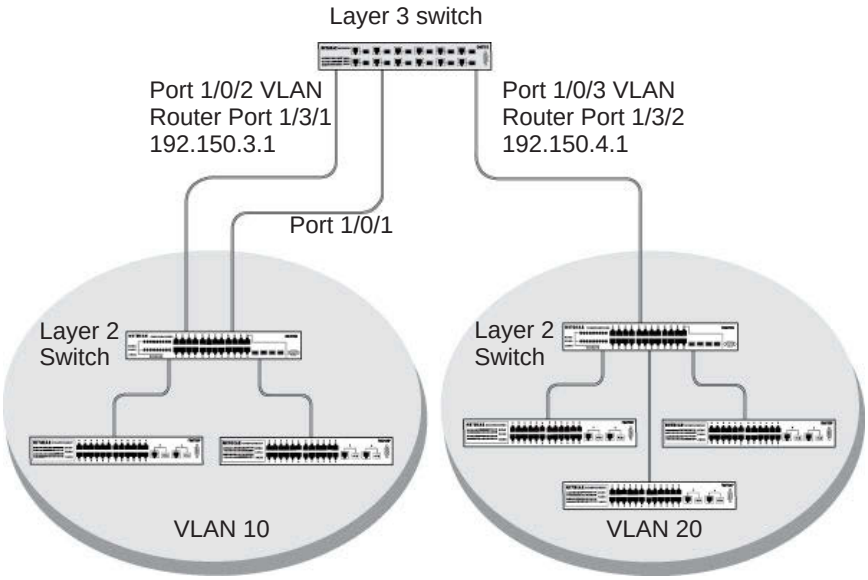


Figure 1. Switch with 4 ports configured for traffic from 2 VLANs

The following examples show how to create VLANs, assign ports to the VLANs, and assign a VLAN as the default VLAN to a port.

Create Two VLANs

The example is shown as CLI commands and as a web interface procedure.

CLI: Create Two VLANs

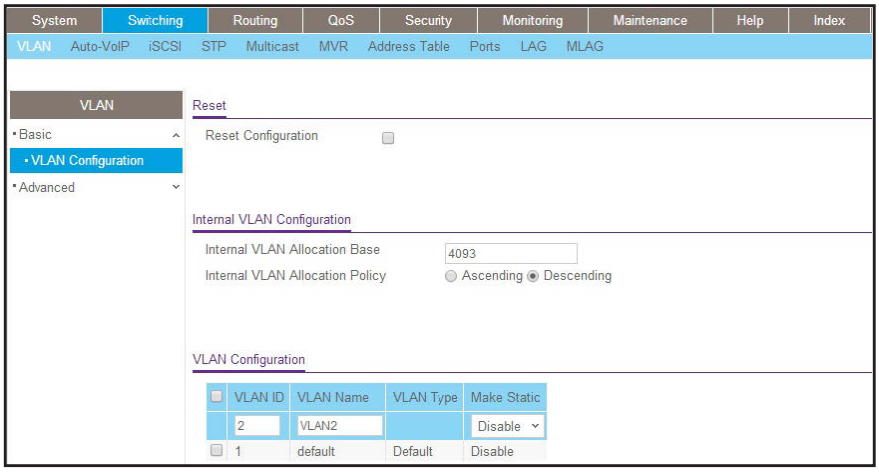
Use the following commands to create two VLANs and to assign the VLAN IDs while leaving the names blank.

```
(Netgear Switch) #vlan database
(Netgear Switch) (Vlan)#vlan 2
(Netgear Switch) (Vlan)#vlan 3
(Netgear Switch) (Vlan)#exit
```

Web Interface: Create Two VLANs

1. Create VLAN2.
   a. Select **Switching > VLAN > Basic > VLAN Configuration**.

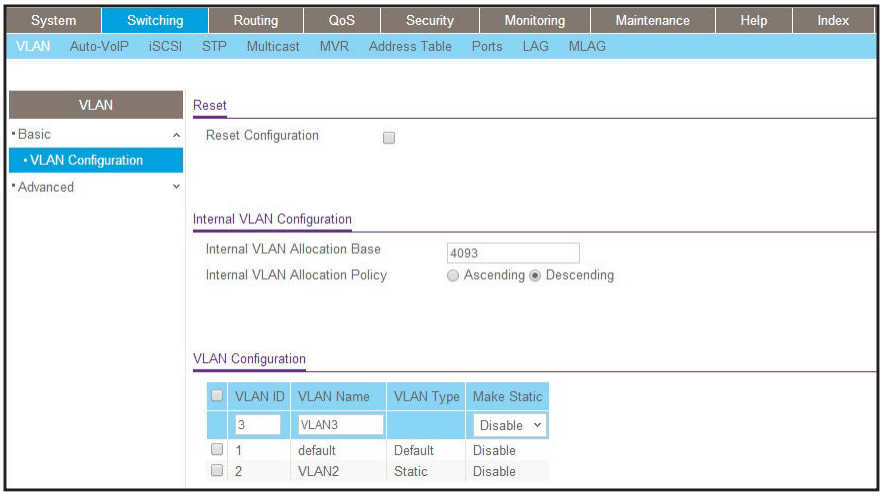
      A screen similar to the following displays.



   b. Enter the following information:
      - In the **VLAN ID** field, enter **2**.
      - In the **VLAN Name** field, enter **VLAN2**.
      - In the **VLAN Type** list, select **Static**.

   c. Click **Add.**
2. Create VLAN3.
   a. Select **Switching > VLAN > Basic > VLAN Configuration**.

A screen similar to the following displays.



b. Enter the following information:

- In the **VLAN ID** field, enter **3**.
- In the **VLAN Name** field, enter **VLAN3**.
- In the **VLAN Type** list, select **Static**.

c. Click **Add.**

Assign Ports to VLAN 2

This sequence shows how to assign ports to VLAN2, and to specify that frames will always be transmitted tagged from all member ports and that untagged frames will be rejected on receipt.

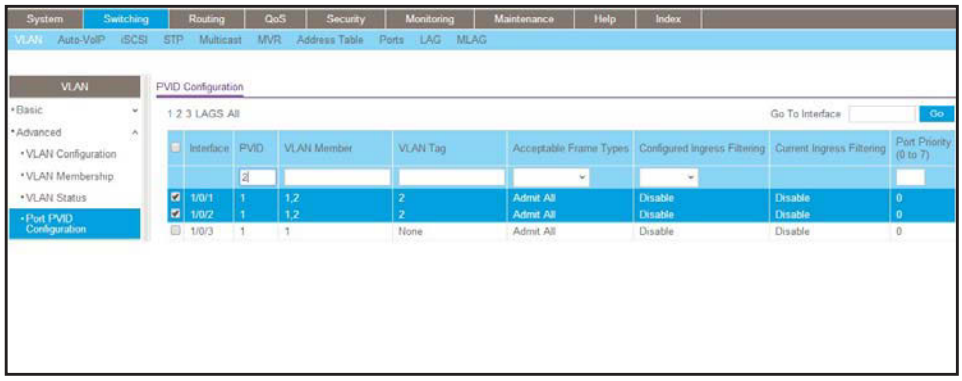
CLI: Assign Ports to VLAN 2

```
(Netgear Switch) #config
(Netgear Switch) (Config)#interface range 1/0/1-1/0/2
(Netgear Switch) (conf-if-range-1/0/1-1/0/2)#vlan participation include 2
(Netgear Switch) (conf-if-range-1/0/1-1/0/2)#vlan acceptframe vlanonly
(Netgear Switch) (conf-if-range-1/0/1-1/0/2)#vlan pvid 2
(Netgear Switch) (conf-if-range-1/0/1-1/0/2)#exit
(Netgear Switch) (Config)#vlan port tagging all 2
(Netgear Switch) (Config)#
```

Web Interface: Assign Ports to VLAN 2

1. Assign ports to VLAN2.
   a. Select **Switching > VLAN > Advanced > VLAN Membership**.

      A screen similar to the following displays.

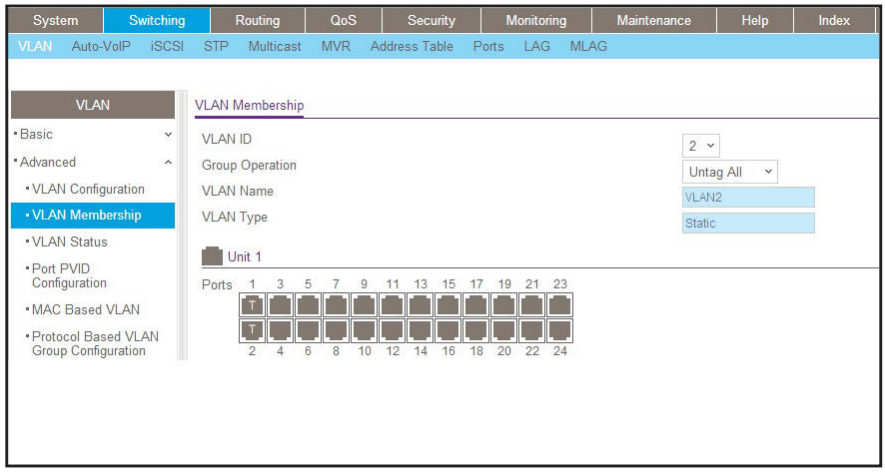


   b. In the **VLAN ID** list, select **2**.
   c. Click **Unit 1**. The ports display.
   d. Click the gray boxes under ports **1** and **2** until **T** displays.

      The T specifies that the egress packet is tagged for the ports.

   e. Click **Apply to** save the settings.
2. Specify that only tagged frames will be accepted on ports 1/0/1 and 1/0/2.
   a. Select **Switching > VLAN > Advanced > Port PVID Configuration**.

      A screen similar to the following displays.



   b. Under PVID Configuration, scroll down and select the check box for Interface **1/0/1**.

      Then scroll down and select the Interface **1/0/2** check box.

c. Enter the following information:
   - In the **Acceptable Frame Type polyhedron** list, select **VLAN Only**.
   - In the **PVID (1 to 4093)** field, enter **2**.

d. Click **Apply** to save the settings.

Create Three VLANs

The example is shown as CLI commands and as a web interface procedure.

CLI: Create Three VLANs

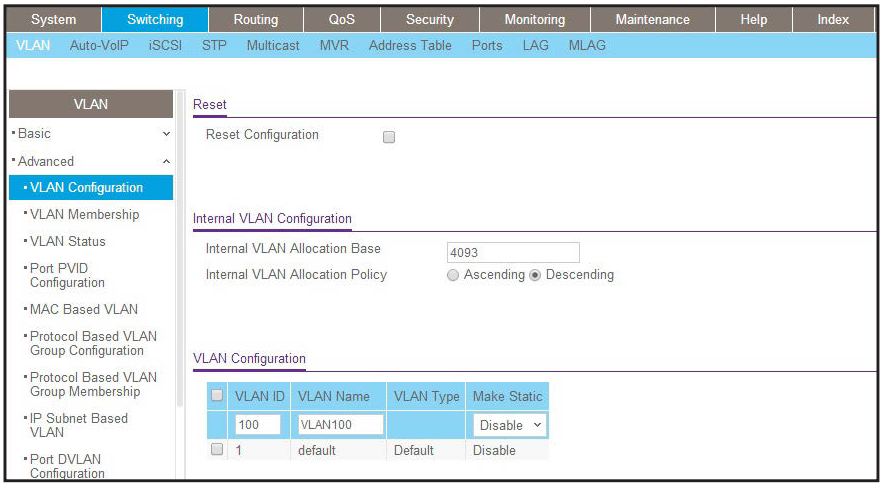
Use the following commands to create three VLANs and to assign the VLAN IDs while leaving the names blank.

```
(Netgear Switch) #vlan database
(Netgear Switch) (Vlan)#vlan 100
(Netgear Switch) (Vlan)#vlan 101
(Netgear Switch) (Vlan)#vlan 102
(Netgear Switch) (Vlan)#exit
```

Web Interface: Create Three VLANs

1. Create VLAN100.
   a. Select **Switching > VLAN > Basic > VLAN Configuration**.

      A screen similar to the following displays.

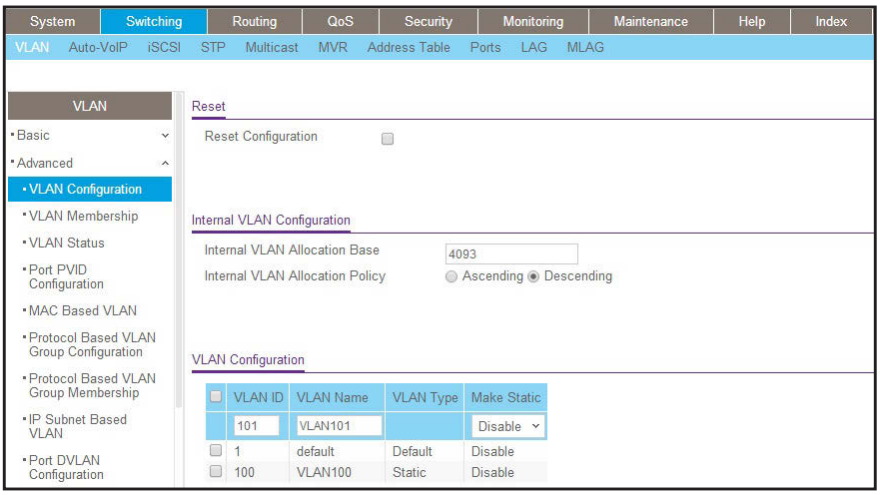


   b. Enter the following information:
      - In the **VLAN ID** field, enter **100**.
      - In the **VLAN Name** field, enter **VLAN100**.

   c. Click **Add.**

2. Create VLAN101.
   a. Select **Switching > VLAN > Basic > VLAN Configuration**.

      A screen similar to the following displays.

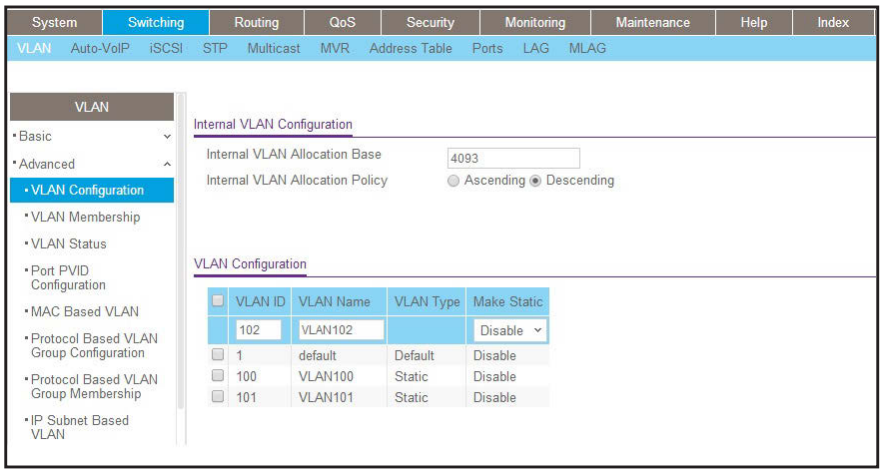


   b. Enter the following information:
      - In the **VLAN ID** field, enter **101**.
      - In the **VLAN Name** field, enter **VLAN101**.

   c. Click **Add.**

3. Create VLAN102.
   a. Select **Switching > VLAN > Basic > VLAN Configuration**.

      A screen similar to the following displays.



   b. Enter the following information:
      - In the **VLAN ID** field, enter **102**.
      - In the **VLAN Name** field, enter **VLAN102**.

   c. Click **Add.**

Assign Ports to VLAN 3

This example shows how to assign the ports that will belong to VLAN 3, and to specify that untagged frames will be accepted on port 1/0/4. Note that port 1/0/2 belongs to both VLANs and that port 1/0/1 can never belong to VLAN 3.

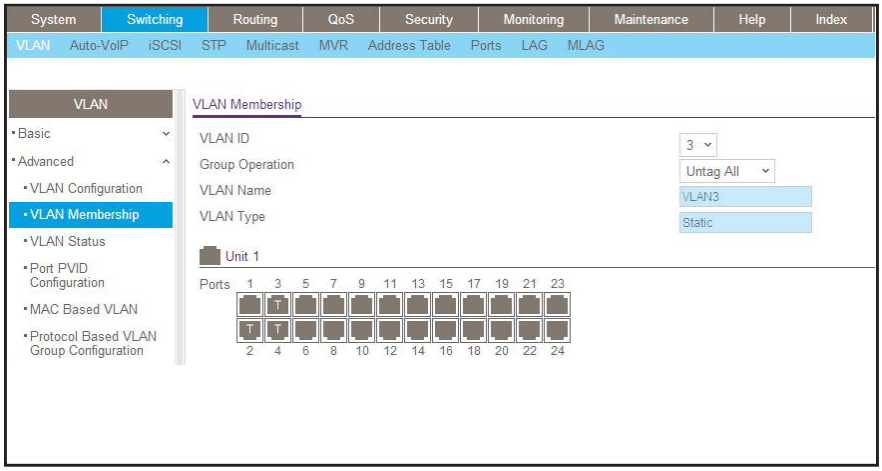
CLI: Assign Ports to VLAN 3

```
(Netgear Switch) (Config)#interface range 1/0/2-1/0/4
(Netgear Switch) (conf-if-range-1/0/2-1/0/4)#vlan participation include 3
(Netgear Switch) (conf-if-range-1/0/2-1/0/4)#exit
(Netgear Switch) (Config)#interface 1/0/4
(Netgear Switch) (Interface 1/0/4)#vlan acceptframe all
(Netgear Switch) (Interface 1/0/4)#exit
(Netgear Switch) (Config)#exit
```

Web Interface: Assign Ports to VLAN 3

1. Assign ports to VLAN3.
   a. Select **Switching > VLAN > Advanced > VLAN Membership**.

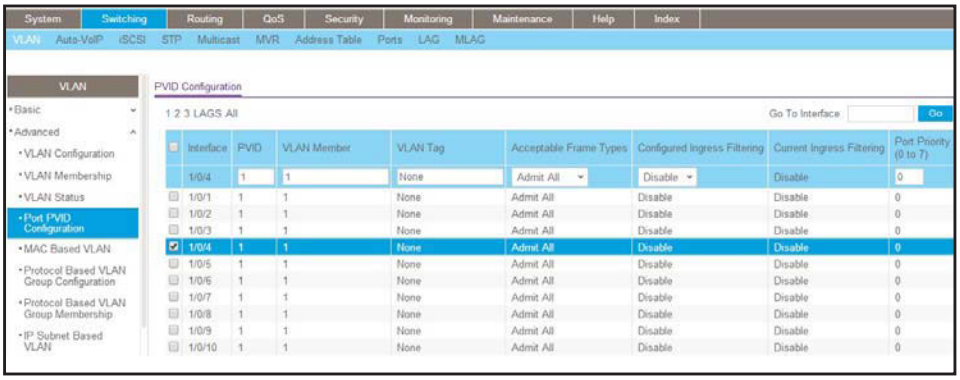
      A screen similar to the following displays.



   b. In the **VLAN ID** list, select **3**.
   c. Click **Unit 1.** The ports display.
   d. Click the gray boxes under ports 2, 3, and 4 until T displays.

      The T specifies that the egress packet is tagged for the ports.
   e. Click **Apply** to save the settings.
2. Specify that untagged frames will be accepted on port 1/0/4.
   a. Select **Switching > VLAN > Advanced > Port PVID Configuration**.

A screen similar to the following displays.



b. Scroll down and select the Interface **1/0/4** check box.

Now 1/0/4 appears in the Interface field at the top.

c. In the **Acceptable Frame Types** list, select **Admit All**.

d. Click **Apply** to save the settings.

Assign VLAN 3 as the Default VLAN for Port 1/0/2

This example shows how to assign VLAN 3 as the default VLAN for port 1/0/2.

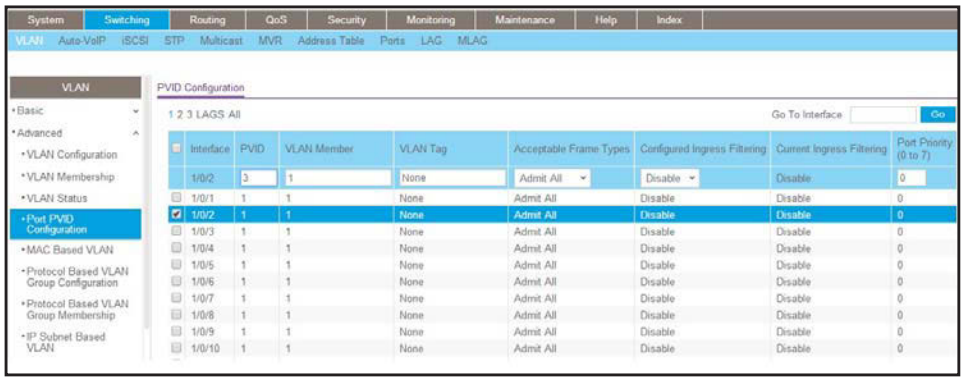
CLI: Assign VLAN 3 as the Default VLAN for Port 1/0/2

```
(Netgear Switch) #config
(Netgear Switch) (Config)#interface 1/0/2
(Netgear Switch) (Interface 1/0/2)#vlan pvid 3
(Netgear Switch) (Interface 1/0/2)#exit
(Netgear Switch) (Config)#exit
```

Web Interface: Assign VLAN 3 as the Default VLAN for Port 1/0/2

1. Select **Switching > VLAN > Advanced > Port PVID Configuration**.

   A screen similar to the following displays.



2. Under PVID Configuration, scroll down and select the Interface **1/0/2** check box. Now 1/0/2 appears in the Interface field at the top.
3. In the **PVID (1 to 4093)** field, enter **3**.
4. Click **Apply** to save the settings.

Create a MAC-Based VLAN

The MAC-based VLAN feature allows incoming untagged packets to be assigned to a VLAN and thus classify traffic based on the source MAC address of the packet.

You define a MAC to VLAN mapping by configuring an entry in the MAC to VLAN table. An entry is specified using a source MAC address and the appropriate VLAN ID. The MAC to VLAN configurations are shared across all ports of the device (i.e., there is a system-wide table that has MAC address to VLAN ID mappings).

When untagged or priority tagged packets arrive at the switch and entries exist in the MAC to VLAN table, the source MAC address of the packet is looked up. If an entry is found, the corresponding VLAN ID is assigned to the packet. If the packet is already priority tagged it will maintain this value; otherwise, the priority will be set to 0 (zero). The assigned VLAN ID is verified against the VLAN table. If the VLAN is valid, ingress processing on the packet continues; otherwise, the packet is dropped. This implies that you can configure a MAC address mapping to a VLAN that has not been created on the system.

CLI: Create a MAC-Based VLAN

1. Create VLAN3.

```
(Netgear Switch)#vlan database
(Netgear Switch)(Vlan)#vlan 3
(Netgear Switch)(Vlan)#exit
```

2. Add port 1/0/23 to VLAN3.

```
(Netgear Switch)#config
(Netgear Switch)(Config)#interface 1/0/23
(Netgear Switch)(Interface 1/0/23)#vlan participation include 3
(Netgear Switch)(Interface 1/0/23)#vlan pvid 3
(Netgear Switch)(Interface 1/0/23)#exit
```

3. Map MAC 00:00:0A:00:00:02 to VLAN3.

```
(Netgear Switch)(Config)#exit
(Netgear Switch)#vlan data
(Netgear Switch)(Vlan)#vlan association mac 00:00:00A:00:00:02 3
(Netgear Switch)(Vlan)#exit
```

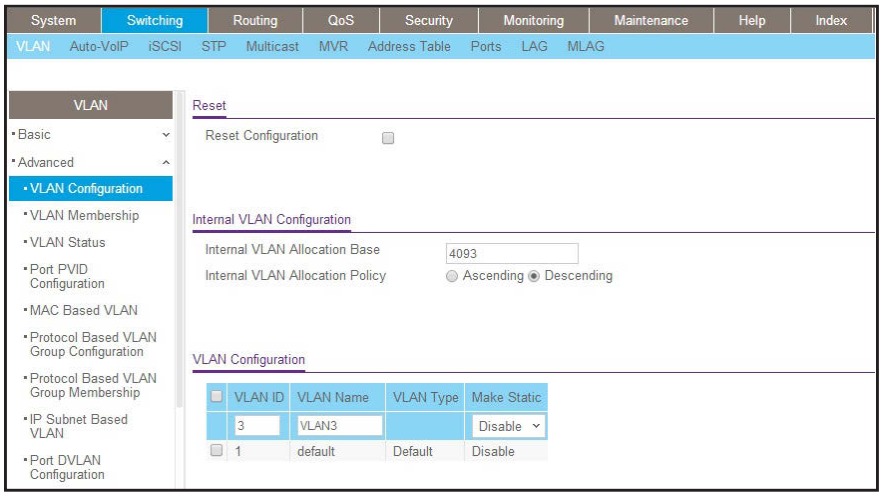
4. Add all the ports to VLAN3.

```
(Netgear Switch)#config
(Netgear Switch)(Config)#interface range 1/0/1-1/0/28
(Netgear Switch)(conf-if-range-1/0/1-1/0/28)#vlan participation include 3
(Netgear Switch)(conf-if-range-1/0/1-1/0/28)#exit
(Netgear Switch)(Config)#exit
```

Web Interface: Assign a MAC-Based VLAN

1. Create VLAN3.
   a. Select **Switching > VLAN > Basic > VLAN Configuration**.

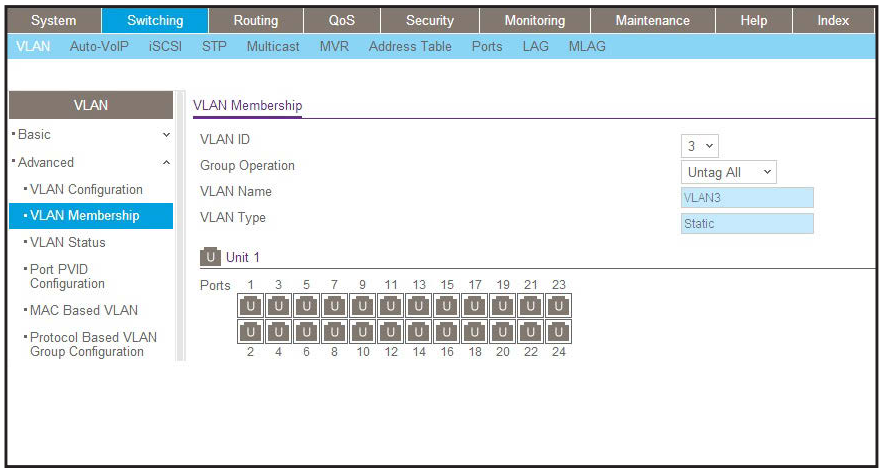
      A screen similar to the following displays.



   b. Enter the following information:
      - In the **VLAN ID** field, enter **3**.
      - In the **VLAN Name** field, enter **VLAN3**.
      - In the **VLAN Type** list, select **Static**.

   c. Click **Add**.
2. Assign ports to VLAN3.
   a. Select **Switching > VLAN > Advanced > VLAN Membership**.

      A screen similar to the following displays.



   b. In the **VLAN ID** list, select **3**.
   c. Click **Unit 1.** The ports display.

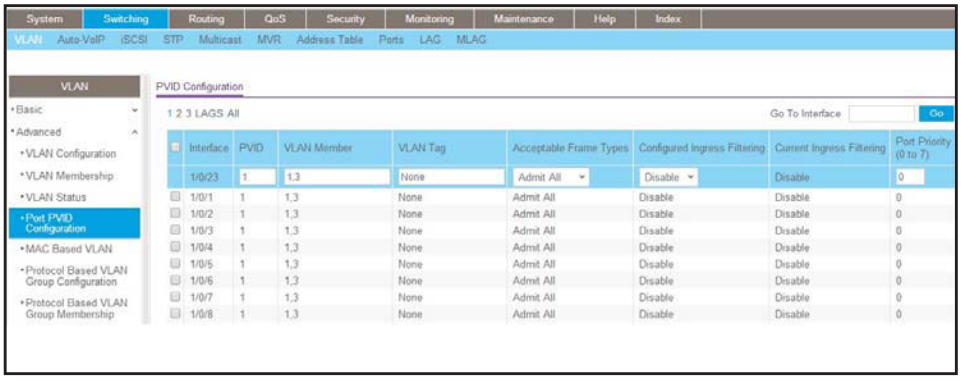
d. Click the gray box before Unit 1 until **U** displays.

e. Click **Apply**.

3. Assign VPID3 to port 1/0/23.

a. Select **Switching > VLAN > Advanced > Port PVID Configuration**.

A screen similar to the following displays.



b. Scroll down and select the **1/0/23** check box.

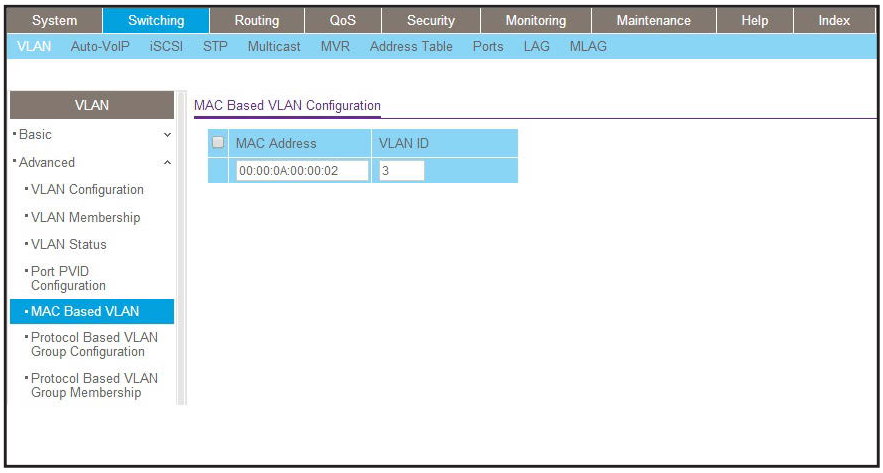
c. In the **PVID (1 to 4093)** field, enter **3**.

d. Click **Apply** to save the settings.

4. Map the specific MAC to VLAN3.

a. Select **Switching > VLAN > Advanced > MAC based VLAN**.

A screen similar to the following displays.



b. Enter the following information:

- In the **MAC Address** field, enter **00:00:0A:00:00:02**.
- In the **PVID (1 to 4093)** field, enter **3**.

c. Click **Add**.

Create a Protocol-Based VLAN

Create two protocol VLAN groups. One is for IPX and the other is for IP/ARP. The untagged IPX packets are assigned to VLAN 4, and the untagged IP/ARP packets are assigned to VLAN 5.

CLI: Create a Protocol-Based VLAN

1. Create a VLAN protocol group vlan_ipx based on IPX protocol.

```
(Netgear Switch)#config
(Netgear Switch)(Config)#vlan protocol group 1
(Netgear Switch)(Config)#vlan protocol group name 1 "vlan_ipx"
(Netgear Switch)(Config)#vlan protocol group add protocol 1 ethertype ipx
```

2. Create a VLAN protocol group vlan_ipx based on IP/ARP protocol.

```
(Netgear Switch)(Config)#vlan protocol group 2
(Netgear Switch)(Config)#vlan protocol group name 2 "vlan_ip"
(Netgear Switch)(Config)#vlan protocol group add protocol 2 ethertype ip
(Netgear Switch)(Config)#vlan protocol group add protocol 2 ethertype arp
(Netgear Switch)(Config)#exit
```

3. Assign VLAN protocol group 1 to VLAN 4.

```
(Netgear Switch)#vlan database
(Netgear Switch)(Vlan)#vlan 4
(Netgear Switch)(Vlan)#vlan 5
(Netgear Switch)(Vlan)#protocol group 1 4
```

4. Assign VLAN protocol group 2 to VLAN 5.

```
(Netgear Switch)(Vlan)#protocol group 2 5
```

5. Enable protocol VLAN group 1 and 2 on the interface.

```
(Netgear Switch)(Vlan)#exit
(Netgear Switch)#config
(Netgear Switch)(Config)#interface 1/0/11
(Netgear Switch)(Interface 1/0/11)#protocol vlan group 1
(Netgear Switch)(Interface 1/0/11)#protocol vlan group 2
(Netgear Switch)(Interface 1/0/11)#exit
```

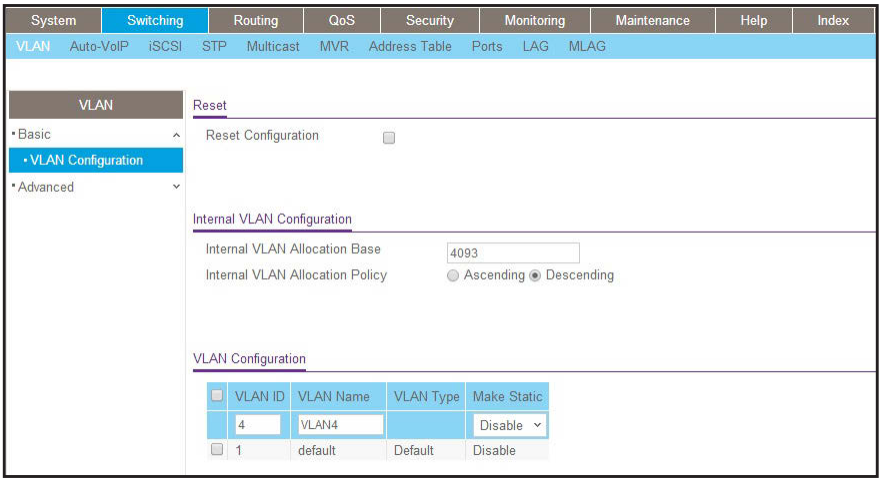
Web Interface: Create a Protocol-Based VLAN

1. Create VLAN4 and VLAN5.

   Create VLAN4.

   a. Select **Switching > VLAN > Basic > VLAN Configuration**.

      A screen similar to the following displays.



   b. Enter the following information:

      In the **VLAN ID** field, enter **4**.

      In the **VLAN Name** field, enter **VLAN4**.

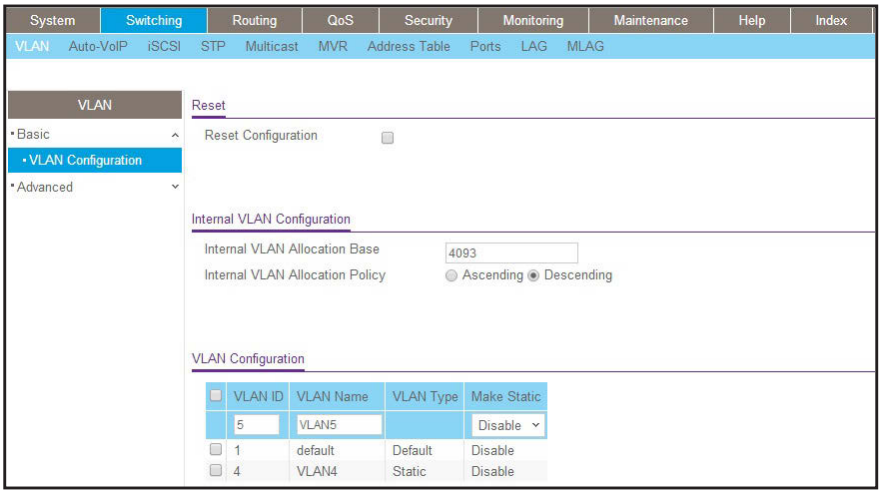
      In the **VLAN Type** list, select **Static**.

   c. Click **Add**.

   Create VLAN5.

   a. Select **Switching > VLAN > Basic > VLAN Configuration**.

      A screen similar to the following displays.



b. Enter the following information:

In the **VLAN ID** field, enter **5**.

In the **VLAN Name** field, enter **VLAN5**.

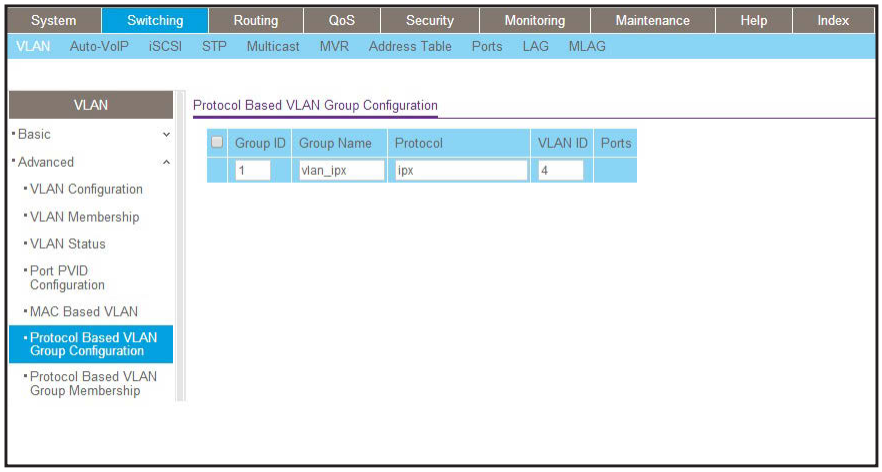
In the **VLAN Type** list, select **Static**.

c. Click **Add**.

2. Create the protocol-based VLAN group vlan_ipx.

a. Select **Switching > VLAN > Advanced > Protocol Based VLAN Group Configuration**.

A screen similar to the following displays.



Enter the following information:

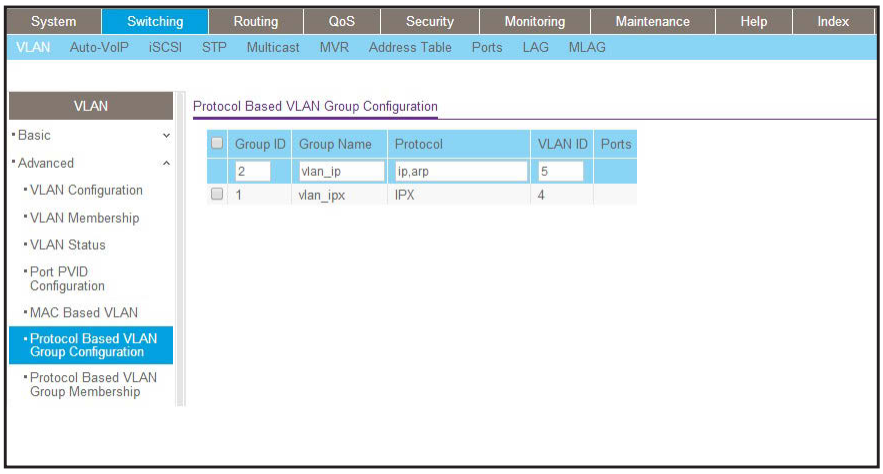
- In the **Group ID** field, enter **1**.
- In the **Group Name** field, enter **vlan_ipx**.
- In the **Protocol** list, enter **ipx**.
- In the **VLAN ID** field, enter **4.**

b. Click **Add**.

3. Create the protocol-based VLAN group vlan_ip.

a. Select **Switching > VLAN >Advanced > Protocol Based VLAN Group Configuration**.

A screen similar to the following displays.



b. Enter the following information:

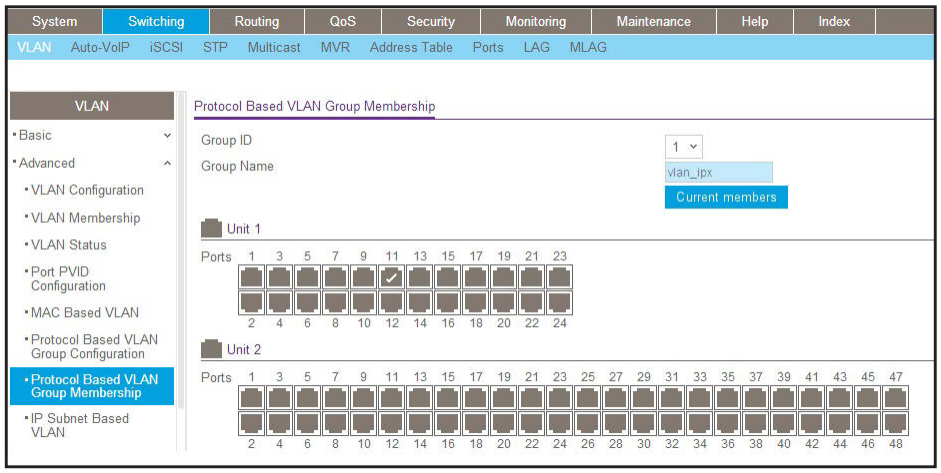
- In the **Group ID** field, enter **2**.
- In the **Group Name** field, enter **vlan_ip**.
- In the **Protocol** list, select **IP** and **ARP** while holding down the **Ctrl** key.
- In the **VLAN** field, enter **5.**

c. Click **Add**.

4. Add port 11 to the group vlan_ipx.

a. Select **Switching > VLAN > Advanced > Protocol Based VLAN Group Membership**.

A screen similar to the following displays.



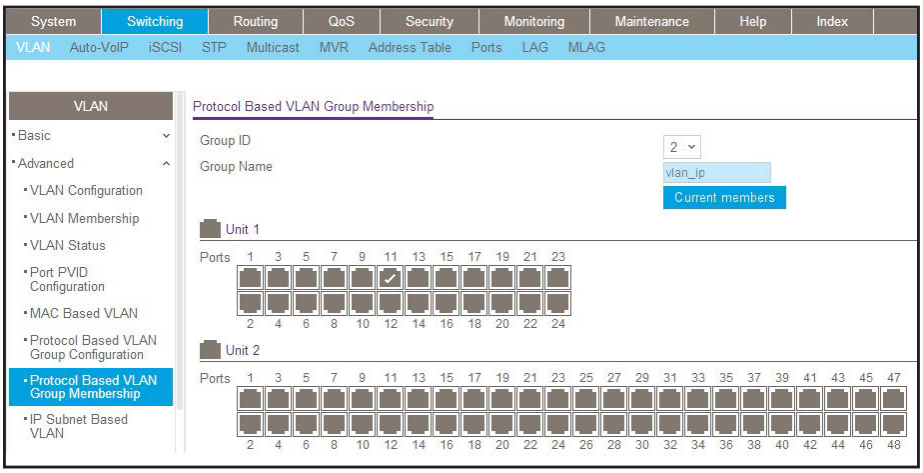
b. In the **Group ID** list, select **1**.

c. Click the gray box under port **11**. A check mark displays in the box.

d. Click the **Apply** button.

5. Add port 11 to the group vlan_ip.
   a. Select **Switching > VLAN > Advanced > Protocol Based VLAN Group Membership**.

      A screen similar to the following displays.



   b. In the **Group ID** list, select **2**.
   c. Click the gray box under port **11**. A check mark displays in the box.
   d. Click **Apply**.

Virtual VLANs: Create an IP Subnet–Based VLAN

In an IP subnet–based VLAN, all the end workstations in an IP subnet are assigned to the same VLAN. In this VLAN, users can move their workstations without reconfiguring their network addresses. IP subnet VLANs are based on Layer 3 information from packet headers. The switch makes use of the network-layer address (for example, the subnet address for TCP/IP networks) in determining VLAN membership. If a packet is untagged or priority tagged, the switch associates the packet with any matching IP subnet classification. If no IP subnet classification can be made, the packet is subjected to the normal VLAN classification rules of the switch. This IP subnet capability does not imply a *routing* function or that the VLAN is routed. The IP subnet classification feature affects only the VLAN assignment of a packet. Appropriate 802.1Q VLAN configuration must exist in order for the packet to be switched.

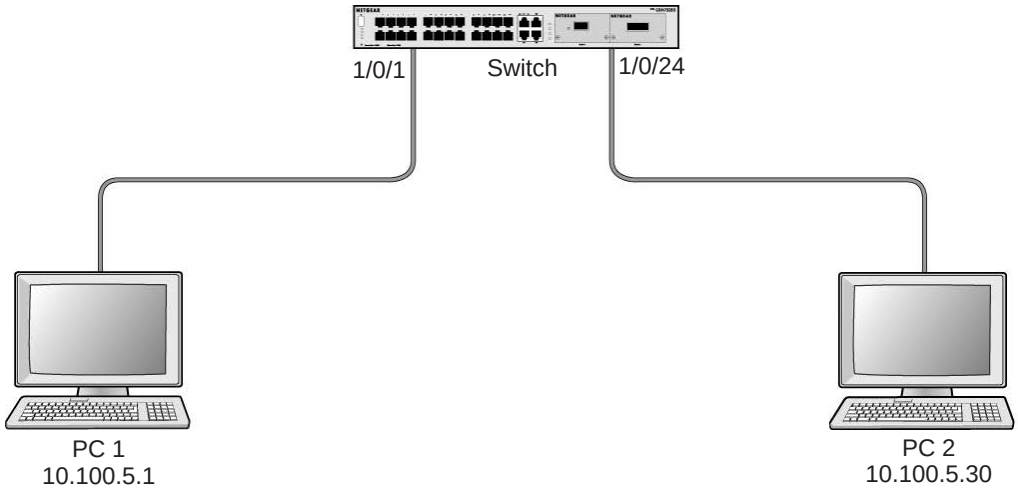


Figure 2. IP subnet–based VLAN

CLI: Create an IP Subnet–Based VLAN

```
(Netgear Switch) #vlan database
(Netgear Switch) (Vlan)#vlan 2000
(Netgear Switch) (Vlan)#vlan association subnet 10.100.0.0 255.255.0.0 2000
(Netgear Switch) (Vlan)#exit
```

Create an IP subnet–based VLAN 2000.

```
(Netgear Switch) #config
(Netgear Switch) (Config)#interface range 1/0/1-1/0/24
(Netgear Switch) (conf-if-range-1/0/1-1/0/24)# vlan participation include 2000
(Netgear Switch) (conf-if-range-1/0/1-1/0/24)#exit
(Netgear Switch) (Config)#
```

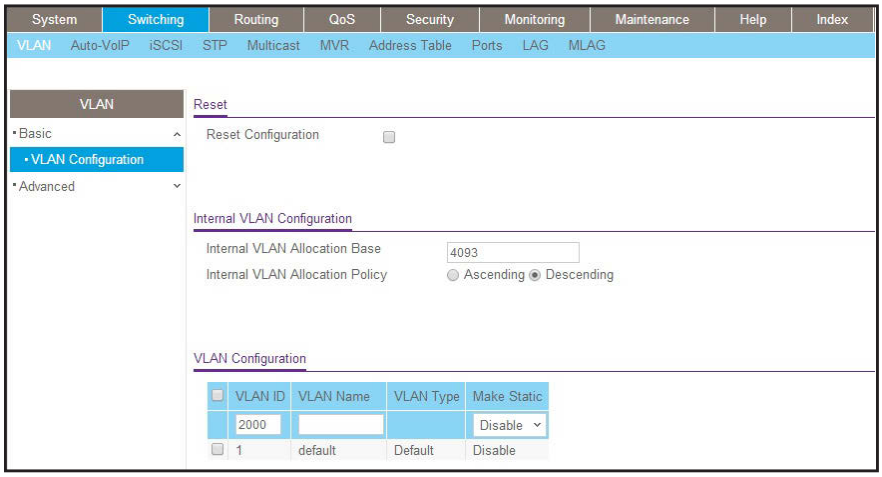
Assign all the ports to VLAN 2000.

```
(Netgear Switch) #show mac-addr-table vlan 2000
MAC Address     Interface     Status
-----------------  ---------  ------------
00:00:24:58:F5:56  1/0/1      Learned
00:00:24:59:00:62  1/0/24     Learned
```

Web Interface: Create an IP Subnet–Based VLAN

1. Create VLAN 2000.
   a. Select **Switching > VLAN > Basic > VLAN Configuration**.

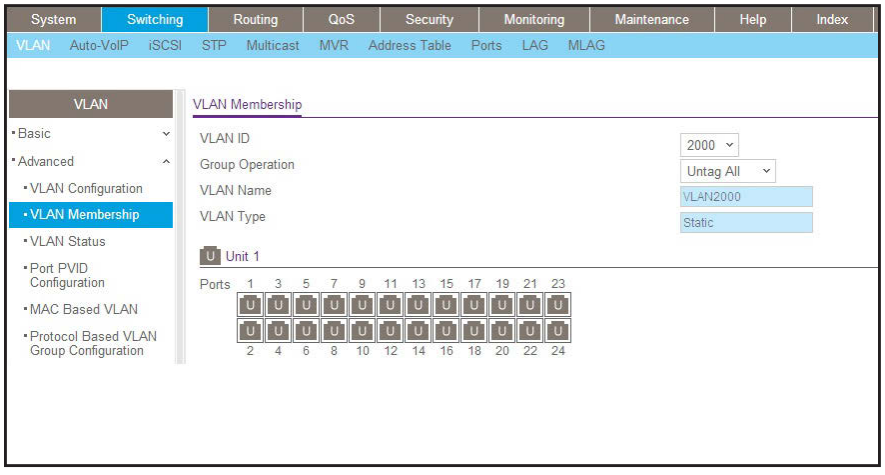
      A screen similar to the following displays.



   b. Enter the following information:
      - In the **VLAN ID** field, enter **2000**.
      - In the **VLAN Type** list, select **Static**.

   c. Click **Add**.
2. Assign all the ports to VLAN 2000.
   a. Select **Switching > VLAN > Advanced > VLAN Membership**.

      A screen similar to the following displays.



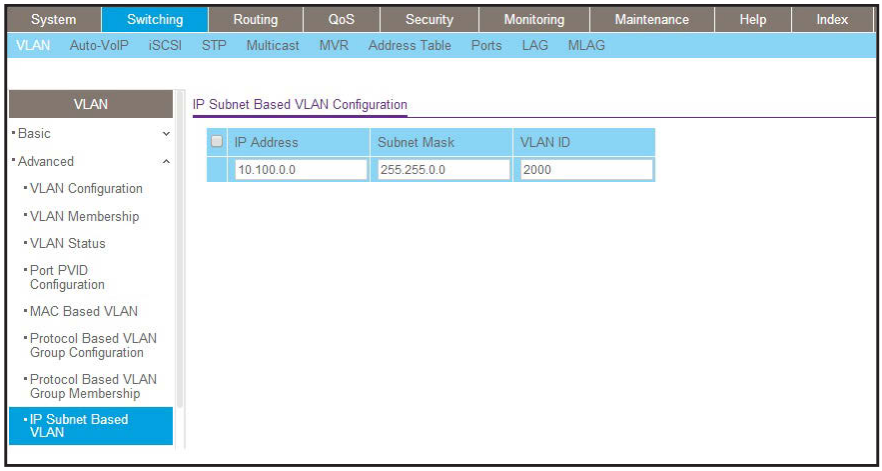
   b. In the **VLAN ID** list, select **2000**.
   c. Click **Unit 1**. The ports display.
   d. Click the gray box before Unit 1 until **U** displays.

e. Click **Apply**.

3. Associate the IP subnet with VLAN 2000.

a. Select **Switching > VLAN > Advanced > IP Subnet Based VLAN**.

A screen similar to the following displays.



b. Enter the following information:

- In the **IP Address** field, enter **10.100.0.0**.
- In the **Subnet Mask** field, enter **255.255.0.0**.
- In the **VLAN (1 to 4093)** field, enter **2000**.

c. Click **Add**.

Voice VLANs

The voice VLAN feature enables switch ports to carry voice traffic with defined priority to enable separation of voice and data traffic coming onto port. Voice VLAN ensures that the sound quality of an IP phone does not deteriorate when the data traffic on the port is high. Also, the inherent isolation provided by VLANs ensures that inter-VLAN traffic is under management control and that clients attached to the network cannot initiate a direct attack on voice components.

Note: For more information about voice VLANs, see*Auto VoIP* on page 255.

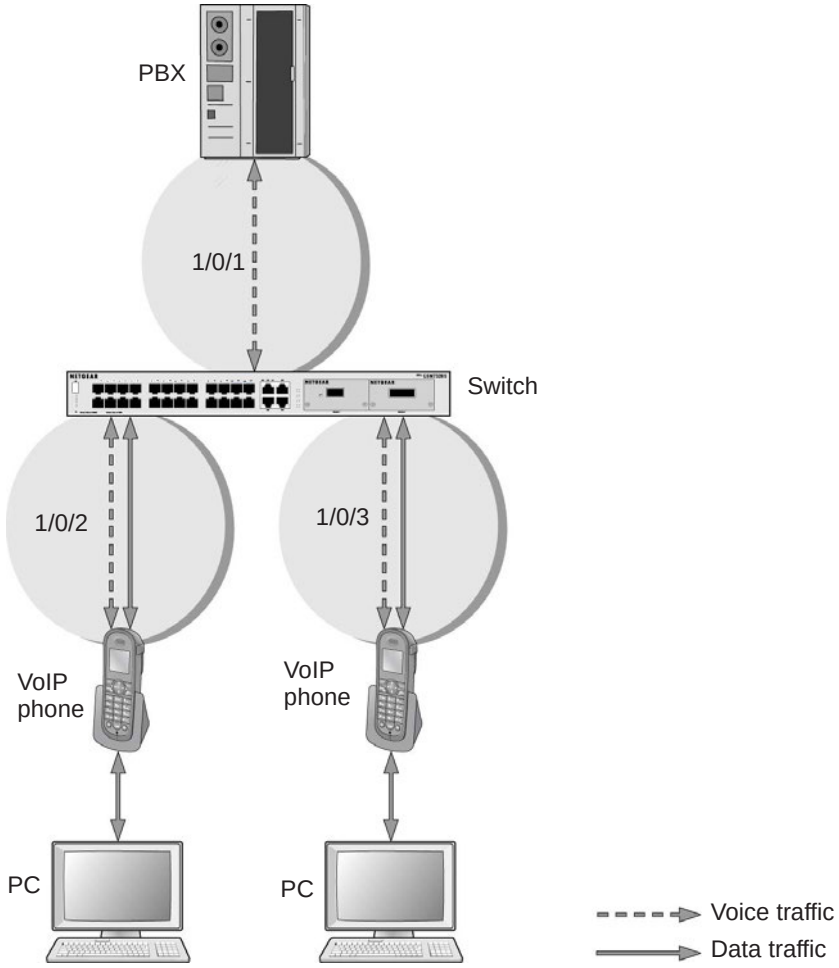


Figure 3. Voice VLAN

The script in this section shows how to configure Voice VLAN and prioritize the voice traffic. Here the Voice VLAN mode is in VLAN ID 10.

CLI: Configure Voice VLAN and Prioritize Voice Traffic

1. Create VLAN 10.

```
(Netgear Switch) #vlan database
(Netgear Switch) (Vlan)#vlan 10
(Netgear Switch) (Vlan)#exit
```

2. Include the ports 1/0/1 and 1/0/2 in VLAN 10.

```
(Netgear Switch) (Config)#interface range 1/0/1-1/0/2
(Netgear Switch) (conf-if-range-1/0/1-1/0/2)#vlan participation include 10
(Netgear Switch) (conf-if-range-1/0/1-1/0/2)#vlan tagging 10
(Netgear Switch) (conf-if-range-1/0/1-1/0/2)#exit
```

3. Configure Voice VLAN globally.

```
(Netgear Switch) (Config)# voice vlan
```

4. Configure Voice VLAN mode in the interface 1/0/2.

```
(Netgear Switch) (Config)#interface 1/0/2
(Netgear Switch) (Interface 1/0/2)#voice vlan 10
(Netgear Switch) (Interface 1/0/2)#exit
```

5. Create the DiffServ class ClassVoiceVLAN.

```
(Netgear Switch) (Config)#class-map match-all ClassVoiceVLAN
```

6. Configure VLAN 10 as the matching criteria for the class.

```
(Netgear Switch) (Config-classmap)#match vlan 10
```

7. Create the DiffServ policy PolicyVoiceVLAN.

```
(Netgear Switch) (Config)#policy-map PolicyVoiceVLAN in
```

8. Map the policy and class and assign them to the higher-priority queue.

```
(Netgear Switch) (Config-policy-map)#class ClassVoiceVLAN
(Netgear Switch) (Config-policy-classmap)#assign-queue 3
(Netgear Switch) (Config-policy-classmap)#exit
```

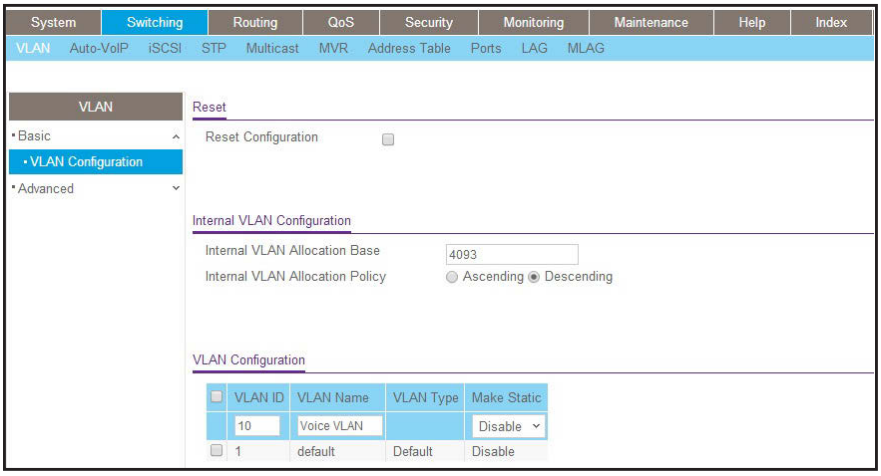
9. Assign it to interfaces 1/0/1 and 1/0/2.

```
(Netgear Switch) (Config)#interface range 1/0/1-1/0/2
(Netgear Switch) (conf-if-range-1/0/1-1/0/2)# service-policy in PolicyVoiceVLAN
```

Web Interface: Configure Voice VLAN and Prioritize Voice Traffic

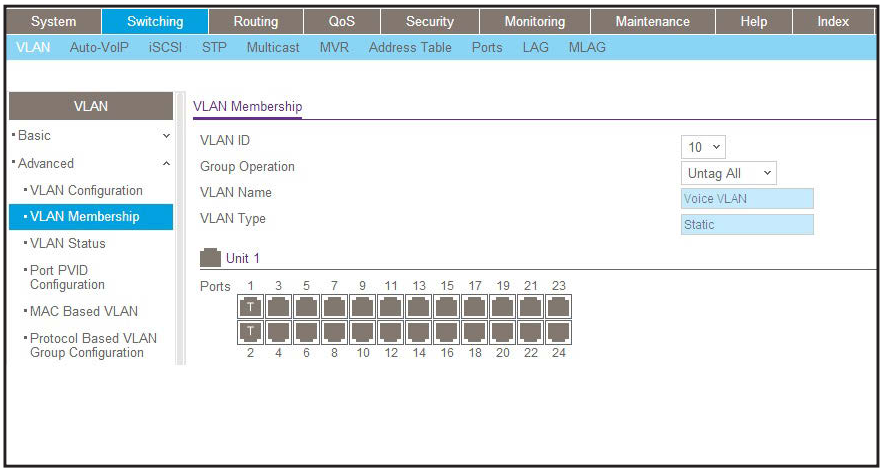
1. Create VLAN 10.
   a. Select **Switching > VLAN > Basic > VLAN Configuration**.

      A screen similar to the following displays.



   b. In the VLAN ID field, enter 10.
   c. In the **VLAN Name** field, enter **Voice VLAN**.
   d. Click **Add**.
2. Include the ports 1/0/1 and 1/0/2 in VLAN 10.
   a. Select **Switching > VLAN > Advanced > VLAN Membership**.

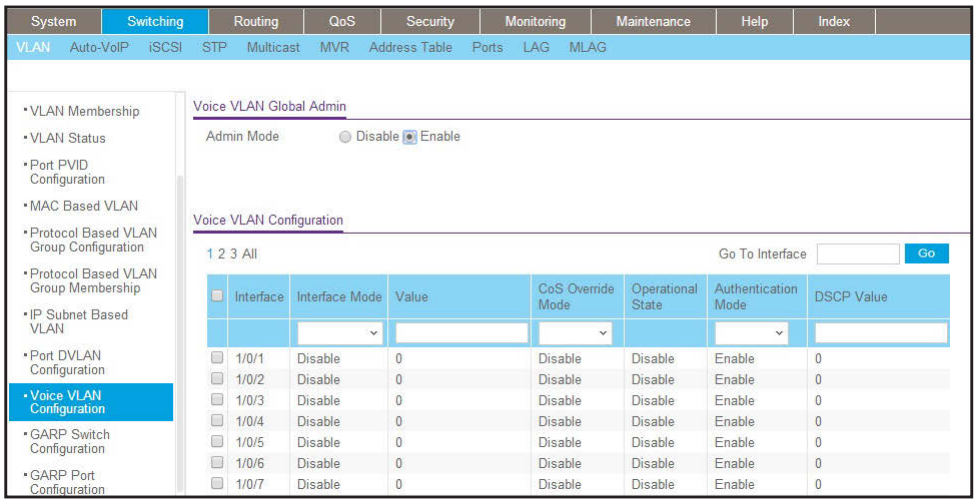
      A screen similar to the following displays.



   b. In the VLAN Membership table, in the **VLAN ID** list, select **10**.
   c. Select Port 1 and Port 2 as tagged.
   d. Click **Apply**.

3. Configure Voice VLAN globally.
   a. Select **Switching > VLAN > Advanced > Voice VLAN Configuration**.

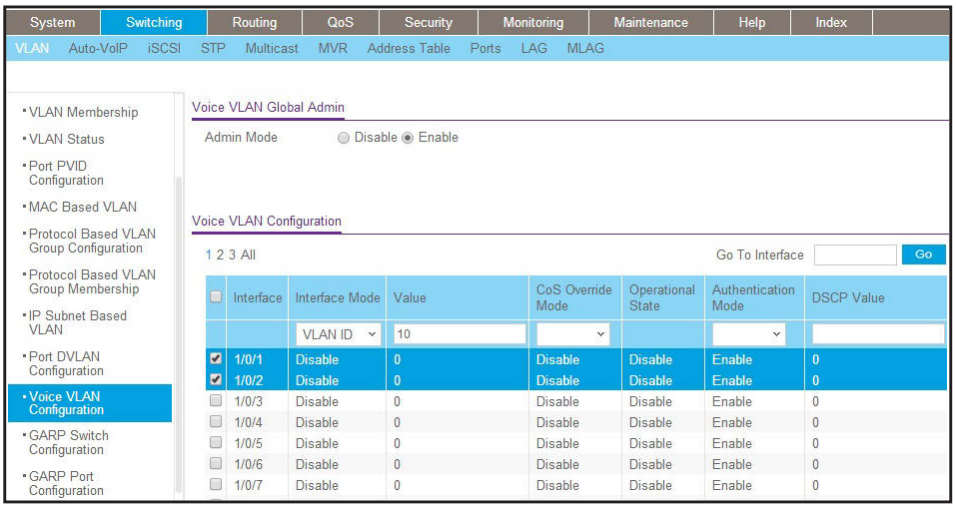
      A screen similar to the following displays.



   b. For Admin Mode, select the **Enable** radio button.
   c. Click **Apply**.

4. Configure Voice VLAN mode in the interface 1/0/2.
   a. Select **Switching > VLAN > Advanced > Voice VLAN Configuration**.
   b. Select the **1/0/2** check box.
   c. In the **Interface Mode** list, select **VLAN ID**.
   d. In the **Value** field, enter **10**.

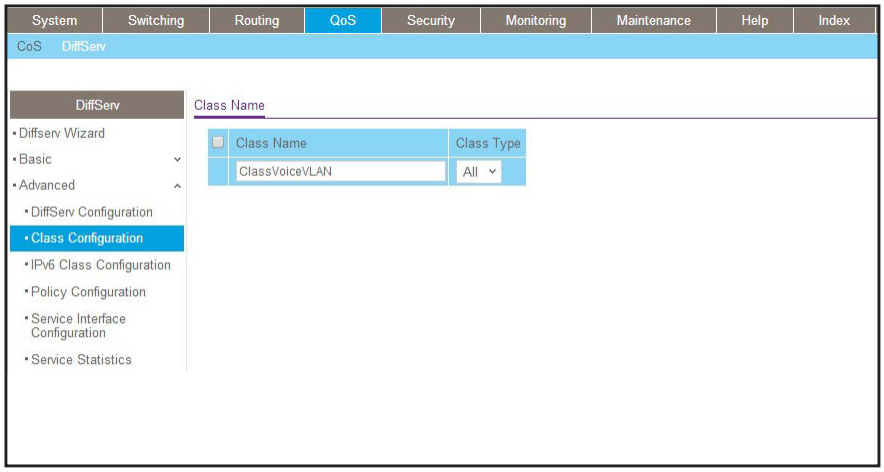
      A screen similar to the following displays.



   e. Click **Apply**.

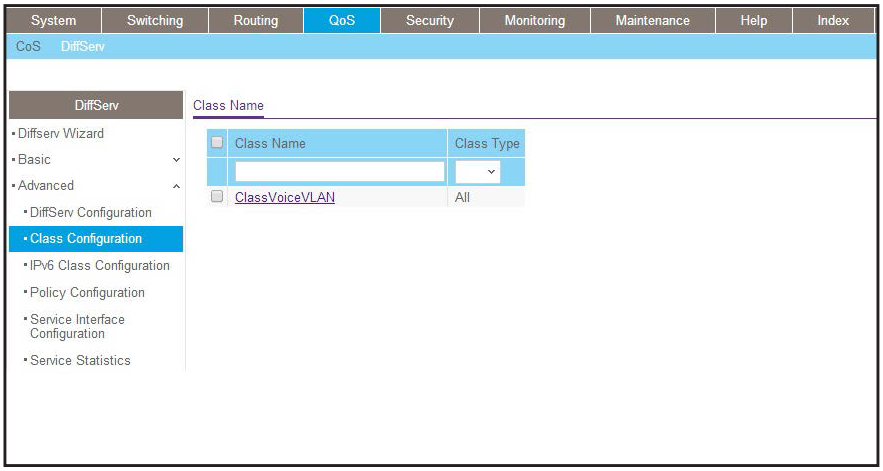
5. Create the DiffServ class ClassVoiceVLAN.
   a. Select **QoS > Advanced > DiffServ > Class Configuration**.

      A screen similar to the following displays.



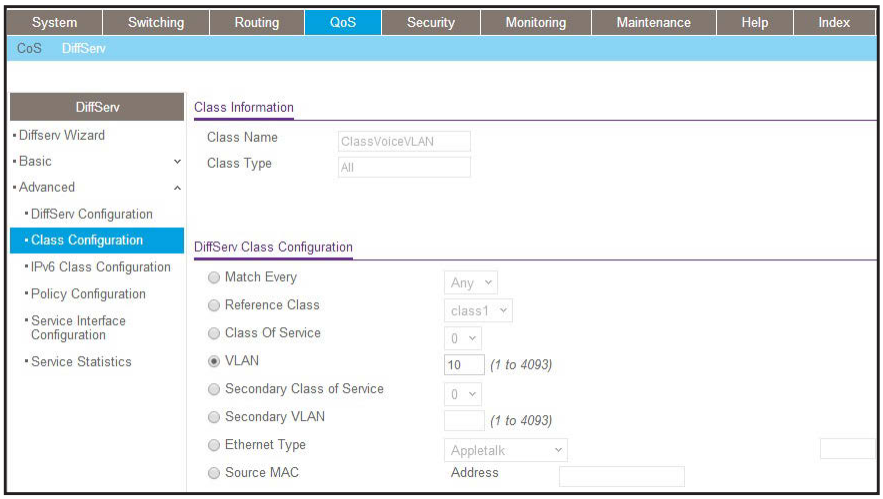
   b. In the **Class Name** field, enter **ClassVoiceVLAN**.
   c. In the **Class Type** list, select **All**.
   d. Click **Add**. The Class Name screen displays, as shown in the next step in this procedure.
6. Configure matching criteria for the class as **VLAN 10**.
   a. Select **QoS > DiffServ > Advanced > Class Configuration**.

      A screen similar to the following displays.



   b. Click the class **ClassVoiceVLAN**.
   c. In the DiffServ Class Configuration table, select **VLAN**.
   d. In the VLAN ID field, enter 10.

A screen similar to the following displays.

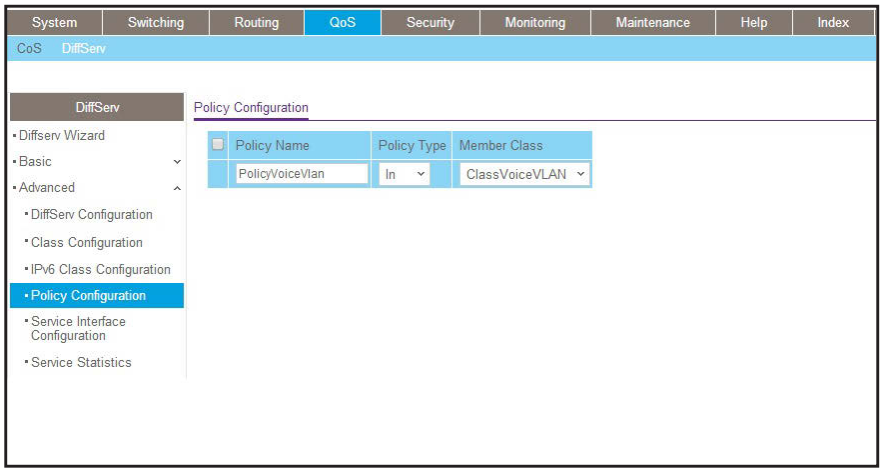


e. Click **Apply**.

7. Create the DiffServ policy PolicyVoiceVLAN.

a. Select **QoS > DiffServ > Advanced > Policy Configuration**.

A screen similar to the following displays.



b. In the **Policy Name** field, enter **PolicyVoiceVLAN**.

c. In the **Policy Type** list, select **In**.

d. In the **Member Class** list, select **ClassVoiceVLAN**.

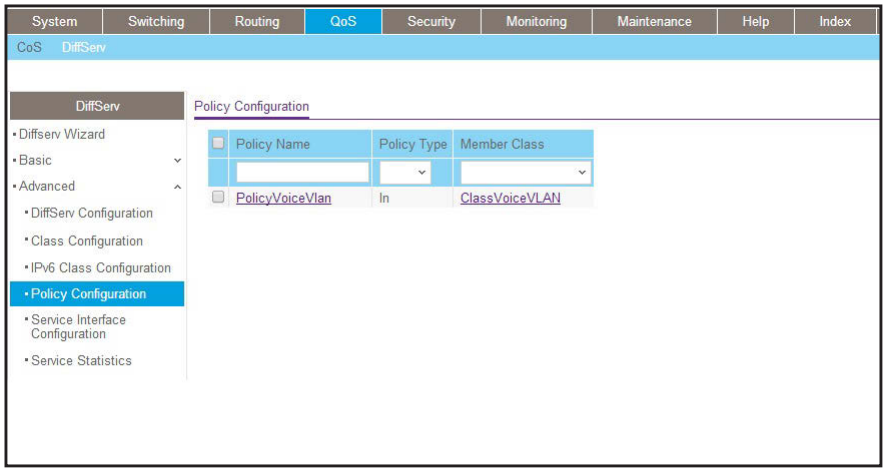
e. Click **Add**.

The Policy Configuration screen displays, as shown in the next step in this procedure.

8. Map the policy and class and assign them to the higher-priority queue.

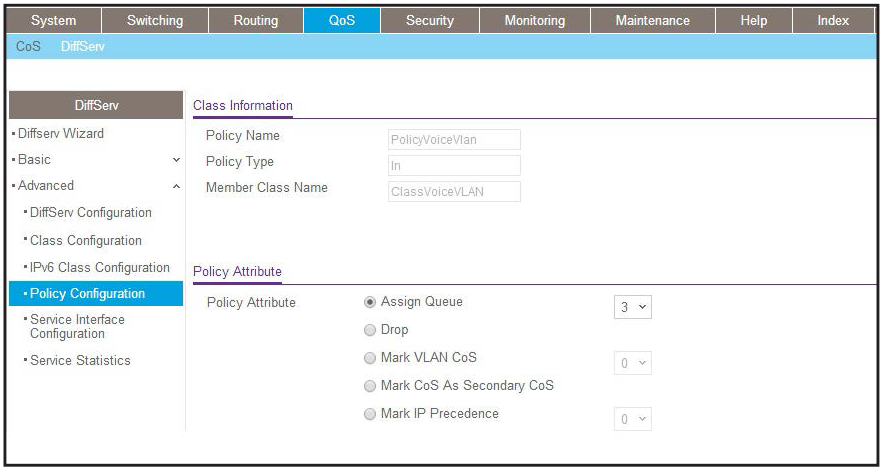
a. Select **QoS > DiffServ > Advanced > Policy Configuration**.

A screen similar to the following displays.



b. Click the **Policy PolicyVoiceVLAN**.

A screen similar to the following displays.



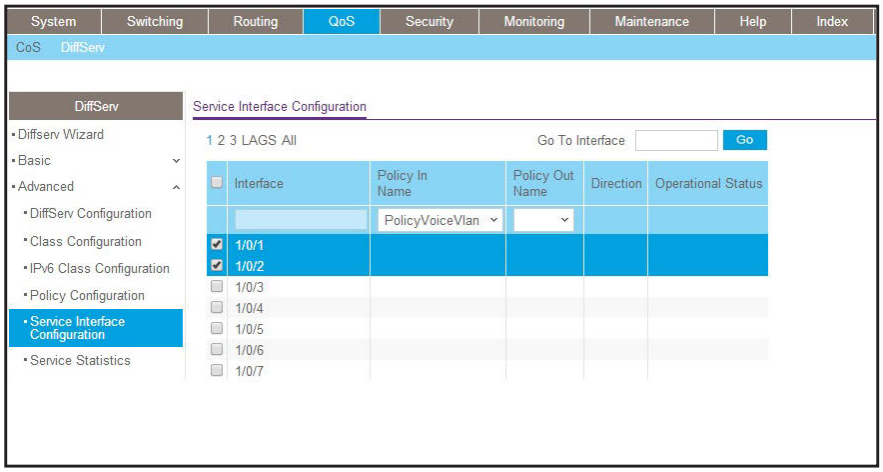
c. In the field next to the **Assign Queue** radio button, select **3**.

d. Click **Apply**.

9. Assign it to interfaces 1/0/1 and 1/0/2.

a. Select **QoS > DiffServ > Advanced > Service Interface Configuration**.

A screen similar to the following displays.



b. Select the check boxes for Interfaces **1/0/1** and **1/0/2**.

c. Set the **Policy Name** field as **PolicyVoiceVLAN**.

d. Click **Apply**.

Configure GARP VLAN Registration Protocol

Generic Attribute Registration Protocol (GARP) VLAN Registration Protocol (GVRP) provides IEEE 802.1Q-compliant VLAN pruning and dynamic VLAN creation on 802.1Q-tagged ports. With GVRP, a switch can exchange VLAN configuration information with other GVRP switches, prune unnecessary broadcast and unknown unicast traffic, and create and manage VLANs dynamically on switches that are connected through 802.1Q-tagged ports.

Figure 4. GVRP configuration

CLI: Enable GVRP

1. On Switch A, create VLANs 1000, 2000, and 3000, and add port 1/0/24 as a tagged port to VLANs 1000, 2000, and 3000.

```
(Netgear Switch) #vlan database
(Netgear Switch) (Vlan)#vlan 1000,2000,3000
(Netgear Switch) (Vlan)#exit
(Netgear Switch) #config
(Netgear Switch) (Config)#interface 1/0/24
(Netgear Switch) (Interface 1/0/24)#vlan participation include 1000
(Netgear Switch) (Interface 1/0/24)#vlan participation include 2000
(Netgear Switch) (Interface 1/0/24)#vlan participation include 3000
(Netgear Switch) (Interface 1/0/24)#vlan tagging 1000,2000,3000
```

2. On Switch A, enable GVRP.

```
(Netgear Switch) #set gvrp adminmode
(Netgear Switch) #config
(Netgear Switch) (Config)#interface 1/0/24
(Netgear Switch) (Interface 1/0/24)#set gvrp interfacemode
```

3. On Switch B, enable GVRP.

```
(Netgear Switch) #set gvrp adminmode
(Netgear Switch) #config
(Netgear Switch) (Config)#interface 1/0/11
(Netgear Switch) (Interface 1/0/11)#set gvrp interfacemode
```

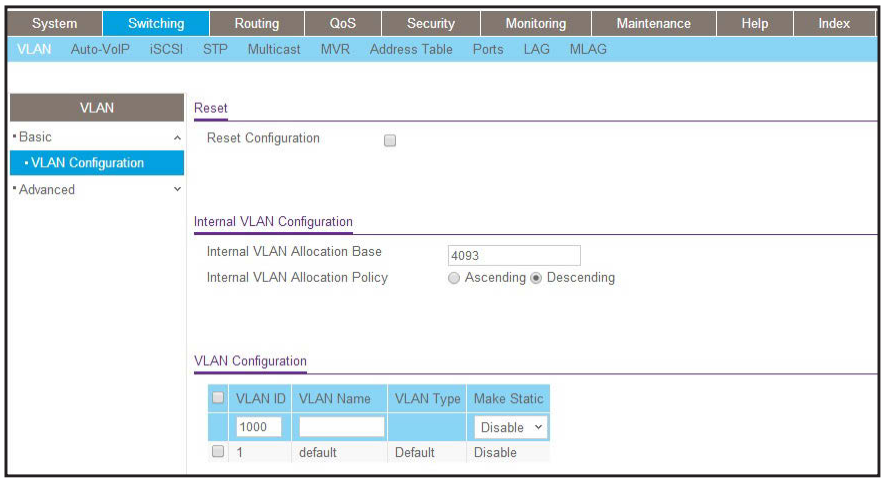
4. On Switch B, verify that VLANs 1000, 2000, and 3000 were created.

```
(Netgear Switch) #show vlan

Maximum VLAN Entries.......................... 1024
VLAN Entries Currently in Use................. 5

VLAN ID VLAN Name                         VLAN Type
------- --------------------------------- -------------------
1       default                            Default
2       Auto VoIP                          AUTO VoIP
1000                                       Dynamic (GVRP)
2000                                       Dynamic (GVRP)
3000                                       Dynamic (GVRP)
(Netgear Switch) #show vlan 1000

VLAN ID: 1000
VLAN Name:
VLAN Type: Dynamic (GVRP)
Interface   Current   Configured   Tagging
----------  --------  -----------  --------
1/0/1         Exclude   Autodetect   Untagged
1/0/2         Exclude   Autodetect   Untagged
1/0/3         Exclude   Autodetect   Untagged
1/0/4         Exclude   Autodetect   Untagged
1/0/5         Exclude   Autodetect   Untagged
1/0/6         Exclude   Autodetect   Untagged
1/0/7         Exclude   Autodetect   Untagged
1/0/8         Exclude   Autodetect   Untagged
1/0/9         Exclude   Autodetect   Untagged
1/0/10        Exclude   Autodetect   Untagged
1/0/11        Include   Autodetect   Tagged
1/0/12        Exclude   Autodetect   Untagged
1/0/13        Exclude   Autodetect   Untagged
1/0/14        Exclude   Autodetect   Untagged
1/0/15        Exclude   Autodetect   Untagged
1/0/16        Exclude   Autodetect   Untagged
```

Web Interface: Configure GVRP on switch A

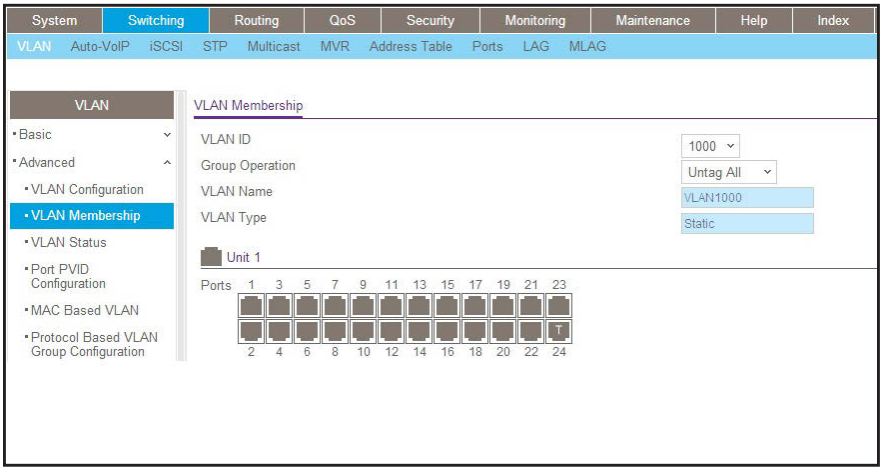
1. On Switch A, create VLANs 1000, 2000, and 3000:
   a. Select **Switching > VLAN > Advanced > VLAN Configuration**.

      A screen similar to the following displays.



   b. In the VLAN ID field, enter **1000**.
   c. Click **Add**.
   d. Repeat *Step a* through *Step c* to create VLANs 2000 and 3000.
2. Add port 1/0/24 as a tagged port to VLANs 1000, 2000, and 3000:
   a. Select **Switching > VLAN > Advanced > VLAN Membership**.

      A screen similar to the following displays.



   a. From the VLAN ID menu, select **1000**.
   b. Click **Unit 1**.

      The ports display.

   c. Click the gray box under port **24** until **T** displays.

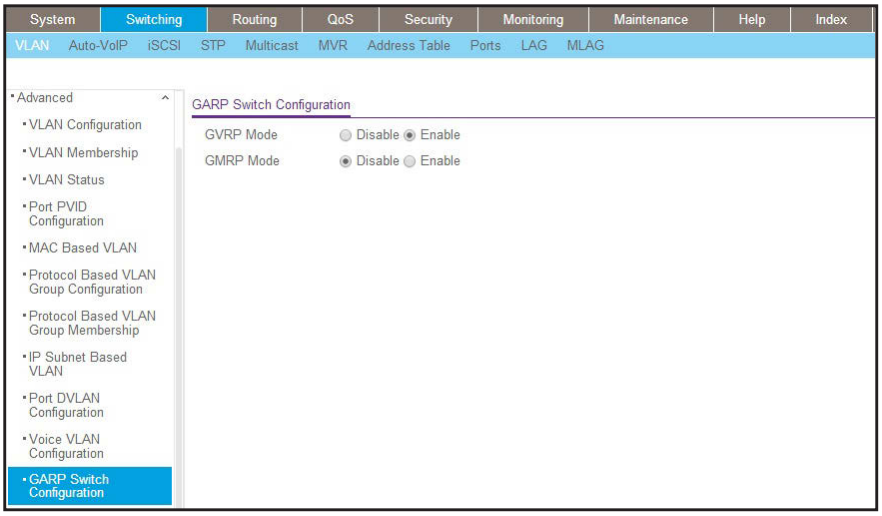
T specifies that the switch tags egress packets for port 24.

d. Click **Apply**.

3. Enable GVRP globally:

a. Select **Switching > VLAN > Advanced > GARP Switch Configuration**.

A screen similar to the following displays.



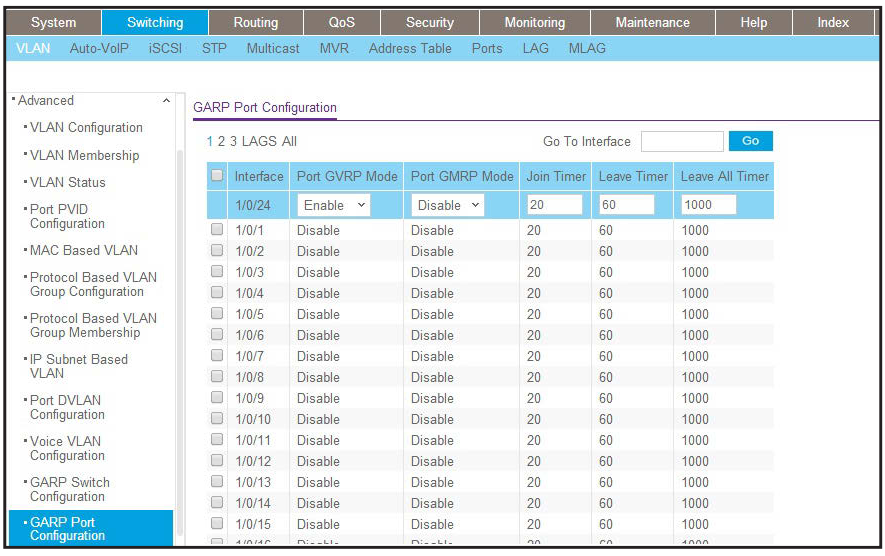
b. Next to GVRP Mode, select the **Enable** radio button.

c. Click **Apply**.

4. Enable GVRP on port 1/0/24.

a. Select **Switching > VLAN > Advanced > GARP Port Configuration**.

A screen similar to the following displays.



b. Scroll down and select the check box that corresponds to interface 1/0/24.

The Interface field in the table heading displays 1/0/24.

c. From the Port GVRP Mode menu, select **Enable**.

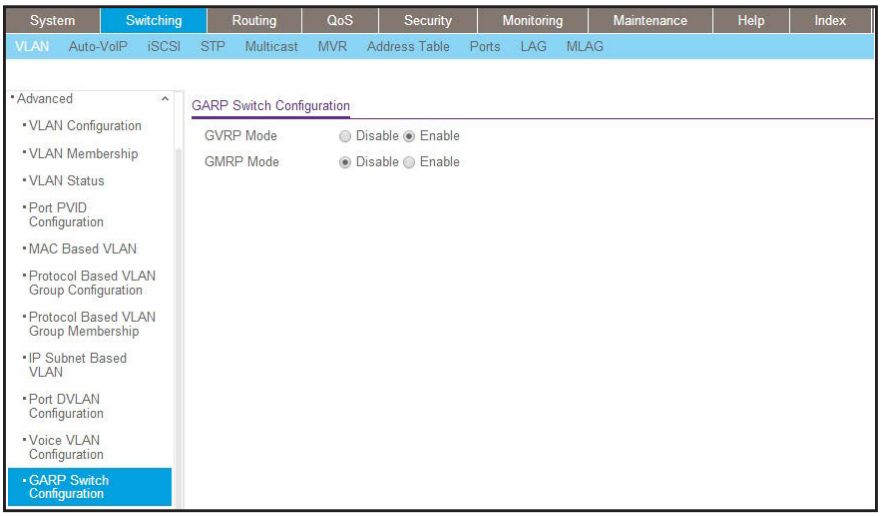
d. Click **Apply**.

Web Interface: Configure GVRP on Switch B

1. Enable GVRP globally:

   a. Select **Switching > VLAN > Advanced > GARP Switch Configuration**.

   A screen similar to the following displays.



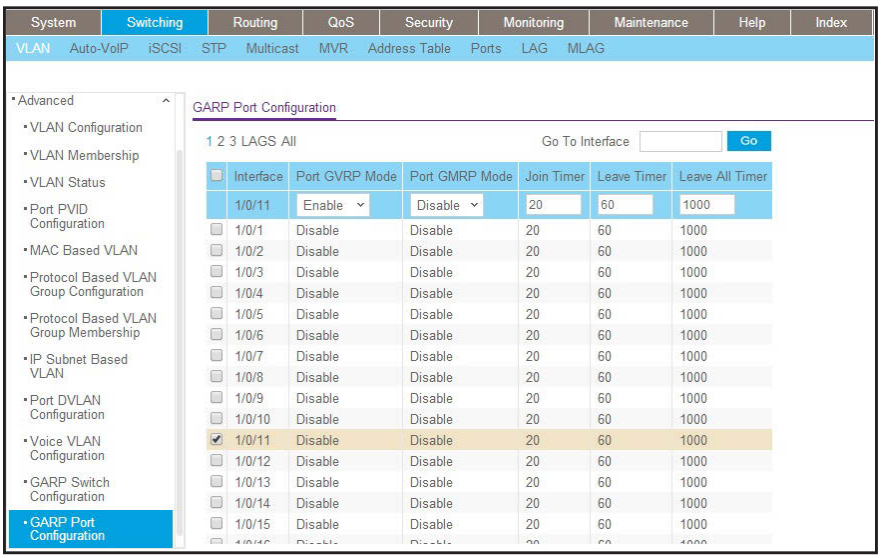
   b. Next to GVRP Mode, select the **Enable** radio button.

   c. Click **Apply**.

2. Enable GVRP on port 1/0/11:

   a. Select **Switching > VLAN > Advanced > GARP Port Configuration**.

   A screen similar to the following displays.



b. Scroll down and select the check box that corresponds to interface 1/0/11.

   The Interface field in the table heading displays 1/0/11.

c. From the Port GVRP Mode menu, select **Enable**.

d. Click **Apply**.

Private VLANs

The Private VLANs feature separates a regular VLAN domain into two or more subdomains. Each subdomain is defined (represented) by a primary VLAN and a secondary VLAN. The primary VLAN ID is the same for all subdomains that belong to a private VLAN. The secondary VLAN ID differentiates subdomains from each other and provides Layer 2 isolation between ports of the same private VLAN.

There are three types of VLAN within a private VLAN:

- **Primary VLAN**. it forwards the traffic from the promiscuous ports to isolated ports, community ports, and other promiscuous ports in the same private VLAN. Only one primary VLAN can be configured per private VLAN. All ports within a private VLAN share the same primary VLAN.
- **Community VLAN**. is a secondary VLAN. It forwards traffic between ports which belong to the same community and to the promiscuous ports. There can be multiple community VLANs per private VLAN.
- **Isolated VLAN**. is a secondary VLAN. It carries traffic from isolated ports to promiscuous ports. Only one isolated VLAN can be configured per private VLAN.

There are three types of port designation within a private VLAN:

- **Promiscuous port**. belongs to a primary VLAN and can communicate with all interfaces in the private VLAN, including other promiscuous ports, community ports, and isolated ports.
- **Community ports**. These ports can communicate with other community ports and promiscuous ports.
- **Isolated ports**. These can ONLY communicate with promiscuous ports.

The following figure shows how private VLANs can be extended across multiple switches through inter-switch/stack links that transport primary, community, and isolated VLANs between devices.

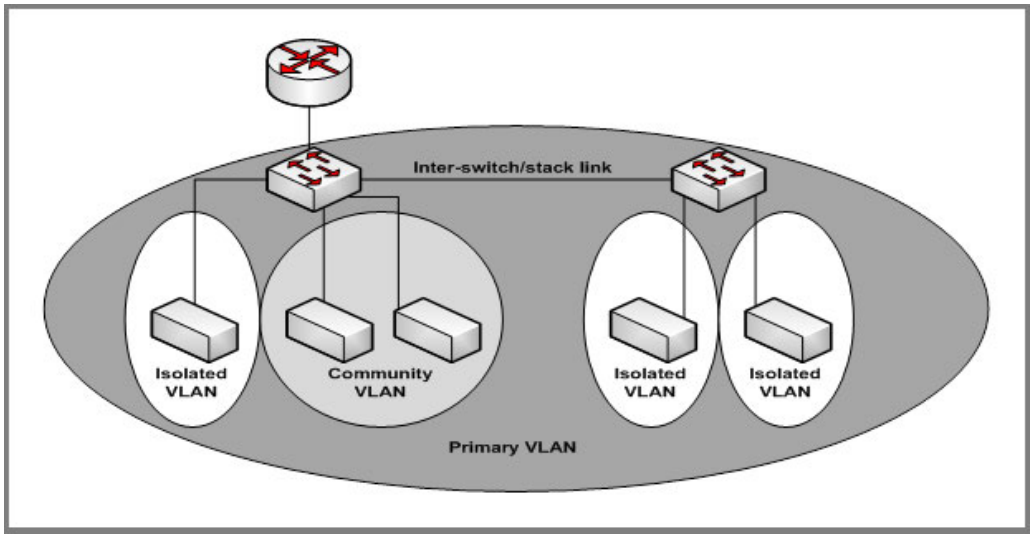


Figure 5. Private VLANs

The following figure illustrates the private VLAN traffic flow. Five ports A, B, C, D, and E make up a private VLAN. Port A is a promiscuous port which is associated with the primary VLAN 100. Ports B and C are the host ports which belong to the isolated VLAN 101. Ports D and E are the community ports which are associated with community VLAN 102. Port F is the inter-switch/stack link. It is configured to transmit VLANs 100, 101 and 102. Colored arrows represent possible packet flow paths in the private VLAN domain.

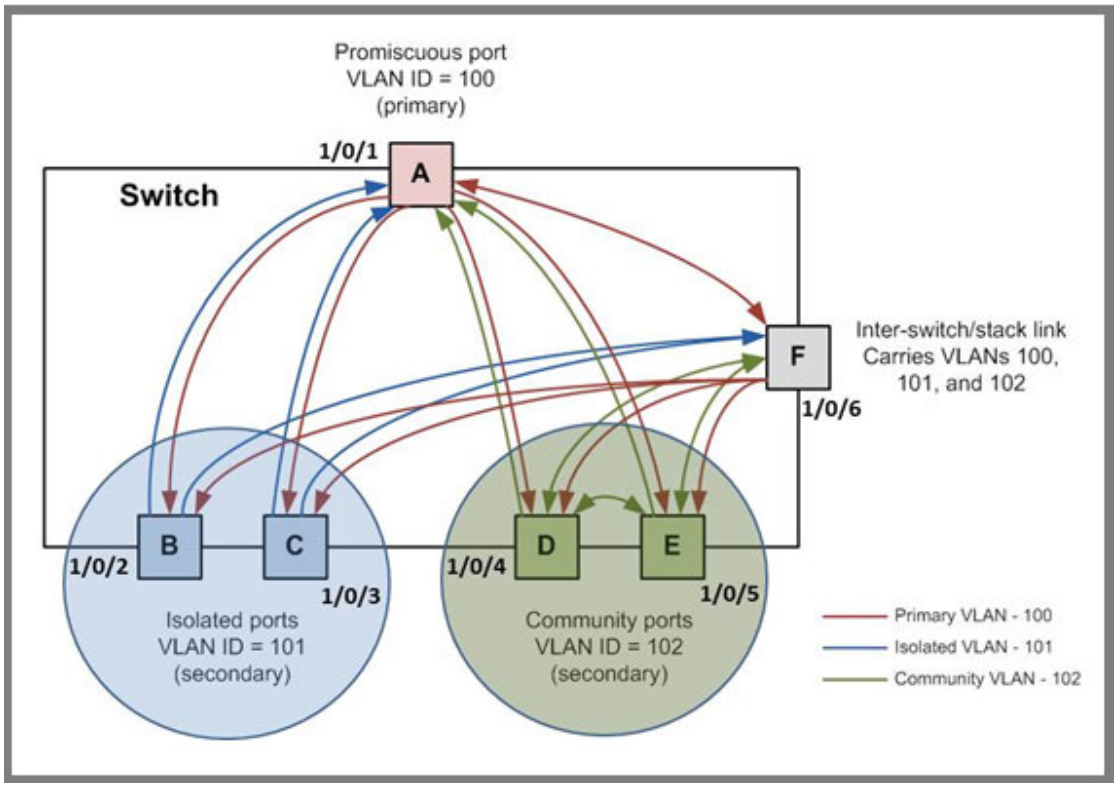


Figure 6. Packet flow within a Private VLAN domain

Assign Private-VLAN Types (Primary, Isolated, Community)

The example is shown as CLI commands and as a web interface procedure.

CLI: Assign Private-VLAN Type (Primary, Isolated, Community)

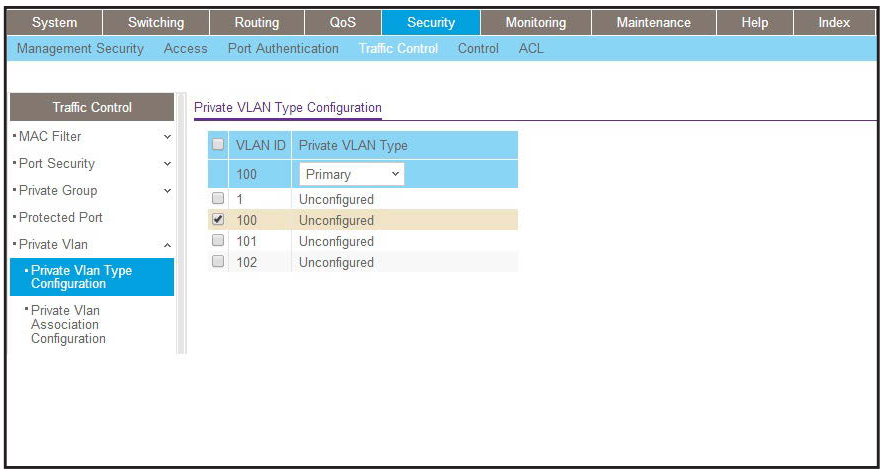
Use the following commands to assign VLAN 100 to primary VLAN, VLAN 101 to isolated VLAN, and VLAN 102 to community VLAN.

```
(Netgear Switch) #config
(Netgear Switch) (Config)#vlan 100
(Netgear Switch) (Config)(Vlan) #private-vlan primary
(Netgear Switch) (Config)(Vlan) #exit
(Netgear Switch) (Config)#vlan 101
(Netgear Switch) (Config)(Vlan) #private-vlan isolated
(Netgear Switch) (Config)(Vlan) #exit
(Netgear Switch) (Config)#vlan 102
(Netgear Switch) (Config)(Vlan) #private-vlan community
(Netgear Switch) (Config)(Vlan) #end
```

Web Interface: Assign Private-VLAN Type (Primary, Isolated, Community)

1. Create VLAN 10.
   a. Select **Security** > **Traffic Control** > **Private VLAN** > **Private VLAN Type Configuration**.

      A screen similar to the following displays.



b. Under **Private VLAN Type Configuration**, select the **VLAN ID 100** check box. Now 100 appears in the interface field at the top.

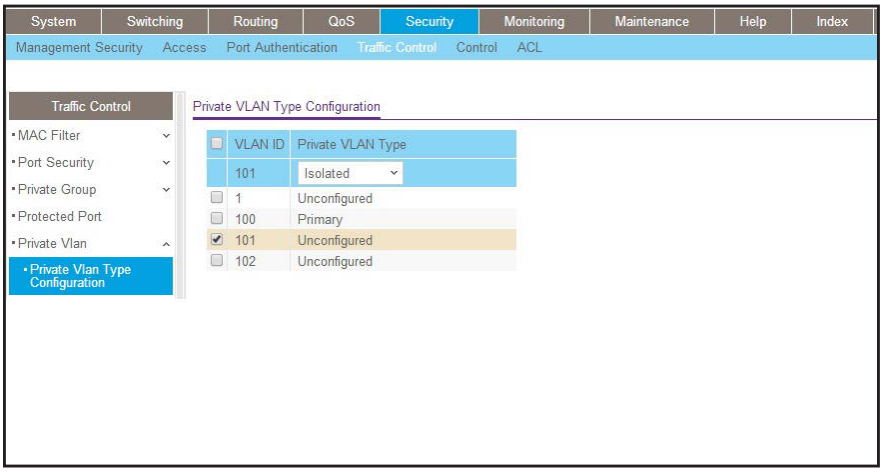
c. In the **Private VLAN Type** field, select **Primary** from the menu.

d. Click **Apply** to save the settings

2. Assign VLAN 101 as an isolated VLAN.

a. Select **Security** > **Traffic Control** > **Private VLAN** > **Private VLAN Type Configuration**.

A screen similar to the following displays.



b. Under **Private VLAN Type Configuration**, select the **VLAN ID 101** check box.

Now 101 appears in the interface field at the top.

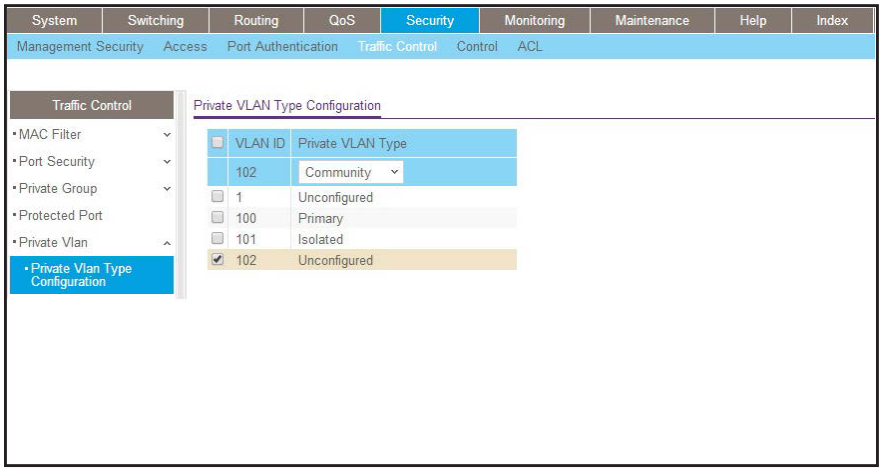
c. In the **Private VLAN Type** field, select **Isolated** from the menu.

d. Click **Apply** to save the settings

3. Assign VLAN 102 to community VLAN.

a. Select **Security** > **Traffic Control** > **Private VLAN** > **Private VLAN Type Configuration**.

A screen similar to the following displays.



b. Under **Private VLAN Type Configuration**, select the **VLAN ID 102** check box. Now 102 appears in the interface field at the top.

c. In the **Private VLAN Type** field, select **Community** from the menu.

d. Click **Apply** to save the settings.

Configure Private-VLAN Association

The example is shown as CLI commands and as a web interface procedure.

CLI: Configure Private-VLAN Association

Use the following commands to associate VLAN 101-102 (secondary VLAN) to VLAN 100 (primary VLAN).

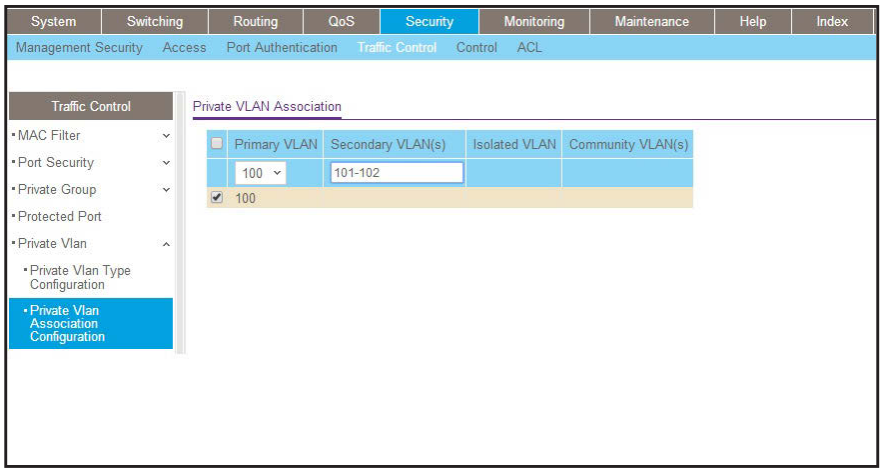
```
(Netgear Switch)  #config
(Netgear Switch)  (Config)#vlan 100
(Netgear Switch)  (Config)(Vlan) #private-vlan association 101-102
(Netgear Switch)  (Config)(Vlan) #end
```

Web Interface: Configure Private-VLAN Association

1. Associate VLAN 101-102 (secondary VLAN) to VLAN 100 (primary VLAN).

   a. Select **Security** > **Traffic Control** > **Private VLAN** > **Private VLAN Association Configuration**.

   A screen similar to the following displays.



   b. Under **Private VLAN Association Configuration**, select the VLAN ID 100.

   c. In the **Secondary VLAN(s)** field, type 101-102.

   d. Click **Apply** to save the settings.

Configure Private-VLAN Port Mode (Promiscuous, Host)

The example is shown as CLI commands and as a web interface procedure.

CLI: Configure Private-VLAN Port Mode (Promiscuous, Host)

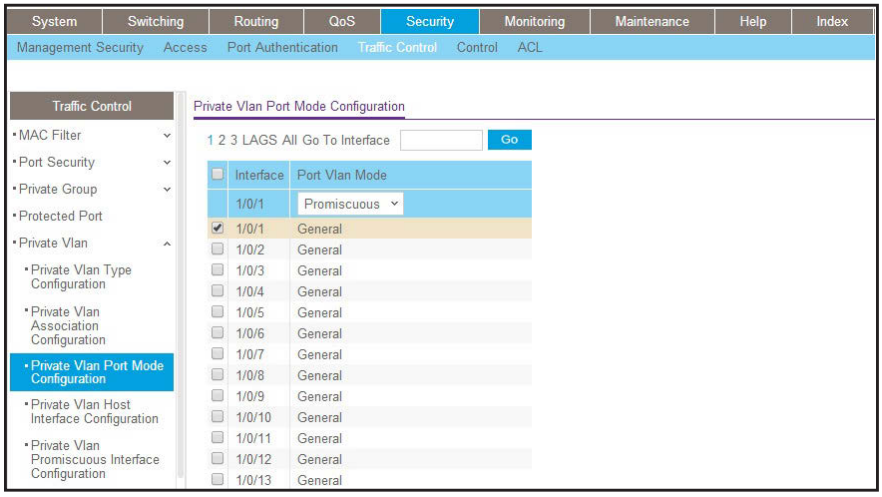
Use the following commands to assign port 1/0/1 to promiscuous port mode and ports 1/0/2-1/0/5 to host port mode.

```
(Netgear Switch)  #config
(Netgear Switch)  (Config)#interface 1/0/1
(Netgear Switch)  (Interface 1/0/1)#switchport mode private-vlan promiscuous
(Netgear Switch)  (Interface 1/0/1)#exit
(Netgear Switch)  (Config)#interface 1/0/2-1/0/5
(Netgear Switch)  (Interface 1/0/2-1/0/5)#switchport mode private-vlan host
(Netgear Switch)  (Interface 1/0/2-1/0/5)#end
```

Web Interface: Configure Private-VLAN Port Mode (Promiscuous, Host)

1. Configure port 1/0/1 to promiscuous port mode.
   a. Select **Security** > **Traffic Control** > **Private VLAN** > **Private VLAN Port Mode Configuration**.

      A screen similar to the following displays.



   b. Under **Private VLAN Port Mode Configuration**, select the 1/0/1 interface check box.

      Now 1/0/1 appears in the **Interface** field at the top.

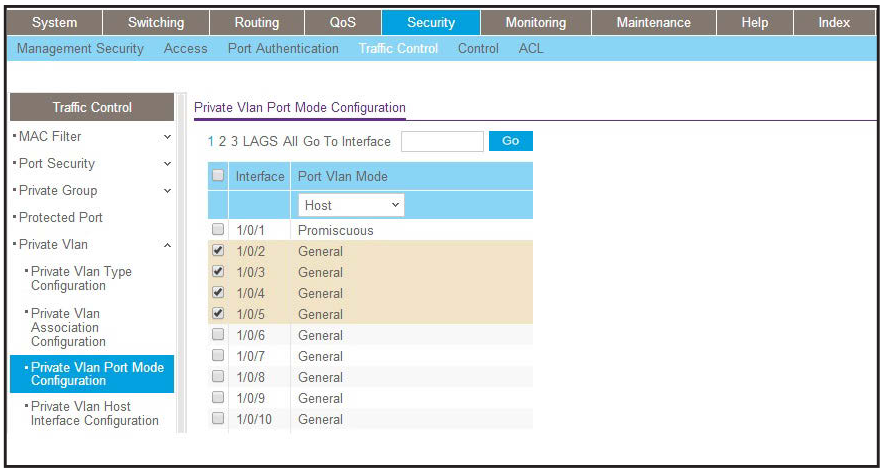
   c. In the **Port VLAN Mode** field, select **Promiscuous** from the menu.

d. Click **Apply** to save the settings.

2. Configure ports 1/0/2-1/0/5 to host port mode.

a. Select **Security** > **Traffic Control** > **Private VLAN** > **Private VLAN Port Mode Configuration**.

A screen similar to the following displays.



b. Under **Private VLAN Port Mode Configuration**, select the 1/0/2 to 1/0/5 interface check box.

c. In the **Port VLAN Mode** field, select Host from the menu.

d. Click **Apply** to save the settings.

Configure Private-VLAN Host Ports

The example is shown as CLI commands and as a web interface procedure.

CLI: Configure Private-VLAN Host Ports

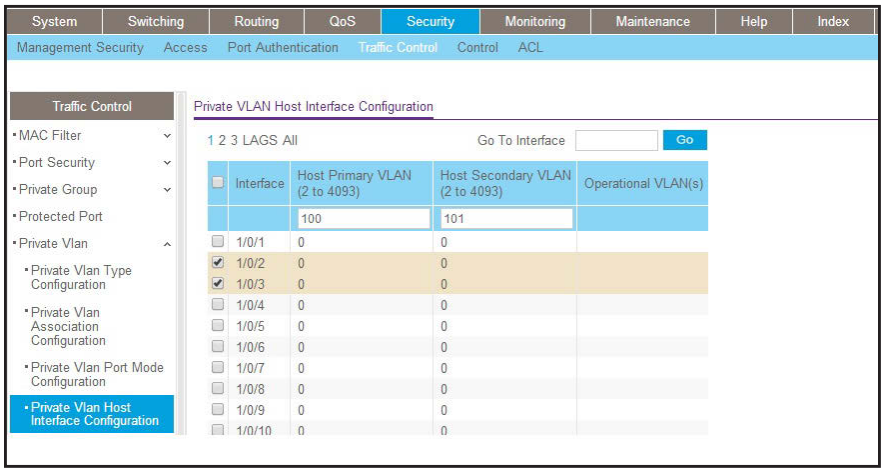
Use the following commands to associate isolated ports 1/0/2-1/0/3 to a private-VLAN (primary=100, secondary=101). Community ports 1/0/4-1/0/5 to a private-VLAN (primary= 100, secondary=102).

```
(Netgear Switch)  #config
(Netgear Switch)  (Config)#interface 1/0/2-1/0/3
(Netgear Switch)  (Interface 1/0/2-1/0/3)#switchport private-vlan host-association
100 101
(Netgear Switch)  (Interface 1/0/2-1/0/3)#exit
(Netgear Switch)  (Config)#interface 1/0/4-1/0/5
(Netgear Switch)  (Interface 1/0/4-1/0/5)#switchport private-vlan host-association
100 102
(Netgear Switch)  (Interface 1/0/4-1/0/5)#end
```

Web Interface: Assign Private-VLAN Port Host Ports

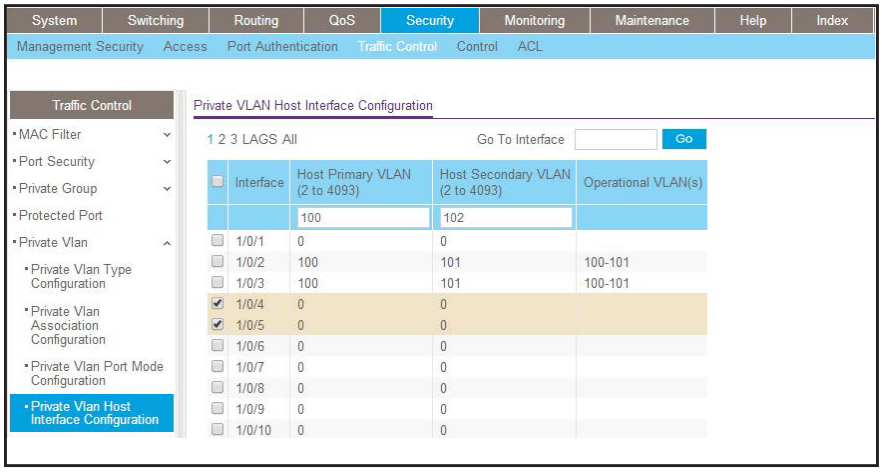
1. Associate isolated ports 1/0/2-1/0/3 to a private-VLAN (primary=100, secondary=101).
   a. Select **Security** > **Traffic Control** > **Private VLAN** > **Private VLAN Host Interface Configuration**.

      A screen similar to the following displays.



   b. Under **Private VLAN Host Interface Configuration**, select the 1/0/2 and 1/0/3 interface check box.
   c. In the **Host Primary VLAN** field, enter 100.
   d. In the **Host Secondary VLAN** field, enter 101.
   e. Click **Apply** to save the settings.
2. Associate isolated ports 1/0/4-1/0/5 to a private-VLAN (primary=100, secondary=102).
   a. Select **Security** > **Traffic Control** > **Private VLAN** > **Private VLAN Host Interface Configuration**.

      A screen similar to the following displays.



   b. Under **Private VLAN Host Interface Configuration**, select the 1/0/4 and 1/0/5 interface check box.

c. In the **Host Primary VLAN** field, enter 100.
d. In the **Host Secondary VLAN** field, enter 102.
e. Click **Apply** to save the settings.

Map Private-VLAN Promiscuous Port

The example is shown as CLI commands and as a web interface procedure.

CLI: Map Private-VLAN Promiscuous Port

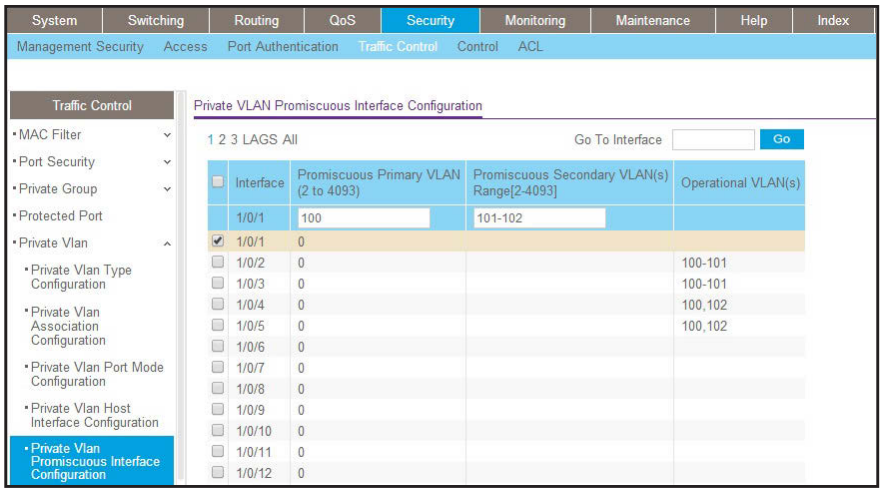
Use the following commands to map private-VLAN promiscuous port 1/0/1 to a primary VLAN (100) and to secondary VLANs (101-102).

```
(Netgear Switch)  #config
(Netgear Switch)  (Config)#interface 1/0/1
(Netgear Switch)  (Interface 1/0/1)#switchport private-vlan mapping 100 101-102
(Netgear Switch)  (Interface 1/0/1)#end
```

Web Interface: Map Private-VLAN Promiscuous Port

1. Map private-VLAN promiscuous port 1/0/1 to a primary VLAN (100) and to selected secondary VLANs (101-102).
   a. Select **Security** > **Traffic Control** > **Private VLAN** > **Private VLAN Promiscuous Interface Configuration**.

      A screen similar to the following displays.



   b. Under **Private VLAN Promiscuous Interface Configuration**, select the 1/0/1 interface check box. Now 1/0/1 appears in the **Interface** field at the top.
   c. In the **Promiscuous Primary VLAN** field, enter 100.

d. In the **Promiscuous Secondary VLAN** field, enter 101-102.
e. Click **Apply** to save the settings

VLAN Access Ports and Trunk Ports

Using switch ports can minimize potential configuration errors. Switch ports also facilitate the configuration of a VLAN by reducing the number of commands that you must enter. To configure a port that is connected to an end user, use a switch port in access mode. To configure a port that is connected to another switch, use a switch port in trunk mode.

In addition, to access mode and trunk mode, you can configure switch ports in general mode, which is the default mode and does not restrict the configuration so you can configure the port as needed.

The switch supports the following switch port modes, each with its own VLAN membership rules:

- **Access mode**. In access mode, the following rules apply to switch ports:
  - Ports belong to a single VLAN, for which the VID is the configured PVID.
  - Ports are intended for end-point connections, which, in general, do not operate with LANs and operate with tagged traffic.
  - Ports accept both tagged and untagged traffic. (You cannot configurable whether the ports accepts tagged or untagged traffic.)
  - All egress traffic must be sent untagged.
  - Ingress filtering is always enabled.
  - Ports are intended for connecting end stations to the switch, especially when end stations are incapable of generating VLAN tags.
- **Trunk mode**. In trunk mode, the following rules apply to switch ports:
  - Ports can belong to as many VLANs as needed.
  - Ports accept both incoming tagged and untagged traffic.
  - All incoming untagged frames are tagged with the native VLAN as the VID.
  - Egress frames are sent tagged for all VLANs other than the native VLAN. Frames that belong to the native VLAN are sent without a VLAN tag.
  - Ingress filtering is always enabled. If incoming frames are tagged correctly (that is, tagged with a VID of one of the VLANs to which the port belongs), they are admitted.
  - Ports are intended for connections between switches, for which the traffic is generally tagged.
  - If you configure a list with allowed VLANs, a trunk port becomes a member of VLANs that are defined in the list with allowed VLANs.
- **General mode**. In general mode, the following rules apply to switch ports:
  - By default, all ports are designated as general mode ports and belong to the default VLAN.
  - Ports conform to NETGEAR legacy switch behavior for switch ports.

- You configure various VLAN parameters such as membership, tagging, and PVID by using legacy commands.
- You can enable or disable ingress filtering.

The following figure shows a configuration with access ports and a trunk port.

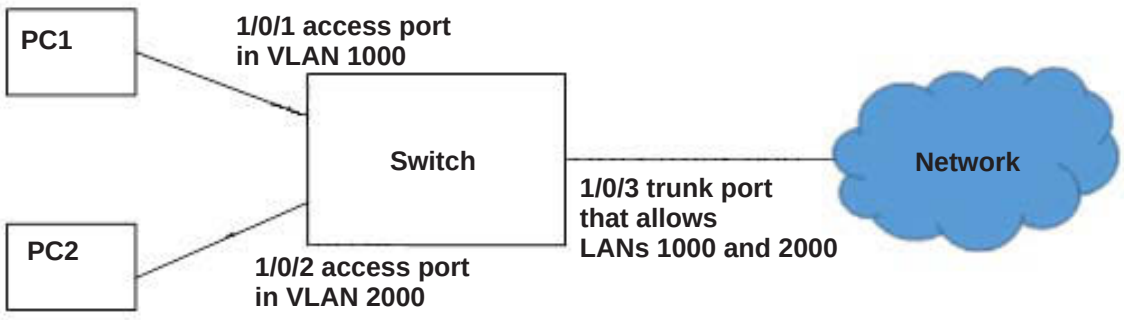


Figure 7. Access and trunk ports

CLI: Configure a VLAN Trunk

1. Create VLAN 1000 and 2000.

```
(Netgear Switch) #vlan database
(Netgear Switch) (Vlan)#vlan 1000
(Netgear Switch) (Vlan)#vlan 2000
(Netgear Switch) (Vlan)#exit
```

2. Configure port 1/0/1 as an access port.

```
(Netgear Switch) #config
(Netgear Switch) (Config)#interface 1/0/1
(Netgear Switch) (Interface 1/0/1)#switchport mode access
(Netgear Switch) (Interface 1/0/1)#switchport access vlan 1000
(Netgear Switch) (Interface 1/0/1)#exit
(Netgear Switch) (Config)#
```

3. Configure port 1/0/2 as an access port.

```
(Netgear Switch) #config
(Netgear Switch) (Config)#interface 1/0/2
(Netgear Switch) (Interface 1/0/2)#switchport mode access
(Netgear Switch) (Interface 1/0/2)#switchport access vlan 2000
(Netgear Switch) (Interface 1/0/2)#exit
(Netgear Switch) (Config)#
```

4. Configure port 1/0/3 as a trunk port.

```
(Netgear Switch) (Interface 1/0/3)#switchport mode trunk
(Netgear Switch) (Interface 1/0/3)#switchport trunk allowed vlan 1000,2000
```

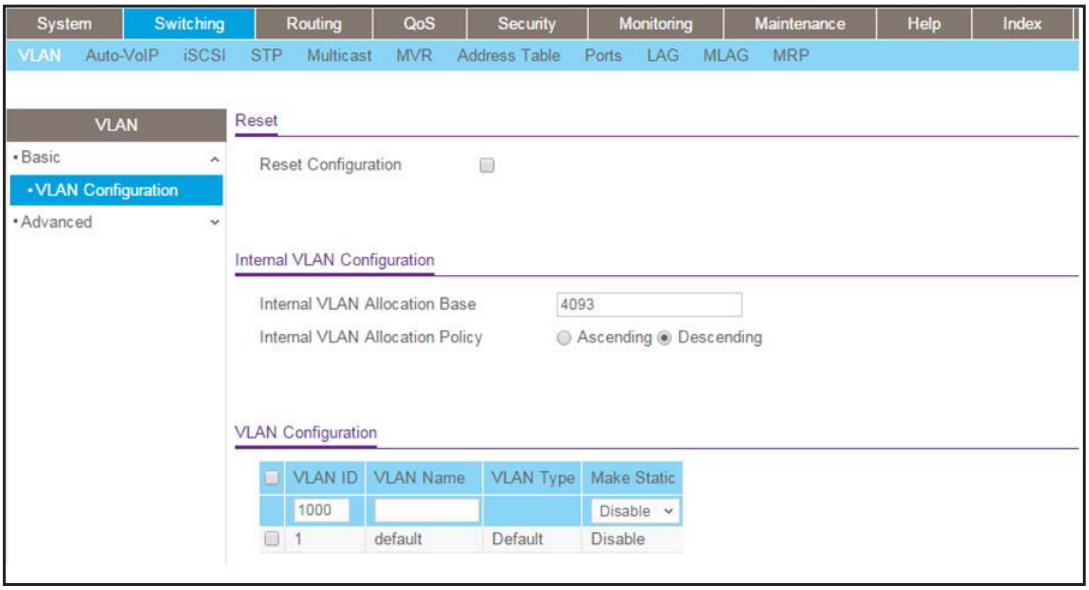
5. Configure all incoming untagged packets to be tagged with the native VLAN ID.

```
(Netgear Switch) (Interface 1/0/3)#switchport trunk native vlan 1000
```

Web Interface: Configure a VLAN Trunk

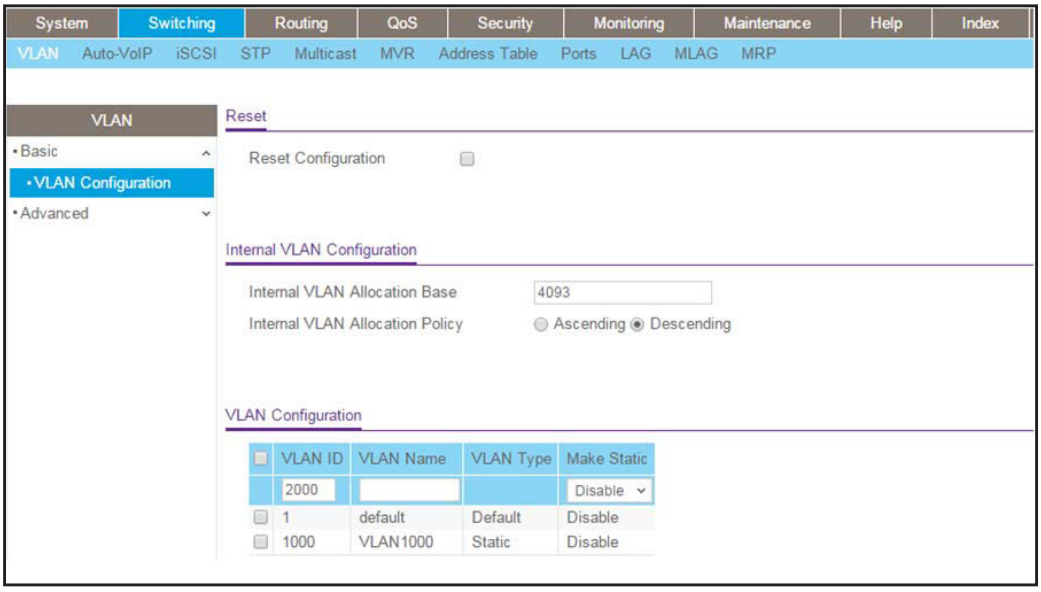
1. Create VLAN 1000
   a. Select **Switching > VLAN > Advanced > VLAN Configuration**.

      A screen similar to the following displays.



   b. In the **VLAN ID** field, enter **1000**.
   c. Click **Add**.

A screen similar to the following displays.



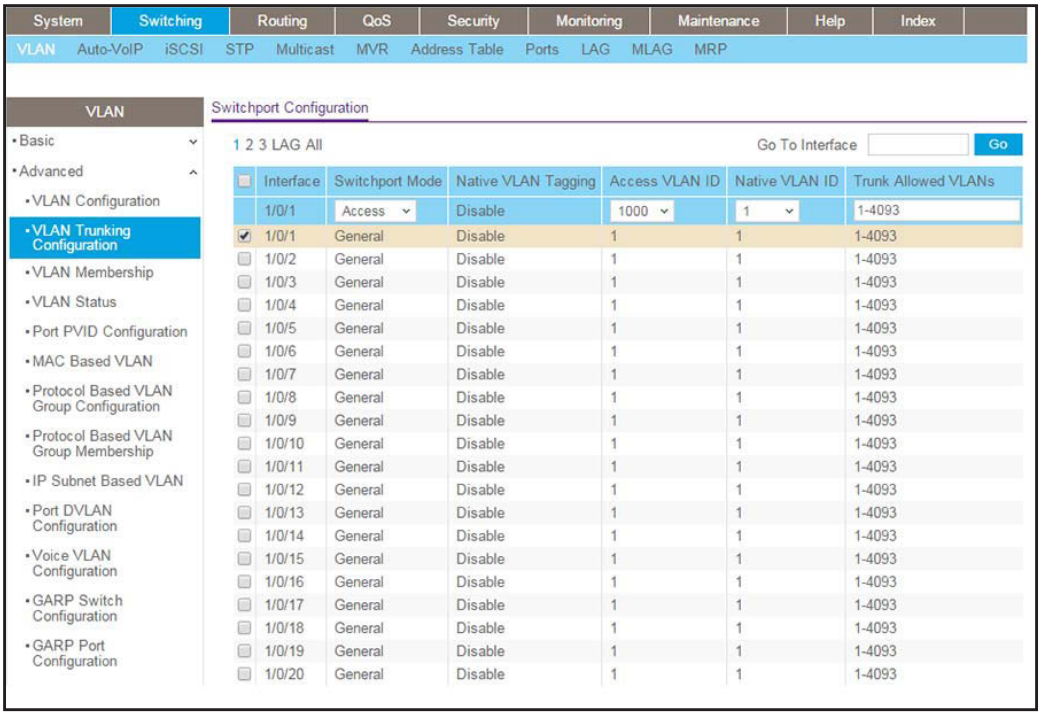
d. In the **VLAN ID** field, enter **2000**.

e. Click **Add**.

2. Configure port 1/0/1 as an access port in VLAN 1000.

a. Select Switching > VLAN > Advanced > VLAN Trunking Configuration.

A screen similar to the following displays.



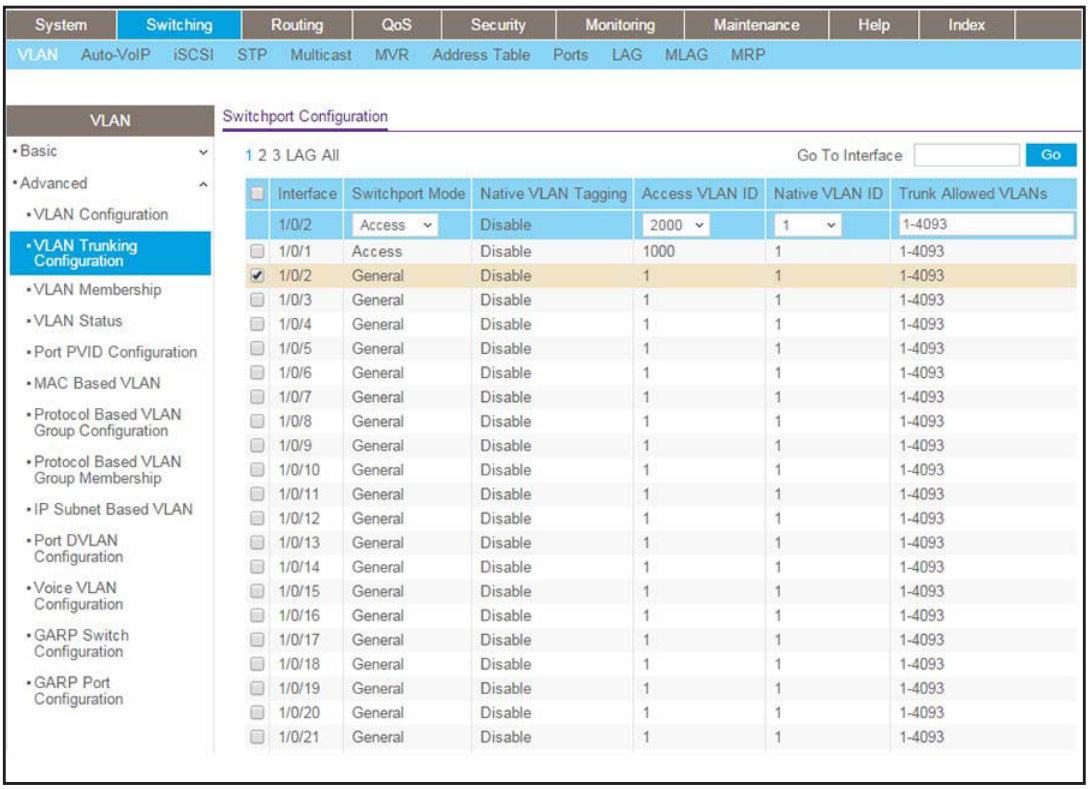
b. Select the check box that corresponds to interface 1/0/1.

The **Interface** field in the table heading displays 1/0/1.

c. In the **Switchport Mode** field, select **Access**.
d. In the **Access VLAN ID** field, select **1000**.
e. Click **Apply**.

3. Configure port 1/0/2 as an access port in VLAN 2000.
   a. **Select Switching > VLAN > Advanced > VLAN Trunking Configuration**.

   A screen similar to the following displays.



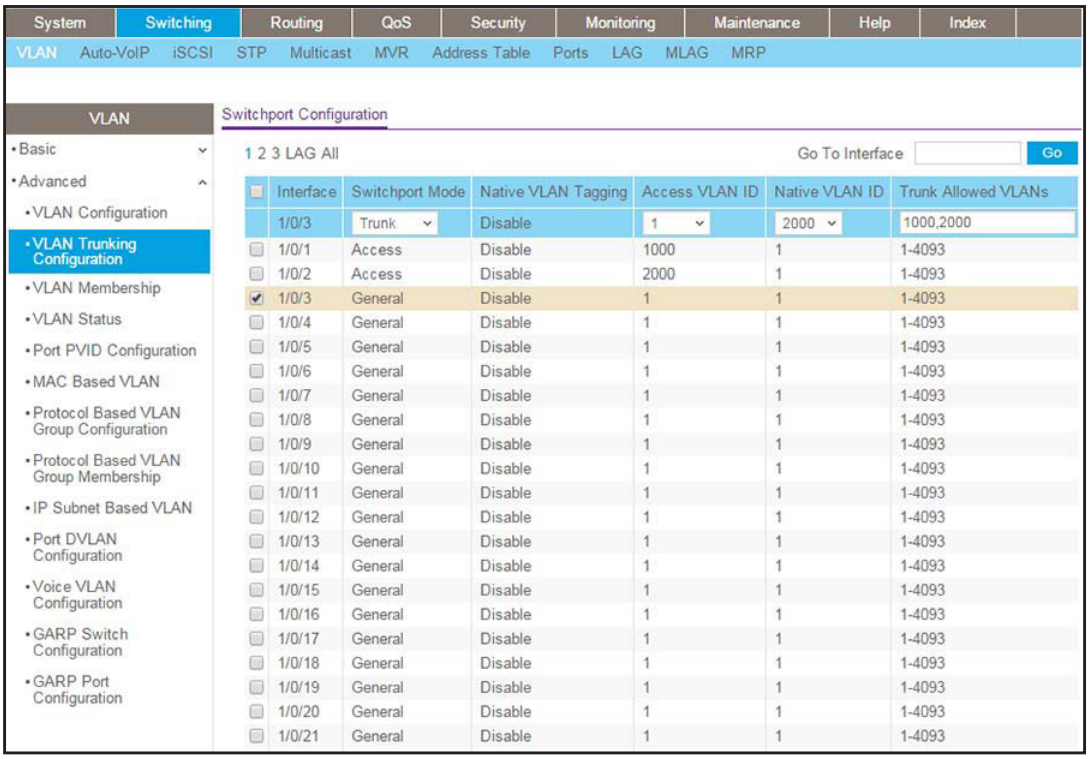
   b. Select the check box that corresponds to interface 1/0/2.

      The **Interface** field in the table heading displays 1/0/2.

   c. In the **Switchport Mode** field, select **Access**.
   d. In the **Access VLAN ID** field, select **2000**.
   e. Click **Apply**.

4. Configure port 1/0/3 as a trunk port that allows VLANs 1000 and 2000.
   a. **Select Switching > VLAN > Advanced > VLAN Trunking Configuration**.

   A screen similar to the following displays.



b. Select the check box that corresponds to interface 1/0/3.

The **Interface** field in the table heading displays 1/0/3.

c. In the **Switchport Mode** field, select **Trunk**.

d. In the **Native VLAN ID** field, select **2000**.

Note: In this step, you configure incoming untagged packets to be tagged with VLAN ID 2000. If you want the switch to drop untagged packets, ignore this step.

e. In the **Trunk Allowed VLANs** field, enter **1000,2000**.

f. Click **Apply**.

LAGs

3

Link Aggregation Groups

This chapter includes the following sections:

- *Link Aggregation Concepts*
- *Add Ports to LAGs*

Link Aggregation Concepts

Link aggregation allows the switch to treat multiple physical links between two endpoints as a single logical link. All the physical links in a given LAG must operate in full-duplex mode at the same speed. LAGs can be used to directly connect two switches when the traffic between them requires high bandwidth and reliability, or to provide a higher-bandwidth connection to a public network. Management functions treat a LAG as if it is a single physical port. You can include a LAG in a VLAN. You can configure more than one LAG for a given switch.

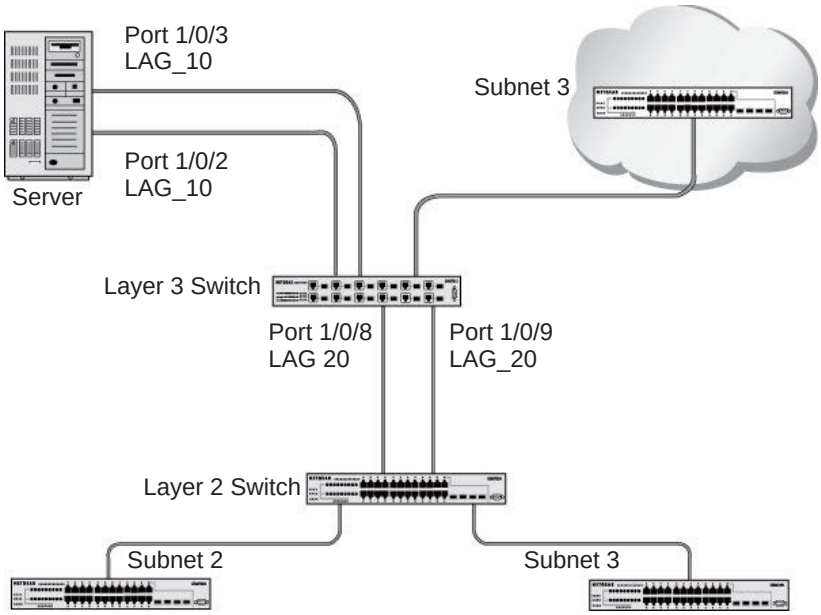


Figure 8. Example network with two LAGs

LAGs offer the following benefits:

- Increased reliability and availability. If one of the physical links in the LAG goes down, traffic is dynamically and transparently reassigned to one of the other physical links.
- Better use of physical resources. Traffic can be load-balanced across the physical links.
- Increased bandwidth. The aggregated physical links deliver higher bandwidth than each individual link.
- Incremental increase in bandwidth. A physical upgrade could produce a tenfold increase in bandwidth; LAG produces a twofold or fivefold increase, which is useful if only a small increase is needed.

Add Ports to LAGs

The example is shown as CLI commands and as a web interface procedure.

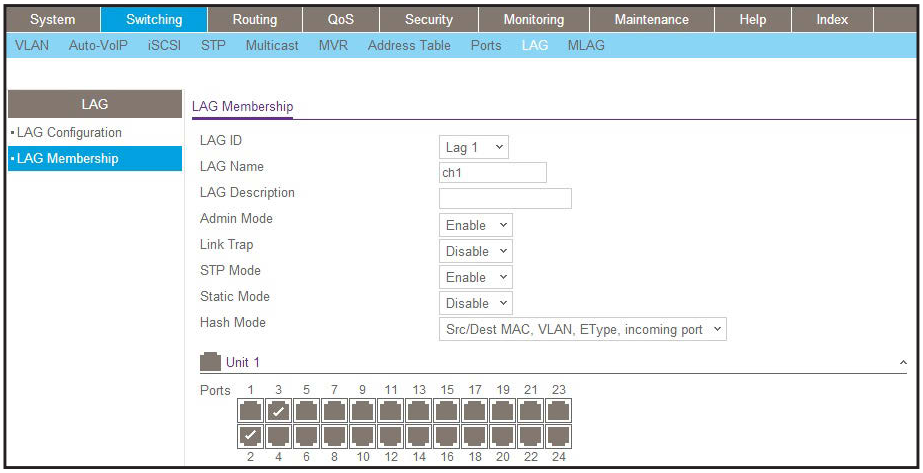
CLI: Add Ports to the LAGs

```
(Netgear Switch) #config
(Netgear Switch) (Config)#interface 0/2
(Netgear Switch) (Interface 0/2)#addport 1/1
(Netgear Switch) (Interface 0/2)#exit
(Netgear Switch) (Config)#interface 0/3
(Netgear Switch) (Interface 0/3)#addport 1/1
(Netgear Switch) (Interface 0/3)#exit
(Netgear Switch) (Config)#interface 0/8
(Netgear Switch) (Interface 0/8)#addport 1/2
(Netgear Switch) (Interface 0/8)#exit
(Netgear Switch) (Config)#interface 0/9
(Netgear Switch) (Interface 0/9)#addport 1/2
(Netgear Switch) (Interface 0/9)#exit
(Netgear Switch) (Config)#exit
```

Web Interface: Add Ports to LAGs

1. Add ports to lag_10.
   a. Select **Switching > LAG > LAG Membership**.

      A screen similar to the following displays.



   b. In the **LAG ID** list, select **LAG 1**.
   c. Click **Unit 1.** The ports display.
   d. Click the gray boxes under port **2** and **3**.

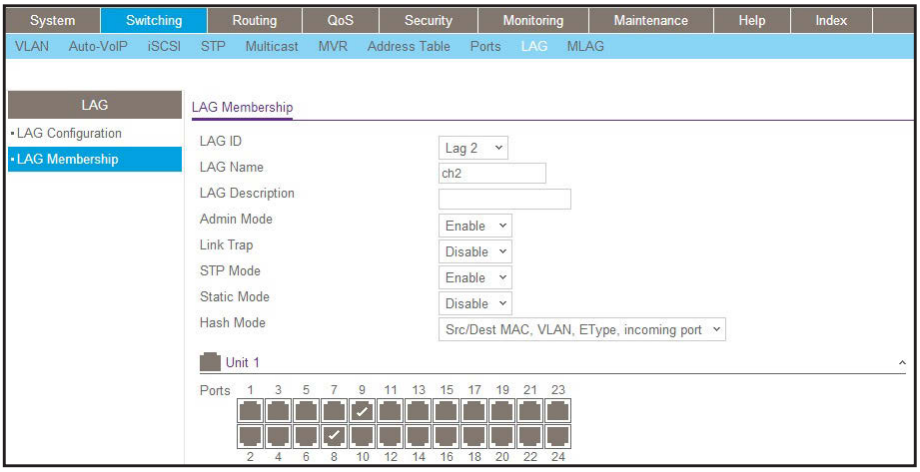
Two check marks display in the box.

e. Click the **Apply** button to save the settings.

2. Add ports to lag_20.

a. Select **Switching > LAG > LAG Membership**.

A screen similar to the following displays.



b. Under LAG Membership, in the **LAG ID** list, select **LAG 2**.

c. Click **Unit 1**. The ports display.

d. Click the gray boxes under ports **8** and **9**.

Two check marks display in the boxes.

e. Click **Apply** to save the settings.

Port Routing

4

Port routing, default routes, and static routes

This chapter includes the following sections:

- *Port Routing Concepts*
- *Port Routing Configuration*
- *Enable Routing for the Switch*
- *Enable Routing for Ports on the Switch*
- *Add a Default Route*
- *Add a Static Route*

Port Routing Concepts

The first networks were small enough for the end stations to communicate directly. As networks grew, Layer 2 bridging was used to segregate traffic, a technology that worked well for unicast traffic, but had problems coping with large quantities of multicast packets. The next major development was routing, where packets were examined and redirected at Layer 3. End stations needed to know how to reach their nearest router, and the routers had to interpret the network topology so that they could forward traffic. Although bridges tended to be faster than routers, using routers allowed the network to be partitioned into logical subnetworks, which restricted multicast traffic and also facilitated the development of security mechanisms.

An end station specifies the destination station's Layer 3 address in the packet's IP header, but sends the packet to the MAC address of a router. When the Layer 3 router receives the packet, it will minimally:

- Look up the Layer 3 address in its address table to determine the outbound port.
- Update the Layer 3 header.
- Re-create the Layer 2 header.

The router's IP address is often statically configured in the end station, although the switch supports protocols such as DHCP that allow the address to be assigned dynamically. Likewise, you can assign some of the entries in the routing tables used by the router statically, but protocols such as RIP and OSPF allow the tables to be created and updated dynamically as the network configuration changes.

Port Routing Configuration

The switch always supports Layer 2 bridging, but Layer 3 routing must be explicitly enabled, first for the switch as a whole, and then for each port that is to be part of the routed network.

The configuration commands used in the example in this section enable IP routing on ports 1/0/2,1/0/3, and 1/0/5. The router ID will be set to the switch's management IP address, or to that of any active router interface if the management address is not configured.

After the routing configuration commands have been issued, the following functions will be active:

- IP forwarding, responsible for forwarding received IP packets.
- ARP mapping, responsible for maintaining the ARP Table used to correlate IP and MAC addresses. The table contains both static entries and entries dynamically updated based on information in received ARP frames.
- Routing Table Object, responsible for maintaining the common routing table used by all registered routing protocols.

You can then activate RIP or OSPF, used by routers to exchange route information, on top of IP Routing. RIP is more often used in smaller networks, while OSPF was designed for larger and more complex topologies.

The following figure shows a Layer 3 switch configured for port routing. It connects three different subnets, each connected to a different port.

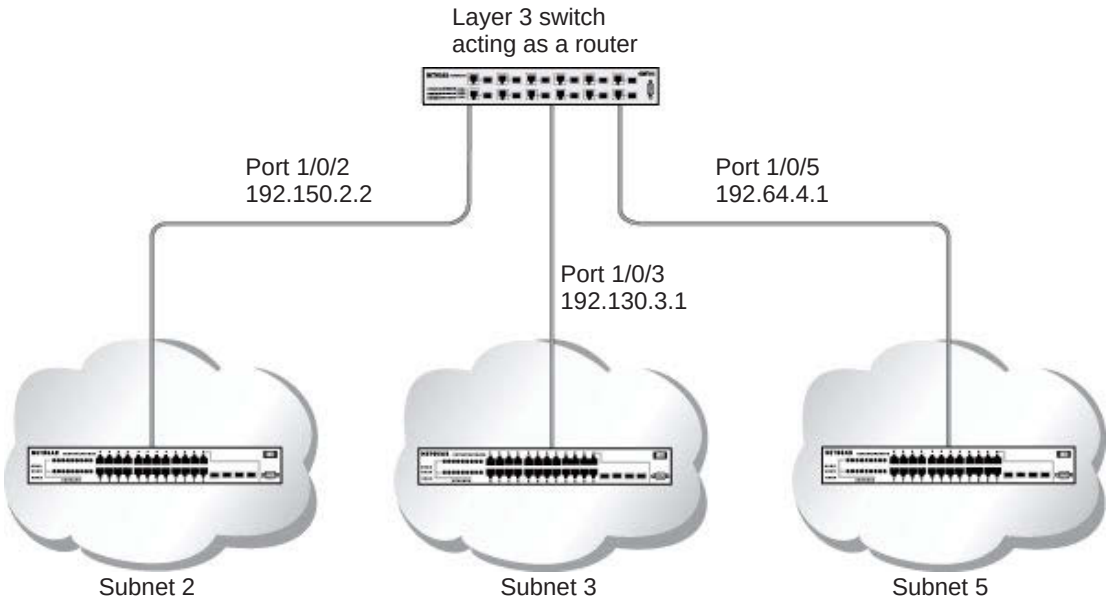


Figure 9. Layer 3 switch configured for port routing

Enable Routing for the Switch

The example is shown as CLI commands and as a web interface procedure.

CLI: Enable Routing for the Switch

The following script shows the commands that you use to configure the switch to provide the port routing support shown in *Figure 9, Layer 3 switch configured for port routing* on page 73.

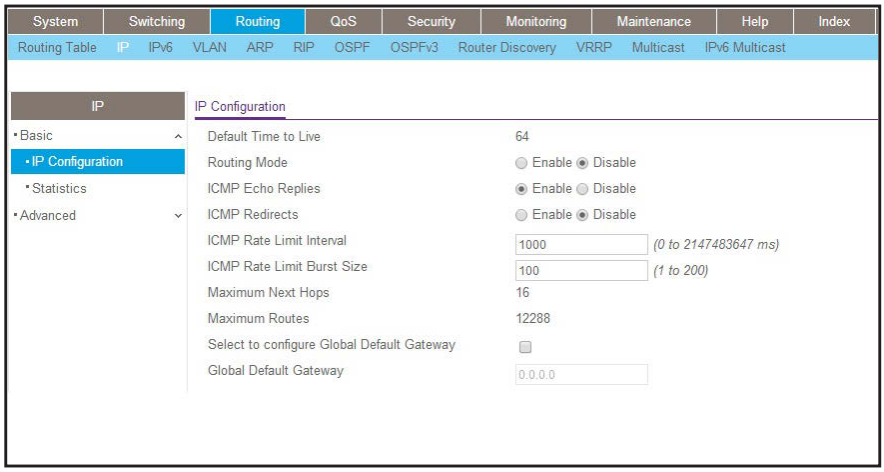
Use the following command to enable routing for the switch. Execution of the command enables IP forwarding by default.

```
(Netgear Switch) #config
(Netgear Switch) (Config)#ip routing
(Netgear Switch) (Config)#exit
```

Web Interface: Enable Routing for the Switch

1. Select **Routing > IP > Basic > IP Configuration**.

   A screen similar to the following displays.



2. For Routing Mode, select the **Enable** radio button.
3. Click **Apply** to save the settings.

Enable Routing for Ports on the Switch

Use the following commands or the web interface to enable routing for ports on the switch. The default link-level encapsulation format is Ethernet. Configure the IP addresses and subnet masks for the ports. Network-directed broadcast frames will be dropped. The maximum transmission unit (MTU) size is 1500 bytes.

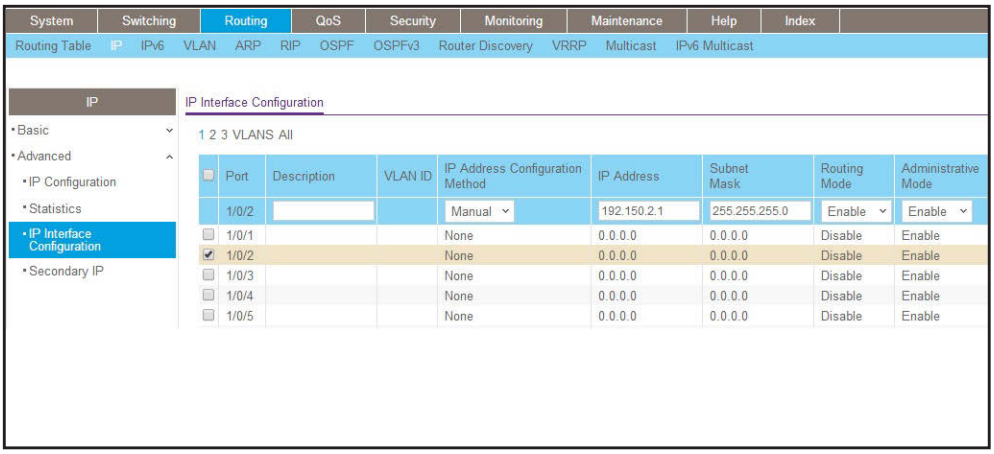
CLI: Enable Routing for Ports on the Switch

```
(Netgear Switch) #config
(Netgear Switch) (Config)#interface 1/0/2
(Netgear Switch) (Interface 1/0/2)#routing
(Netgear Switch) (Interface 1/0/2)#ip address 192.150.2.1 255.255.255.0
(Netgear Switch) (Interface 1/0/2)#exit

(Netgear Switch) (Config)#interface 1/0/3
(Netgear Switch) (Interface 1/0/3)#routing
(Netgear Switch) (Interface 1/0/3)#ip address 192.150.3.1 255.255.255.0
(Netgear Switch) (Interface 1/0/3)#exit

(Netgear Switch) (Config)#interface 1/0/5
(Netgear Switch) (Interface 1/0/5)#routing
(Netgear Switch) (Interface 1/0/5)#ip address 192.150.5.1 255.255.255.0
(Netgear Switch) (Interface 1/0/5)#exit
(Netgear Switch) (Config)#exit
```

Web Interface: Enable Routing for Ports on the Switch

1. Assign IP address 192.150.2.1/24 to interface 1/0/2.
   a. Select **Routing > IP > Advanced > IP Interface Configuration**.

      A screen similar to the following displays.



   b. Scroll down and select the interface **1/0/2** check box.

      Now 1/0/2 appears in the Interface field at the top.

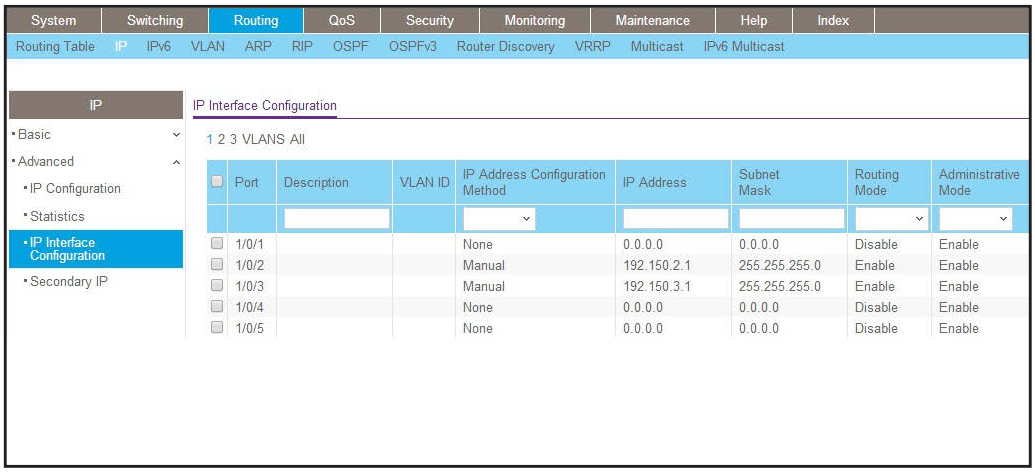
   c. Under the IP Interface Configuration, enter the following information:
      - In the **IP Address** field, enter **192.150.2.1**.
      - In the **Subnet Mask** field, enter **255.255.255.0**.
      - In the **Routing Mode** field, select **Enable**.

d. Click **Apply** to save the settings.

2. Assign IP address 192.150.3.1/24 to interface 1/0/3.

a. Select **Routing > IP> Advanced > IP Interface Configuration**.

A screen similar to the following displays.



b. Scroll down and select the interface **1/0/3** check box.

Now 1/0/3 appears in the Interface field at the top.

c. Enter the following information:

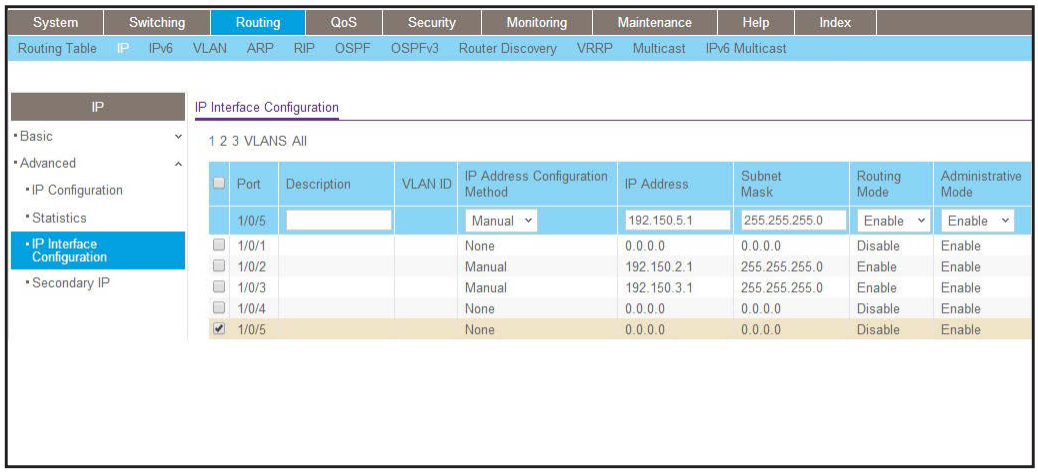
- In the **IP Address** field, enter **192.150.3.1**.
- In the **Subnet Mask** field, enter **255.255.255.0**.
- In the **Routing Mode** field, select **Enable**.

d. Click **Apply** to save the settings.

3. Assign IP address 192.150.5.1/24 to interface 1/0/5.

a. Select **Routing > IP > Advanced > IP Interface Configuration**.

A screen similar to the following displays.



b. Scroll down and select the interface **1/0/5** check box.

Now 1/0/5 appears in the Interface field at the top.

c. Enter the following information:

- In the **IP Address** field, enter **192.150.5.1**.
- In the **Subnet Mask** field, enter **255.255.255.0**.
- In the **Routing Mode** field, select **Enable**.

d. Click **Apply** to save the settings.

Add a Default Route

When IP routing takes place on a switch, a routing table is needed for the switch to forward the packet based on the destination IP address. The route entry in the routing table can either be created dynamically through routing protocols like RIP and OSPF, or be manually created by the network administrator. The route created manually is called the static or default route.

A default route is used for forwarding the packet when the switch cannot find a match in the routing table for an IP packet. The following example shows how to create a default route.

CLI: Add a Default Route

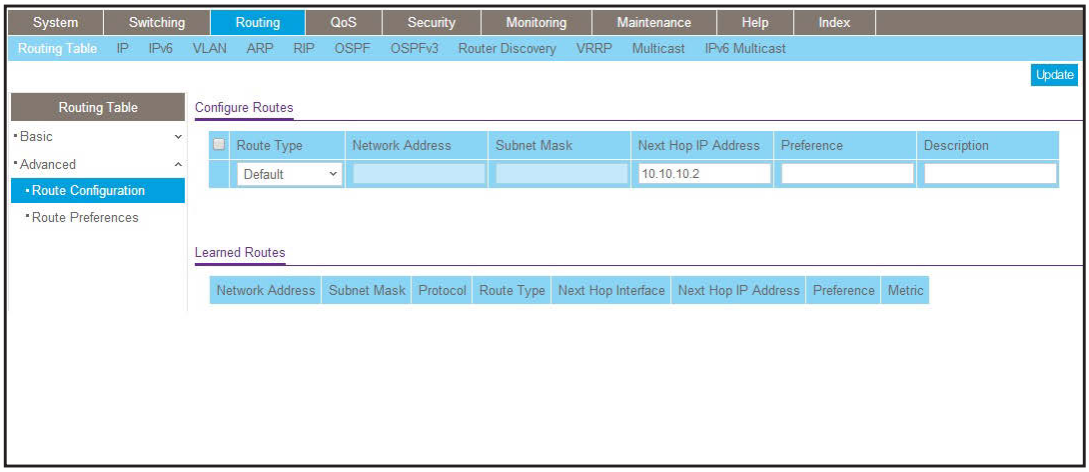
```
(FSM7338S) (Config) #ip route default?
<nexthopip> Enter the IP Address of the next router.
(FSM7328S) (Config)#ip route default 10.10.10.2
```

Note: IP subnet 10.10.10.0 should be configured using either port routing (*Enable Routing for Ports on the Switch* on page 74) or VLAN routing (see *Set Up VLAN Routing for the VLANs and the Switch* on page 86).

Web Interface: Add a Default Route

1. Select **Routing > Routing Table > Basic > Route Configuration**.

   A screen similar to the following displays.



2. In the **Route Type** list, select **DefaultRoute**.
3. In the **Next Hop IP Address** field, enter one of the routing interface's IP addresses.
   - The **Network Address** and **Subnet Mask** fields will not accept input as they are not needed.
   - The **Preference** field is optional. A value of 1 (highest) will be assigned by default if not specified.
4. Click the **Add** button on the bottom of the screen.

   This creates the default route entry in the routing table.

Add a Static Route

When the switch performs IP routing, it forwards the packet to the default route for a destination that is not in the same subnet as the source address. However, you can set a path (static route) that is different than the default route if you prefer. The following procedure shows how to add a static route to the switch routing table.

CLI: Add a Static Route

The following commands assume that the switch already has a defined a routing interface with a network address of 10.10.10.0, and is configured so that all packets destined for network 10.10.100.0 take the path of routing port.

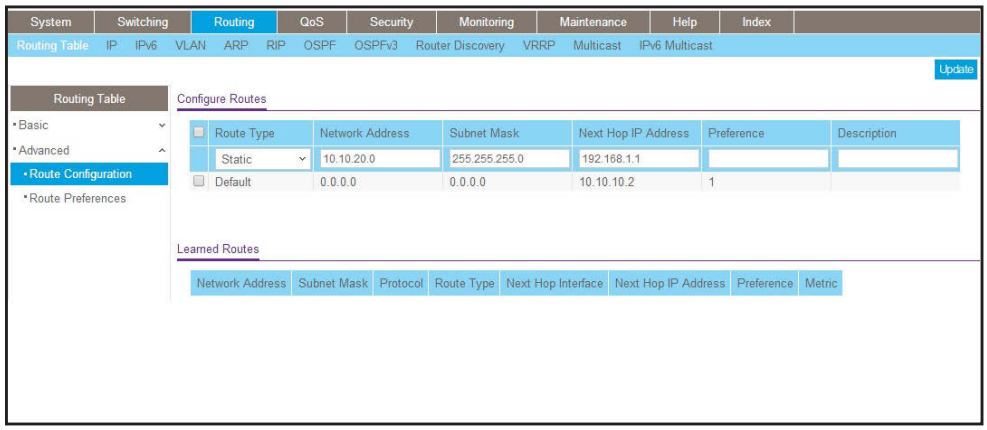
```
(FSM7328S) #show ip route

Total Number of Routes.........................1

Network     Subnet                    Next Hop    Next Hop
Address     Mask           Protocol   Intf        IP Address
----------  -------------  --------   ----------  -----------
10.10.10.0  255.255.255.0  Local      1/0/3       10.10.10.1
```

To delete the static route, simply add the **no** keyword in the front of the **`ip route`** command.

Web Interface: Add a Static Route

1. Select **Routing > Routing Table > Basic > Route Configuration**.

   A screen similar to the following displays.



2. In the **Route Type** list, select **Static**.
3. Fill in the **Network Address** field.

   Note that this field should have a network IP address, not a host IP address. Do not enter something like *10,100.100.1*. The last number should always be 0 (zero).
4. In the **Subnet Mask** field, enter a value that matches the subnet range that you want to use.
5. The **Preference** field is optional. A value of 1 is entered by default if you do not enter a number.
6. Click the **Add** button on the bottom of the screen. The screen is updated with the static route shown in the routing table.
7. To remove a route entry, either static or default, select the check box to the left of the entry, and click the **Delete** button on the bottom of the screen.

VLAN Routing

5

VLAN routing for a VLAN and for the switch

This chapter includes the following sections:

- *VLAN Routing Concepts*
- *Create Two VLANs*
- *Set Up VLAN Routing for the VLANs and the Switch*

VLAN Routing Concepts

You can configure the switch with some ports supporting VLANs and some supporting routing. You can also configure it to allow traffic on a VLAN to be treated as if the VLAN were a router port.

When a port is enabled for bridging (the default) rather than routing, all normal bridge processing is performed for an inbound packet, which is then associated with a VLAN. Its MAC destination address (DA) and VLAN ID are used to search the MAC address table. If routing is enabled for the VLAN and the MAC DA of an inbound unicast packet is that of the internal bridge-router interface, the packet is routed. An inbound multicast packet is forwarded to all ports in the VLAN, and also to the internal bridge-router interface if it was received on a routed VLAN.

Since a port can be configured to belong to more than one VLAN, VLAN routing might be enabled for all of the VLANs on the port, or for a subset. VLAN routing can be used to allow more than one physical port to reside on the same subnet. It could also be used when a VLAN spans multiple physical networks, or when more segmentation or security is required.

The next section shows you how to configure the switch to support VLAN routing and how to use RIP and OSPF. A port can be either a VLAN port or a router port, but not both. However, a VLAN port can be part of a VLAN that is itself a router port.

Create Two VLANs

This section provides an example of how to configure the switch to support VLAN routing. The configuration of the VLAN router port is similar to that of a physical port. The main difference is that, after the VLAN has been created, you must use the **`show ip vlan`** command to determine the VLAN's interface ID so that you can use it in the router configuration commands.

The diagram in this section shows a Layer 3 switch configured for port routing. It connects two VLANs, with two ports participating in one VLAN, and one port in the other. The script shows the commands that you use to configure the switch to provide the VLAN routing support shown in the diagram.

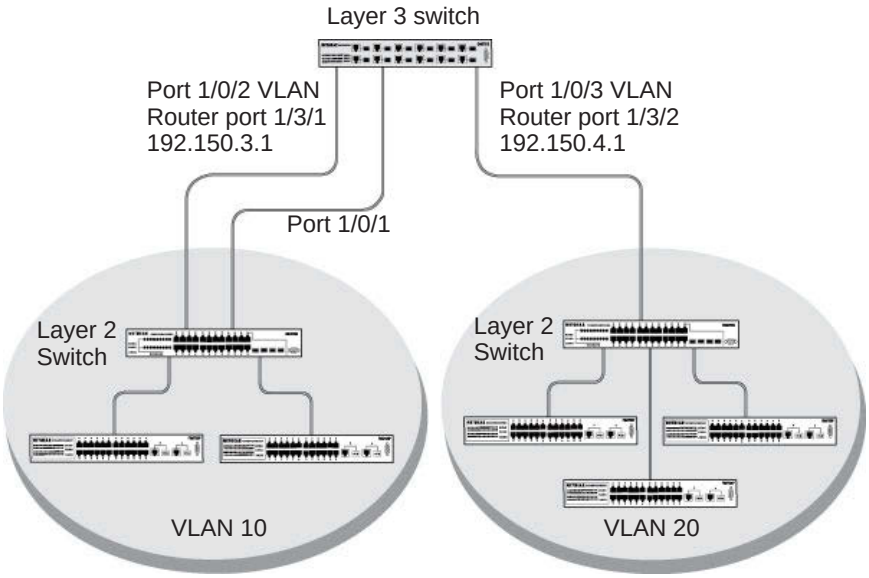


Figure 10. Layer 3 switch configured for port routing

CLI: Create Two VLANs

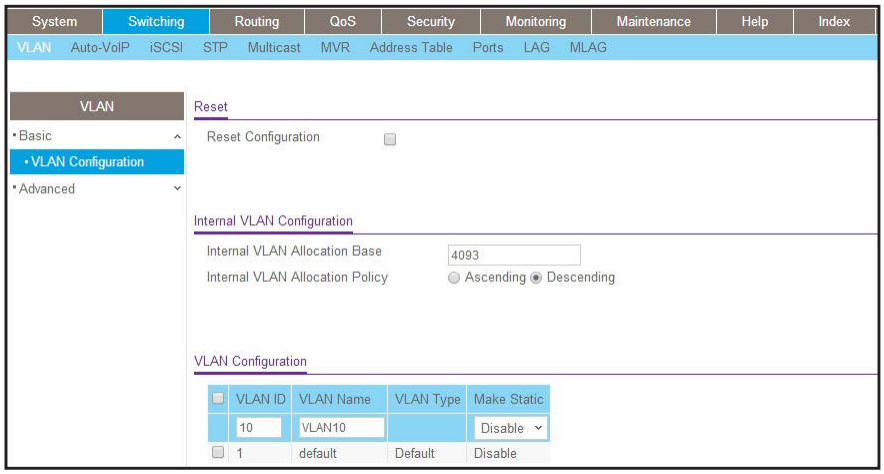
The following code sequence shows an example of creating two VLANs with egress frame tagging enabled.

```
(Netgear Switch) #vlan data
(Netgear Switch) (Vlan)#vlan 10
(Netgear Switch) (Vlan)#vlan 20
(Netgear Switch) (Vlan)#exit
(Netgear Switch) #conf
(Netgear Switch) (Config)#interface range 1/0/1-1/0/2
(Netgear Switch) (conf-if-range-1/0/1-1/0/2)#vlan participation include 10
(Netgear Switch) (conf-if-range-1/0/1-1/0/2)#vlan pvid 10
(Netgear Switch) (conf-if-range-1/0/1-1/0/2)#exit
(Netgear Switch) (Config)#interface 1/0/3
(Netgear Switch) (Interface 1/0/3)#vlan participation include 20
(Netgear Switch) (Interface 1/0/3)#vlan pvid 20
(Netgear Switch) (Interface 1/0/3)#exit
(Netgear Switch) (Config)#exit
```

Web Interface: Create Two VLANs

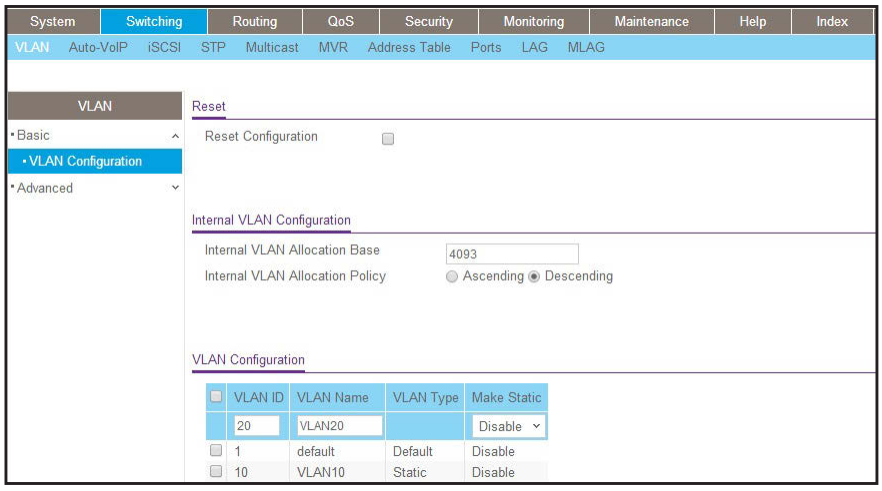
1. Create VLAN 10 and VLAN20.
   a. Select **Switching > VLAN > Advanced > VLAN Configuration**.

      A screen similar to the following displays.



   b. In the **VLAN ID** field, enter **10**.
   c. In the **VLAN Name** field, enter **VLAN10**.
   d. In the **VLAN Type** list, select **Static**.
   e. Click **Add**.
   f. Select **Switching > VLAN > Advanced > VLAN Configuration**.

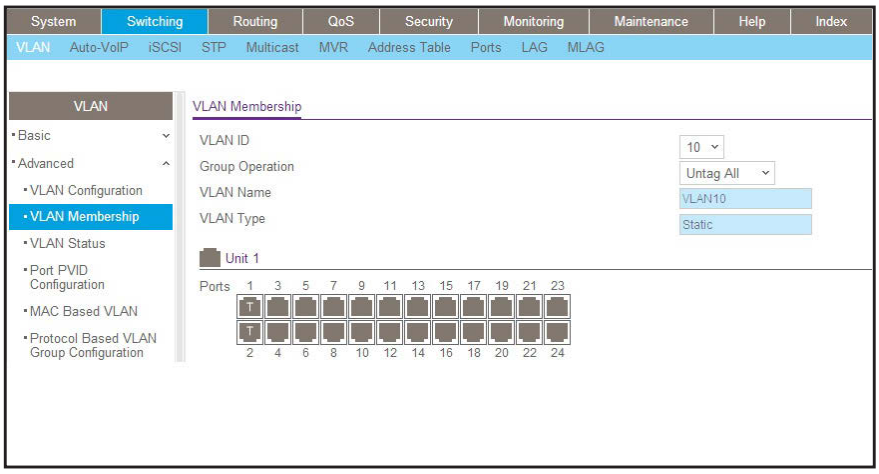
      A screen similar to the following displays.



   g. In the **VLAN ID** field, enter **20**.
   h. In the **VLAN Name** field, enter **VLAN20**.
   i. In the **VLAN Type** list, select **Static**.
   j. Click **Add**.

2. Add ports to the VLAN10 and VLAN20.
   a. Select **Switching > VLAN > Advanced > VLAN Membership**.

      A screen similar to the following displays.

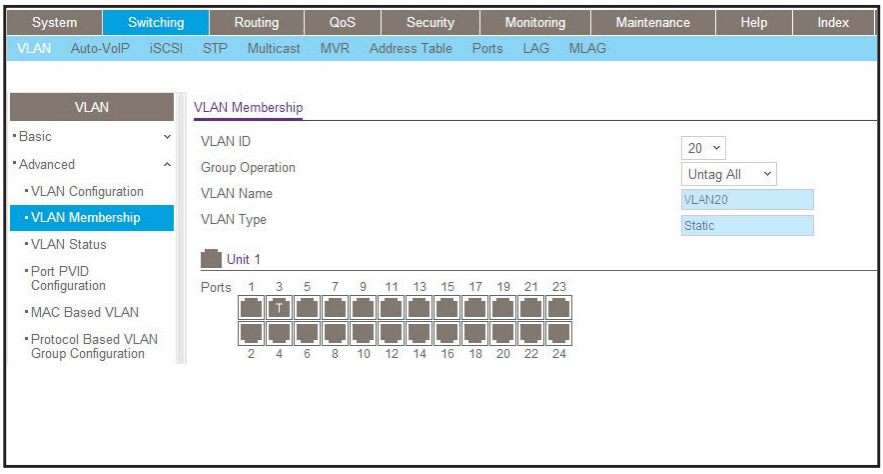


   b. In the **VLAN ID** field, select **10**.
   c. Click the **Unit 1.** The ports display.
   d. Click the gray boxes under ports **1** and **2** until **T** displays.

      The T specifies that the egress packet is tagged for the port.

   e. Click **Apply**.
   f. Select **Switching > VLAN > Advanced > VLAN Membership**.

      A screen similar to the following displays.



   g. In the **VLAN ID** list, select **20**.
   h. Click **Unit 1**. The ports display.
   i. Click the gray box under port **3** until **T** displays.

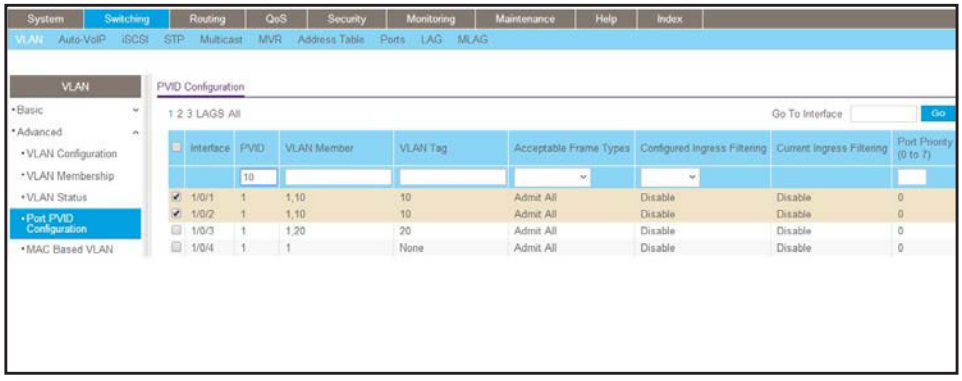
      The T specifies that the egress packet is tagged for the port.

j. Click **Apply**.

3. Assign PVID to VLAN10 and VLAN20.

a. Select **Switching > VLAN > Advanced > Port PVID Configuration**.

A screen similar to the following displays.



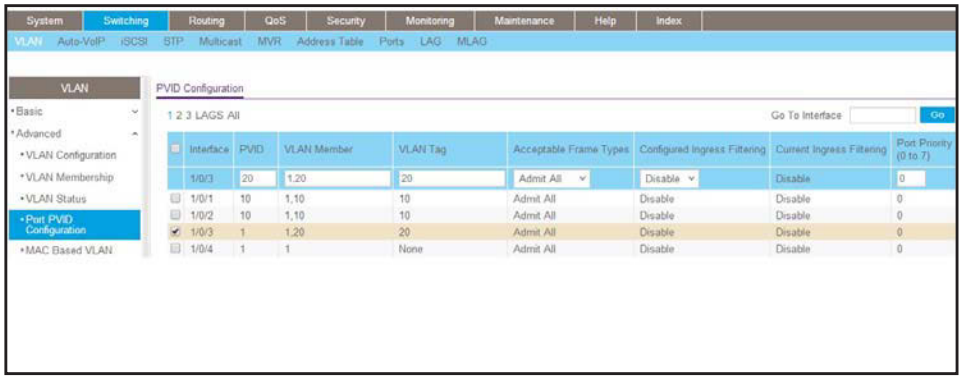
b. Scroll down and select **1/0/1 and 1/0/2 check boxes**.

c. In the **PVID (1 to 4093)** field, enter **10**.

d. Click **Apply** to save the settings.

e. Select **Switching > VLAN > Advanced > Port PVID Configuration**.

A screen similar to the following displays.



f. Scroll down and select the **1/0/3** check box.

g. In the **PVID (1 to 4093)** field, enter **20**.

h. Click **Apply** to save the settings.

Set Up VLAN Routing for the VLANs and the Switch

The example is shown as CLI commands and as a web interface procedure.

CLI: Set Up VLAN Routing for the VLANs and the Switch

1. The following code sequence shows how to enable routing for the VLANs:

```
(Netgear Switch) #vlan data
(Netgear Switch) (Vlan)#vlan routing 10
(Netgear Switch) (Vlan)#vlan routing 20
(Netgear Switch) (Vlan)#exit
```

   This returns the logical interface IDs that will be used instead of the slot/port in subsequent routing commands. Assume that VLAN 10 is assigned the ID 3/1, and VLAN 20 is assigned the ID 3/2.

2. Enable routing for the switch.

```
(Netgear Switch) #config
(Netgear Switch) (Config)#ip routing
(Netgear Switch) (Config)#exit
```

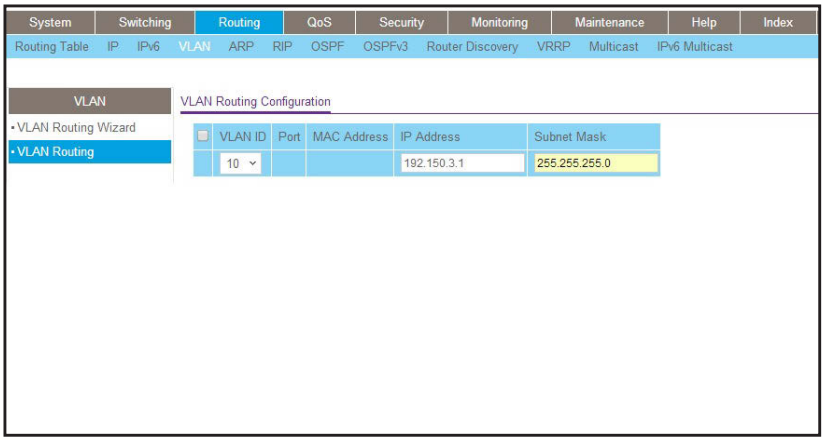
3. The next sequence shows an example of configuring the IP addresses and subnet masks for the virtual router ports.

```
(Netgear Switch) (Config)#interface vlan 10
(Netgear Switch) (Interface-vlan 10)#ip address 192.150.3.1 255.255.255.0
(Netgear Switch) (Interface-vlan 10)#exit
(Netgear Switch) (Config)#interface vlan 20
(Netgear Switch) (Interface-vlan 20)#ip address 192.150.4.1 255.255.255.0
(Netgear Switch) (Interface-vlan 20)#exit
(Netgear Switch) (Config)#exit
```

Web Interface: Set Up VLAN Routing for the VLANs and the Switch

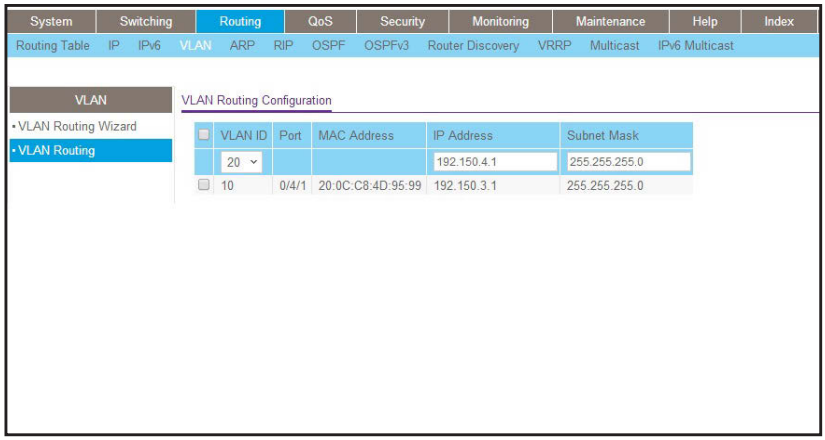
1. Select **Routing > VLAN> VLAN Routing**.

   A screen similar to the following displays.



2. Enter the following information:
   - In the **VLAN ID (1 to 4093)** list, select **10**.
   - In the **IP Address** field, enter **192.150.3.1**.
   - In the **Subnet Mask** field, enter **255.255.255.0**.
3. Click **Add** to save the settings.
4. Select **Routing > VLAN > VLAN Routing**.

   A screen similar to the following displays.



5. Enter the following information:
   - Select **10** in the **VLAN ID** (1 to 4093) field.
   - In the **IP Address** field, enter **192.150.4.1**.
   - In the **Subnet Mask** field, enter **255.255.255.0**.
6. Click **Add** to save the settings.

RIP

6

Routing Information Protocol

This chapter includes the following sections:

- *Routing Information Protocol Concepts*
- *Enable Routing for the Switch*
- *Enable Routing for Ports*
- *Enable RIP on the Switch*
- *Enable RIP for Ports 1/0/2 and 1/0/3*
- *Configure VLAN Routing with RIP Support*

Routing Information Protocol Concepts

Routing Information Protocol (RIP) is a protocol that routers can use to exchange network topology information. It is characterized as an interior gateway protocol, and is typically used in small to medium-sized networks. A router running RIP sends the contents of its routing table to each of its adjacent routers every 30 seconds. When a route is removed from the routing table, it is flagged as unusable by the receiving routers after 180 seconds, and removed from their tables after an additional 120 seconds.

There are two versions of RIP (the switch supports both):

- RIPv1 defined in RFC 1058.
  - Routes are specified by IP destination network and hop count.
  - The routing table is broadcast to all stations on the attached network.
- RIPv2 defined in RFC 1723.
  - Route specification also includes subnet mask and gateway.
  - The routing table is sent to a multicast address, reducing network traffic.
  - Authentication is used for security.

You can configure a given port to do the following:

- Receive packets in either or both formats.
- Send packets formatted for RIPv1 or RIPv2, or send RIPv2 packets to the RIPv1 broadcast address.
- Prevent any RIP packets from being received.
- Prevent any RIP packets from being sent.

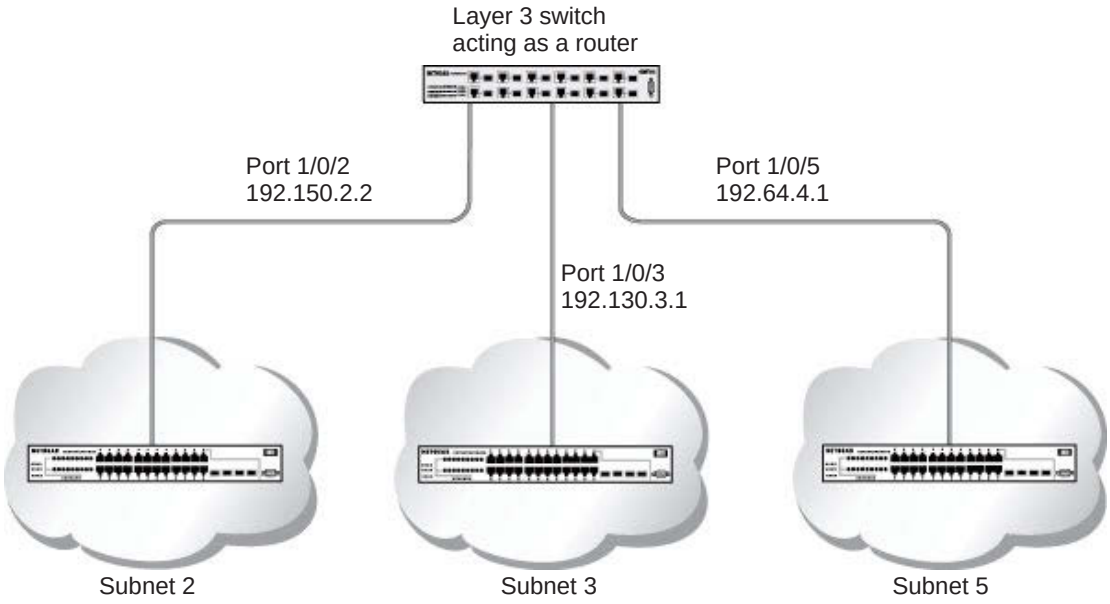


Figure 11. Network with RIP on ports 1/0/2 and 1/0/3

Enable Routing for the Switch

The example is shown as CLI commands and as a web interface procedure.

CLI: Enable Routing for the Switch

```
(Netgear Switch) #config
(Netgear Switch) (Config)#ip routing
(Netgear Switch) (Config)#exit
```

Web Interface: Enable Routing for the Switch

1. Select **Routing > IP > Basic > IP Configuration**.

   A screen similar to the following displays.

2. For Routing Mode, select the **Enable** radio button.
3. Click **Apply** to save the settings.

Enable Routing for Ports

The example is shown as CLI commands and as a web interface procedure.

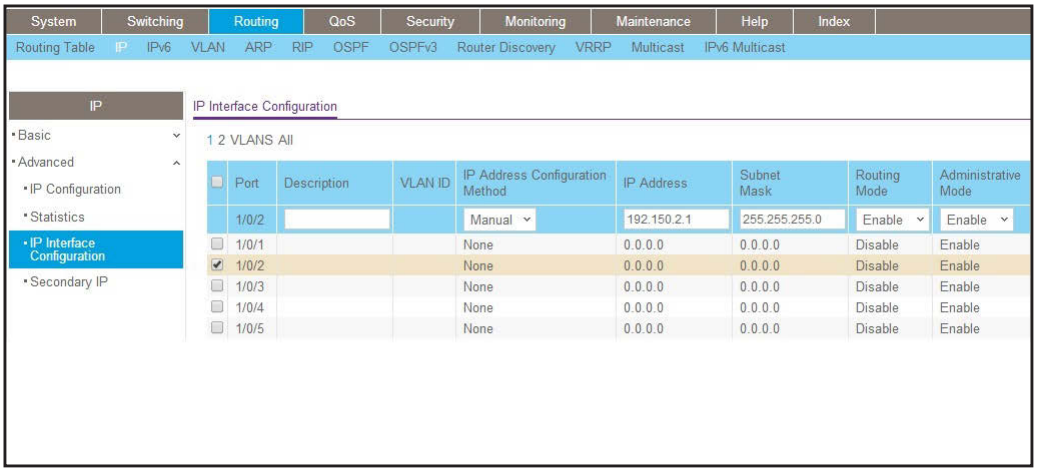
CLI: Enable Routing and Assigning IP Addresses for Ports 1/0/2 and 1/0/3

```
(Netgear Switch) #config
(Netgear Switch) (Config)#interface 1/0/2
(Netgear Switch) (Interface 1/0/2)#routing
(Netgear Switch) (Interface 1/0/2)#ip address 192.150.2.1 255.255.255.0
(Netgear Switch) (Interface 1/0/2)#exit
(Netgear Switch) (Config)#interface 1/0/3
(Netgear Switch) (Interface 1/0/3)#routing
(Netgear Switch) (Interface 1/0/3)#ip address 192.150.3.1 255.255.255.0
(Netgear Switch) (Interface 1/0/3)#exit
(Netgear Switch) (Config)#exit
```

Web Interface: Enable Routing for the Ports

1. Assign IP address 192.150.2.1/24 to interface 1/0/2.
   a. Select **Routing > Advanced > IP Interface Configuration**.

      A screen similar to the following displays.



   b. Scroll down and select the Interface **1/0/2** check box. Now 1/0/2 appears in the Interface field at the top.

   c. Enter the following information:
      - In the **IP Address Configuration Method** field, select **Manual**.
      - In the **IP Address** field, enter **192.150.2.1**.

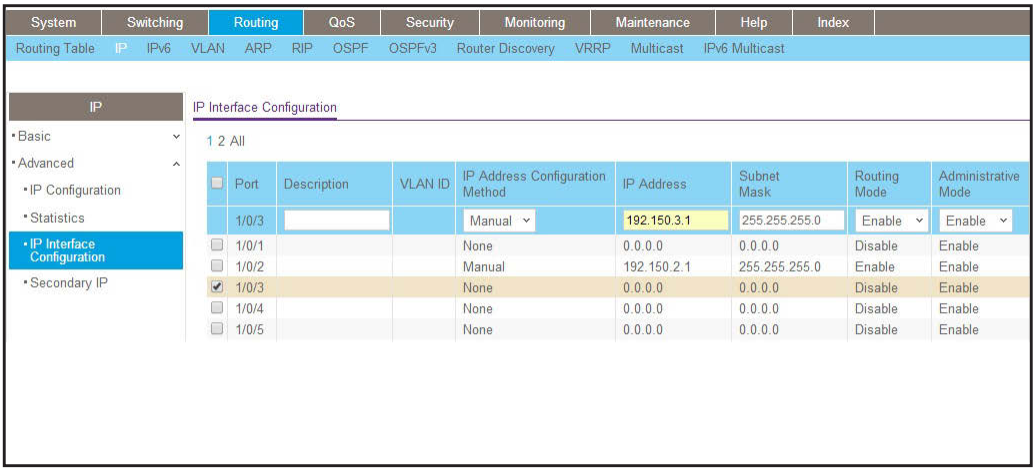
- In the **Subnet Mask** field, enter **255.255.255.0**.
- In the **Routing Mode** field, select **Enable**.

d. Click **Apply** to save the settings.

2. Assign IP address 192.150.3.1/24 to interface 1/0/3.

a. Select **Routing > Advanced >IP Interface Configuration**.

A screen similar to the following displays.



b. Scroll down and select the interface **1/0/3** check box.

Now 1/0/3 appears in the Interface field at the top.

c. Enter the following information:

In the **IP Address Configuration Method** field, select **Manual**.

- In the **IP Address** field, enter **192.150.3.1**.
- In the **Subnet Mask** field, enter **255.255.255.0**.
- In the **Routing Mode** field, select **Enable**.

d. Click **Apply** to save the settings.

Enable RIP on the Switch

Note: Unless you have previously disabled RIP, you can skip this step since RIP is enabled by default.

CLI: Enable RIP on the Switch

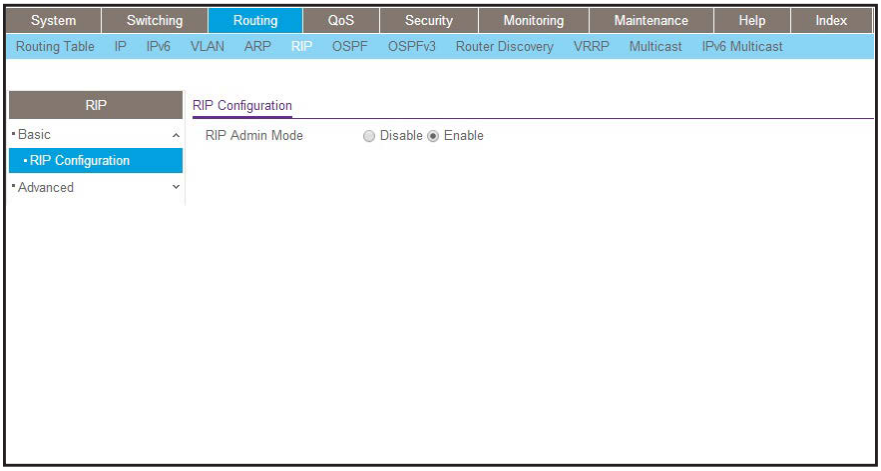
This sequence enables RIP for the switch. The route preference defaults to 15.

```
(Netgear Switch) #config
(Netgear Switch) (Config)#router rip
(Netgear Switch) (Config router)#enable
(Netgear Switch) (Config router)#exit
(Netgear Switch) (Config)#exit
```

Web Interface: Enable RIP on the Switch

1. Select **Routing > RIP > Basic > RIP Configuration**.

   A screen similar to the following displays.



2. For RIP Admin Mode, select **Enable** radio button.
3. Click **Apply** to save the setting.

Enable RIP for Ports 1/0/2 and 1/0/3

The example is shown as CLI commands and as a web interface procedure.

CLI: Enable RIP for Ports 1/0/2 and 1/0/3

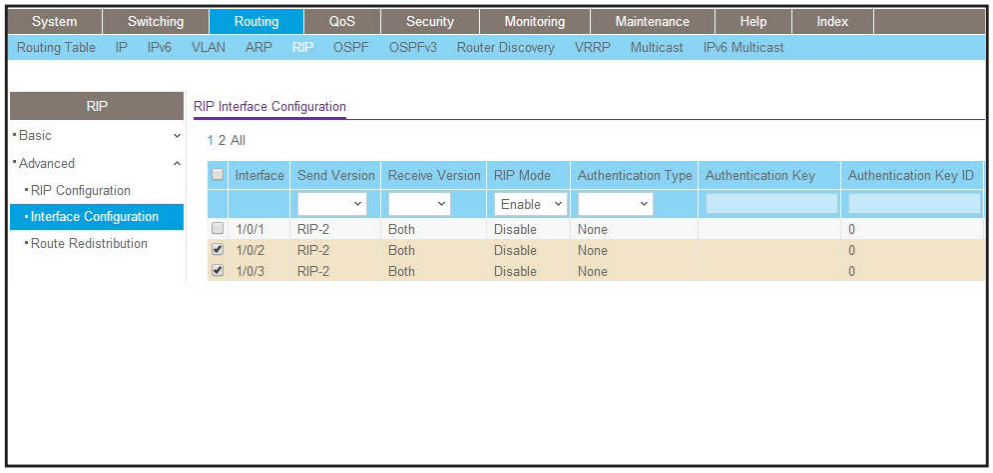
This command sequence enables RIP for ports 1/0/2 and 1/0/3. Authentication defaults to none, and no default route entry is created. The commands specify that both ports receive both RIPv1 and RIPv2 frames, but send only RIPv2-formatted frames.

```
(Netgear Switch) #config
(Netgear Switch) (Config)#interface 1/0/2
(Netgear Switch) (Interface 1/0/2)#ip rip
(Netgear Switch) (Interface 1/0/2)#ip rip receive version both
(Netgear Switch) (Interface 1/0/2)#ip rip send version rip2
(Netgear Switch) (Interface 1/0/2)#exit
(Netgear Switch) (Config)#interface 1/0/3
(Netgear Switch) (Interface 1/0/3)#ip rip
(Netgear Switch) (Interface 1/0/3)#ip rip receive version both
(Netgear Switch) (Interface 1/0/3)#ip rip send version rip2
(Netgear Switch) (Interface 1/0/3)#exit
(Netgear Switch) (Config)#exit
```

Web Interface: Enable RIP for Ports 1/0/2 and 1/0/3

1. Select **Routing > RIP > Advanced > RIP Configuration**.

   A screen similar to the following displays.



2. Scroll down and select the **Interface 1/0/2 and 1/0/3** check box.

3. Enter the following information:
   - For RIP Admin Mode, select the **Enable** radio button.
   - In the **Send Version** field, select **RIP-2**.
4. Click **Apply** to save the settings.

Configure VLAN Routing with RIP Support

Routing Information Protocol (RIP) is one of the protocols that routers can use to exchange network topology information. It is characterized as an interior gateway protocol, and is typically used in small to medium-sized networks.

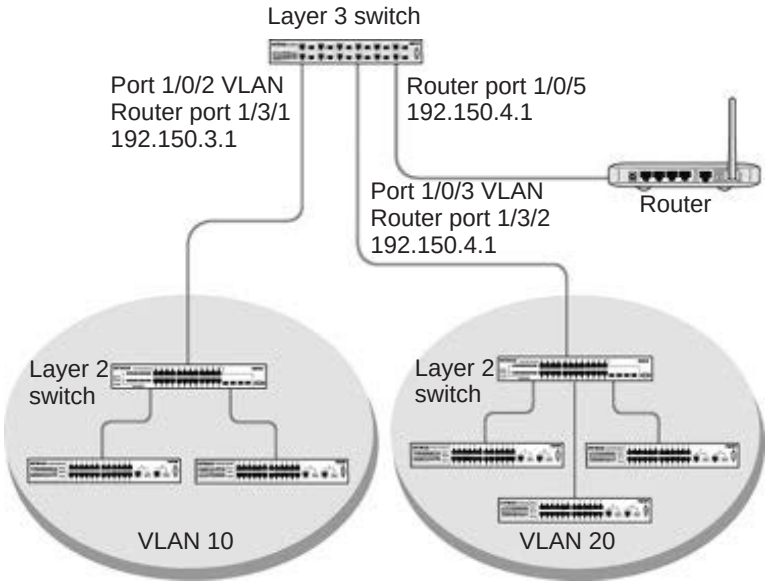


Figure 12. VLAN routing RIP configuration example

This example adds support for RIPv2 to the configuration created in the base VLAN routing example. A second router, using port routing rather than VLAN routing, has been added to the network.

CLI: Configure VLAN Routing with RIP Support

1. Configure VLAN routing with RIP support on the switch.

```
(Netgear Switch) #vlan data
(Netgear Switch) (Vlan)#vlan 10
(Netgear Switch) (Vlan)#vlan 20
(Netgear Switch) (Vlan)#vlan routing 10
(Netgear Switch) (Vlan)#vlan routing 20
(Netgear Switch) (Vlan)#exit
(Netgear Switch) #conf
```

```
(Netgear Switch) (Config)#ip routing
(Netgear Switch) (Config)#vlan port tagging all 10
(Netgear Switch) (Config)#vlan port tagging all 20
(Netgear Switch) (Config)#interface 1/0/2
(Netgear Switch) (Interface 1/0/2)#vlan participation include 10
(Netgear Switch) (Interface 1/0/2)#vlan pvid 10
(Netgear Switch) (Interface 1/0/2)#exit
(Netgear Switch) (Config)#interface 1/0/3
(Netgear Switch) (Interface 1/0/3)#vlan participation include 20
(Netgear Switch) (Interface 1/0/3)#vlan pvid 20
(Netgear Switch) (Interface 1/0/3)#exit
(Netgear Switch) #config
(Netgear Switch) (Config)#interface vlan 10
(Netgear Switch) (Interface vlan 10)#ip address 192.150.3.1 255.255.255.0
(Netgear Switch) (Interface vlan 10)#exit
(Netgear Switch) (Config)#interface vlan 20
(Netgear Switch) (Interface vlan 20)#ip address 192.150.4.1 255.255.255.0
(Netgear Switch) (Interface vlan 20)#exit
```

2. Enable RIP for the switch.

   The route preference defaults to 15.

```
(Netgear Switch) (Config)#router rip
(Netgear Switch) (Config router)#enable
(Netgear Switch) (Config router)#exit
```

3. Configure the IP address and subnet mask for a nonvirtual router port.

```
(Netgear Switch) (Config)#interface 1/0/5
(Netgear Switch) (Interface 1/0/5)#ip address 192.150.5.1 255.255.255.0
(Netgear Switch) (Interface 1/0/5)#exit
```

4. Enable RIP for the VLAN router ports.

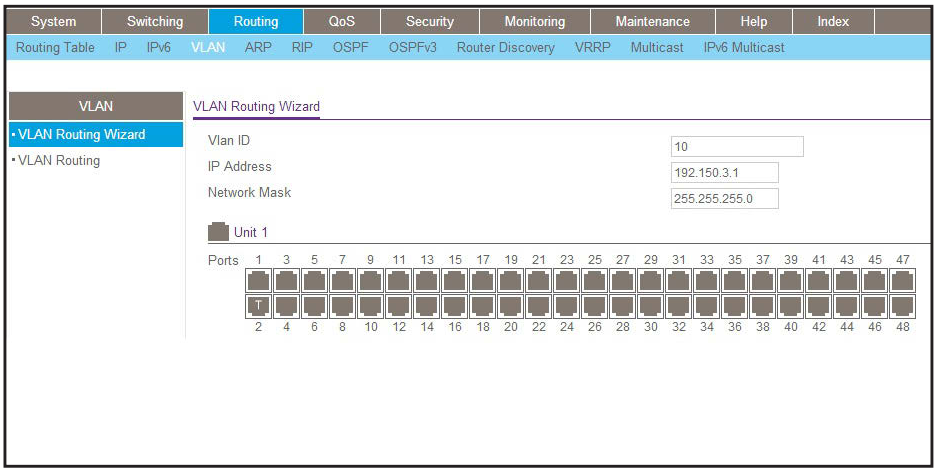
   Authentication defaults to none, and no default route entry is created.

```
(Netgear Switch) (Config)#interface vlan 10
(Netgear Switch) (Interface vlan 10)#ip rip
(Netgear Switch) (Interface vlan 10)#exit
(Netgear Switch) (Config)#interface vlan 20
(Netgear Switch) (Interface vlan 20)#ip rip
(Netgear Switch) (Interface vlan 20)#exit
(Netgear Switch) (Config)#exit
```

Web Interface: Configure VLAN Routing with RIP Support

1. Configure a VLAN and include ports 1/0/2 in the VLAN:
   a. Select **Routing > VLAN > VLAN Routing Wizard**.

      A screen similar to the following displays.



   b. Enter the following information:
      - In the VLAN ID field, enter 10.
      - In the **IP Address** field, enter **192.150.3.1**.
      - In the **Network Mask** field, enter **255.255.255.0**.

   c. Click **Unit 1**. The ports display:

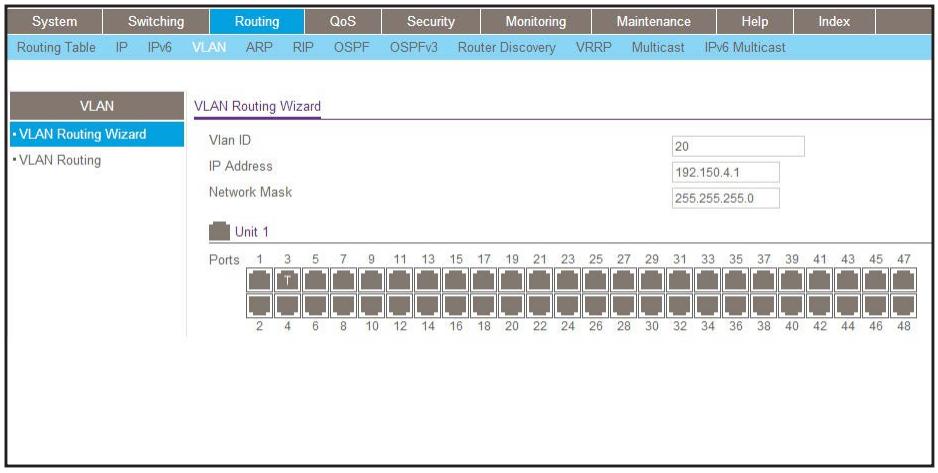
   d. Click the gray box under port **2** until **T** displays.

      The T specifies that the egress packet is tagged for the port.

   e. Click **Apply** to save the VLAN that includes ports 2.

2. Configure a VLAN, and include port 1/0/3 in the VLAN:
   a. Select **Routing > VLAN > VLAN Routing Wizard**.

      A screen similar to the following displays.



b. Enter the following information:
   - In the **Vlan ID** field, enter **20**.
   - In the **IP Address** field, enter **192.150.4.1**.
   - In the **Network Mask** field, enter **255.255.255.0**.

c. Click **Unit 1**. The ports display.

d. Click the gray box under port **3** until **T** displays.

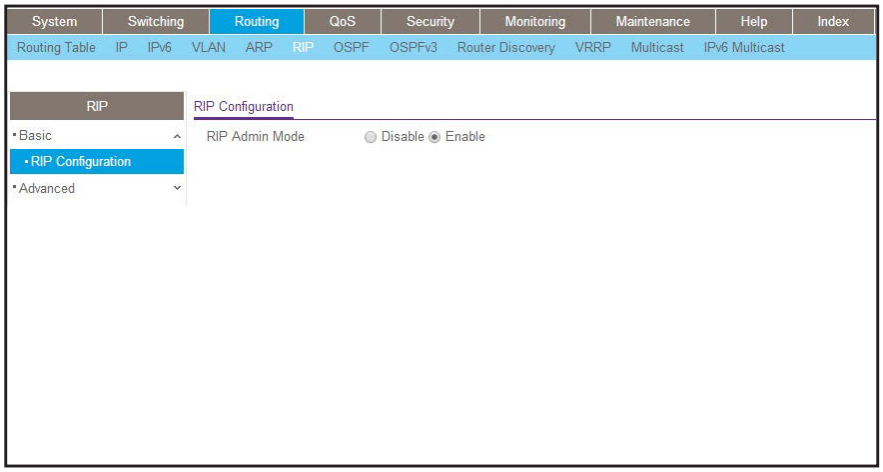
   The T specifies that the egress packet is tagged for the port.

e. Click **Apply** to save the VLAN that includes port 3.

3. Enable RIP on the switch (you can skip this step since the RIP is enabled by default).

   a. Select **Routing > RIP > Basic > RIP Configuration**.

      A screen similar to the following displays.



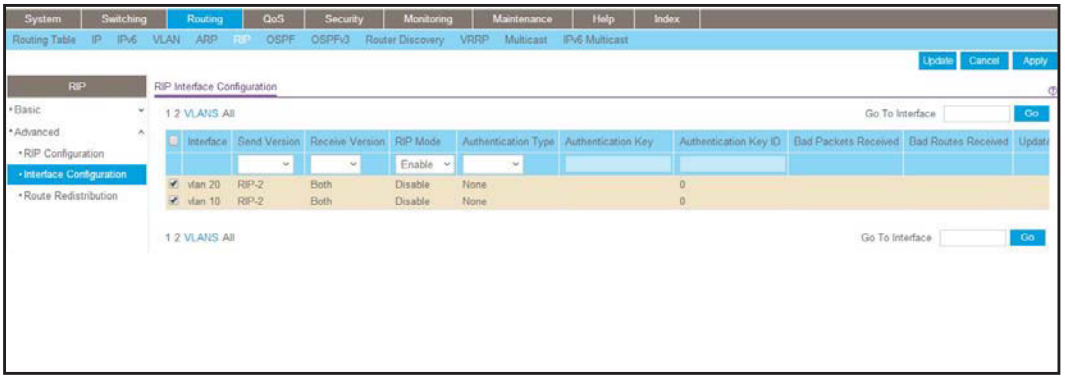
   b. For RIP Admin Mode, select the **Enable** radio button.

   c. Click **Apply** to save the setting.

4. Enable RIP on VLANs 10 and 20.

   a. Select **Routing > RIP > Advanced > RIP Configuration**.

      A screen similar to the following displays.



   b. Click the **VLANS** on the top of table.

c. Scroll down and select the interface **vlan10** and **vlan 20** check boxes.

d. Enter the following information:

For RIP Mode, select the **Enable** radio button.

e. Click **Apply** to save the settings.

OSPF

7

Open Shortest Path First

This chapter includes the following sections:

- *Open Shortest Path First Concepts*
- *Inter-area Router*
- *OSPF on a Border Router*
- *Stub Areas*
- *NSSA Areas*
- *VLAN Routing OSPF*
- *OSPFv3*

Note: OSPF is available on the M4300 series switches only.

Open Shortest Path First Concepts

For larger networks, Open Shortest Path First (OSPF) is generally used in preference to RIP. OSPF offers several benefits to the administrator of a large or complex network:

- Less network traffic:
  - Routing table updates are sent only when a change has occurred.
  - Only the part of the table which has changed is sent.
  - Updates are sent to a multicast, not a broadcast, address.
- Hierarchical management, allowing the network to be subdivided.

The top level of the hierarchy of an OSPF network is known as an autonomous system (AS) or routing domain, and is a collection of networks with a common administration and routing strategy. The AS is divided into areas: Intra-area routing is used when a source and destination address are in the same area, and inter-area routing across an OSPF backbone is used when they are not. An inter-area router communicates with border routers in each of the areas to which it provides connectivity.

The switch operating as a router and running OSPF determines the best route using the assigned cost and the type of the OSPF route. The order for choosing a route if more than one type of route exists is as follows:

- Intra-area.
- Inter-area.
- External type 1: The route is external to the AS.
- External type 2: The route was learned from other protocols such as RIP.

Inter-area Router

The examples in this section show you how to configure the switch first as an inter-area router and then as a border router. They show two areas, each with its own border router connected to one inter-area router.

The following figure shows a network segment with an inter-area router connecting areas 0.0.0.2 and 0.0.0.3. The sample script shows the commands used to configure the switch as the inter-area router in the diagram by enabling OSPF on port 1/0/2 in area 0.0.0.2 and port 1/0/3 in area 0.0.0.3.

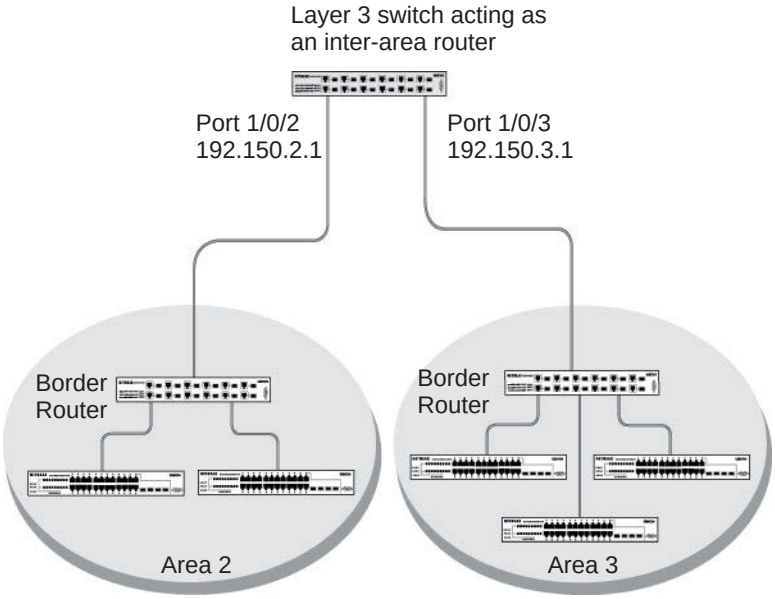


Figure 13. Network segment with an inter-area router connecting areas 0.0.0.2 and 0.0.0.3

CLI: Configure an Inter-area Router

1. Enable routing for the switch.

```
(Netgear Switch) #config
(Netgear Switch) (Config)#ip routing
(Netgear Switch) (Config)#exit
```

2. Assign IP addresses to ports.

```
(Netgear Switch) #config
(Netgear Switch) (Config)#interface 1/0/2
(Netgear Switch) (Interface 1/0/2)#routing
(Netgear Switch) (Interface 1/0/2)#ip address 192.150.2.1 255.255.255.0
(Netgear Switch) (Interface 1/0/2)#exit
(Netgear Switch) (Config)#interface 1/0/3
(Netgear Switch) (Interface 1/0/3)#routing
(Netgear Switch) (Interface 1/0/3)#ip address 192.150.3.1 255.255.255.0
(Netgear Switch) (Interface 1/0/3)#exit
(Netgear Switch) (Config)#exit
```

3. Specify the router ID, and enable OSPF for the switch. Set disable1583 compatibility to prevent a routing loop.

```
(Netgear Switch) #config
(Netgear Switch) (Config)#router ospf
(Netgear Switch) (Config router)#enable
(Netgear Switch) (Config router)#router-id 192.150.9.9
(Netgear Switch) (Config router)#no 1583compatibility
(Netgear Switch) (Config router)#exit
(Netgear Switch) (Config)#exit
```

4. Enable OSPF, and set the OSPF priority and cost for the ports.

```
(Netgear Switch) #config
(Netgear Switch) (Config)#interface 1/0/2
(Netgear Switch) (Interface 1/0/2)#ip ospf
(Netgear Switch) (Interface 1/0/2)#ip ospf areaid 0.0.0.2
(Netgear Switch) (Interface 1/0/2)#ip ospf priority 128
(Netgear Switch) (Interface 1/0/2)#ip ospf cost 32
(Netgear Switch) (Interface 1/0/2)#exit

(Netgear Switch) (Config)#interface 1/0/3
(Netgear Switch) (Interface 1/0/3)#ip ospf
(Netgear Switch) (Interface 1/0/3)#ip ospf areaid 0.0.0.3
(Netgear Switch) (Interface 1/0/3)#ip ospf priority 255
(Netgear Switch) (Interface 1/0/3)#ip ospf cost 64
(Netgear Switch) (Interface 1/0/3)#exit
(Netgear Switch) (Config)#exit
```

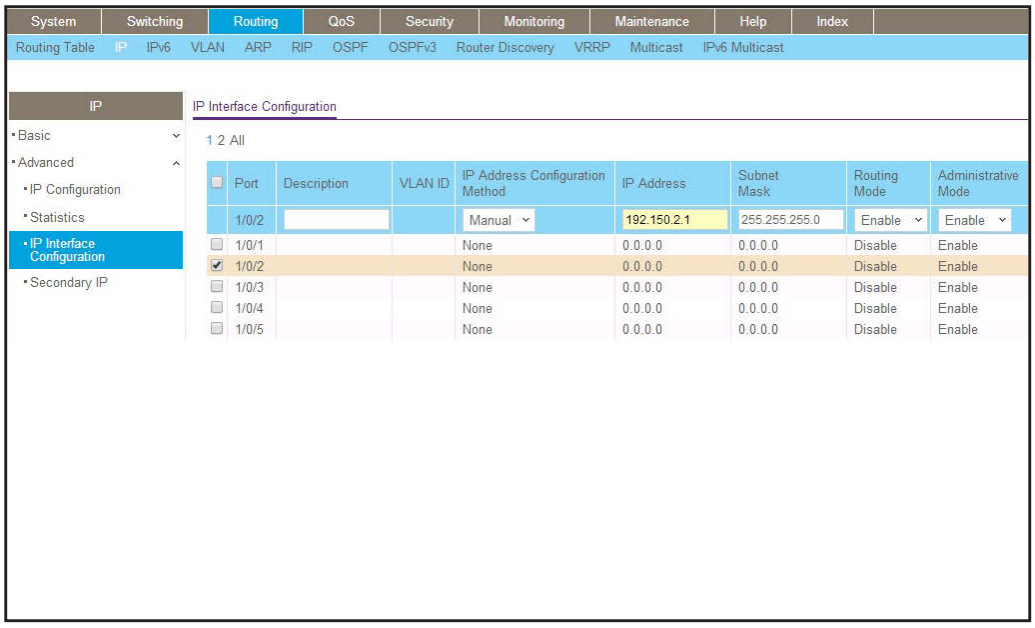
Web Interface: Configure an Inter-area Router

1. Enable IP routing on the switch.
   a. Select **Routing > IP > Basic > IP Configuration**.

      A screen similar to the following displays.

   b. For Routing Mode, select the **Enable** radio button.
   c. Click **Apply** to save the settings.
2. Assign IP address 192.150.2.1 to port 1/0/2.
   a. Select **Routing > IP > Advanced > IP Interface Configuration**.

      A screen similar to the following displays.



   b. Scroll down and select the interface **1/0/2** check box.

      Now 1/0/2 appears in the Interface field at the top.

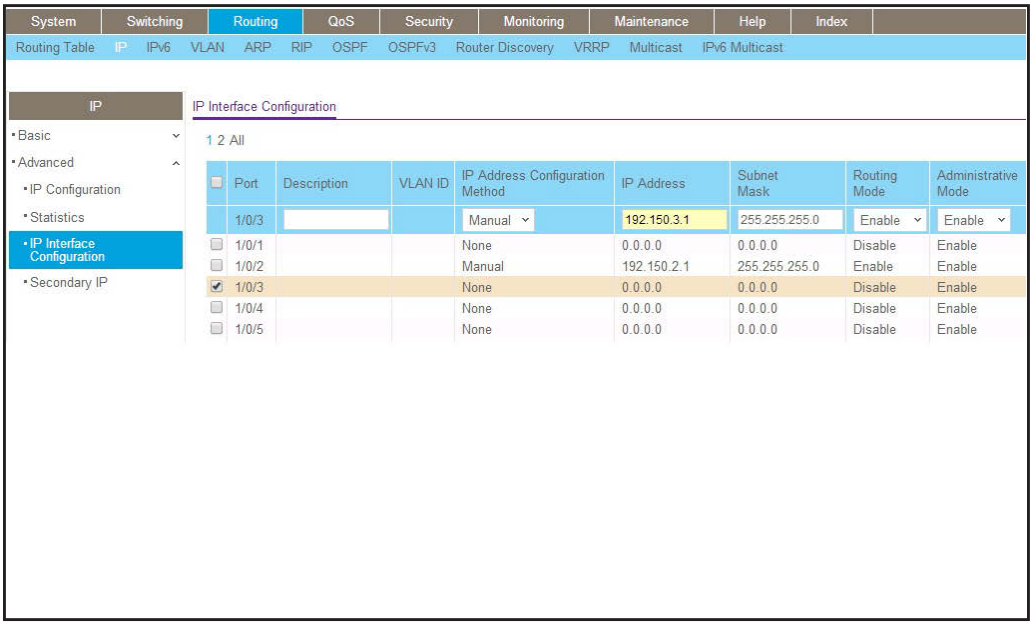
c. Enter the following information:
   - In the **IP Address** field, enter **192.150.2.1**.
   - In the **Subnet Mask** field, enter **255.255.255.0**.
   - In the **Administrative Mode** field, select **Enable**.

d. Click **Apply** to save the settings.

3. Assign IP address 192.150.3.1 to port 1/0/3:

a. Select **Routing > IP > Advanced > IP Interface Configuration**.

A screen similar to the following displays.



b. Scroll down and select the interface **1/0/3** check box.

Now 1/0/3 appears in the Interface field at the top.

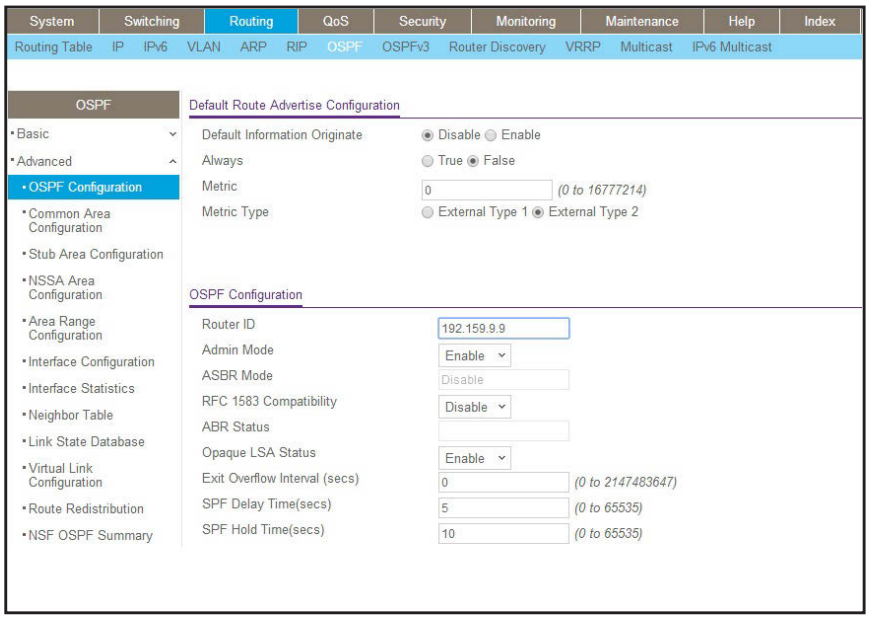
c. Enter the following information:
   - In the **IP Address** field, enter **192.150.3.1**.
   - In the **Network Mask** field, enter **255.255.255.0**.
   - In the **Administrative Mode** field, select **Enable**.

d. Click **Apply** to save the settings.

4. Specify the router ID, and enable OSPF for the switch.

a. Select **Routing > OSPF > Advanced > OSPF Configuration**.

A screen similar to the following displays.



b. Under OSPF Configuration, enter the following information:

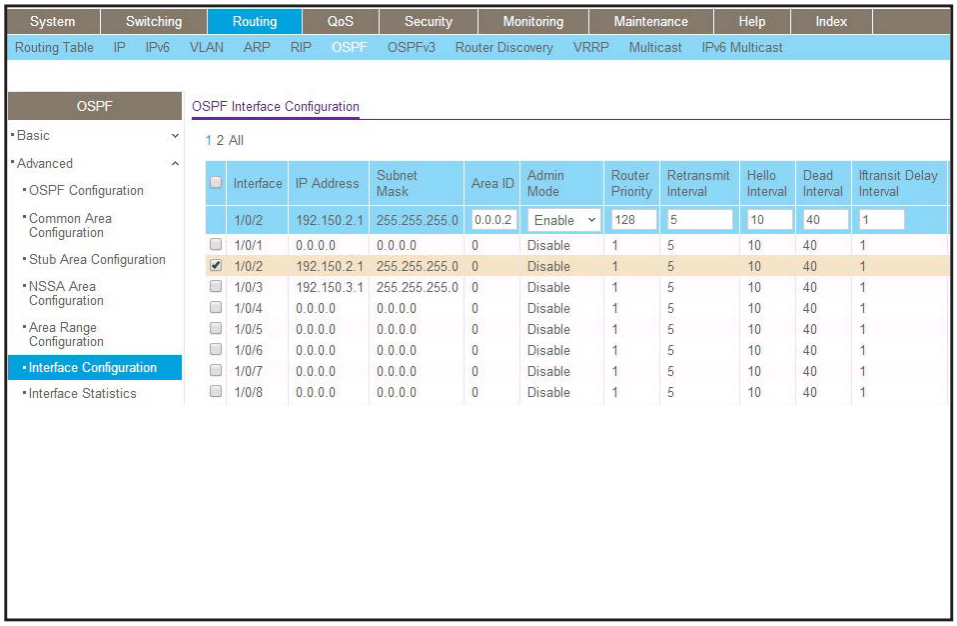
- In the **Router ID** field, enter **192.150.9.9**.
- In the **OSPF Admin Mode** field, select **Enable**.
- In the **RFC 1583 Compatibility** field, select **Disable**.

c. Click **Apply** to save the settings.

5. Enable OSPF on port 1/0/2.

a. Select **Routing > OSPF > Advanced > Interface Configuration**.

A screen similar to the following displays.



b. Scroll down and select the interface **1/0/2** check box.

Now 1/0/2 appears in the Interface field at the top.

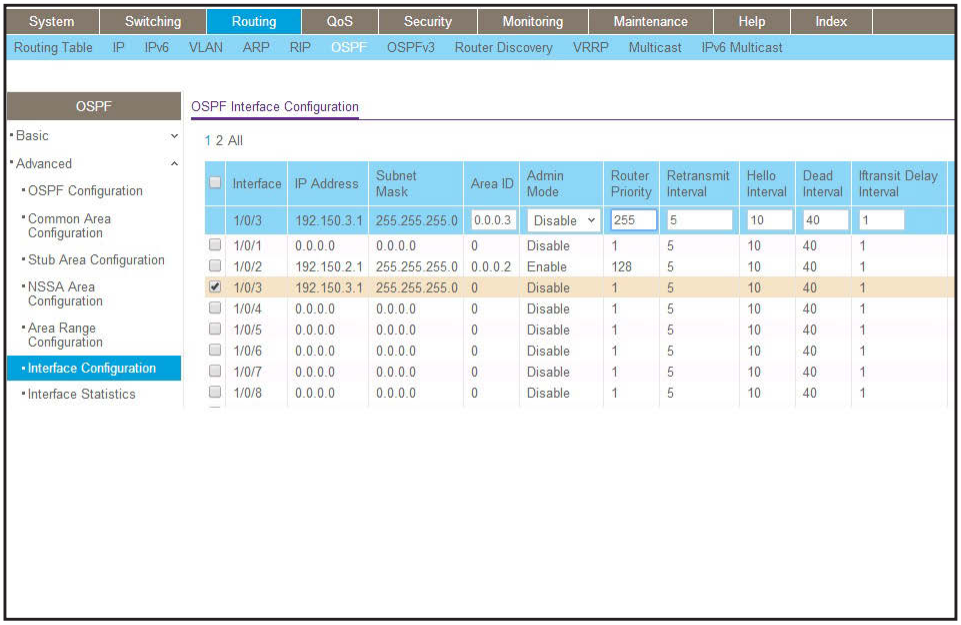
- In the **OSPF Area ID** field, enter **0.0.0.2**.
- In the **OSPF Admin Mode** field, select **Enable**.
- In the **Priority** field, enter **128**.
- In the **Metric Cost** field, enter **32**.

c. Click **Apply** to save the settings.

6. Enable OSPF on port 1/0/3.

a. Select **Routing > OSPF > Advanced > Interface Configuration**.

A screen similar to the following displays.



b. Scroll down and select the interface **1/0/3** check box.

Now 1/0/3 appears in the Interface field at the top.

- In the **OSPF Area ID** field, enter **0.0.0.3**.
- In the **OSPF Admin Mode** field, select **Enable**.
- In the **Priority** field, enter **255**.
- In the **Metric Cost** field, enter **64**.

c. Click **Apply** to save the settings.

OSPF on a Border Router

The example is shown as CLI commands and as a web interface procedure. For an OSPF sample network, see *Figure 13* on page 102.

CLI: Configure OSPF on a Border Router

1. Enable routing for the switch.

```
(Netgear Switch) #config
(Netgear Switch) (Config)#ip routing
```

2. Enable routing and assign IPs for ports 1/0/2, 1/0/3, and 1/0/4.

```
(Netgear Switch) (Config)#interface 1/0/2
(Netgear Switch) (Interface 1/0/2)#routing
(Netgear Switch) (Interface 1/0/2)#ip address 192.150.2.2 255.255.255.0
(Netgear Switch) (Interface 1/0/2)#exit
(Netgear Switch) (Config)#interface 1/0/3
(Netgear Switch) (Interface 1/0/3)#routing
(Netgear Switch) (Interface 1/0/3)#ip address 192.130.3.1 255.255.255.0
(Netgear Switch) (Interface 1/0/3)#exit
(Netgear Switch) (Config)#interface 1/0/4
(Netgear Switch) (Interface 1/0/4)#routing
(Netgear Switch) (Interface 1/0/4)#ip address 192.64.4.1 255.255.255.0
(Netgear Switch) (Interface 1/0/4)#exit
```

3. Specify the router ID, and enable OSPF for the switch.

   Set disable 1583compatibility to prevent a routing loop.

```
(Netgear Switch) (Config)#router ospf
(Netgear Switch) (Config router)#enable
(Netgear Switch) (Config router)#router-id 192.130.1.1
(Netgear Switch) (Config router)#no 1583compatibility
(Netgear Switch) (Config router)#exit
(Netgear Switch) (Config)#exit
```

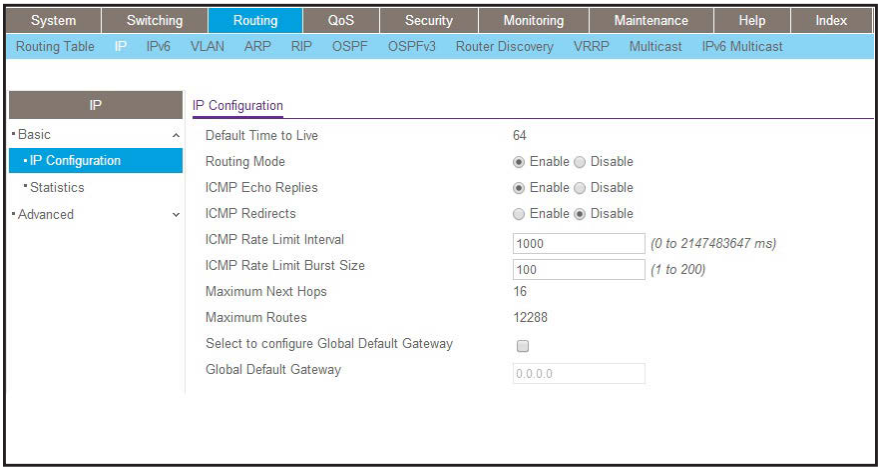
4. Enable OSPF for the ports, and set the OSPF priority and cost for the ports.

```
(Netgear Switch) #config
(Netgear Switch) (Config)#interface 1/0/2
(Netgear Switch) (Interface 1/0/2)#ip ospf
(Netgear Switch) (Interface 1/0/2)#ip ospf areaid 0.0.0.2
(Netgear Switch) (Interface 1/0/2)#ip ospf priority 128
(Netgear Switch) (Interface 1/0/2)#ip ospf cost 32
(Netgear Switch) (Interface 1/0/2)#exit

(Netgear Switch) (Config)#interface 1/0/3
(Netgear Switch) (Interface 1/0/3)#ip ospf
(Netgear Switch) (Interface 1/0/3)#ip ospf areaid 0.0.0.2
(Netgear Switch) (Interface 1/0/3)#ip ospf priority 255
(Netgear Switch) (Interface 1/0/3)#ip ospf cost 64
(Netgear Switch) (Interface 1/0/3)#exit

(Netgear Switch) (Config)#interface 1/0/4
(Netgear Switch) (Interface 1/0/4)#ip ospf
(Netgear Switch) (Interface 1/0/4)#ip ospf areaid 0.0.0.2
(Netgear Switch) (Interface 1/0/4)#ip ospf priority 255
(Netgear Switch) (Interface 1/0/4)#ip ospf cost 64
(Netgear Switch) (Interface 1/0/4)#exit
(Netgear Switch) (Config)#exit
```

Web Interface: Configure OSPF on a Border Router

1. Enable IP routing on the switch.
   a. Select **Routing > IP > Basic > IP Configuration**.

      A screen similar to the following displays.



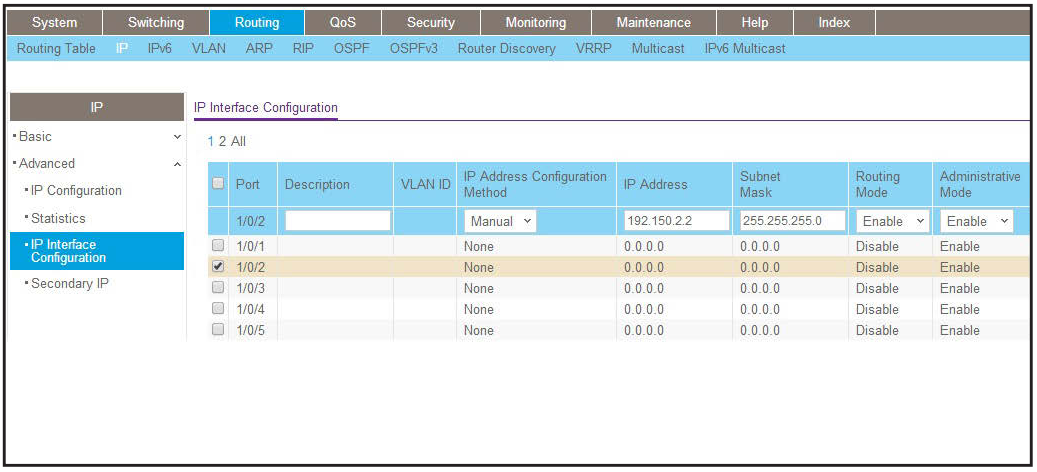
   b. For Routing Mode, select the **Enable** radio button.

c. Click **Apply** to save the settings.

2. Assign IP address 192.150.2.2 to port 1/0/2.

a. Select **Routing > IP > Advanced > IP Interface Configuration**.

A screen similar to the following displays.



b. Scroll down and select the interface **1/0/2** check box.

Now 1/0/2 appears in the Interface field at the top.

c. Enter the following information:

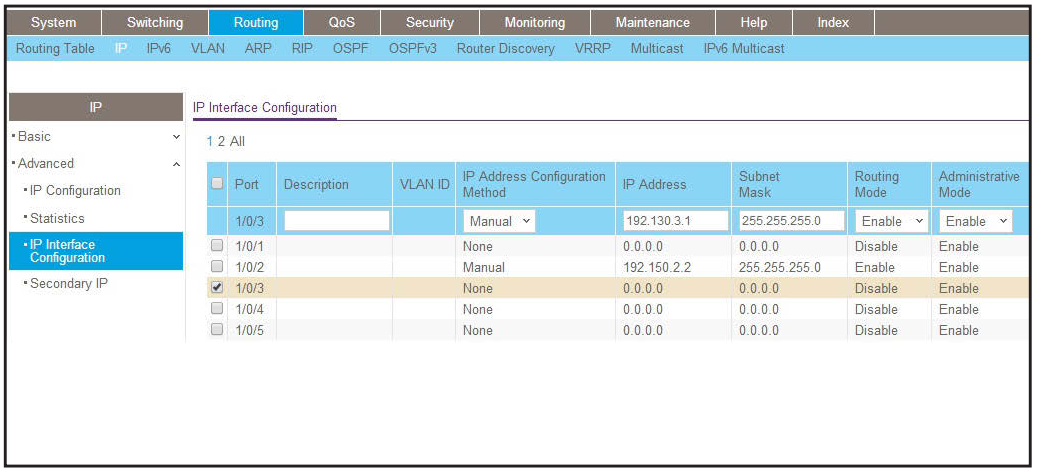
- In the **IP Address Configuration Method** field, select **Manual**.
- In the **IP Address** field, enter **192.150.2.2**.
- In the **Network Mask** field, enter **255.255.255.0**.
- In the **Admin Mode** field, select **Enable**.

d. Click **Apply** to save the settings.

3. Assign IP address 192.130.3.1 to port 1/0/3:

a. Select **Routing > IP > Advanced > IP Interface Configuration**.

A screen similar to the following displays.



b. Scroll down and select the interface **1/0/3** check box.

   Now 1/0/3 appears in the Interface field at the top.

c. Enter the following information:

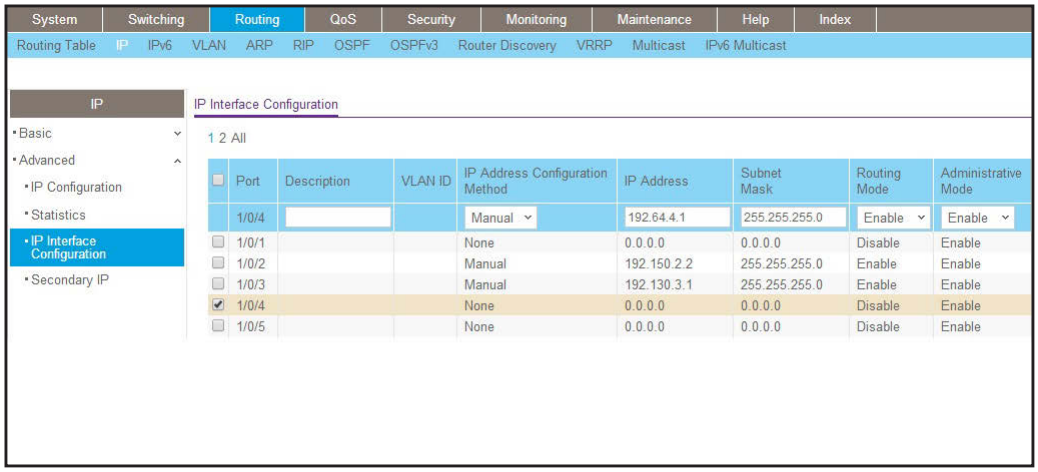
   - In the **IP Address Configuration Method** field, select **Manual**.
   - In the **IP Address** field, enter **192.130.3.1**.
   - In the **Network Mask** field, enter **255.255.255.0**.
   - In the **Admin Mode** field, select **Enable**.

d. Click **Apply** to save the settings.

4. Assign IP address 192.64.4.1 to port 1/0/4.

a. Select **Routing > IP > Advanced > IP Interface Configuration**.

   A screen similar to the following displays.



b. Scroll down and select the interface **1/0/4** check box. Now 1/0/4 appears in the Interface field at the top.

c. Enter the following information:

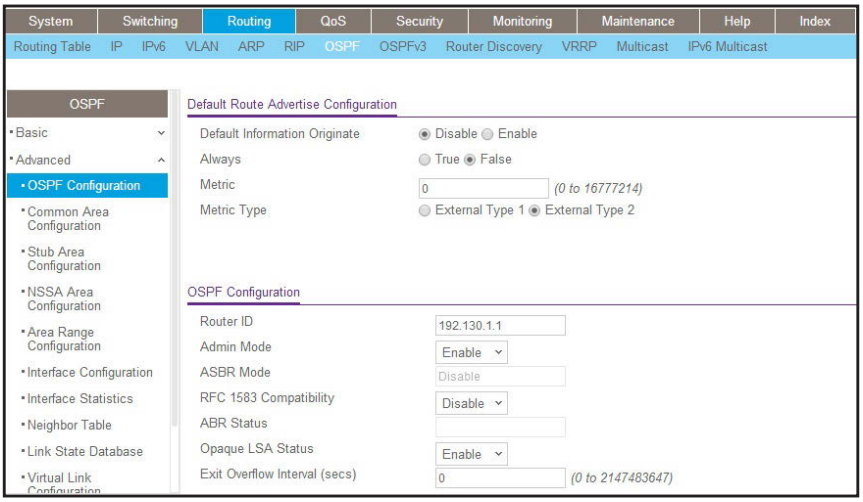
   - In the **IP Address Configuration Method** field, select **Manual**.
   - In the **IP Address** field, enter **192.64.4.1**.
   - In the **Network Mask** field, enter **255.255.255.0**.
   - In the **Admin Mode** field, select **Enable**.

d. Click **Apply** to save the settings.

5. Specify the router ID, and enable OSPF for the switch.

a. Select **Routing > OSPF > Advanced > OSPF Configuration**.

A screen similar to the following displays.



b. Under OSPF Configuration, enter the following information:

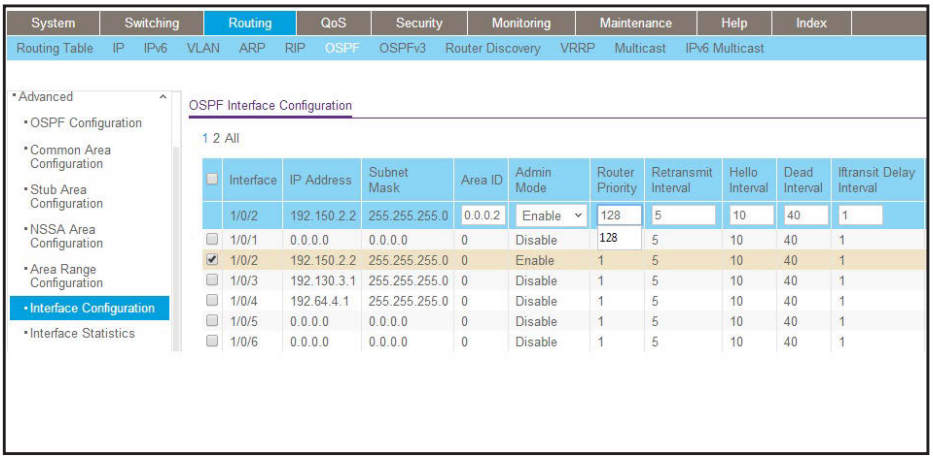
- In the **Router ID** field, enter **192.130.1.1**.
- In the **OSPF Admin Mode** field, select **Enable**.
- In the **RFC 1583 Compatibility** field, select **Disable**.

c. Click **Apply** to save the settings.

6. Enable OSPF on the port 1/0/2.

a. Select **Routing > OSPF > Advanced > Interface Configuration**.

A screen similar to the following displays.



b. Under Interface Configuration, scroll down and select the interface **1/0/2** check box.

Now 1/0/2 appears in the Interface field at the top.

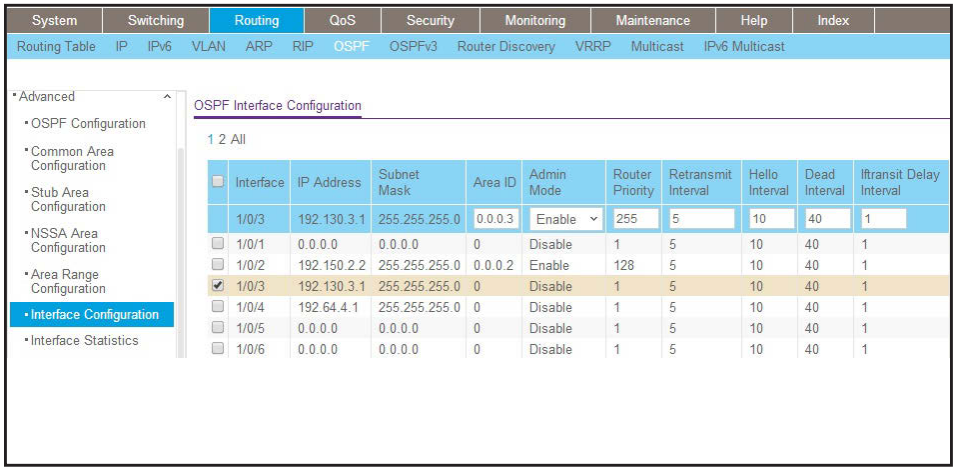
- In the **OSPF Area ID** field, enter **0.0.0.2**.
- In the **OSPF Admin Mode** field, select **Enable**.
- In the **Router Priority (0 to 255)** field, enter **128**.
- In the **Metric Cost** field, enter **32**.

c. Click **Apply** to save the settings.

7. Enable OSPF on port 1/0/3.

a. Select **Routing > OSPF > Advanced > Interface Configuration**.

A screen similar to the following displays.



b. Under Interface Configuration, scroll down and select the interface **1/0/3** check box.

Now 1/0/3 appears in the Interface field at the top.

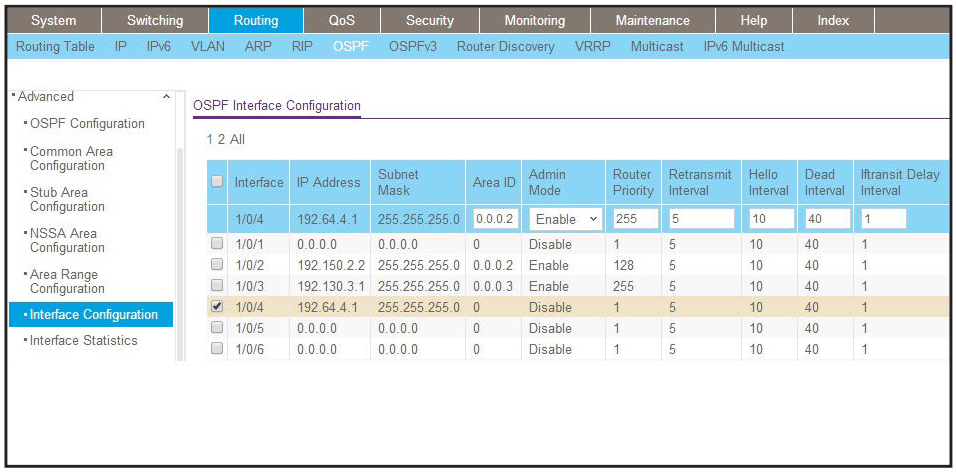
- In the **OSPF Area ID** field, enter **0.0.0.3**.
- In the **OSPF Admin Mode** field, select **Enable**.
- In the **Priority** field, enter **255**.
- In the **Metric Cost** field, enter **64**.

c. Click **Apply** to save the settings.

8. Enable OSPF on port 1/0/4.

a. Select **Routing > OSPF > Advanced > Interface Configuration**.

A screen similar to the following displays.



b. Under Interface Configuration, scroll down and select the interface **1/0/4** check box.

Now 1/0/4 appears in the Interface field at the top.

- In the **OSPF Area ID** field, enter **0.0.0.2**.
- In the **OSPF Admin Mode** field, select the **Enable**.
- In the **Priority** field, enter **255**.
- In the **Metric Cost** field, enter **64**.

c. Click **Apply** to save the settings.

Stub Areas

The example is shown as CLI commands and as a web interface procedure.

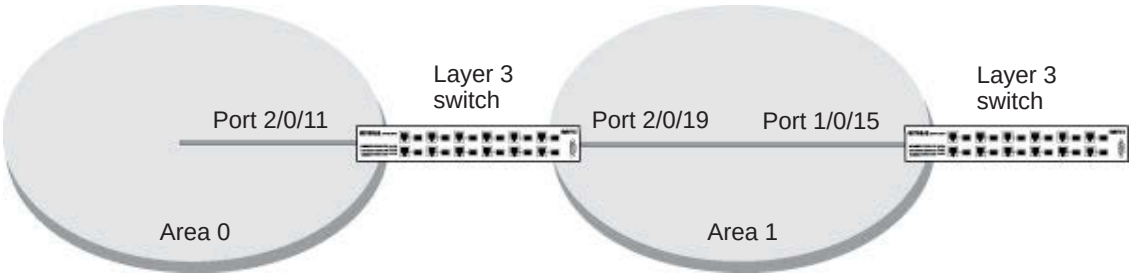


Figure 14. Area 1 is a stub area

CLI: Configure Area 1 as a Stub Area on A1

1. Enable routing on the switch.

```
(Netgear Switch) #config
(Netgear Switch) (Config)#ip routing
```

2. Set the router ID to 1.1.1.1.

```
(Netgear Switch) (Config)#router ospf
(Netgear Switch) (Config-router)#router-id 1.1.1.1
```

3. Configure area 0.0.0.1 as a stub area.

```
(Netgear Switch) (Config-router)#area 0.0.0.1 stub
```

4. Switch A injects a default route only to area 0.0.0.1.

```
(Netgear Switch) (Config-router)#no area 0.0.0.1 stub summarylsa
(Netgear Switch) (Config-router)#exit
```

5. Enable OSPF area 0 on ports 2/0/11.

```
(Netgear Switch) (Config)#interface 2/0/11
(Netgear Switch) (Interface 2/0/11)#routing
(Netgear Switch) (Interface 2/0/11)#ip address 192.168.10.1 255.255.255.0
(Netgear Switch) (Interface 2/0/11)#ip ospf
(Netgear Switch) (Interface 2/0/11)#exit
```

6. Enable OSPF area 0.0.0.1 on 2/0/19.

```
(Netgear Switch) (Config)#interface 2/0/19
(Netgear Switch) (Interface 2/0/19)#routing
(Netgear Switch) (Interface 2/0/19)#ip address 192.168.20.1 255.255.255.0
(Netgear Switch) (Interface 2/0/19)#ip ospf
(Netgear Switch) (Interface 2/0/19)#ip ospf areaid 0.0.0.1
(Netgear Switch) (Interface 2/0/19)#exit
```

```
(Netgear Switch) (Config)#ex
(Netgear Switch) #show ip ospf neighbor interface all
  Router ID       IP Address    Neighbor Interface    State
---------------   -----------   ------------------   ---------
4.4.4.4           192.168.10.2       2/0/11          Full
2.2.2.2           192.168.20.2       2/0/19          Full
(Netgear Switch) #show ip route
Total Number of Routes..................... 4
   Network          Subnet                   Next Hop     Next Hop
   Address           Mask         Protocol     Intf       IP Address
-------------- -------------- -----------  ---------  ---------------
14.1.1.0       255.255.255.0   OSPF Inter    2/0/11     192.168.10.2
14.1.2.0       255.255.255.0   OSPF Inter    2/0/11     192.168.10.2
192.168.10.0   255.255.255.0   Local         2/0/11     192.168.10.1
192.168.20.0   255.255.255.0   Local         2/0/19     192.168.20.1
```

Web Interface: Configure Area 1 as a Stub Area on A1

1. Enable IP routing on the switch.
   a. Select **Routing > IP > Basic > IP Configuration**.

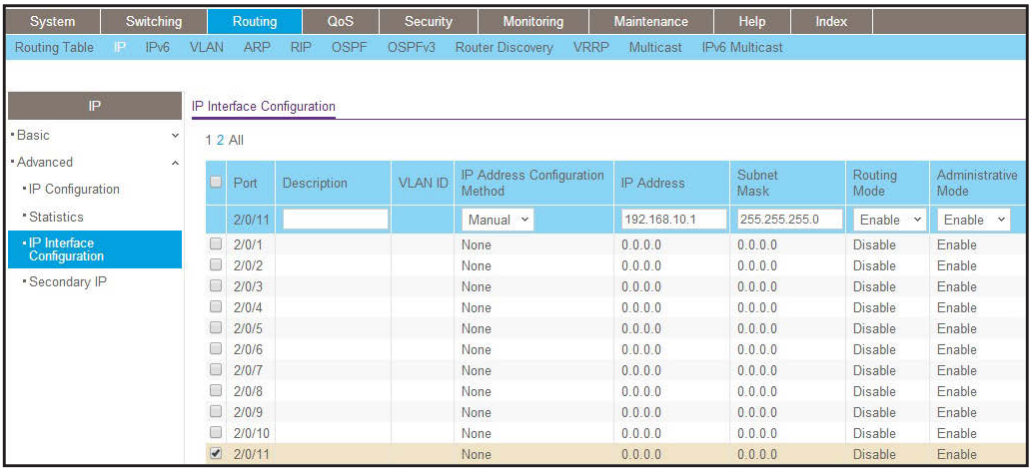
      A screen similar to the following displays.

   b. For Routing Mode, select the **Enable** radio button.

   c. Click **Apply** to save the settings.

2. Assign IP address 192.168.10.1 to port 2/0/11.
   a. Select **Routing > IP > Advanced > IP Interface Configuration**.

      A screen similar to the following displays.



   b. Scroll down and select the interface **2/0/11** check box.

      Now 2/0/11 appears in the Interface field at the top.

   c. Enter the following information:
      - In the **IP Address Configuration Method** field, select **Manual**.
      - In the **IP Address** field, enter **192.168.10.1**.

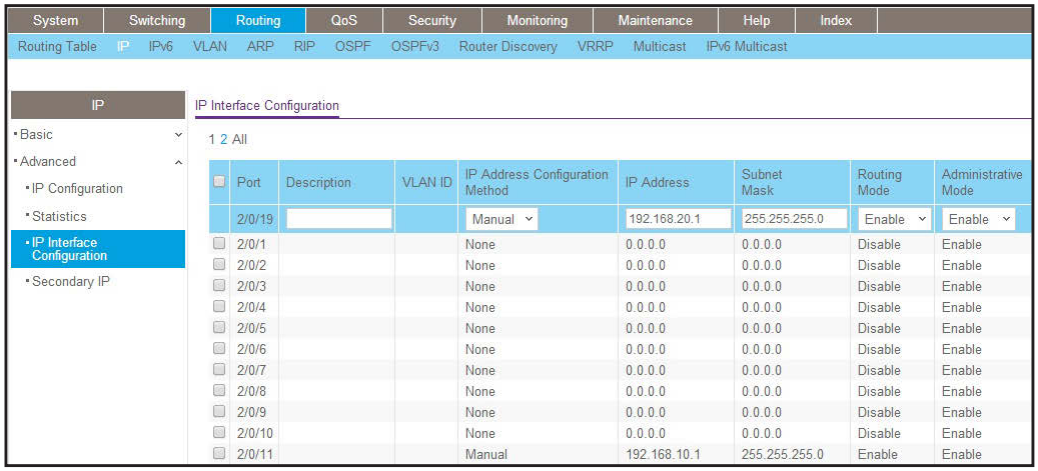
- In the **Network Mask** field, enter **255.255.255.0**.
- In the **Admin Mode** field, select **Enable**.

d. Click **Apply** to save the settings.

3. Assign IP address 192.168.20.1 to port 2/0/19:

a. Select **Routing > IP > Advanced > IP Interface Configuration**.

A screen similar to the following displays.



b. Scroll down and select the interface **2/0/19** check box.

Now 2/0/19 appears in the Interface field at the top.

c. Enter the following information:

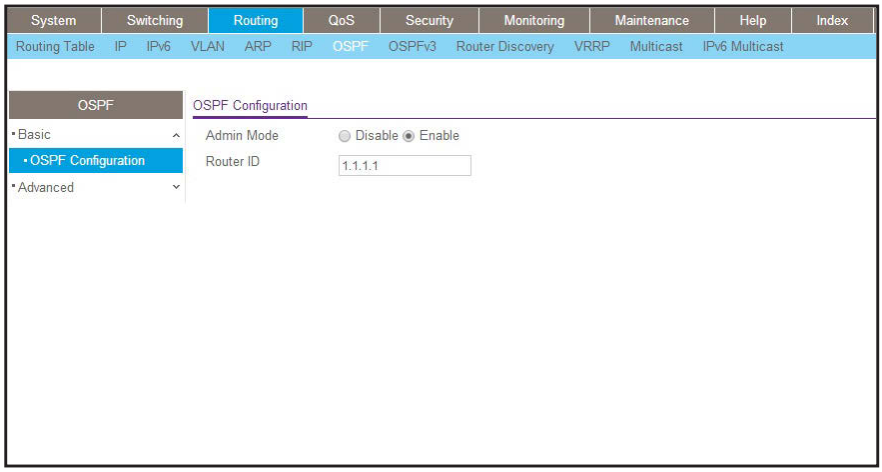
- In the **IP Address Configuration Method** field, select **Manual**.
- In the **IP Address** field, enter **192.168.20.1**.
- In the **Network Mask** field, enter **255.255.255.0**.
- In the **Admin Mode** field, select **Enable**.

d. Click **Apply** to save the settings.

4. Specify the router ID, and enable OSPF for the switch.

a. Select **Routing > OSPF > Basic > OSPF Configuration**.

A screen similar to the following displays.



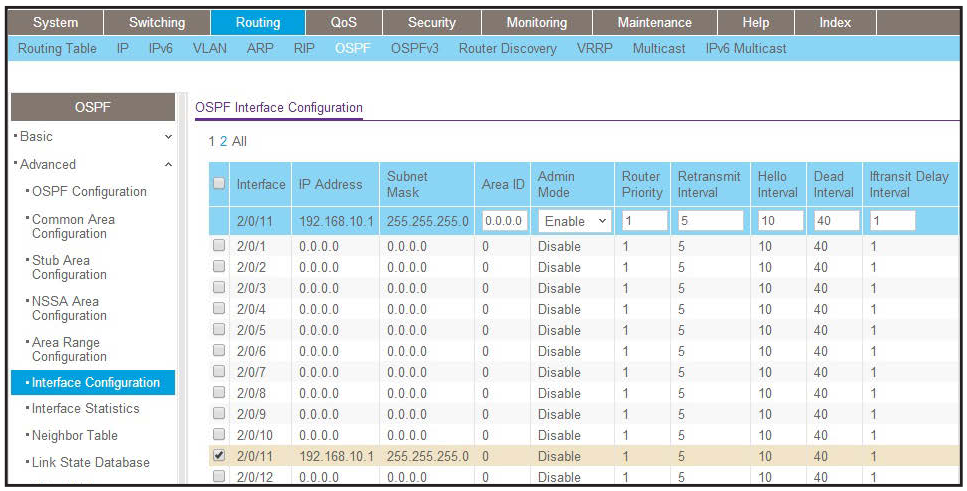
b. Under OSPF Configuration, in the **Router ID** field, enter **1.1.1.1**.

c. Click **Apply** to save the settings.

5. Enable OSPF on the port 2/0/11.

a. Select **Routing > OSPF > Advanced > Interface Configuration**.

A screen similar to the following displays.



b. Under Interface Configuration, scroll down and select the interface **2/0/11** check box.

Now 2/0/11 appears in the Interface field at the top.

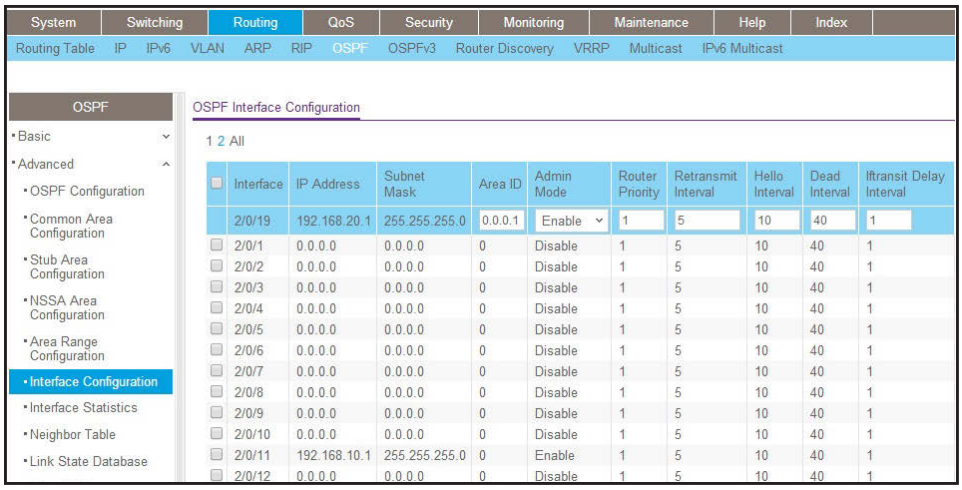
- In the **OSPF Area ID** field, enter **0.0.0.0**.
- In the **Admin Mode** field, select **Enable**.

c. Click **Apply** to save the settings.

6. Enable OSPF on the port 2/0/19.

a. Select **Routing > OSPF > Advanced > Interface Configuration**.

A screen similar to the following displays.



b. Under Interface Configuration, scroll down and select the interface **2/0/19** check box.

Now 2/0/19 appears in the Interface field at the top.

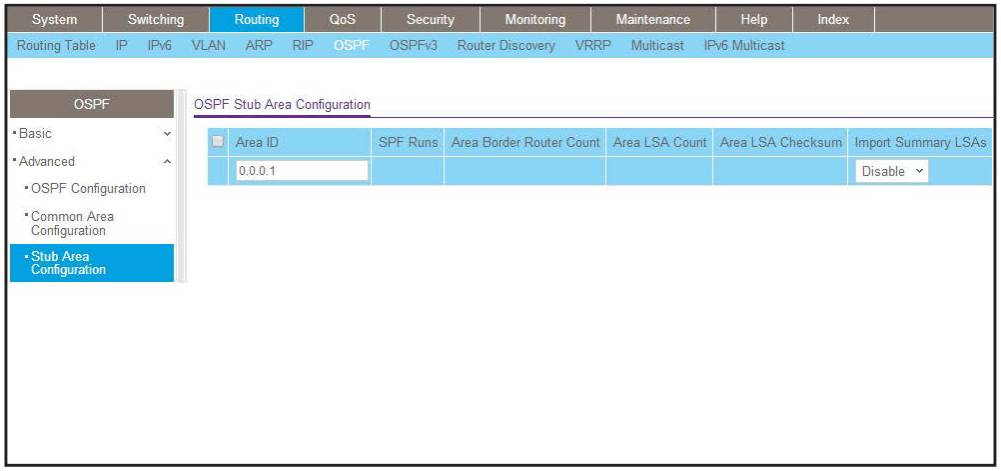
- In the **OSPF Area ID** field, enter **0.0.0.1**.
- In the **OSPF Admin Mode** field, select **Enable**.

c. Click **Apply** to save the settings.

7. Configure area 0.0.0.1 as a stub area.

a. Select **Routing > OSPF > Advanced > Stub Area Configuration**.

A screen similar to the following displays.



b. Enter the following information:

- In the **Area ID** field, enter **0.0.0.1**.
- In the **Import Summary LSAs** field, select **Disable**.

c. Click **Add** to save the settings.

CLI: Configure Area 1 as a Stub Area on A2

1. Enable routing on the switch.

```
(Netgear Switch) #config
(Netgear Switch) (Config)#ip routing
(Netgear Switch) (Config)#router ospf
```

2. Set the router ID to 2.2.2.2.

```
(Netgear Switch) (Config-router)#router-id 2.2.2.2
```

3. Configure area 0.0.0.1 as a stub area.

```
(Netgear Switch) (Config-router)#area 0.0.0.1 stub
```

4. Enable OSPF area 0.0.0.1 on the 1/0/15.

```
(Netgear Switch) (Config-router)#exit
(Netgear Switch) (Config-router)#exit
(Netgear Switch) (Config)#interface 1/0/15
(Netgear Switch) (Interface 1/0/15)#routing
(Netgear Switch) (Interface 1/0/15)#ip address 192.168.20.2  255.255.255.0
(Netgear Switch) (Interface 1/0/15)#ip ospf
(Netgear Switch) (Interface 1/0/15)#ip ospf areaid 0.0.0.1

(Netgear Switch) (Interface 1/0/15)#exit
(Netgear Switch) (Config)#exit
(Netgear Switch) #show ip route

Total Number of Routes..................... 2

   Network          Subnet                   Next Hop     Next Hop
   Address           Mask         Protocol     Intf       IP Address
--------------- --------------- ------------  ---------  ---------------
0.0.0.0         0.0.0.0         OSPF Inter    1/0/15     192.168.20.1
192.168.20.0    255.255.255.0   Local         1/0/15     192.168.20.2
```

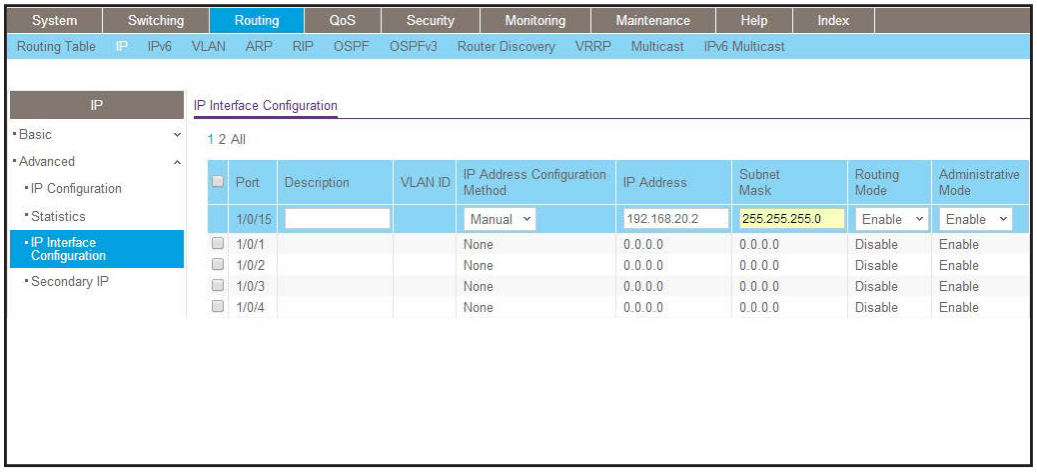
Web Interface: Configure Area 1 as a Stub Area on A2

1. Enable IP routing on the switch.
   a. Select **Routing > IP > Basic > IP Configuration**.

      A screen similar to the following displays.

   b. For Routing Mode, select the **Enable** radio button.
   c. Click **Apply** to save the settings.
2. Assign IP address 192.168.10.1 to port 1/0/15.
   a. Select **Routing > IP > Advanced > IP Interface Configuration**.

      A screen similar to the following displays.



   b. Scroll down and select the interface **1/0/15** check box.

      Now 1/0/15 appears in the Interface field at the top.

   c. Enter the following information:
      - In the **IP Address Configuration Method** field, select **Manual**.
      - In the **IP Address** field, enter **192.168.20.2**.

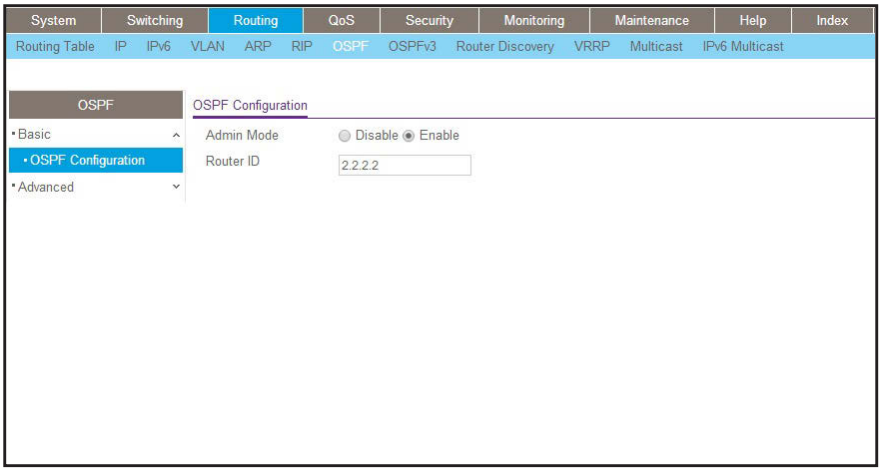
- In the **Network Mask** field, enter **255.255.255.0**.
- In the **Admin Mode** field, select **Enable**.

d. Click **Apply** to save the settings.

3. Specify the router ID, and enable OSPF for the switch.

a. Select **Routing > OSPF > Basic > OSPF Configuration**.

A screen similar to the following displays.



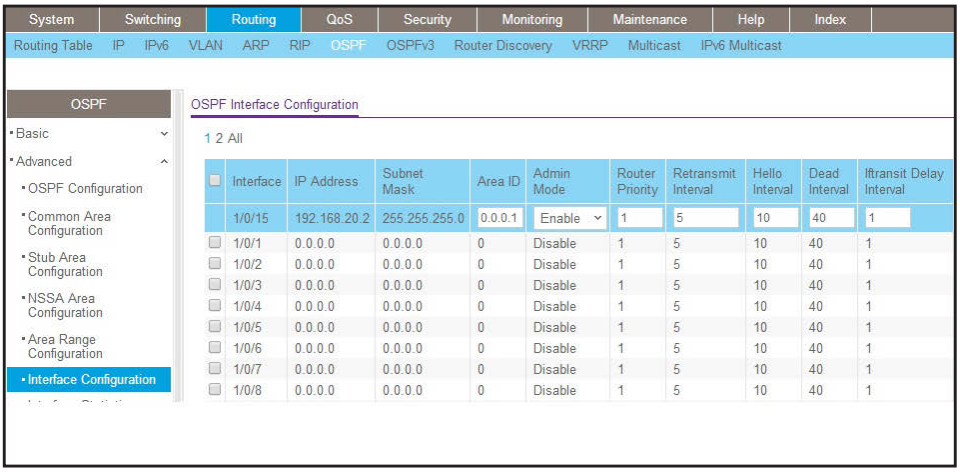
b. In the **Router ID** field, enter **2.2.2.2**.

c. Click **Apply** to save the settings.

4. Enable OSPF on port 1/0/15.

a. Select **Routing > OSPF > Advanced > Interface Configuration**.

A screen similar to the following displays.



b. Under Interface Configuration, scroll down and select the interface **1/0/15** check box.

Now 1/0/15 appears in the Interface field at the top.

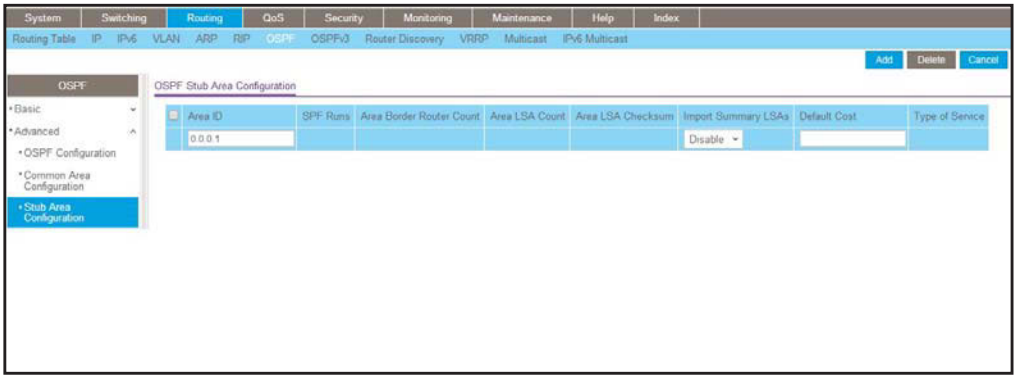
- In the **OSPF Area ID** field, enter **0.0.0.1**.
- In the **OSPF Admin Mode** field, select **Enable**.

c. Click **Apply** to save the settings.

5. Configure area 0.0.0.1 as a stub area.

a. Select **Routing > OSPF > Advanced > Stub Area Configuration**.

A screen similar to the following displays.



b. In the **Area ID** field, enter **0.0.0.1**.

c. Click **Add** to save the settings.

NSSA Areas

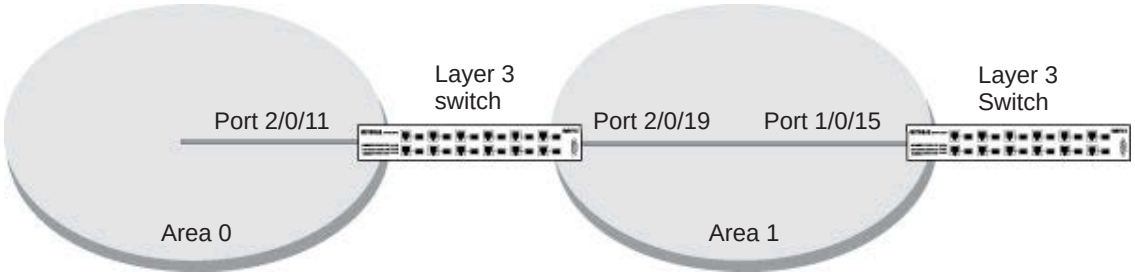


Figure 15. NSSA area

The example is shown as CLI commands and as a web interface procedure.

CLI: Configure Area 1 as an NSSA Area

1. Enable routing on the switch.

```
(Netgear Switch) #config
(Netgear Switch) (Config)#router ospf
(Netgear Switch) (Config)#ip routing
```

2. Configure area 0.0.0.1 as an NSSA area.

```
(Netgear Switch) (Config)#router ospf
(Netgear Switch) (Config-router)#router-id 1.1.1.1
(Netgear Switch) (Config-router)#area 0.0.0.1 nssa
```

3. Stop importing summary LSAs to area 0.0.0.1.

```
(Netgear Switch) (Config-router)#area 0.0.0.1 nssa no-summary
```

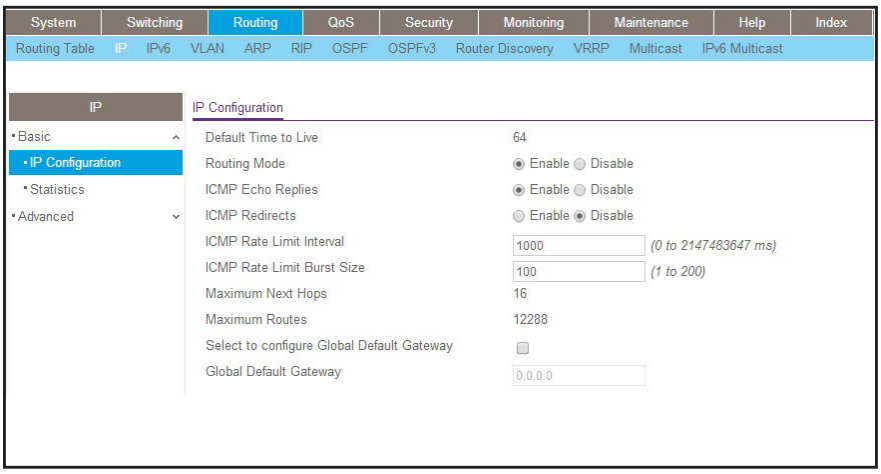
4. Enable area 0.0.0.1 on port 2/0/19.

```
(Netgear Switch) (Config-router)#exit
(Netgear Switch) (Config)#interface 2/0/11
(Netgear Switch) (Interface 2/0/11)#routing
(Netgear Switch) (Interface 2/0/11)#ip address 192.168.10.1 255.255.255.0
(Netgear Switch) (Interface 2/0/11)#ip ospf
(Netgear Switch) (Interface 2/0/11)#exit
(Netgear Switch) (Config)#interface 2/0/19
(Netgear Switch) (Interface 2/0/19)#routing
(Netgear Switch) (Interface 2/0/19)#ip address 192.168.20.1 255.255.255.0
(Netgear Switch) (Interface 2/0/19)#ip ospf
(Netgear Switch) (Interface 2/0/19)#ip ospf areaid 0.0.0.1

(Netgear Switch) (Interface 2/0/19)#exit
(Netgear Switch) (Config)#exit
(Netgear Switch) #show ip route
Total Number of Routes..... 2
   Network          Subnet                    Next Hop     Next Hop
   Address           Mask         Protocol     Intf       IP Address
--------------- --------------- ------------  ---------  ---------------
 14.1.1.0        255.255.255.0   OSPF Inter    2/0/11     192.168.10.2
14.1.2.0        255.255.255.0   OSPF Inter    2/0/11     192.168.10.2
192.168.10.0    255.255.255.0   Local         2/0/11     192.168.10.1
192.168.20.0    255.255.255.0   Local         2/0/19     192.168.20.1
192.168.40.0    255.255.255.0   OSPF NSSA T2  2/0/19     192.168.20.2
192.168.41.0    255.255.255.0   OSPF NSSA T2  2/0/19     192.168.20.2
192.168.42.0    255.255.255.0   OSPF NSSA T2  2/0/19     192.168.20.2
```

Web Interface: Configure Area 1 as an NSSA Area on A1

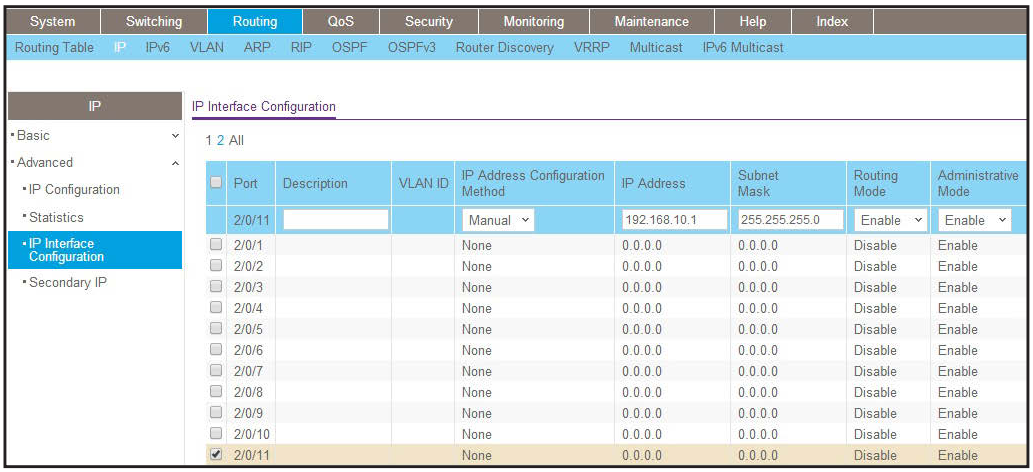
1. Enable IP routing on the switch.
   a. Select **Routing > IP > Basic > IP Configuration**.

      A screen similar to the following displays.



   b. For Routing Mode, select the **Enable** radio button.
   c. Click **Apply** to save the settings.
2. Assign IP address 192.168.10.1 to port 2/0/11.
   a. Select **Routing > IP > Advanced > IP Interface Configuration**.

      A screen similar to the following displays.



   b. Scroll down and select the interface **2/0/11** check box.

      Now 2/0/11 appears in the Interface field at the top.

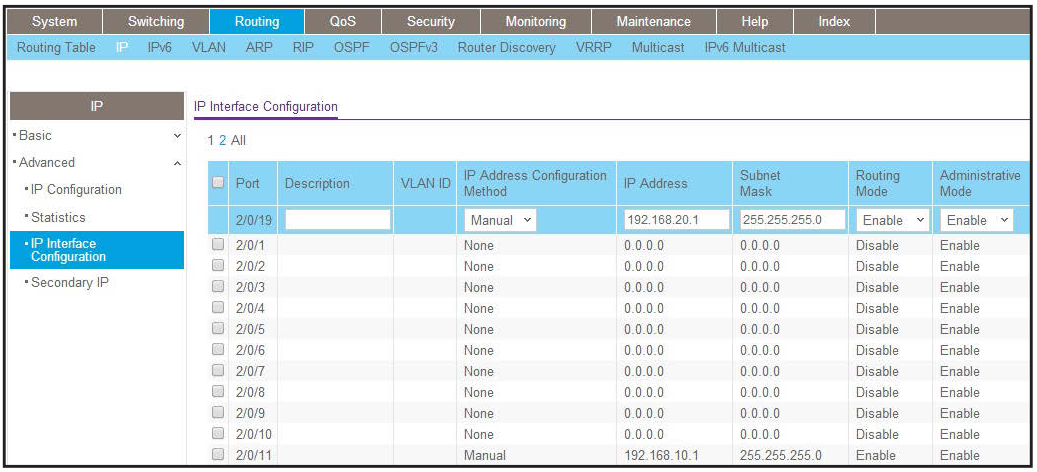
   c. Enter the following information:
      - In the **IP Address** field, enter **192.168.10.1**.
      - In the **Network Mask** field, enter **255.255.255.0**.
      - In the **Admin Mode** field, select **Enable**.

d. Click **Apply** to save the settings.

3. Assign IP address 192.168.20.1 to port 2/0/19.

a. Select **Routing > IP > Advanced > IP Interface Configuration**.

A screen similar to the following displays.



b. Scroll down and select the interface **2/0/19** check box.

Now 2/0/19 appears in the Interface field at the top.

c. Enter the following information:

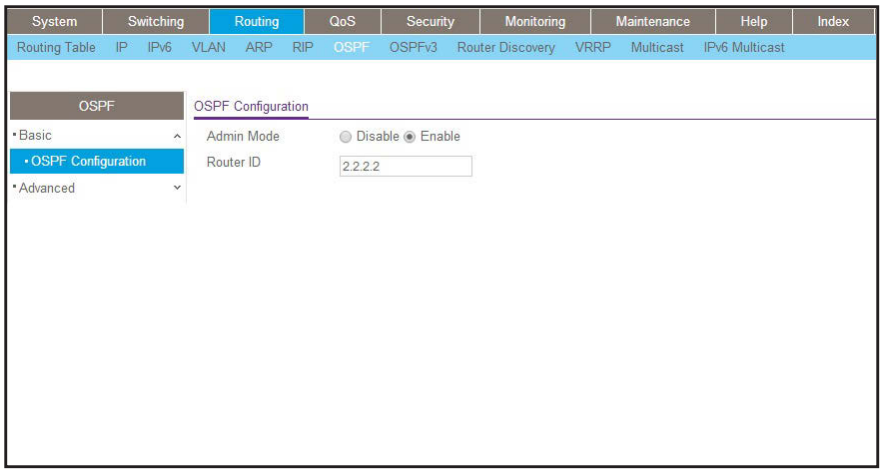
- In the **IP Address** field, enter **192.168.20.1**.
- In the **Subnet Mask** field, enter **255.255.255.0**.
- In the **Admin Mode** field, select **Enable**.

d. Click **Apply** to save the settings.

4. Specify the router ID, and enable OSPF for the switch.

a. Select **Routing > OSPF > Basic > OSPF Configuration**.

A screen similar to the following displays.



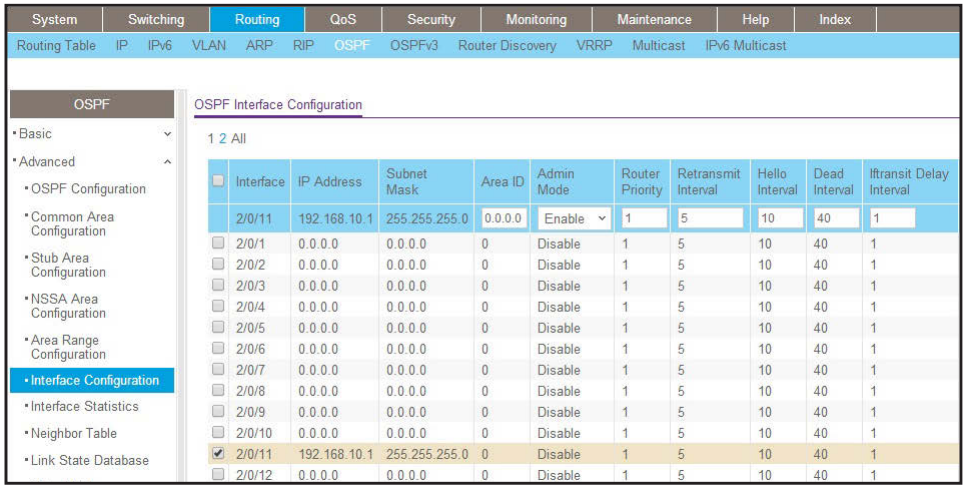
b. Under OSPF Configuration, in the **Router ID** field, enter **2.2.2.2**.

c. Click **Apply** to save the settings.

5. Enable OSPF on port 2/0/11.

a. Select **Routing > OSPF > Advanced > Interface Configuration**.

A screen similar to the following displays.



b. Scroll down and select the interface **2/0/11** check box.

Now 2/0/11 appears in the Interface field at the top.

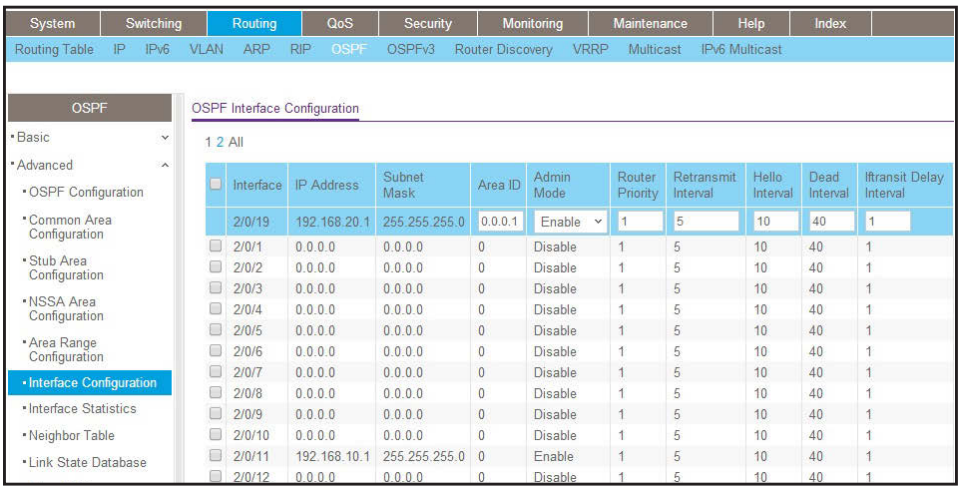
- In the **OSPF Area ID** field, enter **0.0.0.0**.
- In the **OSPF Admin Mode** field, select **Enable**.

c. Click **Apply** to save the settings.

6. Enable OSPF on port 2/0/19.

a. Select **Routing > OSPF > Advanced > Interface Configuration**.

A screen similar to the following displays.



b. Scroll down and select the interface **2/0/19** check box.

2/0/19 now appears in the Interface field at the top.

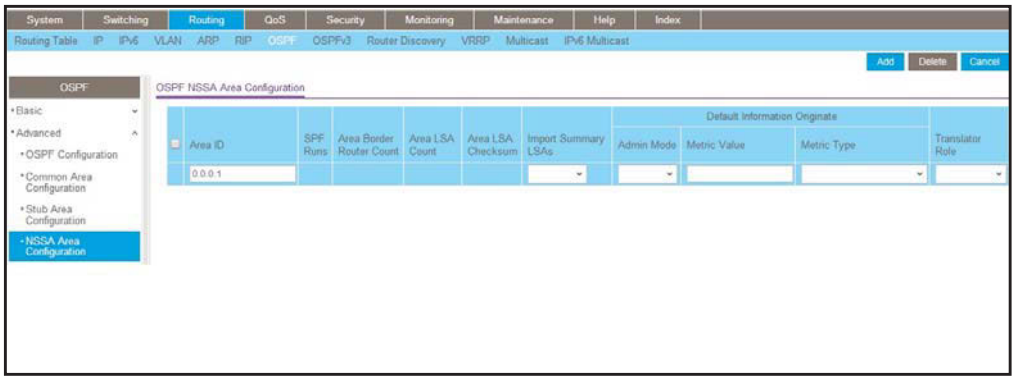
c. Enter the following information:
   - In the **OSPF Area ID** field, enter **0.0.0.1**.
   - In the **OSPF Admin Mode** field, select **Enable**.

d. Click **Apply** to save the settings.

7. Configure area 0.0.0.1 as an NSSA area.

a. Select **Routing > OSPF > Advanced > NSSA Area Configuration**.

A screen similar to the following displays.



b. Enter the following information.
   - In the **Area ID** field, enter **0.0.0.1**.
   - In the **Import Summary LSA's** field, select **Disable**.

c. Click **Add** to save the settings.

CLI: Configure Area 1 as an NSSA Area on A2

1. Enable routing on the switch.

```
(Netgear Switch) #config
(Netgear Switch) (Config)#ip routing
(Netgear Switch) (Config)#router ospf
```

2. Set the router ID to 2.2.2.2.

```
(Netgear Switch) (Config-router)#router-id 2.2.2.2
```

3. Configure the area 0.0.0.1 as an NSSA area.

```
(Netgear Switch) (Config-router)# area 0.0.0.1 nssa
```

4. Redistribute the RIP routes into the OSPF.

```
(Netgear Switch) (Config-router)#redistribute rip
(Netgear Switch) (Config-router)#redistribute rip subnets
```

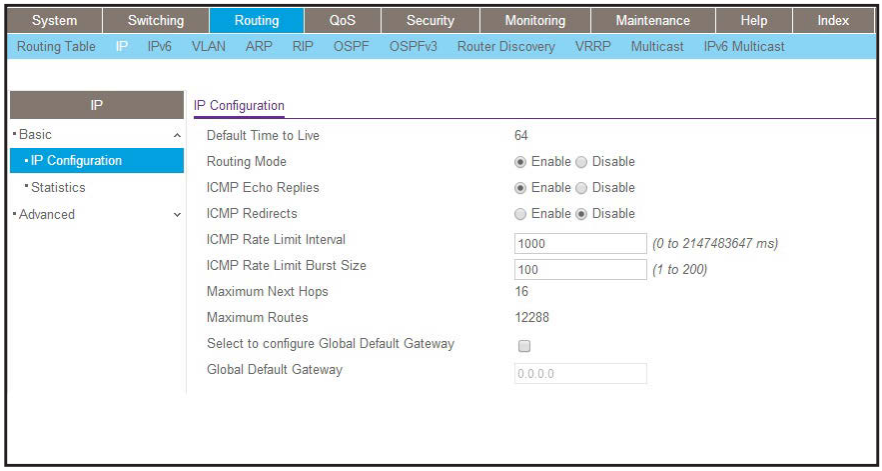
5. Enable OSPF area 0.0.0.1 on port 1/0/15.

```
(Netgear Switch) (Config-router)#exit
(Netgear Switch) (Config)#interface 1/0/11
(Netgear Switch) (Interface 1/0/11)#routing
(Netgear Switch) (Interface 1/0/11)#ip address 192.168.30.1 255.255.255.0
(Netgear Switch) (Interface 1/0/11)#ip rip
(Netgear Switch) (Interface 1/0/11)#exit
(Netgear Switch) (Config)#interface 1/0/15
(Netgear Switch) (Interface 1/0/15)#routing
(Netgear Switch) (Interface 1/0/15)#ip address 192.168.20.2  255.255.255.0
(Netgear Switch) (Interface 1/0/15)#ip ospf
(Netgear Switch) (Interface 1/0/15)#ip ospf areaid 0.0.0.1
(Netgear Switch) (Interface 1/0/15)#exit
(Netgear Switch) (Config)#exit
(Netgear Switch) #show ip route
Total Number of Routes..... 6
   Network          Subnet                    Next Hop     Next Hop
   Address           Mask         Protocol     Intf       IP Address
--------------- --------------- ------------  ---------  ---------------
0.0.0.0         0.0.0.0         OSPF Inter    1/0/15     192.168.20.1
192.168.20.0    255.255.255.0   Local         1/0/15     192.168.20.2
192.168.30.0    255.255.255.0   Local         1/0/11     192.168.30.1
192.168.40.0    255.255.255.0   RIP           1/0/11     192.168.30.2
192.168.41.0    255.255.255.0   RIP           1/0/11     192.168.30.2
192.168.42.0    255.255.255.0   RIP           1/0/11     192.168.30.2
```

Web Interface: Configure Area 1 as an NSSA Area on A2

1. Enable IP routing on the switch.
   a. Select **Routing > IP > Basic > IP Configuration**.

      A screen similar to the following displays.

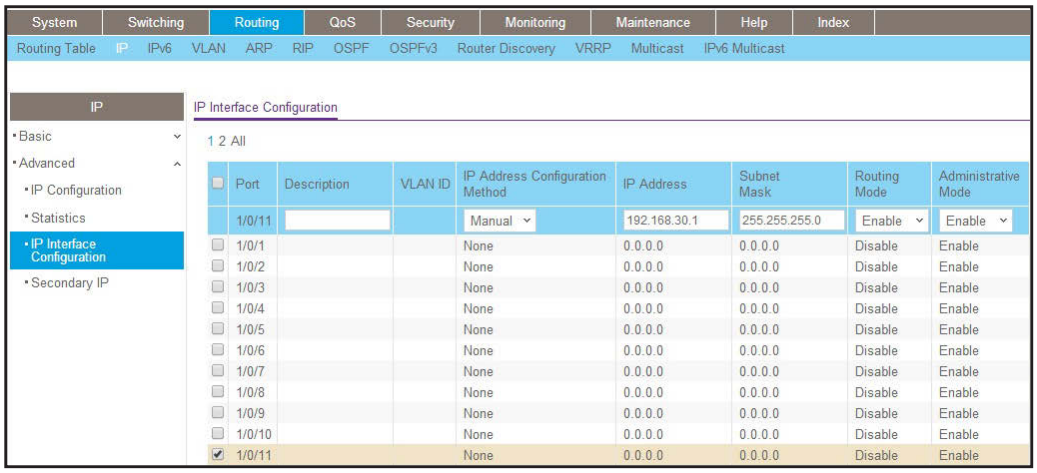


   b. mFor Routing Mode, select the **Enable** radio button.

   c. Click **Apply** to save the settings.

2. Assign IP address 192.168.30.1 to port 1/0/11.
   a. Select **Routing > IP > Advanced > IP Interface Configuration**.

      A screen similar to the following displays.



   b. Scroll down and select the interface **1/0/11** check box.

      Now 1/0/11 appears in the Interface field at the top.

   c. Enter the following information:
      - In the **IP Address Configuration Method** field, select **Manual**.
      - In the **IP Address** field, enter **192.168.30.1**.

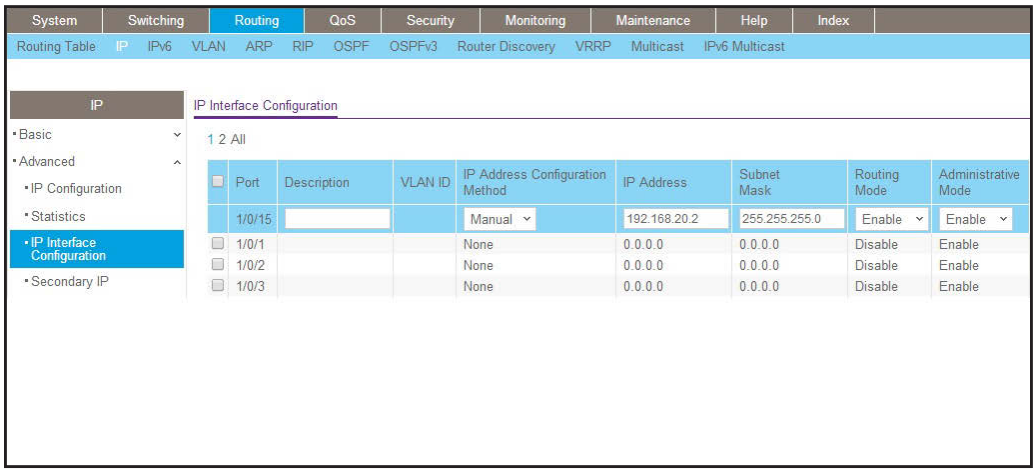
- In the **Network Mask** field, enter **255.255.255.0**.
- In the **Routing Mode** field, select **Enable**.

d. Click **Apply** to save the settings.

3. Assign IP address 192.168.20.2 to port 1/0/15.

a. Select **Routing > IP > Advanced > IP Interface Configuration**.

A screen similar to the following displays.



b. Under Configuration, scroll down and select the interface **1/0/15** check box.

Now 1/0/15 appears in the Interface field at the top.

c. Enter the following information:

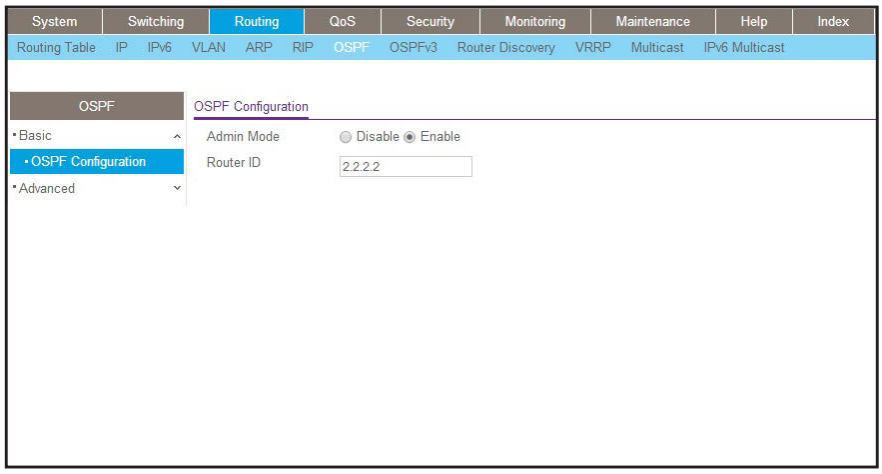
- In the **IP Address Configuration Method** field, select **Manual**.
- In the **IP Address** field, enter **192.168.20.2**.
- In the **Network Mask** field, enter **255.255.255.0**.
- In the **Routing Mode** field, select **Enable**.

d. Click **Apply** to save the settings.

4. Specify the router ID, and enable OSPF for the switch.

a. Select **Routing > OSPF > Basic > OSPF Configuration**.

A screen similar to the following displays.



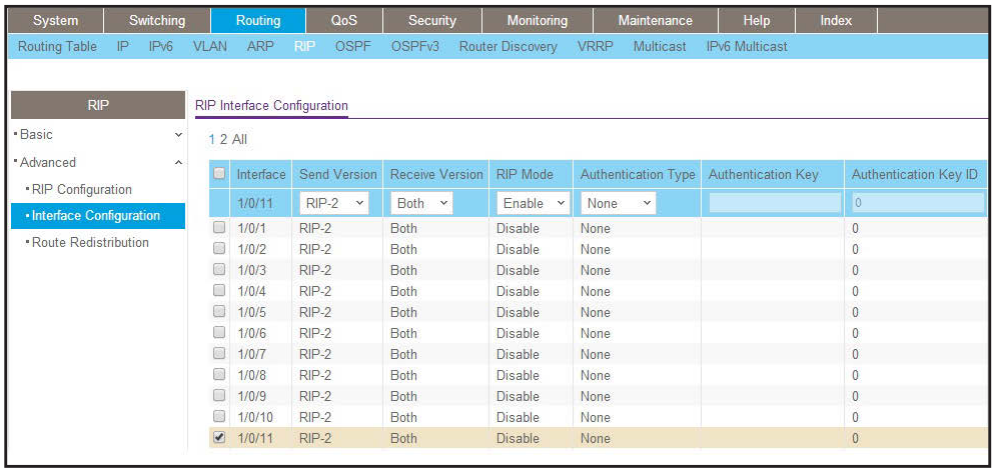
b. Under OSPF Configuration, in the **Router ID** field, enter **2.2.2.2**.

c. Click **Apply** to save the settings.

5. Enable RIP on port 1/0/11.

a. Select **Routing > RIP > Advanced > Interface Configuration**.

A screen similar to the following displays.



b. Enter the following information:

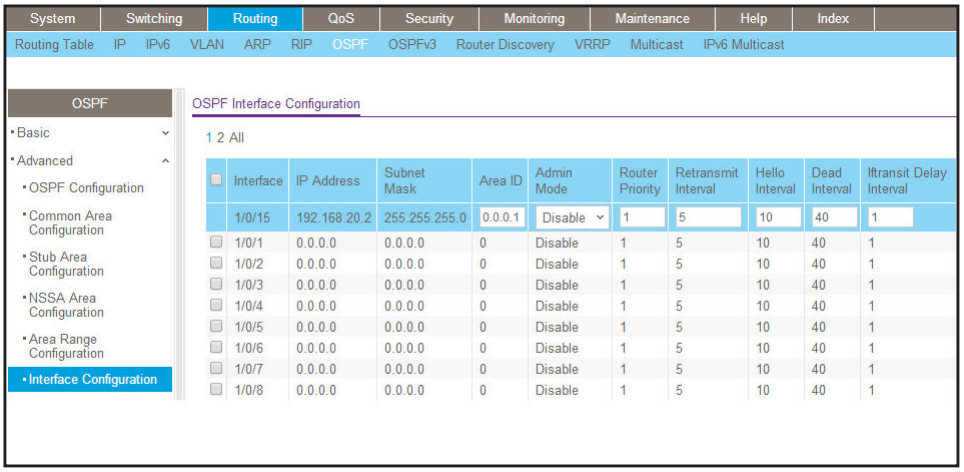
- In the **Interface** field, select **1/0/11**.
- For RIP Admin Mode, select the **Enable** radio button.

c. Click **Apply** to save the settings.

6. Enable OSPF on port 1/0/15.

a. Select **Routing > OSPF > Advanced > Interface Configuration**.

A screen similar to the following displays.



b. Scroll down and select the interface **1/0/15** check box. Now 1/0/15 appears in the Interface field at the top.

c. Enter the following information:

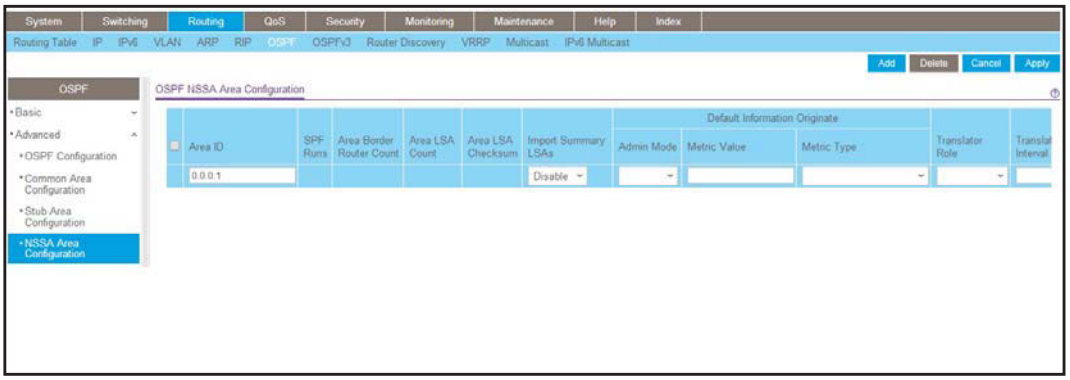
- In the **OSPF Area ID** field, enter **0.0.0.1**.
- In the **OSPF Admin Mode** field, select **Enable**.

d. Click **Apply** to save the settings.

7. Configure area 0.0.0.1 as an NSSA area.

a. Select **Routing > OSPF > Advanced > NSSA Area Configuration**.

A screen similar to the following displays.



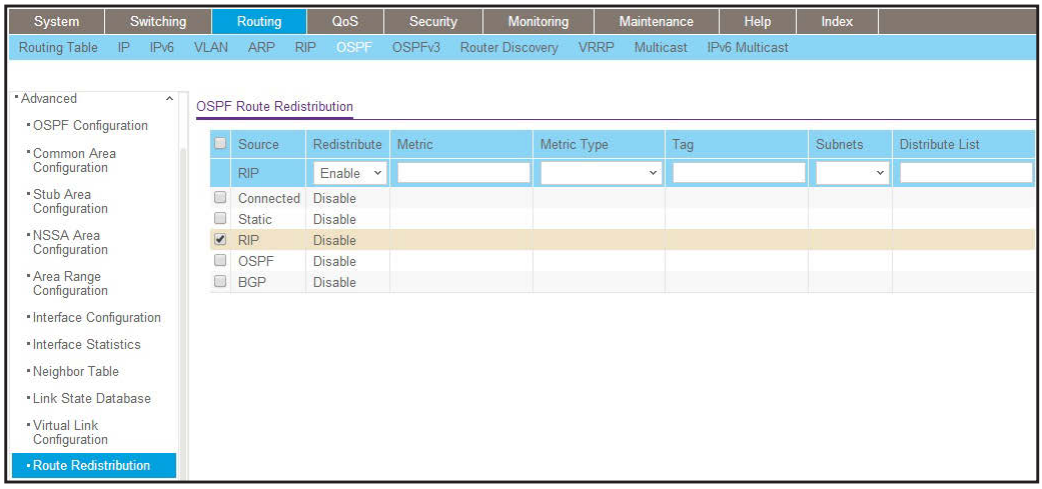
b. In the **Area ID** field, enter **0.0.0.1**.

c. Click **Add** to save the settings.

8. Redistribute the RIP routes into the OSPF area.

a. Select **Routing > OSPF > Advanced > Route Redistribution**.

A screen similar to the following displays.



b. Scroll down and select the **RIP** check box.

Now RIP appears in the **Source** field at the top.

c. Enter the following information:

In the **Redistribute** field, select **Enable**.

d. Under Route Redistribution, in the **Available Source** list, select **RIP**.

e. Click **Add** to add a route redistribution.

VLAN Routing OSPF

For larger networks Open Shortest Path First (OSPF) is generally used in preference to RIP. OSPF offers the following benefits to the administrator of a large and/or complex network:

- Less network traffic:
  - Routing table updates are sent only when a change has occurred
  - Only the part of the table that has changed is sent
  - Updates are sent to a multicast, not a broadcast, address
- Hierarchical management, allowing the network to be subdivided

The top level of the hierarchy of an OSPF network is known as an autonomous system (AS) or routing domain, and is a collection of networks with a common administration and routing strategy. The AS is divided into areas: intra-area routing is used when a source and destination address are in the same area, and inter-area routing across an OSPF backbone is used when they are not. An inter-area router communicates with border routers in each of the areas to which it provides connectivity.

The switch operating as a router and running OSPF will determine the best route using the assigned cost and the type of the OSPF route. The order for choosing a route if more than one type of route exists is as follows:

- Intra-area
- Inter-area
- External type 1: the route is external to the AS
- External Type 2: the route was learned from other protocols such as RIP

CLI: Configure VLAN Routing OSPF

This example adds support for OSPF to the configuration created in the base VLAN routing example in *Figure 10, Layer 3 switch configured for port routing* on page 82.

1. Configure the switch as an inter-area router.

```
(Netgear Switch) #vlan data
(Netgear Switch) (Vlan)#vlan 10
(Netgear Switch) (Vlan)#vlan 20
(Netgear Switch) (Vlan)#vlan routing 10
(Netgear Switch) (Vlan)#vlan routing 20
(Netgear Switch) (Vlan)#exit
(Netgear Switch) #conf
(Netgear Switch) (Config)#ip routing
(Netgear Switch) (Config)#vlan port tagging all 10
(Netgear Switch) (Config)#vlan port tagging all 20
(Netgear Switch) (Config)#interface 1/0/2
(Netgear Switch) (Interface 1/0/2)#vlan participation include 10
(Netgear Switch) (Interface 1/0/2)#vlan pvid 10
(Netgear Switch) (Interface 1/0/2)#exit
(Netgear Switch) (Config)#interface 1/0/3
(Netgear Switch) (Interface 1/0/3)#vlan participation include 20
(Netgear Switch) (Interface 1/0/3)#vlan pvid 20
(Netgear Switch) (Interface 1/0/3)#exit
(Netgear Switch) (Config)#interface vlan 10
(Netgear Switch) (Interface vlan 10)#ip address 192.150.3.1 255.255.255.0
(Netgear Switch) (Interface vlan 10)#exit
(Netgear Switch) (Config)#interface vlan 20
(Netgear Switch) (Interface vlan 20)#ip address 192.150.4.1 255.255.255.0
(Netgear Switch) (Interface vlan 20)#exit
```

2. Specify the router ID and enable OSPF for the switch.

```
(Netgear Switch) (Config)#router ospf
(Netgear Switch) (Config router)#router-id 192.150.9.9
(Netgear Switch) (Config router)#enable
(Netgear Switch) (Config router)#exit
```

3. Enable OSPF for the VLAN and physical router ports.

```
(Netgear Switch) (Config)#interface vlan 10
(Netgear Switch) (Interface vlan 10)#ip ospf areaid 0.0.0.2
(Netgear Switch) (Interface vlan 10)#ip ospf
(Netgear Switch) (Interface vlan 10)#exit
(Netgear Switch) (Config)#interface vlan 20
(Netgear Switch) (Interface vlan 20)#ip ospf areaid 0.0.0.3
(Netgear Switch) (Interface vlan 20)#ip ospf
(Netgear Switch) (Interface vlan 20)#exit
```

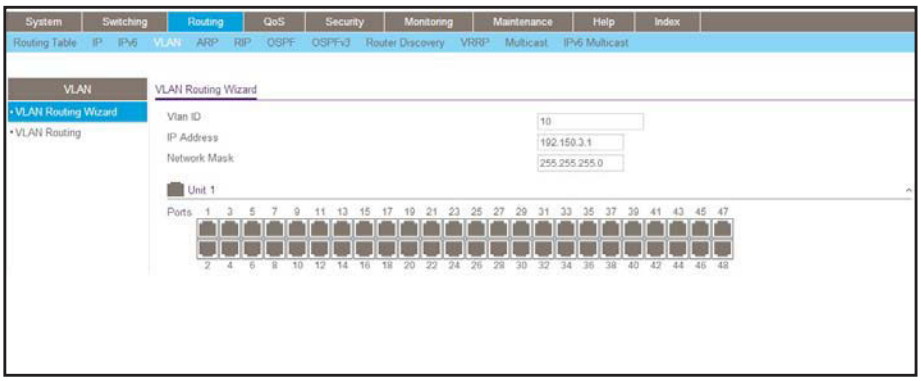
4. Set the OSPF priority and cost for the VLAN and physical router ports.

```
(Netgear Switch) (Config)#interface vlan 10
(Netgear Switch) (Interface vlan 10)#ip ospf priority 128
(Netgear Switch) (Interface vlan 10)#ip ospf cost 32
(Netgear Switch) (Interface vlan 10)#exit
(Netgear Switch) (Config)#interface vlan 20
(Netgear Switch) (Interface vlan 20)#ip ospf priority 255
(Netgear Switch) (Interface vlan 20)#ip ospf cost 64
(Netgear Switch) (Interface vlan 20)#exit
(Netgear Switch) (Config)#exit
```

Web Interface: Configure VLAN Routing OSPF

1. Configure a VLAN and include ports 1/0/2 in the VLAN.
   a. Select **Routing > VLAN > VLAN Routing Wizard**.

      A screen similar to the following displays.



   b. Enter the following information:
      - In the **Vlan ID** field, enter **10**.
      - In the **IP Address** field, enter **192.150.3.1**.
      - In the **Network Mask** field, enter **255.255.255.0**.

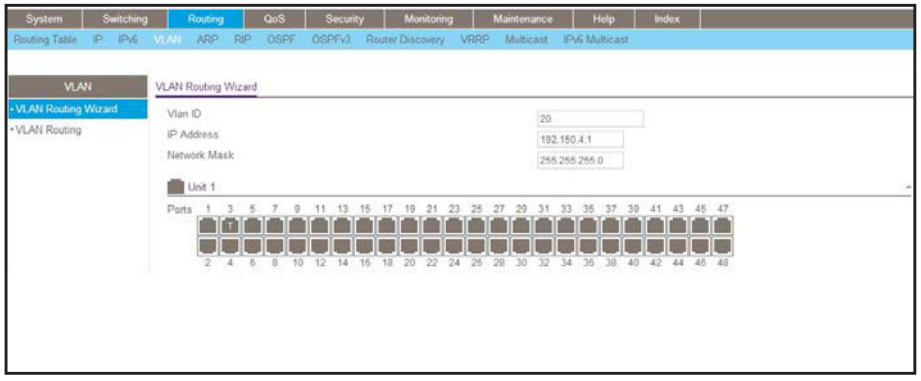
   c. Click **Unit 1**. The ports display:

      Click the gray box under port **2** until **T** displays. The T specifies that the egress packet is tagged for the port.

   d. Click **Apply** to save the VLAN that includes ports 2.

2. Configure a VLAN, and include port 1/0/3 in the VLAN.
   a. Select **Routing > VLAN > VLAN Routing Wizard**.

      A screen similar to the following displays.



   b. Enter the following information:
      - In the **Vlan ID** field, enter **20**.
      - In the **IP Address** field, enter **192.150.4.1**.
      - In the **Network Mask** field, enter **255.255.255.0**.

c. Click **Unit 1**. The ports display:

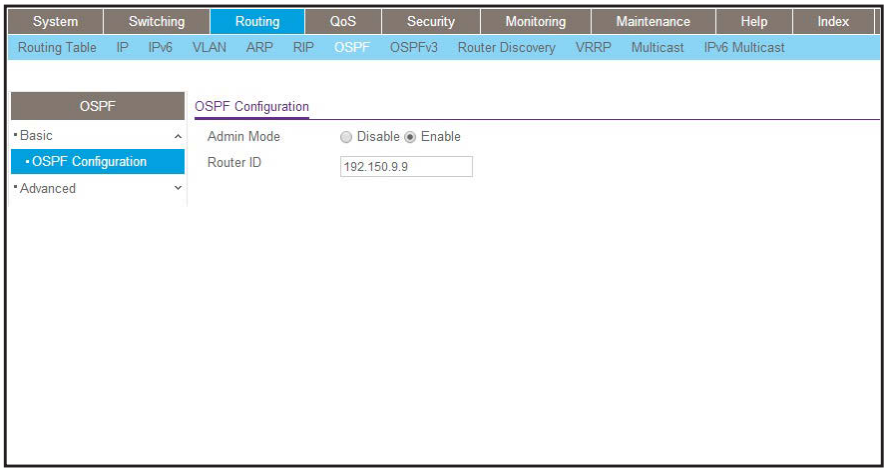
   Click the gray box under port **3** until **T** displays. The T specifies that the egress packet is tagged for the port.

d. Click **Apply** to save the VLAN that includes port 3.

3. Enable OSPF on the switch.

a. Select **Routing > OSPF > Basic > OSPF Configuration**.

   A screen similar to the following displays.



b. For **OSPF Admin Mode**, select the **Enable** radio button.

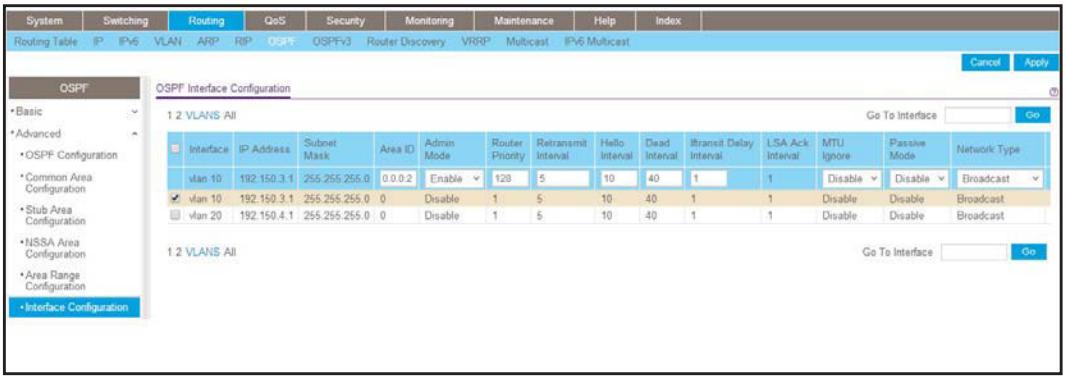
c. In the **Router ID** field, enter **192.150.9.9**.

d. Click **Apply** to save the setting.

4. Enable OSPF on VLAN 10.

a. Select **Routing > OSPF > Advanced > Interface Configuration**.

   A screen similar to the following displays.



b. Under Interface Configuration, click **VLANS** to show all the VLAN interfaces.

c. Scroll down and select the interface **0/2/1** check box. Now 0/2/1 appears in the Interface field at the top.

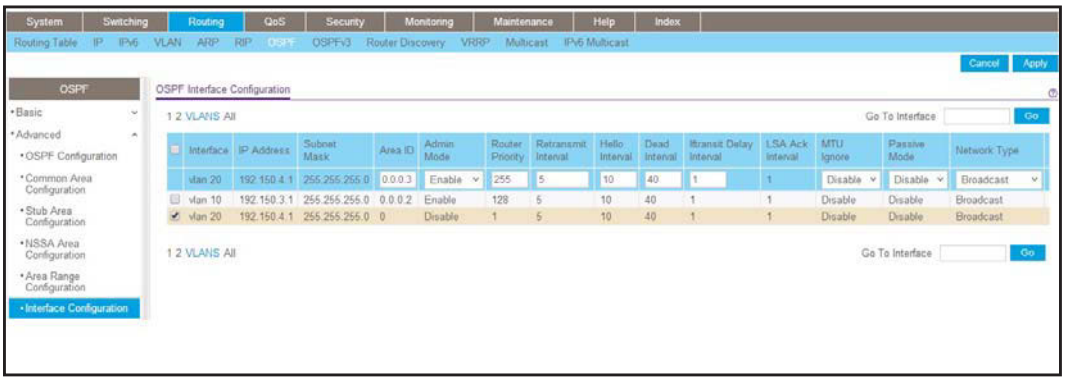
d. Enter the following information:
   - In the **OSPF Area ID** field, enter **0.0.0.2**.
   - In the **OSPF Admin Mode** field, select **Enable**.
   - In the **Priority** field, enter **128**.
   - In the **Metric Cost** field, enter **32**.

e. Click **Apply** to save the settings.

5. Enable OSPF on VLAN 20.

a. Select **Routing > OSPF > Advanced > Interface Configuration**.

A screen similar to the following displays.



b. Under Interface Configuration, click **VLANS** to show all the VLAN interfaces.

c. Scroll down and select the interface **0/2/2** check box. Now 0/2/2 appears in the Interface field at the top.

d. Enter the following information:
   - In the **OSPF Area ID** field, enter **0.0.0.3**.
   - In the **OSPF Admin Mode** field, select the **Enable**.
   - In the **Priority** field, enter **255**.
   - In the **Metric Cost** field, enter **64**.

e. Click **Apply** to save the settings.

OSPFv3

OSPFv3 is the Open Shortest Path First routing protocol for IPv6. It is similar to OSPFv2 in its concept of a link state database, intra- and inter-area, and AS external routes and virtual links. It differs from its IPv4 counterpoint in a number of respects, including the following: Peering is done through link-local addresses; the protocol is link based rather than network based; and addressing semantics have been moved to leaf LSAs, which eventually allow its use for both IPv4 and IPv6. Point-to-point links are also supported in order to enable operation over tunnels. It is possible to enable OSPF and OSPFv3 at the same time. OSPF works with IPv4, and OSPFv3 works with IPv6. The following example shows how to configure OSPFv3 on a IPv6 network.

Figure 16. OSPFv3 Protocol for IPv6

CLI: Configure OSPFv3

1. On A1, enable IPv6 unicast routing on the switch.

```
(Netgear Switch) (Config)#ipv6 unicast-routing
```

2. Enable OSPFv3, and assign 1.1.1.1 to router ID.

```
(Netgear Switch) (Config)#ipv6 router ospf
(Netgear Switch) (Config-rtr)#enable
(Netgear Switch) (Config-rtr)#router-id 1.1.1.1
(Netgear Switch) (Config-rtr)#exit
```

3. Enable routing mode on the interface 1/0/1, and assign the IP address 2000::1 to IPv6.

```
(Netgear Switch) (Config)#interface 1/0/1
(Netgear Switch) (Interface 1/0/1)#routing
(Netgear Switch) (Interface 1/0/1)#ipv6 address 2000::1/64
(Netgear Switch) (Interface 1/0/1)#ipv6 enable
```

4. Enable OSPFv3 on the interface 1/0/1, and set the OSPF network mode to broadcast.

```
(Netgear Switch) (Interface 1/0/1)#ipv6 ospf
(Netgear Switch) (Interface 1/0/1)#ipv6 ospf network broadcast
(Netgear Switch) #show ipv6 ospf neighbor

Router ID   Priority   Intf ID   Interface       State        DeadTime
----------  --------   -------   ---------   --------------   -------
 2.2.2.2      1          13        1/0/1     Full/BACKUP-DR     34
```

5. On A2, enable IPv6 unicast routing on the switch.

```
(Netgear Switch) (Config)#ipv6 unicast-routing
```

6. Enable OSPFv3, and assign 2.2.2.2 as the router ID.

```
(Netgear Switch) (Config)#ipv6 router ospf
(Netgear Switch) (Config-rtr)#enable
(Netgear Switch) (Config-rtr)#router-id 2.2.2.2
(Netgear Switch) (Config-rtr)#exit
```

7. Enable routing mode on interface 1/0/13, and assign the IP address 2000::2 to IPv6.

```
(Netgear Switch) (Config)#interface 1/0/13
(Netgear Switch) (Interface 1/0/13)#routing
(Netgear Switch) (Interface 1/0/13)#ipv6 address 2000::2/64
(Netgear Switch) (Interface 1/0/13)#ipv6 enable
```

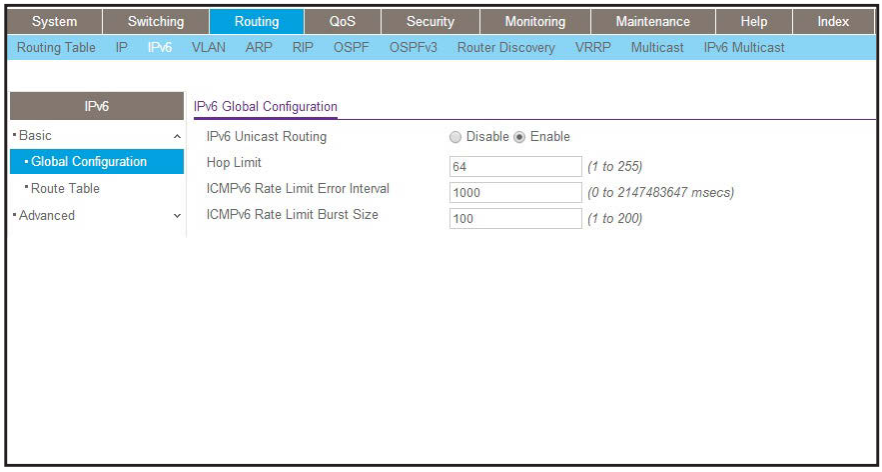
8. Enable OSPFv3 on interface 1/0/13, and set the OSPF network mode to broadcast.

```
(Netgear Switch) (Interface 1/0/13)#ipv6 ospf
(Netgear Switch) (Interface 1/0/13)#ipv6 ospf network broadcast
(Netgear Switch) #show ipv6 ospf neighbor

Router ID Priority  IntfID   Interface    State     DeadTime
--------  --------  ------   ---------   ---------   ----
1.1.1.1      1        1      1/0/13      Full/ DR     34
```

Web Interface: Configure OSPFv3

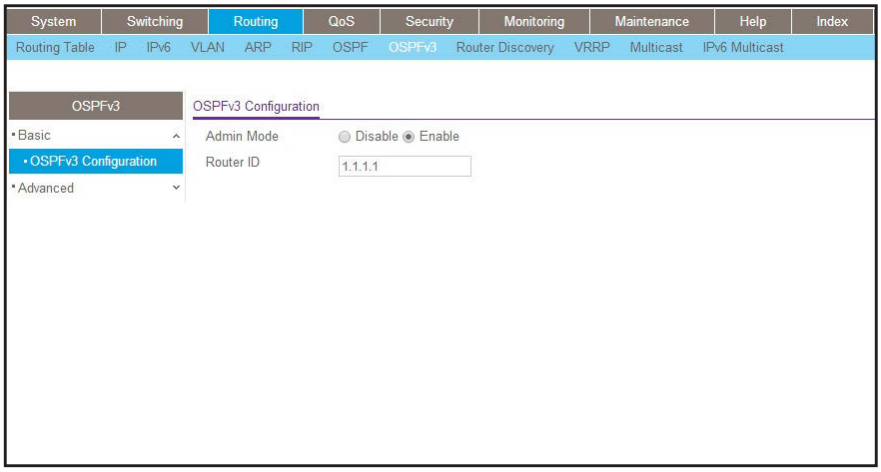
1. Enable IPv6 unicast routing on the switch.
   a. Select **Routing > IPv6 > Basic > IPv6 Global Configuration**.

      A screen similar to the following displays.



   b. For IPv6 Unicast Routing Mode, select the **Enable** radio button.
   c. Click **Apply** to save the settings.
2. Specify the router ID, and enable OSPFv3 for the switch.
   a. Select **Routing > OSPFv3 > Basic > OSPFv3 Configuration**.

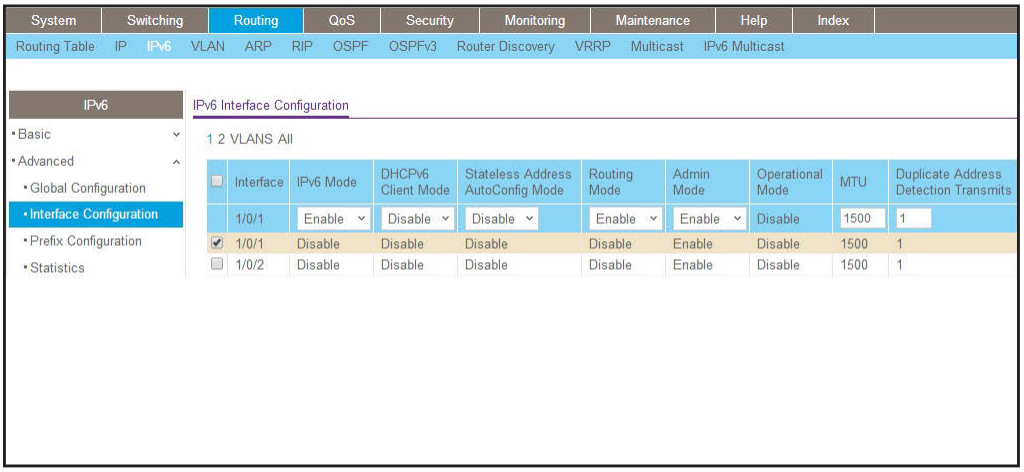
      A screen similar to the following displays.



   b. Under the OSPF Configuration, enter the following information:
      - In the **Router ID** field, enter **1.1.1.1**.
      - For Admin Mode, select the **Enable** radio button.
   c. Click **Apply** to save the settings.

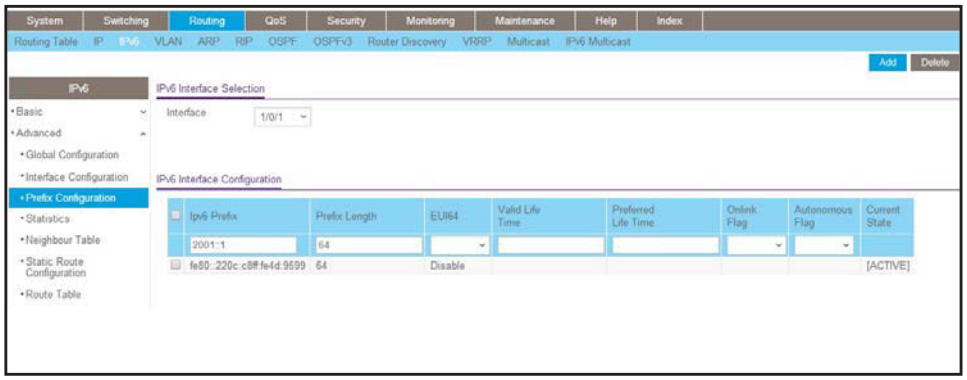
3. Enable IPv6 on port 1/0/1.
   a. Select **Routing > IPv6 > Advanced > IP Interface Configuration**.

      A screen similar to the following displays.



   b. Scroll down and select the interface **1/0/1** check box. Now 1/0/1 appears in the Interface field at the top.
   c. Enter the following information:
      - In the **IPv6 Mode** field, select **Enable**.
      - In the **Routing Mode** field, select **Enable**.
   d. Click **Apply** to save the settings.
4. Assign the IP address 2001::1 to port 1/0/1.
   a. Select **Routing > IPv6 > Advanced > IP Interface Configuration**.

      A screen similar to the following displays.



   b. Under IPv6 Prefix Selection, in the **Interface** list, select **1/0/1**.
   c. Under IPv6 Interface Configuration, enter the following information:
      - In the **IPv6 Prefix** field, enter **2001::1**.
      - In the **Length** field, enter **64**.
      - In the **EUI64** field, select **Disable**.

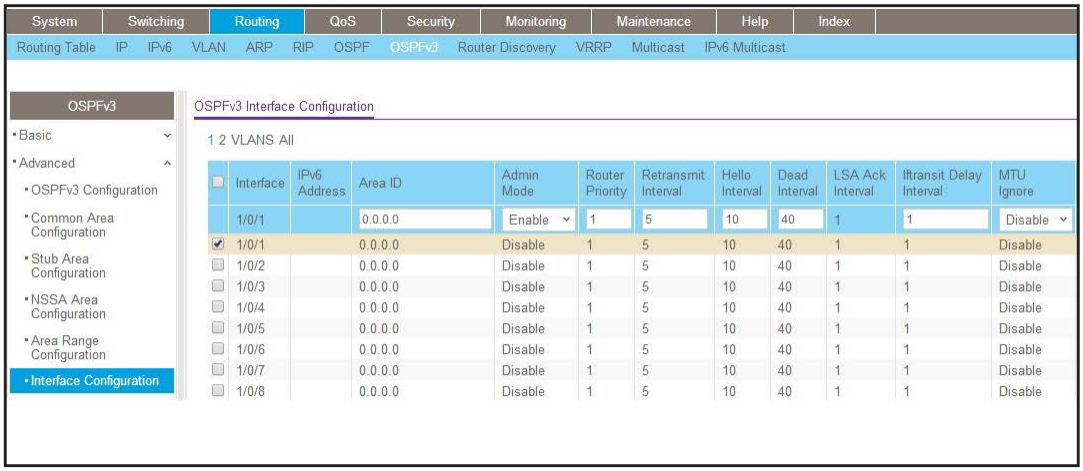
- In the **Onlink Flag** field, select **Disable**.
- In the **Autonomous Flag** field, select **Disable**.

d. Click **Add** to save the settings.

5. Enable OSPFv3 on port 1/0/1.

a. Select **Routing > OSPFv3 > Advanced > Interface Configuration**.

A screen similar to the following displays.



b. Under IP Interface Configuration, scroll down and select the interface **1/0/1** check box. Now 1/0/1 appears in the Interface field at the top.

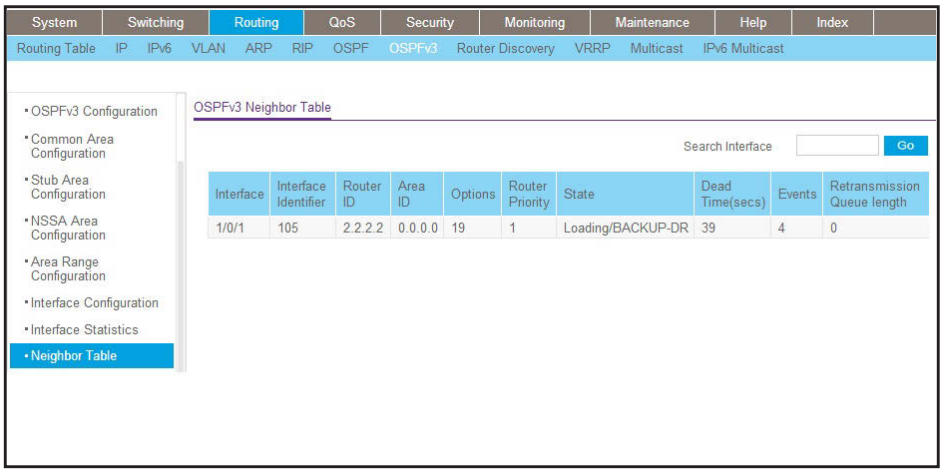
- In the **OSPF Area ID** field, enter **0.0.0.0**.
- In the **Admin Mode** field, select **Enable**.

c. Click **Apply** to save the settings.

6. Display the OSPFv3 Neighbor Table.

a. Select **Routing > OSPFv3 > Advanced > Neighbor Table**.

A screen similar to the following displays.



To use the web interface to configure OSPF on switch A2, repeat this process for switch A2.

8 PBR

Policy-based routing

This chapter includes the following sections:

- *Policy-Based Routing Concepts*
- *Route-Map Statements*
- *PBR Processing Logic*
- *PBR Configurations*
- *PBR Example*

Policy-Based Routing Concepts

Normally, switches make forwarding decisions based on routing tables, which get populated by information given by dynamic routing protocols or static routing, to forward packets to destination addresses. Policy-based routing (PBR) is a feature that enables network administrators to define forwarding behavior based on packet contents. PBR is used to override traditional destination-based routing behavior.

Configuring PBR involves configuring a route map with the `match` and `set` commands and then applying the corresponding route map to the inbound traffic on routing interfaces. One interface can contain only one route-map tag, but administrators can create multiple route-map entries with different sequence numbers. These entries are evaluated in sequence-number order until the first match is found. If no match is found, packets are routed as usual.

Route-Map Statements

A route-map statement that is used for PBR is configured as permit or deny. If the statement is marked as deny, traditional destination-based routing is performed on the packet that meet the match criteria:

- If users specify any match/set statements in a route-map statement that are marked as deny, they will not be effective because traditional destination-based routing is performed on packets meeting the specified match criteria.
- If the statement is marked as permit, and if the packet meets all the match criteria, then the `set` commands in the route-map statement are applied.

If no match is found in the route map, the packet is not dropped. Packets are forwarded using the routing decision that is made by performing destination-based routing.

If network administrators do not want to revert to normal forwarding, but instead want to drop a packet that does not match the specified criteria, a set statement needs to be configured to route the packets to interface null 0 as the last entry in the route map.

Packets that are generated by the switch itself are not normally policy routed. But a provision in other industry standard products applies a policy through a local PBR. All packets originating on the switch are then subject to the local PBR. However, this feature is not supported.

Starting with Software Version 10.2, the NETGEAR switch supports the route-map infrastructure for BGP. Match parameters defined in this chapter for policy-based routing operate in isolation with BGP. These options do not interfere with BGP protocol processing or policy propagation in any way.

For example, if a match clause is placed in a route-map statement based on the length of the packet, BGP does not honor that clause. As stated earlier, these statements apply for L3 routed traffic (mainly data traffic) to override a routing decision.

To classify L3 routed traffic, the switch supports the following packet entities:

- The size of the packet
- Protocol of the payload (Protocol ID field in IP header)
- Source MAC address
- Source IP address
- Destination IP address
- Priority (802.1P priority)

NETGEAR's policy-based routing feature overrides routing decisions taken by the switch and makes the packet follow different actions specified in the following order to define forwarding criteria:

- **List of next hop IP addresses**. The IP address can specify the adjacent next hop router in the path toward the destination to which the packets should be forwarded. The first IP address associated with a currently active ARP entry is used to route the packets.
- **List of default next hop IP addresses**. This list indicates the next-hop routers to which a packet must be routed if no active route exists for the packet's destination address in the routing table. With the policy-based routing feature, a default route in the routing table is not considered an active route for an unknown destination address.
- **IP precedence**. A numeric value can be specified to set the precedence in the IP packets being forwarded. IP precedence value implies 3 IP precedence bits in the IP packet header. With 3 bits, network administrators have 8 possible values for the IP precedence. This value will be set in IPV4 header of packets when configured.

PBR Processing Logic

The processing logic used by policy-based routing is as follows when a packet is received on an interface configured with a route map, the forwarding logic processes each route-map statement according to the sequence number.

The route map with a permit statement uses the following logic:

- The incoming packet is matched against the criteria in the match term specified in the route map. This match command can refer to an IP/MAC access list. An ACL that is used in the match term itself includes one or more permit or deny rules. Now, the incoming packet is matched against the rules in the AC, and a permit or deny decision is reached.
- If the decision reached in the previous step is permit, then policy-based routing executes the action specified in set terms of the route-map statement over an incoming packet.
- If the decision reached in the earlier step is deny, then policy-based routing does not apply any action that is specified in set terms in the route-map statement. In this situation, the counter for this match statement is not incremented and the processing logic moves to next route-map statement in the sequence. If no next route-map statement exists, the processing logic terminates and the packet goes through standard destination-based routing logic.

The route map with a deny statement uses the following logic:

- The incoming packet is matched against the criteria in the match term specified in the route map. This match command can refer to an IP/MAC access list. An ACL that is used in the match term itself has one or more permit or deny rules. Now, the incoming packet is matched against the rules in the ACL, and a permit or deny decision is reached.
- If the decision reached in the previous step is permit, then policy-based routing processing logic terminates and the packet goes through standard destination-based routing logic.
- If the decision reached in the earlier step is deny, the counter for this match statement is not incremented and the processing logic moves to next route-map statement in the sequence. If no next route-map statement exists, the processing logic terminates and the packet goes through standard destination-based routing logic.

The following table specifies the desired actions:

Table 1. Desired actions

ACL	Match	Outcome	Route Map	Action
Permit	Yes	Permit	Permit	Set
Permit	No	Deny	Permit	Next
Permit	Yes	Permit	Deny	Route
Permit	No	Deny	Deny	Next
Deny	Yes	Deny	Permit	Next
Deny	No	Deny	Permit	Next
Deny	Yes	Deny	Deny	Next
Deny	No	Deny	Deny	Next

The following actions are taken:

- **Next**. Fall through to the next route map, and if no further route maps exist, route using the default routing table.
- **Set**. Route according to the action in the set clause.
- **Route** (alone). Route using the default routing table.

PBR Configurations

PBR is configurable on the following types of eligible routing interfaces:

- Physical ports
- VLAN interfaces

On VLAN interfaces, when an ACL is applied, it implies that when any packet arrives with a corresponding VLAN ID on any port, it is matched and a corresponding action is taken.

The same phenomenon applies to ACLs specified in the match clause of PBR. That is, if a PBR route map is applied on a VLAN interface, any packet coming with a corresponding VLAN ID on any port is matched against PBR rules corresponding to the match ACL clause and the corresponding set actions are taken into effect. To perform policy-based routing based on VLAN ID as the matching criteria for incoming packets, apply an ACL rule on the VLAN interface, but do not configure a rule with the VLAN ID as the match condition.

PBR supports the preconfiguration of the route map on routing interfaces. If routing is not enabled on an interface, the route map can still be applied on that particular interface. When routing is not enabled on an interface, route-map configuration is not pushed into hardware. Rather, it is maintained only in configuration. As soon as routing is enabled on that particular interface, configuration is applied to hardware.

PBR Example

Network administrators can use PBR when load sharing must be done for the incoming traffic across multiple paths based on packet entities in the incoming traffic.

Normally, to optimally utilize the data networks of the organization, the bulk traffic associated with the company activity must use a higher-bandwidth, high-cost (price of link) link while the basic connectivity continues over a lower bandwidth, low-cost link for interactive traffic. For such applications, policy-based routing is the right fit.

Consider the network that is composed of two groups with different IP address ranges. If group1 addresses must be routed through ISP1 and group2 addresses must be routed through ISP2, the switch that is connected with different groups must be policy routed. Configure a match in the route map on the IP address range of different groups. This way, an equal access as well as source IP address-sensitive routing is achieved through PBR.

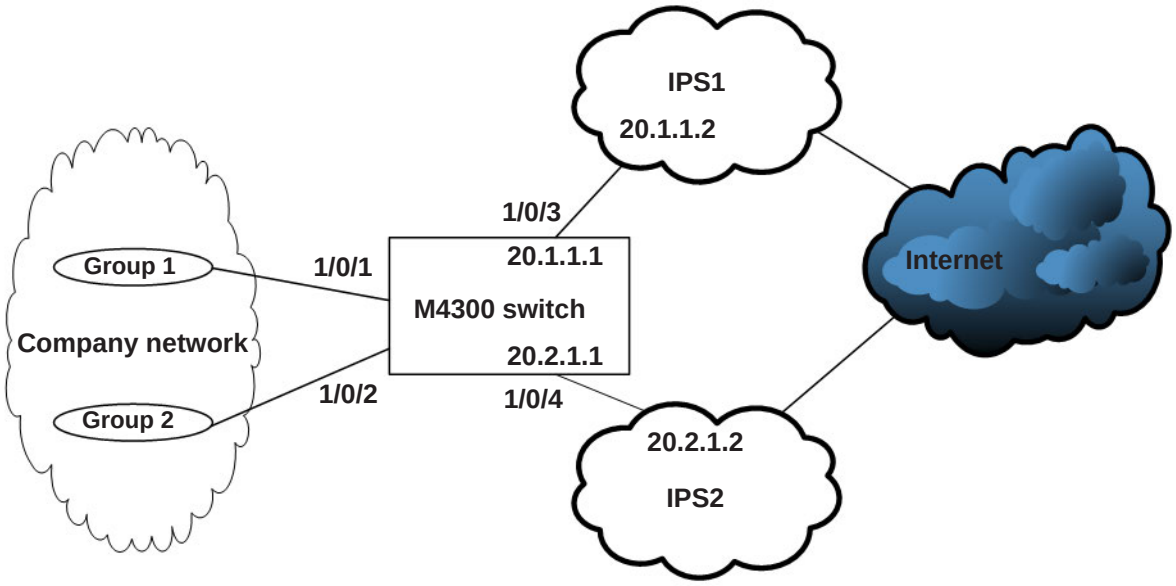


Figure 17. PBR topology

1. Create an IP ACL 1 to match 10.1.0.0/16.

```
(Netgear Switch) (Config) #access-list 1 permit 10.1.0.0 0.0.255.255
```

2. Create an IP ACL 2 to match 10.2.0.0/16.

```
(Netgear Switch) (Config)#access-list 2 permit 10.2.0.0 0.0.255.255
```

3. Create a route map pbr_1 with sequence number 10 to match ip ACL 1.

```
(Netgear Switch) (Config) #route-map pbr_1 permit 10
(Netgear Switch) (route-map) #match ip address 1
(Netgear Switch) (route-map) #set ip next-hop 20.1.1.2
(Netgear Switch) (route-map) #exit
```

4. Create a route map pbr_1 with sequence number 11 to match ip ACL 2.

```
(Netgear Switch) (Config) # route-map pbr_1 permit 11
(Netgear Switch) (route-map) #match ip address 2
(Netgear Switch) (route-map) #set ip next-hop 20.2.1.2
(Netgear Switch) (route-map) #exit
```

5. Create VLAN 30 and put interface 1/0/1 and 1/0/2 into it.

```
(Netgear Switch) #vlan database
(Netgear Switch) (Vlan) #vlan 30
(Netgear Switch) (Vlan) #vlan routing 30
(Netgear Switch) (Vlan) #exit
(Netgear Switch) (Config) #interface 1/0/1-1/0/2
(Netgear Switch) (Interface 1/0/1-1/0/2) #vlan participation include 30
(Netgear Switch) (Interface 1/0/1-1/0/2) #vlan pvid 30
(Netgear Switch) (Interface 1/0/1-1/0/2) #exit
(Netgear Switch) (Config) #interface vlan 30
(Netgear Switch) (Interface vlan 30) #routing
(Netgear Switch) (Interface vlan 30) #ip address 10.1.1.1 255.0.0.0
(Netgear Switch) (Interface vlan 30) #exit
```

6. Enable PBR on VLAN 30.

```
(Netgear Switch) (Config) #interface vlan 30
(Netgear Switch) (Interface vlan 30) #routing
(Netgear Switch) (Interface vlan 30) #ip policy route-map pbr_1
(Netgear Switch) (Interface vlan 30) #exit
```

7. Configure IP address 20.1.1.1 on interface 1/0/3.

```
(Netgear Switch) (Config) #interface 1/0/3
(Netgear Switch) (Interface 1/0/3) #routing
(Netgear Switch) (Interface 1/0/3) #ip add 20.1.1.1 /16
```

8. Configure IP address 20.2.1.1 on interface 1/0/4.

```
 Netgear Switch) (Config) #interface 1/0/4
(Netgear Switch) (Interface 1/0/4) #routing
(Netgear Switch) (Interface 1/0/4) #ip add 20.2.1.1 /16
```

ARP

9

Proxy Address Resolution Protocol

This chapter includes the following sections:

- *Proxy ARP Concepts*
- *Proxy ARP Examples*

Proxy ARP Concepts

Proxy ARP allows a router to answer ARP requests when the target IP address is not that of the router itself but a destination that the router can reach. If a host does not know the default gateway, proxy ARP can learn the first hop. Machines in one physical network appear to be part of another logical network. Without proxy ARP, a router responds to an ARP request only if the target IP address is an address configured on the interface where the ARP request arrived.

Proxy ARP Examples

The following are examples of the commands used in the proxy ARP feature.

CLI: show ip interface

```
(Netgear Switch) #show ip interface ?

<slot/port>              Enter an interface in slot/port format.
brief                    Display summary information about IP configuration
                         settings for all ports.

(Netgear Switch) #show ip interface 0/24

Routing Mode................................. Disable
Administrative Mode.......................... Enable
Forward Net Directed Broadcasts.............. Disable
Proxy ARP.................................... Disable
Active State................................. Inactive
Link Speed Data Rate......................... Inactive
MAC Address.................................. 08:00:17:05:05:02
Encapsulation Type........................... Ethernet
IP MTU....................................... 1500
```

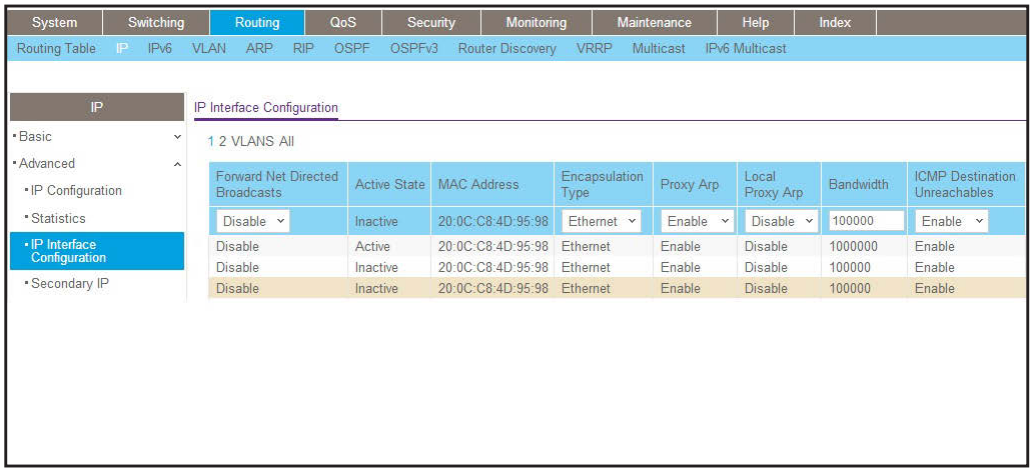
CLI: ip proxy-arp

```
(Netgear Switch) (Interface 0/24)#ip proxy-arp ?

<cr>                     Press Enter to execute the command.

(Netgear Switch) (Interface 0/24)#ip proxy-arp
```

Web Interface: Configure Proxy ARP on a Port

1. Select **Routing > IP > Advanced > IP Interface Configuration**.

   A screen similar to the following displays.



2. Under Configuration, scroll down and select the Interface **1/0/3** check box. Now 1/0/3 appears in the Interface field at the top.
3. In the **Proxy Arp** field, select **Enable**.
4. Click **Apply** to save the settings.

VRRP

10

Virtual Router Redundancy Protocol

This chapter includes the following sections:

- *Virtual Router Redundancy Protocol Concepts*
- *VRRP on a Master Router*
- *VRRP on a Backup Router*

Note: VRRP is available on the M4300 series switches only.

Virtual Router Redundancy Protocol Concepts

When an end station is statically configured with the address of the router that will handle its routed traffic, a single point of failure is introduced into the network. If the router goes down, the end station is unable to communicate. Since static configuration is a convenient way to assign router addresses, Virtual Router Redundancy Protocol (VRRP) was developed to provide a backup mechanism.

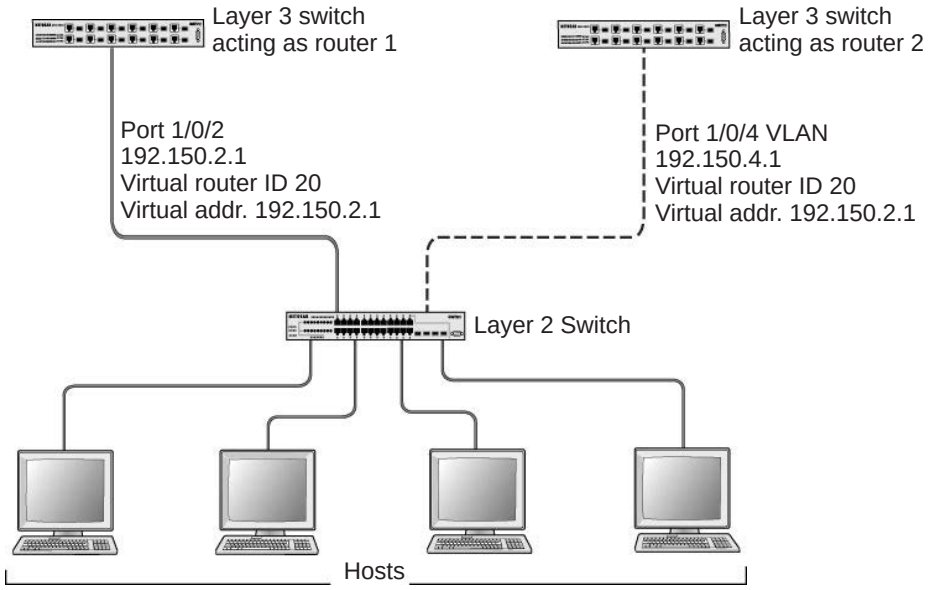


Figure 18. VRRP

VRRP eliminates the single point of failure associated with static default routes by enabling a backup router to take over from a master router without affecting the end stations using the route. The end stations use a virtual IP address that is recognized by the backup router if the master router fails. Participating routers use an election protocol to determine which router is the master router at any given time. A given port could appear as more than one virtual router to the network. Also, more than one port on the switch can be configured as a virtual router. Either a physical port or a routed VLAN can participate.

VRRP on a Master Router

This example shows how to configure the switch to support VRRP. Router 1 is the default master router for the virtual route, and Router 2 is the backup router.

CLI: Configure VRRP on a Master Router

1. Enable routing for the switch. IP forwarding will then be enabled by default.

```
(Netgear Switch) #config
(Netgear Switch) (Config)#ip routing
```

2. Configure the IP addresses and subnet masks for the port that will participate in the protocol.

```
(Netgear Switch) (Config)#interface 1/0/2
(Netgear Switch) (Interface 1/0/2)#routing
(Netgear Switch) (Interface 1/0/2)#ip address 192.150.2.1 255.255.0.0
(Netgear Switch) (Interface 1/0/2)#exit
```

3. Enable VRRP for the switch.

```
   (Netgear Switch) (Config)#ip vrrp
```

4. Assign virtual router IDs to port that will participate in the protocol.

```
(Netgear Switch) (Config)#interface 1/0/2
(Netgear Switch) (Interface 1/0/2)#ip vrrp 20
```

5. Specify the IP address that the virtual router function will recognize. Note that the virtual IP address on port 1/0/2 is the same as the port's actual IP address therefore, this router will always be the VRRP master when it is active. The default priority is 255.

```
   (Netgear Switch) (Interface 1/0/2)#ip vrrp 20 ip 192.150.2.1
```

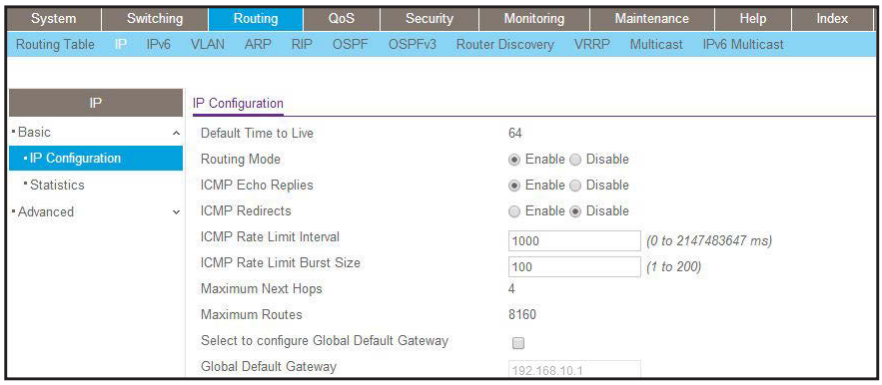
6. Enable VRRP on the port.

```
(Netgear Switch) (Interface 1/0/2)#ip vrrp 20 mode
(Netgear Switch) (Interface 1/0/2)#exit
(Netgear Switch) (Config)#exit
```

Web Interface: Configure VRRP on a Master Router

1. Enable IP routing on the switch.
   a. Select **Routing > IP > Basic > IP Configuration**.

      A screen similar to the following displays.

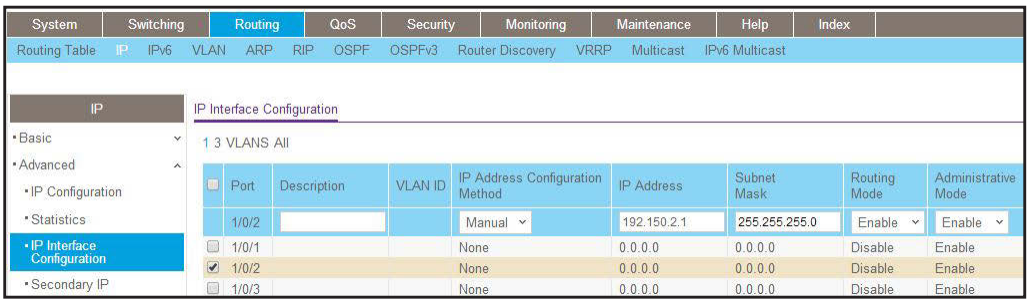


   b. For Routing Mode, select the **Enable** radio button.

   c. Click **Apply** to save the settings.

2. Assign the IP address 192.150.2.1 to port 1/0/2:
   a. Select **Routing > IP > Advanced > IP Interface Configuration**.

      A screen similar to the following displays.



   b. Scroll down and select the Interface **1/0/2** check box.

      Now 1/0/2 appears in the Interface field at the top.

   c. Enter the following information:
      - In the **IP Address** field, enter **192.150.2.1**.
      - In the **Network Mask** field, enter **255.255.0.0**.
      - In the **Routing Mode** field, select **Enable**.

   d. Click **Apply** to save the settings.

3. Enable VRRP on port 1/0/2.
   a. Select **Routing > VRRP > Advanced > VRRP Configuration**.

A screen similar to the following displays.

b. Under Global Configuration, next to the Admin Mode, select **Enable** radio button.

c. Enter the following information in the VRRP Configuration:

- In the **VRID (1 to 255)** field, enter **20**.
- In the **Interface** field, select **1/0/2**.
- In the **Primary IP Address** field, enter **192.150.2.1**.
- In the **Mode** field, select **Active**.

d. Click **Apply** to save the settings.

VRRP on a Backup Router

The example is shown as CLI commands and as a web interface procedure.

CLI: Configure VRRP on a Backup Router

1. Enable routing for the switch. IP forwarding will then be enabled by default.

```
(Netgear Switch) #config
(Netgear Switch) (Config)#ip routing
```

2. Configure the IP addresses and subnet masks for the port that will participate in the protocol.

```
(Netgear Switch) (Config)#interface 1/0/4
(Netgear Switch) (Interface 1/0/4)#routing
(Netgear Switch) (Interface 1/0/4)#ip address 192.150.4.1 255.255.0.0
(Netgear Switch) (Interface 1/0/4)#exit
```

3. Enable VRRP for the switch.

```
(Netgear Switch) (Config)#ip vrrp
```

4. Assign virtual router IDs to port that will participate in the protocol.

```
(Netgear Switch) (Config)#interface 1/0/4
(Netgear Switch) (Interface 1/0/4)#ip vrrp 20
```

5. Specify the IP address that the virtual router function will recognize. Since the virtual IP address on port 1/0/4 is the same as Router 1's port 1/0/2 actual IP address, this router will always be the VRRP backup when Router 1 is active.

```
(Netgear Switch) (Interface 1/0/4)#ip vrrp 20 ip 192.150.2.1
```

6. Set the priority for the port. The default priority is 100.

```
(Netgear Switch) (Interface 1/0/4)#ip vrrp 20 priority 254
```

7. Enable VRRP on the port.

```
(Netgear Switch) (Interface 1/0/4)#ip vrrp 20 mode
(Netgear Switch) (Interface 1/0/4)#exit
(Netgear Switch) (Config)#exit
```

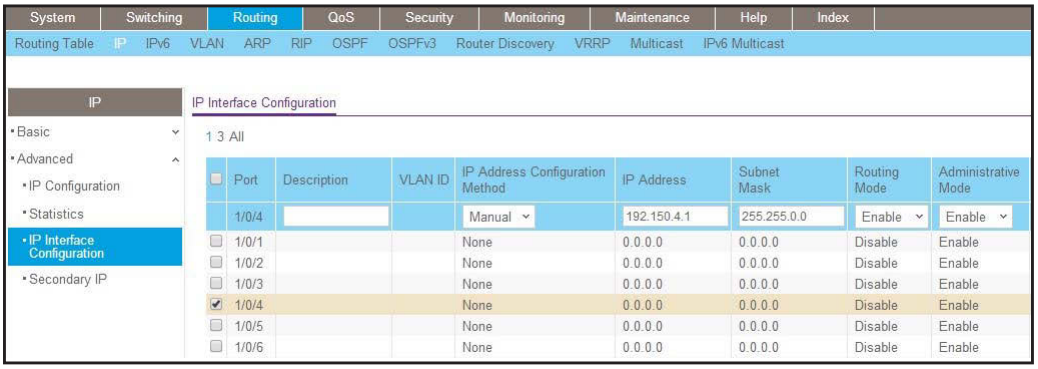
Web Interface: Configure VRRP on a Backup Router

1. Enable IP routing on the switch.
   a. Select **Routing > IP > IP Configuration**.

      A screen similar to the following displays.

   b. For Routing Mode, select the **Enable** radio button.
   c. Click **Apply** to save the settings.
2. Assign IP address 192.150.4.1 to port 1/0/4.
   a. Select **Routing > IP > Advanced > IP Interface Configuration**.

A screen similar to the following displays.



b. Scroll down and select the Interface **1/0/4** check box.

Now 1/0/4 appears in the Interface field at the top.

c. Enter the following information:

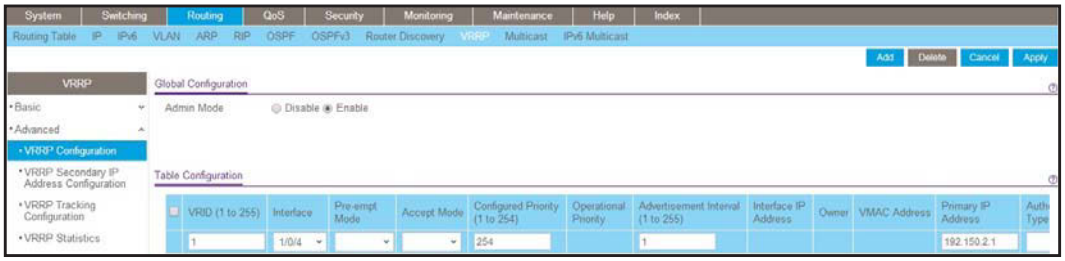
- In the **IP Address** field, enter **192.150.4.1**.
- In the **Network Mask** field, enter **255.255.0.0**.
- In the **Administrative Mode** field, select **Enable**.

d. Click **Apply** to save the settings.

3. Enable VRRP on port 1/0/4.

a. Select **Routing > VRRP > Basic > VRRP Configuration**.

A screen similar to the following displays.



b. Under Global Configuration, for Admin Mode, select the **Enable** radio button.

c. Enter the following information:

- In the **VRID (1 to 255)** field, enter **20**.
- In the **Interface** field, select **1/0/4**.
- In the **Priority (1 to 255)**, enter **254**.
- In the **Primary IP Address** field, enter **192.150.2.1**.
- In the **Status** list, select **Active**.

d. Click **Add** to save the settings.

11 ACLs

Access Control Lists

This chapter includes the following sections:

- *Access Control List Concepts*
- *MAC ACLs*
- *Set Up an IP ACL with Two Rules*
- *One-Way Access Using a TCP Flag in an ACL*
- *Use ACLs to Configure Isolated VLANs on a Layer 3 Switch*
- *Set up a MAC ACL with Two Rules*
- *Configure ACL Mirroring*
- *Configure ACL Redirection*
- *Add ACL Remarks*
- *Change the Sequence of an ACL Rule*
- *Configure a Management ACL*
- *Configure IPv6 ACLs*

Access Control List Concepts

Access control lists (ACLs) can control the traffic entering a network. Normally ACLs reside in a firewall router or in a router connecting two internal networks. When you configure ACLs, you can selectively admit or reject inbound traffic, thereby controlling access to your network or to specific resources on your network.

You can set up ACLs to control traffic at Layer 2-, or Layer 3. MAC ACLs are used for Layer 2. IP ACLs are used for Layer 3. Each ACL contains a set of rules that apply to inbound traffic. Each rule specifies whether the contents of a given field should be used to permit or deny access to the network, and may apply to one or more of the fields within a packet.

The following limitations apply to ACLs. These limitations are platform-dependent.

- The maximum of number of ACLs is 100.
- The maximum number of rules per ACL is 8–10.
- Stacking systems do not support redirection.
- The system does not support MAC ACLs and IP ACLs on the same interface.
- The system supports ACLs set up for inbound traffic only.

MAC ACLs

MAC ACLs are Layer 2 ACLs. You can configure the rules to inspect the following fields of a packet (limited by platform):

- Source MAC address with mask.
- Destination MAC address with mask.
- VLAN ID (or range of IDs).
- Class of Service (CoS) (802.1p).
- EtherType:
  - Secondary CoS (802.1p).
  - Secondary VLAN (or range of IDs).
- L2 ACLs can apply to one or more interfaces.
- Multiple access lists can be applied to a single interface: the sequence number determines the order of execution.
- You can assign packets to queues using the assign queue option.
- You can redirect packets using the redirect option.

IP ACLs

IP ACLs classify for Layer 3. Each ACL is a set of up to 10 rules applied to inbound traffic. Each rule specifies whether the contents of a given field should be used to permit or deny access to the network, and can apply to one or more of the following fields within a packet:

- Source IP address
- Destination IP address
- Source Layer 4 port
- Destination Layer 4 port
- ToS byte
- Protocol number

Note that the order of the rules is important: When a packet matches multiple rules, the first rule takes precedence. Also, once you define an ACL for a given port, all traffic not specifically permitted by the ACL is denied access.

ACL Configuration

To configure ACLs:

1. Create an ACL by specifying a name (MAC ACL or named IP ACL) or a number (IP ACL).
2. Add new rules to the ACL.
3. Configure the match criteria for the rules.
4. Apply the ACL to one or more interfaces.

Set Up an IP ACL with Two Rules

This section shows you how to set up an IP ACL with two rules, one applicable to TCP traffic and one to UDP traffic. The content of the two rules is the same. TCP and UDP packets will be accepted by the switch only if the source and destination stations have IP addresses within the defined sets.

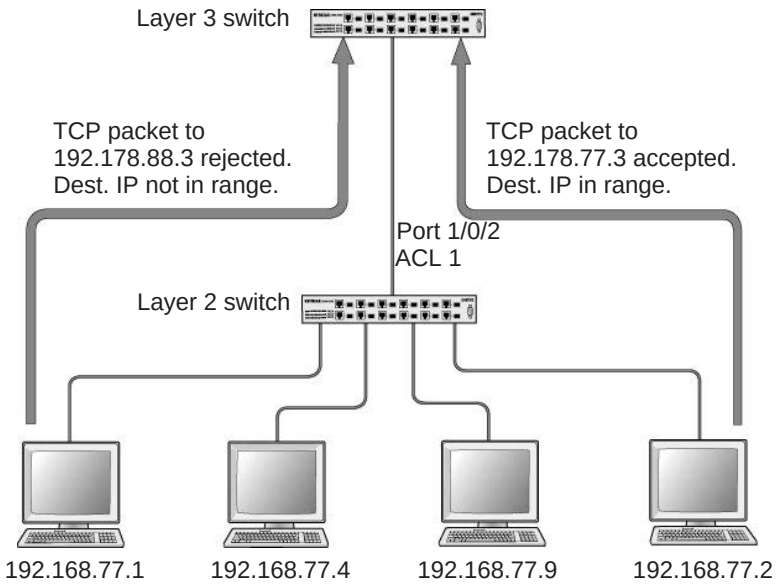


Figure 19. IP ACL with rules for TCP traffic and UDP traffic

CLI: Set Up an IP ACL with Two Rules

The following is an example of configuring ACL support on a 7000 Series Managed Switch.

Create ACL 101. Define the first rule: The ACL will permit packets that match the specified source IP address (after the mask has been applied), that are carrying TCP traffic, and that are sent to the specified destination IP address.

1. Enter these commands:

```
(Netgear Switch) #config
(Netgear Switch) (Config)#access-list 101 permit tcp 192.168.77.0 0.0.0.255
192.178.77.0 0.0.0.255
```

2. Define the second rule for ACL 101 to set conditions for UDP traffic similar to those for TCP traffic.

```
(Netgear Switch) (Config)#access-list 101 permit udp 192.168.77.0 0.0.0.255
192.178.77.0 0.0.0.255
```

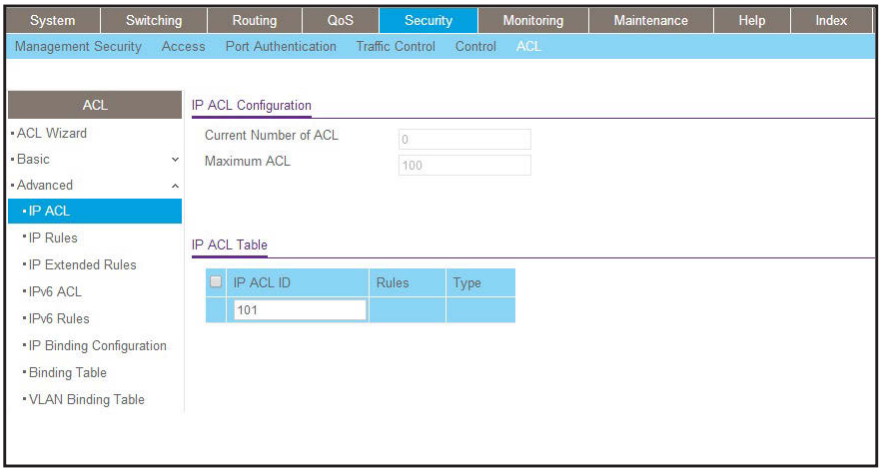
3. Apply the rule to inbound traffic on port 1/0/2. Only traffic matching the criteria will be accepted.

```
(Netgear Switch) (Config)#interface 1/0/2
(Netgear Switch) (Interface 1/0/2)#ip access-group 101 in
(Netgear Switch) (Interface 1/0/2)#exit
(Netgear Switch) (Config)#exit
```

Web Interface: Set Up an IP ACL with Two Rules

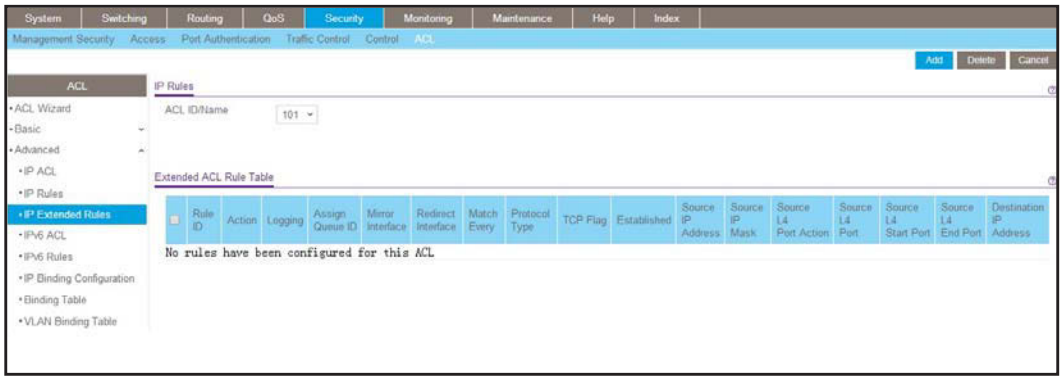
1. Create IP ACL 101 on the switch.
   a. Select **Security > ACL > IP ACL**.

      A screen similar to the following displays.



   b. In the **IP ACL ID** field, enter **101**.
   c. Click **Add** to create ACL 101.
2. Create a new rule associated with ACL 101.
   a. Select **Security > ACL > IP ACL > IP Extended Rules**.

      A screen similar to the following displays.

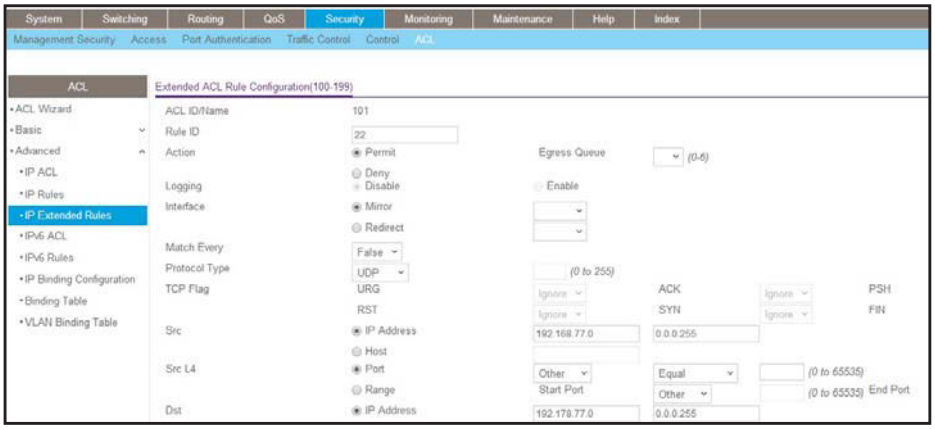


   b. For ACL ID, select **101**.

c. Click **Add** to create a new rule.

3. Create a new ACL rule and add it to ACL 101.

a. After you click the **Add** button in step 2, a screen similar to the following displays.



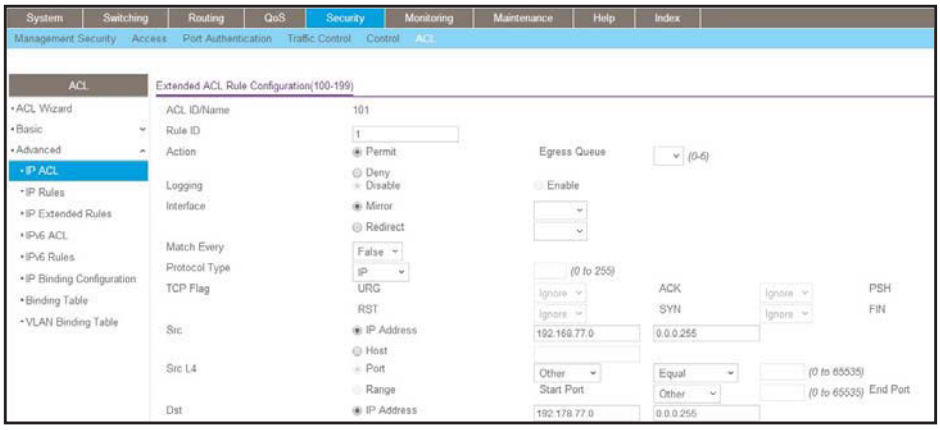
a. In the Extended ACL Rule Configuration, enter the following information:

- In the **Rule ID (1 to 23)** field, enter **1**.
- For Action, select the **Permit** radio button.
- In the **Protocol Type** list, select **TCP**.
- In the **Source IP Address** field, enter **192.168.77.0**.
- In the **Source IP Mask** field, enter **0.0.0.255**.
- In the **Destination IP Address** field, enter **192.178.77.0**.
- In the **Destination IP Mask** field, enter **0.0.0.255**.

b. Click **Apply** to save the settings.

4. Create another ACL rule and add it to the ACL 101.

a. After you click the **Add** button in step 3, a screen similar to the following displays.



b. Under Extended ACL Rule Configuration, enter the following information:

- In the **Rule ID (1 to 23)** field, enter **22**.
- For Action, select the **Permit** radio button.
- In the **Protocol Type** list, select **UDP**.

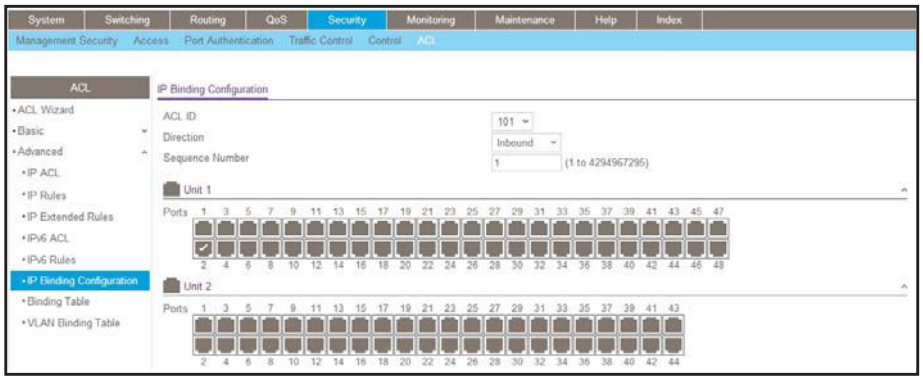
- In the **Source IP Address** field, enter **192.168.77.0**.
- In the **Source IP Mask** field, enter **0.0.0.255**.
- In the **Destination IP Address** field, enter **192.178.77.0**.
- In the **Destination IP Mask** field, enter **0.0.0.255**.

c. Click **Apply** to save the settings.

5. Apply ACL 101 to port 2.

a. Select **Security > ACL > IP ACL > IP Binding Configuration**.

A screen similar to the following displays.



b. Under IP Binding Configuration, enter the following information:

- In the **ACL ID** list, select **10**.
- In the **Sequence Number** field, enter **1**.

c. Click **Unit 1.** The ports display.

d. Click the gray box under port **2**. A check mark displays in the box.

e. Click **Apply** to save the settings.

One-Way Access Using a TCP Flag in an ACL

This example shows how to set up one-way access using a TCP flag in an ACL. PC 1 can access FTP server 1 and FTP server 2, but PC 2 can access only FTP server 2.

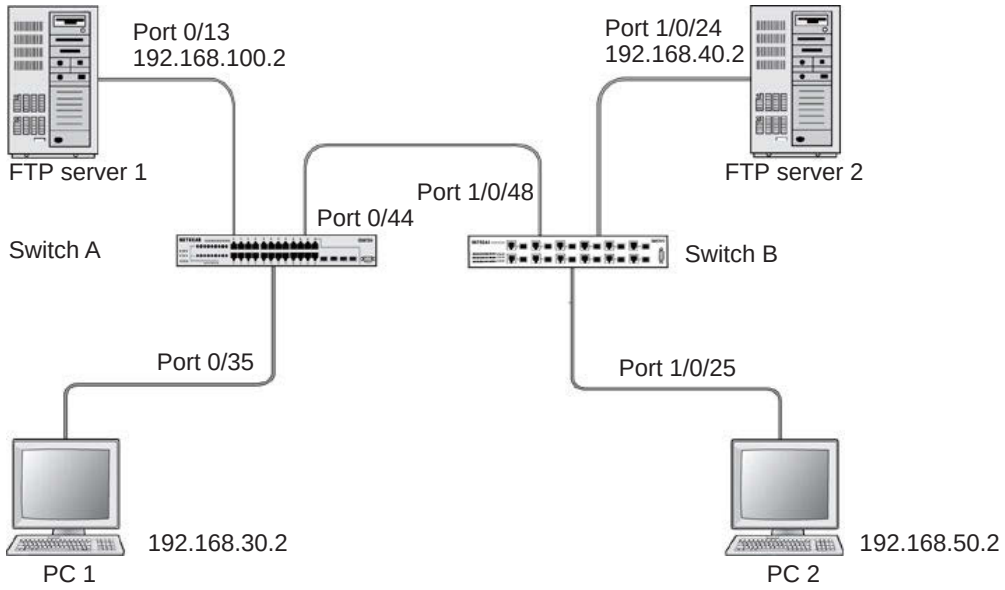


Figure 20. One-Way Web access using a TCP flag in an ACL

CLI: Configure One-Way Access Using a TCP Flag in an ACL

This is a two-step process:

- *Step 1: Configure the VLAN and IP addresses on Switch A* on page 170
- *Step 2: Configure on Switch B* on page 172

Step 1: Configure the VLAN and IP addresses on Switch A

(See *Figure 20, One-Way Web access using a TCP flag in an ACL.)*

1. Create VLAN 30 with port 0/35 and assign IP address 192.168.30.1/24.

```
(Netgear Switch) #vlan database
(Netgear Switch) (Vlan)#vlan 30
(Netgear Switch) (Vlan)#vlan routing 30
(Netgear Switch) (Vlan)#exit
(Netgear Switch) #config
(Netgear Switch) (Config)#interface 0/35
(Netgear Switch) (Interface 0/35)#vlan pvid 30
(Netgear Switch) (Interface 0/35)#vlan participation include 30
(Netgear Switch) (Interface 0/35)#exit
(Netgear Switch) (Config)#interface vlan 30
(Netgear Switch) (Interface-vlan 30)#routing
(Netgear Switch) (Interface-vlan 30)#ip address 192.168.30.1 255.255.255.0
(Netgear Switch) (Interface-vlan 30)#exit
(Netgear Switch) (Config)#exit
```

2. Create VLAN 100 with port 0/13 and assign IP address 192.168.100.1/24.

```
(Netgear Switch) #vlan database
(Netgear Switch) (Vlan)#vlan 100
(Netgear Switch) (Vlan)#vlan routing 100
(Netgear Switch) (Vlan)#exit
(Netgear Switch) #configure
(Netgear Switch) (Config)#interface 0/13
(Netgear Switch) (Interface 0/13)#vlan pvid 100
(Netgear Switch) (Interface 0/13)#vlan participation include 100
(Netgear Switch) (Interface 0/13)#exit
(Netgear Switch) (Config)#interface vlan 100
(Netgear Switch) (Interface-vlan 100)#routing
(Netgear Switch) (Interface-vlan 100)#ip address 192.168.100.1 255.255.255.0
(Netgear Switch) (Interface-vlan 100)#exit
(Netgear Switch) (Config)#exit
```

3. Create VLAN 200 with port 0/44 and assign IP address 192.168.200.1/24.

```
(Netgear Switch) #vlan database
(Netgear Switch) (Vlan)#vlan 200
(Netgear Switch) (Vlan)#vlan routing 200
(Netgear Switch) (Vlan)#exit
(Netgear Switch) #configure
(Netgear Switch) (Config)#interface 0/44
(Netgear Switch) (Interface 0/44)#vlan pvid 200
(Netgear Switch) (Interface 0/44)#vlan participation include 200
(Netgear Switch) (Interface 0/44)#exit
(Netgear Switch) (Config)#interface vlan 200
(Netgear Switch) (Interface-vlan 200)#routing
(Netgear Switch) (Interface-vlan 200)#ip address 192.168.200.1 255.255.255.0
(Netgear Switch) (Interface-vlan 200)#exit
```

4. Add two static routes so that the switch forwards the packets for which the destinations are 192.168.40.0/24 and 192.168.50.0/24 to the correct next hops.

```
(Netgear Switch) (Config)#ip routing
(Netgear Switch) (Config)#ip route 192.168.40.0 255.255.255.0 192.168.200.2
(Netgear Switch) (Config)#ip route 192.168.50.0 255.255.255.0 192.168.200.2
```

5. Create an ACL that denies all the packets with TCP flags +syn-ack.

```
(Netgear Switch) (Config)#access-list 101 deny tcp any flag +syn -ack
```

6. Create an ACL that permits all the IP packets.

```
(Netgear Switch) (Config)#access-list 102 permit ip any
```

7. Apply ACLs 101 and 102 to port 0/44; the sequence of 101 is 1 and of 102 is 2.

```
(Netgear Switch) (Config)#interface 0/44
(Netgear Switch) (Interface 0/44)#ip access-group 101 in 1
(Netgear Switch) (Interface 0/44)#ip access-group 102 in 2
(Netgear Switch) (Interface 0/44)#exit
```

Step 2: Configure on Switch B

(See *Figure 20, One-Way Web access using a TCP flag in an ACL on page 169.*)

1. Create VLAN 40 with port 1/0/24 and assign IP address 192.168.40.1/24.

```
(Netgear Switch) #vlan database
(Netgear Switch) (Vlan)#vlan 40
(Netgear Switch) (Vlan)#vlan routing 40
(Netgear Switch) #configure
(Netgear Switch) (Config)#interface 1/0/24
(Netgear Switch) (Interface 1/0/24)#vlan pvid 40
(Netgear Switch) (Interface 1/0/24)#vlan participation include 40
(Netgear Switch) (Interface 1/0/24)#exit
(Netgear Switch) (Config)#interface vlan 40
(Netgear Switch) (Interface-vlan 40)#routing
(Netgear Switch) (Interface-vlan 40)#ip address 192.168.40.1 255.255.255.0
(Netgear Switch) (Interface-vlan 40)#exit
```

2. Create VLAN 50 with port 1/0/25 and assign IP address 192.168.50.1/24.

```
(Netgear Switch)(Config)#exit
(Netgear Switch) #vlan database
(Netgear Switch) (Vlan)#vlan 50
(Netgear Switch) (Vlan)#vlan routing 50
(Netgear Switch) (Vlan)#exit
(Netgear Switch) #configure
(Netgear Switch) (Config)#interface 1/0/25
(Netgear Switch) (Interface 1/0/25)#vlan pvid 50
(Netgear Switch) (Interface 1/0/25)#vlan participation include 50
(Netgear Switch) (Interface 1/0/25)#exit
(Netgear Switch) (Config)#interface vlan 50
(Netgear Switch) (Interface-vlan 50)#routing
(Netgear Switch) (Interface-vlan 50)#ip address 192.168.50.1 255.255.255.0
(Netgear Switch) (Interface-vlan 50)#exit
(Netgear Switch) (Config)#exit
```

3. Create VLAN 200 with port 1/0/48 and assign IP address 192.168.200.1/24.

```
(Netgear Switch) #vlan database
(Netgear Switch) (Vlan)#vlan 200
(Netgear Switch) (Vlan)#vlan routing 200
(Netgear Switch) (Config)#interface 1/0/48
(Netgear Switch) (Interface 1/0/48)#vlan pvid 200
(Netgear Switch) (Interface 1/0/48)#vlan participation include 200
(Netgear Switch) (Interface 1/0/48)#exit
(Netgear Switch) #interface vlan 200
(Netgear Switch) (Interface-vlan 200)#routing
(Netgear Switch) (Interface-vlan 200)#ip address 192.168.200.2 255.255.255.0
(Netgear Switch) (Interface-vlan 200)#exit
```

4. Add two static routes so that the switch forwards the packets with destinations 192.168.100.0/24 and 192.168.30.0/24 to the correct next hops.

```
(Netgear Switch) (Config)#ip routing
(Netgear Switch) (Config)#ip route 192.168.100.0 255.255.255.0 192.168.200.1
(Netgear Switch) (Config)#ip route 192.168.30.0 255.255.255.0 192.168.200.1
```

Web Interface: Configure One-Way Access Using a TCP Flag in an ACL

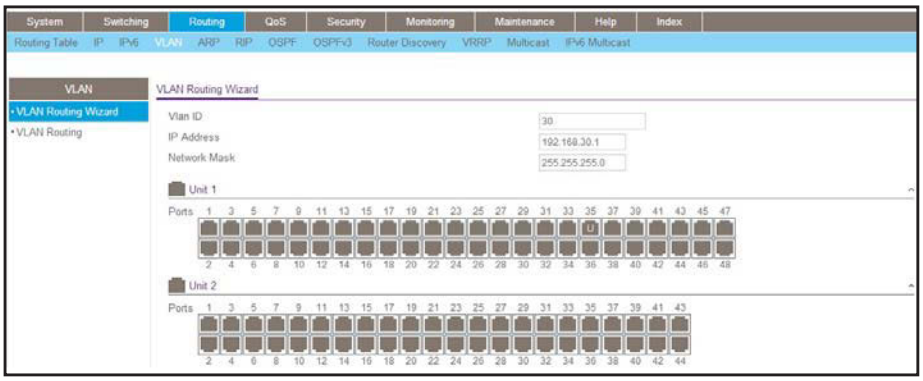
This is a two-part process:

- *Configuring VLAN and IP addresses on switch A* on page 173
- *Configuring the Switch B* on page 181

Configuring VLAN and IP addresses on switch A

1. Create VLAN 30 with IP address 192.168.30.1/24.
   a. Select **Routing > VLAN > VLAN Routing Wizard**.

      A screen similar to the following displays.



b. In the VLAN Routing Wizard, enter the following information:
   - In the **Vlan ID** field, enter **30**.
   - In the **IP Address** field, enter **192.168.30.1**.
   - In the **Network Mask** field, enter **255.255.255.0**.

c. Click **Unit 1**. The ports display.

d. Click the gray box under port **35** twice until **U** displays.

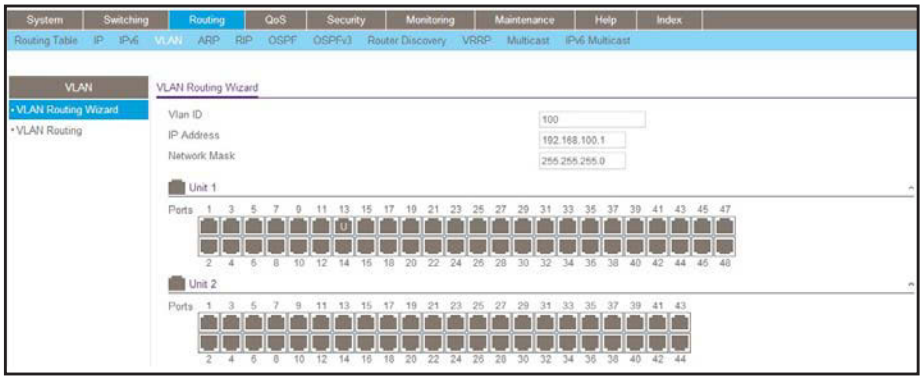
   The U specifies that the egress packet is untagged for the port.

e. Click **Apply** to save VLAN 30.

2. Create VLAN 100 with IP address 192.168.100.1/24.

a. Select **Routing > VLAN > VLAN Routing Wizard**.

   A screen similar to the following displays.



b. Enter the following information:
   - In the **Vlan ID** field, enter **100**.
   - In the **IP Address** field, enter **192.168.100.1**.
   - In the **Network Mask** field, enter **255.255.255.0**.

c. Click **Unit 1**. The ports display.

d. Click the gray box under port **13** twice until **U** displays.

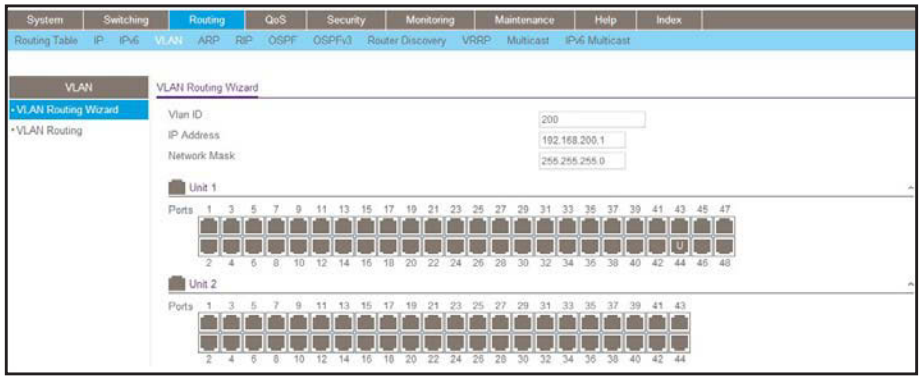
   The U specifies that the egress packet is untagged for the port.

e. Click **Apply** to save VLAN 100.

3. Create VLAN 200 with IP address 192.168.200.1/24.

a. Select **Routing > VLAN > VLAN Routing Wizard**.

A screen similar to the following displays.



b. Enter the following information:

- In the **Vlan ID** field, enter **200**.
- In the **IP Address** field, enter **192.168.200.1**.
- In the **Network Mask** field, enter **255.255.255.0**.

c. Click **Unit 1**. The ports display.

d. Click the gray box under port **44** twice until **U** displays.

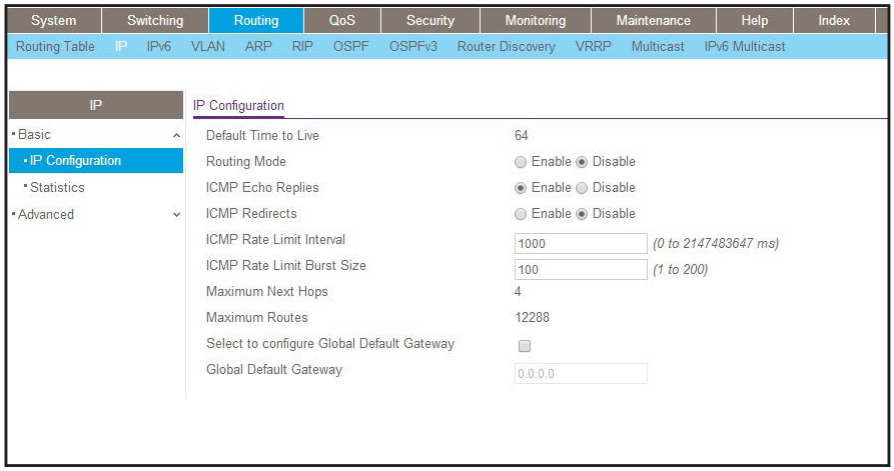
The U specifies that the egress packet is untagged for the port.

e. Click **Apply** to save VLAN 200.

4. Enable IP routing.

a. Select **Routing > IP > Basic > IP Configuration**.

A screen similar to the following displays.



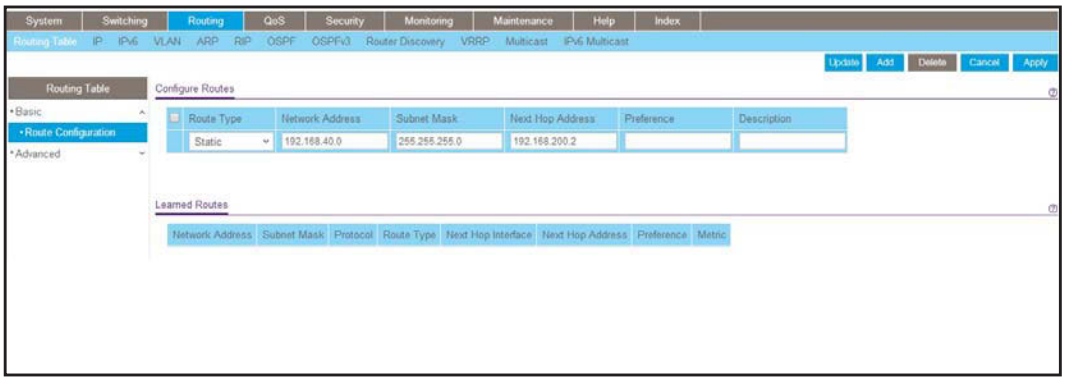
b. Under IP Configuration, make the following selections:

- For Routing Mode, select the **Enable** radio button.
- For IP Forwarding Mode, select the **Enable** radio button.

c. Click **Apply** to enable IP routing.

5. Add a static route with IP address 192.268.40.0/24:
   a. Select **Routing > Routing Table > Basic > Route Configuration**.

      A screen similar to the following displays.

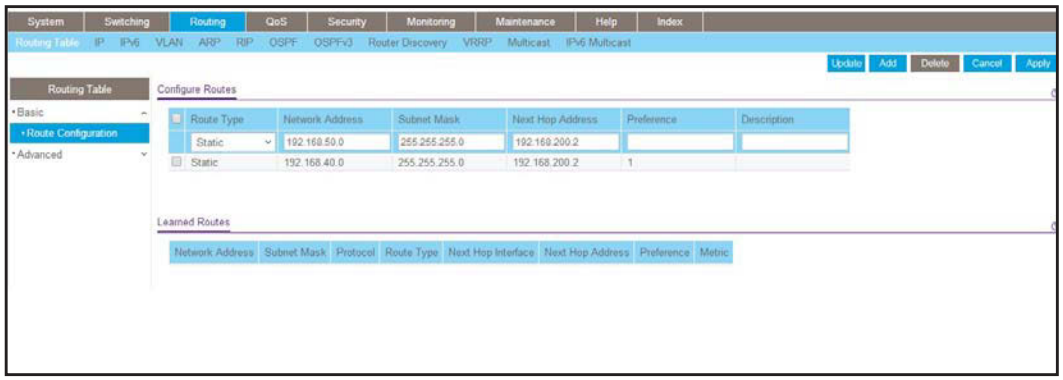


   b. Under Configure Routes, make the following selection and enter the following information:
      - In the Route Type list, select **Static**.
      - In the **Network Address** field, enter **192.168.40.0**.
      - In the **Subnet Mask** field, enter **255.255.255.0**.
      - In the **Next Hop IP Address** field, enter **192.168.200.2**.

   c. Click **Add**.

6. Create a static route with IP address 192.168.50.0/24:
   a. Select **Routing > Routing Table > Basic > Route Configuration**.

      A screen similar to the following displays.

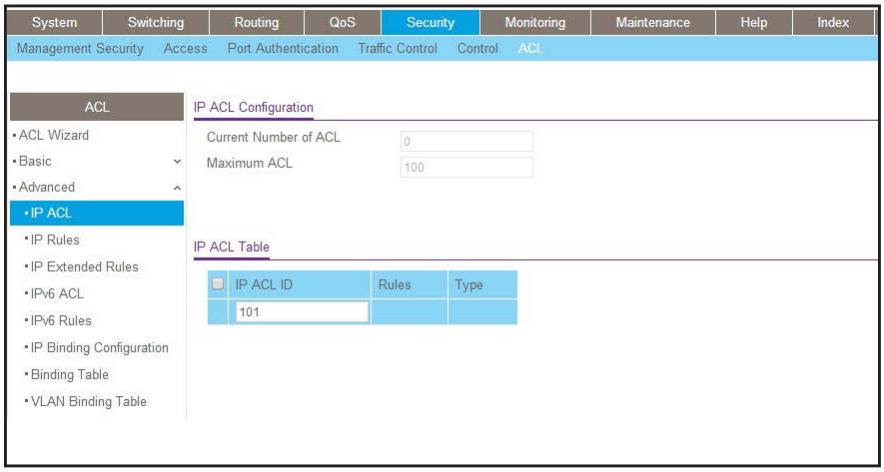


   b. Under Configure Routes, make the following selection and enter the following information:
      - In the **Route Type** list, select **Static**.
      - In the **Network Address** field, enter **192.168.50.0**.
      - In the **Subnet Mask** field, enter **255.255.255.0**.
      - In the **Next Hop IP Address** field, enter **192.168.200.2**.

   c. Click **Add**.

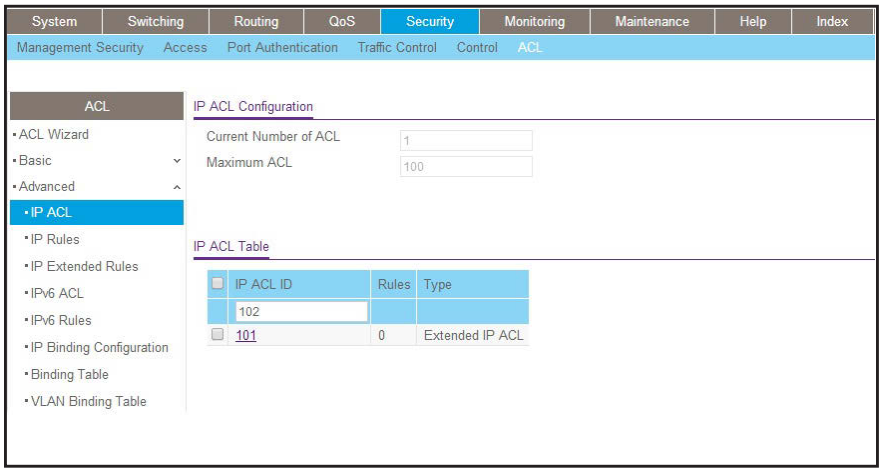
7. Create an ACL with ID 101.
   a. Select **Security > ACL > Advanced > IP ACL**.

      A screen similar to the following displays.



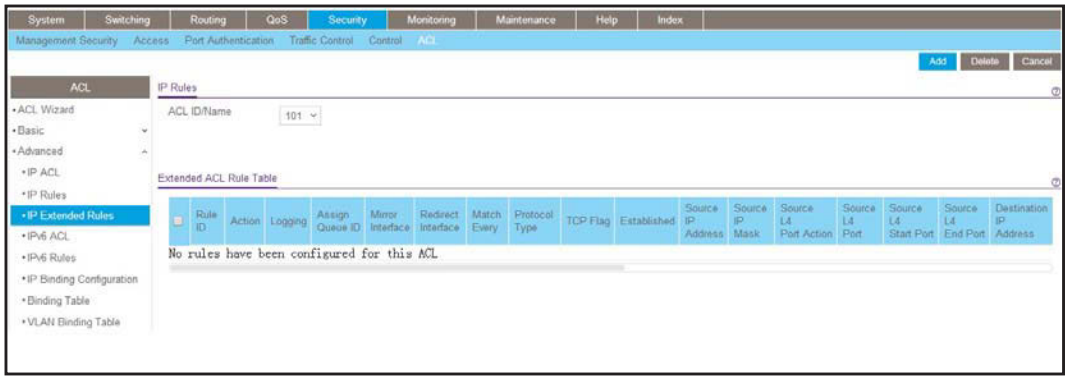
   b. In the IP ACL Table, in the **IP ACL ID** field, enter **101**.
   c. Click **Add**.
8. Create an ACL with ID 102.
   a. Select **Security > ACL > Advanced > IP ACL**.

      A screen similar to the following displays.



   b. In the IP ACL Table, in the **IP ACL ID** field, enter **102**.
   c. Click **Add**.
9. Add and configure an IP extended rule that is associated with ACL 101.
   a. Select **Security > ACL > Advanced > IP Extended Rules**.

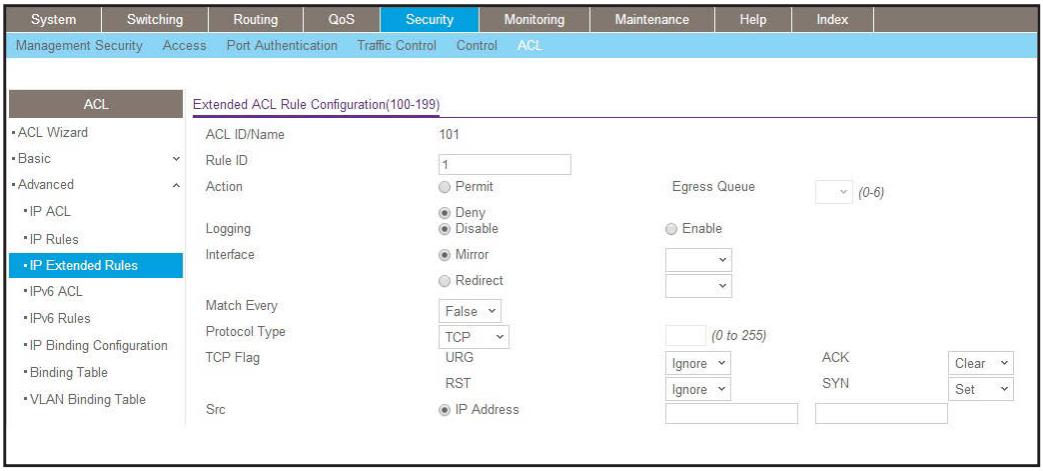
A screen similar to the following displays.



b. Under IP Extended Rules, in the **ACL ID** list, select **101**.

c. Click **Add**.

A screen similar to the following displays.



d. Under Extended ACL Rule Configuration (100-199), enter the following information and make the following selections:

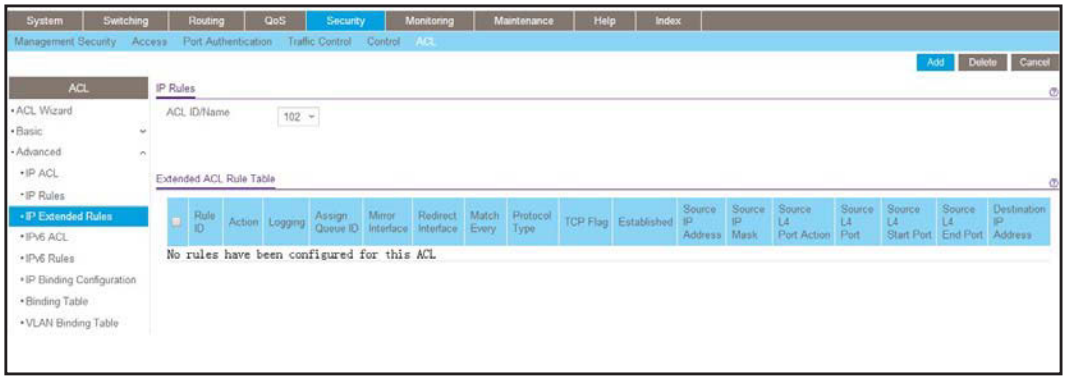
- In the **Rule ID** field, enter **1**.
- For Action mode, select the **Deny** radio button.
- In the **Match Every** field, select **False**.
- In the **Protocol Type** list, select **TCP**.
- For TCP Flag, in the **SYN** field, select **Set**, and in the **ACK** field, select **Clear**.

e. Click **Apply** to save the settings.

10. Add and configure an IP extended rule that is associated with ACL 102.

a. Select **Security > ACL > Advanced > IP Extended Rules**.

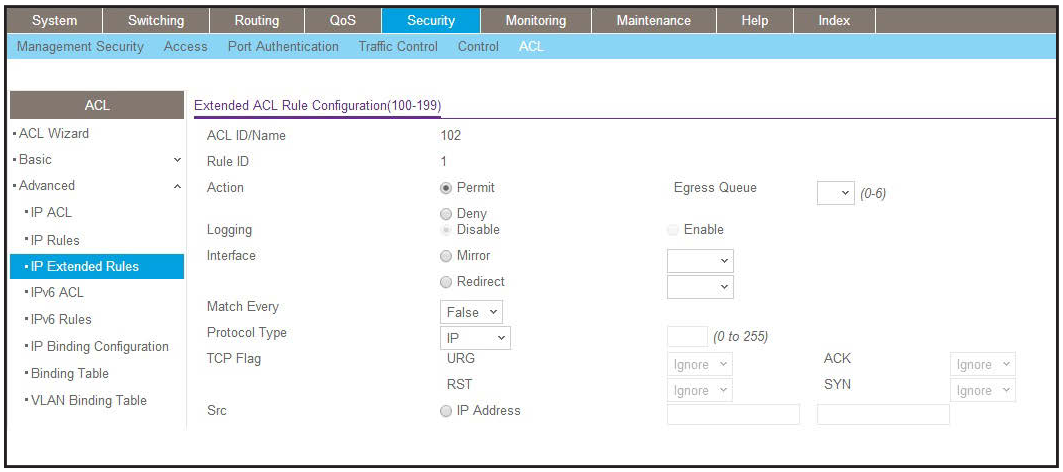
A screen similar to the following displays.



b. Under IP Extended Rules, in the **ACL ID** list, select **102**.

c. Click **Add**.

A screen similar to the following displays.



d. Under Extended ACL Rule Configuration (100-199), enter the following information and make the following selections:

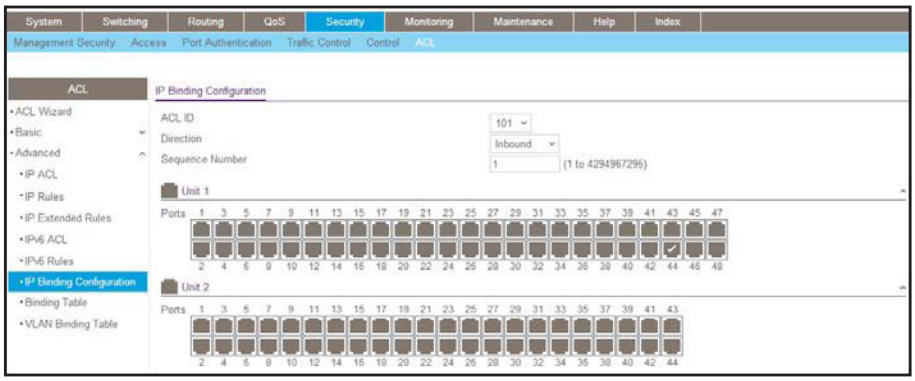
- In the **Rule ID** field, enter **1**.
- For Action, select the **Permit** radio button.
- In the **Match Every** field, select **False**.
- In the **Protocol Type** list, select **IP**.

e. Click **Apply** to save the settings.

11. Apply ACL 101 to port 44.

a. Select **Security > ACL > Advanced > IP Binding Configuration**.

A screen similar to the following displays.



b. Under Binding Configuration, specify the following:

- In the **ACL ID** list, select **101**.
- In the **Sequence Number** field, enter **1**.

c. Click **Unit 1**. The ports display.

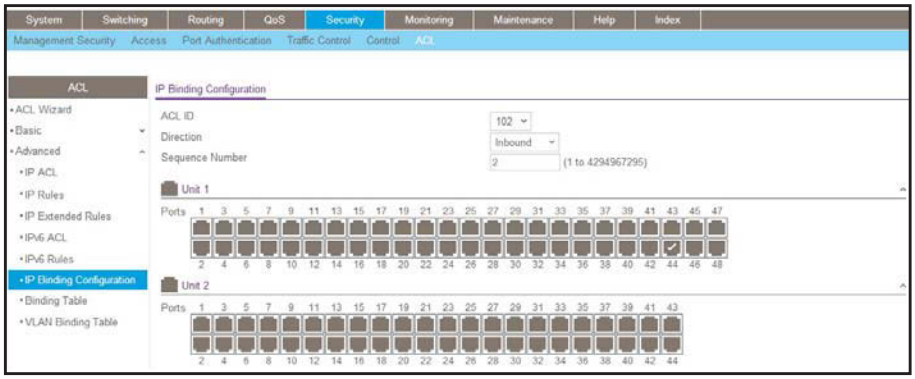
d. Click the gray box under port **44**. A check mark displays in the box.

e. Click **Apply** to save the settings.

12. Apply ACL 102 to port 44.

a. Select **Security > ACL > Advanced > IP Binding Configuration**.

A screen similar to the following displays.



b. Under Binding Configuration, make the following selection and enter the following information:

- In the **ACL ID** list, select **102**.
- In the **Sequence Number** field, enter **2**.

c. Click **Unit 1**. The ports display.

d. Click the gray box under port **44**.

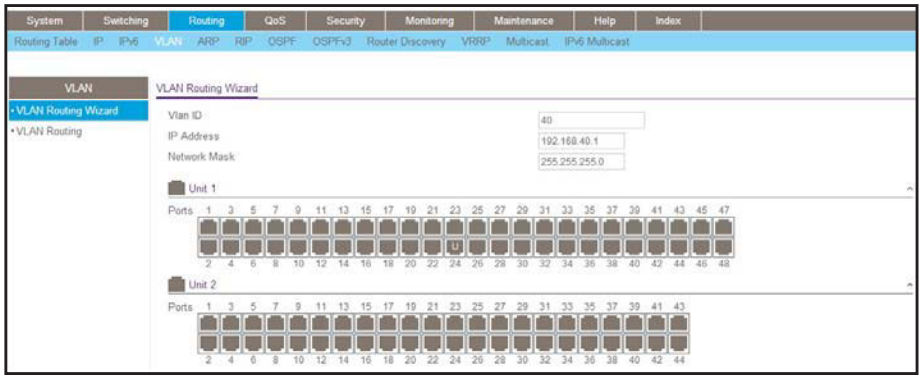
A check mark displays in the box.

e. Click **Apply** to save the settings.

Configuring the Switch B

1. Create VLAN 40 with IP address 192.168.40.1/24.
   a. Select **Routing > VLAN > VLAN Routing Wizard**.

      A screen similar to the following displays.



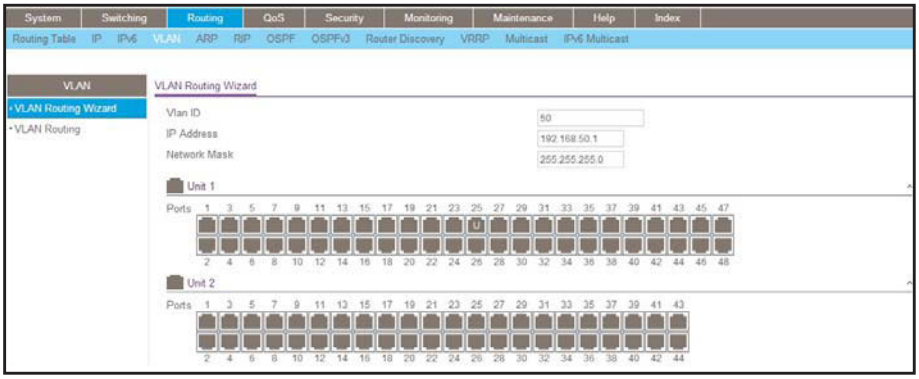
   b. Enter the following information:
      - In the **Vlan ID** field, enter **40**.
      - In the **IP Address** field, enter **192.168.40.1**.
      - In the **Network Mask** field, enter **255.255.255.0**.

   c. Click **Unit 1**. The ports display.
   d. Click the gray box under port **24** twice until **U** displays.

      The U specifies that the egress packet is untagged for the port.

   e. Click **Apply** to save VLAN 40.
2. Create VLAN 50 with IP address 192.168.50.1/24:
   a. Select **Routing > VLAN > VLAN Routing Wizard**.

      A screen similar to the following displays.



   b. Enter the following information:
      - In the **Vlan ID** field, enter **50**.
      - In the **IP Address** field, enter **192.168.50.1**.
      - In the **Network Mask** field, enter **255.255.255.0**.

c. Click **Unit 1**. The ports display.

d. Click the gray box under port **25** twice until **U** displays.

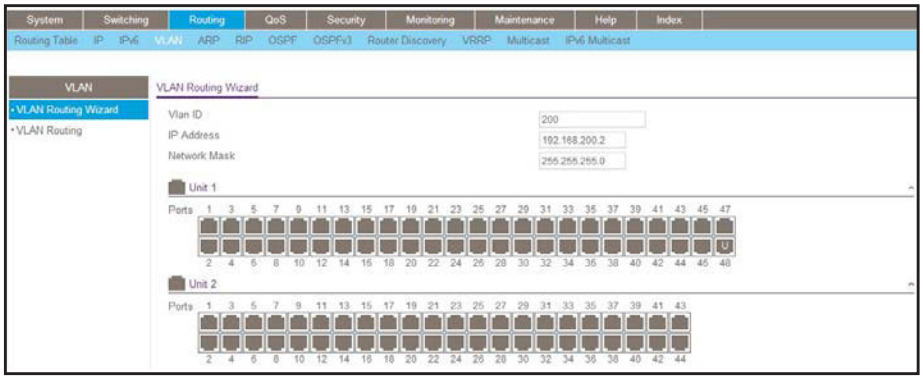
The U specifies that the egress packet is untagged for the port.

e. Click **Apply** to save VLAN 50.

3. Create VLAN 200 with IP address 192.168.200.2/24.

a. Select **Routing > VLAN > VLAN Routing Wizard**.

A screen similar to the following displays.



b. Enter the following information:

- In the **Vlan** ID field, enter **200**.
- In the **IP Address** field, enter **192.168.200.2**.
- In the **Network Mask** field, enter **255.255.255.0**.

c. Click **Unit 1**. The ports display.

d. Click the gray box under port **48** twice until U displays.

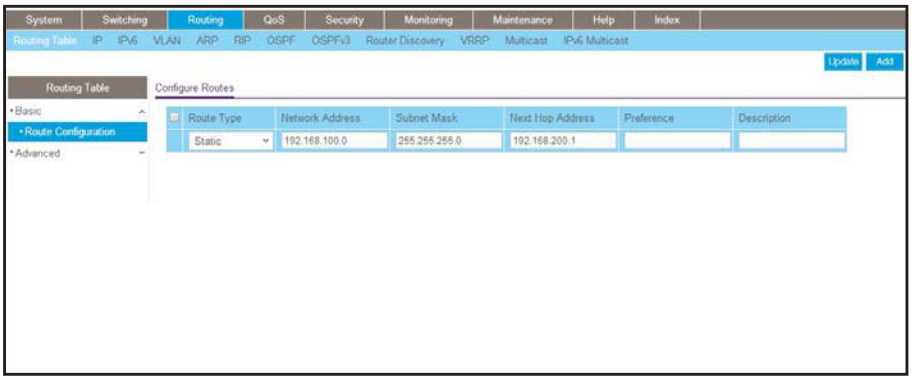
The U specifies that the egress packet is untagged for the port.

e. Click **Apply** to save VLAN 200.

4. Create a static route with IP address 192.168.100.0/24:

a. Select **Routing > Routing Table > Basic > Route Configuration**.

A screen similar to the following displays.



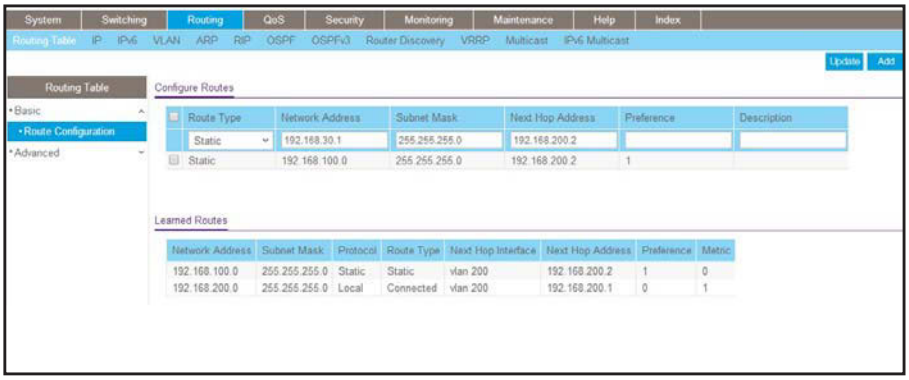
b. Under Configure Routes, make the following selections and enter the following information:
   - Select **Static** in the **Route Type** field.
   - In the **Network Address** field, enter **192.168.100.0**.
   - In the **Subnet Mask** field, enter **255.255.255.0**.
   - In the **Next Hop IP Address** field, enter **192.168.200.1**.

c. Click **Add**.

5. Create a static route with IP address 192.168.30.0/24:

a. Select **Routing > Routing Table > Basic > Route Configuration**.

A screen similar to the following displays.



b. Under Configure Routes, make the following selection and enter the following information:
   - In the **Route Type** field, select **Static**.
   - In the **Network Address** field, enter **192.168.30.0**.
   - In the **Subnet Mask** field, enter **255.255.255.0**.
   - In the **Next Hop IP Address** field, enter **192.168.200.1**.

c. Click **Add**.

Use ACLs to Configure Isolated VLANs on a Layer 3 Switch

This example shows how to isolate VLANs on a Layer 3 switch by using ACLs. In this example, PC 1 is in VLAN 24, PC 2 is in VLAN 48, and the server is in VLAN 38. PC 1 and PC 2 are isolated by an ACL but can both access the server. The example is shown as CLI commands and as a web interface procedure.

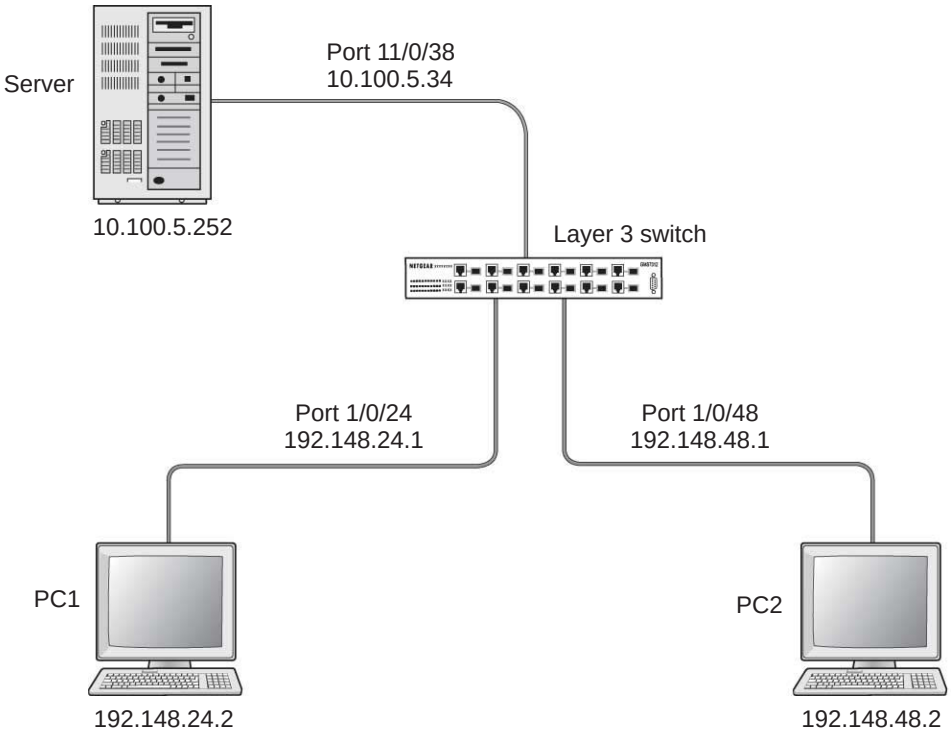


Figure 21. Using ACLs to isolate VLANs on a Layer 3 switch

CLI: Configure One-Way Access Using a TCP Flag in ACL Commands

1. Enter the following CLI commands.

```
(Netgear Switch) #vlan database
(Netgear Switch) (Vlan)#vlan 24
(Netgear Switch) (Vlan)#vlan routing 24
(Netgear Switch) (Vlan)#exit
(Netgear Switch) #config
(Netgear Switch) (Config)#interface 1/0/24
(Netgear Switch) (Interface 1/0/24)#vlan participation include 24
(Netgear Switch) (Interface 1/0/24)#vlan pvid 24
(Netgear Switch) (Interface 1/0/24)#exit

(Netgear Switch) (Config)#interface vlan 24
(Netgear Switch) (Interface-vlan 24)#routing
(Netgear Switch) (Interface-vlan 24)#ip address 192.168.24.1 255.255.255.0
(Netgear Switch) (Interface-vlan 24)#exit
(Netgear Switch) (Config)#exit
```

2. Create VLAN 48, add port 1/0/48 to it, and assign IP address 192.168.48.1 to it.

```
(Netgear Switch) #vlan database
(Netgear Switch) (Vlan)#vlan 48
(Netgear Switch) (Vlan)#vlan routing 48
(Netgear Switch) (Vlan)#exit
(Netgear Switch) #config
(Netgear Switch) (Config)#interface 1/0/48
(Netgear Switch) (Interface 1/0/48)#vlan participation include 48
(Netgear Switch) (Interface 1/0/48)#vlan pvid 48
(Netgear Switch) (Interface 1/0/48)#exit

(Netgear Switch) (Config)#vlan interface vlan 48
(Netgear Switch) (Interface-vlan 48)#routing
(Netgear Switch) (Interface-vlan 48)#ip address 192.168.48.1 255.255.255.0
(Netgear Switch) (Interface-vlan 48)#exit
(Netgear Switch) (Config)#exit
```

3. Create VLAN 38, add port 1/0/38 to it, and assign IP address 10.100.5.34 to it.

```
(Netgear Switch) #vlan database
(Netgear Switch) (Vlan)#vlan 38
(Netgear Switch) (Vlan)#vlan routing
(Netgear Switch) (Vlan)#exit
(Netgear Switch) #config
(Netgear Switch) (Config)#interface 1/0/38
(Netgear Switch) (Interface 1/0/38)#vlan participation include 38
(Netgear Switch) (Interface 1/0/38)#vlan pvid 38
(Netgear Switch) (Interface 1/0/38)#exit
(Netgear Switch) (Config)#interface vlan 38
(Netgear Switch) (Interface-vlan 38)#routing
(Netgear Switch) (Interface-vlan 38)#ip address 10.100.5.34 255.255.255.0
(Netgear Switch) (Interface-vlan 38)#exit
```

4. Enable IP routing on the switch.

```
(Netgear Switch) (Config)#ip routing
```

5. Add a default route so that all the traffic without a destination is forwarded according to this default route.

```
(Netgear Switch) (Config)#ip route default 10.100.5.252
```

6. Create ACL 101 to deny all traffic that has the destination IP address 192.168.24.0/24.

```
(Netgear Switch) (Config)#access-list 101 deny ip any 192.168.24.0 0.0.0.255
```

7. Create ACL 102 to deny all traffic that has the destination IP address 192.168.48.0/24.

```
(Netgear Switch) (Config)#access-list 102 deny ip any 192.168.48.0 0.0.0.255
```

8. Create ACL 103 to permit all other traffic.

```
(Netgear Switch) (Config)#access-list 103 permit ip any any
```

9. Deny all traffic with the destination IP address 192.168.48.0/24, and permit all other traffic.

```
(Netgear Switch) (Config)#interface 1/0/24
(Netgear Switch) (Interface 1/0/24)#ip access-group 102 in 1
(Netgear Switch) (Interface 1/0/24)#ip access-group 103 in 2
(Netgear Switch) (Interface 1/0/24)#exit
```

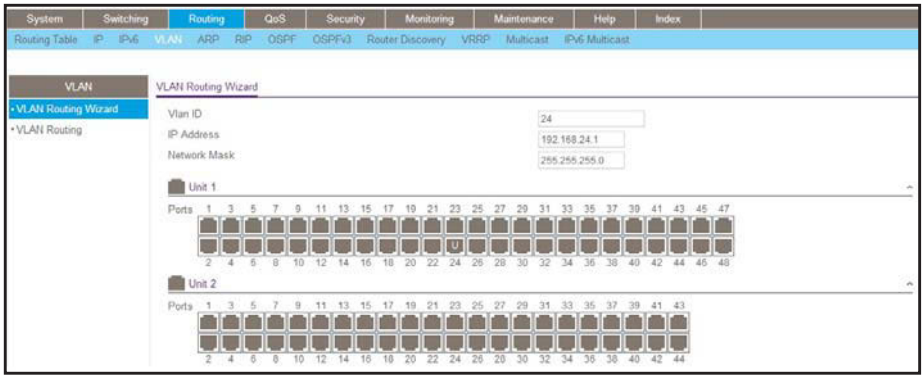
10. Deny all traffic with the destination IP address 192.168.24.0/24, and permit all other traffic.

```
(Netgear Switch) (Config)#interface 1/0/48
(Netgear Switch) (Interface 1/0/48)#ip access-group 101 in 1
(Netgear Switch) (Interface 1/0/48)#ip access-group 103 in 2
(Netgear Switch) (Interface 1/0/48)#exit
```

Web Interface: Configure One-Way Access Using a TCP Flag in an ACL

1. Create VLAN 24 with IP address 192.168.24.1.
   a. Select **Routing > VLAN > VLAN Routing Wizard**.

      A screen similar to the following displays.



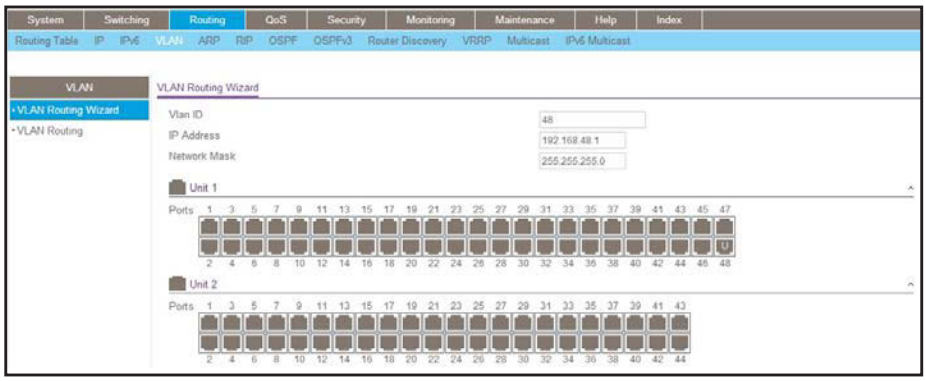
   b. Enter the following information:
      - In the **Vlan ID** field, enter **24**.
      - In the **IP Address** field, enter **192.168.24.1**.
      - In the **Network Mask** field, enter **255.255.255.0**.

   c. Click **Unit 1**. The ports display.
   d. Click the gray box under port **24** twice until **U** displays.

      The U specifies that the egress packet is untagged for the port.

   e. Click **Apply** to save VLAN 24.
2. Create VLAN 48 with IP address 192.168.48.1.
   a. Select **Routing > VLAN > VLAN Routing Wizard**.

A screen similar to the following displays.



b. Enter the following information:

- In the **Vlan ID** field, enter **48**.
- In the **IP Address** field, enter **192.168.48.1**.
- In the **Network Mask** field, enter **255.255.255.0**.

c. Click **Unit 1**. The ports display.

d. Click the gray box under port **48** twice until **U** displays.

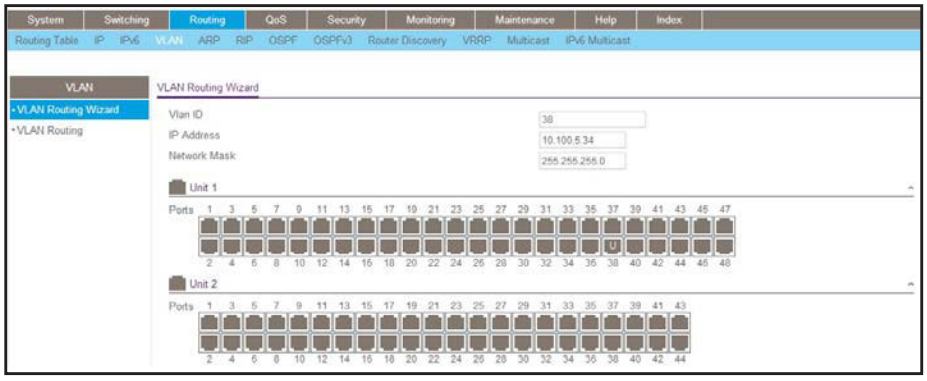
The U specifies that the egress packet is untagged for the port.

e. Click **Apply** to save VLAN 48.

3. Create VLAN 38 with IP address 10.100.5.34.

a. Select **Routing > VLAN > VLAN Routing Wizard**.

A screen similar to the following displays.



b. Enter the following information in the VLAN Routing Wizard:

- In the **Vlan ID** field, enter **38**.
- In the **IP Address** field, enter **10.100.5.34**.
- In the **Network Mask** field, enter **255.255.255.0**.

c. Click **Unit 1**. The ports display.

d. Click the gray box under port **38** twice until **U** displays.

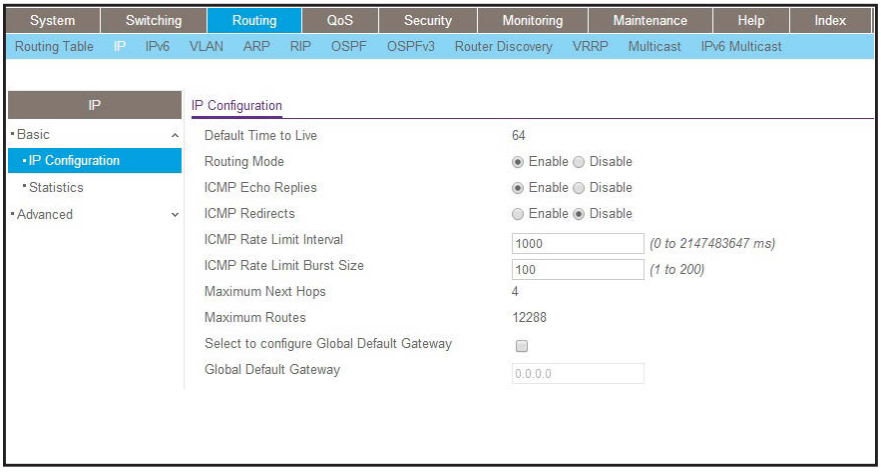
The U specifies that the egress packet is untagged for the port.

e. Click **Apply** to save VLAN 38.

4. Enable IP routing:

   a. Select **Routing > IP > Basic > IP Configuration**.

      A screen similar to the following displays.



   b. Under IP Configuration, make the following selections:

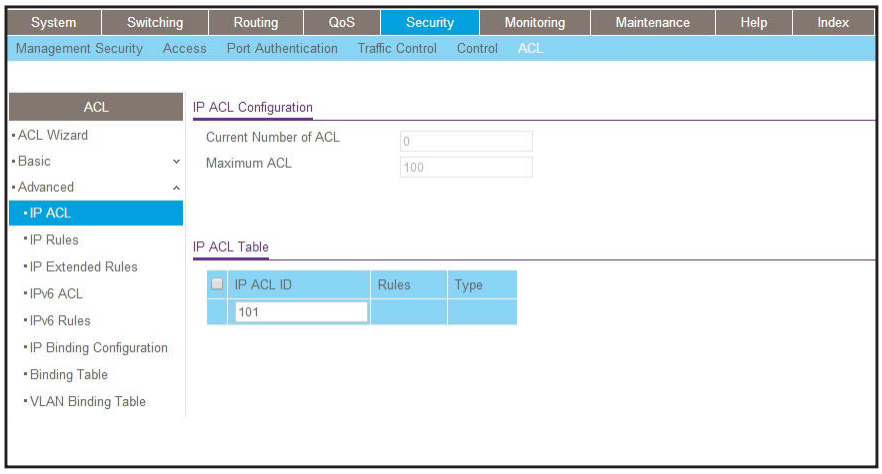
      - For Routing Mode, select the **Enable** radio button.
      - For IP Forwarding Mode, select the **Enable** radio button.

   c. Click **Apply** to enable IP routing.

5. Create an ACL with ID 101.

   a. Select **Security > ACL > Advanced > IP ACL**.

      A screen similar to the following displays.



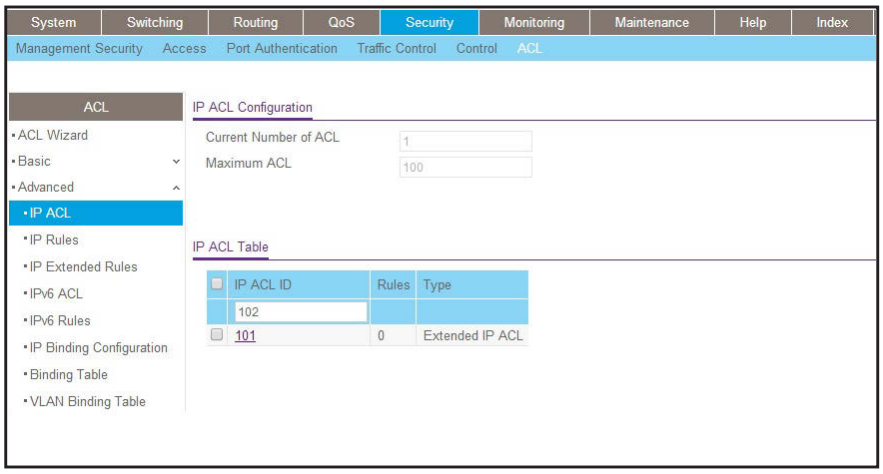
   b. In the IP ACL Table, in the **IP ACL ID** field, enter **101**.

   c. Click **Add**.

6. Create an ACL with ID 102.

   a. Select **Security > ACL > Advanced > IP ACL**.

A screen similar to the following displays.



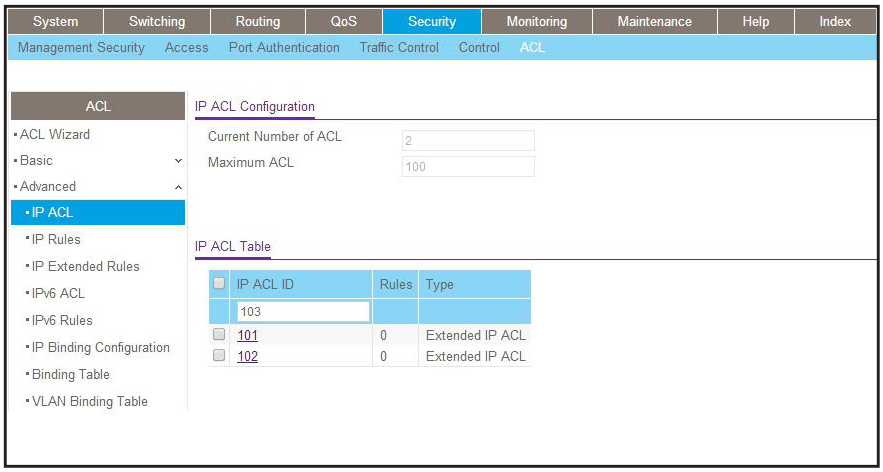
b. In the IP ACL Table, in the **IP ACL ID** field, enter **102**.

c. Click **Add**.

7. Create an ACL with ID 103.

a. Select **Security > ACL > Advanced > IP ACL**.

A screen similar to the following displays.



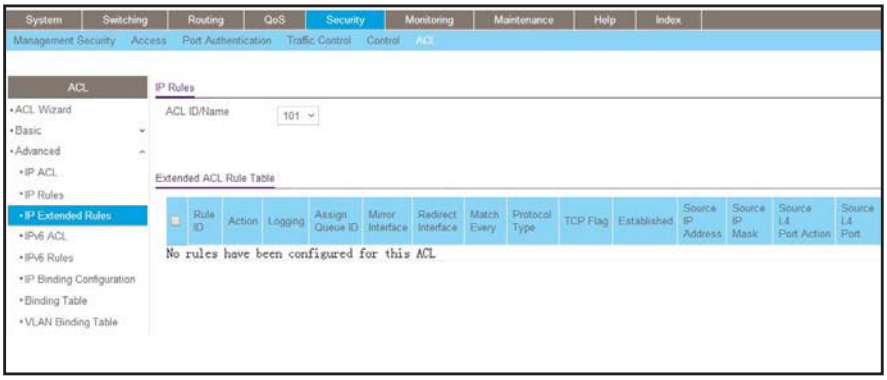
b. In the **IP ACL ID** field of the IP ACL Table, enter **103**.

c. Click **Add**.

8. Add and configure an IP extended rule that is associated with ACL 101:

a. Select **Security > ACL > Advanced > IP Extended Rules**.

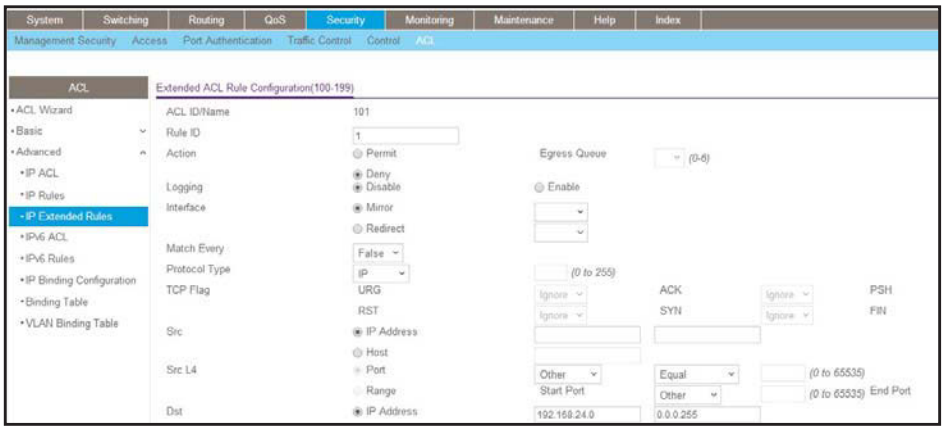
A screen similar to the following displays.



b. Under IP Extended Rules, in the **ACL ID** field, select **101**.

c. Click **Add**.

A screen similar to the following displays.



d. Under Extended ACL Rule Configuration (100-199), enter the following information and make the following selections:

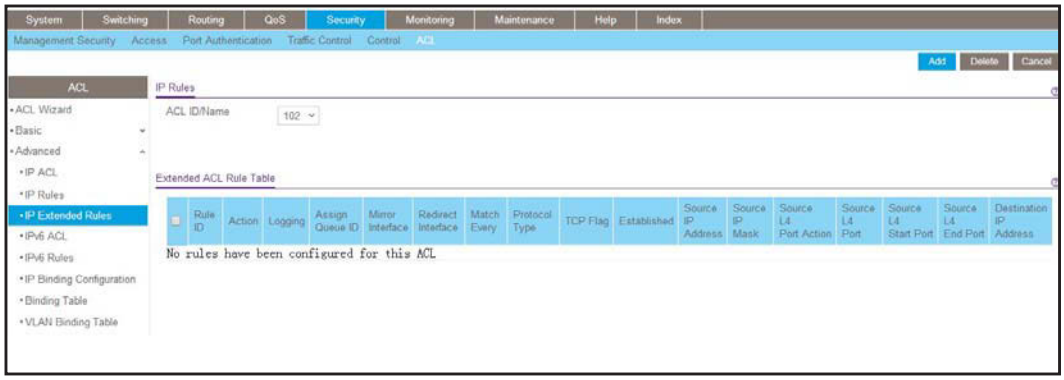
- In the **Rule ID** field, enter **1**.
- For Action, select the **Deny** radio button.
- In the **Match Every** field, select **False**.
- In the **Destination IP Address** field, enter **192.168.24.0**.
- In the **Destination IP Mask** field, enter **0.0.0.255**.

e. Click **Apply** to save the settings.

9. Add and configure an IP extended rule that is associated with ACL 102.

a. Select **Security > ACL > Advanced > IP Extended Rules**.

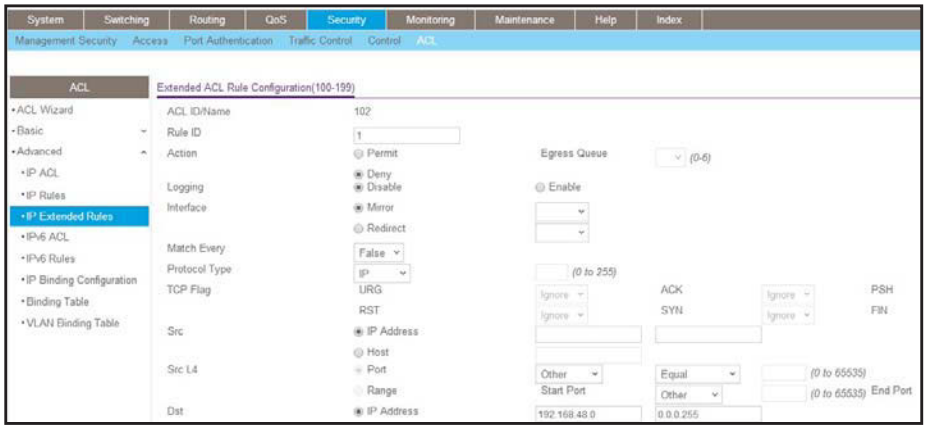
A screen similar to the following displays.



b. Under IP Extended Rules, in the **ACL ID** field, select **102**.

c. Click **Add**.

A screen similar to the following displays.



d. Under Extended ACL Rule Configuration (100-199), enter the following information and make the following selections:

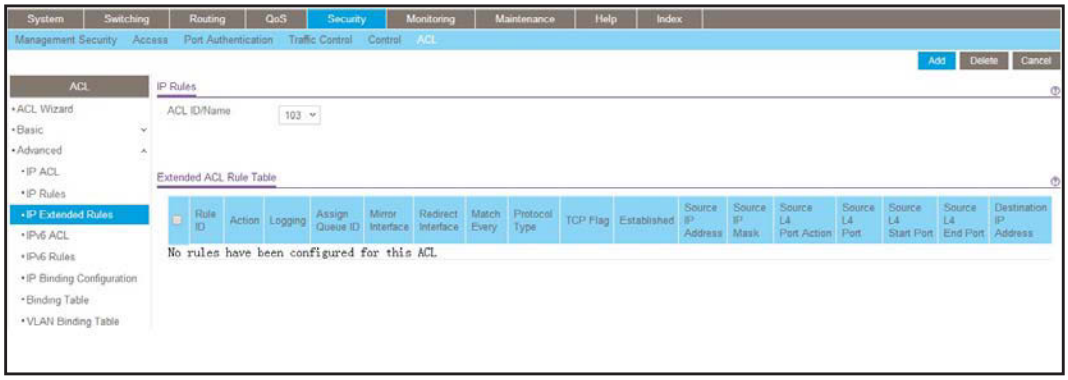
- In the **Rule ID** field, enter **1**.
- For Action mode, select the **Deny** radio button.
- In the **Match Every** field, select **False**.
- In the **Destination IP Address** field, enter **192.168.48.0**.
- In the **Destination IP Mask** field, enter **0.0.0.255**.

e. Click **Apply** to save the settings.

10. Add and configure an IP extended rule that is associated with ACL 103:

a. Select **Security > ACL > Advanced > IP Extended Rules**.

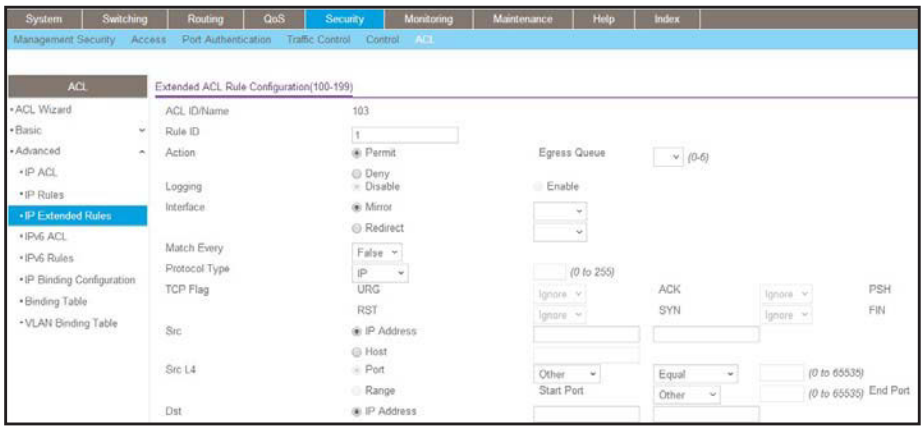
A screen similar to the following displays.



b. Under IP Extended Rules, in the **ACL ID** field, select **103**.

c. Click **Add**.

A screen similar to the following displays.



d. Under Extended ACL Rule Configuration (100-199), enter the following information and make the following selections:

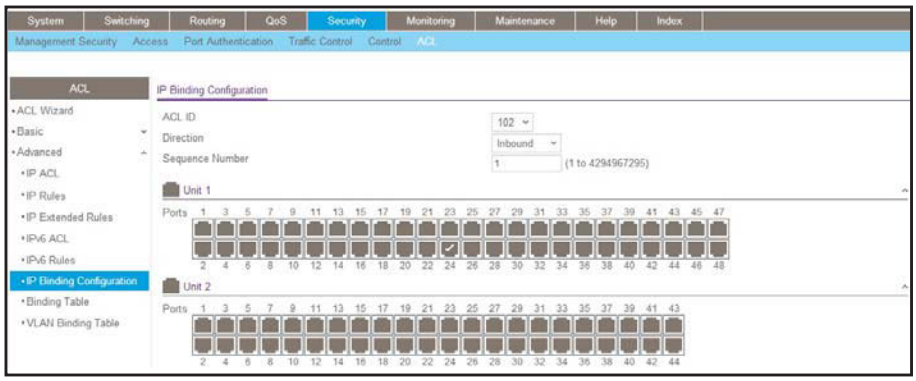
- In the **Rule ID** field, enter **1**.
- For Action mode, select the **Permit** radio button.
- In the **Match Every** field, select **False**.
- In the **Protocol Type** field, select **IP**.

e. Click **Apply** to save the settings.

11. Apply ACL 102 to port 24:

a. Select **Security > ACL > Advanced > IP Binding Configuration**.

A screen similar to the following displays.



b. Under Binding Configuration, make the following selection and enter the following information:

- In the **ACL ID** field, select **102**.
- In the **Sequence Number** field, enter **1**.

c. Click **Unit 1**. The ports display.

d. Click the gray box under port **24**.

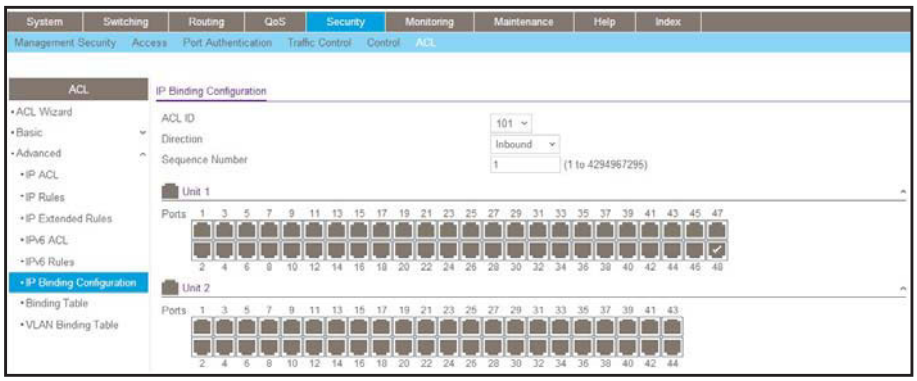
A check mark displays in the box.

e. Click **Apply** to save the settings.

12. Apply ACL 101 to port 48:

a. Select **Security > ACL > Advanced > IP Binding Configuration**.

A screen similar to the following displays.



b. Under Binding Configuration, make the following selection and enter the following information:

- In the **ACL ID** field, select **101**.
- In the **Sequence Number** field, enter **1**.

c. Click **Unit 1**. The ports display.

d. Click the gray box under port **48**.

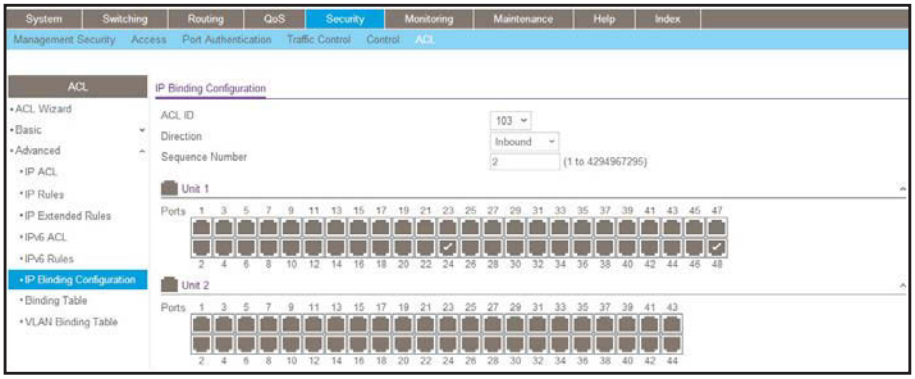
A check mark displays in the box.

e. Click **Apply** to save the settings.

13. Apply ACL 103 to port 24 and port 48:

a. Select **Security > ACL > Advanced > IP Binding Configuration**.

A screen similar to the following displays.



b. Under Binding Configuration, make the following selection and enter the following information:

- In the **ACL ID** field, select **103**.
- In the **Sequence Number** field, enter **2**.

c. Click **Unit 1**. The ports display.

Configure the following ports:

- Click the gray box under port **24**. A check mark displays in the box.
- Click the gray box under port **48**. A check mark displays in the box.

d. Click **Apply** to save the settings.

Set up a MAC ACL with Two Rules

The example is shown as CLI commands and as a web interface procedure.

CLI: Set up a MAC ACL with Two Rules

1. Create a new MAC ACL acl_bpdu.

```
(Netgear Switch) #
(Netgear Switch) #config
(Netgear Switch) (Config)#mac access-list extended acl_bpdu
```

2. Deny all the traffic that has destination MAC 01:80:c2:xx:xx:xx.

```
(Netgear Switch) (Config-mac-access-list)#deny any 01:80:c2:00:00:00
00:00:00:ff:ff:ff
```

3. Permit all the other traffic.

```
(Netgear Switch) (Config-mac-access-list)#permit any
(Netgear Switch) (Config-mac-access-list)#exit
```

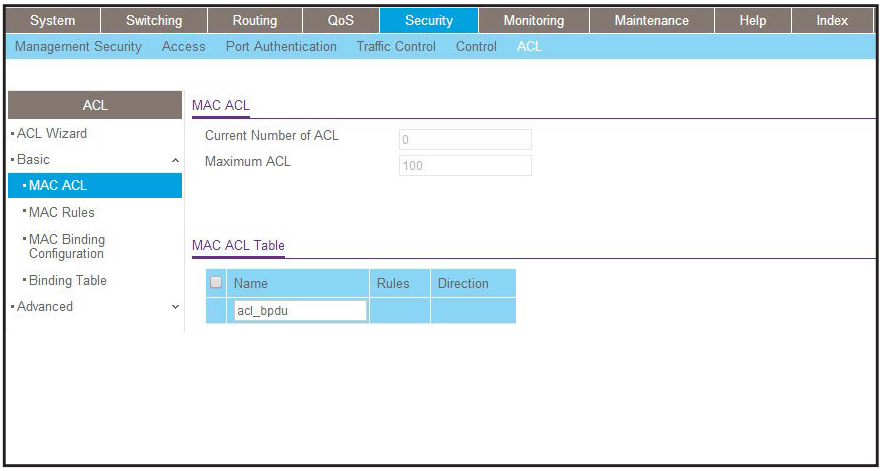
4. Apply the MAC ACL acl_bpdu to port 1/0/2.

```
(Netgear Switch) (Config)#interface 1/0/2
(Netgear Switch) (Interface 1/0/2)#mac access-group acl_bpdu in
```

Web Interface: Set up a MAC ACL with Two Rules

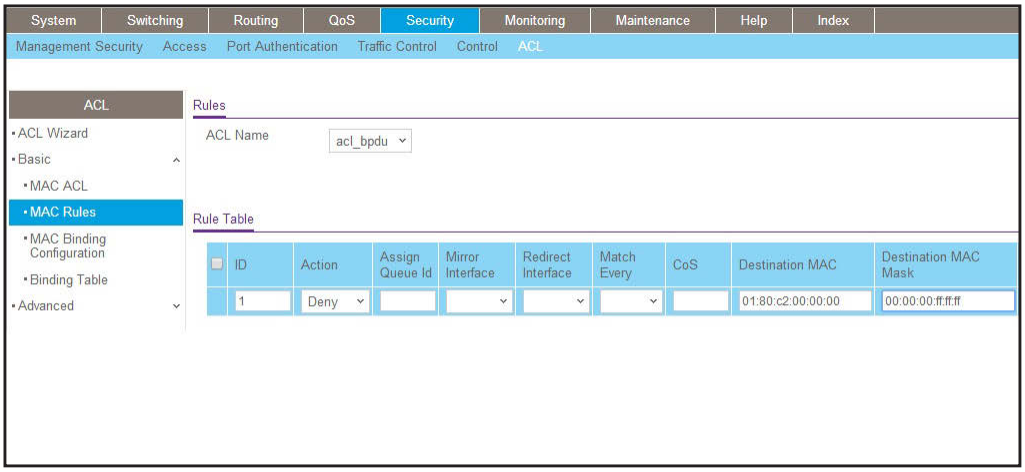
1. Create MAC ACL 101 on the switch.
   a. Select **Security > ACL > MAC ACL**.

      A screen similar to the following displays.



   b. In the **Name** field, enter **acl_bpdu**.
   c. Click **Add** to create ACL acl_bpdu.
2. Create a new rule that is associated with the ACL acl_bpdu.
   a. Select **Security > ACL > MAC ACL > MAC Rules**.

A screen similar to the following displays.



a. In the **ACL Name** field, select **acl_bpdu**.

b. In the **Action** field, select **Deny**.

c. Enter the following information in the Rule Table.

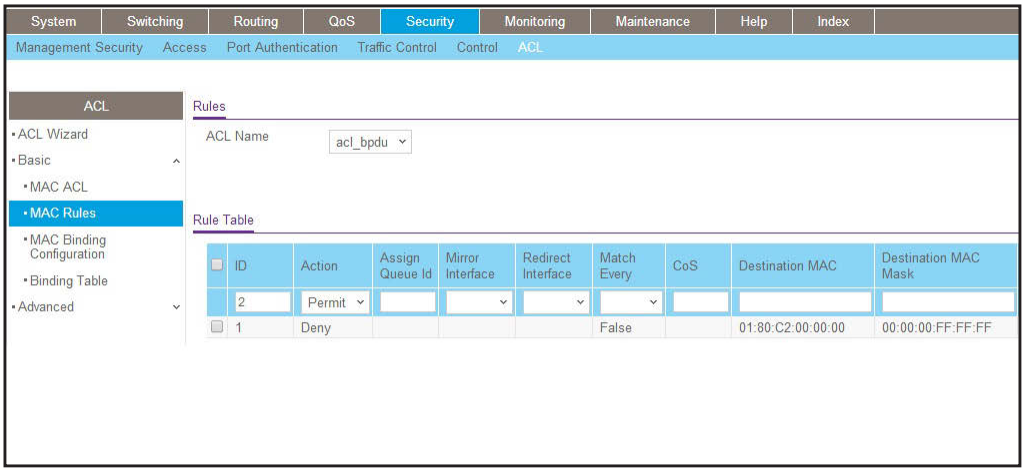
- In the **ID** field, enter **1**.
- In the **Destination MAC** field, enter **01:80:c2:00:00:00**.
- In the **Destination MAC Mask** field, enter **00:00:00:ff:ff:ff**.

d. Click the **Add** button.

3. Create another rule that is associated with the ACL acl_bpdu.

a. Select **Security > ACL > MAC ACL > MAC Rules**.

A screen similar to the following displays.



a. Select **acl_bpdu** in the **ACL Name** field.

b. Enter the following information in the Rule Table.

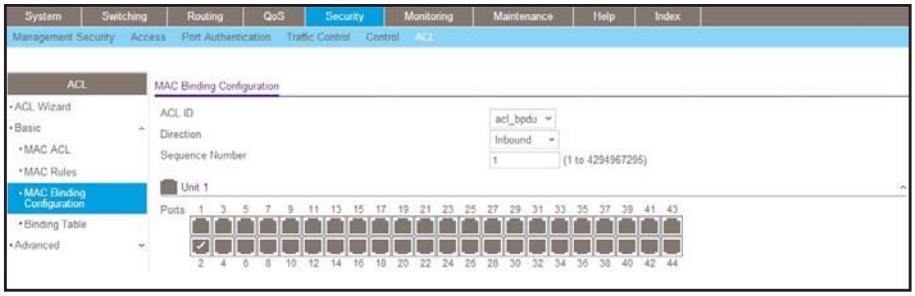
- In the **ID** field, enter **2**.
- In the **Action** field, select **Permit**.

c. Click the **Add** button.

4. Apply the ACL acl_bpdu to port 2.

a. Select **Security > ACL > MAC ACL > MAC Binding Configuration**.

A screen similar to the following displays.



b. Enter the following information in the MAC Binding Configuration.

- IN the **ACL ID** field, select **acl_bpdu**.
- In the **Sequence Number** field, enter **1**.

c. Click the **Unit 1.** The ports display.

d. Click the gray box under port **2**. A check mark displays in the box.

e. Click **Apply** to save the settings.

Configure ACL Mirroring

This feature extends the existing port mirroring functionality by allowing you to mirror a designated traffic stream in an interface using ACL rules. Define an ACL rule matching the desired traffic with the option mirror to an interface. Any traffic matching this rule will be copied to the specified mirrored interface.

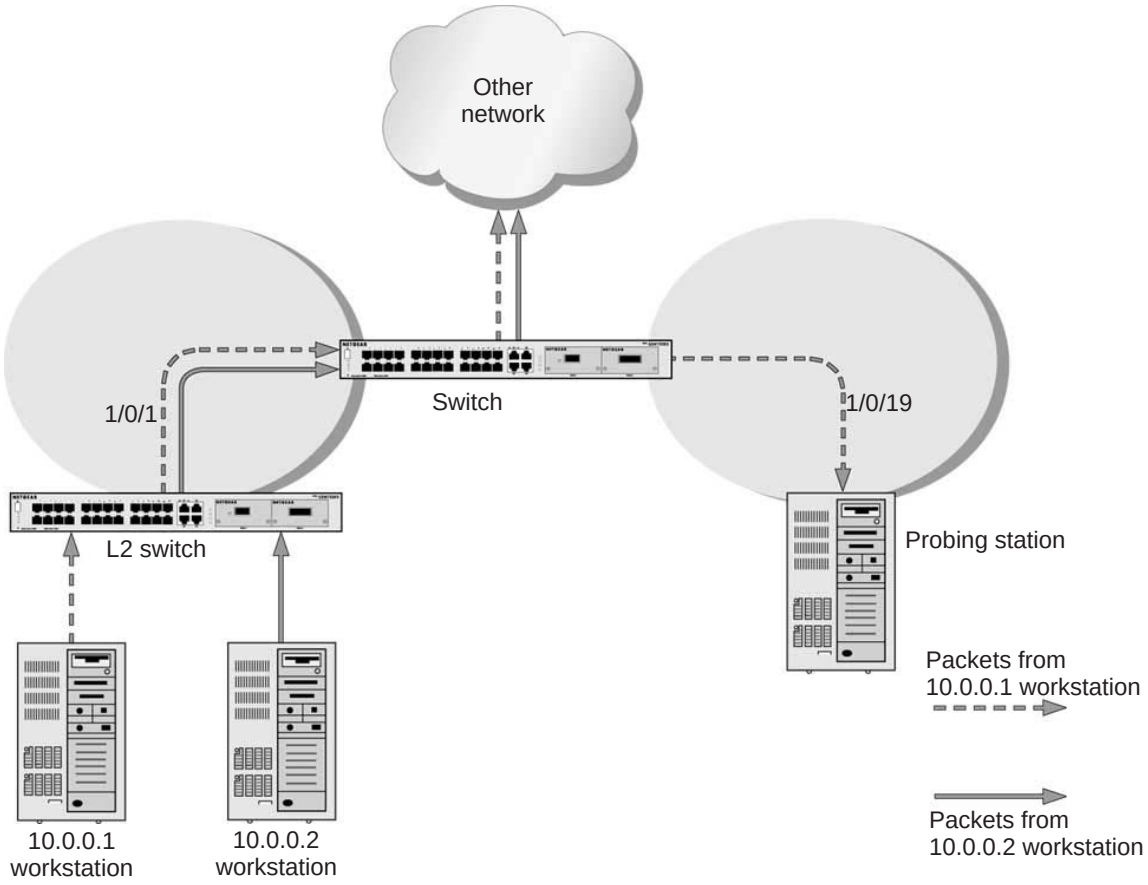


Figure 22. ACL mirroring

CLI: Configure ACL Mirroring

The script in this section shows how to mirror the traffic stream received from a host in an interface. These examples mirror the traffic from the host 10.0.0.1 connected to the interface 1/0/1.

1. Create an IP access control list with the name monitorHost.

```
(Netgear Switch) (Config)# ip access-list monitorHost
```

2. Define the rules to match host 10.0.0.1 and to permit all others.

```
(Netgear Switch) (Config-ipv4-acl)# permit ip 10.0.0.1 0.0.0.0 any mirror 1/0/19
(Netgear Switch) (Config-ipv4-acl)# permit every
```

3. Bind the ACL with interface 1/0/1.

```
(Netgear Switch) (Interface 1/0/1)#ip access-group monitorHost in 1
```

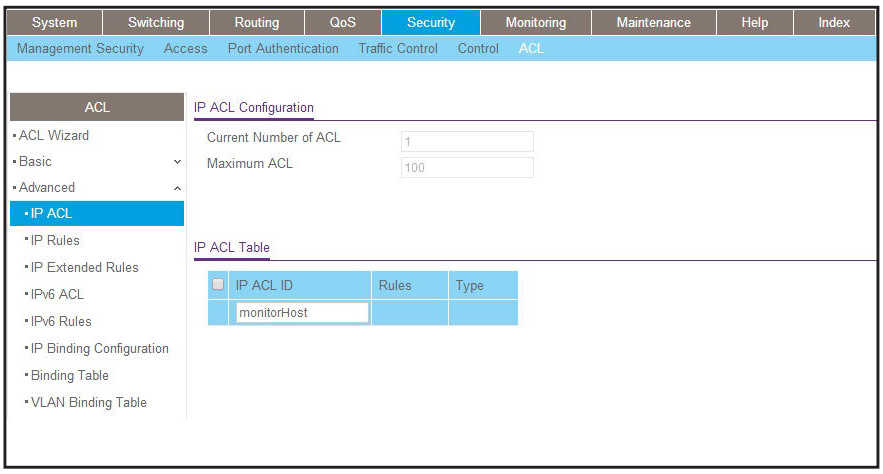
4. View the configuration.

```
(Netgear Switch) # show ip access-lists
Current number of ACLs: 1  Maximum number of ACLs: 100

ACL ID/Name          Rules  Direction      Interface(s)        VLAN(s)
-------------------  -----  ----------    ------------------   -------
monitorHost          2      inbound       1/0/1

(Netgear Switch)  #show ip access-lists monitorHost

   ACL Name: monitorHost
   Inbound Interface(s): 1/0/1

   Rule Number: 1
   Action..................................... permit
   Match All.................................. FALSE
   Protocol................................... 255(ip)
   Source IP Address.......................... 10.0.0.1
   Source IP Mask............................. 0.0.0.0
   Mirror Interface........................... 1/0/19

   Rule Number: 2
   Action..................................... permit
   Match All.................................. TRUE
```

Web Interface: Configure ACL Mirroring

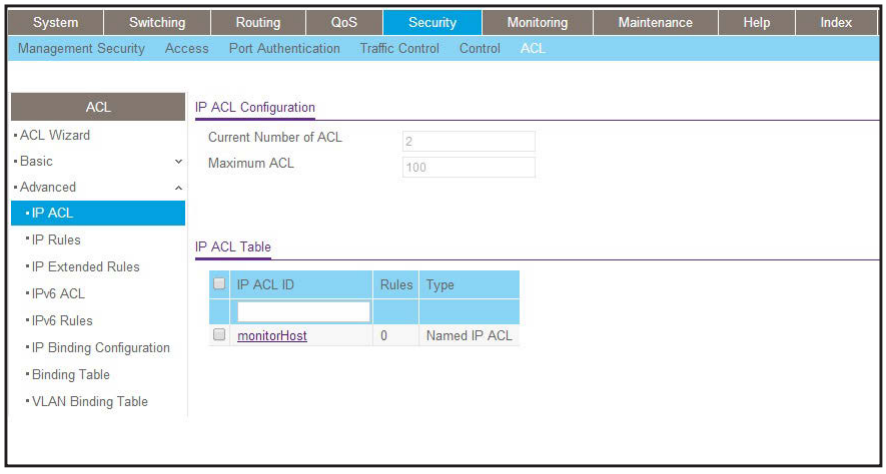
1. Create an IP access control list with the name monitorHost on the switch.
   a. Select **Security > ACL > Advanced > IP ACL**.

      A screen similar to the following displays.



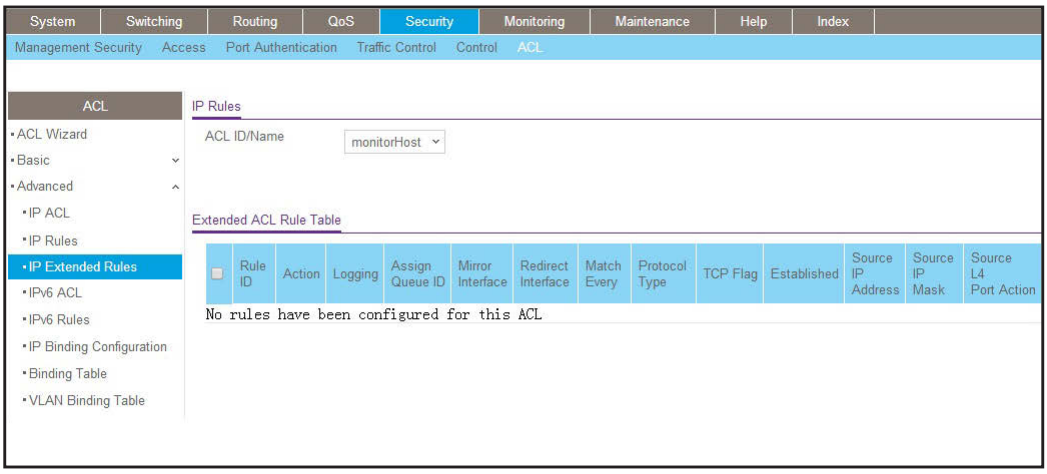
   b. In the **IP ACL ID** field, enter **monitorHost**.
   c. Click **Add** to create ACL monitorHost.

      A screen similar to the following displays.



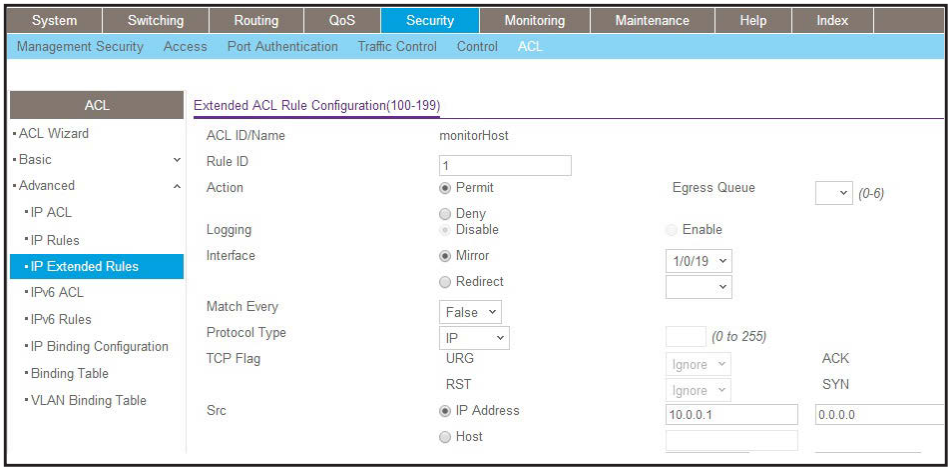
2. Create a rule to match host 10.0.0.1 in the ACL monitorHost.
   a. Select **Security > ACL > Advanced > IP Extended Rules**.

A screen similar to the following displays.



b. Click **Add**.

A screen similar to the following displays.



c. In the **Rule ID** field, enter **1**.

d. For Action, select the **Permit** radio button.

e. In the **Mirror Interface** list, select **1/0/19**.

f. In the **Src IP Address** field, enter **10.0.0.1**.

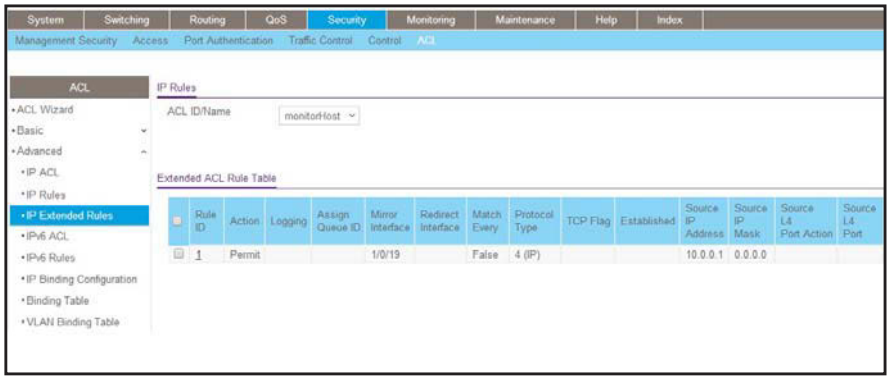
g. In the **Src IP Mask** field, enter **0.0.0.0**.

h. Click **Apply**.

3. Create a rule to match every other traffic.

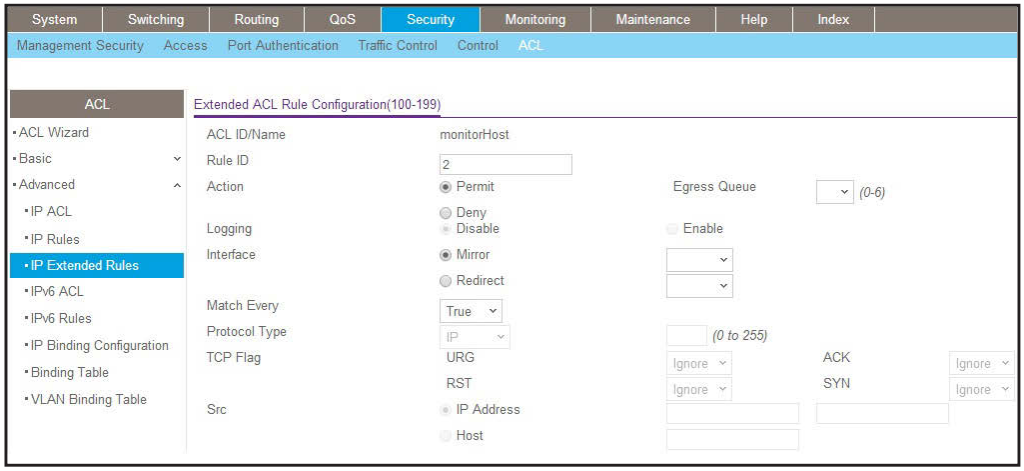
a. Select **Security > ACL > Advanced > IP Extended Rules**.

A screen similar to the following displays.



b. Click **Add**.

A screen similar to the following displays.



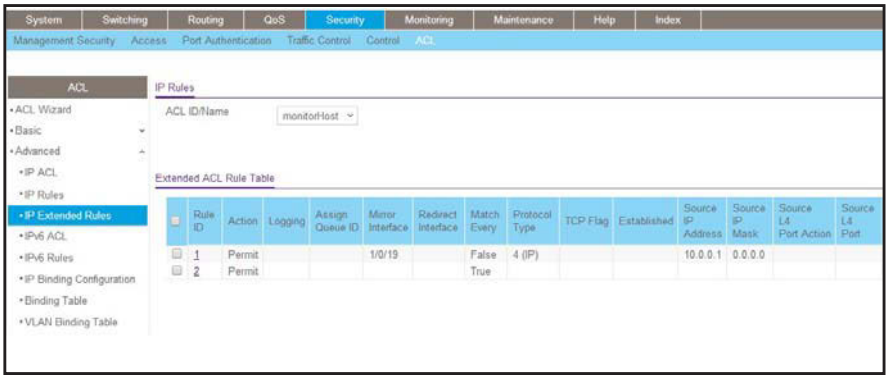
c. In the **Rule ID** field, enter **2**.

d. Select the **Permit** radio button.

e. In the **Match Every** field, select **True**.

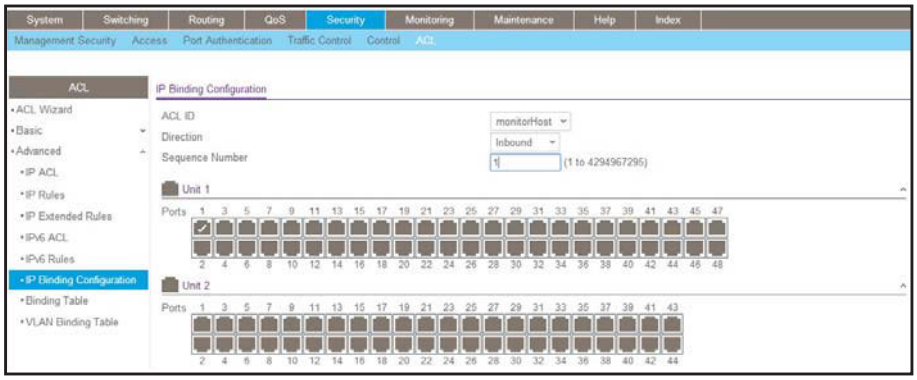
f. Click **Apply**.

A screen similar to the following displays.



4. Bind the ACL with interface 1/0/1.
   a. Select **Security > ACL > Advanced > IP Binding Configuration**.

      A screen similar to the following displays.



   b. In the **Sequence Number** field, enter **1**.
   c. In the Port Selection Table, click **Unit 1** to display all the ports for the device.
   d. Select the **Port 1** check box.
   e. Click **Apply**.

Configure ACL Redirection

This feature redirects a specified traffic stream to a specified interface.

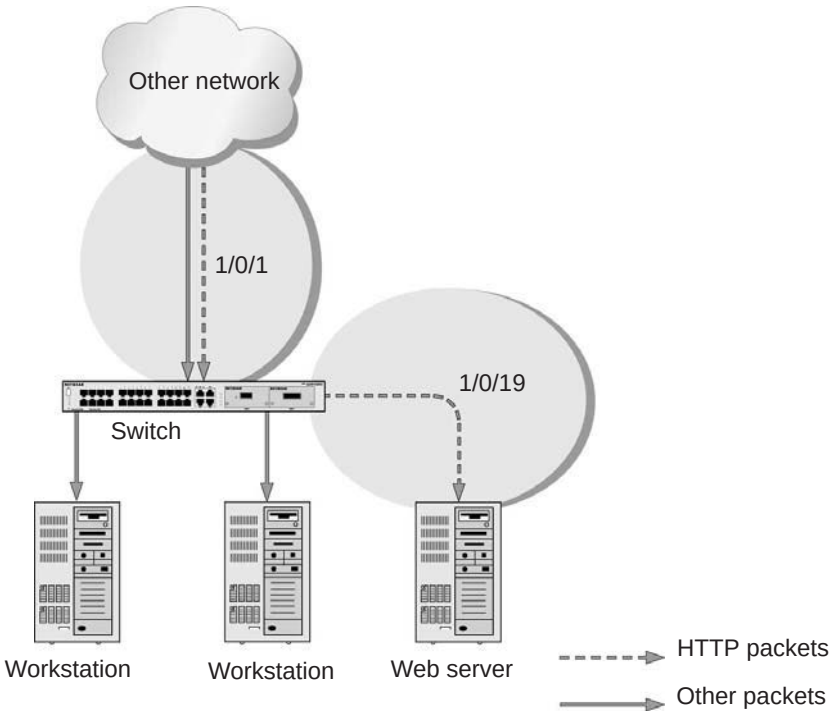


Figure 23. ACL Redirect

CLI: Redirect a Traffic Stream

The script in this section shows how to redirect an HTTP traffic stream received in an interface to the specified interface. This example redirects the HTTP traffic stream received in port 1/0/1 to port 1/0/19.

1. Create an IP access control list with the name redirectHTTP.

```
(Netgear Switch) (Config)#ip access-list redirectHTTP
```

2. Define a rule to match the HTTP stream and define a rule to permit all others.

```
(Netgear Switch) (Config-ipv4-acl)# permit tcp any any eq http redirect 1/0/19
(Netgear Switch) (Config-ipv4-acl)# permit every
```

3. Bind the ACL with interface 1/0/1.

```
(Netgear Switch) (Interface 1/0/1)#ip access-group redirectHTTP in 1
```

4. View the configuration.

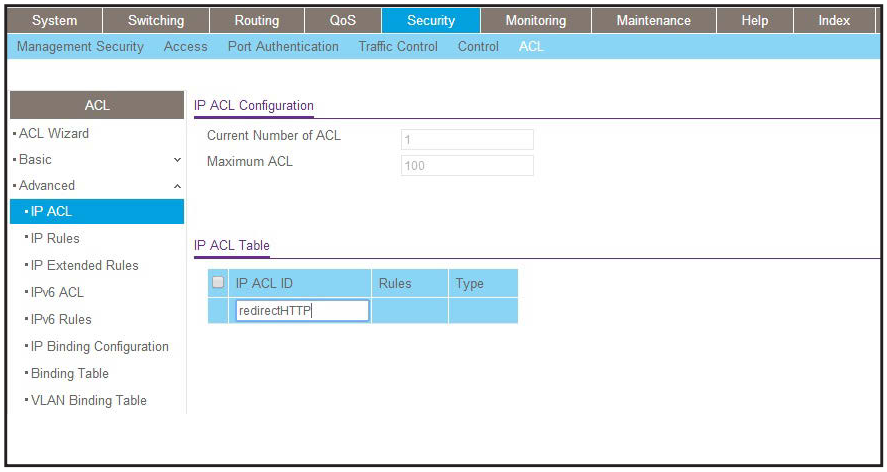
```
(Netgear Switch) # show ip access-lists
Current number of ACLs: 1  Maximum number of ACLs: 100

ACL ID/Name         Rules   Direction    Interface(s)         VLAN(s)
------------------  -----   ----------   -------------------  -------
redirectHTTP        2       inbound      1/0/1

(Netgear Switch)  #show ip access-lists redirectHTTP

ACL Name: redirectHTTP
Inbound Interface(s): 1/0/1

Rule Number: 1
Action..................................... permit
Match All.................................. FALSE
Protocol................................... 6(tcp)
Destination L4 Port Keyword................ 80(www/http)
Redirect Interface......................... 1/0/19

Rule Number: 2
Action..................................... permit
Match All.................................. TRUE
```

Web Interface: Redirect a Traffic Stream

This example redirects the HTTP traffic stream received in port 1/0/1 to port 1/0/19.

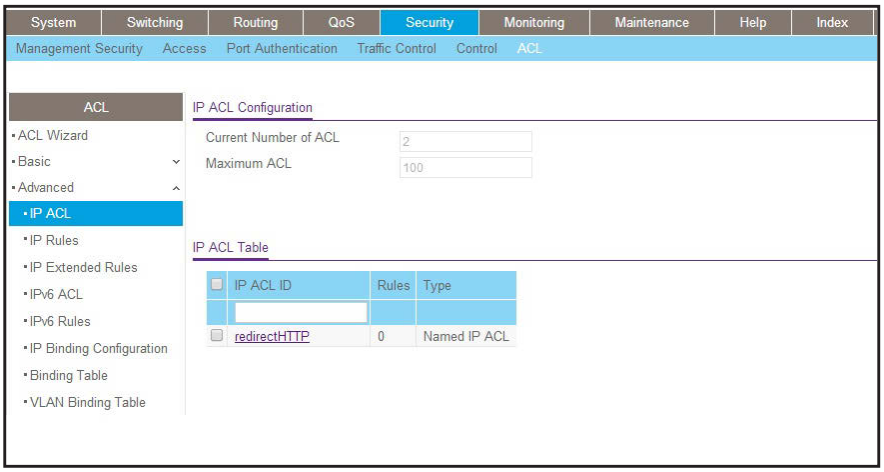
1. Create an IP access control list with the name redirectHTTP.
   a. Select **Security > ACL > Advanced > IP ACL**.

      A screen similar to the following displays.



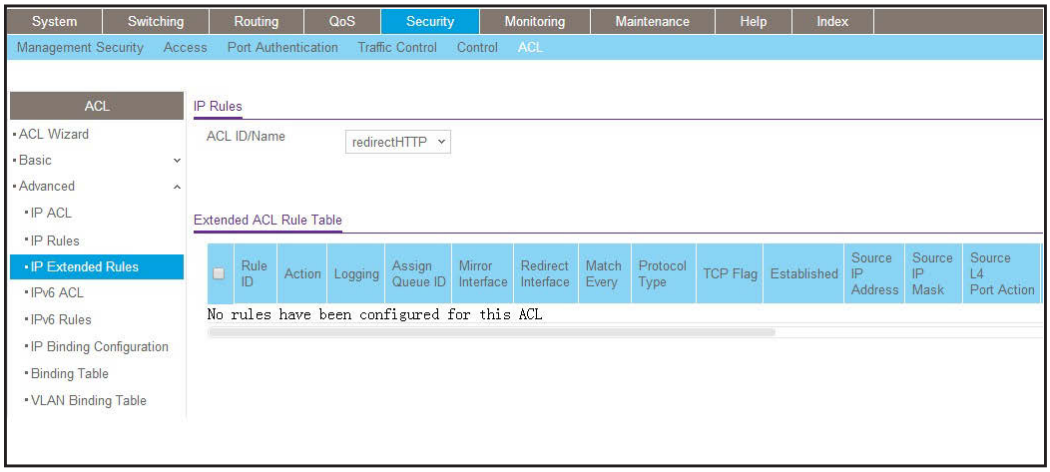
   b. In the **IP ACL** field, enter **redirectHTTP**.
   c. Click **Add** to create the IP ACL redirectHTTP.

      A screen similar to the following displays.



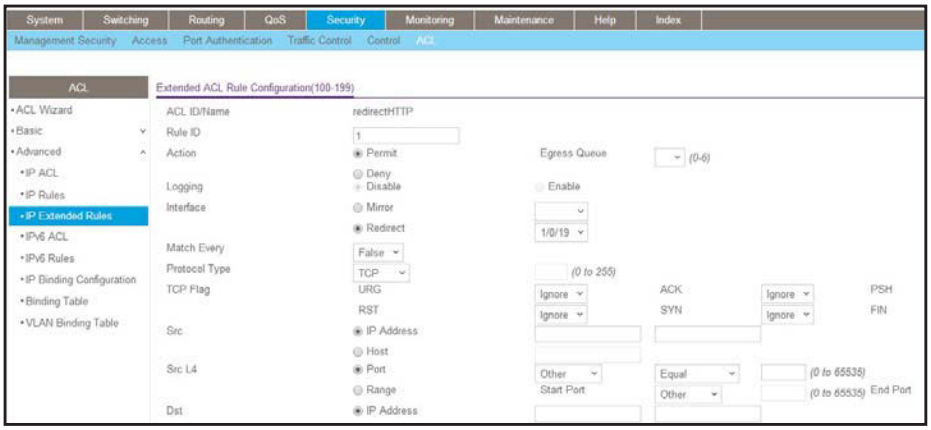
2. Create a rule to redirect HTTP traffic.
   a. Select **Security > ACL > Advanced > IP Extended Rules**.

A screen similar to the following displays.



b. Click **Add**.

A screen similar to the following displays.



c. In the **Rule ID** field, enter **1**.

d. In the **protocol** field, select **www-http**.

e. For Action, select the **Permit** radio button.

f. In the **Redirect Interface** list, select **1/0/19**.

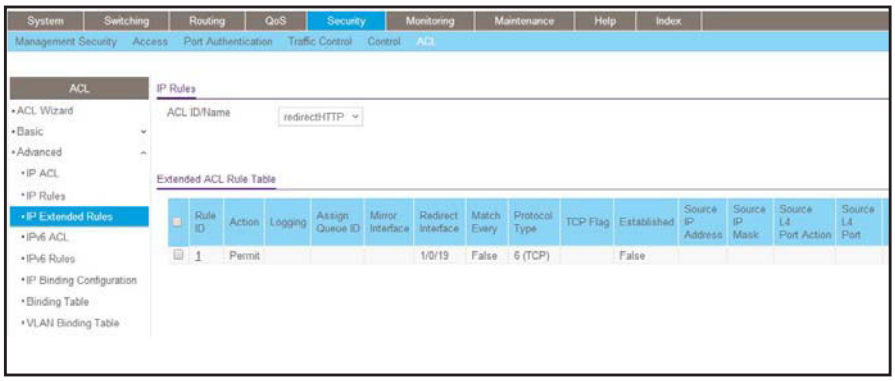
g. In the **Dst L4 Por**t list, select **http**.

h. Click **Apply**. The Extended ACL Rules screen displays, as described in the next step in this procedure.

3. Create a rule to match every other traffic.

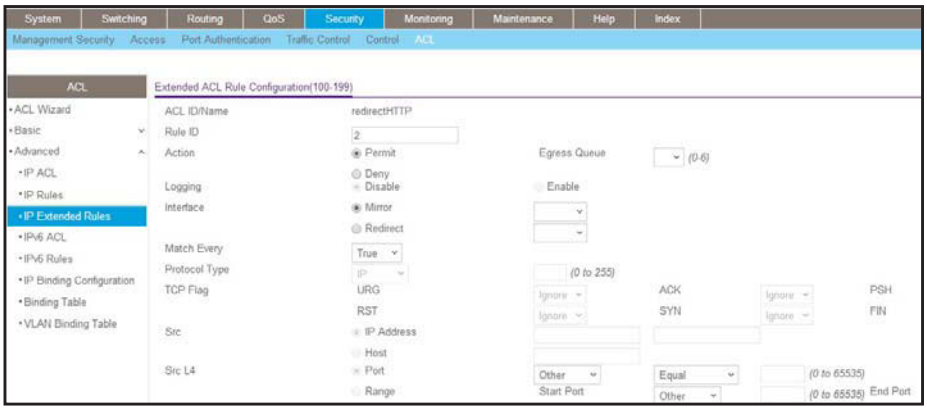
a. Select **Security > ACL > Advanced > IP Extended Rules**.

A screen similar to the following displays.



b. Click **Add**.

A screen similar to the following displays.



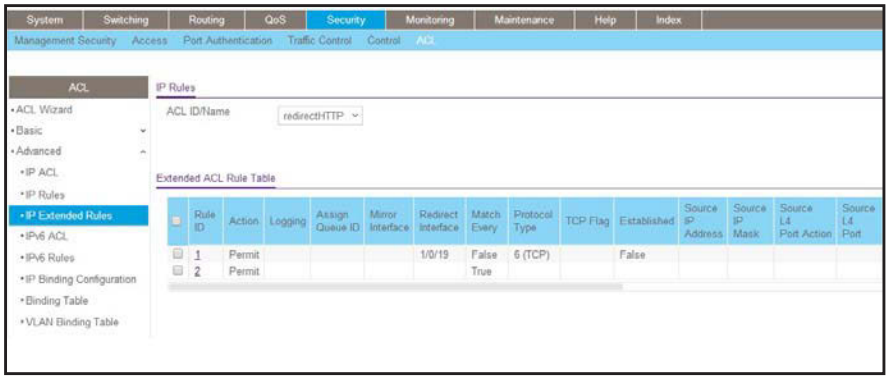
c. In the **Rule ID** field, enter **2**.

d. For Action, select the **Permit** radio button.

e. In the **Match Every** field, select **True**.

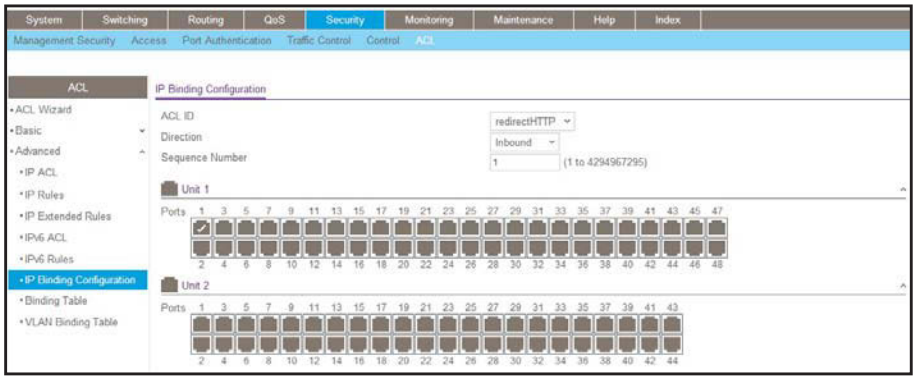
f. Click **Apply**.

A screen similar to the following displays.



4. Bind the ACL with interface 1/0/1.
   a. Select **Security > ACL > Advanced > IP Binding Configuration**.

      A screen similar to the following displays.



   b. In the **Sequence Number** field, enter **1**.
   c. In the Port Selection Table, click **Unit 1** to display all the ports.
   d. Select the check box below Port 1.
   e. Click **Apply**.

Add ACL Remarks

You can use the **remark** keyword to include comments (remarks) for ACL rule entries in a MAC or IP ACL. Remarks can help you and other users to understand ACL rules. Each remark line is limited to 100 characters. Remarks can consist of characters in the range A–Z, a–z, and 0–9 and of special characters such as spaces, hyphens, and underscores. If you want to create remarks for a permit or deny rule, you must create the remarks before you create the rule. If you remove a rule, all associated remarks are removed as well. If remarks are no longer applicable, you can remove them. You can also add remarks to a MAC or IP ACL without adding any rules, save the remarks, and add the rules later.

The following example shows how you can add remarks to rules:

1. Create an ACL.

```
(Netgear Switch) (Config)#ip access-list acl_voice
```

2. Add a remark before you add a rule.

```
(Netgear Switch) (Config-ipv4-acl)#remark "permit VOIP packets whose DSCP is EF"
(Netgear Switch) (Config-ipv4-acl)#permit ip any any dscp ef
(Netgear Switch) (Config-ipv4-acl)#remark "deny all of other packets" (Netgear Switch)
(Config-ipv4-acl)#deny ip any any
(Netgear Switch) (Config-ipv4-acl)#exit
(Netgear Switch) (Config)#exit
```

3. Check the configuration using the **show running-config** command.

```
(Netgear Switch) #show running-config
……….
ip access-list acl_voice
remark "permit VOIP packets whose DSCP is EF"
permit ip any any dscp ef
remark "deny all of other packets"
deny ip any any
exit
```

Change the Sequence of an ACL Rule

The association of sequence numbers with access control list (ACL) rules can simplify the process of changing an ACL and can make it easier to identify the rules. Sequence numbers let you position ACL rule entries within an ACL, resort entries, and remove entries.

You can renumber ACL rule entries to create room to insert a new rule entry. For example, you can specify a sequence number to insert a rule entry in the middle of an existing ACL.

Each ACL rule entry requires a sequence number: If you do not assign a number manually, the switch assigns it automatically. The following applies to sequence numbers:

- If you do not manually assign a sequence number for the rule, the switch automatically assign a sequence number that is 10 greater than the last sequence number in the ACL, and the rule is placed at the end of the list. If the rule is the first one in the ACL, a sequence number of 10 is assigned. If the automatically assigned sequence number exceeds the maximum possible value, creation of the ACL rule fails.
- You cannot create a rule with a sequence number that duplicates an existing sequence number.
- If you reboot the switch, the start sequence number and increment number for ACL rules are not saved.

The following example shows how you can insert an ACL rule, let the switch automatically assign a sequence number, change the start sequence number and the sequence increment number (that is, the number by which the sequence increases), and insert an ACL rule at a particular position:

1. Create an IP ACL named voice_acl without specifying a sequence number.

```
(Netgear Switch) #config
(Netgear Switch) (Config)#ip access-list voice_acl
(Netgear Switch) (Config-ipv4-acl)#permit ip any any dscp cs5
(Netgear Switch) (Config-ipv4-acl)#permit ip any any dscp ef
(Netgear Switch) (Config-ipv4-acl)#deny ip any any
(Netgear Switch) (Config-ipv4-acl)#exit
```

2. Verify that the sequence numbers are assigned by the switch.

   The first sequence number is 10, the second sequence number is 20, and so on.

```
(Netgear Switch) (Config)#show ip access-lists voice_acl
ACL Name: voice_acl

Sequence Number: 10
Action..................................... permit
Match All.................................. False
Protocol................................... 255(ip)
IP DSCP.................................... 40(cs5)

Sequence Number: 20
Action..................................... permit
Match All.................................. False
Protocol................................... 255(ip)
IP DSCP.................................... 46(ef)

Sequence Number: 30
Action..................................... deny
Match All.................................. TRUE
```

3. If you must add more than 10 ACL rules, change the start sequence number and sequence increment number before you add ACL rules. In the following example, the start sequence number is 1000 and the sequence increment number is 100.

```
(Netgear Switch) (Config)#ip access-list resequence voice_acl 1000 100
(Netgear Switch) (Config)#show ip access-lists voice_acl
ACL Name: voice_acl

Sequence Number: 1000
Action..................................... permit
Match All.................................. False
Protocol................................... 255(ip)
IP DSCP.................................... 40(cs5)

Sequence Number: 1100
Action..................................... permit
Match All.................................. False
Protocol................................... 255(ip)
IP DSCP.................................... 46(ef)

Sequence Number: 1200
Action..................................... deny
Match All.................................. TRUE
```

4. Insert a new ACL rule at a particular position. For example, insert a new ACL rule with sequence number 900 at the first position. The new rule drops all packets that arrive from IP address 192.168.1.1.

```
(Netgear Switch) #config
(Netgear Switch) (Config)#ip access-list voice_acl
(Netgear Switch) (Config-ipv4-acl)#900 deny ip 192.168.1.1 255.255.255.0 any
(Netgear Switch) (Config-ipv4-acl)#exit
(Netgear Switch) (Config)#exit
(Netgear Switch) #show ip access-lists voice_acl

ACL Name: voice_acl

Sequence Number: 900
Action..................................... deny
Match All.................................. False
Protocol................................... 255(ip)
Source IP Address.......................... 192.168.1.1
Source IP Wildcard Mask.................... 255.255.255.0

Sequence Number: 1000
Action..................................... permit
Match All.................................. False
Protocol................................... 255(ip)
IP DSCP.................................... 40(cs5)

Sequence Number: 1100
Action..................................... permit
Match All.................................. False
Protocol................................... 255(ip)
IP DSCP.................................... 46(ef)

Sequence Number: 1200
Action..................................... deny
Match All.................................. TRUE
```

Configure a Management ACL

A management ACL lets you control access to the switch. You can permit specific hosts to access the switch and deny access to all other hosts. You can also specify a specific access method for a permitted host. For example, you can specify that a host can access the switch over a Telnet connection only

The following examples show how to configure a management ACL.

Example 1: Permit Any Host to Access the Switch Through Telnet or HTTP:

Permit any host to access the managed VLAN IP address of 169.254.100.100 through a Telnet or HTTP connection:

```
(Netgear Switch) (Config)#ip access-list acl_for_cpu
(Netgear Switch) (Config-ipv4-acl)#permit tcp any 169.254.100.100 0.0.0.0 eq telnet
(Netgear Switch) (Config-ipv4-acl)#deny tcp any any eq http
(Netgear Switch) (Config-ipv4-acl)#permit tcp any 169.254.100.100 0.0.0.0 eq http
(Netgear Switch) (Config-ipv4-acl)#deny tcp any any eq http
(Netgear Switch) (Config-ipv4-acl)#deny every
(Netgear Switch) (Config-ipv4-acl)#exit
(Netgear Switch) (Config)#ip access-group acl_for_cpu control-plane
```

Example 2: Permit a Specific Host to Access the Switch Through SSH Only

Permit a specific host access the switch over an SSH connection only.

```
(Netgear Switch) (Config)#ip access-list acl_for_cpu
(Netgear Switch) (Config-ipv4-acl)#permit tcp 10.100.5.13  0.0.0.0 any  eq ssh
(Netgear Switch) (Config-ipv4-acl)#deny tcp any any  eq ssh
(Netgear Switch) (Config-ipv4-acl)#permit every
(Netgear Switch) (Config-ipv4-acl)#exit
(Netgear Switch) (Config)#ip access-group acl_for_cpu control-plane
```

Configure IPv6 ACLs

This feature extends the existing IPv4 ACL by providing support for IPv6 packet classification. Each ACL is a set of up to 12 rules applied to inbound traffic. Each rule specifies whether the contents of a given field should be used to permit or deny access to the network, and can apply to one or more of the following fields within a packet:

- Source IPv6 prefix
- Destination IPv6 prefix
- Protocol number
- Source Layer 4 port
- Destination Layer 4 port
- DSCP value
- Flow label

Note that the order of the rules is important: When a packet matches multiple rules, the first rule takes precedence. Also, once you define an ACL for a given port, all traffic not specifically permitted by the ACL is denied access.

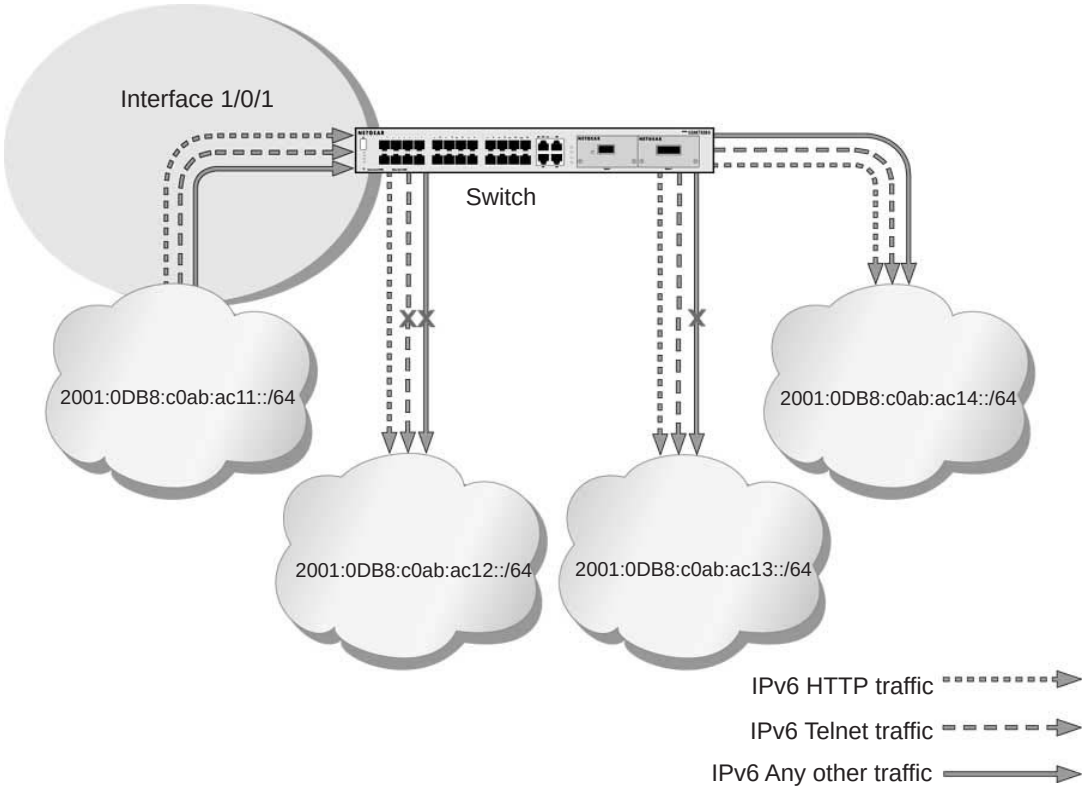


Figure 24. IPv6 ACLs

The script in this section shows you how to set up an IPv6 ACL with the following three rules:

- **Rule-1**. Permits every traffic to the destination network 2001:DB8:C0AB:AC14::/64.
- **Rule-2**. Permits IPv6 TELNET traffic to the destination network 2001:DB8:C0AB:AC13::/64.
- **Rule-3**. Permits IPv6 HTTP traffic to any destination.

CLI: Configure an IPv6 ACL

1. Create the access control list with the name ipv6-acl.

```
(Netgear Switch) (Config)# ipv6 access-list ipv6-acl
```

2. Define three rules to:
   - Permit *any* IPv6 traffic to the destination network 2001:DB8:C0AB:AC14::/64 from the source network 2001:DB8:C0AB:AC11::/64.
   - Permit IPv6 *Telnet* traffic to the destination network 2001:DB8:C0AB:AC13::/64 from the source network 2001:DB8:C0AB:AC11::/64.
   - Permit IPv6 HTTP traffic to *any* destination network from the source network 2001:DB8:C0AB:AC11::/64.

```
(Netgear Switch) (Config-ipv6-acl)# permit ipv6 2001:DB8:C0AB:AC11::/64
 2001:DB8:C0AB:AC14::/64
(Netgear Switch) (Config-ipv6-acl)# permit tcp 2001:DB8:C0AB:AC11::/64
2001:DB8:C0AB:AC13::/64 eq telnet
(Netgear Switch) (Config-ipv6-acl)# permit tcp 2001:DB8:C0AB:AC11::/64 any eq http
```

3. Apply the rules to inbound traffic on port 1/0/1. Only traffic matching the criteria will be accepted.

```
(Netgear Switch) (Config)#interface 1/0/1
(Netgear Switch) (Interface 1/0/1)# ipv6 traffic-filter ipv6-acl in
(Netgear Switch) (Interface 1/0/1)# exit
(Netgear Switch) (Config)#exit
```

4. View the configuration.

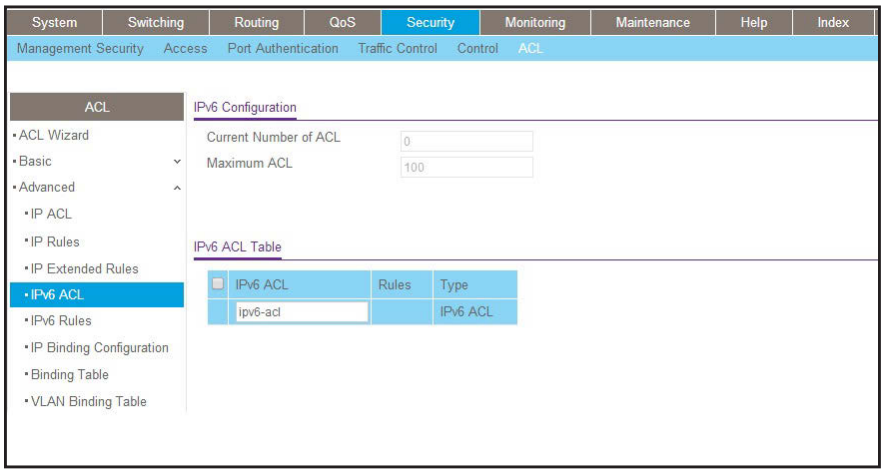
```
(Netgear Switch) #show ipv6 access-lists
Current number of all ACLs: 1  Maximum number of all ACLs: 100

IPv6 ACL Name          Rules   Direction     Interface(s)     VLAN(s)
---------------------  -----   ---------     -------------    ------------
ipv6-acl               3       inbound       1/0/1

(Netgear Switch) #show ipv6 access-lists ipv6-acl

ACL Name: ipv6-acl
Inbound Interface(s): 1/0/1

Rule Number: 1
Action..................................... permit
Protocol................................... 255(ipv6)
Source IP Address.......................... 2001:DB8:C0AB:AC11::/64
Destination IP Address..................... 2001:DB8:C0AB:AC14::/64

Rule Number: 2
Action..................................... permit
Protocol................................... 6(tcp)
Source IP Address.......................... 2001:DB8:C0AB:AC11::/64
Destination IP Address..................... 2001:DB8:C0AB:AC13::/64
Destination L4 Port Keyword................ 23(telnet)
```

```
Rule Number: 3
Action..................................... permit
Protocol................................... 6(tcp)
Source IP Address.......................... 2001:DB8:C0AB:AC11::/64
Destination L4 Port Keyword................ 80(www/http)
```

Web Interface: Configure an IPv6 ACL

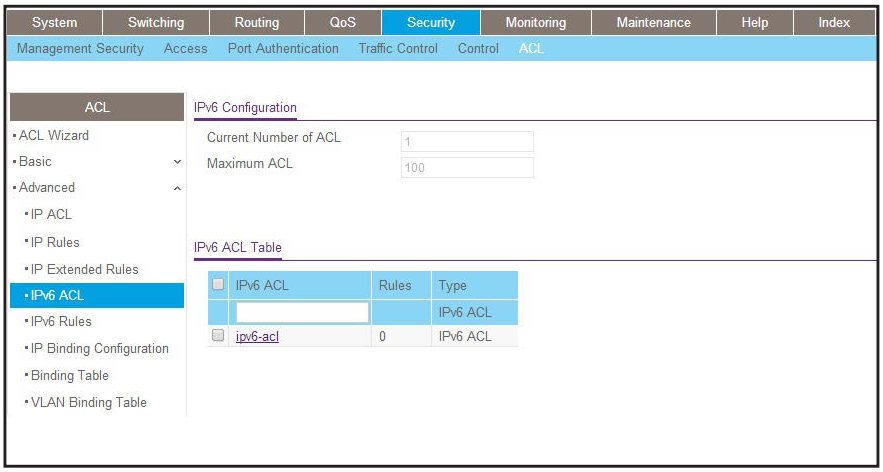
1. Create the access control list with the name ipv6-acl.
   a. Select **Security > ACL > Advanced > IPv6 ACL**.
   b. In the IPv6 ACL Table, in the **IPv6 ACL** field, enter **ipv6-acl**.

A screen similar to the following displays.



c. Click **Add**.

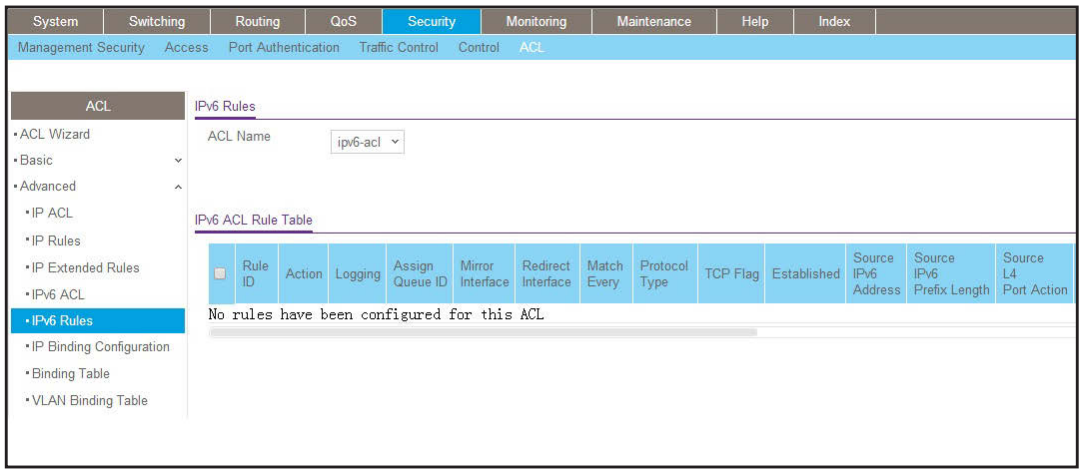
A screen similar to the following displays.



2. Define the first rule (1 of 3).

   a. Select **Security > ACL > Advanced > IPv6 Rules**.

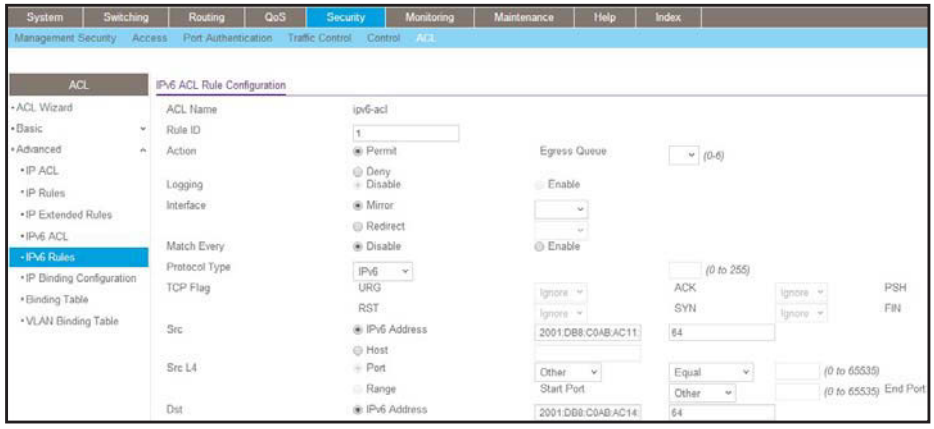
A screen similar to the following displays.



b. In the **ACL Name** list, select **ipv6-acl**.

c. Click **Add**.

A screen similar to the following displays.



d. In the **Rule ID** field, enter **1**.

e. For Action, select the **Permit** radio button.

f. In the **Source Prefix** field, enter **2001:DB8:C0AB:AC11::**.

g. In the **Source Prefix Length** field, enter **64**.

h. In the **Destination Prefix** field, enter **2001:DB8:C0AB:AC14::**.

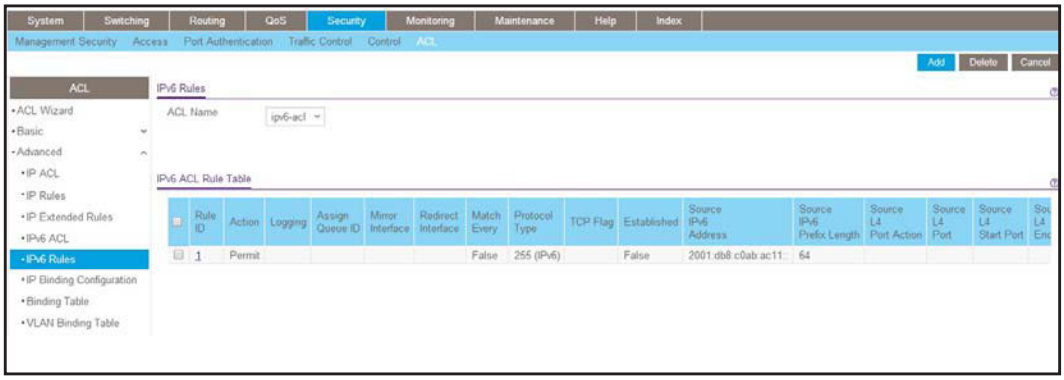
i. In the **Destination Prefix Length** field, enter **64**.

j. Click **Apply**.

3. Add Rule 2.

a. Select **Security > ACL > Advanced > IPv6 Rules**.

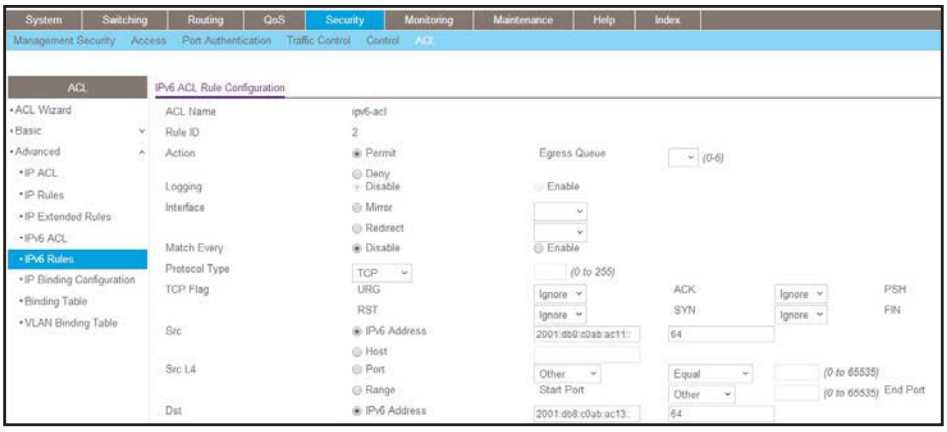
A screen similar to the following displays.



b. In the **ACL Name** list, select **ipv6-acl**.

c. Click **Add**.

A screen similar to the following displays.



d. In the **Rule ID** field, enter **2**.

e. For Action, select the **Permit** radio button.

f. In the **Protocol Type** list, select **TCP**.

g. In the **Source Prefix** field, enter **2001:DB8:C0AB:AC11::**.

h. In the **Source Prefix Length** field, enter **64**.

i. In the **Destination Prefix** field, enter **2001:DB8:C0AB:AC13::**.

j. In the **Destination Prefix Length** field, enter **64**.

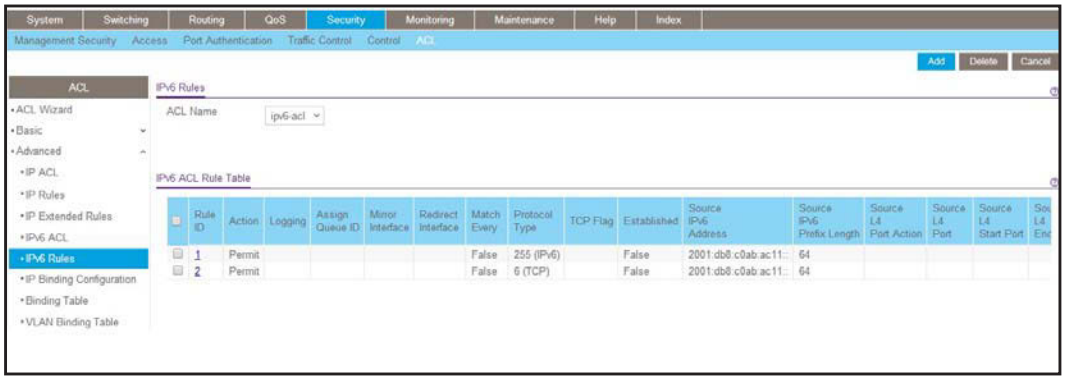
k. In the **Destination L4 Port** list, select **telnet**.

l. Click **Apply**.

4. Add Rule 3.

a. Select **Security > ACL > Advanced > IPv6 Rules**.

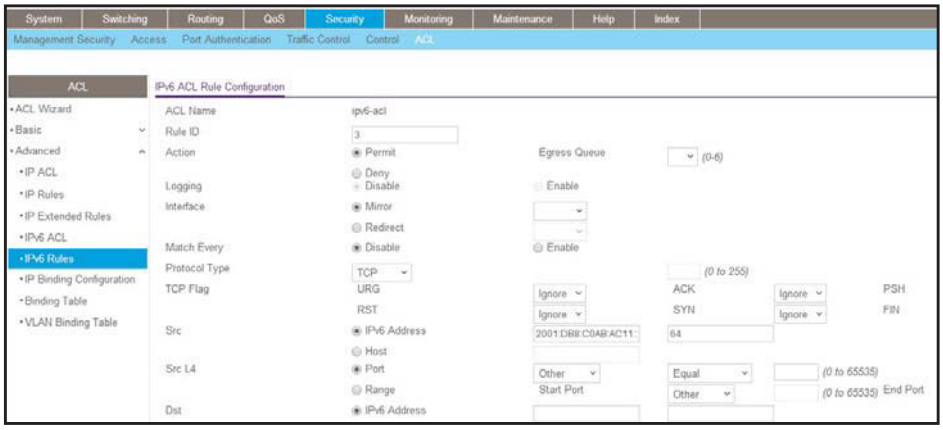
A screen similar to the following displays.



b. In the **ACL Name** list, select **ipv6-acl**.

c. Click **Add**.

A screen similar to the following displays.



d. In the **Rule ID** field, enter **3**.

e. For Action, select the **Permit** radio button.

f. In the **Protocol Type** list, select **TCP**.

g. In the **Source Prefix** field, enter **2001:DB8:C0AB:AC11::**.

h. In the **Source Prefix Length** field, enter **64**.

i. In the **Destination L4 Port** list, select **http**.

j. Click **Apply**.

5. Apply the rules to inbound traffic on port 1/0/1.

Only traffic matching the criteria will be accepted.

a. Select **Security > ACL > Advanced > IP Binding Configuration**.

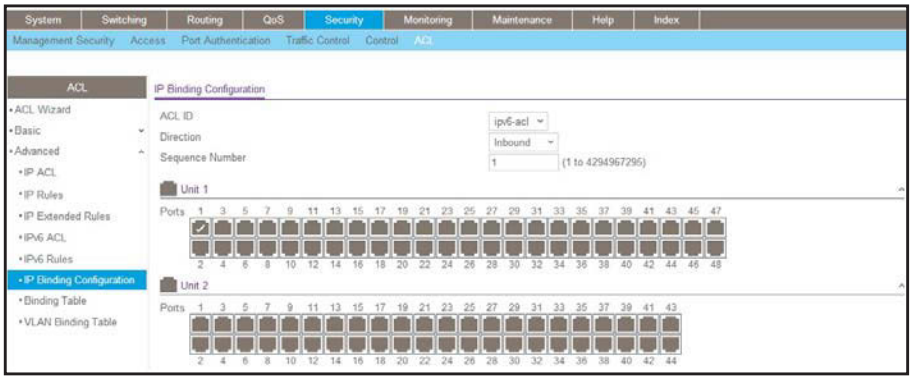
b. In the **ACL ID** list, select **ipv6-acl**.

c. In the **Sequence Number** list, select **1**.

d. Click **Unit 1**.

e. Select **Port 1**.

A screen similar to the following displays.

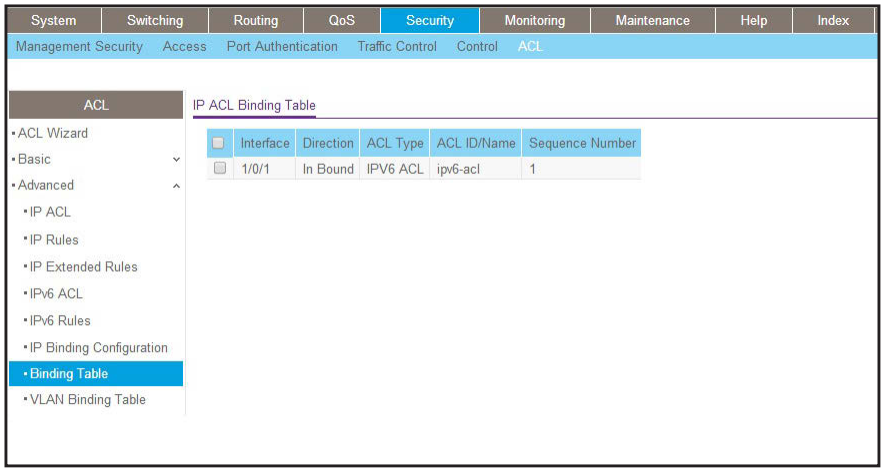


f. Click the **Apply** button.

6. View the binding table.

Select **Security > ACL > Advanced > Binding Table**.

A screen similar to the following displays.



CoS Queuing

12

Class of Service queuing

This chapter describes Class of Service (CoS) queue mapping, CoS Configuration, and traffic shaping features. The chapter includes the following sections:

- *CoS Queuing Concepts*
- *Show classofservice Trust*
- *Set classofservice Trust Mode*
- *Configure Cos-queue Min-bandwidth and Strict Priority Scheduler Mode*
- *Set CoS Trust Mode for an Interface*
- *Configure Traffic Shaping*

CoS Queuing Concepts

Each port has one or more queues for packet transmission. During configuration, you can determine the mapping and configuration of these queues.

Based on the service rate and other criteria you configure, queues provide preference to specified packets. If a delay is necessary, the system holds packets until the scheduler authorizes transmission. As queues become full, packets are dropped. Packet drop precedence indicates the packet's sensitivity to being dropped during queue congestion.

You can CoS on a per-interface basis:

- You can configure CoS mapping.
- Queue parameters and queue management are configurable per interface.
- Some hardware implementations allow queue depth management using tail dropping or weighted random early discard (WRED).
- Some hardware implementations allow queue depth management using tail dropping.
- The operation of CoS queuing involves queue mapping and queue configuration.

CoS Queue Mapping

CoS queue mapping uses trusted and untrusted ports.

Trusted Ports

- The system takes at face value certain priority designations for arriving packets.
- Trust applies only to packets that have that trust information.
- There can be only one trust field at a time - per port.
  - 802.1p user priority (This is the default trust mode and is managed through switching configuration.)
  - IP precedence
  - IP DiffServ Code Point (DSCP)

The system can assign the service level based upon the 802.1p priority field of the L2 header. You configure this by mapping the 802.1p priorities to one of three traffic class queues. These queues are:

- **Queue 2**. Minimum of 50 percent of available bandwidth
- **Queue 1**. Minimum of 33 percent of available bandwidth
- **Queue 0**. Lowest priority, minimum of 17 percent of available bandwidth

For untagged traffic, you can specify the default 802.1p priority on a per-port basis.

Untrusted Ports

- No incoming packet priority designation is trusted; therefore, the default priority value for the port is used.
- All ingress packets from untrusted ports, where the packet is classified by an ACL or a DiffServ policy, are directed to specific CoS queues on the appropriate egress port. That specific CoS queue is determined by either the default priority of the port or a DiffServ or ACL-assigned queue attribute.
- Used when trusted port mapping is unable to be honored - for instance, when a non-IP DSCP packet arrives at a port configured to trust IP DSCP.

CoS Queue Configuration

CoS queue configuration involves port egress queue configuration and drop precedence configuration (per queue). The design of these on a per-queue, per-drop precedence basis allows you to create the service characteristics that you want for different types of traffic.

Port egress queue configuration:

- Scheduler type, strict vs. weighted
- Minimum guaranteed bandwidth
- Maximum allowed bandwidth per-queue shaping
- Queue management type, tail drop vs. WRED

Drop precedence configuration (per queue):

- WRED parameters
  - Minimum threshold
  - Maximum threshold
  - Drop probability
  - Scale factor
- Tail drop parameters, threshold

Per-interface basis:

- Queue management type, rail Drop vs. WRED

Only if per-queue configuration is not supported

- WRED decay exponent
- Traffic shaping for an entire interface

Show classofservice Trust

The example is shown as CLI commands and as a web interface procedure.

CLI: Show classofservice Trust

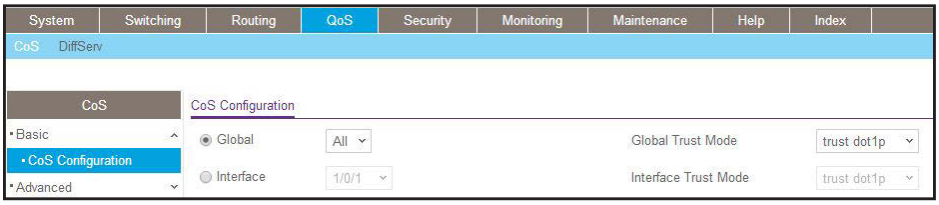
To use the CLI to show CoS trust mode, use these commands:

```
(Netgear Switch) #show classofservice trust?
<cr>   Press Enter to execute the command.
(Netgear Switch) #show classofservice trust
Class of Service Trust Mode: Dot1P
```

Web Interface: Show classofservice Trust

Select **QoS > CoS > Basic > CoS Configuration**.

A screen similar to the following displays.



Set classofservice Trust Mode

The example is shown as CLI commands and as a web interface procedure.

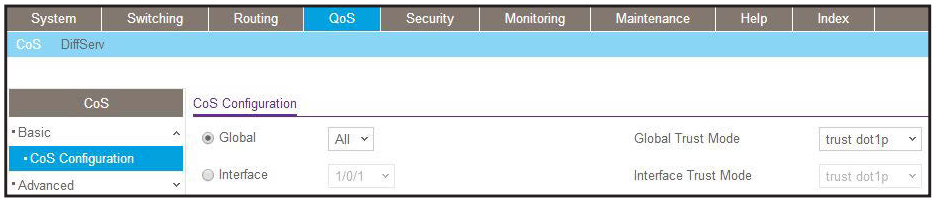
CLI: Set classofservice Trust Mode

```
(Netgear Switch) (Config)#classofservice?
dot1p-mapping            Configure dot1p priority mapping.
ip-dscp-mapping          Maps an IP DSCP value to an internal traffic class.
trust                    Sets the Class of Service Trust Mode of an Interface.
(Netgear Switch) (Config)#classofservice trust?
dot1p                    Sets the Class of Service Trust Mode of an Interface
                         to 802.1p.
ip-dscp                  Sets the Class of Service Trust Mode of an Interface
                         to IP DSCP.
(Netgear Switch) (Config)#classofservice trust dot1p?
<cr>                     Press Enter to execute the command.
(Netgear Switch) (Config)#classofservice trust dot1p
```

Web Interface: Set classofservice Trust Mode

1. Select **QoS > CoS > Basic > CoS Configuration**.

   A screen similar to the following displays.



2. Select the **Global** radio button.
3. In the **Global Trust Mode** list, select **trust dot1p**.
4. Click **Apply** to save the settings.

Configure Cos-queue Min-bandwidth and Strict Priority Scheduler Mode

The example is shown as CLI commands and as a web interface procedure.

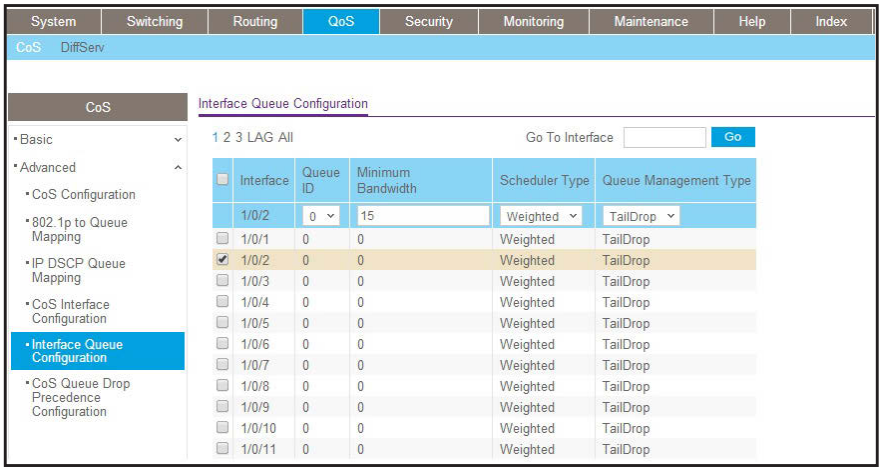
CLI: Configure Cos-queue Min-bandwidth and Strict Priority Scheduler Mode

```
(Netgear Switch) (Config)#cos-queue min-bandwidth?
<bw-0>                    Enter the minimum bandwidth percentage for Queue 0.
(Netgear Switch) (Config)#cos-queue min-bandwidth 15
Incorrect input! Use 'cos-queue min-bandwidth <bw-0>..<bw-7>.
(Netgear Switch) (Config)#cos-queue min-bandwidth 15 25 10 5 5 20 10 10
(Netgear Switch) (Config)#cos-queue strict?
<queue-id>                Enter a Queue Id from 0 to 7.
(Netgear Switch) (Config)#cos-queue strict 1?
<cr>                      Press Enter to execute the command.
<queue-id>                Enter an additional Queue Id from 0 to 7.
(Netgear Switch) (Config)#cos-queue strict 1
```

Web Interface: Configure CoS-queue Min-bandwidth and Strict Priority Scheduler Mode

1. For Interface 1/0/2, set the minimum bandwidth to 15 for queue 0.
   a. Select **QoS > CoS > Advanced > Interface Queue Configuration**.

A screen similar to the following displays.



b. In the **Queue ID** list, select **0**.

c. Under Interface Queue Configuration, scroll down and select the interface **1/0/2** check box.

Now 1/0/2 appears in the Interface field at the top.

d. Enter the following information:

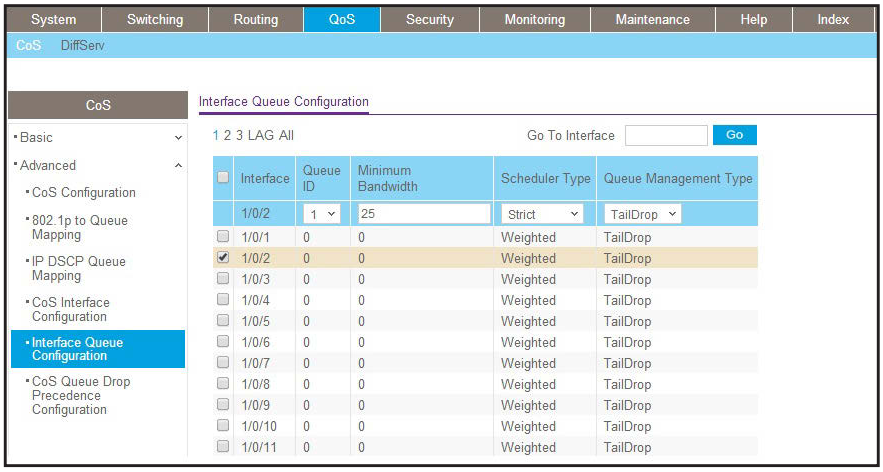
- In the **Minimum Bandwidth** field, enter **15**.
- In the **Scheduler Type** list, select **Weighted**.

e. Click **Apply** to save the settings.

2. For interface 1/0/2, set the minimum bandwidth 25 for queue 1, and set the scheduler type to strict.

a. Select **QoS > CoS > Advanced > Interface Queue Configuration**.

A screen similar to the following displays.



b. In the **Queue ID** list, select **1**.

c. Under Interface Queue Configuration, scroll down and select the interface **1/0/2** check box.

Now 1/0/2 appears in the Interface field at the top.

d. Enter the following information:

- In the **Minimum Bandwidth** field, enter **25**.
- In the **Scheduler Type** list, select **Strict**.

e. Click **Apply** to save the settings.

Set CoS Trust Mode for an Interface

The example is shown as CLI commands and as a web interface procedure.

CLI: Set CoS Trust Mode for an Interface

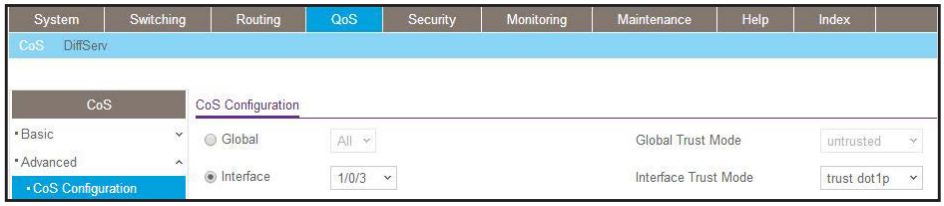
```
(Netgear Switch) (Interface 1/0/3)#classofservice trust?
dot1p                    Sets the Class of Service Trust Mode of an Interface
                         to 802.1p.
ip-dscp                  Sets the Class of Service Trust Mode of an Interface
                         to IP DSCP.
(Netgear Switch) (Interface 1/0/3)#classofservice trust dot1p?
<cr>                     Press Enter to execute the command.
(Netgear Switch) (Interface 1/0/3)#classofservice trust dot1p
```

Note: The traffic class value range is 0–-6 instead of 0–-7 because queue 7 is reserved in a stacking build for stack control, and therefore you cannot configure it.

Web Interface: Set CoS Trust Mode for an Interface

1. Select **QoS > CoS > Advanced > CoS Configuration**.

   A screen similar to the following displays.



2. Under CoS Configuration, select the **Interface** radio button.
3. In the **Interface** list, select **1/0/3**.
4. In the **Interface Trust Mode** list, select **trust dot1p**.
5. Click **Apply** to save the settings.

Configure Traffic Shaping

Traffic shaping controls the amount and volume of traffic transmitted through a network. This has the effect of smoothing temporary traffic bursts over time. Use the **traffic-shape** command to enable traffic shaping by specifying the maximum transmission bandwidth limit for all interfaces (Global Config) or for a single interface (Interface Config).

The <*bw*> value is a percentage that ranges from 0 to 100 in increments of 5. The default bandwidth value is 0, meaning no upper limit is enforced, which allows the interface to transmit up to its maximum line rate.

The <*bw*> value is independent of any per-queue maximum bandwidth values in effect for the interface and should be considered as a second-level transmission rate control mechanism that regulates the output of the entire interface regardless of which queues originate the outbound traffic.

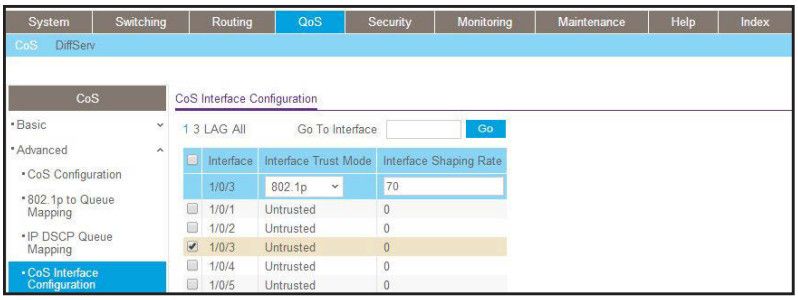
CLI: Configure traffic-shape

```
(Netgear Switch) (Config)#traffic-shape?
<bw>                    Enter the shaping bandwidth percentage from 0 to 100
                        in increments of 5.
(Netgear Switch) (Config)#traffic-shape 70?
<cr>                    Press Enter to execute the command.
(Netgear Switch) (Config)#traffic-shape 70
(Netgear Switch) (Config)#
```

Web Interface: Configure Traffic Shaping

1. Set the shaping bandwidth percentage to 70 percent.
   a. Select **QoS > CoS > Advanced > CoS Interface Configuration**.

      A screen similar to the following displays.



   b. Under CoS Interface Configuration, scroll down and select the interface **1/0/3** check box.

      Now 1/0/3 appears in the Interface field at the top.

   c. In the **Interface Shaping Rate (0 to 100)** field, enter **70**.
   d. Click **Apply** to save the settings.

DiffServ

Differentiated Services

13

This chapter includes the following sections:

- *Differentiated Services Concepts*
- *DiffServ*
- *DiffServ for VoIP*
- *Auto VoIP*
- *DiffServ for IPv6*
- *Color Conform Policy*
- *WRED Explicit Congestion Notification*

Differentiated Services Concepts

Differentiated services (DiffServ) is one technique for implementing Quality of Service (QoS) policies. Using DiffServ in your network allows you to directly configure the relevant parameters on the switches and routers rather than using a resource reservation protocol.This section explains how to configure the switch to identify which traffic class a packet belongs to, and how it should be handled to provide the quality of service you want. As implemented on the switch, DiffServ allows you to control what traffic is accepted and what traffic is discarded.

How you configure DiffServ support on the switch varies, depending on the role of the switch in your network:

- **Edge device**. An edge device handles ingress traffic, flowing toward the core of the network, and egress traffic, flowing away from the core. An edge device segregates inbound traffic into a small set of traffic classes, and is responsible for determining a packet's classification. Classification is based primarily on the contents of the Layer 3 and Layer 4 headers, and is recorded in the Differentiated Services Code Point (DSCP) added to a packet's IP header.
- **Interior node**. A switch in the core of the network is responsible for forwarding packets, rather than for classifying them. It decodes the DSCP code point in an incoming packet, and provides buffering and forwarding services using the appropriate queue management algorithms.

Before configuring DiffServ on a particular switch, you must determine the QoS requirements for the network as a whole. The requirements are expressed in terms of rules, which are used to classify inbound traffic on a particular interface. The switch software does not support DiffServ in the outbound direction.

Rules are defined in terms of classes, policies, and services:

- **Class**. A class consists of a set of rules that identify which packets belong to the class. Inbound traffic is separated into traffic classes based on Layer 3 and Layer 4 header data and the VLAN ID, and marked with a corresponding DSCP value. One type of class is supported: All, which specifies that every match criterion defined for the class must be true for a match to occur.
- **Policy**. Defines the QoS attributes for one or more traffic classes. An example of an attribute is the ability to mark a packet at ingress. The 7000 Series Managed Switch supports a traffic conditions policy. This type of policy is associated with an inbound traffic class and specifies the actions to be performed on packets meeting the class rules:
  - Marking the packet with a given DSCP code point, IP precedence, or CoS
  - Policing packets by dropping or re-marking those that exceed the class's assigned data rate
  - Counting the traffic within the class
- **Service**. Assigns a policy to an interface for inbound traffic.

DiffServ

This example shows how a network administrator can provide equal access to the Internet (or other external network) to different departments within a company. Each of four departments has its own Class B subnet that is allocated 25 percent of the available bandwidth on the port accessing the Internet.

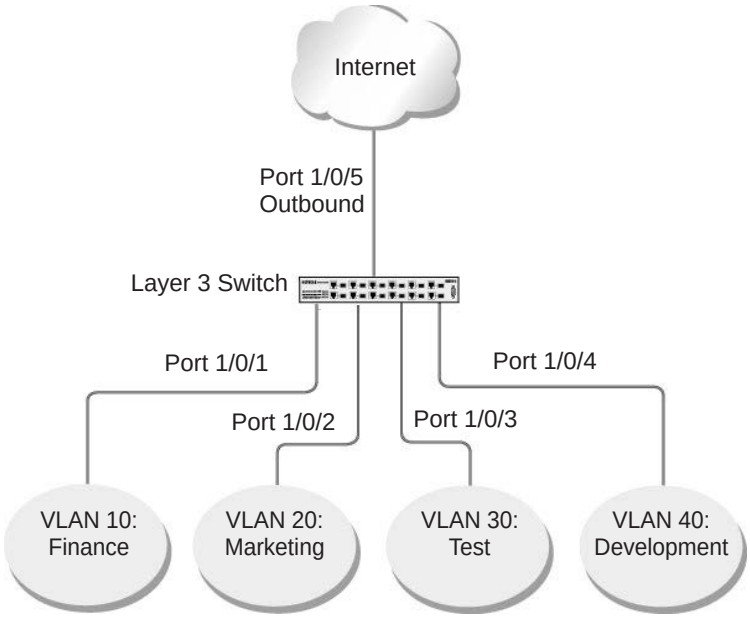


Figure 25. Class B subnet with differentiated services

The example is shown as CLI commands and as a web interface procedure.

CLI: Configure DiffServ

1. Ensure that the DiffServ operation is enabled for the switch.

```
(Netgear Switch) #config
(Netgear Switch) (Config)#diffserv
```

2. Create a DiffServ class of type all for each of the departments, and name them. Define the match criteria of source IP address for the new classes.

```
(Netgear Switch) (Config)#class-map match-all finance_dept
(Netgear Switch) (Config class-map)#match srcip 172.16.10.0 255.255.255.0
(Netgear Switch) (Config class-map)#exit

(Netgear Switch) (Config)#class-map match-all marketing_dept
(Netgear Switch) (Config class-map)#match srcip 172.16.20.0 255.255.255.0
(Netgear Switch) (Config class-map)#exit

(Netgear Switch) (Config)#class-map match-all test_dept
(Netgear Switch) (Config class-map)#match srcip 172.16.30.0 255.255.255.0
(Netgear Switch) (Config class-map)#exit

(Netgear Switch) (Config)#class-map match-all development_dept
(Netgear Switch) (Config class-map)#match srcip 172.16.40.0 255.255.255.0
(Netgear Switch) (Config class-map)#exit
```

3. Create a DiffServ policy for inbound traffic named 'internet_access', adding the previously created department classes as instances within this policy.

   This policy uses the assign-queue attribute to put each department's traffic on a different egress queue. This is how the DiffServ inbound policy connects to the CoS queue settings established in the following example.

```
(Netgear Switch) (Config)#policy-map internet_access in
(Netgear Switch) (Config policy-map)#class finance_dept
(Netgear Switch) (Config policy-class-map)#assign-queue 1
(Netgear Switch) (Config policy-class-map)#exit
(Netgear Switch) (Config policy-map)#class marketing_dept
(Netgear Switch) (Config policy-class-map)#assign-queue 2
(Netgear Switch) (Config policy-class-map)#exit
(Netgear Switch) (Config policy-map)#class test_dept
(Netgear Switch) (Config policy-class-map)#assign-queue 3
(Netgear Switch) (Config policy-class-map)#exit
(Netgear Switch) (Config policy-map)#class development_dept
(Netgear Switch) (Config policy-class-map)#assign-queue 4
(Netgear Switch) (Config policy-class-map)#exit
(Netgear Switch) (Config policy-map)#exit
```

4. Attach the defined policy to interfaces 1/0/1 through 1/0/4 in the inbound direction.

```
(Netgear Switch) (Config)#interface 1/0/1
(Netgear Switch) (Interface 1/0/1)#service-policy in internet_access
(Netgear Switch) (Interface 1/0/1)#exit

(Netgear Switch) (Config)#interface 1/0/2
(Netgear Switch) (Interface 1/0/2)#service-policy in internet_access
(Netgear Switch) (Interface 1/0/2)#exit

(Netgear Switch) (Config)#interface 1/0/3
(Netgear Switch) (Interface 1/0/3)#service-policy in internet_access
(Netgear Switch) (Interface 1/0/3)#exit

(Netgear Switch) (Config)#interface 1/0/4
(Netgear Switch) (Interface 1/0/4)#service-policy in internet_access
(Netgear Switch) (Interface 1/0/4)#exit
```

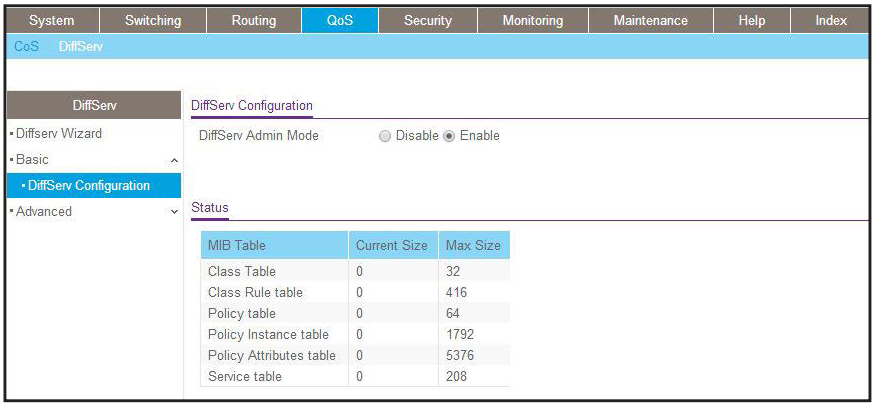
5. Set the CoS queue configuration for the (presumed) egress interface 1/0/5 such that each of queues 1, 2, 3, and 4 gets a minimum guaranteed bandwidth of 25 percent. All queues for this interface use weighted round robin scheduling by default. The DiffServ inbound policy designates that these queues are to be used for the departmental traffic through the assign-queue attribute. It is presumed that the switch will forward this traffic to interface 1/0/5 based on a normal destination address lookup for Internet traffic.

```
(Netgear Switch) (Config)#interface 1/0/5
(Netgear Switch) (Interface 1/0/5)#cos-queue min-bandwidth 0 25 25 25 25 0 0 0
(Netgear Switch) (Interface 1/0/5)#exit
(Netgear Switch) (Config)#exit
```

Web Interface: Configure DiffServ

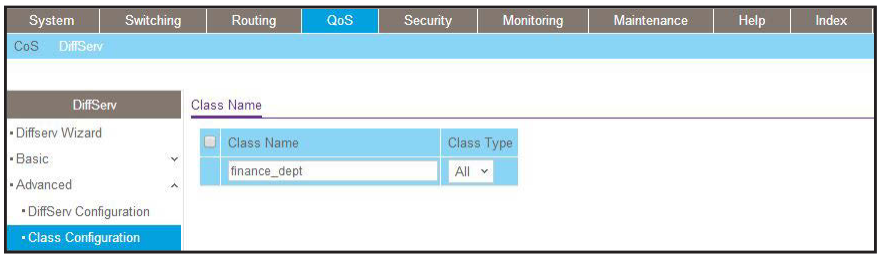
1. Enable Diffserv.
   a. Select **QoS > DiffServ > Basic > DiffServ Configuration**.

      A screen similar to the following displays.



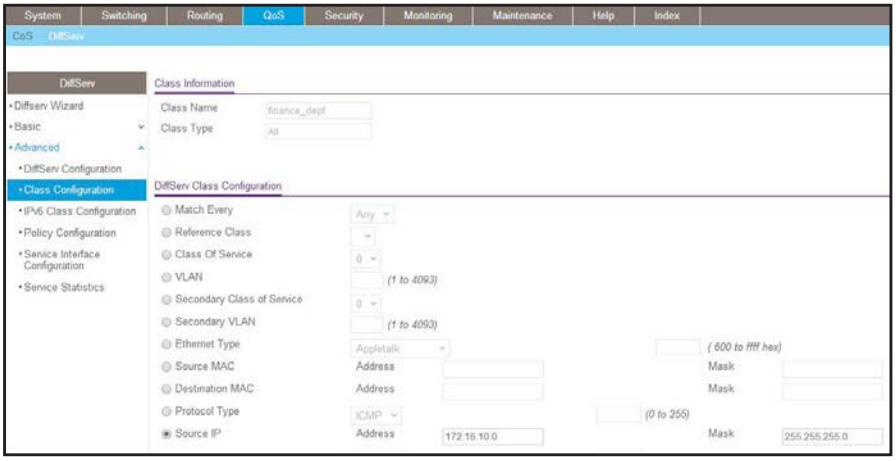
   b. For Diffserv Admin Mode, select the **Enable** radio button.
   c. Click **Apply** to save the settings.
2. Create the class finance_dept.
   a. Select **QoS > DiffServ > Advanced > Class Configuration**.

      A screen similar to the following displays.



   b. Enter the following information:
      - In the **Class Name** field, enter **finance_dept**.
      - In the **Class Type** list, select **All**.
   c. Click **Add** to create a new class finance_dept.
   d. Click the **finance_dept** to configure this class.

A screen similar to the following displays.



e. Under Diffserv Class Configuration, enter the following information:

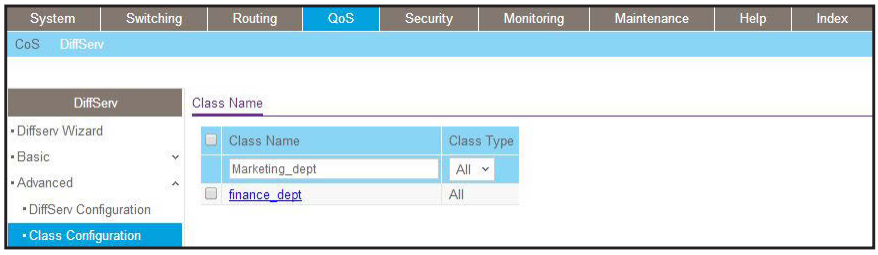
- In the **Source IP Address** field, enter **172.16.10.0**.
- In the **Source Mask** field, enter **255.255.255.0**.

f. Click **Apply**.

3. Create the class marketing_dept:

a. Select **QoS > DiffServ > Advanced >Class Configuration**.

A screen similar to the following displays.



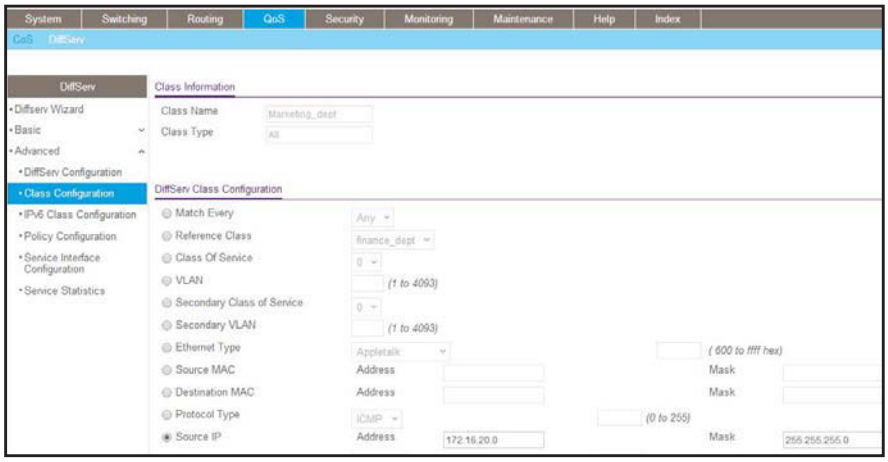
b. Enter the following information:

- In the **Class Name** field, enter **marketing_dept**.
- In the **Class Type** list, select **All**.

c. Click **Add** to create a new class marketing_dept.

d. Click **marketing_dept** to configure this class.

A screen similar to the following displays.



e. Under Diffserv Class Configuration, enter the following information:

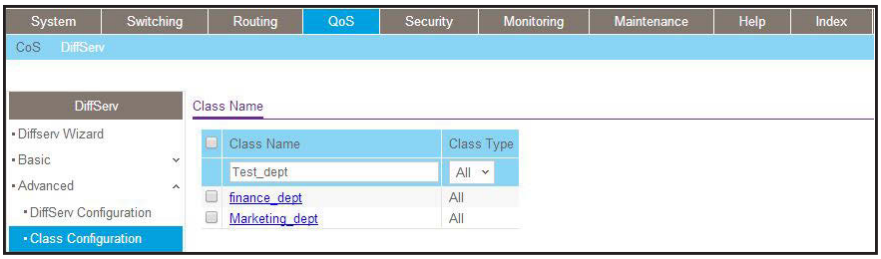
- In the **Source IP Address** field, enter **172.16.20.0**.
- In the **Source Mask** field, enter **255.255.255.0**.

f. Click **Apply**.

4. Create the class test_dept:

a. Select **QoS > DiffServ > Advanced >Class Configuration**.

A screen similar to the following displays.



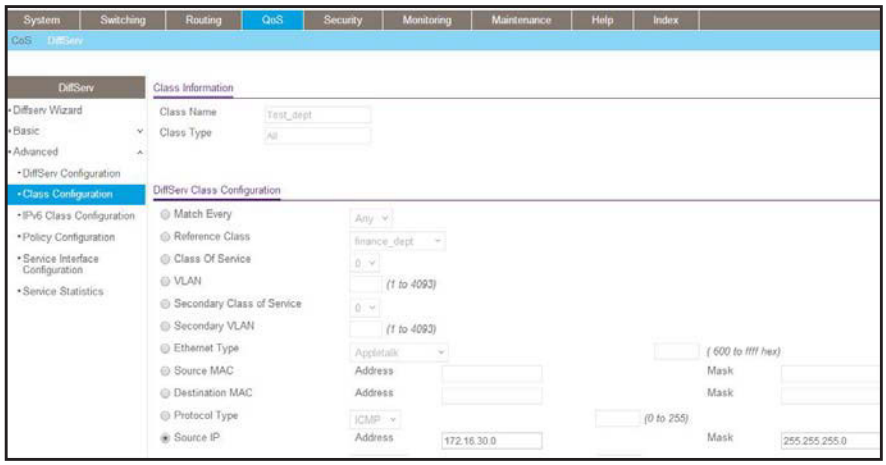
b. Enter the following information:

- In the **Class Name** field, enter **test_dept**.
- In the **Class Type** list, select **All**.

c. Click **Add** to create a new class test_dept.

d. Click **test_dept** to configure this class.

A screen similar to the following displays.



e. Under Diffserv Class Configuration, enter the following information:

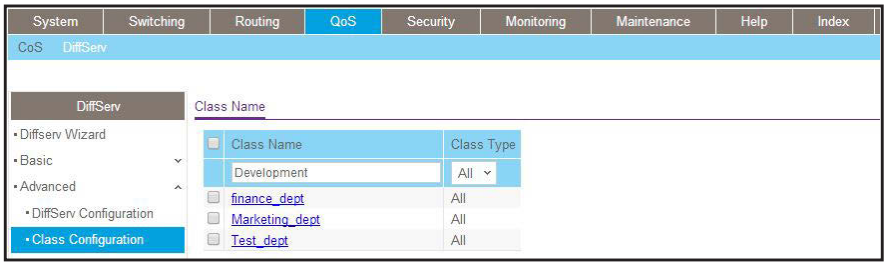
- In the **Source IP Address** field, enter **172.16.30.0**.
- In the **Source Mask** field, enter **255.255.255.0**.

f. Click **Apply**.

5. Create class development_dept.

a. Select **QoS > DiffServ > Advanced > Class Configuration**.

A screen similar to the following displays.



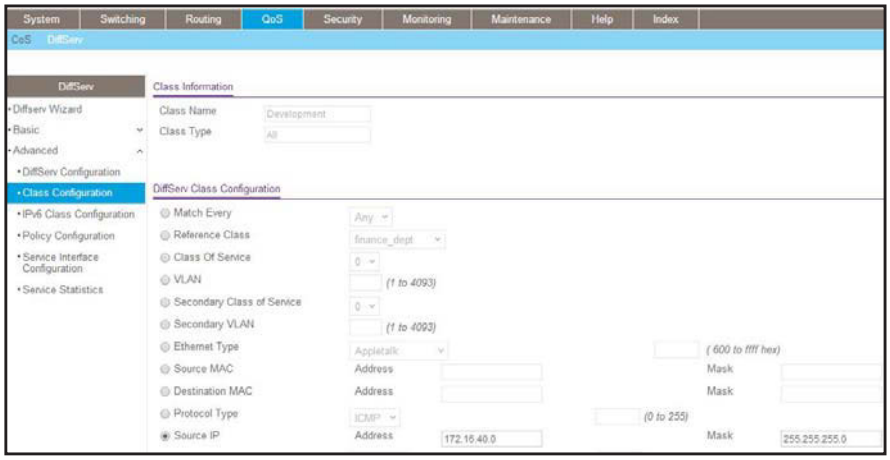
b. Enter the following information:

- In the **Class Name** field, enter **development_dept**.
- In the **Class Type** list, select **All**.

c. Click the **Add** to create a new class development_dept.

d. Click **development_dept** to configure this class.

A screen similar to the following displays.



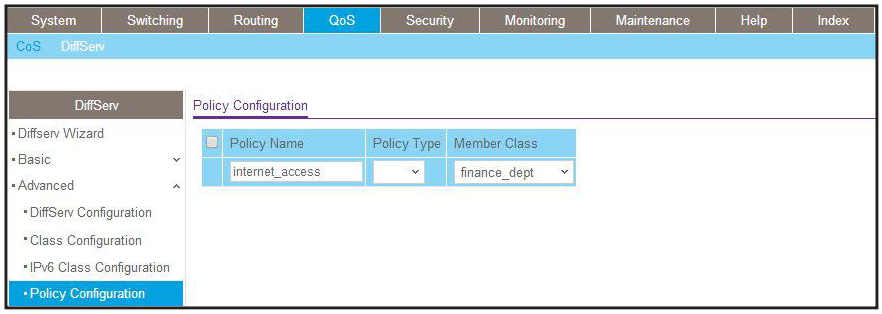
e. Under Diffserv Class Configuration, enter the following information:
   - In the **Source IP Address** field, enter **172.16.40.0**.
   - In the **Source Mask** field, enter **255.255.255.0**.

f. Click **Apply**.

6. Create a policy named internet_access and add the class finance_dept to it.

a. Select **QoS > DiffServ > Advanced > Policy Configuration**.

A screen similar to the following displays.



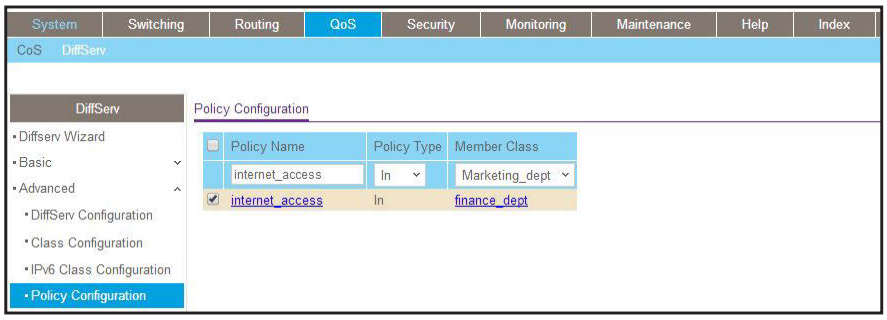
b. Enter the following information:
   - In the **Policy Selector** field, enter **internet_access**.
   - In the **Member Class** list, select the **finance_dept**.

c. Click **Add** to create a new policy internet_access.

7. Add the class marketing_dept into the policy internet_access.

a. Select **QoS > DiffServ > Advanced > Policy Configuration**.

A screen similar to the following displays.



b. Under Policy Configuration, scroll down and select the **internet_access** check box. internet_access now appears in the Policy Selector field at the top.

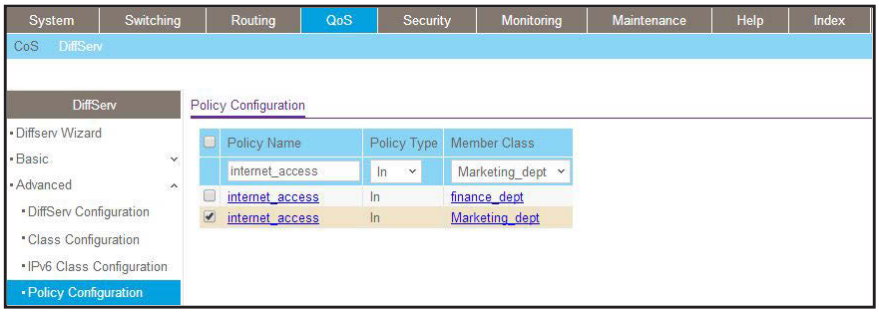
c. In the **Member Class** list, select **marketing_dept**.

d. Click **Apply** to add the class marketing_dept to the policy internet_access.

8. Add the class test_dept into the policy internet_access.

a. Select **QoS > DiffServ > Advanced >Policy Configuration**.

A screen similar to the following displays.



b. Under Policy Configuration, scroll down and select the **internet_access** check box. Internet_access now appears in the Policy Selector field at the top.

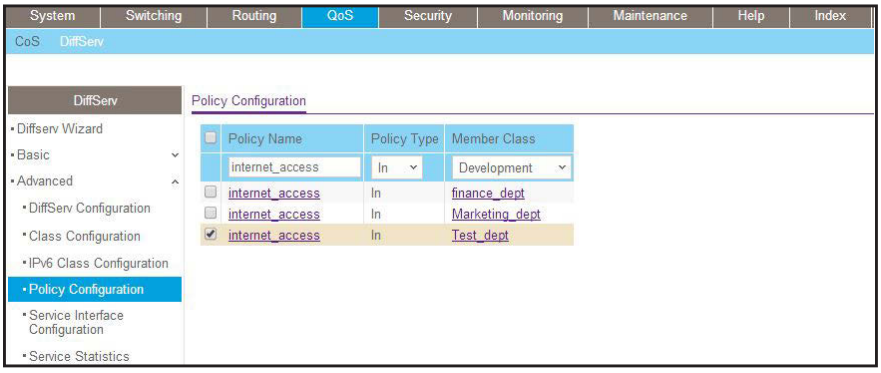
c. In the **Member Class** list, select **test_dept**.

d. Click **Apply** to add the class test_dept to the policy internet_access.

9. Add the class development_dept into the policy internet_access.

a. Select **QoS > DiffServ > Advanced > Policy Configuration**.

A screen similar to the following displays.



b. Under Policy Configuration, scroll down and select the **internet_access** check box. Now internet_access appears in the Policy Selector field at the top.

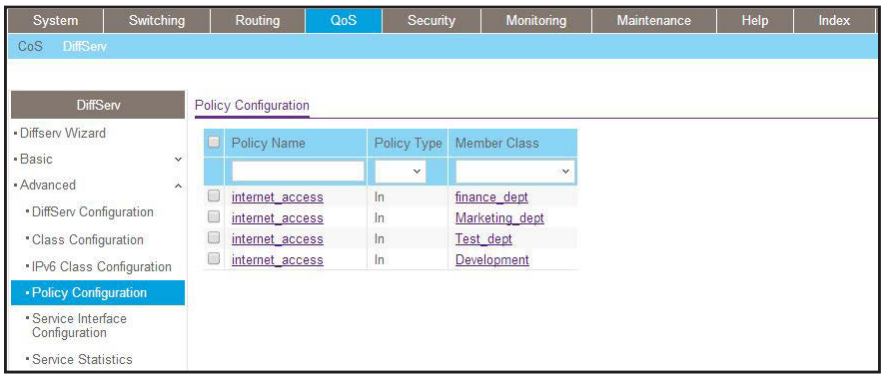
c. In the **Member Class** list, select **development_dept**.

d. Click **Apply** to add the class development_dept to the policy internet_access.

10. Assign queue 1 to finance_dept.

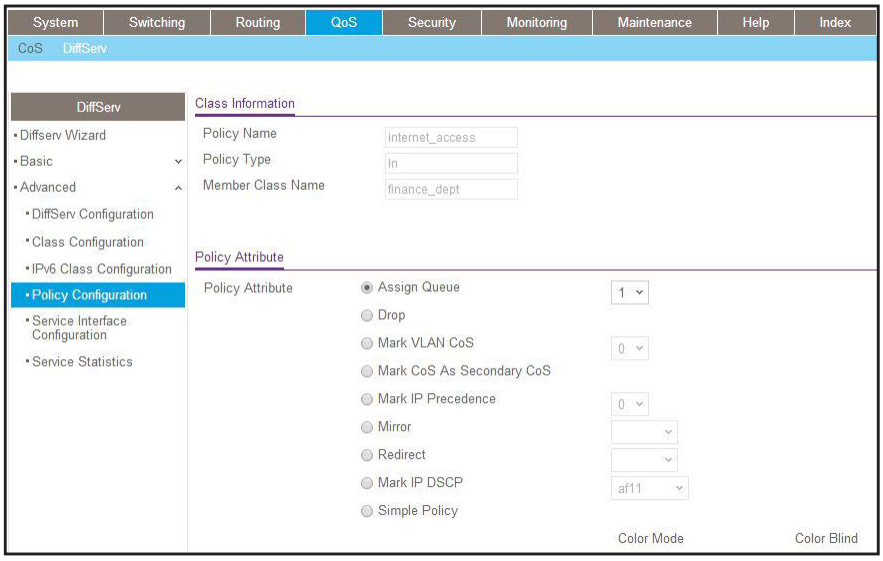
a. Select **QoS > DiffServ > Advanced > Policy Configuration**.

A screen similar to the following displays.



b. Click the **internet_access** check box for the member class finance_dept.

A screen similar to the following displays.



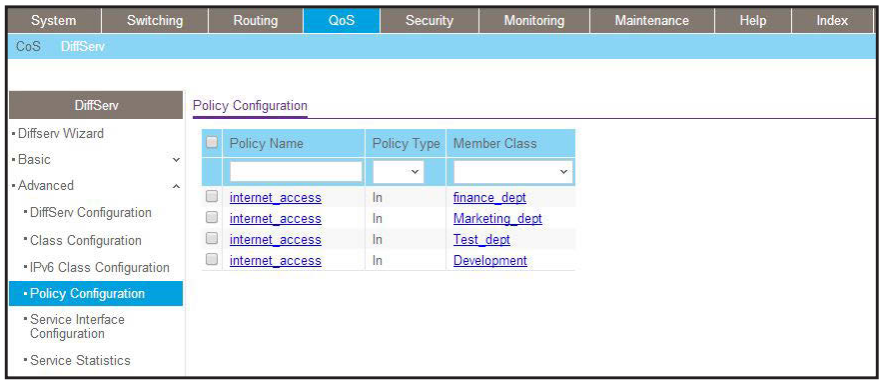
c. In the **Assign Queue** list, select **1**.

d. Click **Apply**.

11. Assign queue 2 to marketing_dept.

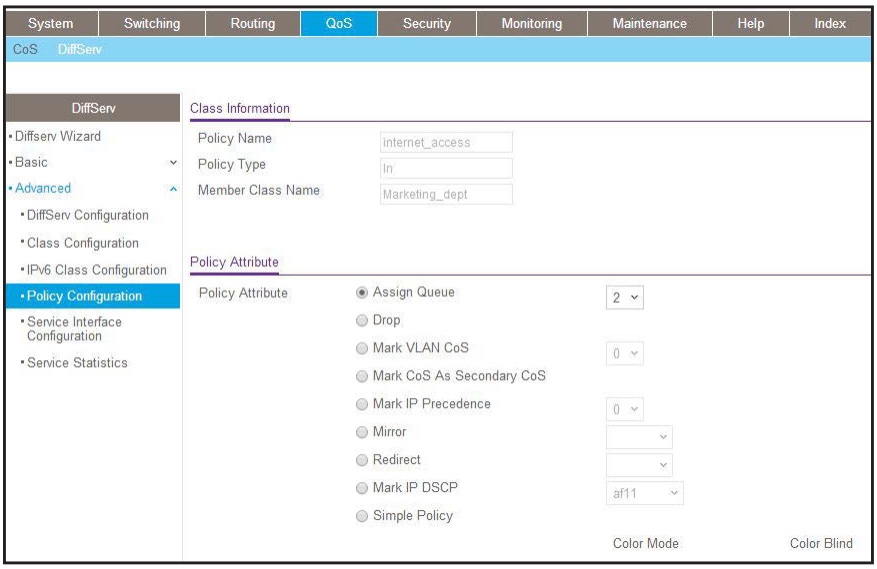
a. Select **QoS > DiffServ > Advanced > Policy Configuration**.

A screen similar to the following displays.



b. Click the **internet_access** check box for marketing_dept.

A screen similar to the following displays.



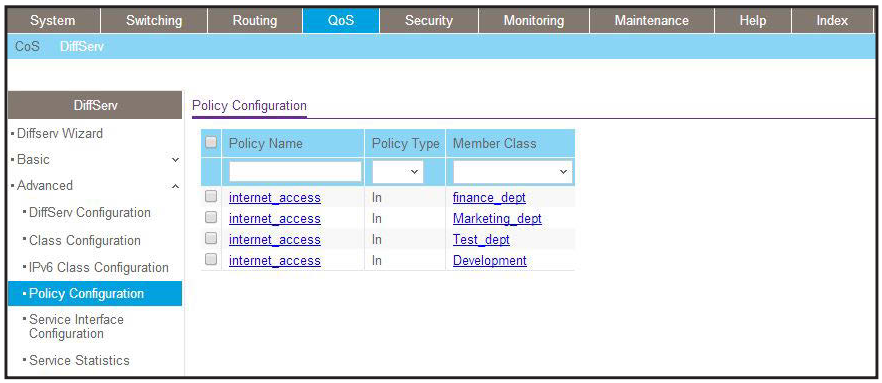
c. In the **Assign Queue** list, select **2**.

d. Click **Apply**.

12. Assign queue 3 to test_dept.

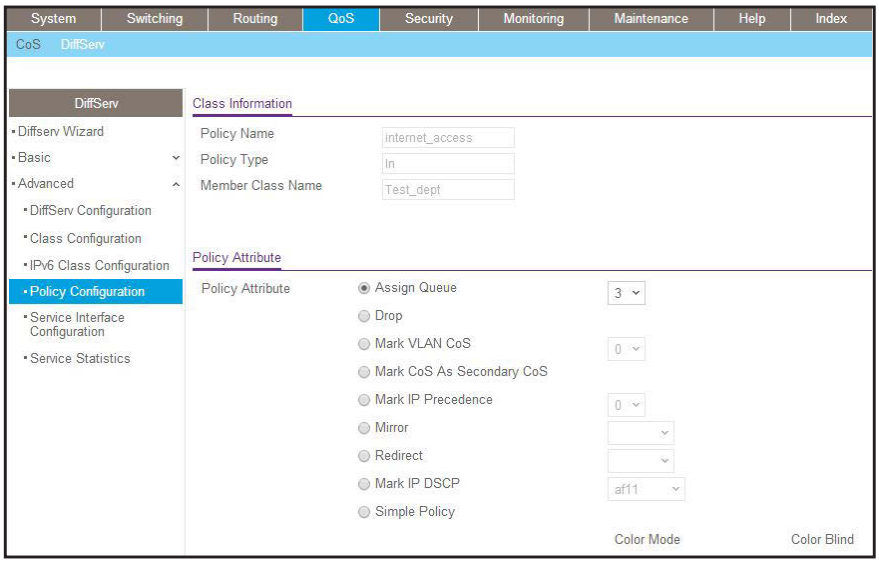
a. Select **QoS > DiffServ > Advanced > Policy Configuration**.

A screen similar to the following displays.



b. Click the **internet_access** check mark for test_dept.

A screen similar to the following displays.



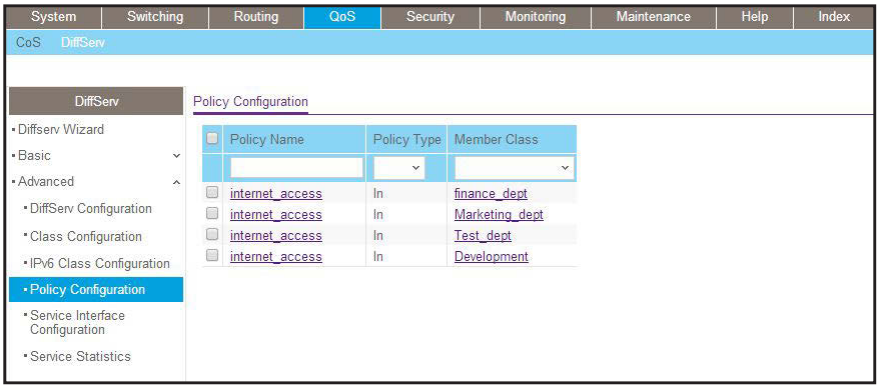
c. In the **Assign Queue** list, select **3**.

d. Click **Apply**.

13. Assign queue 4 to development_dept.

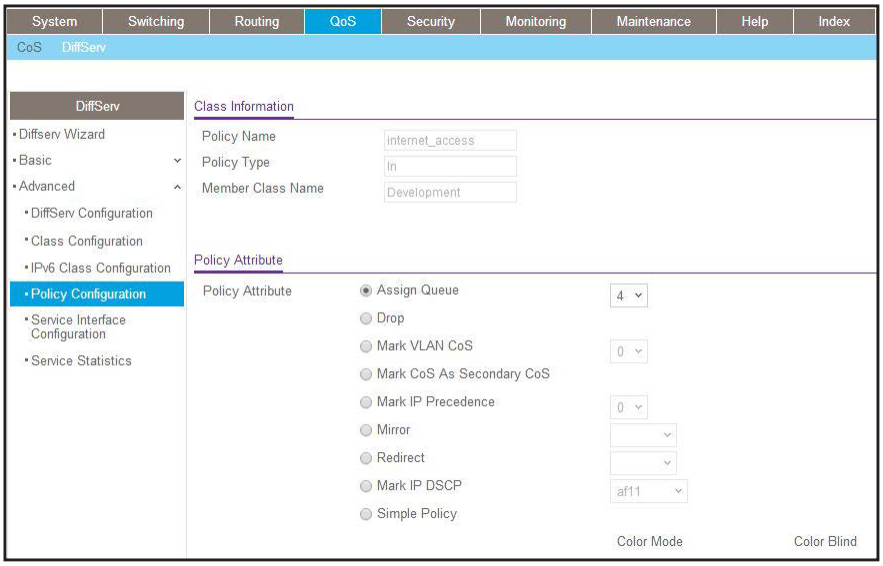
a. Select **QoS > DiffServ > Advanced > Policy Configuration**.

A screen similar to the following displays.



b. Click the **internet_access** check mark for development_dept.

A screen similar to the following displays.



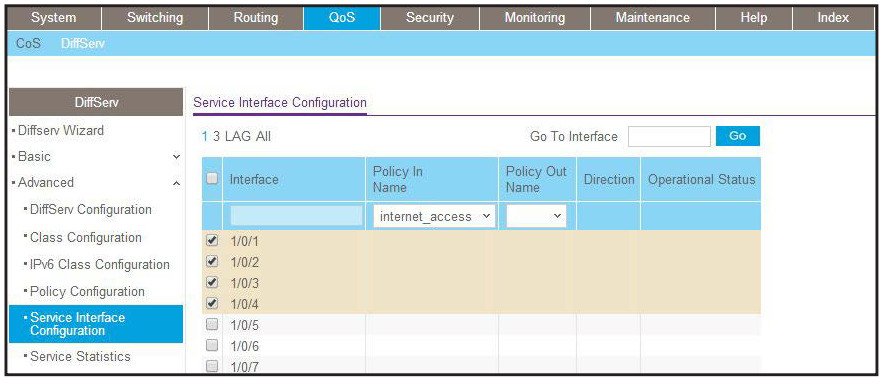
c. In the **Assign Queue** list, select **4**.

d. Click **Apply**.

14. Attach the defined policy to interfaces 1/0/1 through 1/0/4 in the inbound direction.

a. Select **QoS > DiffServ > Advanced > Service Configuration**.

A screen similar to the following displays.



b. Scroll down and select the check boxes for interfaces **1/0/1**, **1/0/2**, **1/0/3**, and **1/0/4**.

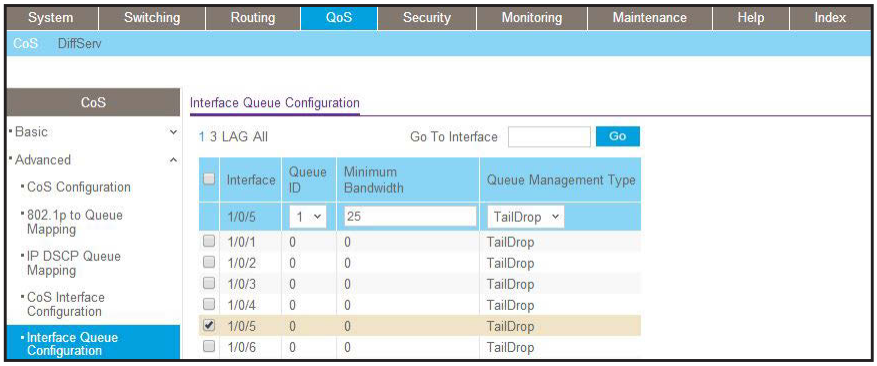
c. In the **Policy In** list, select **internet_access**.

d. Click **Apply**.

15. Set the CoS queue 1 configuration for interface 1/0/5.

a. Select **QoS > CoS > Advanced > Interface Queue Configuration**.

A screen similar to the following displays.



b. Scroll down and select the Interface **1/0/5** check box.

Now 1/0/5 appears in the Interface field at the top.

c. In the **Queue ID** list, select **1**.

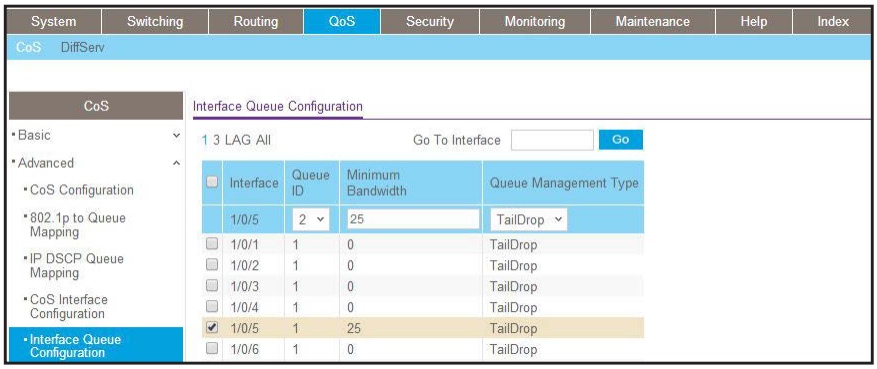
d. In the **Minimum Bandwidth** field, enter **25**.

e. Click **Apply**.

16. Set the CoS queue 2 configuration for interface 1/0/5.

a. Select **QoS > CoS > Advanced > Interface Queue Configuration**.

A screen similar to the following displays.



b. Under Interface Queue Configuration, scroll down and select the interface **1/0/5** check box.

Now 1/0/5 appears in the Interface field at the top.

c. In the **Queue ID** list, select **2**.

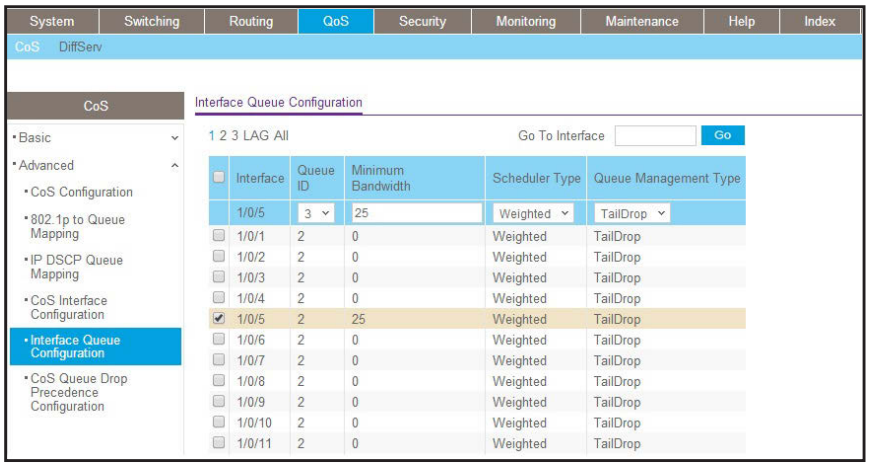
d. In the **Minimum Bandwidth** field, enter **25**.

e. Click **Apply**.

17. Set the CoS queue 3 configuration for interface 1/0/5.

a. Select **QoS > CoS > Advanced > Interface Queue Configuration**.

A screen similar to the following displays.



b. Under Interface Queue Configuration, scroll down and select the interface **1/0/5** check box.

Now 1/0/5 appears in the Interface field at the top.

c. In the **Queue ID** list, select **3**.

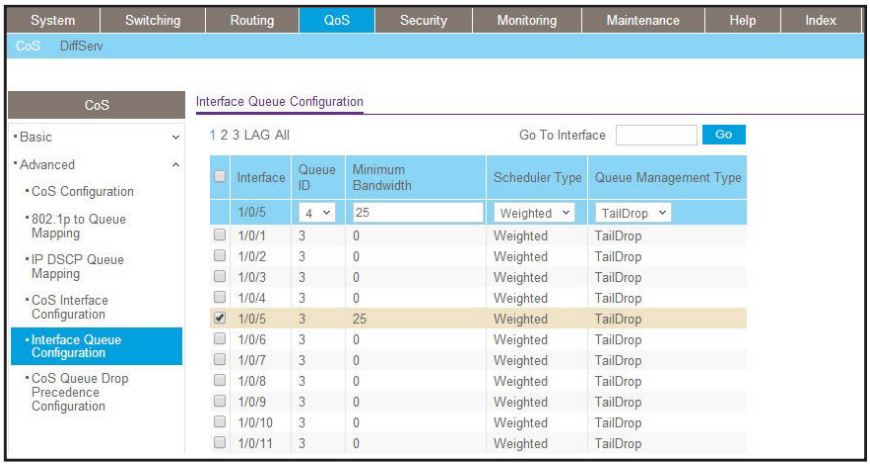
d. In the **Minimum Bandwidth** field, enter **25**.

e. Click **Apply**.

18. Set the CoS queue 4 configuration for interface 1/0/5.

a. Select **QoS > CoS > Advanced > Interface Queue Configuration**.

A screen similar to the following displays.



b. Under Interface Queue Configuration, scroll down and select the Interface **1/0/5** check box.

Now 1/0/5 appears in the Interface field at the top.

c. In the **Queue ID** list, select **4**.

d. In the **Minimum Bandwidth** field, enter **25**.

e. Click **Apply**.

DiffServ for VoIP

One of the most valuable uses of DiffServ is to support Voice over IP (VoIP). VoIP traffic is inherently time sensitive: For a network to provide acceptable service, a guaranteed transmission rate is vital. This example shows one way to provide the necessary quality of service: how to set up a class for UDP traffic, have that traffic marked on the inbound side, and then expedite the traffic on the outbound side. The configuration script is for Router 1 in the accompanying diagram: A similar script should be applied to Router 2.

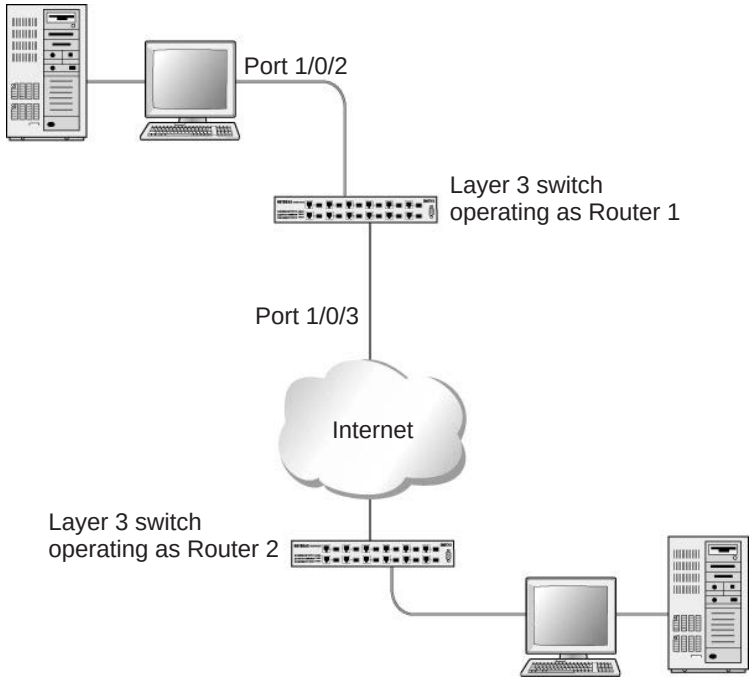


Figure 26. Diffserv for VoIP in Router 1

The example is shown as CLI commands and as a web interface procedure.

CLI: Configure DiffServ for VoIP

1. Enter Global configuration mode. Set queue 5 on all ports to use strict priority mode. This queue will be used for all VoIP packets. Activate DiffServ for the switch.

```
(Netgear Switch) #config
(Netgear Switch) (Config)#cos-queue strict 5
(Netgear Switch) (Config)#diffserv
```

2. Create a DiffServ classifier named **class_voip** and define a single match criterion to detect UDP packets. The class type **match-all** indicates that all match criteria defined for the class must be satisfied in order for a packet to be considered a match.

```
(Netgear Switch) (Config)#class-map match-all class_voip
(Netgear Switch) (Config class-map)#match protocol udp
(Netgear Switch) (Config class-map)#exit
```

3. Create a second DiffServ classifier named **class_ef** and define a single match criterion to detect a DiffServ code point (DSCP) of **EF** (expedited forwarding). This handles incoming traffic that was previously marked as expedited somewhere in the network.

```
(Netgear Switch) (Config)#class-map match-all class_ef
(Netgear Switch) (Config class-map)#match ip dscp ef
(Netgear Switch) (Config class-map)#exit
```

4. Create a DiffServ policy for inbound traffic named **pol_voip**, then add the previously created classes **class_ef** and **class_voip** as instances within this policy.

   This policy handles incoming packets already marked with a DSCP value of **EF** (according to the **class_ef** definition), or marks UDP packets according to the **class_voip** definition) with a DSCP value of **EF**. In each case, the matching packets are assigned internally to use queue 5 of the egress port to which they are forwarded.

```
(Netgear Switch) (Config)#policy-map pol_voip in
(Netgear Switch) (Config policy-map)#class class_ef
(Netgear Switch) (Config policy-class-map)#assign-queue 5
(Netgear Switch) (Config policy-class-map)#exit
(Netgear Switch) (Config policy-map)#class class_voip
(Netgear Switch) (Config policy-class-map)#mark ip-dscp ef
(Netgear Switch) (Config policy-class-map)#assign-queue 5
(Netgear Switch) (Config policy-class-map)#exit
(Netgear Switch) (Config policy-map)#exit
```

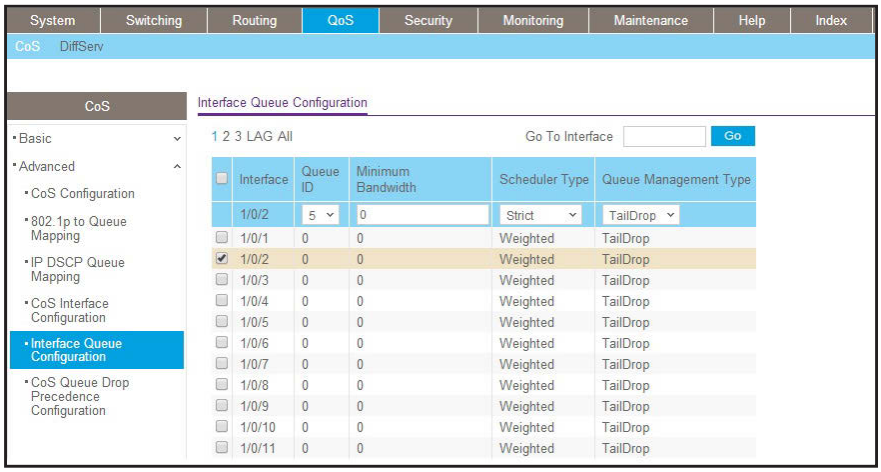
5. Attach the defined policy to an inbound service interface.

```
(Netgear Switch) (Config)#interface 1/0/2
(Netgear Switch) (Interface 1/0/2)#service-policy in pol_voip
(Netgear Switch) (Interface 1/0/2)#exit
(Netgear Switch) (Config)#exit
```

Web Interface: Diffserv for VoIP

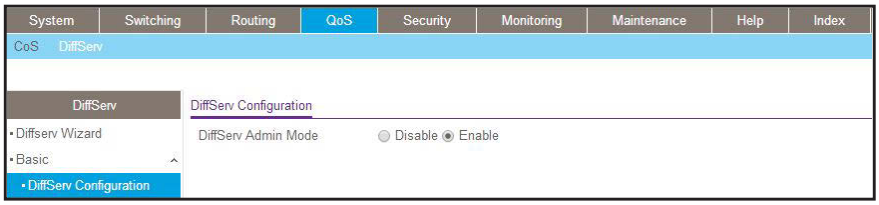
1. Set queue 5 on all interfaces to use strict mode.
   a. Select **QoS > CoS > Advanced > CoS Interface Configuration**.

      A screen similar to the following displays.



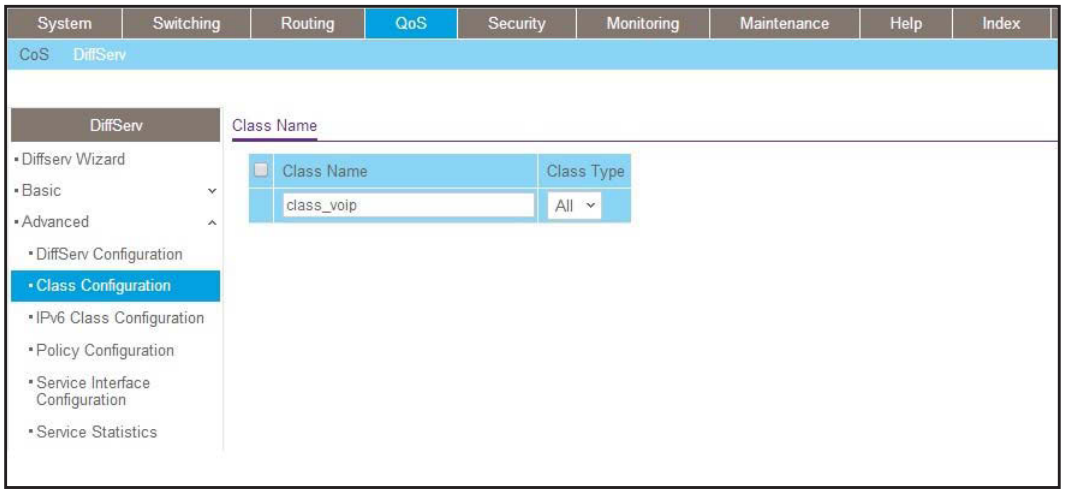
   b. Under Interface Queue Configuration, select all the interfaces.
   c. In the **Queue ID** list, select **5**.
   d. In the **Scheduler Type** list, select **Strict**.
   e. Click **Apply** to save the settings.
2. Enable DiffServ.
   a. Select **QoS > DiffServ > Basic > DiffServ Configuration**.

      A screen similar to the following displays.



   b. For Diffserv Admin Mode, select the **Enable** radio button.
   c. Click **Apply** to save the settings.
3. Create a class class_voip.
   a. Select **QoS > DiffServ > Advanced > DiffServ Configuration**.

A screen similar to the following displays.



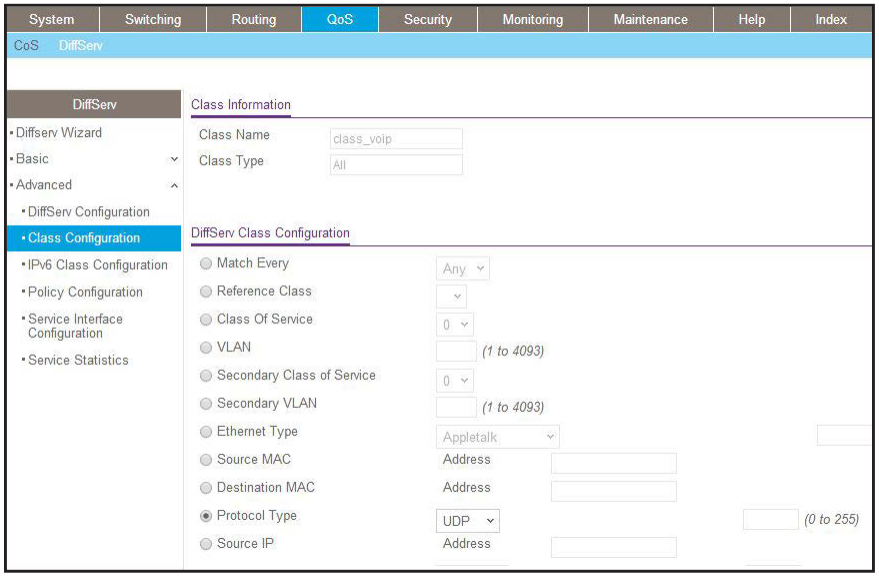
b. In the **Class Name** field, enter **class_voip**.

c. In the **Class Type** list, select **All**.

d. Click **Add** to create a new class.

e. Click **class_voip**.

A screen similar to the following displays.



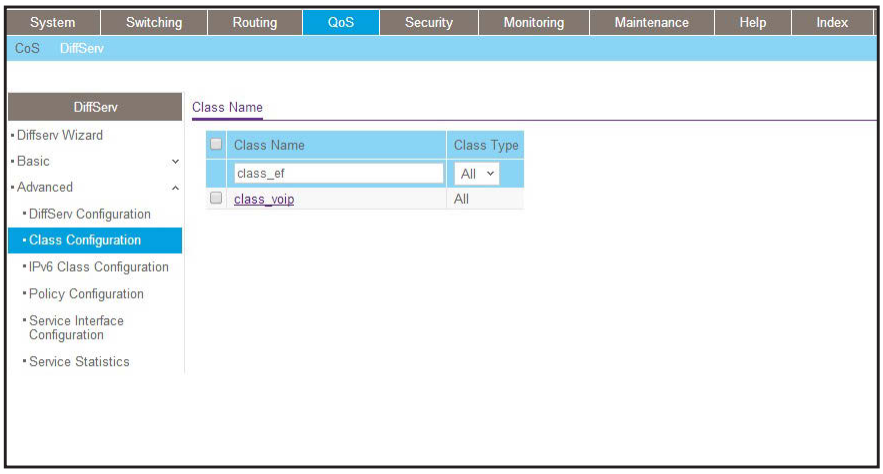
f. In the **Protocol Type** list, select **UDP**.

g. Click **Apply** to create a new class.

4. Create a class class_ef:

a. Select **QoS > DiffServ > Advanced > DiffServ Configuration**.

A screen similar to the following displays.



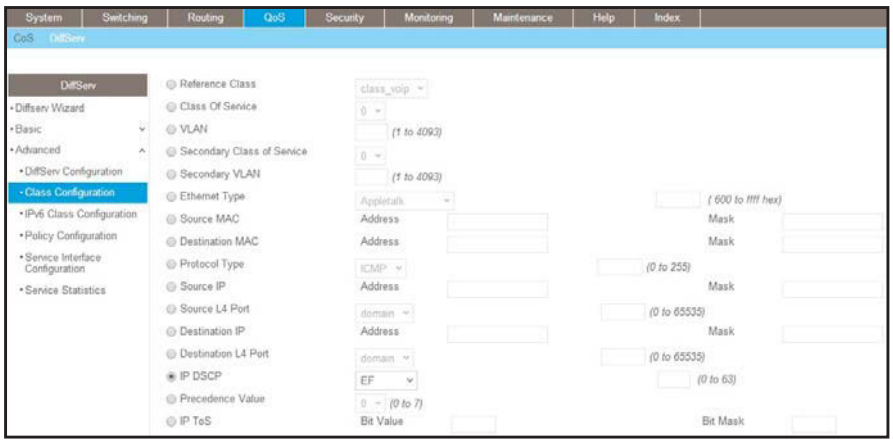
b. In the **Class Name** field, enter **class_ef**.

c. In the **Class Type** list, select **All**.

d. Click **Add** to create a new class.

e. Click **class_ef**.

A screen similar to the following displays.



f. In the **IP DSCP** list, select **ef**.

g. Click **Apply** to create a new class.

5. Create a policy pol_voip. and add class_voip to this policy.

a. Select **QoS > DiffServ > Advanced > Policy Configuration**.

A screen similar to the following displays.

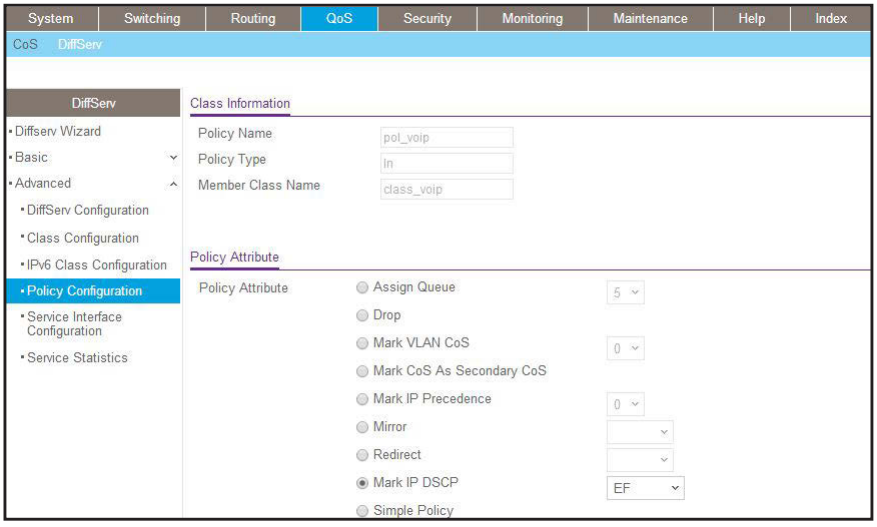
b. In the **Policy Selector** field, enter **pol_voip**.

c. In the **Member Class** list, select **class_voip**.

d. Click **Add** to create a new policy.

e. Click the **pol_voip** whose class member is class_voip.

A screen similar to the following displays.



f. In the **Assign Queue** list, select **5**.

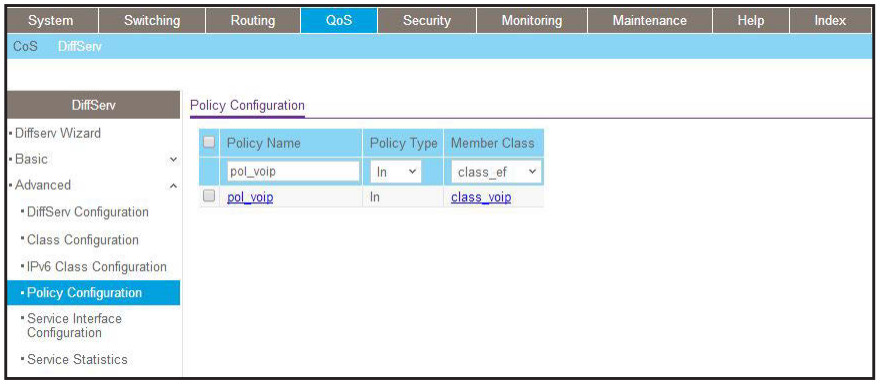
g. For Policy Attribute, select the **Mark IP DSCP** radio button, and select **ef**.

h. Click **Apply** to create a new policy.

6. Add class_ef to the policy pol_voip.

a. Select **QoS > DiffServ > Advanced > Policy Configuration**.

A screen similar to the following displays.



b. Under Policy Configuration, scroll down and select the **pol_voip** check box.

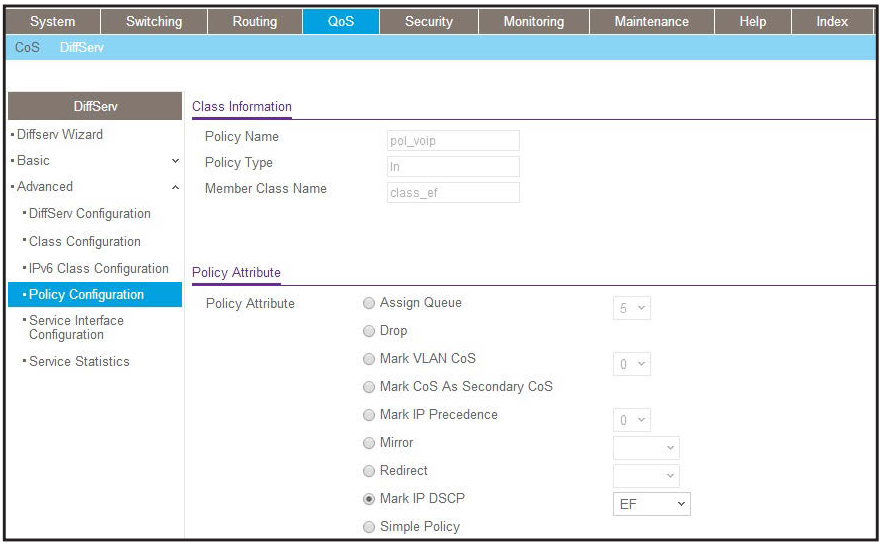
Pol_voip now appears in the Policy Selector field at the top.

c. In the **Member Class** list, select **class_ef** in.

d. Click **Apply** to add the class class_ef to the policy pol_voip.

e. Click the **pol_voip** whose class member is class_ef.

A screen similar to the following displays.



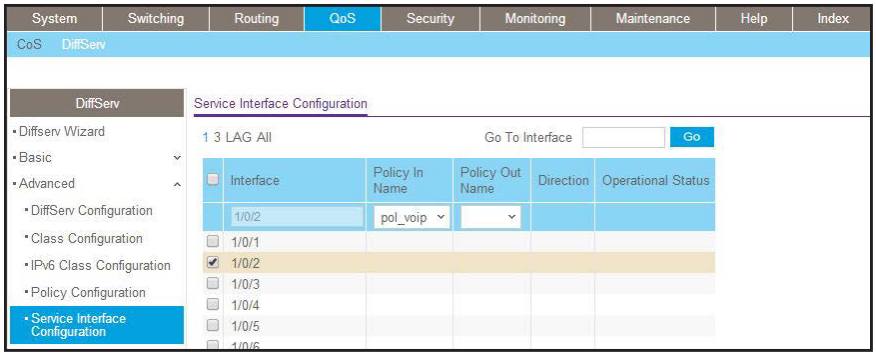
f. In the **Assign Queue** list, select **5**.

g. Click **Apply** to create a new policy.

7. Attach the defined policy to interface 1/0/2 in the inbound direction.

a. Select **QoS > DiffServ > Advanced > Service Configuration**.

A screen similar to the following displays.



b. Scroll down and select the Interface **1/0/2** check box.

Now 1/0/2 appears in the Interface field at the top.

c. In the **Policy In** list, select **pol_voip**.

d. Click **Apply** to create a new policy.

Auto VoIP

The Auto VoIP feature makes it easy to set up voice over IP (VoIP) for IP phones on a switch. From software release 10.0.0 on, the switch supports both protocol-based and OUI-based Auto-VoIP configurations.

Protocol-Based Auto VoIP

In a VoIP system, various signaling protocols are used to establish the connection between two VoIP devices. Protocol-based Auto VoIP provides a better class of service (CoS) to data and signaling VoIP streams than to other traffic. The supported signaling protocols are Session Initiation Protocol (SIP), H.323, and Skinny Call Control Protocol (SCCP). Depending on your configuration, after VoIP packets are identified, the switch takes the following actions:

- If you enable remarking, the switch remarks the voice traffic 802.1p priority with the configured priority at the ingress port to ensure that voice traffic always receives the highest priority throughout the network. You must enable egress tagging on the appropriate uplink port to let the switch carry the remarked priority to the egress port.
- If you assign a queue, make sure that you allocate sufficient bandwidth to the queue to fullfil the priority treatment for VoIP traffic.

Note: Queue assignment and remark 802.1p priority are mutually exclusive configurations. You can configure each configuration on a per-port basis.

After a call session completes and the call is disconnected, the QoS rules are removed.

The ports on which you configure protocol-based Auto VoIP are made members of the voice VLAN automatically. By default, no VLAN is used for the voice VLAN. You must create a voice VLAN first.

OUI-Based Auto VoIP

OUI-based Auto VoIP prioritizes VoIP packets based on the bytes of the organizationally unique identifiers (OUIs) in the source MAC address. The switch is preconfigured with a default list of OUIs. You can also add OUIs that need prioritization. The switch can support up to 128 OUIs, including the default OUIs.

By default, the switch uses the highest available priority for all frames that match OUIs on the OUI list. You can override the default priority and configure a different priority. You need to map the priority to a traffic class to achieve the desired egress queuing for VoIP traffic.

The switch assigns all VoIP traffic that matches a known OUI list to the VoIP VLAN. If you modify the VoIP VLAN, all existing MAC VLAN entries are removed. The MAC entries are deleted from the forwarding database and relearned with the new VLAN as the devices transmit packets. The port VLAN membership also changes.

The switch assigns untagged VoIP traffic only to the VoIP VLAN and uses the associated priority for egress queuing.

If you enable port mirroring on a port that is configured for Auto VoIP, the port remains nonoperational.

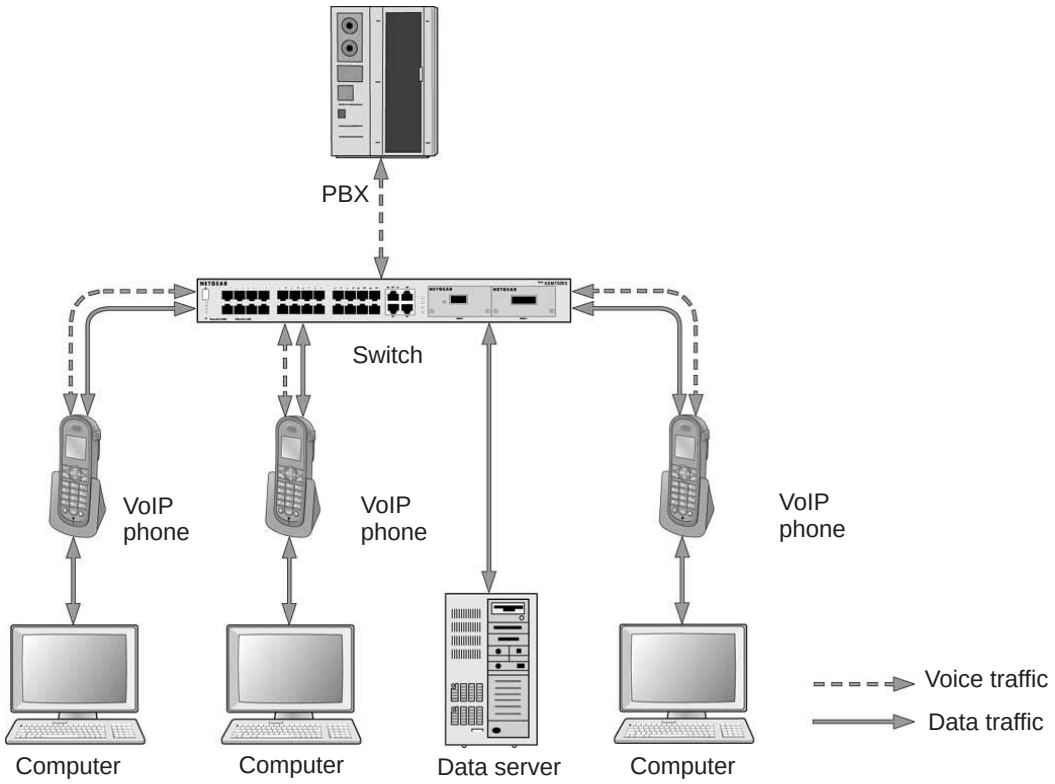


Figure 27. OUI-based Auto VoIP topology

Example 1: Enable Protocol-Based Auto VoIP

This example is provided as CLI commands and as a web interface procedure.

CLI: Protocol-Based Auto VoIP

This script in this section shows how to set up Auto VoIP per port.

1. Enable protocol-based Auto VoIP on a specific port of the switch.

```
(Netgear Switch)(Configure)#interface 2/0/1
(Netgear Switch)(Interface 2/0/1)#auto-voip protocol-based
```

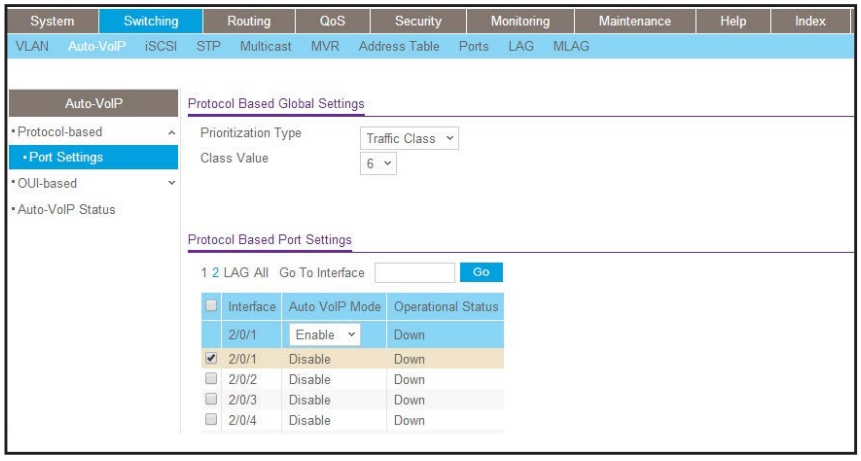
2. Display the Auto VoIP information.

```
(Netgear Switch) #show auto-voip protocol-based interface 2/0/1
VoIP VLAN Id..................................... 2
Prioritization Type.............................. traffic-class
Class Value...................................... 6
Interface  Auto VoIP Mode Operational Status
---------  -------------- -----------------
2/0/1      Enabled        Up
```

Web Interface: Configure Protocol-Based Auto VoIP

1. Enable protocol-based Auto VoIP on a specific port of the switch:
   a. Select **Switching > Auto-VoIP > Protocol-based > Port Settings**.

      A screen similar to the following displays.



   b. Scroll down and select the interface **2/0/1** check box.

      The Interface field in the table heading displays 2/0/1.

   c. From the Auto VoIP Mode mode, select **Enable**.
   d. Click **Apply**.

Example 2: Change the Queue of Protocol-Based Auto VoIP

This example is provided as CLI commands and as a web interface procedure.

CLI: Change the Queue of Protocol-Based Auto VoIP

Protocol-based VoIP classifies and prioritizes packets and places them in the higher-priority queue. By default, the packets are placed in egress queue 6. However, you can override the egress queue setting. The following example shows how to assign the protocol-based Auto VoIP to egress queue 4.

1. Change the egress queue of protocol-based Auto VoIP.

```
(Netgear Switch) (Config)#auto-voip protocol-based traffic-class 4
```

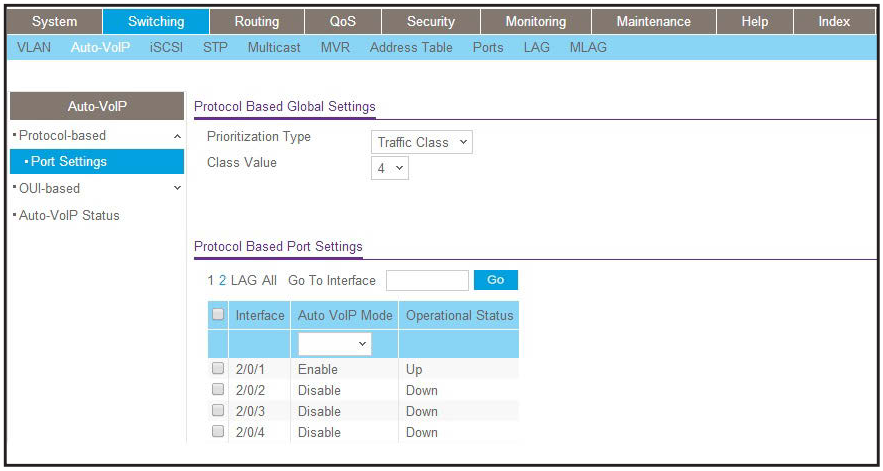
2. Display the Auto VoIP information.

```
(Netgear Switch) #show auto-voip protocol-based interface 2/0/1
VoIP VLAN Id................................ 2
Prioritization Type......................... traffic-class
Class Value................................. 4
Interface  Auto VoIP Mode Operational Status
---------  -------------- ----------------
2/0/1      Enabled        Up
```

Web Interface: Configure Protocol-Based Auto VoIP

1. Change the queue of protocol-based Auto VoIP.
   a. Select **Switching > Auto-VoIP > Protocol-based > Port Settings**.

      A screen similar to the following displays.



   b. From the Class Value menu, select **4**.
   c. Click **Apply**.

Example 3: Create an Auto VoIP VLAN

This example is provided as CLI commands and as a web interface procedure.

CLI: Create an Auto VoIP VLAN

Since no default VoIP VLAN is specified, you must create a VLAN first to use auto VoIP.

1. Create VLAN 5.

```
(Netgear Switch) #vlan database
(Netgear Switch) (Vlan)#vlan 5
(Netgear Switch) (Vlan)#exit
```

2. Assign the VoIP traffic to VLAN 5, which becomes the VoIP VLAN.

```
(Netgear Switch) (Config)#auto-voip vlan 5
```

3. Display the protocol-based Auto VoIP information.

```
(Netgear Switch) #show auto-voip protocol-based interface 2/0/1

VoIP VLAN Id................................. 5
Prioritization Type.......................... traffic-class
Class Value.................................. 6

Interface  Auto VoIP Mode Operational Status
---------  -------------- -----------------
2/0/1      Enabled        Up
```

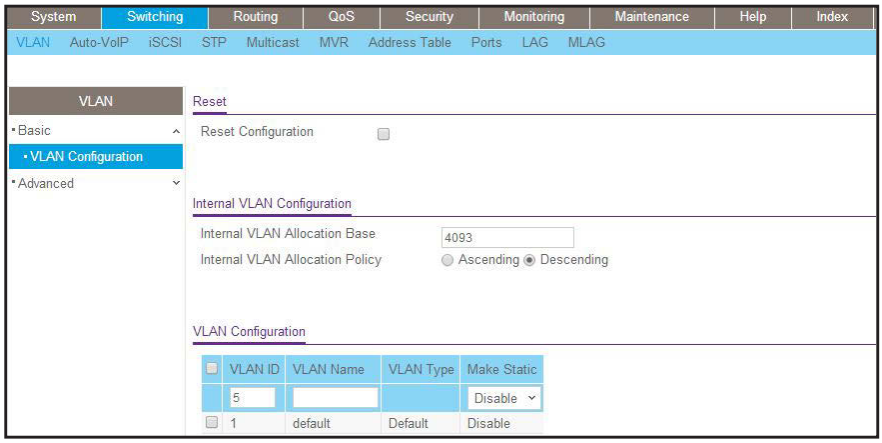
4. Display the OUI-based Auto VoIP information.

```
(Netgear Switch) #show auto-voip oui-based interface 2/0/1

VoIP VLAN Id................................. 5
Priority..................................... 7
Interface  Auto VoIP Mode Operational Status
---------  -------------- -----------------
2/0/1      Disabled       Down
```

Web Interface: Change the Auto VoIP VLAN

1. Create a VLAN 5:
   a. Select **Switching > VLAN > Basic > Vlan Configuration**.

      A screen similar to the following displays.



   b. In the VLAN ID field, enter **5**.
   c. Click **Add**.
2. Assign the VoIP traffic to VLAN 5.
   a. Select **Switching > Auto-VoIP > Protocol-based > Port Settings**.

      A screen similar to the following displays.

   b. From the **VoIP VLAN Id** menu, select **5**.
   c. Click **Apply**.

DiffServ for IPv6

This feature extends the existing QoS ACL and DiffServ functionality by providing support for IPv6 packet classification.

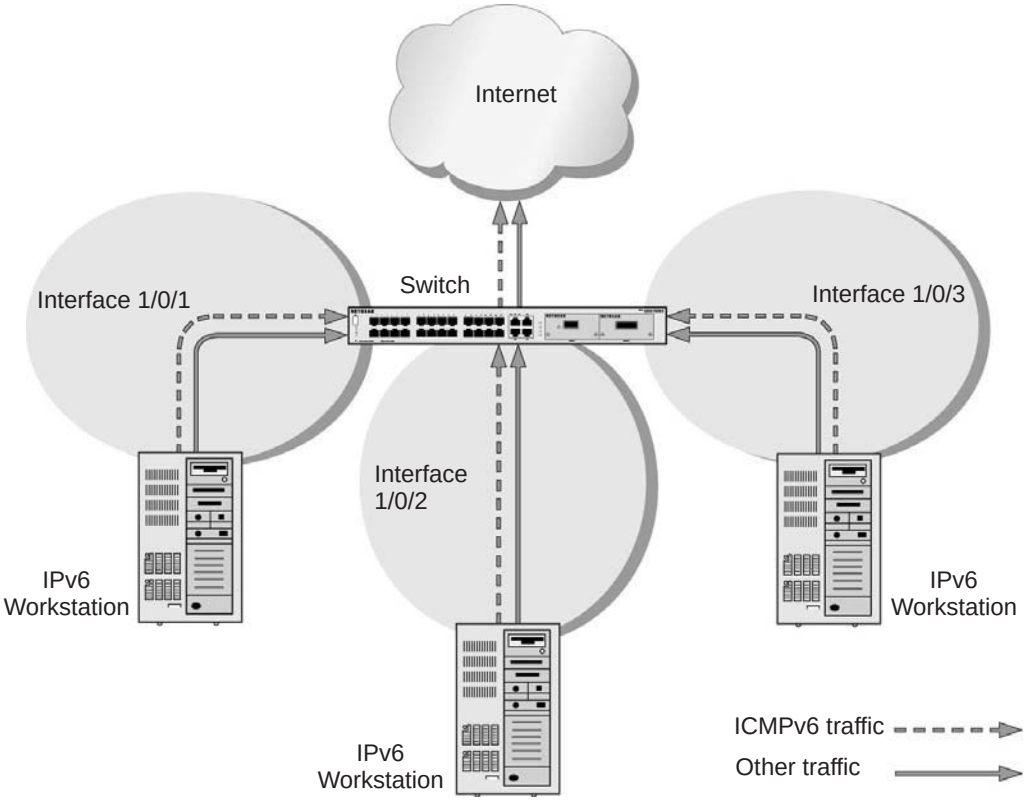


Figure 28. DiffServ for IPv6

The example is shown as CLI commands and as a web interface procedure.

CLI: Configure DiffServ for IPv6

The script in this section shows how to prioritize ICMPv6 traffic over other IPv6 traffic.

1. Create the IPv6 class classicmpv6.

```
(Netgear Switch) (Config)# class-map match-all classicmpv6 ipv6
```

2. Define matching criteria as protocol ICMPv6.

```
(Netgear Switch) (Config-classmap) # match protocol 58
(Netgear Switch) (Config-classmap) # exit
```

3. Create the policy policyicmpv6.

```
(Netgear Switch) (Config)# policy-map policyicmpv6 in
```

4. Associate the previously created class classicmpv6.

```
(Netgear Switch) (Config-policy-map)# class classicmpv6
```

5. Set the attribute as assign queue 6.

```
(Netgear Switch) (Config-policy-classmap)# assign-queue 6
(Netgear Switch) (Config-policy-map)# exit
```

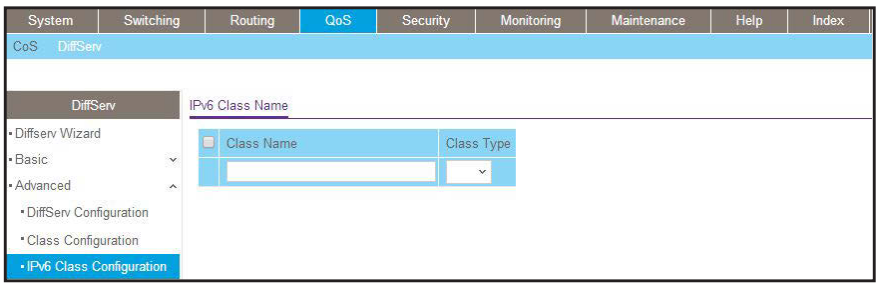
6. Attach the policy policy_icmpv6 to interfaces 1/0/1,1/0/2 and 1/0/3:

```
(Netgear Switch) (Config)# interface 1/0/1
(Netgear Switch) (Interface 1/0/1)# service-policy in policyicmpv6
(Netgear Switch) (Interface 1/0/1)# exit

(Netgear Switch) (Config)# interface 1/0/2
(Netgear Switch) (Interface 1/0/2)# service-policy in policyicmpv6
(Netgear Switch) (Interface 1/0/2)# exit

(Netgear Switch) (Config)# interface 1/0/3
(Netgear Switch) (Interface 1/0/3)# service-policy in policyicmpv6
(Netgear Switch) (Interface 1/0/3)# exit
```

Web Interface: Configure DiffServ for IPv6

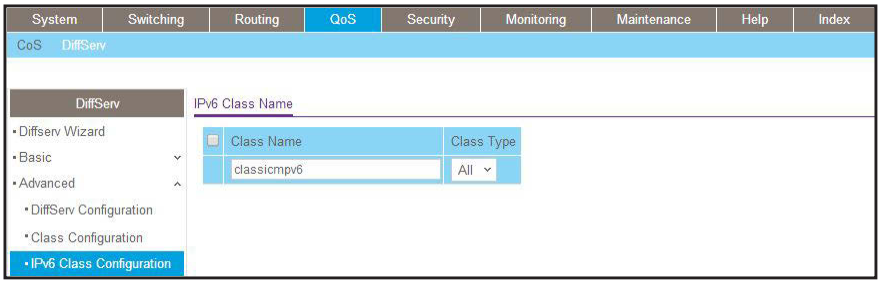
1. Create the IPv6 class classicmpv6.
   a. Select **QoS > DiffServ > Advanced > IPv6 Class Configuration**.

      A screen similar to the following displays.



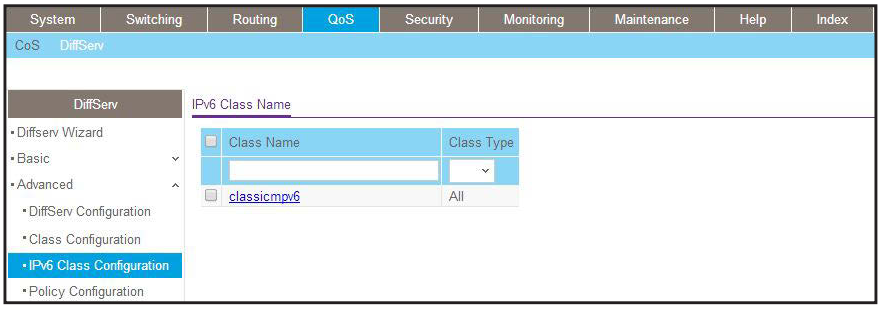
   b. In the **Class Name** field, enter **classicmpv6**.
   c. In the **Class Type** list, select **All**.

A screen similar to the following displays.



d. Click **Add** to create the IPv6 class.

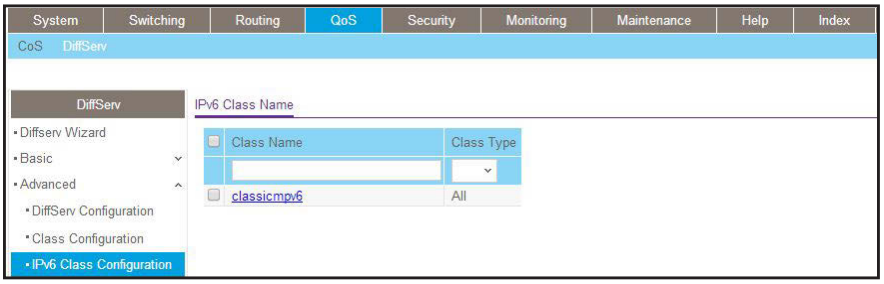
A screen similar to the following displays.



2. Define matching criteria as protocol ICMPv6.

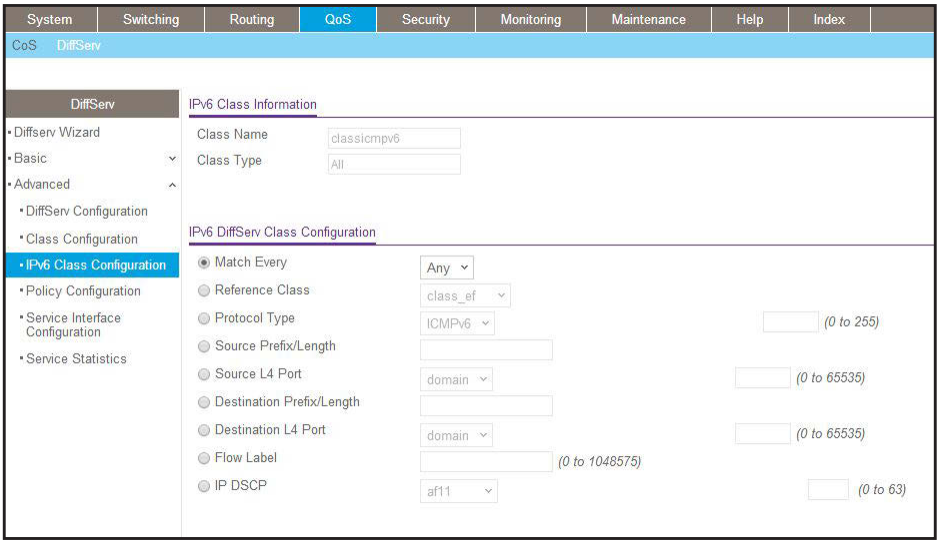
a. Select **QoS > DiffServ > Advanced > IPv6 Class Configuration**.

A screen similar to the following displays.



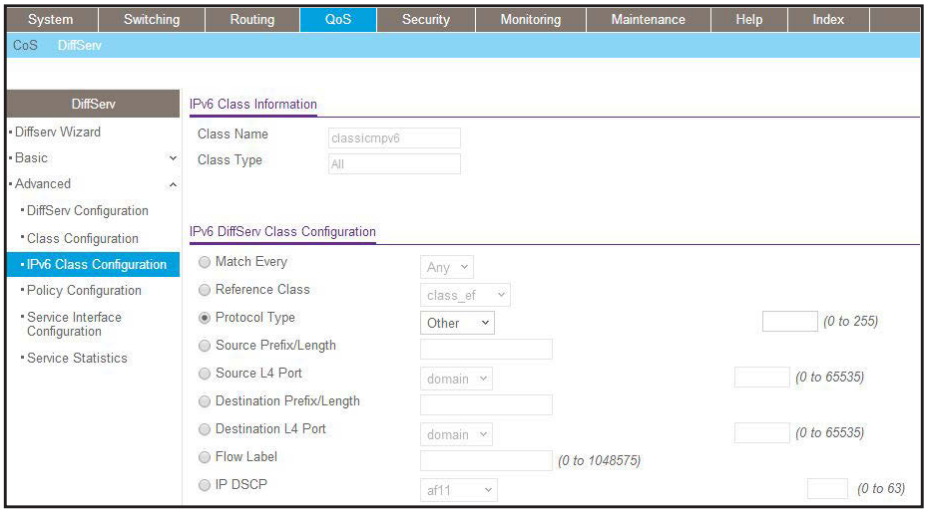
b. Click the class **classicmpv6**.

A screen similar to the following displays.

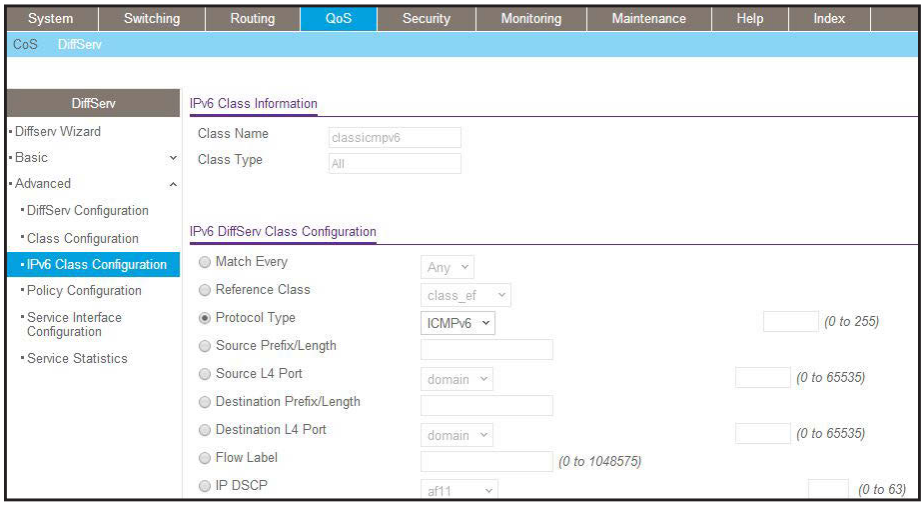


c. Select the **Protocol Type** radio button, select **Other**, and enter **58**.

A screen similar to the following displays.



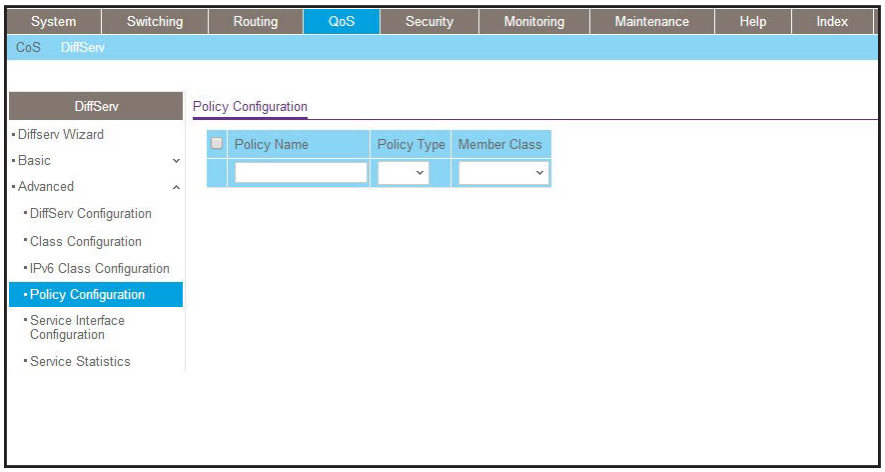
d. Click the **Apply** button.



3. Create the policy policyicmpv6, and associate the previously created class classicmpv6.

a. Select **QoS > DiffServ > Advanced > Policy Configuration**.

A screen similar to the following displays.

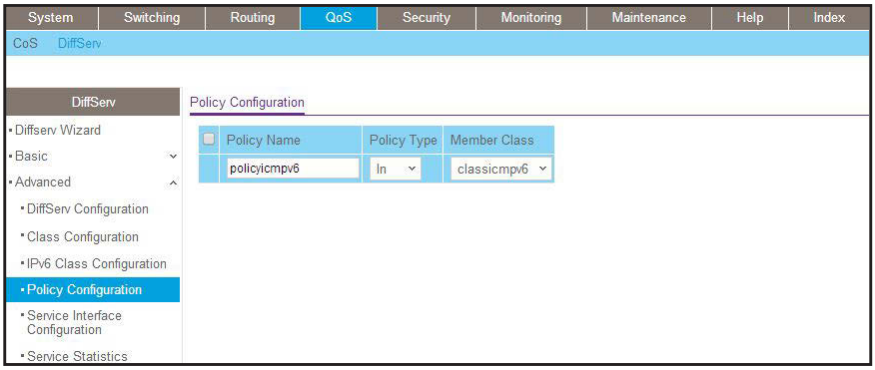


b. In the **Policy Name** field, enter **policyicmpv6**.

c. In the **Policy Type** list, select **In**.

d. In the **Member Class** list, select **classicmpv6**.

A screen similar to the following displays.

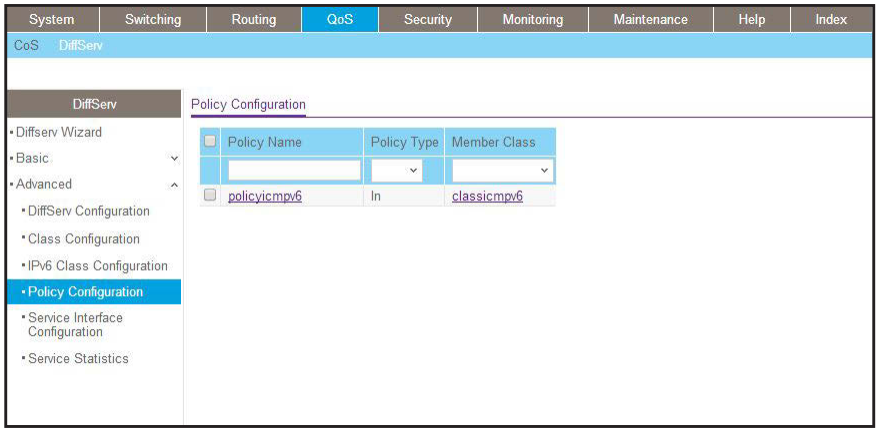


e. Click **Add**.

4. Set the attribute as assign queue 6.

a. Select **QoS > DiffServ > Advanced > Policy Configuration**.

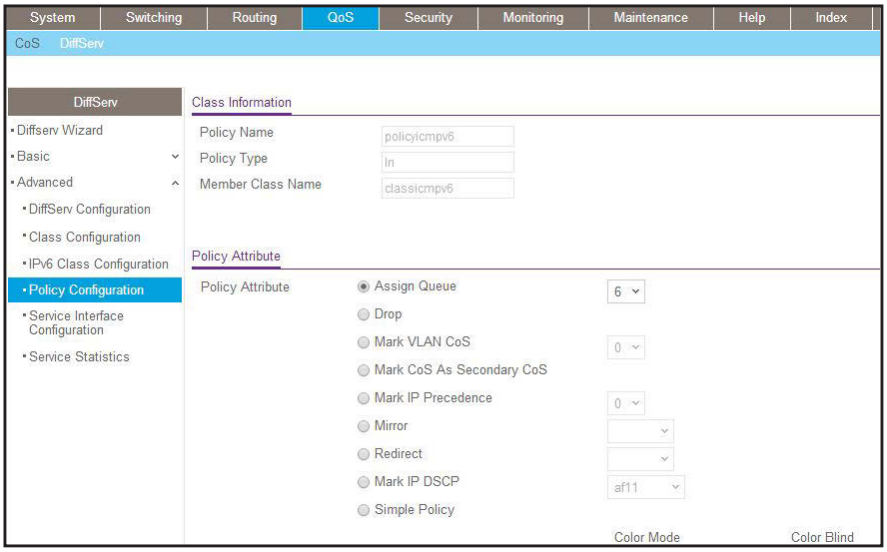
A screen similar to the following displays.



b. Click the policy **policyicmpv6**.

c. In the **Assign Queue** list, select **6**.

A screen similar to the following displays.

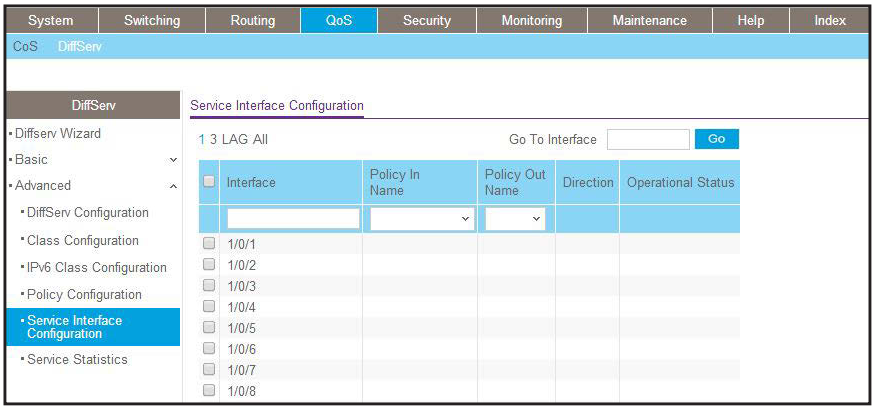


d. Click **Apply**.

5. Attach the policy policyicmpv6 to interfaces 1/0/1,1/0/2 and 1/0/3.

a. Select **QoS > DiffServ > Advanced > Service Interface Configuration**.

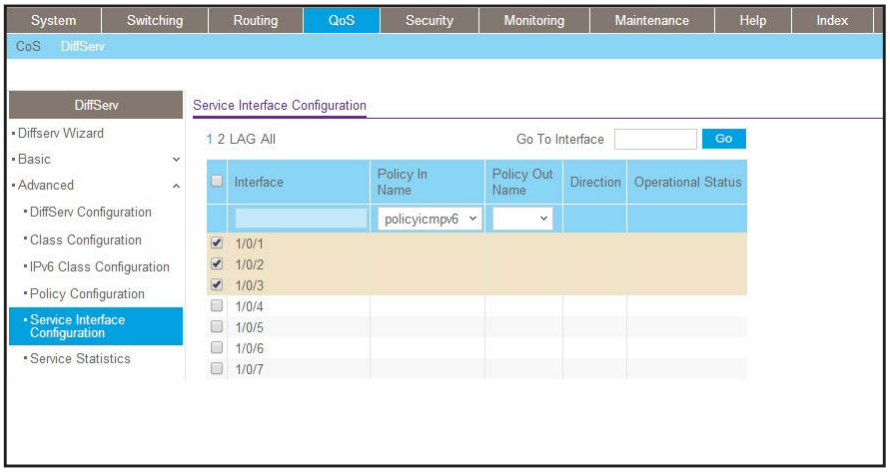
A screen similar to the following displays.



b. In the **Policy Name** list, select **policyicmpv6**.

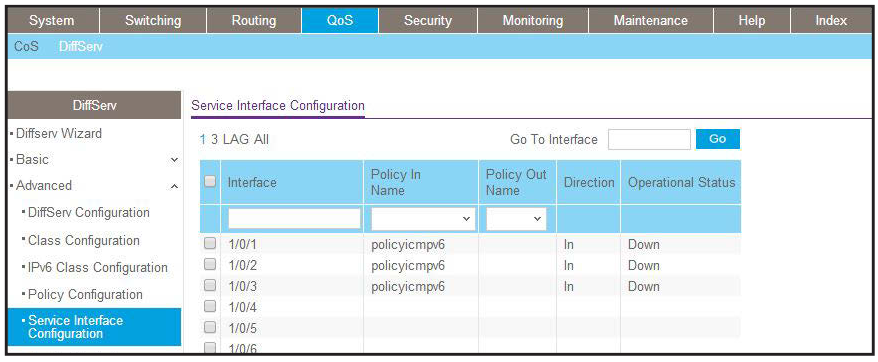
c. Select the Interface **1/0/1**, **1/0/2**, and **1/0/3** check boxes.

A screen similar to the following displays.



d. Click **Apply**.

A screen similar to the following displays.



Color Conform Policy

This example shows how to create a policy to police the traffic to a committed rate. The packets with IP precedence value of 7 are colored green to ensure that these packets are the last to be dropped when there is congestion. The example is shown as CLI commands and as a web interface procedure.

CLI: Configure a Color Conform Policy

1. Create a VLAN 5 and configure ports 1/0/13 and 1/0/25 as its members.

```
(Netgear Switch) #vlan database
(Netgear Switch) (Vlan)#vlan 5
(Netgear Switch) (Vlan)#exit
(Netgear Switch) #config
(Netgear Switch) (Config)#interface 1/0/13
(Netgear Switch) (Interface 1/0/13)#vlan participation include 5
(Netgear Switch) (Interface 1/0/13)#vlan tagging 5
(Netgear Switch) (Interface 1/0/13)#exit
(Netgear Switch) (Config)#interface 1/0/25
(Netgear Switch) (Interface 1/0/25)#vlan participation include 5
(Netgear Switch) (Interface 1/0/25)#vlan tagging 5
(Netgear Switch) (Interface 1/0/25)#exit
```

2. Create classes class_vlan and class_color.

Note: DiffServ service is enabled by default.

```
(Netgear Switch) (Config)#class-map match-all class_vlan
(Netgear Switch) (Config-classmap)#match vlan 5
(Netgear Switch) (Config-classmap)#exit
(Netgear Switch) (Config)#class-map match-all class_color
(Netgear Switch) (Config-classmap)#match ip precedence 7
(Netgear Switch) (Config-classmap)#exit
```

3. Create a policy to police the traffic to a rate of 1000 kbps with an allowed burst size of 64 KB. Furthermore, the packets with IP precedence value of 7 will be colored green. That means these packets will be the last packets to be dropped in the event of congestion beyond the policed rate.

```
(Netgear Switch) (Config)#policy-map policy_vlan in
(Netgear Switch) (Config-policy-map)#class class_vlan
(Netgear Switch) (Config-policy-classmap)#police-simple 1000 64 conform-action
transmit violate-action drop
(Netgear Switch) (Config-policy-classmap)#conform-color class_color
(Netgear Switch) (Config-policy-classmap)#exit
(Netgear Switch) (Config-policy-map)#exit
```

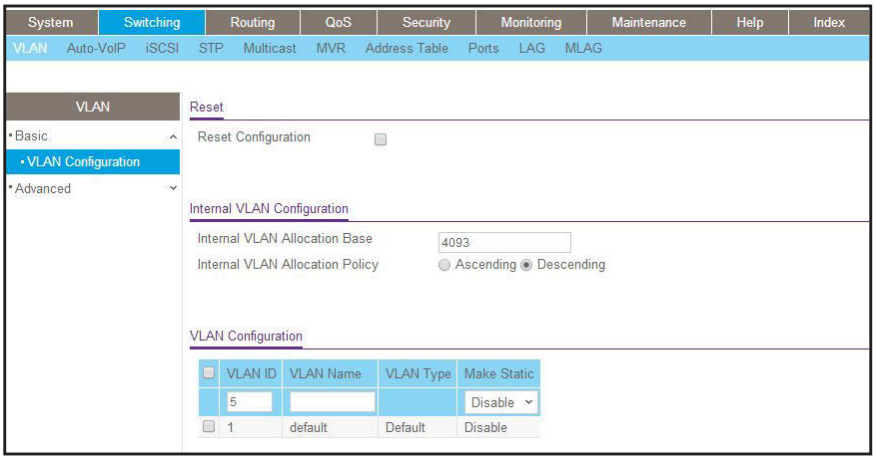
4. Apply this policy to port 1/0/13.

```
(Netgear Switch) (Config)#interface 1/0/13
(Netgear Switch) (Interface 1/0/13)#service-policy in policy_vlan
(Netgear Switch) (Interface 1/0/13)#exit
(Netgear Switch) (Config)#exit
```

Web Interface: Configure a Color Conform Policy

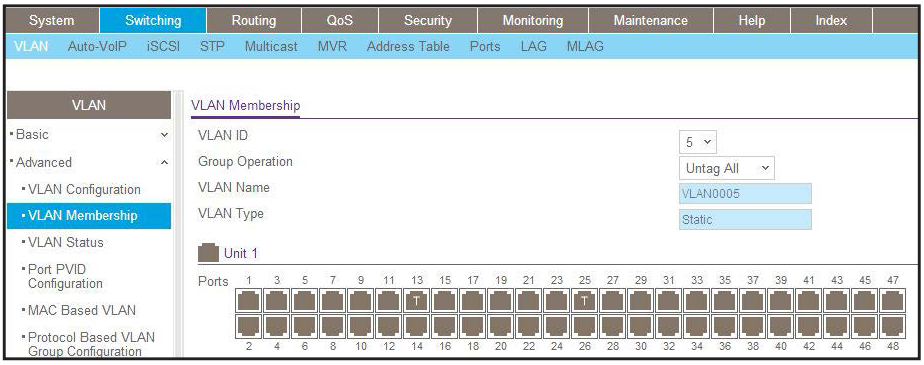
1. Create a VLAN.
   a. Select **Switching > VLAN > Basic > VLAN Configuration**.

      A screen similar to the following displays.



   b. In the **VLAN ID** field, enter **5**.
   c. Click **Add**.
2. Add ports 1/0/13 and 1/0/25 to VLAN 5.
   a. Select **Switching > VLAN > Advanced > VLAN Membership**.

      A screen similar to the following displays.



   b. In the **VLAN ID** list, select **5**.
   c. Click **Unit 1**. The ports display.

d. Click the gray boxes under ports **13** and **25** until **T** displays.

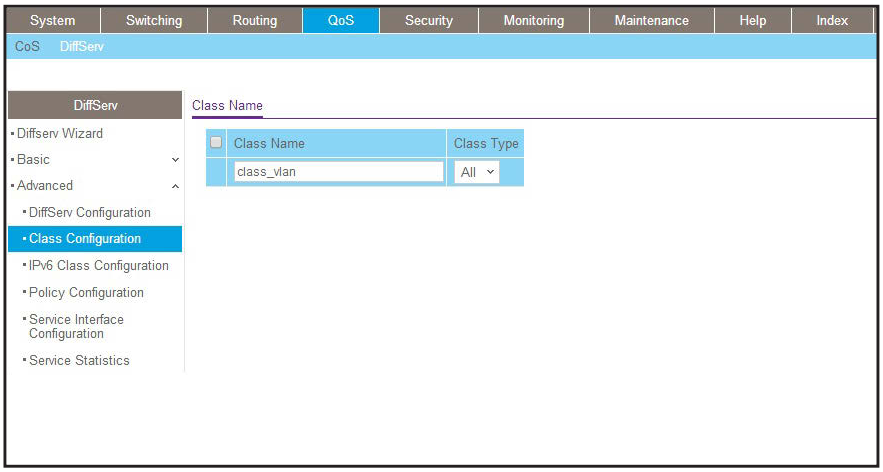
The T specifies that the egress packet is tagged for the port.

e. Click **Apply**.

3. Create a class class_vlan:

a. Select **QoS > DiffServ > Advanced > Class Configuration**.

A screen similar to the following displays.

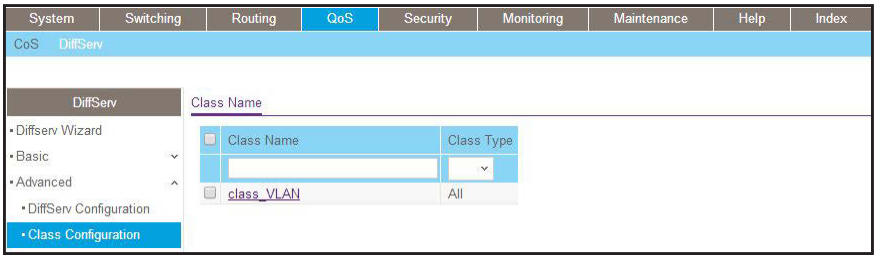


b. Enter the following information:

- In the **Class Name** field, enter **class_vlan**.
- In the **Class Type** list, select **All**.

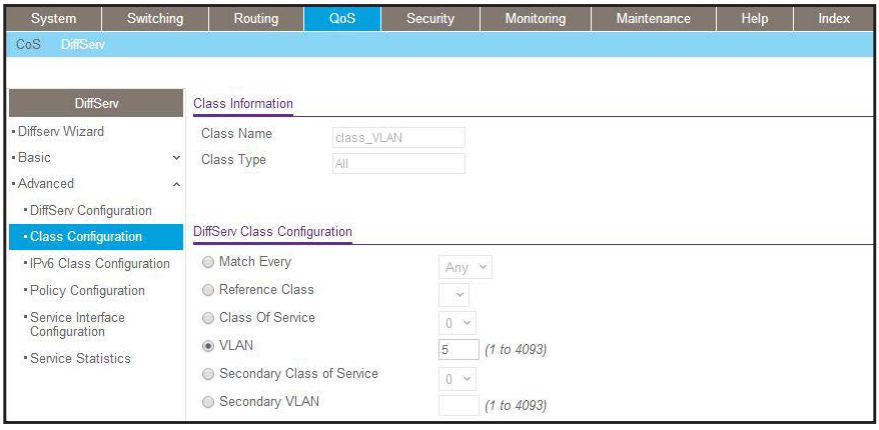
c. Click **Add** to create a new class class_vlan.

A screen similar to the following displays.



d. Click **class_vlan** to configure this class.

A screen similar to the following displays.



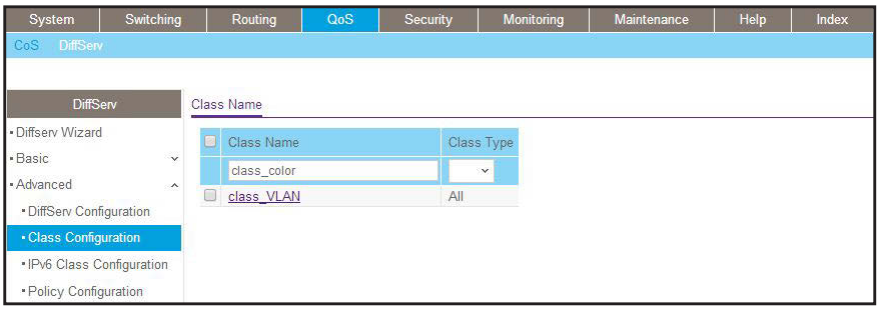
e. Under Diffserv Class Configuration, in the **VLAN** field, enter **5**.

f. Click **Apply**.

4. Create a class class_color.

a. Select **QoS > DiffServ > Advanced > Class Configuration**.

A screen similar to the following displays.

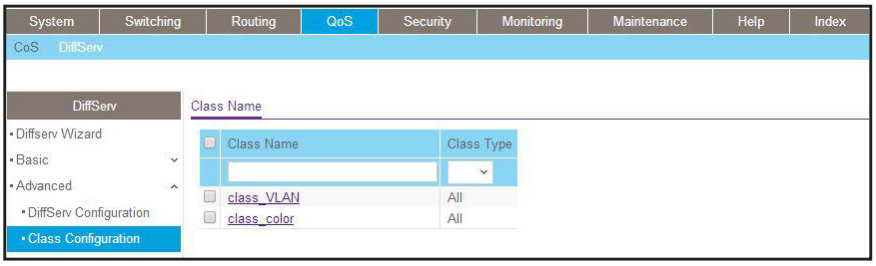


b. Enter the following information:

- In the **Class Name** field, enter **class_color**.
- In the **Class Type** list, select **All**.

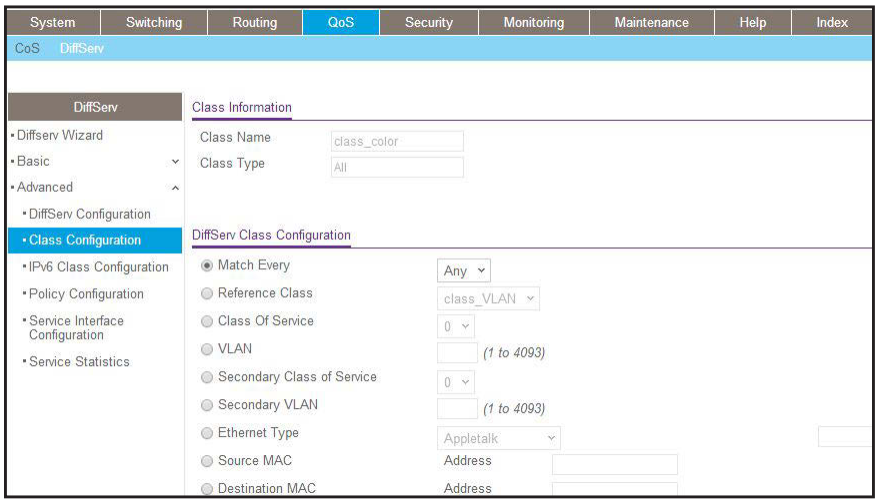
c. Click **Add** to create a new class class_color.

A screen similar to the following displays.



d. Click **class_color** to configure this class.

A screen similar to the following displays.



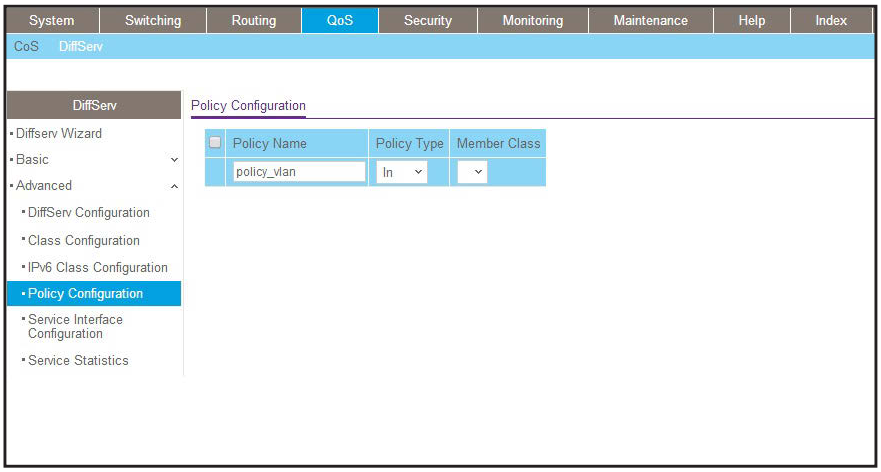
e. Under Diffserv Class Configuration, in the **Precedence Value** list, select **7**.

f. Click **Apply**.

5. Create a policy policy_vlan.

a. Select **QoS > DiffServ > Advanced > Policy Configuration**.

A screen similar to the following displays.



b. In the **Policy Name** field, enter **policy_vlan**.

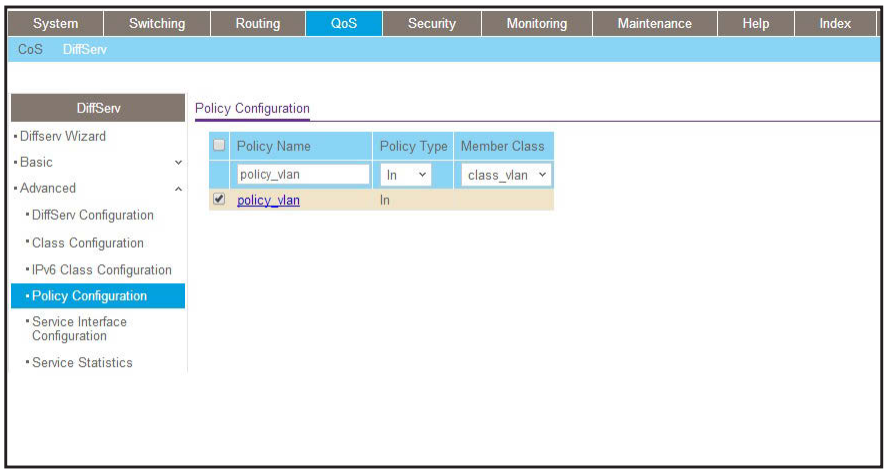
c. In the **Policy Type** list, select **In**.

d. Click **Add**.

6. Associate policy_vlan with class_vlan.

a. Select **QoS > DiffServ > Advanced > Policy Configuration**.

A screen similar to the following displays.



b. Under Policy Configuration, scroll down and select the **policy_vlan** check box.

c. In the **Member Class** field, enter **class_vlan**.

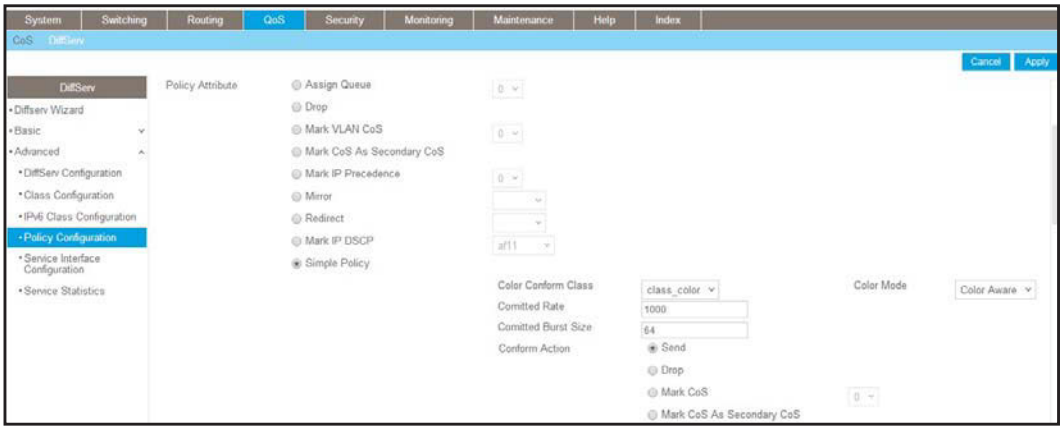
d. Click **Apply**.

7. Configure policy_vlan.

a. Select **QoS > DiffServ > Advanced > Policy Configuration**.

b. Click **policy_vlan**.

A screen similar to the following displays.



c. Select the **Simple Policy** radio button.

d. In the **Color Mode** list, select **Color Aware**.

e. In the **Color Conform Class** list, select **class_color**.

f. In the **Committed Rates** field, enter **1000**.

g. In the **Committed Burst Size** field, enter **64**.

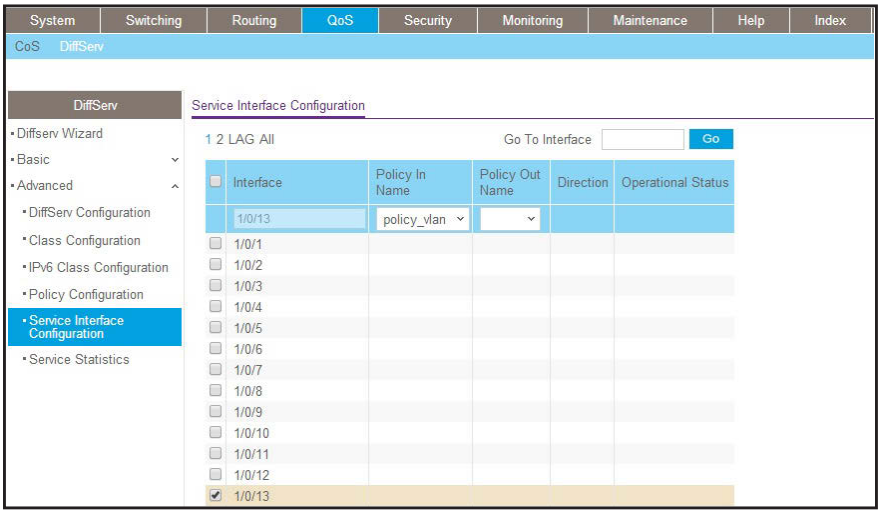
h. For Conform Action, select the **Send** radio button.

i. For Violate Action, select the **Drop** radio button.

j. Click **Apply.**

8. Apply policy_vlan to interface 1/0/13.
   a. Select **QoS > DiffServ > Advanced > Service Interface Configuration**.

      A screen similar to the following displays.



   b. Under Service Interface Configuration, scroll down and select the Interface **1/0/13** check box.
   c. In the **Policy Name** list, select **policy_vlan**.
   d. Click **Apply** to save the settings.

WRED Explicit Congestion Notification

Explicit Congestion Notification (ECN) is defined in RFC 3168. Conventional TCP networks address congestion by dropping packets using the tail drop algorithm. Random early discard (RED, also referred to as random early detection) provides earlier notification than the tail drop algorithm and can drop packets that are already queued for transmission. ECN marks congested packets that would otherwise be dropped and sends a message to the transmitter so that the packets are not retransmitted. That is, the receiver advertises a reduced window size to the transmitter but does not request retransmission of the CE-marked packets.

ECN uses the two least significant bits of the Diffserv field (that is, the ToS octet in IPv4 and the Traffic Class octet in IPv6) and codes them as follows:

- 00. Non ECN-Capable Transport, Non-ECT
- 10. ECN Capable Transport, ECT (0)
- 01. ECN Capable Transport, ECT (1)
- 11. Congestion Encountered, CE

TCP also supports ECN through two flags in the TCP header:

- ECN-Echo (ECE)
- Congestion Window Reduced (CWR)

Weighted random early discard (WRED, also referred to as weighted random early detection) considers packets for early discard only when the number of packets that are queued for transmission on a port exceeds the relevant minimum WRED threshold. The green, yellow, and red thresholds operate on TCP packets. A fourth threshold operates on non-TCP packets.

If ECN is enabled and congestion occurs, ECN-capable TCP packets that are queued for transmission and that are selected to be discarded by WRED are instead CE-marked and transmitted. Packets that exceed the WRED upper threshold are also transmitted. If severe congestion occurs on the switch (that is, no buffers are available), the packets are discarded.

On managed switches, ECN is implemented as part of the WRED configuration process. You can configure any CoS queue to operate in ECN marking mode and you can configure different discard thresholds for each color.

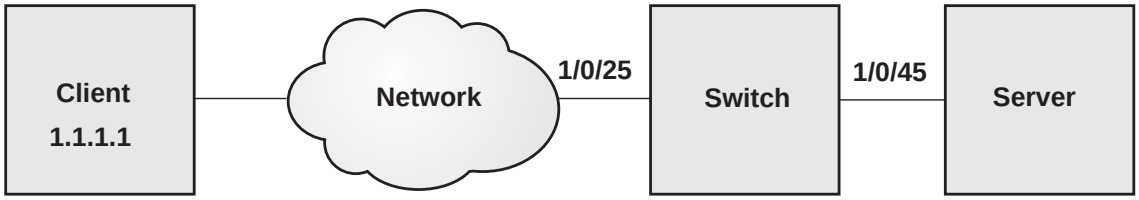


Figure 29. WRED Explicit Congestion Notification configuration

To configure WRED Explicit Congestion Notification configuration:

1. Create class 1 and class 2.

```
(Netgear Switch) (Config)#class-map
(Netgear Switch) (Config)#class-map match-all class1
(Netgear Switch) (Config-classmap)#match srcip 1.1.1.1 255.255.255.255
(Netgear Switch) (Config-classmap)#exit
(Netgear Switch) (Config)#class-map match-all class2
(Netgear Switch) (Config-classmap)#match ip dscp 46
(Netgear Switch) (Config-classmap)#exit
```

2. Create a policy and configure the conform color for class 2.

```
(Netgear Switch) (Config)#policy-map p1 in
(Netgear Switch) (Config-policy-map)#class class1
(Netgear Switch) (Config-policy-classmap)#police-single-rate 1000000 128 128
conform-action transmit exceed-action transmit violate-action transmit
(Netgear Switch) (Config-policy-classmap)#conform-color class2
(Netgear Switch) (Config-policy-classmap)#exit
```

3. Apply the policy on port 1/0/25.

```
(Netgear Switch) (Config)#interface 1/0/25
(Netgear Switch) (Interface 1/0/25)#service-policy in p1
```

4. Let the packets with dot1p priority 3 be placed in queue 3.

```
(Netgear Switch) (Config)#classofservice dot1p-mapping 3 3
(Netgear Switch) #show classofservice dot1p-mapping

 User Priority    Traffic Class
 -------------    -------------
       0                1
       1                0
       2                0
       3                3
       4                2
       5                2
       6                3
       7                3
```

5. Enable WRED on queue 3.

```
(Netgear Switch) (Config)#cos-queue random-detect 3
(Netgear Switch) #show interfaces cos-queue

Global Configuration
Interface Shaping Rate..................... 0
WRED Decay Exponent........................ 9

Queue ID   Min. Bandwidth   Scheduler Type   Queue Management Type
--------   --------------   --------------   ---------------------
0          0                Weighted         Tail Drop
1          0                Weighted         Tail Drop
2          0                Weighted         Tail Drop
3          0                Weighted         WRED
4          0                Weighted         Tail Drop
5          0                Weighted         Tail Drop
6          0                Weighted         Tail Drop
```

6. Configure the queue threshold and enable ECN on queue 3.

```
(Netgear Switch) (Config)#random-detect queue-parms 3 min-thresh 60 20 10 10
max-thresh 100 80 70 60 drop-prob 10 10 10 10 ecn
```

14 IGMP Snooping and Querier

Internet Group Management Protocol features

This chapter includes the following sections:

- *Internet Group Management Protocol Concepts*
- *IGMP Snooping*
- *Show igmpsnooping*
- *Show mac-address-table igmpsnooping*
- *External Multicast Router*
- *Multicast Router Using VLAN*
- *IGMP Querier Concepts*
- *Enable IGMP Querier*
- *Show IGMP Querier Status*

Internet Group Management Protocol Concepts

NETGEAR implements Internet Group Management Protocol (IGMP) in the following way:

- IGMP uses version 1, version 2, or version 3.
- IGMP includes snooping.
- By default, IGMP snooping is enabled on VLAN 1.

IGMP Snooping

The following are examples of the commands used in the IGMP snooping feature.

CLI: EnaP Snooping

The following example shows how to enable IG**ble IGMMP snooping.**

```
(Netgear Switch) #config
(Netgear Switch) (Config)#set igmp
(Netgear Switch) (Config)#exit
```

Web Interface: Enable IGMP Snooping

Configure IGMP snooping:

1. Select **Switching > Multicast > IGMP Snooping Configuration**.

   A screen similar to the following displays.

2. For Admin Mode select the **Enable** radio button.
3. For Unknown Multicast Filtering, select the **Enable** radio button.
4. Click **Apply**.

Show igmpsnooping

The example is shown as CLI commands and as a web interface procedure.

CLI: Show igmpsnooping

```
(Netgear Switch) #show igmpsnooping
Admin Mode..................................... Disable
Multicast Control Frame Count.................. 0
Interfaces Enabled for IGMP Snooping........... None
VLANs enabled for IGMP snooping................ None
```

Web Interface: Show igmpsnooping

Select **Switching > Multicast > IGMP Snooping Configuration**. A screen similar to the following displays.

Show mac-address-table igmpsnooping

The example is shown as CLI commands and as a web interface procedure.

CLI for IGMPv1 and IGMPv2: Show mac-address-table igmpsnooping

```
(Netgear Switch) #show mac-address-table igmpsnooping ?

<cr>                      Press Enter to execute the command.

(Netgear Switch) #show mac-address-table igmpsnooping

                            Type       Description       Interfaces
-----------------------     -------    --------------    -----------
00:01:01:00:5E:00:01:16     Dynamic    Network Assist    Fwd: 1/0/47
00:01:01:00:5E:00:01:18     Dynamic    Network Assist    Fwd: 1/0/47
00:01:01:00:5E:37:96:D0     Dynamic    Network Assist    Fwd: 1/0/47
00:01:01:00:5E:7F:FF:FA     Dynamic    Network Assist    Fwd: 1/0/47
00:01:01:00:5E:7F:FF:FE     Dynamic    Network Assist    Fwd: 1/0/47
```

CLI for IGMPv3: show igmpsnooping ssm entries

```
(Netgear Switch) #show igmpsnooping ssm entries

VLAN                                                Source
ID   Group                  Source Ip               Filter Mode Interfaces

---- ---------------------- ---------------------- ----------- --------------

1000 224.1.1.1              1.1.1.1                 include     1/0/2
```

Web Interface: Show mac-address-table igmpsnooping

Select **Switching > Multicast > IGMP Snooping Table**.

A screen similar to the following displays.

External Multicast Router

The example is shown as CLI commands and as a web interface procedure.

CLI: Configure the Switch with an External Multicast Router

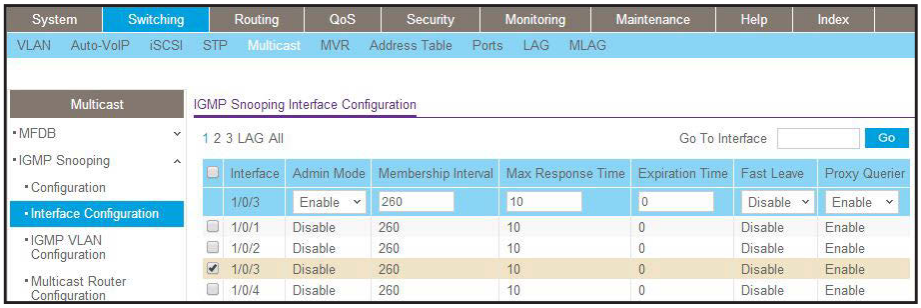
This example configures the interface as the one the multicast router is attached to. All IGMP packets that are snooped by the switch are forwarded to the multicast router that is reachable from this interface.

```
(Netgear Switch)(Interface 1/0/3)# set igmp mrouter interface
```

Web Interface: Configure the Switch with an External Multicast Router

1. Select **Switching > Multicast > Multicast Router Configuration**.

   A screen similar to the following displays.



2. Under Multicast Router Configuration, scroll down and select the Interface **1/0/3** check box.

   Now 1/0/3 appears in the Interface field at the top.

3. In the Admin Mode field, select **Enable**.
4. Click **Apply**.

Multicast Router Using VLAN

The example is shown as CLI commands and as a web interface procedure.

CLI: Configure the Switch with a Multicast Router Using VLAN

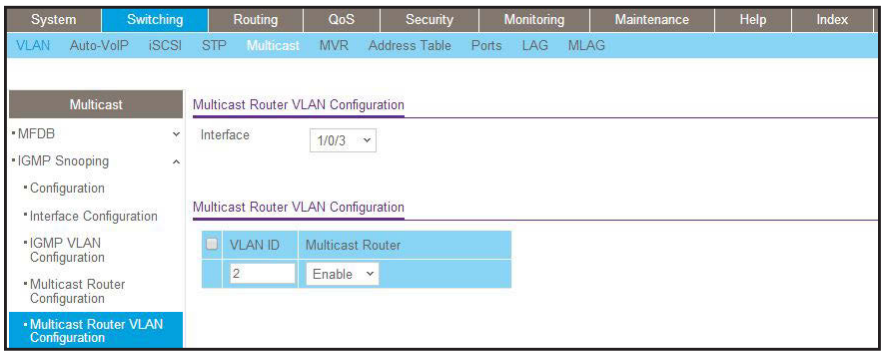
This example configures the interface to forward only the snooped IGMP packets that come from VLAN ID (<VLAN Id>) to the multicast router attached to this interface.

```
(Netgear Switch)(Interface 1/0/3)# set igmp mrouter 2
```

Web Interface: Configure the Switch with a Multicast Router Using VLAN

1. Select **Switching > Multicast > Multicast Router VLAN Configuration**.

   A screen similar to the following displays.



2. Under Multicast Router VLAN Configuration, scroll down and select the Interface **1/0/3** check box.
3. Enter the following information in the Multicast Router VLAN Configuration.
   - In the **VLAN ID** field, enter **2**.
   - In the **Multicast Router** field, select **Enable**.
4. Click **Apply**.

IGMP Querier Concepts

When the switch is used in network applications where video services such as IPTV, video streaming, and gaming are deployed, the video traffic is normally flooded to all connected ports because such traffic packets usually have multicast Ethernet addresses. IGMP snooping can be enabled to create a multicast group to direct that traffic only to those users that require it.

However, the IGMP snooping operation usually requires an extra network device—usually a router—that can generate an IGMP membership query and solicit interested nodes to respond. With the built-in IGMP querier feature inside the switch, such an external device is no longer needed.

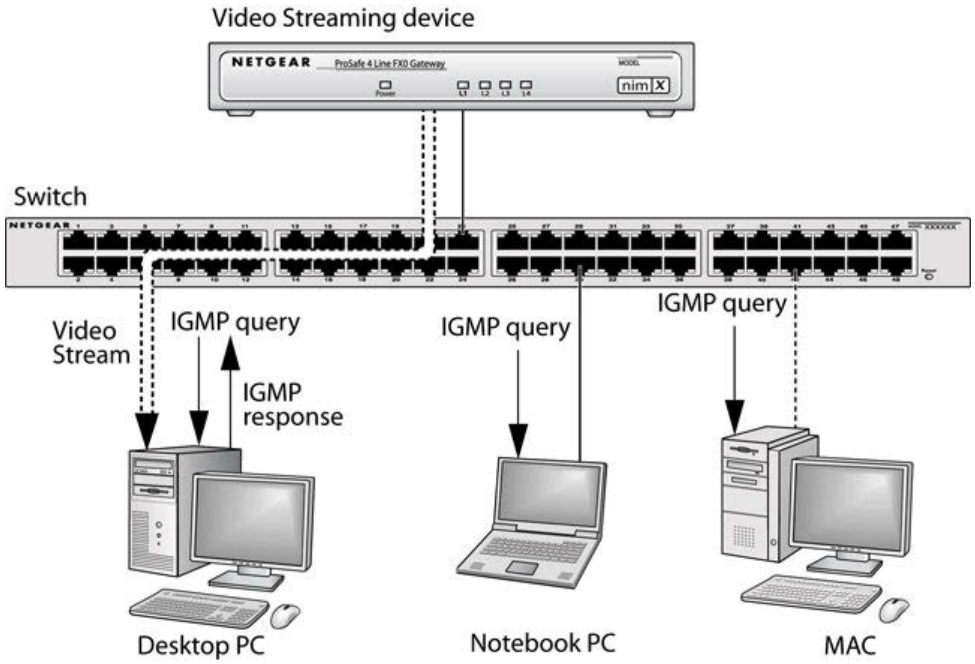


Figure 30. IGMP querier

Since the IGMP querier is designed to work with IGMP snooping, it is necessary to enable IGMP snooping when using it. The following figure shows a network application for video streaming service using the IGMP querier feature.

Enable IGMP Querier

The example is shown as CLI commands and as a web interface procedure.

CLI: Enable IGMP Querier

Use the following CLI commands to set up the switch to generate an IGMP querier packet for a designated VLAN. The IGMP packet will be transmitted to every port on the VLAN. The following example enables the querier for VLAN 1 and uses 10.10.10.1 as the source IP address in querier packets. See the *Command Line Reference* for more details about other IGMP querier command options.

```
(Netgear switch) #vlan database
(Netgear switch) (vlan)#set igmp 1
(Netgear switch) (vlan)#set igmp querier 1
(Netgear switch) (vlan)#exit
(Netgear switch) #config
(Netgear switch) (config)#set igmp querier
(Netgear switch) (config)#set igmp querier address 10.10.10.1
(Netgear switch) (config)#exit
```

Web Interface: Enable IGMP Querier

1. Select **Switching > Multicast > IGMP VLAN Configuration**.

   A screen similar to the following displays.

2. Enable IGMP snooping on VLAN 1.
   a. Select **Switching > Multicast > IGMP Snooping > IGMP VLAN Configuration**.

A screen similar to the following displays.

b. Enter the following information:

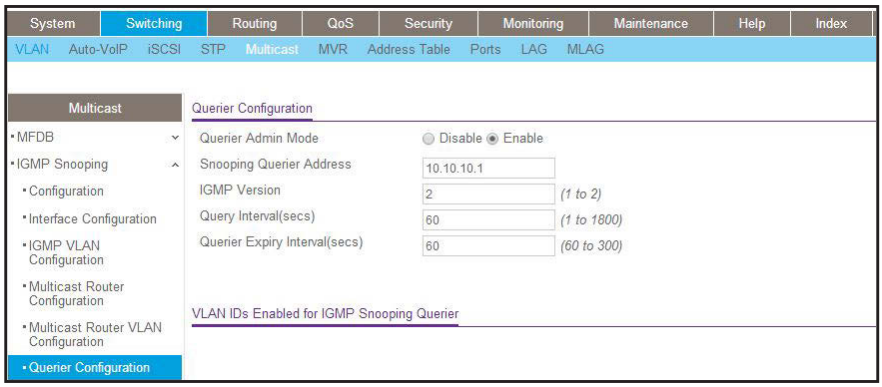
- In the **VLAN ID** field, enter **1**.
- In the **Admin Mode** field, select **Enable**.

c. Click **Add**.

3. Enable the IGMP snooping querier globally.

a. Select **Switching > Multicast > IGMP Snooping > IGMP VLAN Configuration**.

A screen similar to the following displays.



b. Enter the following information:

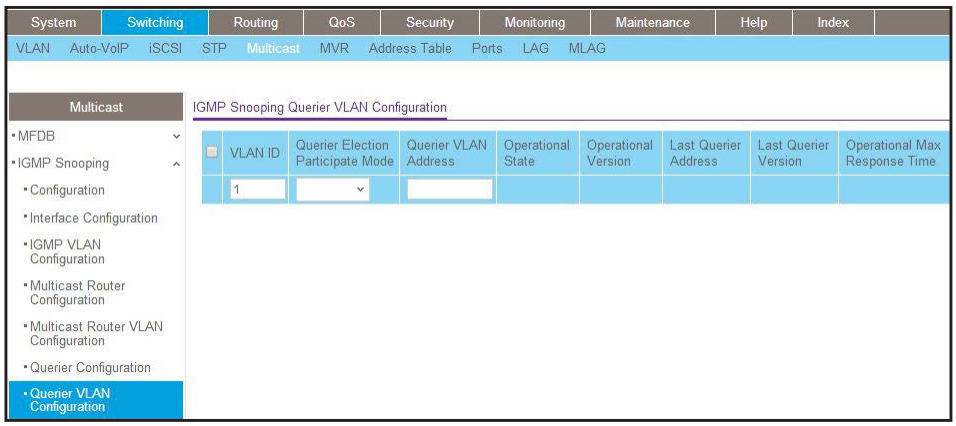
- For Querier Admin Mode, select the **Enable** radio button.
- In the **Querier IP Address** field, enter **10.10.10.1**.

c. Click **Apply**.

4. Enable the IGMP snooping querier on VLAN 1.

a. Select **Switching > Multicast > IGMP Snooping Querier VLAN Configuration**.

A screen similar to the following displays.



b. In the **VLAN ID** field, enter **1**.

5. Click **Add**.

Show IGMP Querier Status

The example is shown as CLI commands and as a web interface procedure.

CLI: Show IGMP Querier Status

To see the IGMP querier status, use the following command.

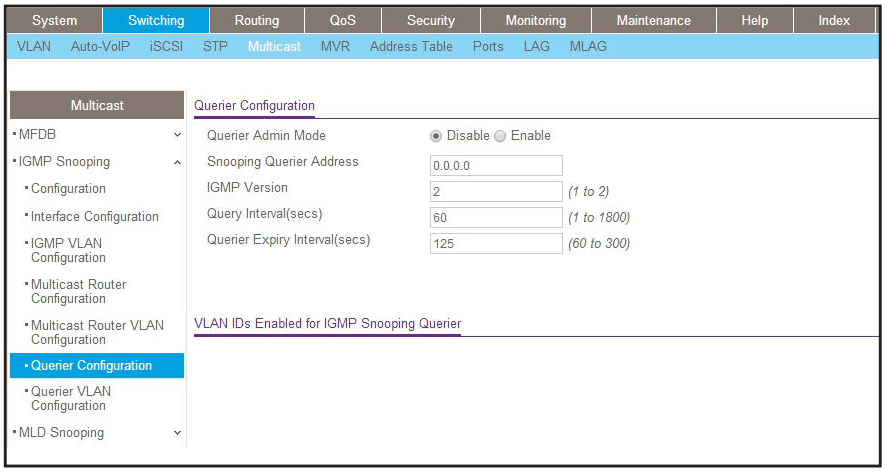
```
(Netgear Switch) #show igmpsnooping querier vlan 1
VLAN 1 : IGMP Snooping querier status
---------------------------------------------
IGMP Snooping Querier VLAN Mode.............. Enable
Querier Election Participate Mode.............. Disable
Querier VLAN Address.......................... 0.0.0.0
Operational State............................. Disabled
Operational version........................... 2
```

The command shows that the IGMP admin mode is Active. The mode is controlled by the **`set igmp`** command. If the mode is inactive, no query packet is sent.

Web Interface: Show IGMP Querier Status

1. Select **Switching > Multicast > IGMP Snooping > Querier Configuration**.

   A screen similar to the following displays.



2. Click **Refresh**.

MVR

15

Multicast VLAN registration

This chapter includes the following sections:

- *Multicast VLAN Registration*
- *Configure MVR in Compatible Mode*
- *Configure MVR in Dynamic Mode*

Multicast VLAN Registration

The IGMP Layer 3 protocol is widely used for IPv4 network multicasting. In Layer 2 networks, the IGMP protocol uses resources inefficiently. For example, a Layer 2 switch multicast traffic to all ports even if there are receivers connected to only a few ports.

To fix this problem, the IGMP snooping protocol was developed. But the problem reappears when receivers are in different VLANs. Multicast VLAN registration (MVR) is intended to solve the problem of receivers in different VLANs. It uses a dedicated manually configured VLAN, called the multicast VLAN, to forward multicast traffic over Layer 2 network in conjunction with IGMP snooping.

MVR, like the IGMP Snooping protocol, allows a Layer 2 switch to snoop on the IGMP control protocol. Both protocols operate independently of each other. Both protocols can be enabled on the switch interfaces at the same time. In such a case, MVR listens to the join and report messages only for groups configured statically. All other groups are managed by IGMP snooping.

There are two types of MVR ports: source and receiver.

- The source port is the port to which the multicast traffic flows using the multicast VLAN.
- The receiver port is the port where a listening host is connected to the switch. It can utilize any (or no) VLAN, except the multicast VLAN. This implies that the MVR switch performs VLAN tag substitution from the multicast VLAN source port to the VLAN tag used by the receiver port.

The multicast VLAN is the VLAN that you configure in the specific network for MVR purposes. The multicast VLAN is used to transfer multicast traffic over the network to avoid duplication of multicast streams for clients in different VLANs. The operator must configure the multicast VLAN manually for all source ports in the network. A diagram of a network configured for MVR is shown in the following illustration. SP is the source port and RP is the receiver port.

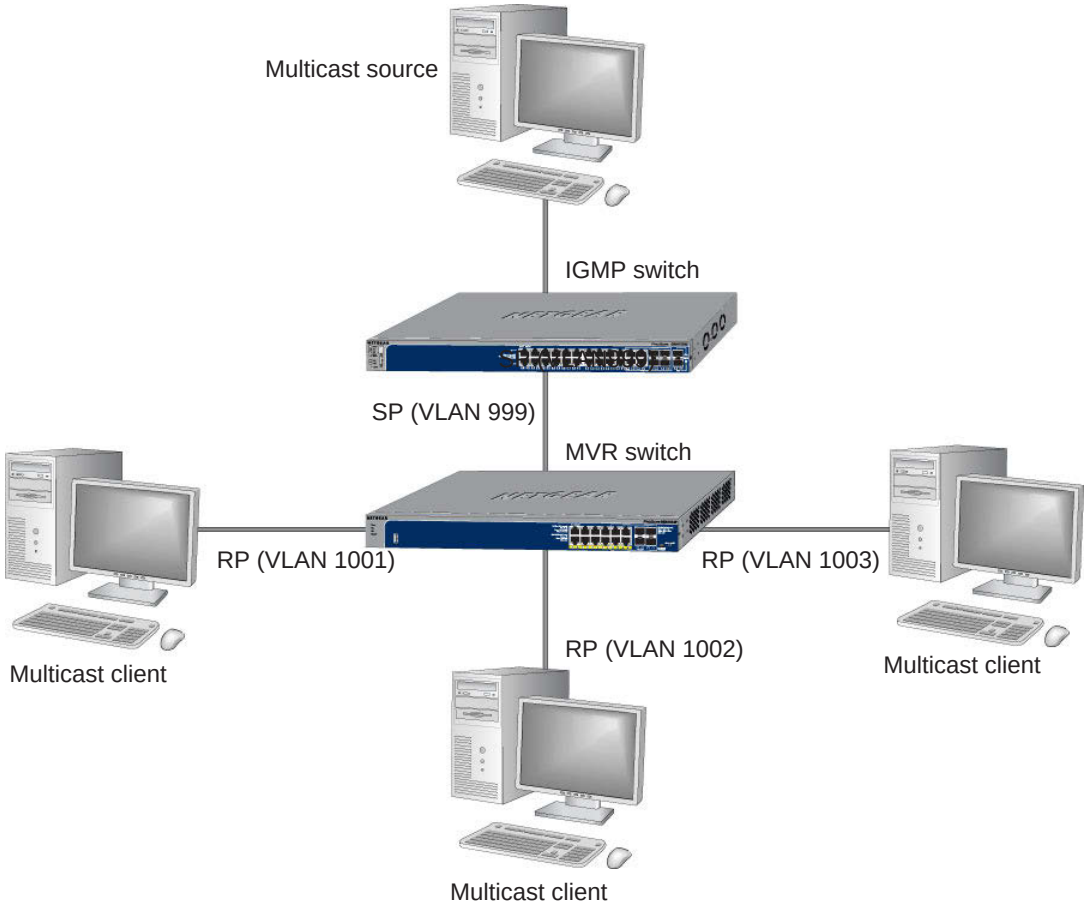


Figure 31. Network configured for MVR

Note: The following examples show how to configure the MVR on the MVR switch.

Configure MVR in Compatible Mode

In compatible mode, the MVR switch does not learn multicast groups; the groups have to be configured by the operator as the MVR does not forward IGMP reports from the hosts (RP port) to the IGMP router (SP port). To operate in this mode, the IGMP router has to be statically configured to transmit all required multicast streams to the MVR switch.

CLI: Configure MVR in Compatible Mode

1. Create MVLAN, VLAN1, VLAN2, and VLAN3.

```
(Netgear Switch) #vlan database
(Netgear Switch) (Vlan)#vlan 999,1001, 1002, 1003
(Netgear Switch) (Vlan)#vlan name 999 mVlan
(Netgear Switch) (Vlan)#vlan name 1001 Vlan1
(Netgear Switch) (Vlan)#vlan name 1002 Vlan2
(Netgear Switch) (Vlan)#vlan name 1003 Vlan3
(Netgear Switch) (Vlan)#exit
```

2. Enable MVR, configure VLAN 999 as a multicast VLAN, and add group 224.1.2.3 to MVR.

```
(Netgear Switch) #config
(Netgear Switch) (Config)#mvr
(Netgear Switch) (Config)#mvr vlan 999
(Netgear Switch) (Config)#mvr group 224.1.2.3
```

3. Configure multicast VLAN on the source port.

```
(Netgear Switch) (Config)#interface 0/9
(Netgear Switch) (Interface 0/9)#vlan participation include 999
(Netgear Switch) (Interface 0/9)#vlan tagging 999
(Netgear Switch) (Interface 0/9)#mvr
(Netgear Switch) (Interface 0/9)#mvr type source
(Netgear Switch) (Interface 0/9)#exit
```

4. Configure the receive ports.

Note: The receive port can participate in only one VLAN.

```
(Netgear Switch) (Config)#interface 0/1
(Netgear Switch) (Interface 0/1)#vlan participation include 1001
(Netgear Switch) (Interface 0/1)#vlan pvid 1001
(Netgear Switch) (Interface 0/1)#vlan participation exclude 1
(Netgear Switch) (Interface 0/1)#mvr
(Netgear Switch) (Interface 0/1)#mvr type receiver
(Netgear Switch) (Interface 0/1)#mvr vlan 999 group 224.1.2.3
(Netgear Switch) (Interface 0/1)#exit

(Netgear Switch) (Config)#interface 0/5
(Netgear Switch) (Interface 0/5)#vlan participation include 1002
(Netgear Switch) (Interface 0/5)#vlan pvid 1002
(Netgear Switch) (Interface 0/5)#vlan participation exclude 1
(Netgear Switch) (Interface 0/5)#mvr
(Netgear Switch) (Interface 0/5)#mvr stype receiver
(Netgear Switch) (Interface 0/5)#mvr vlan 999 group 224.1.2.3
(Netgear Switch) (Interface 0/5)#exit

(Netgear Switch) (Config)#interface 0/7
(Netgear Switch) (Interface 0/7)#vlan participation include1003
(Netgear Switch) (Interface 0/7)#vlan pvid 1003
(Netgear Switch) (Interface 0/7)#vlan participation exclude 1
(Netgear Switch) (Interface 0/7)#mvr
(Netgear Switch) (Interface 0/7)#mvr type receiver
(Netgear Switch) (Interface 0/7)#mvr vlan 999 group 224.1.2.3
(Netgear Switch) (Interface 0/7)#exit
```

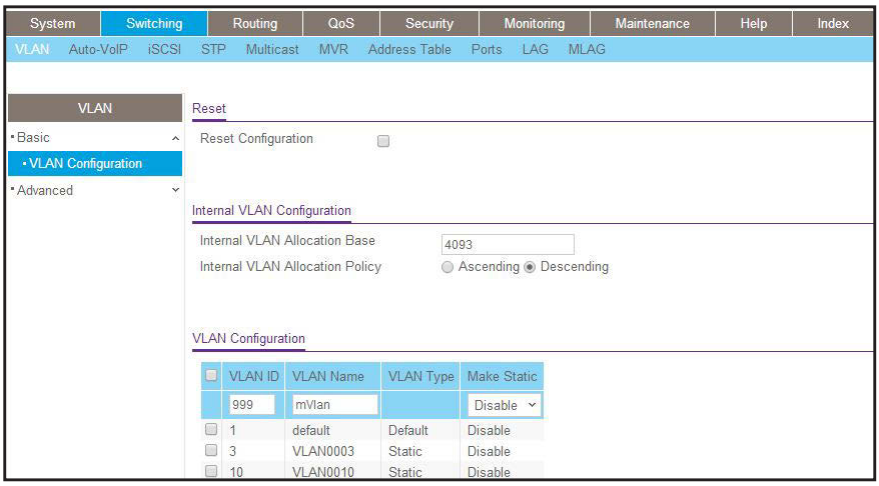
5. Display the MVR status.

```
(Netgear Switch) #show mvr
MVR Running...................... TRUE
MVR multicast VLAN............... 999
MVR Max Multicast Groups......... 256
MVR Current multicast groups..... 1
MVR Global query response time.... 5 (tenths of sec)
MVR Mode......................... compatible
 (Netgear Switch) #show mvr interface
Port         Type               Status                 Immediate Leave
-----------  ---------------    -------------------    ----------
0/1          RECEIVER           ACTIVE/InVLAN          DISABLED
0/5          RECEIVER           ACTIVE/InVLAN          DISABLED
0/7          RECEIVER           ACTIVE/InVLAN          DISABLED
0/9          SOURCE             ACTIVE/InVLAN          DISABLED
```

Web Interface: Configure MVR in Compatible Mode

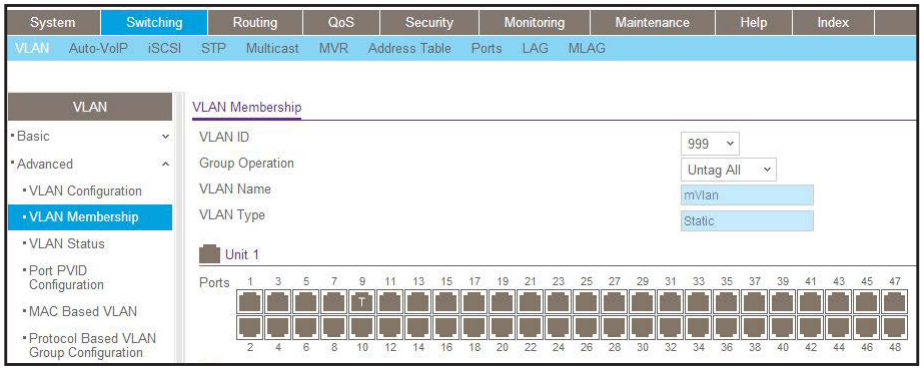
1. Create MVLAN 999, VLAN1 1001, VLAN2 1002 and VLAN3 1003.
   a. Select **Switching > VLAN > Basic > VLAN Configuration**.

      A screen similar to the following displays.



   b. In the VLAN ID field, enter **999**, and in the VLAN Name field, enter **mVlan**.
   c. Click **Add**.
   d. Repeat step b and c to create VLAN1 1001, VLAN2 1002, and VLAN3 1003.
2. Add port 9 into MVLAN 999 with tagged mode.
   a. Select **Switching > VLAN > Advanced > VLAN Membership**.

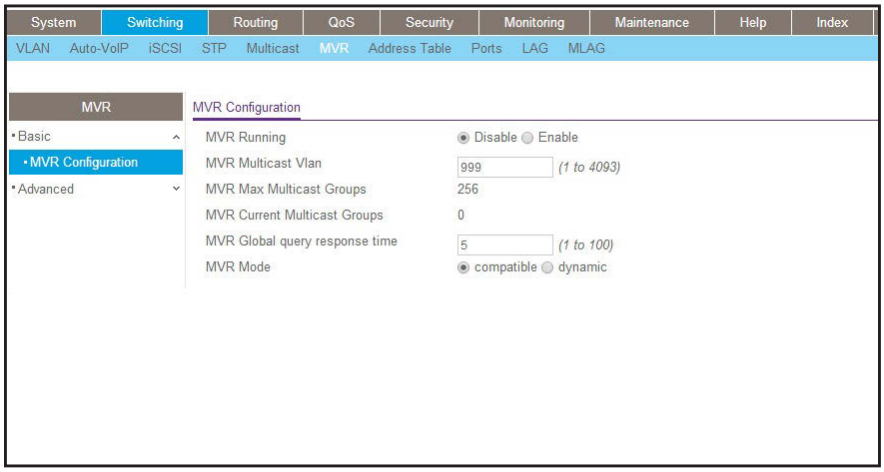
      A screen similar to the following displays.



   b. In the VLAN ID list, select **999**.
   c. Click **Unit 1**. The ports display.
   d. Click the gray box under port 9 until T displays. The T specifies that the egress packet is tagged for the ports.
   e. Click **Apply** to save the settings.
   f. Repeat steps from b to e, add port 0/1 to VLAN1 1001, add port 0/5 to VLAN2 1002, and add port 0/7 to VLAN3 1003.

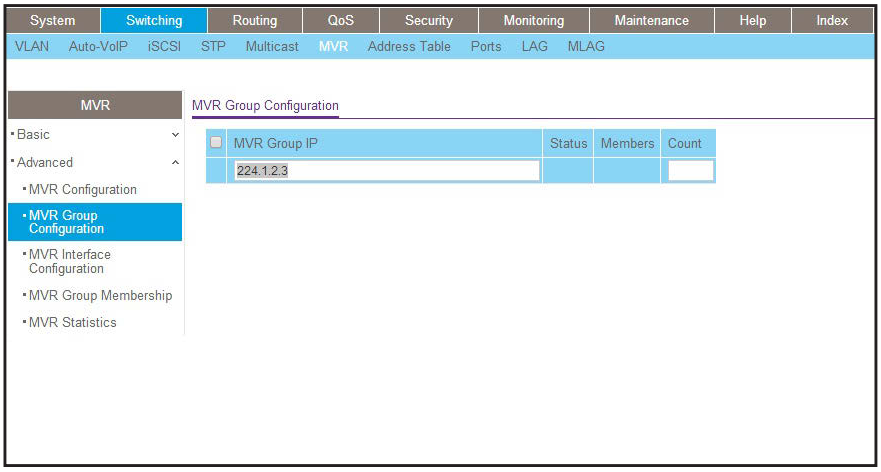
3. Enable MVR and multicast VLAN
   a. Select **Switching > MVR > Basic > MVR Configuration**.

      A screen similar to the following displays.



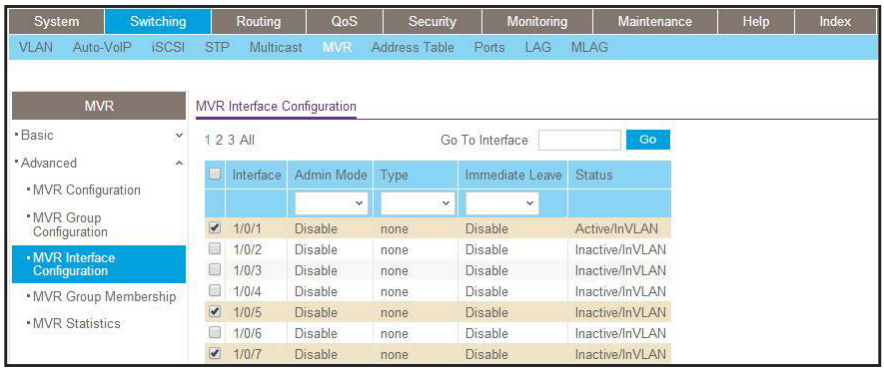
   b. For MVR Running, select **Enable**.
   c. In the MVR Multicast VLAN field, enter **999**.
   d. Click **Apply**.
4. Add multicast group 224.1.2.3 to MVR.
   a. Select **Switching > MVR > Basic > MVR Group Configuration**.

      A screen similar to the following displays.



   b. In the MVR Group IP field, enter **224.1.2.3**.
   c. Click **Add**.
5. Configure a receiver on interface 0/1, 0/5, and 0/7.
   a. Select **Switching > MVR > Basic > MVR Interface Configuration**.

A screen similar to the following displays.



b. Under MVR Interface Configuration, scroll down and select the Interface **0/1**, **0/5** and **0/7** check boxes.

c. Enter the following information:

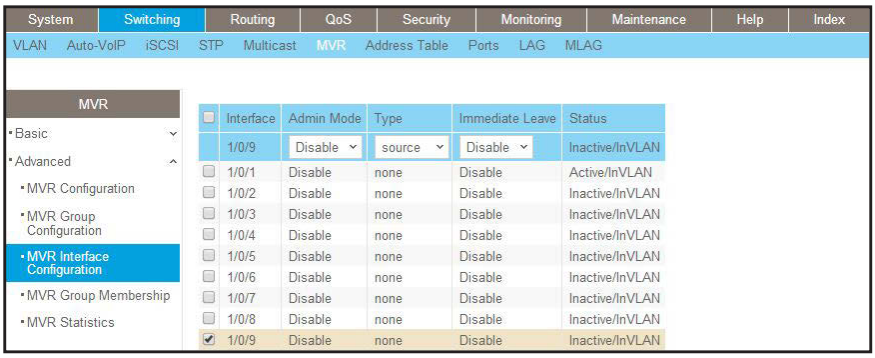
- In the Admin Mode list, select **Enable**.
- In the Type list, select **Receiver**.

d. Click **Apply** to save the settings.

6. Configure source interface.

a. Select **Switching > MVR > Basic > MVR Interface Configuration**.

A screen similar to the following displays.



b. Under MVR Interface Configuration, scroll down and select the Interface **0/9** check box.

c. Enter the following information:

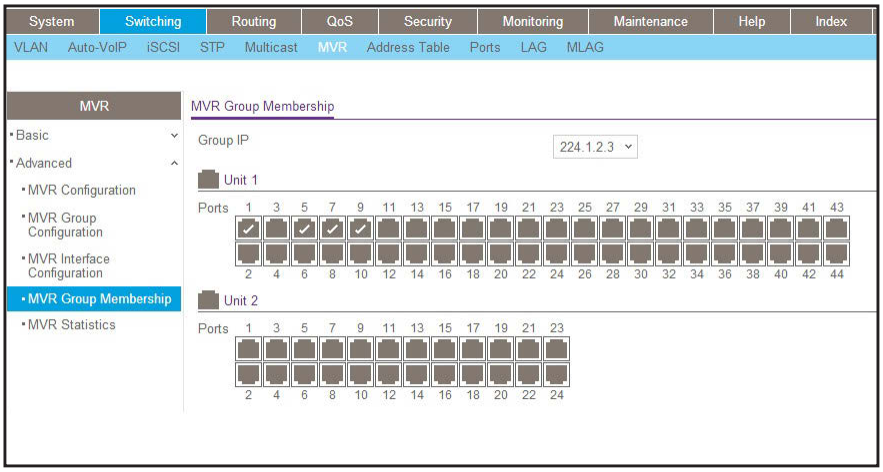
- In the Admin Mode list, select **Enable**.
- In the Type list, select **source**.

d. Click **Apply** to save the settings.

7. Configure MVR Group Membership.

a. Select **Switching > MVR > Advanced > MVR Membership**.

A screen similar to the following displays.



b. In the Group IP list, select **224.1.2.3**.

c. Click **Unit 1**. The ports display.

d. Click the gray boxes under ports **1**, **5**, and **7**. (Port 9 is already in MVR group 224.1.2.3 because it is configured as the source port.)

e. Click **Apply** to save the settings.

Configure MVR in Dynamic Mode

CLI: Configure MVR in Dynamic Mode

In dynamic mode, the MVR switch learns existing multicast groups by snooping the IGMP queries from router on source ports and forwarding the IGMP reports from the hosts to the IGMP router on the Multicast VLAN (with appropriate translation of the VLAN ID).

1. Create MVLAN, VLAN1, VLAN2, and VLAN3.

```
(Netgear Switch) #vlan database
(Netgear Switch) (Vlan)#vlan 999,1001, 1002, 1003
(Netgear Switch) (Vlan)#vlan name 999 mVlan
(Netgear Switch) (Vlan)#vlan name 1001 Vlan1
(Netgear Switch) (Vlan)#vlan name 1002 Vlan2
(Netgear Switch) (Vlan)#vlan name 1003 Vlan3
(Netgear Switch) (Vlan)#exit
```

2. Enable MVR, configure VLAN 999 as a multicast VLAN, and add group 224.1.2.3 to MVR.

```
(Netgear Switch) #config
(Netgear Switch) (Config)#mvr
(Netgear Switch) (Config)#mvr vlan 999
(Netgear Switch) (Config)#mvr group 224.1.2.3
```

3. Configure MVR in dynamic mode.

```
(Netgear Switch) (Config)#mvr mode dynamic
```

4. Configure multicast VLAN on the source port.

```
(Netgear Switch) (Config)#interface 0/9
(Netgear Switch) (Interface 0/9)#vlan participation include 999
(Netgear Switch) (Interface 0/9)#vlan tagging 999
(Netgear Switch) (Interface 0/9)#mvr
(Netgear Switch) (Interface 0/9)#mvr type source
(Netgear Switch) (Interface 0/9)#exit
```

5. Configure the receive ports.

Note: A receive port can participate in only one VLAN.

```
(Netgear Switch) (Config)#interface 0/1
(Netgear Switch) (Interface 0/1)#vlan participation include 1001
(Netgear Switch) (Interface 0/1)#vlan pvid 1001
(Netgear Switch) (Interface 0/1)#vlan participation exclude 1
(Netgear Switch) (Interface 0/5)#mvr
(Netgear Switch) (Interface 0/1)#mvr type receiver
(Netgear Switch) (Interface 0/1)#exit

(Netgear Switch) (Config)#interface 0/5
(Netgear Switch) (Interface 0/5)#vlan participation include 1002
(Netgear Switch) (Interface 0/5)#vlan pvid 1002
(Netgear Switch) (Interface 0/5)#vlan participation exclude 1
(Netgear Switch) (Interface 0/5)#mvr
(Netgear Switch) (Interface 0/5)#mvr stype receiver
(Netgear Switch) (Interface 0/5)#exit

(Netgear Switch) (Config)#interface 0/7
(Netgear Switch) (Interface 0/7)#vlan participation include1003
(Netgear Switch) (Interface 0/7)#vlan pvid 1003
(Netgear Switch) (Interface 0/7)#vlan participation exclude 1
(Netgear Switch) (Interface 0/7)#mvr
(Netgear Switch) (Interface 0/7)#mvr type receiver
(Netgear Switch) (Interface 0/7)#exit
```

6. Show the MVR status.

```
(Netgear Switch) #show mvr
MVR Running...................... TRUE
MVR multicast VLAN............... 999
MVR Max Multicast Groups.......... 256
MVR Current multicast groups...... 1
MVR Global query response time.... 5 (tenths of sec)
MVR Mode......................... compatible
 (Netgear Switch) #show mvr interface
Port         Type               Status                 Immediate Leave
---------    ---------------    -------------------    ---------------
0/1          RECEIVER           ACTIVE/InVLAN          DISABLED
0/5          RECEIVER           ACTIVE/InVLAN          DISABLED
0/7          RECEIVER           ACTIVE/InVLAN          DISABLED
0/9          SOURCE             ACTIVE/InVLAN          DISABLED
```

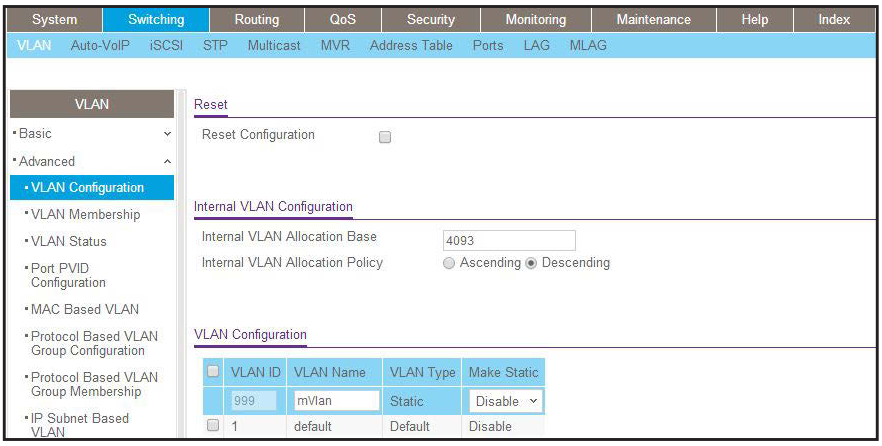
7. After port 0/1 receive IGMP report for Multicast Group 224.1.2.3, it will be added to the MVR Group 224.1.2.3.

```
(Netgear Switch) #show mvr members

MVR Group IP         Status              Members
---------------      --------------      --------------------------------
224.1.2.3            ACTIVE              0/1(d)
```

Web Interface: Configure MVR in Dynamic Mode

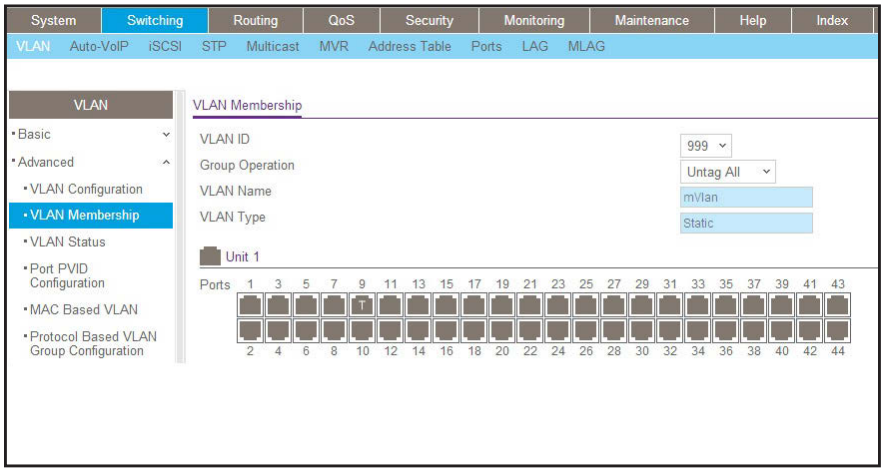
1. Create MVLAN 999, VLAN1 1001, VLAN2 1002, and VLAN3 1003.
   a. Select **Switching > VLAN > Basic > VLAN Configuration**.

      A screen similar to the following displays.



   b. In the VLAN ID field, enter **999**, and in the VLAN Name field, enter **mVlan**.
   c. Click **Add**.
   d. Repeat step b and c to create VLAN1 1001, VLAN2 1002, and VLAN3 1003.
   e. Add port 9 into MVLAN 999 with tagged mode.
   f. Select **Switching > VLAN > Advanced > VLAN Membership**.

A screen similar to the following displays.



g. In the VLAN ID list, select **999**.

h. Click **Unit 1**. The ports display.

i. Click the gray boxes under port **9** until T displays. The T specifies that the egress packet is tagged for the ports.

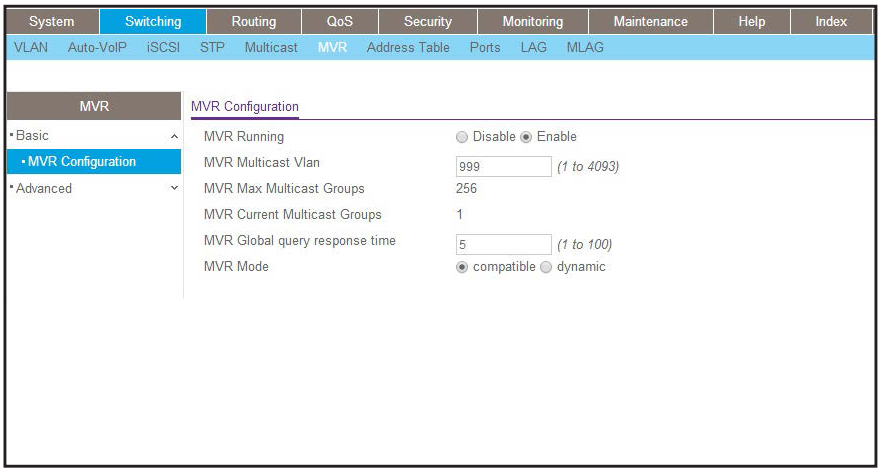
j. Click **Apply** to save the settings.

k. Repeat steps from b to e, add port 0/1 to VLAN1 1001, add port 0/5 to VLAN2 1002, and add port 0/7 to VLAN3 1003.

2. Enable MVR and multicast VLAN.

a. Select **Switching > MVR > Basic > MVR Configuration**.

A screen similar to the following displays.



b. From the MVR Running list, select **Enable**.

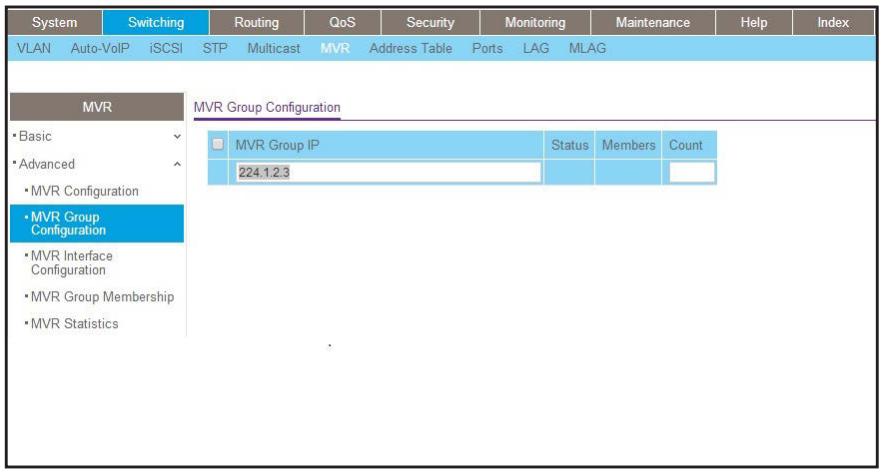
c. In the MVR Multicast Vlan field, enter **999**.

d. From the MVR mode list, select **dynamic**.

e. Click **Apply**.

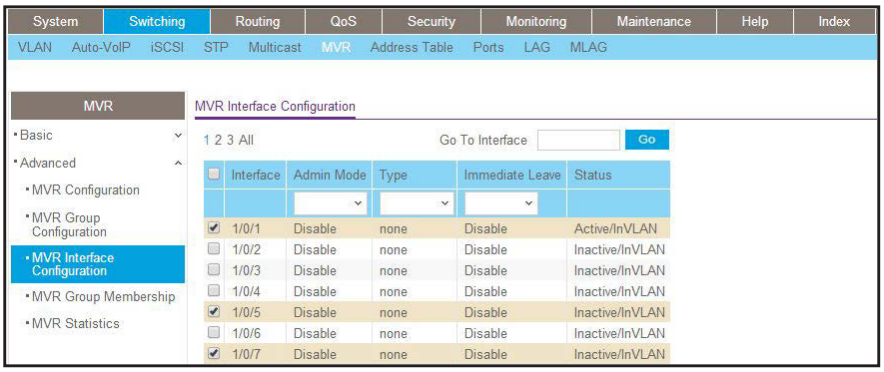
3. Add multicast group 224.1.2.3 to the MVR.
   a. Select **Switching > MVR > Basic > MVR Group Configuration**.

      A screen similar to the following displays.



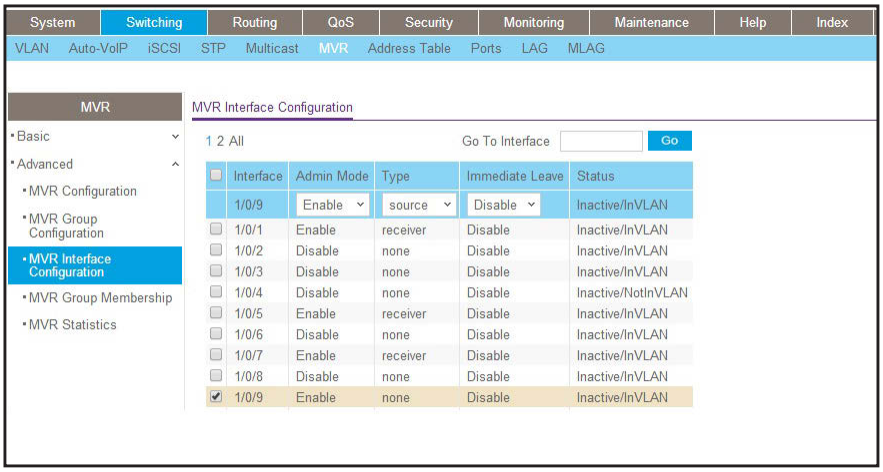
   b. In the MVR Group IP field, enter **224.1.2.3**.
   c. Click **Add**.
4. Configure a receiver on interface 0/1, 0/5 and 0/7.
   a. Select **Switching > MVR > Basic > MVR Interface Configuration**.

      A screen similar to the following displays.



   b. Under MVR Interface Configuration, scroll down and select the Interface **0/1**, **0/5** and **0/7** check boxes
   c. Enter the following information:
      - In the Admin Mode list, select **Enable**.
      - In the Type list, select **Receiver**.
   d. Click **Apply** to save the settings.
5. Configure a source interface.
   a. Select **Switching > MVR > Basic > MVR Interface Configuration**.

A screen similar to the following displays.



b. Under MVR Interface Configuration, scroll down and select the Interface **0/9** check box.

c. Enter the following information:

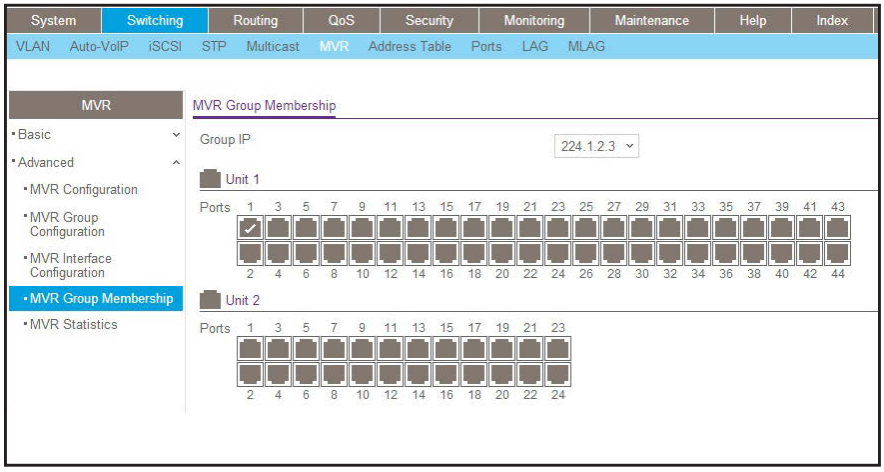
- In the Admin Mode list, select **Enable**.
- In the Type list, select **source**.

d. Click **Apply** to save the settings.

6. After port 1 receives an IGMP report for multicast group 224.1.2.3, it is added into MVR group 224.1.2.3.

a. Select **Switching > MVR > Advanced > MVR Group Membership**.

A screen similar to the following displays.



16 Security Management

Port security features

This chapter includes the following sections:

- *Port Security Concepts*
- *Set the Dynamic and Static Limit on Port 1/0/1*
- *Convert the Dynamic Address Learned from 1/0/1 to a Static Address*
- *Create a Static Address*
- *Protected Ports*
- *802.1x Port Security*
- *Create a Guest VLAN*
- *Assign VLANs Using RADIUS*
- *Dynamic ARP Inspection*
- *Static Mapping*
- *DHCP Snooping*
- *Find a Rogue DHCP Server*
- *Enter Static Binding into the Binding Database*
- *Maximum Rate of DHCP Messages*
- *IP Source Guard*
- *Command Authorization*
- *Privileged Exec Command Mode Authorization*
- *Accounting*
- *Use the Authentication Manager to Set Up an Authentication Method List*
- *RADIUS Change of Authorization*
- *IPv6 Stateless RA Guard*

Port Security Concepts

Port security helps to secure the network by preventing unknown devices from forwarding packets. When a link goes down, all dynamically locked addresses are freed. The port security feature offers the following benefits:

- You can limit the number of MAC addresses on a given port. Packets that have a matching MAC address (secure packets) are forwarded; all other packets (unsecure packets) are restricted.
- You can enable port security on a per port basis.

Port security implements two traffic filtering methods, dynamic locking and static locking. These methods can be used concurrently.

- **Dynamic locking**. You can specify the maximum number of MAC addresses that can be learned on a port. The maximum number of MAC addresses is platform-dependent and is listed in the software release notes. After the limit is reached, additional MAC addresses are not learned. Only frames with allowable source MAC addresses are forwarded.

  Note: If you want to set a specific MAC address for a port, set the dynamic entries to 0, then allow only packets with a MAC address matching the MAC address in the static list.

  Dynamically locked addresses can be converted to statically locked addresses. Dynamically locked MAC addresses are aged out if another packet with that address is not seen within the age-out time. You can set the time-out value. Dynamically locked MAC addresses are eligible to be learned by another port. Static MAC addresses are not eligible for aging.
- **Static locking**. You can manually specify a list of static MAC addresses for a port. Dynamically locked addresses can be converted to statically locked addresses.

Set the Dynamic and Static Limit on Port 1/0/1

The example is shown as CLI commands and as a web interface procedure.

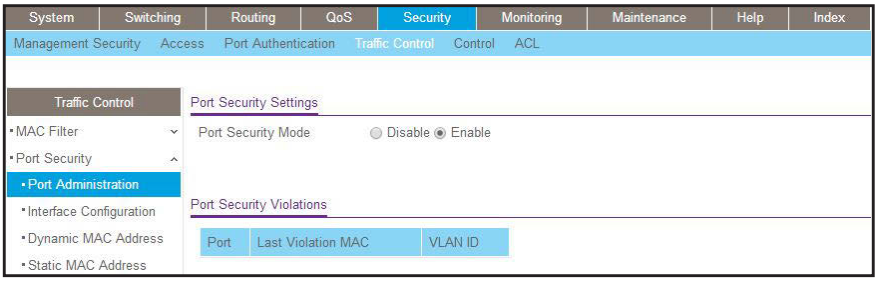
CLI: Set the Dynamic and Static Limit on Port 1/0/1

```
(Netgear Switch) (Config)#port-security
Enable port-security globally
(Netgear Switch) (Config)#interface 1/0/1
(Netgear Switch) (Interface 1/0/1)#port-security
Enable port-security on port 1/0/1
(Netgear Switch) (Interface 1/0/1)#port-security max-dynamic 10
Set the dynamic limit to 10
(Netgear Switch) (Interface 1/0/1)#port-security max-static 3
Set the static limit to 3
(Netgear Switch) (Interface 1/0/1)#ex
(Netgear Switch) (Config)#ex
(Netgear Switch) #show port-security 1/0/1
          Admin        Dynamic          Static         Violation
Intf      Mode         Limit            Limit          Trap Mode
------    -------      ----------       ---------      ----------
1/0/1     Disabled     10               3              Disabled
```

Web Interface: Set the Dynamic and Static Limit on Port 1/0/1

1. Select **Security > Traffic Control > Port Security >Port Administrator**.

   A screen similar to the following displays.



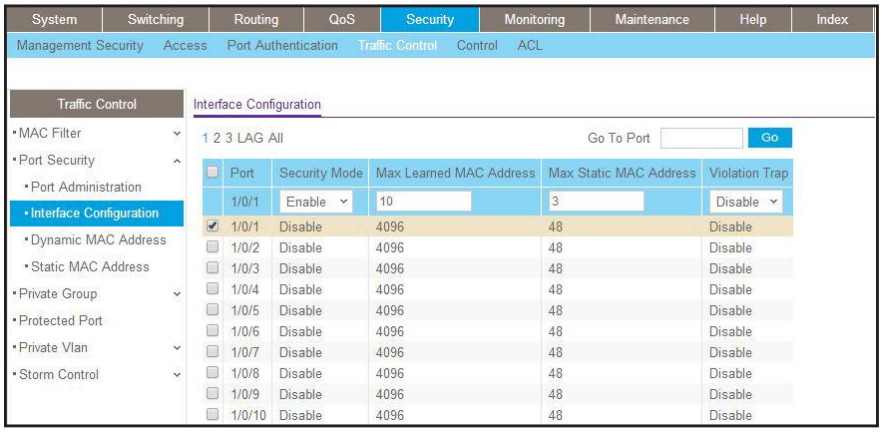
   b. Under Port Security Configuration, next to Port Security Mode, select the **Enable** radio button.

   c. Click **Apply** to save the settings.

2. Set the dynamic and static limit on the port 1/0/1:

   a. Select **Security > Traffic Control > Port Security >Interface Configuration**.

A screen similar to the following displays.



b. Scroll down and select the Interface **1/0/1** check box.

Now 1/0/1 appears in the Interface field at the top.

c. Enter the following information:

- In the **Port Security** field, select **Enable**.
- In the **Max Allowed Dynamically Learned MAC** field, enter **10**.
- In the **Max Allowed Statically Locked MAC** field, enter **3**.

d. Click **Apply** to save the settings.

Convert the Dynamic Address Learned from 1/0/1 to a Static Address

The example is shown as CLI commands and as a web interface procedure.

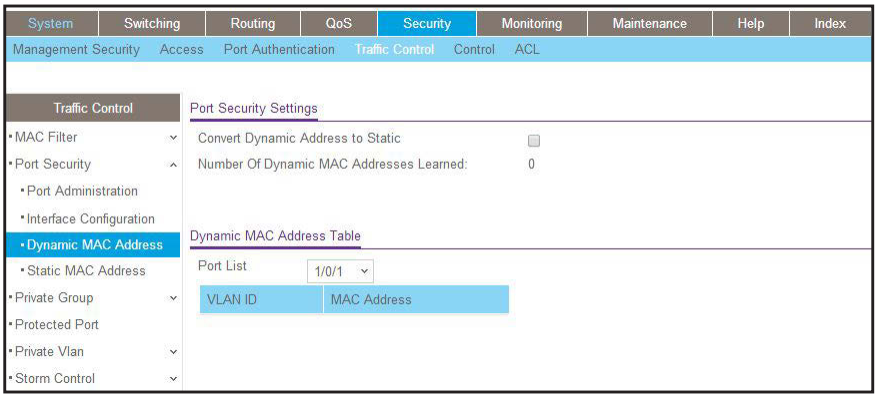
CLI: Convert the Dynamic Address Learned from 1/0/1 to the Static Address

```
(Netgear Switch)(Interface 1/0/1)#port-security mac-address move
Convert the dynamic address learned from 1/0/1 to the static address
(Netgear Switch)(Interface 1/0/1)#exit
(Netgear Switch)(Config)#exit
(Netgear Switch)#show port-security static 1/0/1
 Number of static MAC addresses configured: 3
 Statically configured MAC Address VLAN ID
 ------------------------------------------
 00:0E:45:30:15:F3  1
 00:13:46:EC:2F:62  1
 00:14:6C:E8:81:23  1
```

Web Interface: Convert the Dynamic Address Learned from 1/0/1 to the Static Address

1. Select **Security > Traffic Control > Port Security > Dynamic MAC Address**.

   A screen similar to the following displays.



2. Under Port Security Configuration, in the **Port List** field, select **1/0/1**.
3. Select the **Convert Dynamic Address to Static** check box.
4. Click **Apply** to save the settings.

Create a Static Address

The example is shown as CLI commands and as a web interface procedure.

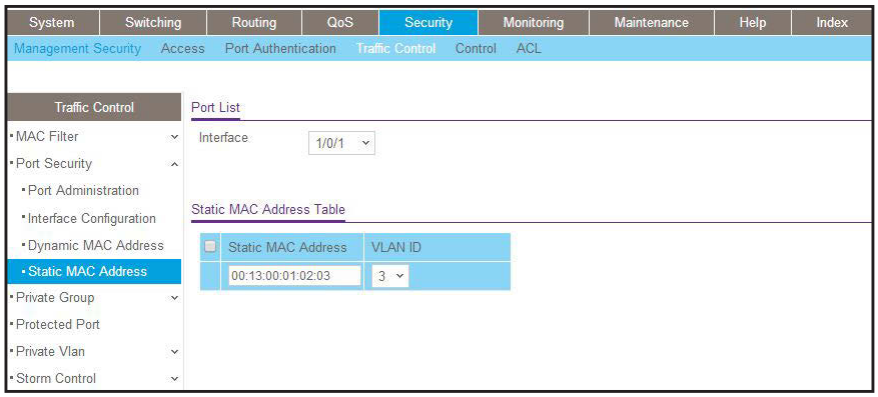
CLI: Create a Static Address

```
(Netgear Switch) (Interface 1/0/1)#port-security mac-address 00:13:00:01:02:03
```

Web Interface: Create a Static Address

1. Select **Security > Traffic Control > Port Security > Static MAC address**.

   A screen similar to the following displays.



2. Under Port List, in the **Interface** list, select **1/0/1**.
3. In the Static MAC Address section of the screen, enter the following information:
   - In the **Static MAC Address** field, enter **00:13:00:01:02:03.**
   - In the **Vlan ID** list, select **3**.
4. Click **Add**.

Protected Ports

This section describes how to set up protected ports on the switch. Some situations might require that traffic is prevented from being forwarded between any ports at Layer 2 so that one user cannot see the traffic of another user on the same switch. Protected ports can:

- Prevent traffic from being forwarded between protected ports.
- Allow traffic to be forwarded between a protected port and a non-protected port.

In following example, PC 1 and PC 2 can access the Internet as usual, but PC 1 cannot see the traffic that is generated by PC 2, that is, no traffic is forwarded between PC 1 and PC 2.

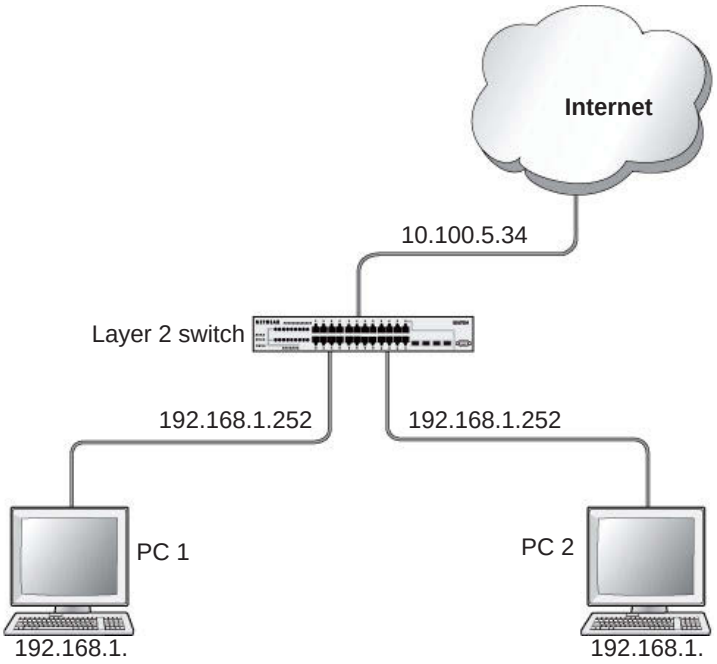


Figure 32. Protected ports

CLI: Configure a Protected Port to Isolate Ports on the Switch

1. Create one VLAN 192 including PC 1 and PC 2.

```
(Netgear Switch) #vlan database
(Netgear Switch) #vlan 192
(Netgear Switch) #vlan routing 192
(Netgear Switch) #exit
(Netgear Switch) #configure
(Netgear Switch) (Config)#interface 1/0/23
(Netgear Switch) (Interface 1/0/23)#vlan pvid 192
(Netgear Switch) (Interface 1/0/23)#vlan participation include 192
(Netgear Switch) (Interface 1/0/23)#exit
(Netgear Switch) (Config)#interface 1/0/24
(Netgear Switch) (Interface 1/0/24)#vlan pvid 192
(Netgear Switch) (Interface 1/0/24)#vlan participation include 192
(Netgear Switch) (Interface 1/0/24)#exit
(Netgear Switch) (Interface-vlan 192)#interface vlan 192
(Netgear Switch) (Interface-vlan 192)#routing
(Netgear Switch) (Interface-vlan 192)#ip address 192.168.1.254 255.255.255.0
(Netgear Switch) (Interface-vlan 192)#exit
```

2. Create one VLAN 202 connected to the Internet.

```
(Netgear Switch) #vlan database
(Netgear Switch) (Vlan)#vlan 202
(Netgear Switch) (Vlan)#vlan routing 202
(Netgear Switch) (Vlan)#exit
(Netgear Switch) #configure
(Netgear Switch) (Config)#interface 1/0/48
(Netgear Switch) (Interface 1/0/48)#vlan pvid 202
(Netgear Switch) (Interface 1/0/48)#vlan participation include 202
(Netgear Switch) (Interface 1/0/48)#exit
(Netgear Switch) (Config)#interface vlan 202
(Netgear Switch) (Interface-vlan 202)#routing
(Netgear Switch) (Interface-vlan 202)ip address 10.100.5.34 255.255.255.0
(Netgear Switch) (Interface-vlan 202)#exit
```

3. Create a DHCP pool to allocated IP addresses to PCs.

```
(Netgear Switch) (config)#service dhcp
(Netgear Switch) (config)#ip dhcp pool pool-a
(Netgear Switch) (Config-dhcp-pool)#dns-server 12.7.210.170
(Netgear Switch) (Config-dhcp-pool)#default-router 192.168.1.254
(Netgear Switch) (Config-dhcp-pool)#network 192.168.1.0 255.255.255.0
(Netgear Switch) (Config-dhcp-pool)#exit
```

4. Enable IP routing and configure a default route.

```
(Netgear Switch)(config)#ip routing
(Netgear Switch)(config)#ip route 0.0.0.0 0.0.0.0 10.100.5.252
```

5. Enable a protected port on 1/0/23 and 1/0/24.

```
(Netgear Switch) (Config)#interface 1/0/23
(Netgear Switch) (Interface 1/0/23)#switchport protected
(Netgear Switch) (Interface 1/0/23)#exit
(Netgear Switch) (Config)#interface 1/0/24
(Netgear Switch) (Interface 1/0/24)#switchport protected
(Netgear Switch) (Interface 1/0/24)#exit
```

Web Interface: Configure a Protected Port to Isolate Ports on the Switch

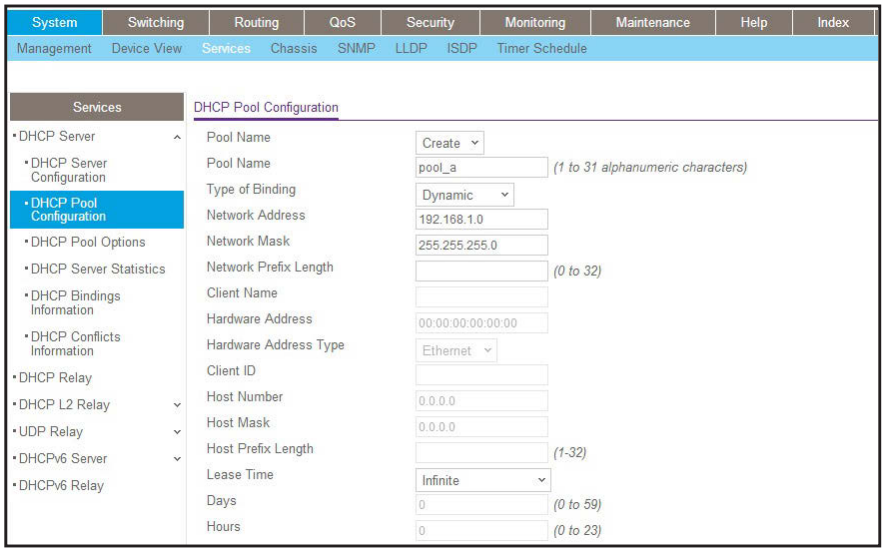
1. Create a DHCP pool:

Note: This example assumes that the DHCP service is enabled. For information about how to enable the DHCP service, see the web interface procedure in *Configure a DHCP Server in Dynamic Mode* on page 466.

---

a. Select **System > Services > DHCP Server > DHCP Server Configuration**.

A screen similar to the following displays.



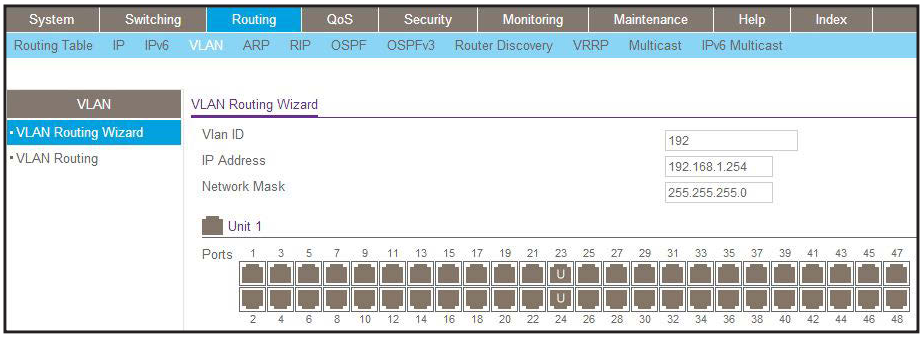
b. Under DHCP Pool Configuration, enter the following information:

- In the **Pool Name** field, select **Create**.
- In the **Pool Name** field, enter **pool-a**.
- In the **Type of Binding** field, select **Dynamic**.
- In the **Network Number** field, enter **192.168.1.0**.
- In the **Network Mask** field, enter **255.255.255.0**.
- In the **Days** field, enter **1**.
- Click **Default Router Addresses**. The DNS server address fields display. In the first **Router Address** field, enter **192.168.1.254**.
- Click **DNS Server Addresses**. The router address fields display. In the first **DNS Server Address** field, enter **12.7.210.170**.

c. Click **Add**.

2. Configure a VLAN and include ports 1/0/23 and 1/0/24 in the VLAN:
   a. Select **Routing > VLAN > VLAN Routing Wizard**.

      A screen similar to the following displays.



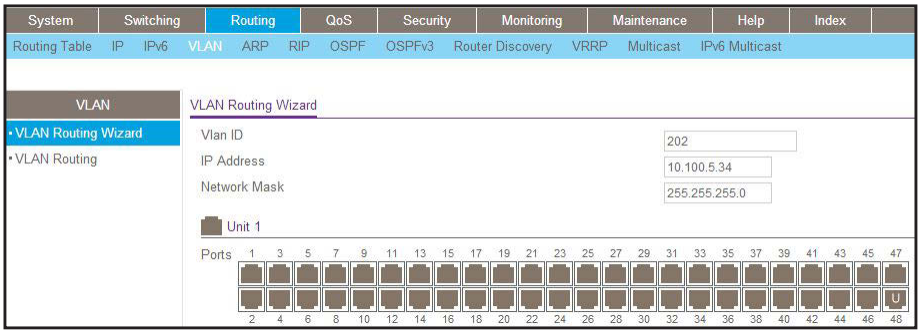
   b. Enter the following information:
      - In the **Vlan ID** field, enter **192**.
      - In the **IP Address** field, enter **192.168.1.254**.
      - In the **Network Mask** field, enter **255.255.255.0**.

   c. Click **Unit 1**. The ports display:
      - Click the gray box under port **23** twice until **U** displays.
      - Click the gray box under port **24** twice until **U** displays.

      The U specifies that the egress packet is untagged for the port.

   d. Click **Apply** to save the VLAN that includes ports 23 and 24.
3. Configure a VLAN and include port 1/0/48 in the VLAN:
   a. Select **Routing > VLAN > VLAN Routing Wizard**.

      A screen similar to the following displays.



   b. Enter the following information:
      - In the **Vlan ID** field, enter **202**.
      - In the **IP Address** field, enter **10.100.5.34**.
      - In the **Network Mask** field, enter **255.255.255.0**.

   c. Click **Unit 1**. The ports display:

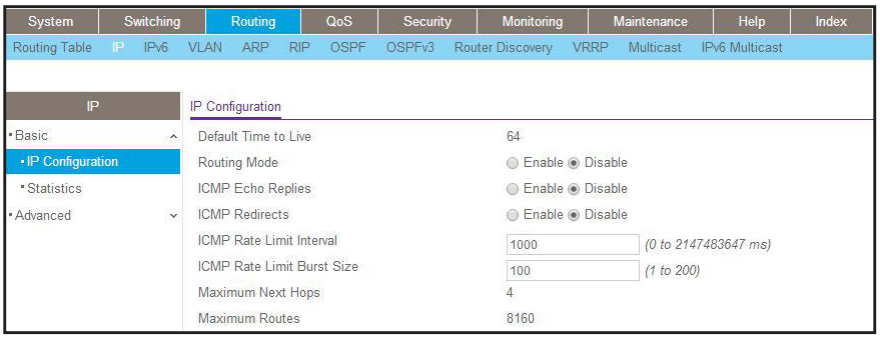
d. Click the gray box under port **48** twice until **U** displays. The U specifies that the egress packet is untagged for the port.

e. Click **Apply** to save the VLAN that includes port 48.

4. Enable IP routing:

a. Select **Routing > IP > Basic > IP Configuration**.

A screen similar to the following displays.



b. Under IP Configuration, make the following selections:

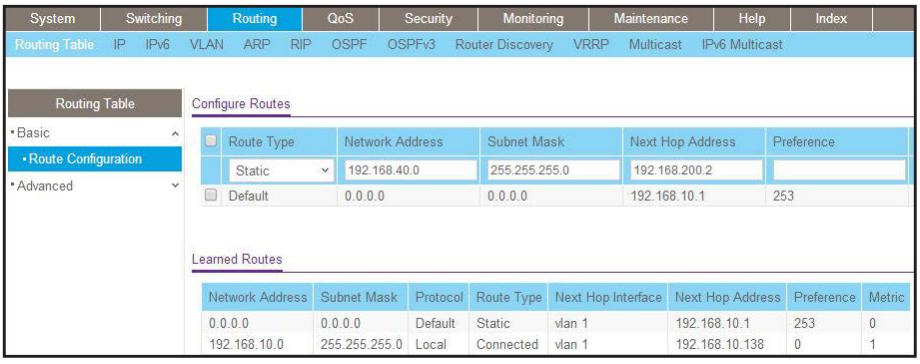
- For Routing Mode, select the **Enable** radio button.
- For IP Forwarding Mode, select the **Enable** radio button.

c. Click **Apply** to enable IP routing.

5. Configure default route for VLAN 202:

a. Select **Routing > Routing Table > Basic > Route Configuration**.

A screen similar to the following displays.



b. Under Configure Routes, in the **Route Type** list, select **Default Route**.

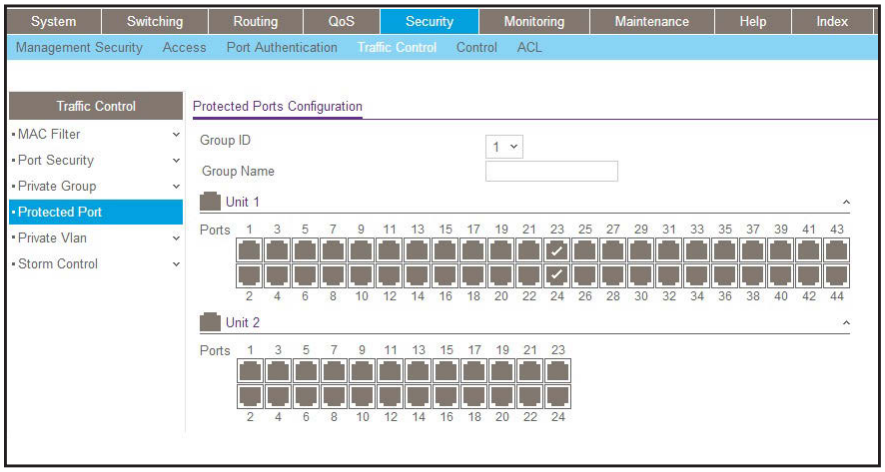
c. In the **Next Hop IP Address** field, enter **10.100.5.252**.

d. Click **Add** to add the route that is associated to VLAN 202 to the Learned Routes table.

6. Configure port 23 and port 24 as protected ports:

a. Select **Security > Traffic Control > Protected Port**.

A screen similar to the following displays.



b. Under Protected Ports Configuration, click **Unit 1**. The ports display.

- Click the gray box under port **23**. A check mark displays in the box.
- Click the gray box under port **24**. A check mark displays in the box.

c. Click **Apply** to activate ports 23 and 24 as protected ports.

802.1x Port Security

This section describes how to configure the 802.1x port security feature on a switch port. IEEE 802.1x authentication prevents unauthorized clients from connecting to a VLAN unless these clients are authorized by the server. 802.1x port security prevents unauthorized clients from connecting to a VLAN. It can be configured on a per-port basis.

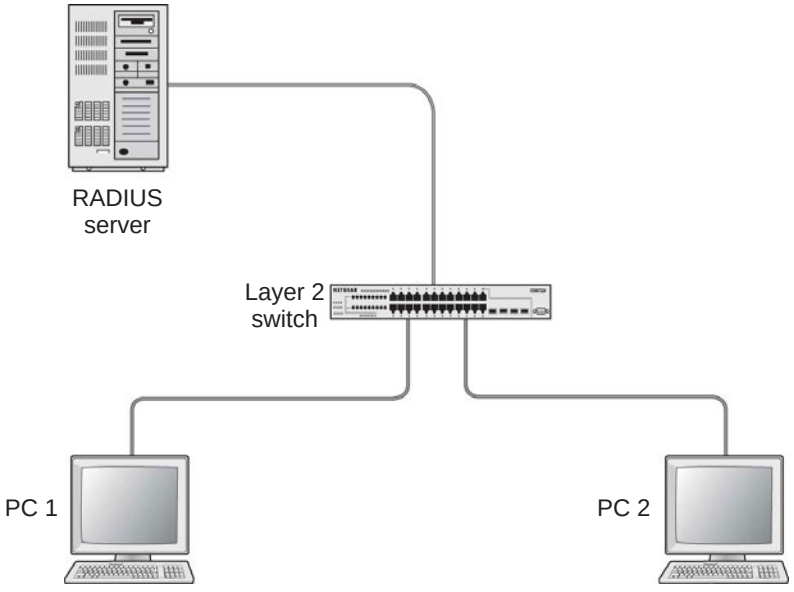


Figure 33. Using 802.1x port security

The following example shows how to authenticate the dot1x users by a RADIUS server. The management IP address is 10.100.5.33/24. The example is shown as CLI commands and as a web interface procedure.

CLI: Authenticating dot1x Users by a RADIUS Server

1. Assign an IP address to 1/0/19, and set force authorized mode to this port, and create a user name list dot1xList.

```
(Netgear Switch) #config
(Netgear Switch) (Config)#ip routing
(Netgear Switch) (Config)#interface 1/0/1
(Netgear Switch) (Interface 1/0/1)#routing
(Netgear Switch) (Interface 1/0/1)#ip address 192.168.1.1 255.255.255.0
(Netgear Switch) (Config)#dot1x system-auth-control
(Netgear Switch) (Config)#interface 1/0/19
(Netgear Switch) (Interface 1/0/19)#routing
(Netgear Switch) (Interface 1/0/19)#ip address 10.100.5.33 255.255.255.0
(Netgear Switch) (Interface 1/0/19)#dot1x port-control force-authorized
```

2. Use RADIUS to authenticate the dot1x users.

```
(Netgear Switch) (Config)#aaa authentication dot1x default radius
```

3. Configure a RADIUS authentication server.

```
(Netgear Switch) (Config)#radius server host auth 10.100.5.17
```

4. Configure the shared secret between the RADIUS client and the server.

```
Netgear Switch) (Config)#radius server key auth 10.100.5.17
Enter secret (16 characters max):123456
Re-enter secret:123456
```

5. Set the RADIUS server as a primary server.

```
(Netgear Switch) (Config)#radius server msgauth 10.100.5.17
(Netgear Switch) (Config)# radius server primary 10.100.5.17
```

6. Configure an accounting server.

```
(Netgear Switch) (Config)#radius accounting mode
(Netgear Switch) (Config)#radius server host acct 10.100.5.17
```

7. Configure the shared secret between the accounting server and the client.

```
(Netgear Switch) (Config)#radius server key acct 10.100.5.17
Enter secret (16 characters max):123456
Re-enter secret:123456
```

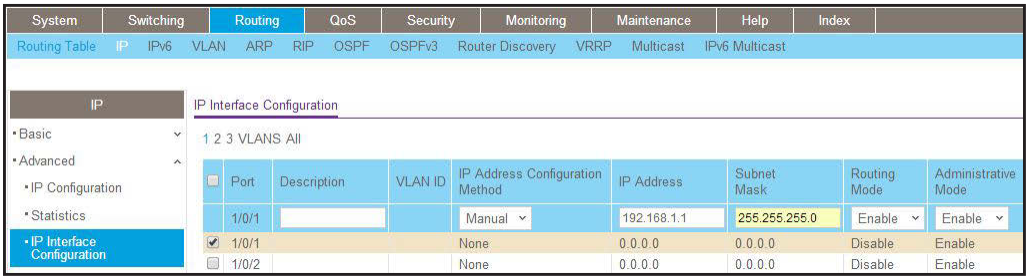
Web Interface: Authenticating dot1x Users by a RADIUS Server

1. Enable routing for the switch.
   a. Select **Routing > Basic > IP Configuration**.

      A screen similar to the following displays.

   b. For Routing Mode, select the **Enable** radio button.
   c. Click **Apply** to save the settings.
2. Assign IP address 192.168.1.1/24 to the interface 1/0/1.
   a. Select **Routing > Advanced > IP Interface Configuration**.

      A screen similar to the following displays.



   b. Under IP Interface Configuration, scroll down and select the Interface **1/0/1** check box.

      Now 1/0/1 appears in the Interface field at the top.

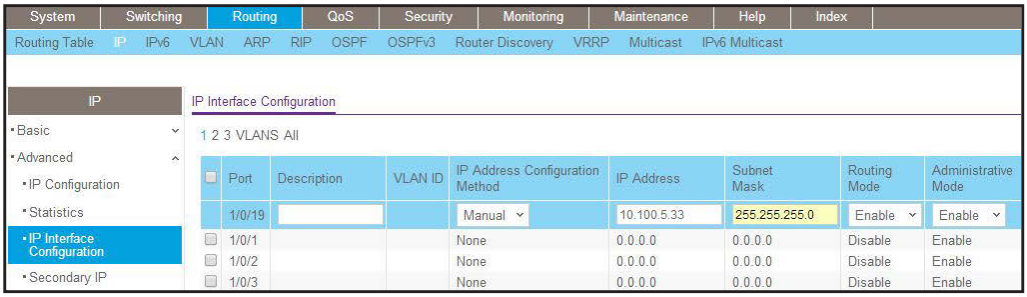
c. Enter the following information:
   - In the **IP Address** field, enter **192.168.1.1**.
   - In the **Subnet Mask** field, enter **255.255.255.0**.
   - In the **Routing Mode** field, select **Enable**.

d. Click **Apply** to save the settings.

3. Assign IP address 10.100.5.33/24 to interface 1/0/19:

a. Select **Routing > Advanced > IP Interface Configuration**.

A screen similar to the following displays.



b. Scroll down and select the interface **1/0/19** check box.

Now 1/0/19 appears in the Interface field at the top.

c. Enter the following information:
   - In the **IP Address** field, enter **10.100.5.33**.
   - In the **Subnet Mask** field, enter **255.255.255.0**.
   - In the **Routing Mode** field, select **Enable**.

d. Click **Apply** to save the settings.

4. Create an authentication name list.

a. Select **Security > Management Security > Login > Authentication List**.

A screen similar to the following displays.

b. Select the check box before **dot1xList**.

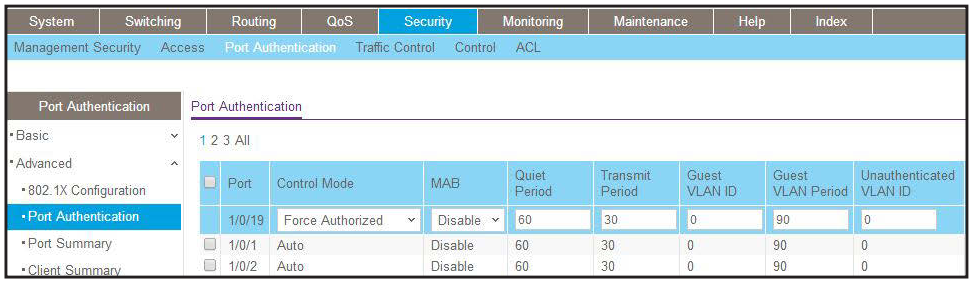
c. In the **1** list, select **Radius**.

d. Click **Apply**.

5. Set port 1/0/19 to force authorized mode. (In this case, the RADIUS server is connected to this interface.)

a. Select **Security > Port Authentication > Advanced > Port Authentication**.

A screen similar to the following displays.



b. Scroll down and select the Interface **1/0/19** check box. Now 1/0/19 appears in the Interface field at the top.

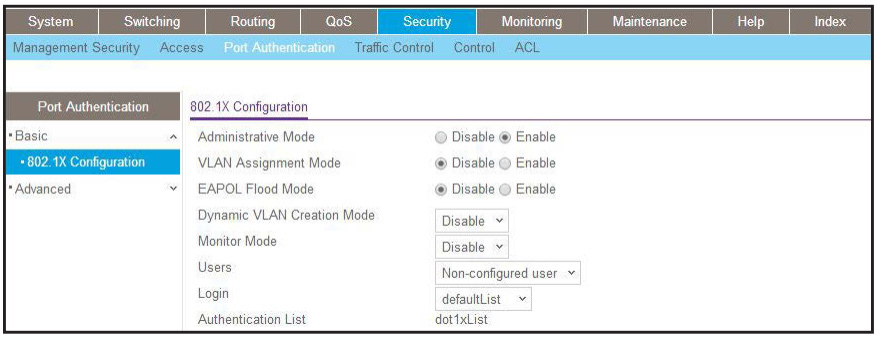
c. In the **Control Mode** list, select **Force Authorized**.

d. Click **Apply** to save the settings.

6. Enable dot1x on the switch.

a. Select **Security > Port Authentication > Server Configuration**.

A screen similar to the following displays.



b. For Administrative Mode, select the **Enable** radio button.

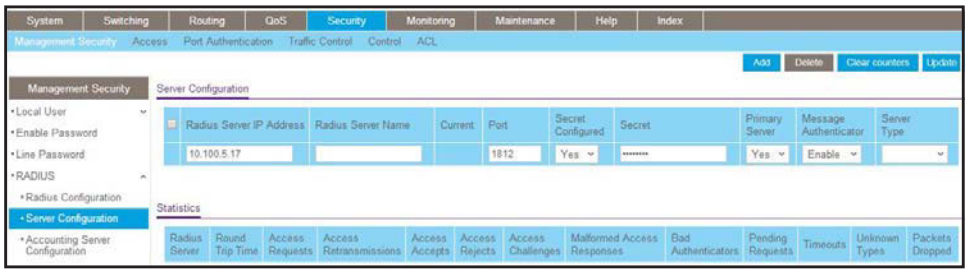
c. In the **Login** list, select **dot1xList**.

d. Click **Apply** to save settings.

7. Configure the RADIUS authentication server.

a. Select **Security > Management Security > Server Configuration**.

A screen similar to the following displays.



b. In the **Server Address** field, enter **10.100.5.17**.

c. In the **Secret Configured** field, select **Yes**.
d. In the **Secret** field, enter **123456**.
e. In the **Primary Server** field, select **Yes**.
f. In the **Message Authenticator** field, select **Enable**.
g. Click **Add**.

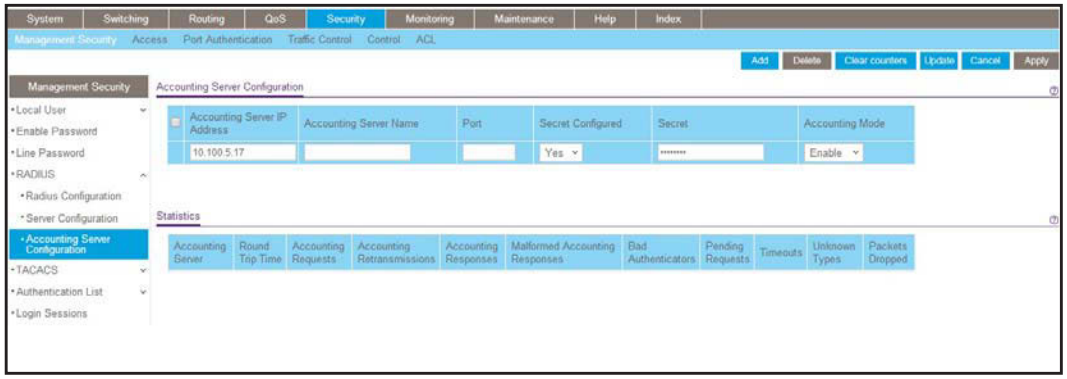
8. Enable accounting.
   a. Select **Security > Management Security > RADIUS > Radius Configuration**.

      A screen similar to the following displays.

   b. In the **Server Address** field, enter **10.100.5.17**.
   c. In the **Accounting Mode** field, select **Enable**.
   d. Click **Apply**.

9. Configure the accounting server.
   a. Select **Security > Management Security > RADIUS > Radius Accounting Server Configuration**.

      A screen similar to the following displays.



   b. In the **Accounting Server Address** field, enter **10.100.5.17**.
   c. In the **Accounting Mode** field, select **Enable**.
   d. Click **Apply**.

Create a Guest VLAN

The guest VLAN feature allows a switch to provide a distinguished service to dot1x unaware clients (not rogue users who fail authentication). This feature provides a mechanism to allow visitors and contractors to have network access to reach an external network with no ability to surf the internal LAN.

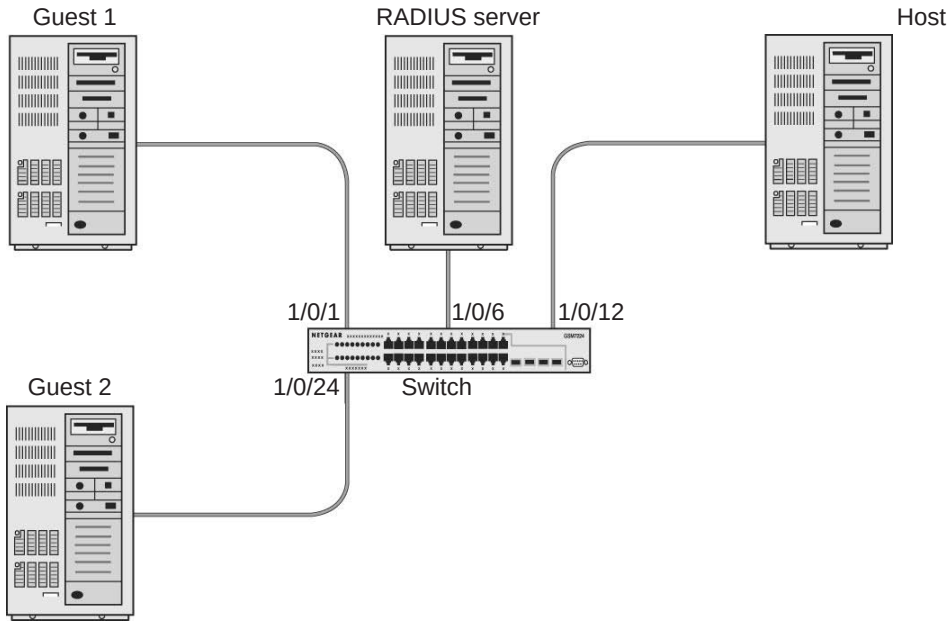


Figure 34. Guest VLAN

If a port is in port-based mode, and a client that does not support 802.1X is connected to an unauthorized port that has 802.1X enabled, the client does not respond to the 802.1X requests from the switch. The port remains in the unauthorized state, and the client is not granted access to the network. If the guest VLAN is configured for that port, then the port is placed in the configured guest VLAN and the port is moved to the authorized state, allowing access to the client after a certain amount of time (determined by the guest VLAN period). If the client attached is 802.1x aware, then this allows the client to respond to 802.1X requests from the switch.

For a port in MAC-based mode, if a guest VLAN has been configured on the port and if traffic from an unauthenticated client is detected on the port, the guest VLAN timer is started for that client. If the client is 802.1x unaware and does not respond to any 802.1x requests, when the guest VLAN timer expires, the client is authenticated and associated with the guest VLAN. This ensures that traffic from the client is accepted and switched through the guest VLAN.

In this example, dot1x is enabled on all the ports so that all the hosts that are authorized are assigned to VLAN 1. On ports 1/0/1 and 1/0/24, guest VLAN is enabled. If guests connect to the port, they are assigned to VLAN 2000, so that guests cannot access the internal VLAN, but can access each other in the guest VLAN.

CLI: Create a Guest VLAN

1. Enter the following commands:

```
(Netgear Switch) #vlan database
(Netgear Switch) (Vlan)#vlan 2000
(Netgear Switch) (Vlan)#exit
(Netgear Switch) (Config)#interface 1/0/1
(Netgear Switch) (Interface 1/0/1)#vlan participation include 2000
(Netgear Switch) (Interface 1/0/1)#exit
(Netgear Switch) (Config)#interface 1/0/24
(Netgear Switch) (Interface 1/0/24)#vlan participation include 2000
(Netgear Switch) (Interface 1/0/24)#exit
```

2. Create VLAN 2000, and have 1/0/1 and 1/0/24 as members of VLAN 2000.

```
(Netgear Switch) (Config)#aaa authentication dot1x default radius
(Netgear Switch) (Config)#dot1x system-auth-control
(Netgear Switch) (Config)#radius server host auth 192.168.0.1
(Netgear Switch) (Config)#radius server key auth 192.168.0.1
Enter secret (16 characters max):12345
Re-enter secret:12345
(Netgear Switch) (Config)#interface 1/0/6
(Netgear Switch) (Interface 1/0/6)#dot1x port-control force-authorized
(Netgear Switch) (Interface 1/0/6)#exit
(Netgear Switch) (Config)#interface 1/0/12
(Netgear Switch) (Interface 1/0/12)#dot1x port-control force-authorized
(Netgear Switch) (Interface 1/0/12)#exit
```

3. Enable dot1x and RADIUS on the switch.

```
(Netgear Switch) (Config)#interface 1/0/1
(Netgear Switch) (Interface 1/0/1)#dot1x guest-vlan 2000
(Netgear Switch) (Interface 1/0/1)#exit
(Netgear Switch) (Config)#interface 1/0/24
(Netgear Switch) (Interface 1/0/24)#dot1x guest-vlan 2000
(Netgear Switch) (Interface 1/0/24)#exit
```

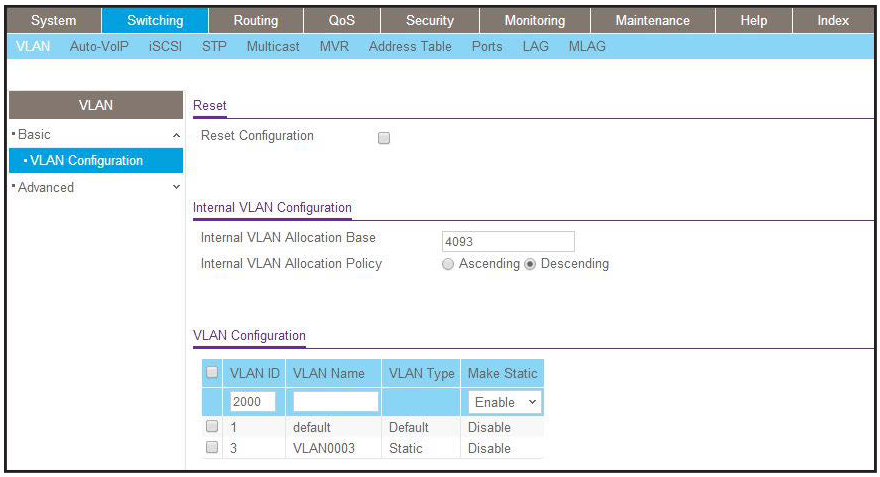
4. Enable the guest VLAN on ports 1/0/1 and 1/0/24.

```
(Netgear Switch) #show dot1x detail 1/0/1
Protocol Version..............................  1
PAE Capabilities..............................  Authenticator
Control Mode..................................  auto
Authenticator PAE State.......................  Authenticated
Backend Authentication State..................  Idle
Quiet Period (secs)...........................  60
Transmit Period (secs)........................  30
Guest VLAN ID.................................  2000
Guest VLAN Period (secs)......................  90
Supplicant Timeout (secs).....................  30
Server Timeout (secs).........................  30
Maximum Requests..............................  2
VLAN Id.......................................  2000
VLAN Assigned Reason..........................  Guest
Reauthentication Period (secs)................  3600
Reauthentication Enabled......................  FALSE
Key Transmission Enabled......................  FALSE
Control Direction.............................  both
Maximum Users.................................  16
Unauthenticated VLAN ID.......................  0
Session Timeout...............................  0
Session Termination Action....................  Default
```

Web Interface: Create a Guest VLAN

1. Create VLAN 2000.
   a. Select **Switching > VLAN > Basic > VLAN Configuration**.

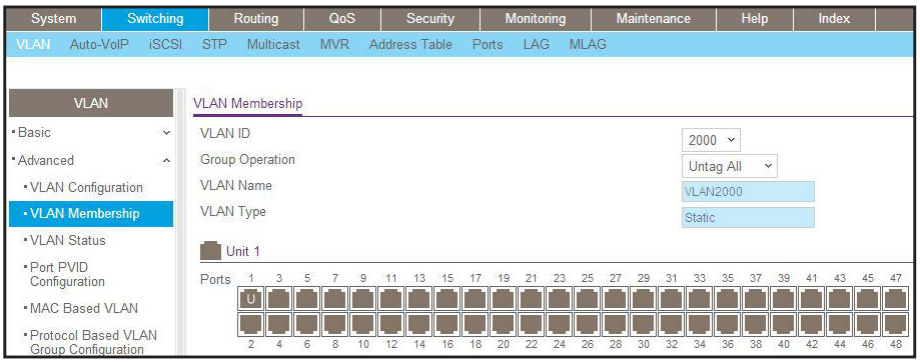
      A screen similar to the following displays.



b. In the **VLAN ID** field, enter **2000**.
c. In the **VLAN Type** field, select **Static**.
d. Click **Add**.

2. Add ports to VLAN 2000.
   a. Select **Switching > VLAN > Advanced > VLAN Membership**.

      A screen similar to the following displays.



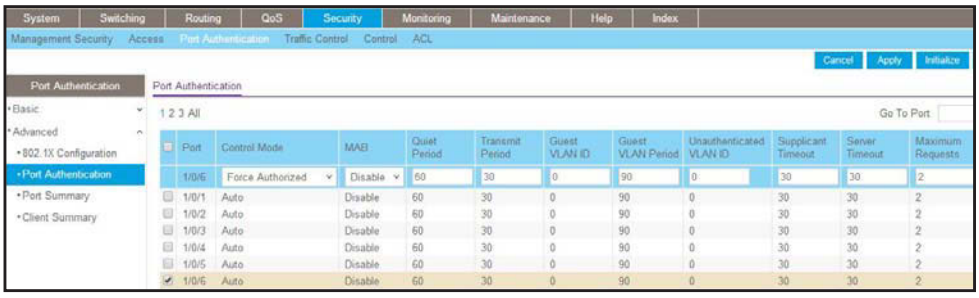
   b. In the **VLAN ID** list, select **2000**.
   c. Click **Unit 1**. The ports display.
   d. Click the gray boxes under ports **1** and **24** until **U** displays.

      The U specifies that the egress packet is untagged for the port.

   e. Click **Apply**.

3. Set force authorized mode on ports 1/0/6 and 1/0/12.
   a. Select **Security > Port Authentication > Advanced > Port Authentication**.

      A screen similar to the following displays.



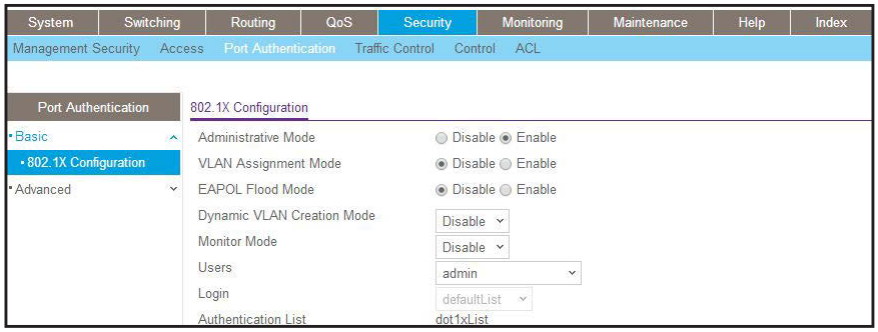
   b. Scroll down and select the Interface **1/0/6** and **1/0/12**, check boxes.
   c. In the **Control Mode** list, select **Force Authorized**.
   d. Click **Apply** to save settings.

4. Enable dot1x on the switch.

   Make sure that 1/0/12 and 1/0/6 are configured as force authorized before you do this step; otherwise you cannot access the switch through the Web Interface.

   a. Select **Security > Port Authentication > Basic > 802.1x Configuration**.

A screen similar to the following displays.



b. For Administrative Mode, select the **Enable** radio button.

c. Click **Apply** to save settings.

5. Configure the dot1x authentication list.

a. Select **Security > Management Security > Authentication List > Dot1x Authentication List**.

A screen similar to the following displays.

b. Select the **defaultList** check box.

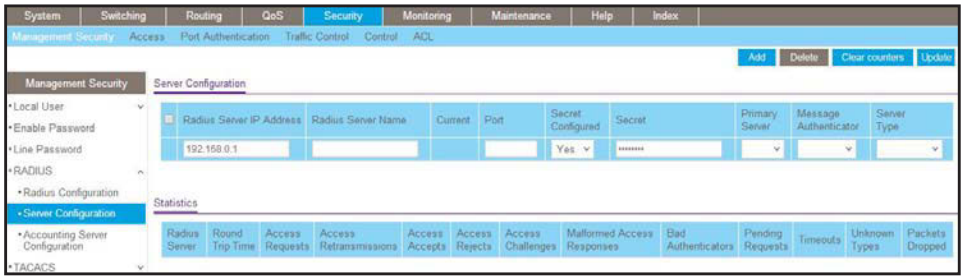
c. In the **1** list, select **RADIUS**.

d. Click **Add**.

6. Configure the RADIUS authentication server.

a. Select **Security > Management Security > Radius > Server Configuration**.

A screen similar to the following displays.



b. In the **Radius Server IP Address** field, enter **192.168.0.1**.

c. In the **Secret Configured** field, select **Yes**.

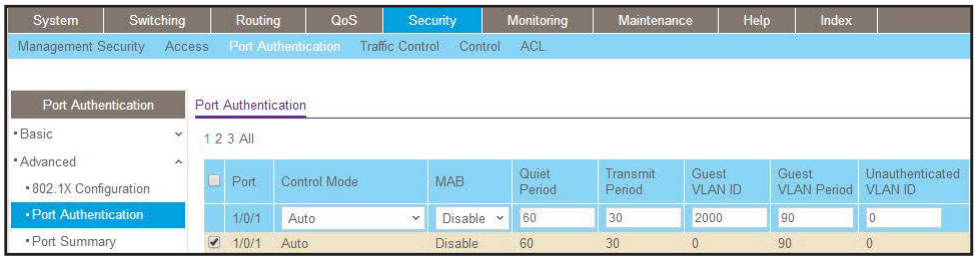
d. In the **Secret** field, enter **12345**.

e. Click **Add**.

7. Configure the guest VLAN.

a. Select **Security > Port Authentication > Advanced > Port Authentication**.

A screen similar to the following displays.



b. Scroll down and select the port 1/0/1 and 1/0/24 check boxes.

c. In the **Guest VLAN ID** field, enter **2000**.

d. Click **Apply** to save your settings.

Assign VLANs Using RADIUS

This feature allows the client to connect from any port and be assigned to the appropriate VLAN assigned by the RADIUS server. This gives flexibility for the clients to move around the network without requiring the administrator to do static VLAN configuration. When multiple hosts are connected to the switch on the same port, only one host uses authentication. If any VLAN information is applied on the port based on the authenticated host, the VLAN applies that information to all the hosts that are connected to that port.

- After a port is in an authorized state, if any client initiates dot1x authentication, the port clears authenticated clients' states, and in the process clears the VLAN assigned to the port (if any). Then the port continues with the new client authentication and authorization process.
- When a client authenticates itself initially on the network, the switch acts as the authenticator to the clients on the network and forwards the authentication request to the RADIUS server in the network.

For use in VLAN assignment, the following tunnel attributes are used:

- Tunnel-Type = VLAN (13)
- Tunnel-Medium-Type = 802
- Tunnel-Private-Group-ID = VLANID where VLANID is 12 bits, with a value between 1 and 4094.

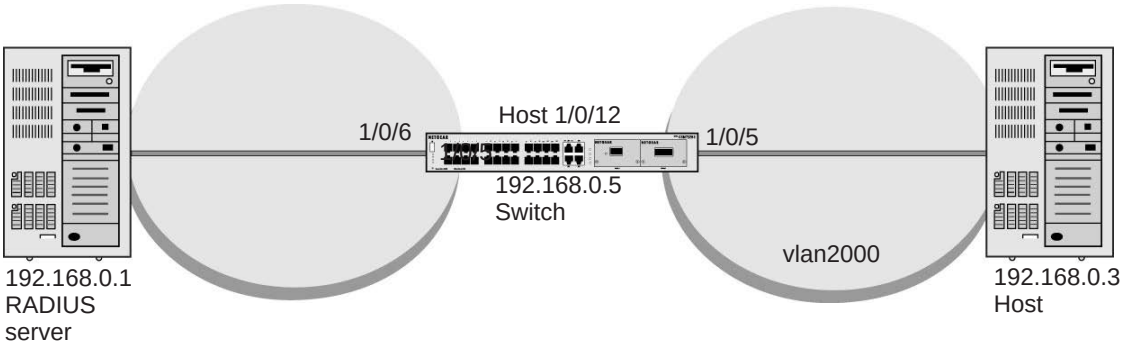


Figure 35. VLAN assignment using RADIUS

In the previous figure, the switch has placed the host in the VLAN (vlan2000) based on the user details of the clients.

The configuration on a RADIUS server for a user logged in as admin is:

- Tunnel-Type = VLAN (13)
- Tunnel-Medium-Type = 802
- Tunnel-Private-Group-ID = 2000

CLI: Assign VLANS Using RADIUS

1. Create VLAN 2000.

```
(Netgear Switch) #network protocol none
Changing protocol mode will reset ip configuration.
Are you sure you want to continue? (y/n) y
(Netgear Switch) #network parms 192.168.0.5 255.255.255.0
(Netgear Switch) #vlan database
(Netgear Switch) (Vlan)#vlan 2000
(Netgear Switch) #exit
```

2. Enable dot1x authentication on the switch

```
(Netgear Switch) (Config)#dot1x system-auth-control
```

3. Use the RADIUS as the authenticator.

```
(Netgear Switch) (Config)#aaa authentication dot1x default radius
```

4. Enable the switch to accept VLAN assignment by the RADIUS server.

```
(Netgear Switch) (Config)#authorization network radius
```

5. Set the RADIUS server IP address.

```
(Netgear Switch) (Config)#radius server host auth 192.168.0.1
```

6. Set the NAS-IP address for the RADIUS server.

```
(Netgear Switch) (Config)#radius server key auth 192.168.0.1
Enter secret (16 characters max):12345
Re-enter secret:12345
Set the radius server key.
(Netgear Switch) (Config)#radius server attribute 4 192.168.0.1
```

7. Force 1/0/6 to be authorized for it to connect to the RADIUS server.

```
(Netgear Switch) (Config)#interface 1/0/6
(Netgear Switch) (Interface 1/0/6)#dot1x port-control force-authorized
(Netgear Switch) (Interface 1/0/6)#exit
```

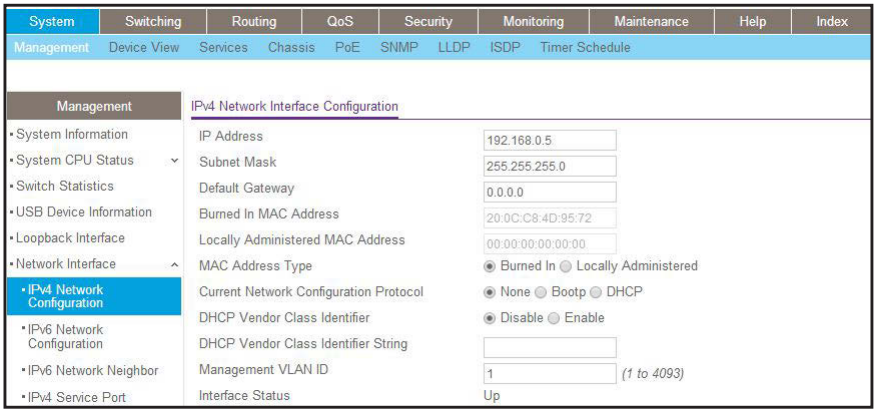
8. Show the dot1x detail for 1/0/5.

```
(Netgear Switch) #show dot1x detail 1/0/5
Port..................................... 1/0/5
Protocol Version......................... 1
PAE Capabilities......................... Authenticator
Control Mode............................. auto
Authenticator PAE State.................. Authenticated
Backend Authentication State............. Idle
Quiet Period (secs)...................... 60
Transmit Period (secs)................... 30
Guest VLAN ID............................ 0
Guest VLAN Period (secs)................. 90
Supplicant Timeout (secs)................ 30
Server Timeout (secs).................... 30
Maximum Requests......................... 2
VLAN Id.................................. 2000
VLAN Assigned Reason..................... RADIUS
Reauthentication Period (secs)........... 3600
Reauthentication Enabled................. FALSE
Key Transmission Enabled................. FALSE
Control Direction........................ both
Maximum Users............................ 16
Unauthenticated VLAN ID.................. 0
Session Timeout.......................... 0
Session Termination Action............... Default
```

Web Interface: Assign VLANS Using RADIUS

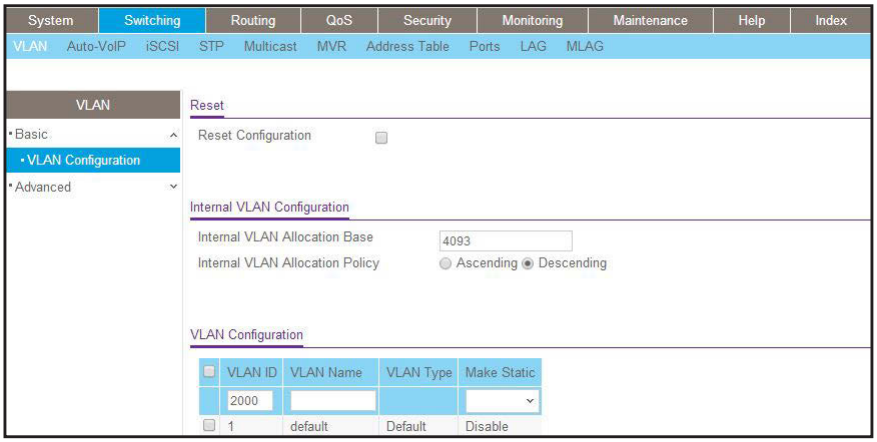
1. Assign the IP address for the web management interface.
   a. Select **System > Management > Network Interface > IPv4 Network Configuration**.

      A screen similar to the following displays.



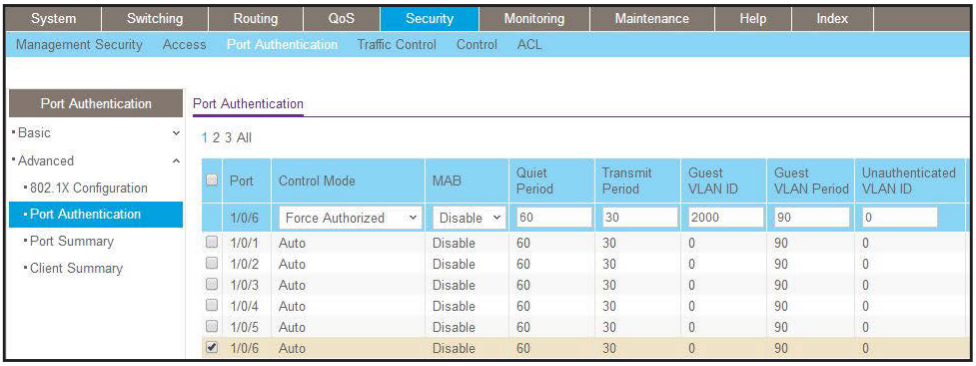
   b. For Current Network Configuration Protocol, select the **None** radio button.
   c. In the **IP Address** field, enter **192.168.0.5**.
   d. In the **Subnet Mask** field, enter **255.255.255.0**.
   e. Click **Apply**.
2. Create VLAN 2000.
   a. Select **Switching > VLAN > Basic > VLAN Configuration**.

      A screen similar to the following displays.



   b. In the **VLAN ID** field, enter **2000**.
   c. In the **VLAN Type** field, select **Static**.
   d. Click **Add**.
3. Set force authorized mode on ports 1/0/6 and 1/0/12.
   a. Select **Security > Port Authentication > Advanced > Port Authentication**.

A screen similar to the following displays.



b. Under Port Authentication, scroll down and select the 1/0/6 and 1/0/12 check boxes.

c. In the **Control Mode** list, select **Force Authorized**.

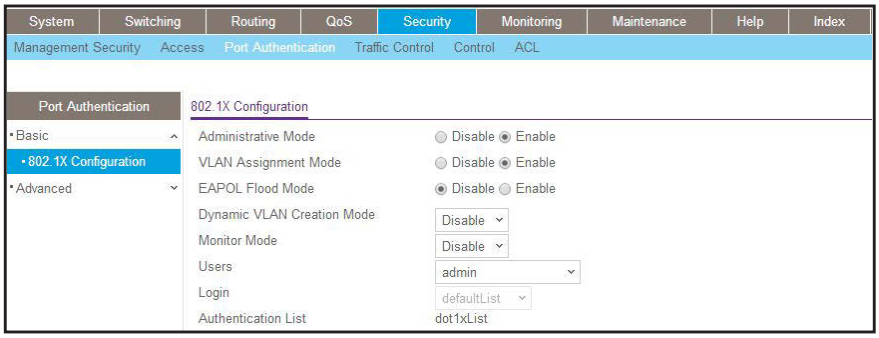
d. Click **Apply** to save settings.

4. Enable dot1x on the switch.

   Make sure that 1/0/12 and 1/0/6 are configured as force authorized before you do this step; otherwise, you cannot access the switch through the web management interface.

   a. Select **Security > Port Authentication > Basic > 802.1x Configuration**.

   A screen similar to the following displays.



   b. For Administrative Mode, select the **Enable** radio button.

   c. For VLAN Assignment Mode, select the **Enable** radio button.

   d. Click **Apply** to save settings.

5. Configure the dot1x authentication list.

   a. Select **Security > Management Security > Authentication List > Dot1x Authentication List**.

A screen similar to the following displays.

b. Select the **defaultList** check box.

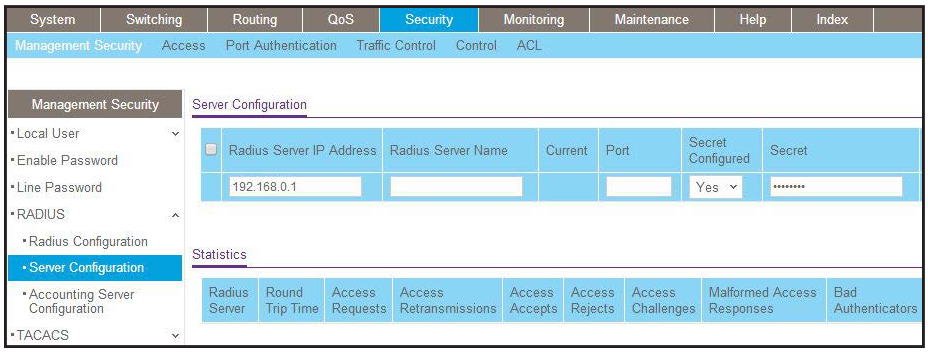
c. In the **1** list, select **RADIUS**.

d. Click **Add**.

6. Configure the RADIUS authentication server.

a. Select **Security > Management Security > Radius > Server Configuration**.

A screen similar to the following displays.



b. In the **Radius Server IP Address** field, enter **192.168.0.1**.

c. In the **Secret Configured** field, select **Yes**.

d. In the **Secret** field, enter **12345**.

e. Click **Add**.

Dynamic ARP Inspection

Dynamic ARP inspection (DAI) is a security feature that rejects invalid and malicious ARP packets. The feature prevents a class of man-in-the-middle attacks, where an unfriendly station intercepts traffic for other stations by poisoning the ARP caches of its unsuspecting neighbors. The miscreant sends ARP requests or responses mapping another station's IP address to its own MAC address.

DAI relies on DHCP snooping. DHCP snooping listens to DHCP message exchanges and builds a bindings database of valid tuples (MAC address, IP address, VLAN interface).

When DAI is enabled, the switch drops ARP packet if the sender MAC address and sender IP address do not match an entry in the DHCP snooping bindings database. However, it can be overcome through static mappings. Static mappings are useful when hosts configure static IP addresses, DHCP snooping cannot be run, or other switches in the network do not run dynamic ARP inspection. A static mapping associates an IP address to a MAC address on a VLAN.

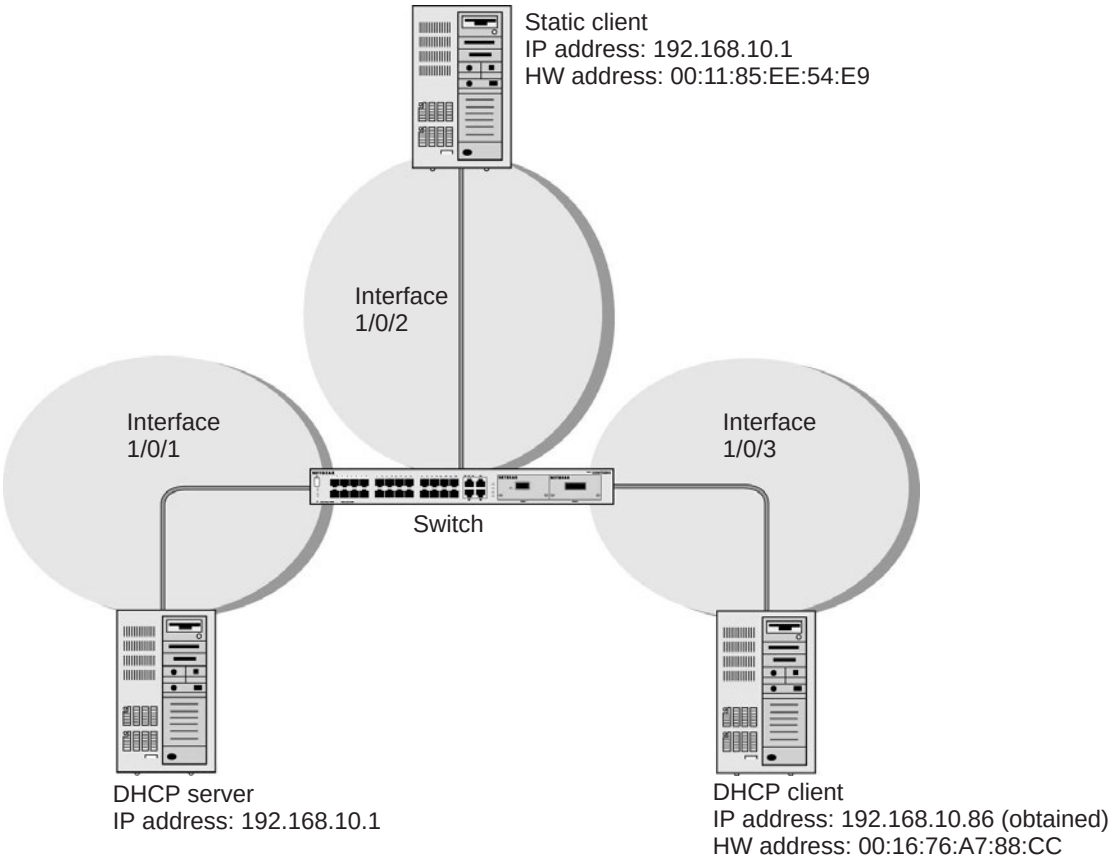


Figure 36. Dynamic ARP inspection

CLI: Configure Dynamic ARP Inspection

1. Enable DHCP snooping globally.

```
(Netgear Switch) (Config)# ip dhcp snooping
```

2. Enable DHCP snooping in a VLAN.

```
(Netgear Switch) (Config)# ip dhcp snooping vlan 1
```

3. Configure the port through which the DHCP server is reached as trusted.

```
(Netgear Switch) (Config)# interface 1/0/1
(Netgear Switch) (Interface 1/0/1)# ip dhcp snooping trust
```

4. View the DHCP Snooping Binding table.

```
(Netgear Switch) #show ip dhcp snooping binding
Total number of bindings:  1

MAC Address        IP Address      VLAN  Interface   Type     Lease (Secs)
-----------------  --------------  ----  ----------  -------  -----------
00:16:76:A7:88:CC  192.168.10.86   1     1/0/2       DYNAMIC  86400
```

5. Enable ARP inspection in VLAN 1.

```
(Netgear Switch) (Config)# ip arp inspection vlan 1
```

   Now all ARP packets received on ports that are members of the VLAN are copied to the CPU for ARP inspection. If there are trusted ports, you can configure them as trusted in the next step. ARP packets received on trusted ports are not copied to the CPU.

6. Configure port 1/0/1 as trusted.

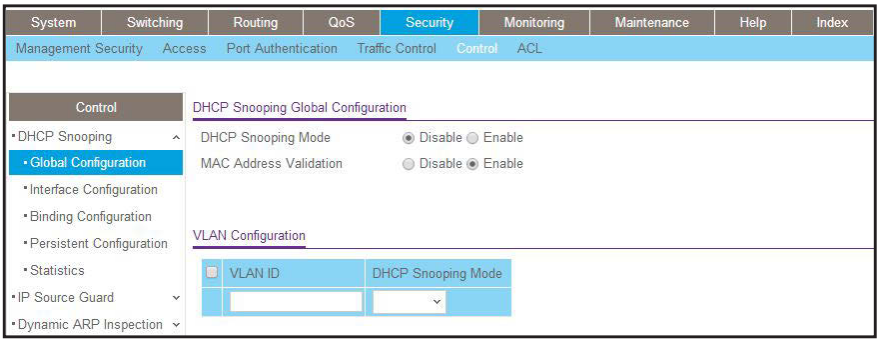
```
(Netgear Switch) (Config)# interface 1/0/1
(Netgear Switch) (Interface 1/0/1)# ip arp inspection trust
```

Now, ARP packets from the DHCP client go through because a DHCP snooping entry exists. However, ARP packets from the static client are dropped. For information about how to prevent ARP packets from static clients to be dropped, see *Static Mapping* on page 337.

Web Interface: Configure Dynamic ARP Inspection

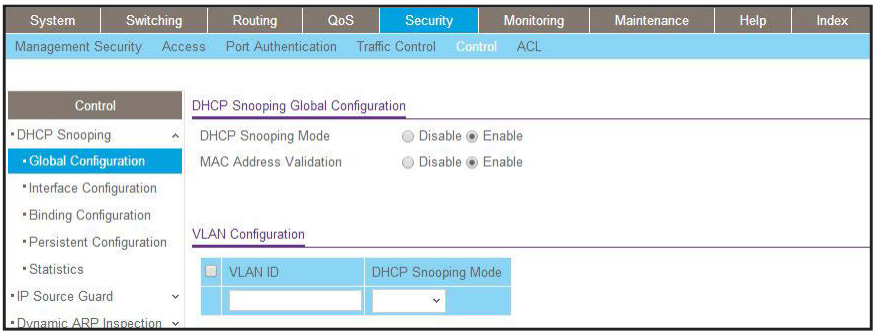
1. Enable DHCP snooping globally.
   a. Select **Security > Control > DHCP Snooping Global Configuration**.

      A screen similar to the following displays.



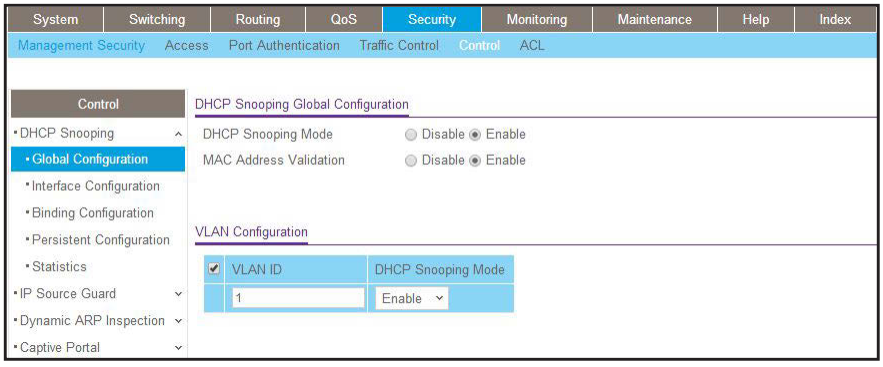
   b. For DHCP Snooping Mode, select the **Enable** radio button.
   c. Click **Apply**.
2. Enable DHCP snooping in a VLAN.
   a. Select **Security > Control > DHCP Snooping Global Configuration**.

      A screen similar to the following displays.



   b. In the **VLAN ID** field, enter **1**.
   c. In the **DHCP Snooping Mode** field, select **Enable**.

      A screen similar to the following displays.

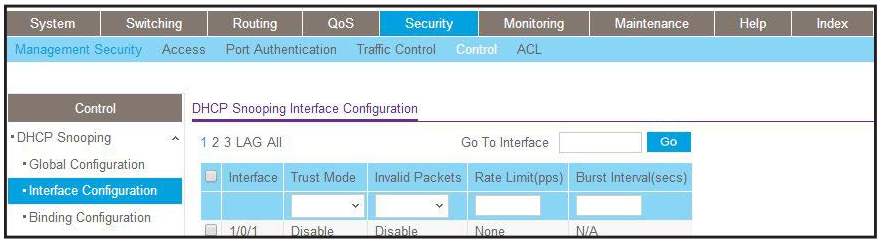


3. Configure the port through which the DHCP server is reached as trusted.

   Here interface 1/0/1 is trusted.

   a. Select **Security > Control > DHCP Snooping Interface Configuration**.

      A screen similar to the following displays.

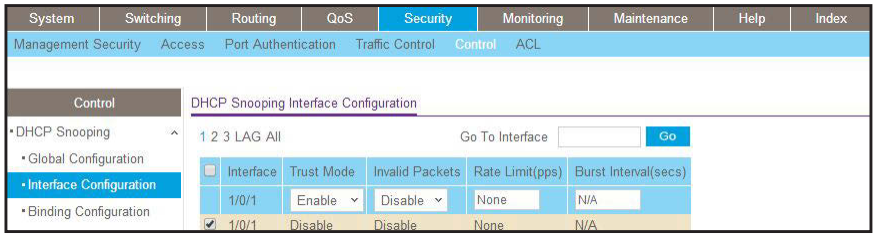


   b. Select the check box for Interface **1/0/1**.

   c. For Interface 1/0/1, set the Trust Mode as **Enable**.

   d. Click **Apply**.

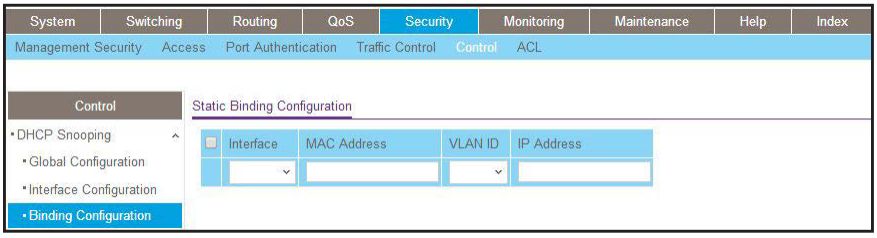
      A screen similar to the following displays.



4. View the DHCP Snooping Binding table.

   a. Select **Security > Control > DHCP Snooping Binding Configuration**.

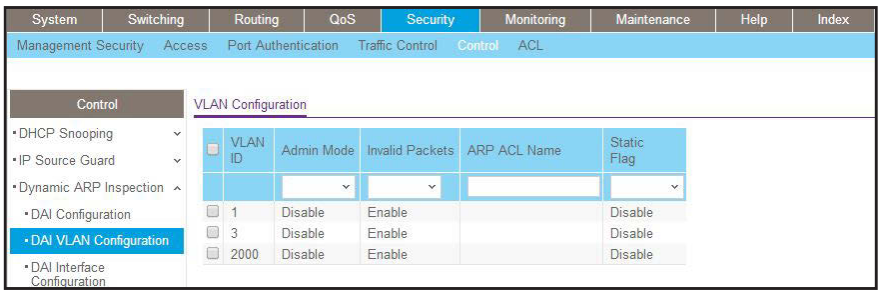
      A screen similar to the following displays.



5. Enable ARP Inspection in VLAN 1.

   a. Select **Security > Control > Dynamic ARP Inspection > DAI VLAN Configuration**.

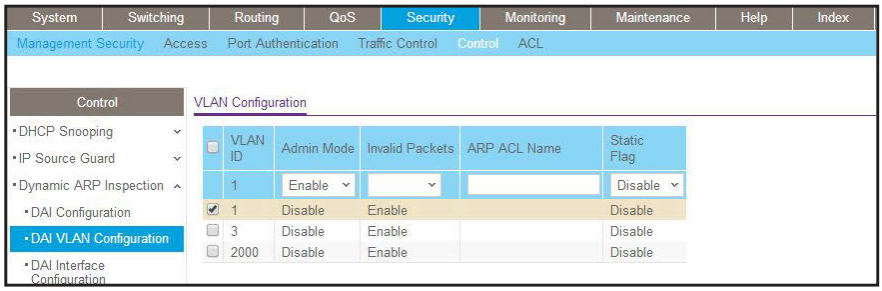
A screen similar to the following displays.



b. In the **VLAN ID** field, enter **1**.

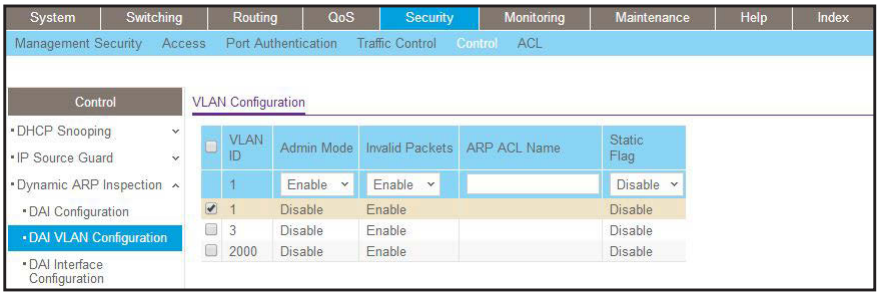
c. In the **Dynamic ARP Inspection** field, select **Enable**.

A screen similar to the following displays.



d. Click **Apply**.

A screen similar to the following displays.



Now all the ARP packets received on the ports that are member of the VLAN are copied to the CPU for ARP inspection. If there are trusted ports, you can configure them as trusted in the next step. ARP packets received on the trusted ports are not copied to the CPU.

Note: Make sure that the administrator computer has a DHCP snooping entry or can access the device through the trusted port for ARP. Otherwise, you might get disconnected from the device.

6. Configure port 1/0/1 as trusted.
   a. Select **Security > Control > Dynamic ARP Inspection > DAI Interface Configuration**.
   b. Select the Interface **1/0/1** check box.
   c. For the **Trust Mode**, select **Enable**.
   d. Click **Apply**.

   A screen similar to the following displays.

Now ARP packets from the DHCP client will go through; however ARP packets from the static client are dropped, since it does have a DHCP snooping entry. It can be overcome by static configuration as described in the following section, *Static Mapping* on page 337.

Static Mapping

The example is shown as CLI commands and as a web interface procedure.

CLI: Configure Static Mapping

1. Create an ARP ACL.

```
(Netgear Switch) (Config)# arp access-list ArpFilter
```

2. Configure the rule to allow the static client.

```
 (Netgear Switch) (Config-arp-access-list)# permit ip host 192.168.10.2
      mac host 00:11:85:ee:54:e9
```

3. Configure ARP ACL used for VLAN 1.

```
(Netgear Switch) (Config)# ip arp inspection filter ArpFilter vlan 1
```

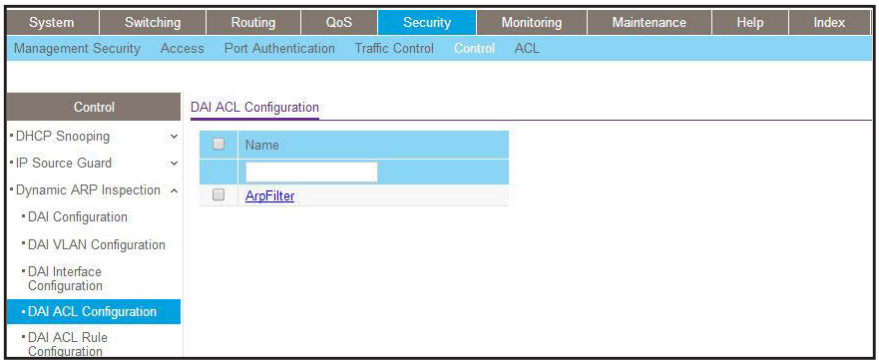
Now the ARP packets from the static client go through because the client has an entry in the ARP table. ACL ARP packets from the DHCP client go also through because the client has a DHCP snooping entry.

This command can include the optional static keyword. If the **`static`** keyword is given, packets that do not match a permit statement are dropped without consulting the DHCP snooping bindings. In this example, ARP packets from the DHCP client are dropped since it does not have a matching rule, though it has a DHCP snooping entry.

Web Interface: Configure Static Mapping

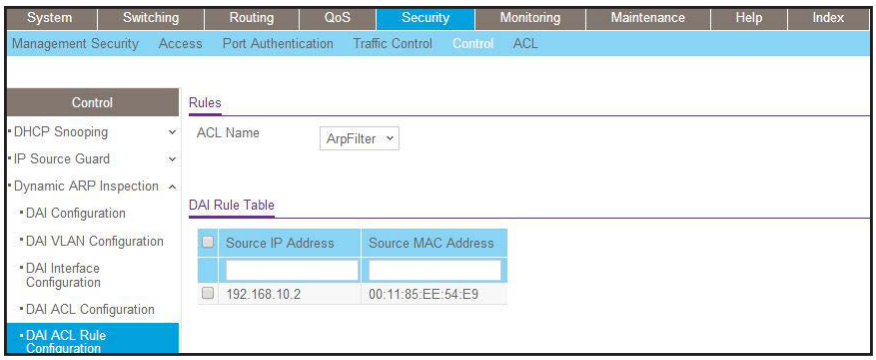
1. Create an ARP ACL.
   a. Select **Security > Control > Dynamic ARP Inspection > DAI ACL Configuration**.
   b. In the **Name** field, enter **ArpFilter**.
   c. Click **Add**.

   A screen similar to the following displays.



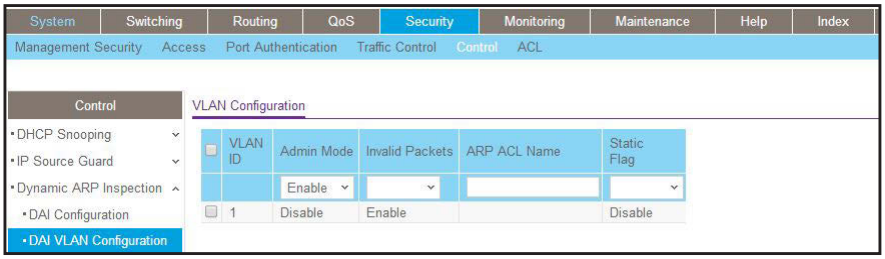
2. Configure a rule to allow the static client.
   a. Select **Security > Control > Dynamic ARP Inspection > DAI ACL Rule Configuration**.
   b. In the **ACL Name** list, select **ArpFilter**.
   c. In the **Source IP Address** field, enter **192.168.10.2**.
   d. In the **Source MAC Address** field, enter **00:11:85:EE:54:E9**.
   e. Click **Add**.

A screen similar to the following displays.



3. Configure the ARP ACL used for VLAN 1.
   a. Select **Security > Control > Dynamic ARP Inspection > DAI VLAN Configuration**.
   b. In the **ARP ACL Name** field, enter **ArpFilter**.
   c. Click **Apply**.

   A screen similar to the following displays.



DHCP Snooping

DHCP snooping is a security feature that monitors DHCP messages between a DHCP client and DHCP server to filter harmful DHCP message and to build a bindings database of (MAC address, IP address, VLAN ID, port) tuples that are considered authorized. The network administrator enables DHCP snooping globally and on specific VLANs and configures ports within the VLAN to be trusted or untrusted. DHCP servers must be reached through trusted ports.

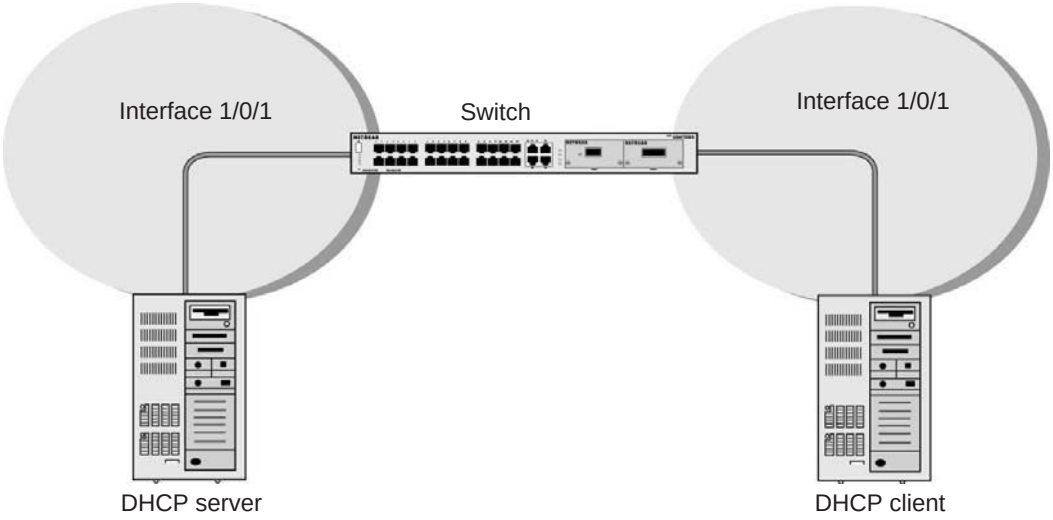


Figure 37. DHCP Snooping

The example is shown as CLI commands and as a web interface procedure.

CLI: Configure DHCP Snooping

1. Enable DHCP snooping globally.

```
(Netgear Switch) (Config)# ip dhcp snooping
```

2. Enable DHCP snooping in a VLAN.

```
(Netgear Switch) (Config)# ip dhcp snooping vlan 1
```

3. Configure the port through which the DHCP server is reached as trusted.

```
(Netgear Switch) (Config)# interface 1/0/1
(Netgear Switch) (Interface 1/0/1)# ip dhcp snooping trust
```

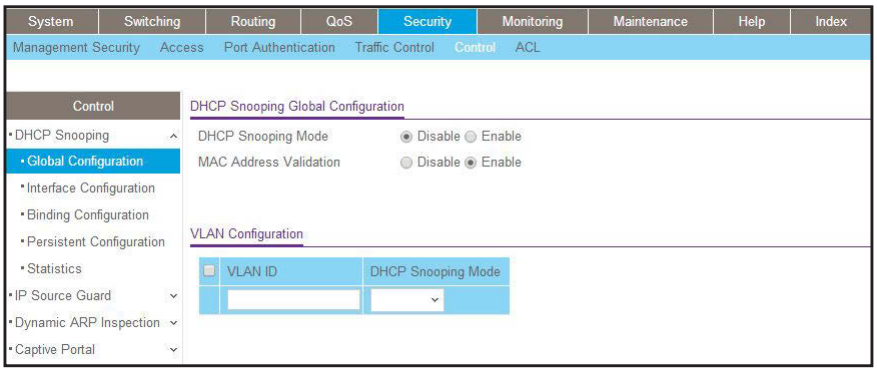
4. View the DHCP Snooping Binding table.

```
(Netgear Switch) #show ip dhcp snooping binding

Total number of bindings:  1

MAC Address        IP Address       VLAN  Interface  Type     Lease (Secs)
-----------------  ---------------  ----  ---------- -------  -----------
00:16:76:A7:88:CC  192.168.10.89    1     1/0/2      DYNAMIC  86400
```

Web Interface: Configure DHCP Snooping

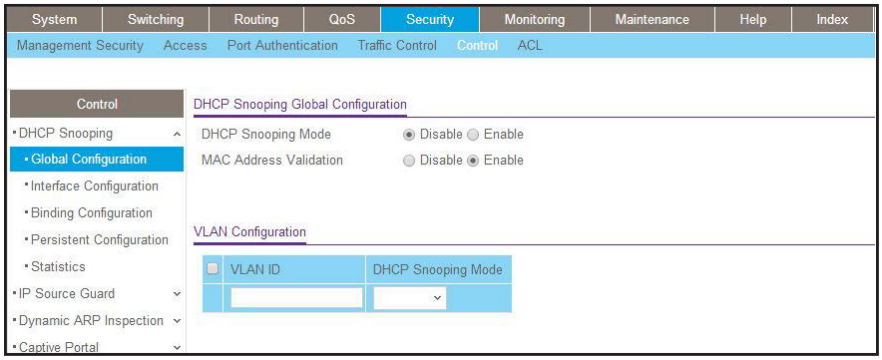
1. Enable DHCP snooping globally:
   a. Select **Security > Control > DHCP Snooping Global Configuration**.

      A screen similar to the following displays.



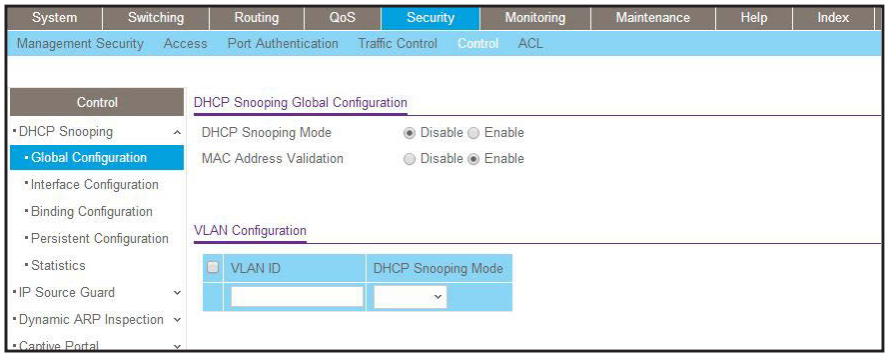
   b. For DHCP Snooping Mode, select **Enable**.
   c. Click **Apply**.

      A screen similar to the following displays.



2. Enable DHCP snooping in a VLAN.
   a. Select **Security > Control > DHCP Snooping Global Configuration**.

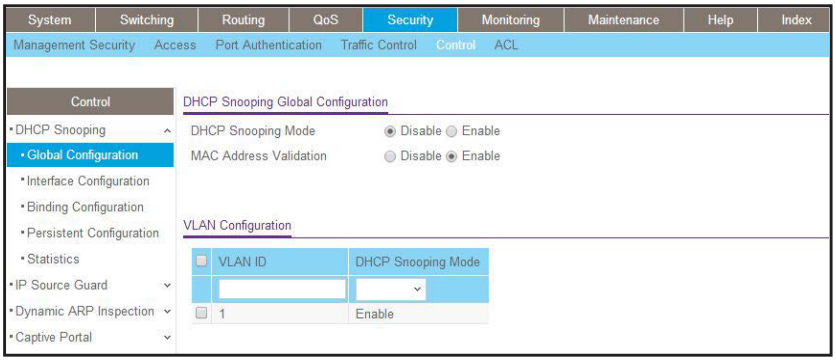
      A screen similar to the following displays.



   b. In the **VLAN ID** list, select **1**.

c. For DHCP Snooping Mode, select the **Enable** radio button.

A screen similar to the following displays.

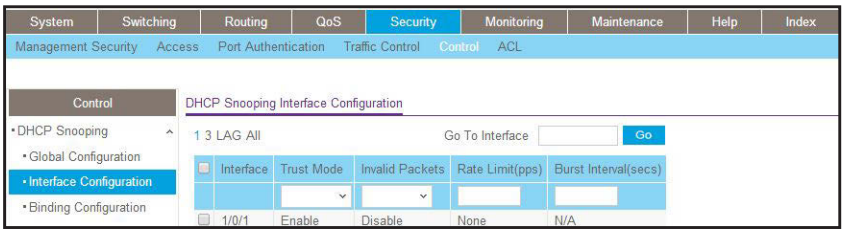


d. Click **Apply**.

3. Configure the port through which DHCP server is reached as trusted.

a. Select **Security > Control > DHCP Snooping Interface Configuration**.

A screen similar to the following displays.

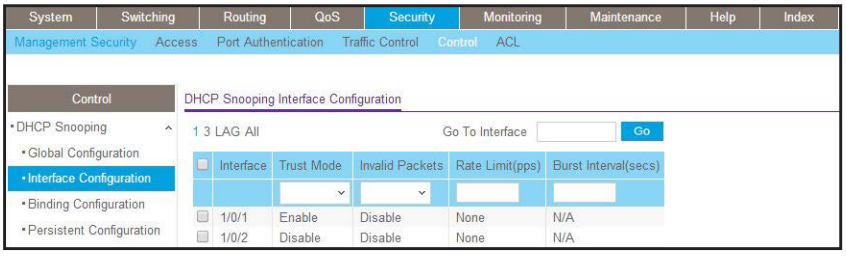


b. Select the Interface **1/0/1**check box.

c. For Interface 1/01/, in the Trust Mode field, select **Enable**.

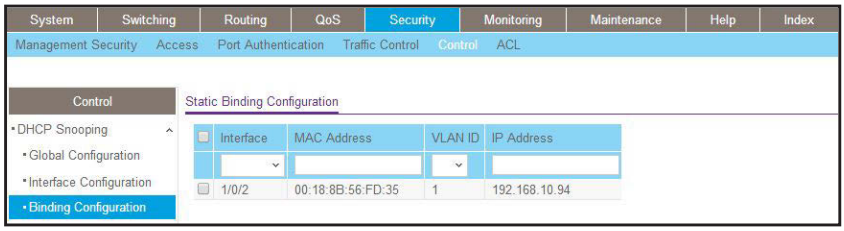
d. Click **Apply**.

A screen similar to the following displays.



4. Select **Security > Control > DHCP Snooping Binding Configuration**.

A screen similar to the following displays.



Find a Rogue DHCP Server

If you enable DHCP snooping, you can find a rogue DHCP server in the network.

CLI: Find a Rogue DHCP server

1. Check the statistics on the untrusted ports.

```
(NETGEAR) #show ip dhcp snooping statistics

Interface         MAC Verify                Client Ifc               DHCP Server
                  Failures                  Mismatch                 Msgs Rec'd
-----------       ----------                ----------               -----------
1/0/1                 0                           0                        0
1/0/2                 0                           0                        0
1/0/3                 0                           0                        0
1/0/4                 0                           0                        0
1/0/5                 0                           0                        0
1/0/6                 0                           0                        0
1/0/7                 0                           0                        0
1/0/8                 0                           0                        0
1/0/9                 0                           0                        0
1/0/10                0                           0                        0
1/0/11                0                           0                        0
1/0/12                0                           0                        0
1/0/13                0                           0                        0
1/0/14                0                           0                        0
1/0/15                0                           0                        0
1/0/16                0                           0                        0
1/0/17                0                           0                        0
1/0/18                0                           0                        0
1/0/19                0                           0                        0
1/0/20                0                           0                        0
1/0/21                0                           0                        0
1/0/22                0                           0                        0
1/0/23                0                           0                        0
1/0/24                0                           0                        0
1/0/25                0                           0                        0
1/0/26                0                           0                        0
1/0/27             3704                           0                     4634
```

In the previous command output, the messages in the DHCP Server Msgs Rec’d column for port 1/0/27 increased, indicating that the port is connected to a rogue DHCP server.

2. Control the logging DHCP messages filtration by the DHCP Snooping application for port 1/0/27.

```
(Netgear Switch) (Interface 1/0/27)#ip dhcp snooping log-invalid
```

3. Display the buffered logging output and search for “DHCP packet; op Reply” so you can determine the IP address and MAC address of the rogue DHCP server.

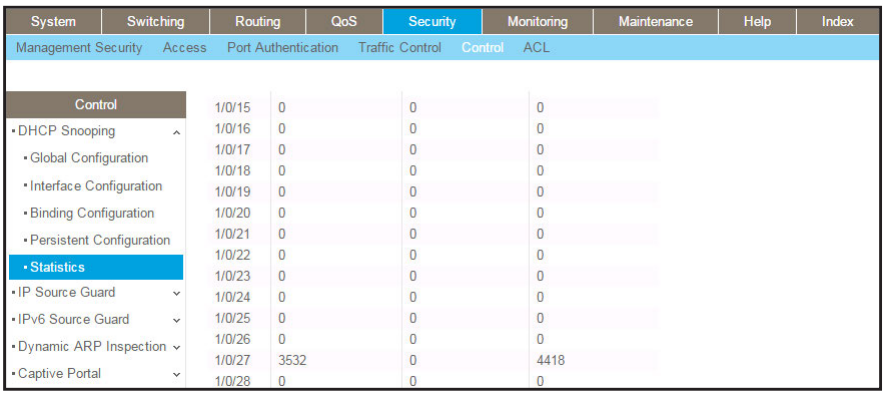
```
(Netgear Switch) #show logging buffered
<12> Jan  1 05:45:02 172.26.2.129-1 DHCP_SNP[108612668]: ds_util.c(1777) 1112 %%
DHCP packet: op Reply, htype 1, hlen 6, hops 0, xid 3478478447, secs 0, ciaddr
0.0.0.0, yiaddr 10.100.4.14, server 10.100.5.253, giaddr 0.0.0.0, chaddr
6C:B0:CE:19:AE:3D.
<12> Jan  1 05:45:02 172.26.2.129-1 DHCP_SNP[108612668]: ds_util.c(1735) 1111 %% IP
packet: ver/hlen 0x45, tos 0, len 299, id 0, flags/offset   00, ttl 64, proto 17,
src 10.100.5.253, dst 255.255.255.255.
<12> Jan  1 05:45:02 172.26.2.129-1 DHCP_SNP[108612668]: ds_util.c(1702) 1110 %%
Ethernet header: dest FF:FF:FF:FF:FF:FF, src 00:26:F2:F6:B3:6C, type/len 0x8100.
<12> Jan  1 05:45:02 172.26.2.129-1 DHCP_SNP[108612668]: ds_main.c(2596) 1109 %%
DHCP snooping dropping DHCP server message received on untrusted interface 1/0/27 on
vlan 1. This message appears when DHCP Snooping untrusted port drops the DHCP Server
message.
```

In the previous example, the IP address of the DHCP server is 10.100.5.253 and the MAC address is 00:26:F2:F6:B3:6C.

Web Interface: Find a Rogue DHCP server

1. Check the statistics on the untrusted ports:
   a. Select **Security > Control > DHCP Snooping > Statistics**.

      A screen similar to the following displays.



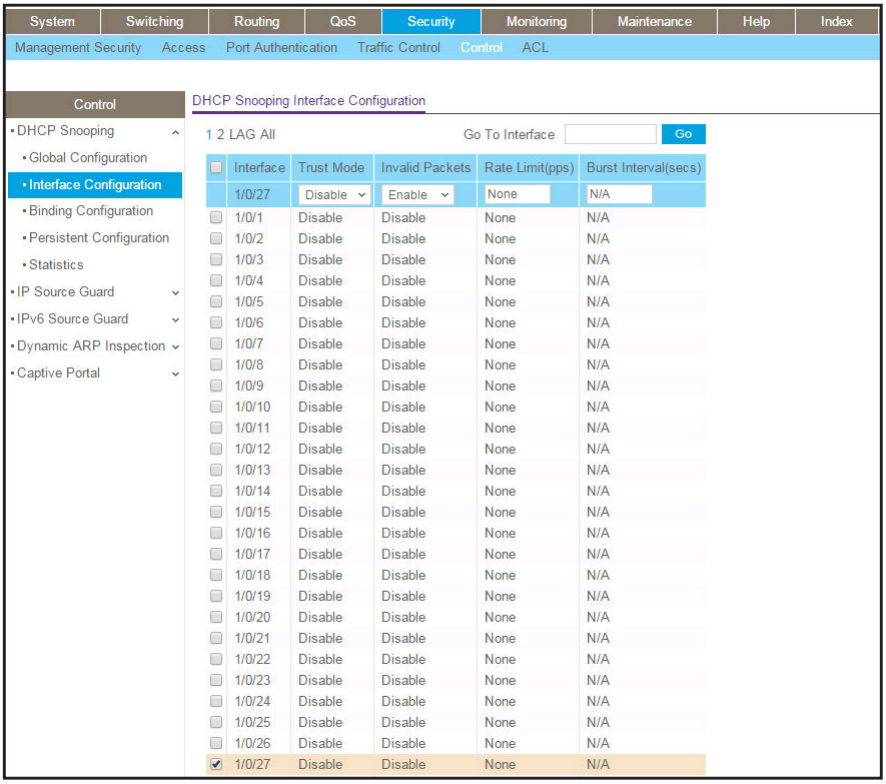
   b. Determine if messages in the DHCP Server Msgs Rec’d column increase for any port.

a. The previous figure shows that the messages increased for port 1/0/27, indicating that the port is connected to a rogue DHCP server.

2. Enable the logging of invalid packets for port 1/0/27.

a. Select **Security > Control > DHCP Snooping > Interface Configuration**.

A screen similar to the following displays.



b. Select the **1/0/27** check box.

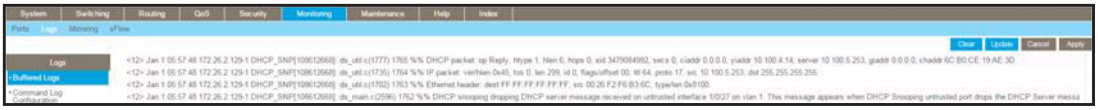
c. In the **Invalid Packets** field, select **Enable**.

d. Click **Apply**.

3. Determine the IP address and MAC address for the rogue DHCP server:

a. Select **Monitoring > Logs > Logs > Buffered logs**.

A screen similar to the following displays.



b. Search for “DHCP packet; op Reply”.

In the previous figure, the IP address of the DHCP server is 10.100.5.253 and the MAC address is 00:26:F2:F6:B3:6C.

Enter Static Binding into the Binding Database

You can also enter the static binding into the binding database.

CLI: Enter Static Binding into the Binding Database

1. Enter the DHCP snooping static binding.

```
(Netgear Switch) (Config)# ip dhcp snooping binding 00:11:11:11:11:11
vlan 1 192.168.10 .1 interface 1/0/2
```

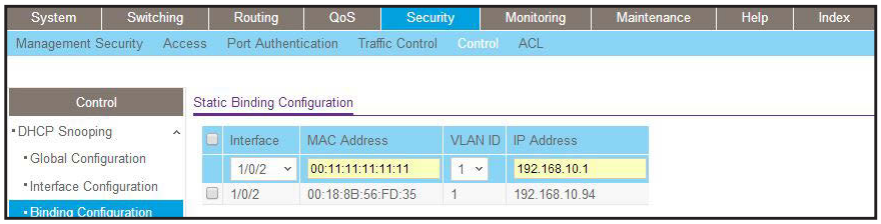
2. Check to make sure that the binding database has the static entry.

```
(Netgear Switch) #show ip dhcp snooping binding
Total number of bindings:  2

MAC Address        IP Address      VLAN   Interface   Type     Lease (Secs)
-----------------  --------------  -----  ----------  -------  -----------
00:11:11:11:11:11  192.168.10.1    1      1/0/2       STATIC
00:16:76:A7:88:CC  192.168.10.89   1      1/0/2       DYNAMIC  86348
```

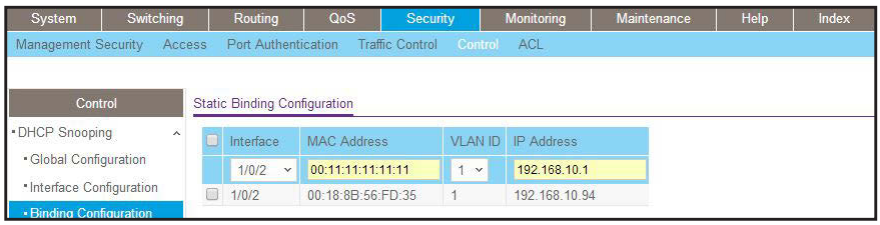
Web Interface: Enter Static Binding into the Binding Database

1. Select **Security > Control > DHCP Snooping > Binding Configuration**.

   A screen similar to the following displays.



2. Fill in the fields for the static binding and click **Apply**.
3. Check to make sure that the binding database shows the entry in the Static Binding Configuration table.



Maximum Rate of DHCP Messages

To prevent DHCP packets being used as DoS attachments when DHCP snooping is enabled, the snooping application enforces a rate limit for DHCP packets received on untrusted interfaces. DHCP snooping monitors the receive rate on each interface separately. If the receive rate exceeds the configured limit, DHCP snooping brings down the interface. The user must specify “no shutdown” on this interface to further work with that port.

CLI: Configure the Maximum Rate of DHCP Messages

1. Control the maximum rate of DHCP messages.

```
(Netgear Switch) (Interface 1/0/2)# ip dhcp snooping limit rate 5
```

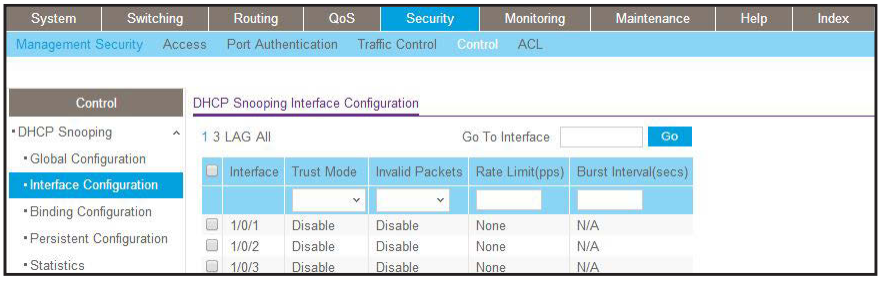
2. View the rate configured.

```
(Netgear Switch) #show ip dhcp snooping interfaces 1/0/2

Interface     Trust State     Rate Limit      Burst Interval
                                 (pps)          (seconds)
----------   -------------   -------------   ---------------

1/0/2              No               5                1
```

Web Interface: Configure the Maximum Rate of DHCP Messages

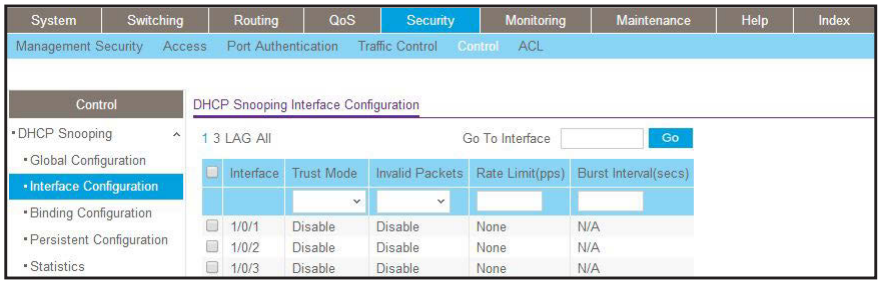
1. Select **Security > Control > DHCP Snooping > Interface Configuration**.

   A screen similar to the following displays.



2. Select the interface, fill in the **Rate Limit (pps)** field, and then click **Apply**.

A screen similar to the following displays.



IP Source Guard

IP Source Guard uses the DHCP snooping bindings database. When IP Source Guard is enabled, the switch drops incoming packets that do not match a binding in the bindings database. IP Source Guard can be configured to enforce just the source IP address or both the source IP address and source MAC address.

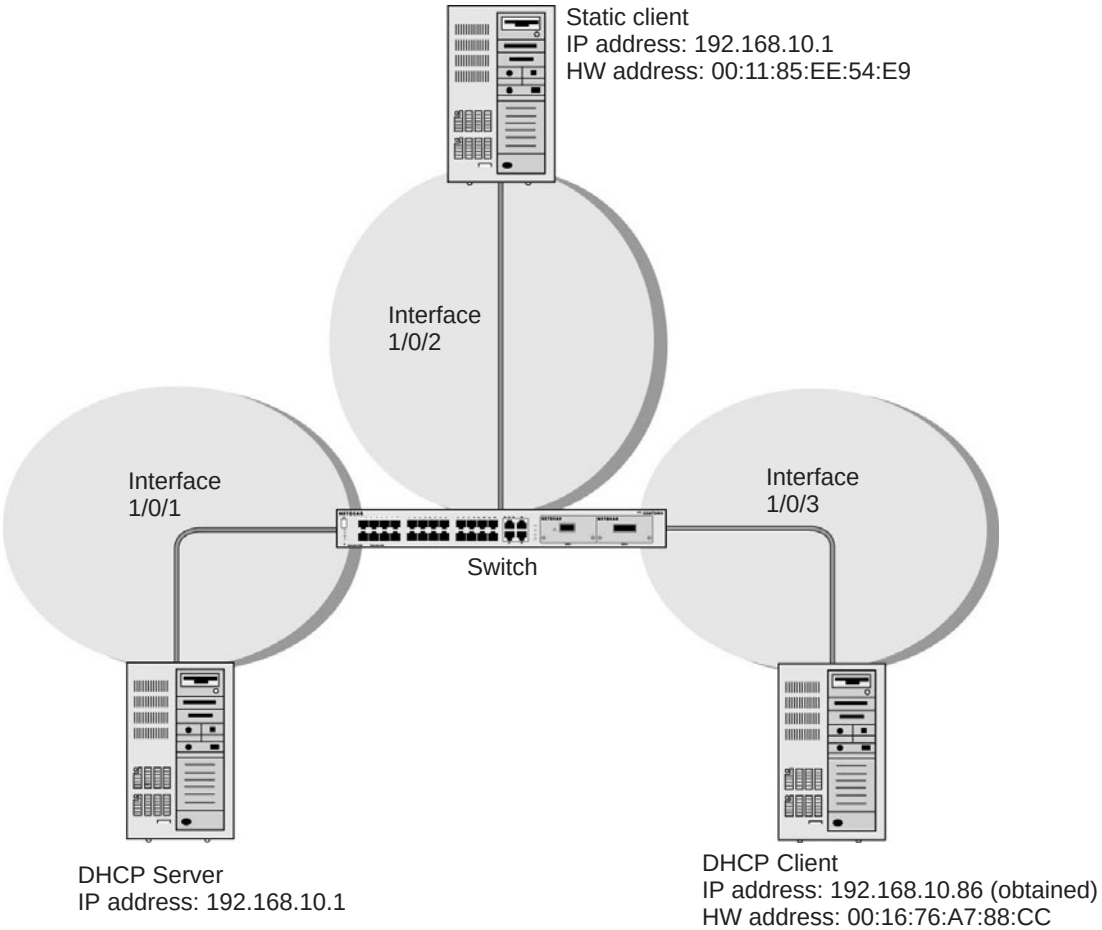


Figure 38. IP Source Guard

The example is shown as CLI commands and as a web interface procedure.

CLI: Configure Dynamic ARP Inspection

1. Enable DHCP snooping globally.

```
(Netgear Switch) (Config)# ip dhcp snooping
```

2. Enable DHCP snooping in a VLAN.

```
(Netgear Switch) (Config)# ip dhcp snooping vlan 1
```

3. Configure the port through which the DHCP server is reached as trusted.

```
(Netgear Switch) (Config)# interface 1/0/1
(Netgear Switch) (Interface 1/0/1)# ip dhcp snooping trust
```

4. View the DHCP Snooping Binding table.

```
(Netgear Switch) #show ip dhcp snooping binding

Total number of bindings:  1

MAC Address        IP Address      VLAN  Interface    Type     Lease (Secs)
-----------------  --------------  ----  -----------  -------  -----------
00:16:76:A7:88:CC  192.168.10.86   1     1/0/2        DYNAMIC  86400
```

   If the entry does not exist in the DHCP Snooping Binding table, you can add the entry manually through the **ip verify binding** *mac-address* **vlan** *vlan-id ip-address* **interface** *interface-id* command in global configuration mode.

5. Enable IP Source Guard in interface 1/0/2.

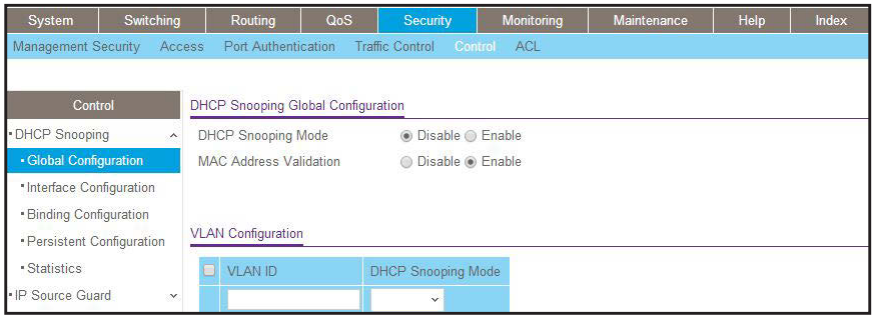
```
(Netgear Switch) (Interface 1/0/2)#ip verify source port-security
```

With this configuration, the device verifies both the source IP address and the source MAC address. If the port-security option is skipped, the device verifies only the source IP address.

Web Interface: Configure Dynamic ARP Inspection

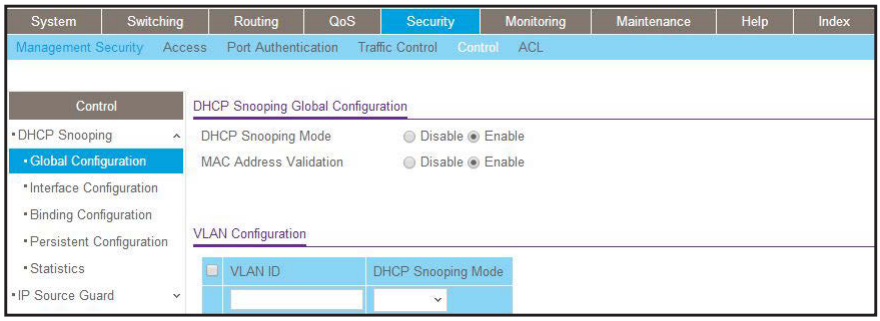
1. Enable DHCP snooping globally.
   a. Select **Security > Control > DHCP Snooping Global Configuration**.

      A screen similar to the following displays.



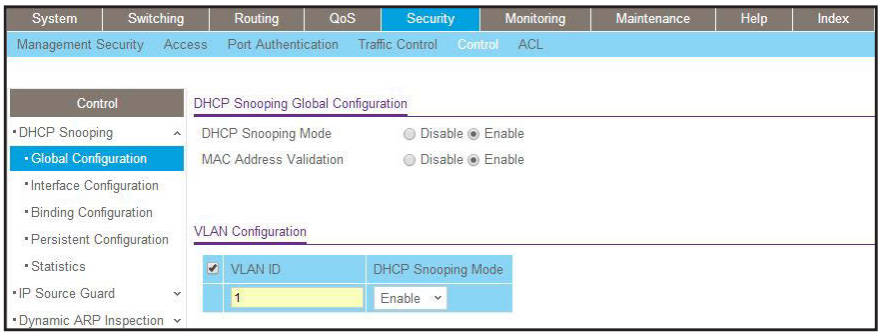
   b. For DHCP Snooping Mode, select the **Enable** radio button.
   c. Click **Apply**.
2. Enable DHCP snooping in a VLAN.
   a. Select **Security > Control > DHCP Snooping Global Configuration**.

      A screen similar to the following displays.



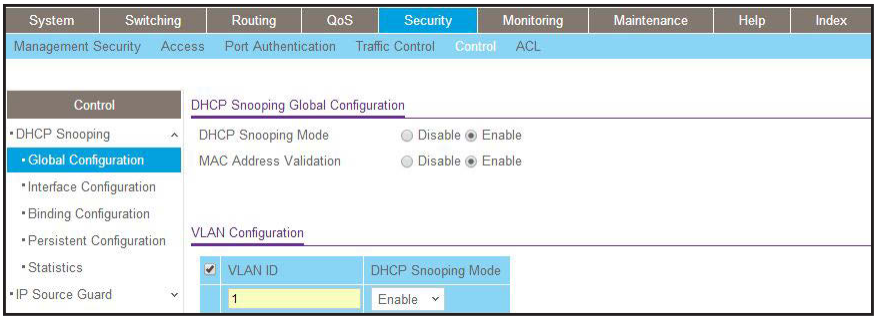
   b. In the VLAN Configuration table, in the **VLAN ID** list, select **1**.
   c. In the **DHCP Snooping Mode** field, select **Enable**.

      A screen similar to the following displays.



   d. Click **Apply**.

A screen similar to the following displays.

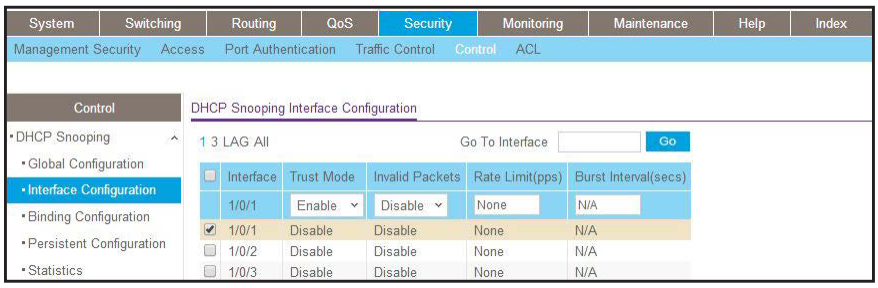


3. Configure the port through which the DHCP server is reached as trusted.

   Here interface 1/0/1 is trusted.

   a. Select **Security > Control > DHCP Snooping Interface Configuration**.

      A screen similar to the following displays.



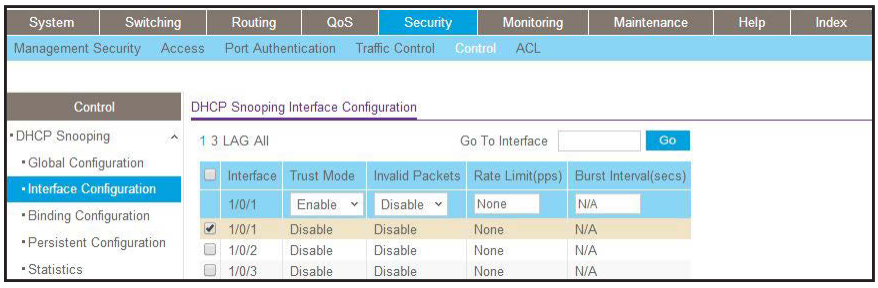
   b. Select Interface **1/0/1** check box.

   c. For interface 1/0/1, in the **Trust Mode** field, select **Enable**.

   d. Click **Apply**.

   a. Select **Security > Control > DHCP Snooping Interface Configuration**.

      A screen similar to the following displays.



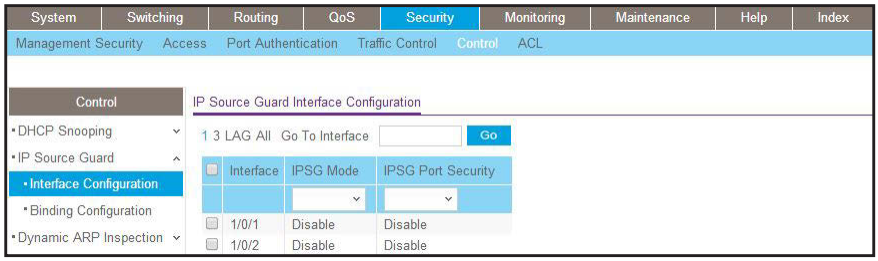
4. View the DHCP Snooping Binding table.

   Select **Security > Control > DHCP Snooping Binding Configuration**.

A screen similar to the following displays.

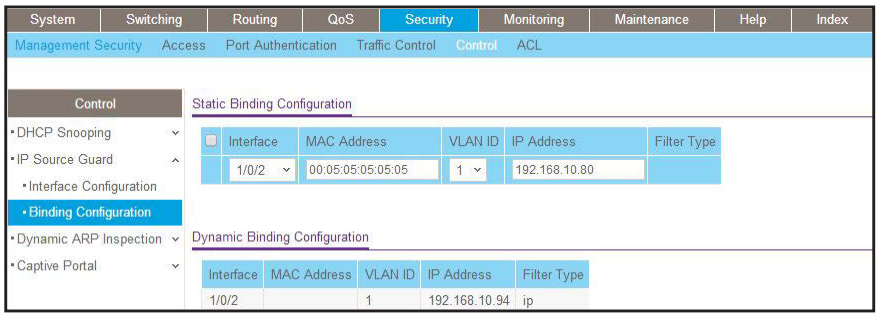
5. Enable IP source guard in the interface 1/0/2.
   a. Select **Security > Control > IP Source Guard > Interface Configuration**.
   b. Select the Interface **1/0/2** check box.
   c. For the IPSG mode, select **Enable**.
   d. Click **Apply**.

      A screen similar to the following displays.



6. Set up IP source guard static binding.
   a. Select **Security > Control > IP Source Guard > Binding Configuration**.
   b. Select the Interface **1/0/2** check box.
   c. In the **MAC Address** field, enter **00:05:05:05:05:05**.
   d. In the **VLAN ID** field, enter **1**.
   e. In the **IP Address** field, enter **192.168.10.80**.
   f. Click **Add**.

      A screen similar to the following displays.



Command Authorization

Authorization determines if a user is authorized to perform certain activities such as entering specific EXEC commands.

TACACS+ servers support command authorization. The RADIUS protocol does not support command authorization but you can use a vendor-specific attribute (VSA) with attribute value (AV) pair 26 to download a list of commands that are permitted or denied for a user. This list of commands is downloaded from the RADIUS server. When a user executes a command, the command is validated against the downloaded command list for the user. Any change in a user command authorization access list takes effect after a user has logged on and logged in again.

The vendor-specific attribute netgear-cmdAuth is defined as follows:

```
VENDOR     netgear    4526
ATTRIBUTE  netgear-cmdAuth       1       string   netgear
```

Specify the command in the following format.

```
netgear-cmdAuth = "deny:spanning-tree;interface *",
```

Note: The maximum length of the command string in the vendor attribute cannot be longer than 64 bytes. RADIUS-based command authorization supports a maximum of 50 commands.

Note: You can use both a TACACS+ server and a RADIUS server for command authorization. If the first method of command authorization returns an error, the second method is used for command authorization.

CLI Example 1: Configure Command Authorization by a TACACS+ Server

The following example shows how to use the CLI to configure command authorization by a TACACS+ server for a Telnet user and allow the user to access specific commands only.

1. Change the authentication mode for Telnet users to TACACS.

```
(Netgear Switch)(Config)#aaa authentication login "networkList" tacacs
```

2. Verify that TACACS authentication is set up for Telnet users.

```
(Netgear Switch)#show authentication methods

Login Authentication Method Lists
---------------------------------
defaultList         :  local
networkList         :  tacacs

Enable Authentication Method Lists
----------------------------------
enableList          :  enable   none
enableNetList       :  enable   none

Line     Login Method List    Enable Method List
-------  -----------------    ------------------
Console  defaultList          enableList
Telnet   networkList          enableList
SSH      networkList          enableList

HTTPS       :local
HTTP        :local
DOT1X       :
```

3. Create a command authorization list and configure TACACS as the authorization.

```
(Netgear Switch)(Config)#aaa authorization commands "commandList" tacacs
```

4. Configure command and privileged EXEC authorization for Telnet.

```
(Netgear Switch)(Config)#line telnet
(Netgear Switch)(Config-telnet) #authorization commands commandList
(Netgear Switch)(Config-telnet) #exit
(Netgear Switch)(Config) #exit
```

5. Configure a TACACS+ server.

```
(Netgear Switch)(Config)#tacacs-server host 10.100.5.13
(Netgear Switch)(Config)#tacacs-server key 12345678
```

6. Verify that command and privileged EXEC authorization are set up for Telnet.

```
(Netgear Switch)#show authorization methods
Command Authorization Method Lists
-----------------------------------
dfltCmdAuthList               :      none
commandlist                   :      tacacs
Line       Command Method List
---------  --------------------
Console    dfltCmdAuthList
Telnet     commandlist
SSH        dfltCmdAuthList
Exec Authorization Method Lists
-----------------------------------
dfltExecAuthList               :      none
Line       Exec Method List
---------  --------------------
Console    dfltExecAuthList
Telnet     dfltExecAuthList
SSH        dfltExecAuthList
```

7. Using Linux on the TACACS server, configure an encryption key in the file tac_plus.conf.

```
key = "12345678"
accounting syslog;
accounting file = /var/log/tac_plus/tac_plus.acct
```

8. Using Linux on the TACACS server, allow a user named eric to access specific commands in the file tac_plus.conf.

```
user = eric {
     #  member = network_user {
       default service = deny
       login = des qbVVseTcbtzS2

       service = exec {
       priv-lvl = 15
       }
        cmd = show {
                permit .*
        }
        cmd = exit {
                permit .*
        }
        cmd = configure {
                permit .*
        }
        cmd = interface {
                permit .*
        }
        cmd =  switchport  {
                permit "switchport access vlan.*"
                permit "switchport mode.*"
                permit "switchport trunk allowed vlan.*"
        }
}
```

CLI Example 2: Configure Command Authorization by a RADIUS Server

The following example shows how to use the CLI to configure command authorization by a RADIUS server for a Telnet user and deny the user to access specific commands.

1. Configure a RADIUS server on the switch.

```
(Netgear Switch) #config
(Netgear Switch) (Config)#radius server host auth 172.26.2.41
(Netgear Switch) (Config)#radius server key auth 172.26.2.41
Enter secret (64 characters max):12345678
Re-enter secret:12345678
```

2. Change the authentication mode for Telnet users to RADIUS.

```
(Netgear Switch)(Config)#aaa authentication login networkList radius
```

3. Verify that RADIUS authentication is set up for Telnet users.

```
(Netgear Switch) #show authentication methods
Login Authentication Method Lists
---------------------------------
defaultList         :  local
networkList         :  radius

Enable Authentication Method Lists
----------------------------------
enableList          :  enable   none
enableNetList       :  enable   none

Line     Login Method List    Enable Method List
-------  -----------------    ------------------
Console  defaultList          enableList
Telnet   networkList          enableList
SSH      networkList          enableList

HTTPS       :local
HTTP        :local
DOT1X       :
```

4. Create a command authorization list and configure RADIUS as the authorization.

```
(Netgear Switch)(Config)# aaa authorization commands commandList radius
```

5. Configure command authorization list for Telnet.

```
Netgear Switch) (Config)#line telnet
(Netgear Switch) (Config-telnet)#authorization commands commandList
(Netgear Switch) (Config-telnet)#exit
```

6. Verify that command authorization is set up for Telnet.

```
(Netgear Switch) #show authorization methods
Command Authorization Method Lists
-----------------------------------
dfltCmdAuthList                :      none
commandList                    :      radius

Line       Command Method List
---------  --------------------
Console    dfltCmdAuthList
Telnet     commandList
SSH        dfltCmdAuthList

Exec Authorization Method Lists
-----------------------------------
dfltExecAuthList               :      none

Line       Exec Method List
---------  --------------------
Console    dfltExecAuthList
Telnet     dfltExecAuthList
SSH        dfltExecAuthList
```

7. Using Linux on the RADIUS server, configure NETGEAR as the vendor and 4526 as the vendor-specific value in the dictionary file for FreeRADIUS.

```
VENDOR     netgear    4526
BEGIN-VENDOR netgear
ATTRIBUTE netgear-cmdAuth-deny    1     string
END-VENDOR netgear
```

8. Using Linux on the RADIUS server, deny a user named eric access to specific commands in the user file for FreeRADIUS.

```
eric  Cleartext-Password := "testing"
       Service-Type = Login-User,
       netgear-cmdAuth-deny = "deny:poe *;spanningtree *;"
```

Privileged Exec Command Mode Authorization

Authorization determines if a user is authorized to perform certain activities such entering privileged EXEC commands.

When user command authentication succeeds, the user receives access to the user EXEC mode. You can also provide a user direct access to the privileged EXEC mode by using the EXEC authorization method.

If the EXEC authorization method uses a TACACS+ authorization server, a separate session is established with the TACACS+ server to return the authorization attributes.

If the EXEC authorization method uses a RADIUS authorization server, service–type attribute 6 or Cisco vendor-specific attribute (VSA) “shell:priv-lvl” is used. If the service-type attribute value is returned as administrator or the Cisco VSA “shell:priv-lvl” is at least FD_USER_MGR_ADMIN_ACCESS_LEVEL(15), the user receives access to the privileged EXEC mode.

Because the RADIUS protocol does not support authorization, the privilege level attribute must be returned with the authentication response. If the service-type attribute is already present in RADIUS response packet as administrator, the Cisco VSA “shell:priv-lvl” is ignored.

CLI Example 1: Configure EXEC Authorization by a TACACS+ Server

The following example shows how to use the CLI to configure command authorization by a TACACS+ server for a Telnet user and allow the user to access privileged EXEC mode directly.

1. Change the authentication mode for Telnet users to TACACS.

```
(Netgear Switch)(Config)#aaa authentication login "networkList" tacacs
```

2. Verify that TACACS authentication is set up for Telnet users.

```
(Netgear Switch) #show authentication methods

Login Authentication Method Lists
---------------------------------
defaultList         :  local
networkList         :  tacacs

Enable Authentication Method Lists
----------------------------------
enableList          :  enable   none
enableNetList       :  enable   none

Line     Login Method List    Enable Method List
-------  -----------------    ------------------
Console  defaultList          enableList
Telnet   networkList          enableList
SSH      networkList          enableList

HTTPS       :local
HTTP        :local
DOT1X       :
```

3. Create an EXEC authorization list and configure TACACS as the authorization.

```
(Netgear Switch)(Config)#aaa authorization exec "execList" tacacs
```

4. Configure EXEC authorization for Telnet.

```
(Netgear Switch)(Config)#line telnet
(Netgear Switch)(Config-telnet)#authorization exec execList
(Netgear Switch)(Config-telnet)#exit
```

5. Verify that EXEC authorization is set up for Telnet.

```
(Netgear Switch) #show authorization methods

Command Authorization Method Lists
-------------------------------------
dfltCmdAuthList                :      none
commandlist                    :      tacacs

Line       Command Method List
---------  --------------------
Console    dfltCmdAuthList
Telnet     dfltCmdAuthList
SSH        dfltCmdAuthList

Exec Authorization Method Lists
-------------------------------------
dfltExecAuthList               :      none
execList                       :      tacacs

Line       Exec Method List
---------  --------------------
Console    dfltExecAuthList
Telnet     execList
SSH        dfltExecAuthList
```

6. Using Linux on the TACACS server, configure an encryption key for the TACACS server in the file tac_plus.conf.

```
key = "12345678"
accounting syslog;
accounting file = /var/log/tac_plus/tac_plus.acct
```

7. Using Linux on the TACACS server, allow a user named eric to access privileged EXEC mode directly as defined in the file tac_plus.conf.

```
user = eric {
     #  member = network_user {
       default service = permit
       login = des qbVVseTcbtzS2

       service = exec {
       priv-lvl = 15
       }
```

CLI Example 2: Configure EXEC Authorization by a RADIUS Server

The following example shows how to use the CLI to configure command authorization by a RADIUS server for a Telnet user and allow the user to access privileged EXEC mode directly.

1. Configure a RADIUS server on the switch.

```
(Netgear Switch) #config
(Netgear Switch) (Config)#radius server host auth 172.26.2.41
(Netgear Switch) (Config)#radius server key auth 172.26.2.41
Enter secret (64 characters max):12345678
Re-enter secret:12345678
```

2. Change the authentication mode for Telnet users to RADIUS.

```
(Netgear Switch)(Config)#aaa authentication login networkList radius
```

3. Verify that the RADIUS authentication is set up for Telnet users.

```
(Netgear Switch) #show authentication methods
Login Authentication Method Lists
---------------------------------
defaultList         :  local
networkList         :  radius

Enable Authentication Method Lists
----------------------------------
enableList          :  enable   none
enableNetList       :  enable   none

Line     Login Method List    Enable Method List
-------  -----------------    ------------------
Console  defaultList          enableList
Telnet   networkList          enableList
SSH      networkList          enableList

HTTPS       :local
HTTP        :local
DOT1X       :
```

4. Create an EXEC authorization list and configure RADIUS as the authorization.

```
(Netgear Switch)(Config)# aaa authorization exec execList radius
```

5. Configure EXEC authorization for Telnet.

```
(Netgear Switch) (Config)#line telnet
(Netgear Switch) (Config-telnet)# authorization exec execList
(Netgear Switch) (Config-telnet)#exit
```

6. Verify that EXEC authorization is set up for Telnet.

```
(Netgear Switch) #show authorization methods
Command Authorization Method Lists
-------------------------------------
dfltCmdAuthList                :      none

Line       Command Method List
---------  --------------------
Console    dfltCmdAuthList
Telnet     dfltCmdAuthList
SSH        dfltCmdAuthList

Exec Authorization Method Lists
-------------------------------------
dfltExecAuthList               :      none
execList                       :      radius

Line       Exec Method List
---------  --------------------
Console    dfltExecAuthList
Telnet     execList
SSH        dfltExecAuthList
```

7. Using Linux on the RADIUS server, configure a user named eric as an administrator in the user file for FreeRADIUS.

```
eric  Cleartext-Password := "testing"
       Service-Type = Administrative-User,
```

Note: Instead, you can also configure a user named eric with Cisco-AVPair "shell:priv-lvl=15".

```
eric  Cleartext-Password := "testing"
       Service-Type = Login-User,
       Cisco-AVPair = "shell:priv-lvl=15
```

Accounting

The accounting process records what a user does or has done on the switch. You can configure a TACACS+ accounting server or RADIUS accounting server to account for the following actions:

- Account for services that were used, such as in a billing environment. You can use this type of accounting as an auditing tool for security services.
- Account when a user logs in and logs out of a user EXEC session.

CLI: Configure Telnet Command Accounting by a TACACS+ Server

Note: TACACS+ accounting supports both user EXEC command authorization and privileged EXEC command authorization.

```
(Netgear Switch)(Config)#tacacs-server host 10.100.5.13
(Netgear Switch)(Tacacs)#key 12345678

(Netgear Switch)(Tacacs)#exit
(Netgear Switch)(Config)#
(Netgear Switch)(Config)#aaa accounting commands default stop-only tacacs
(Netgear Switch)(Config)#line telnet
(Netgear Switch)(Config-telnet)#accounting commands default
(Netgear Switch)(Config-telnet)#exit

(Netgear Switch)#show accounting methods
AcctType  MethodName       MethodType    Method1   Method2
--------- ---------------- ------------- --------- ---------
Exec      dfltExecList     start-stop    radius
Commands  dfltCmdList      stop-only     tacacs

Line      EXEC Method List     Command Method List
--------- -------------------- --------------------
Console   none                 none
Telnet    dfltExecList         dfltCmdList
SSH       none                 none
HTTPS     none                 none
HTTP      none                 none
```

Configure Telnet EXEC Accounting by RADIUS Server

RADIUS accounting supports EXEC mode but does not support command mode.

```
(Netgear Switch)(Config)#radius server host acct 10.100.5.13
(Netgear Switch)(Config)#radius server key acct 10.100.5.13
Enter secret (64 characters max):12345678
Re-enter secret:12345678
(Netgear Switch)(Config)#radius accounting mode
(Netgear Switch)(Config)#aaa accounting exec default stop-only radius
(Netgear Switch)#show radius
Number of Configured Authentication Servers.... 0
Number of Configured Accounting Servers........ 1
Number of Named Authentication Server Groups... 0
Number of Named Accounting Server Groups....... 1
Number of Retransmits.......................... 4
Timeout Duration............................... 5
RADIUS Accounting Mode......................... Enable
RADIUS Attribute 4 Mode........................ Disable
RADIUS Attribute 4 Value....................... 0.0.0.0

(Netgear Switch) #show accounting methods
AcctType  MethodName        MethodType    Method1   Method2
--------- ----------------  ------------ --------- ---------
Exec      dfltExecList      stop-only     radius
Commands  dfltCmdList       stop-only     tacacs

Line      EXEC Method List     Command Method List
--------- -------------------- --------------------
Console   none                 none
Telnet    dfltExecList         dfltCmdList
SSH       none                 none
HTTPS     none                 none
HTTP      none                 none
```

Use the Authentication Manager to Set Up an Authentication Method List

The authentication manager lets you configure an authentication method list, which you can apply on a per-port basis. If authentication is disabled, no authentication method is applied and the port provides open access. By default, authentication is disabled for all ports.

The authentication manager lets you configure the following authentication methods in an authentication method list:

- dot1x
- MAB
- captive portal (that is, web authentication)

The default authentication method list applies these authentication methods in the order dot1x, MAB, and captive portal as the default methods for all ports.

You cannot configure another authentication method after the captive portal method, that is, the captive portal method must be the last method in an authentication method list.

When a client connects to a port, the switch attempts to authenticate the client through the port-based authentication method list. If an authentication method times out (or an error occurs), the switch attempts to authenticate with the next authentication method in the list. If all authentication methods time out, the switch starts a timer for which the value is equal to the authentication restart timer. At the expiration of the timer, the authentication manager restarts the authentication process for the first method in the list. If the client connection goes down and comes up again, the authentication manager restarts the authentication sequence.

Note: The authentication manager controls only the order in which the switch executes the authentication methods. The authentication manager does not configure or change the authentication methods. You need to ensure that the switch is configured correctly so that the switch can execute the authentication methods as presented in the authentication method list.

The priority of an authentication method is determined by its position in authentication method list. If you do not configure authentication method priorities, the relative priorities (that is, the highest first) are in the same order as that of the port-based authentication list.

Authentication priority allows a higher-priority method to interrupt an authentication process that is in progress with a lower-priority method. Alternatively, if a client is already authenticated, an interrupt from a higher priority method can cause a client that is already authenticated through a lower-priority method to be reauthenticated through the higher-priority method.

Configure a Dot1x–MAB Authentication Method List with Dot1x–MAB Priority

Note: This section describes how to configure the authentication order and priority. For information about configuring the dot1x authentication method, which is also referred to as 802.1x port security, see *802.1x Port Security* on page 315.

In this example, the authentication manager first selects dot1x as the authentication method. If dot1x authentication is successful, the client is authenticated. If the client is not enabled, dot1x and dot1x authentication time out, and the authentication manager selects MAB as the next authentication method. If MAB authentication is successful, the client is authenticated. If MAB authentication fails, the port is placed in the unauthorized state and the authentication manager starts a timer. When the timer expires, the authentication manager restarts the authentication process with dot1x authentication.

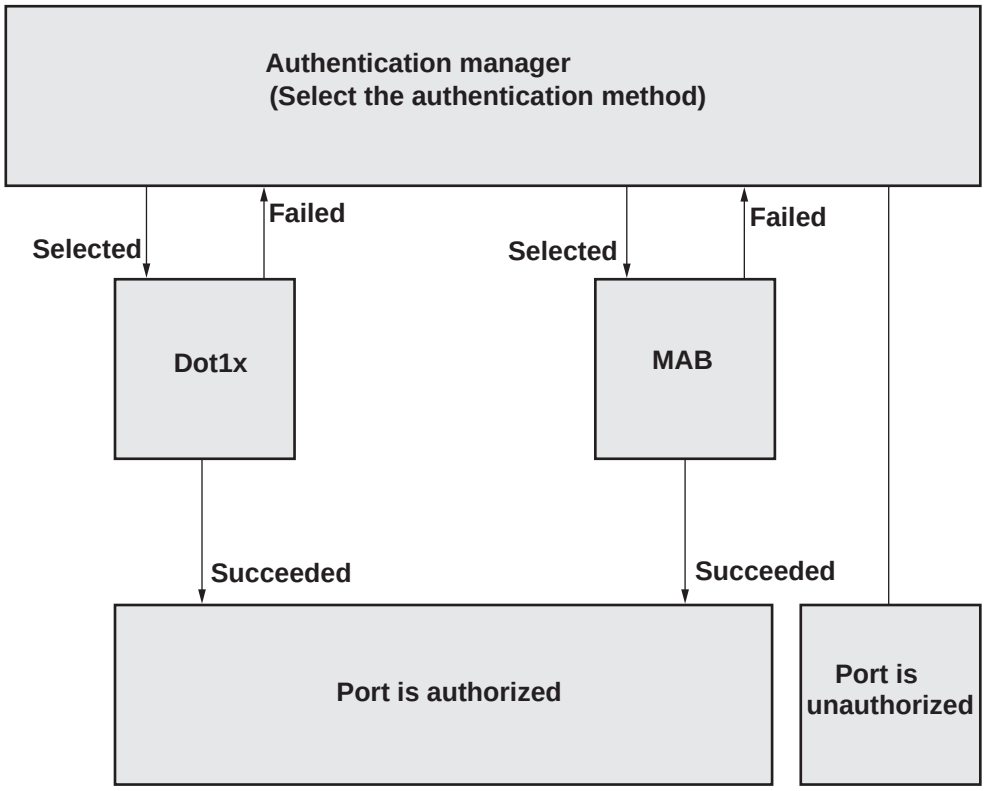


Figure 39. Dot1x, MAB, and captive portal authentication method list with default priority

The CLI command to enable authentication is as follows.

```
(Netgear Switch)#configure
(Netgear Switch)(Config)#authentication enable
```

Configure a Dot1x–MAB Authentication Method List with MAB–Dot1x Priority

Note: This section describes how to configure the authentication order and priority. For information about configuring the MAB authentication method, see *Configure MAC Authentication Bypass on a Switch* on page 377.

If the switch authenticated a client by using MAB but the client is enabled for dot1x after it is authenticated, the EAPOL start frames that the client sends to the authentication manager causes the port to be placed in the unauthorized state and the switch then attempts to authenticate the client by using dot1x. This situation occurs because the default priority for dot1x authentication is higher than the default priority for MAB authentication.

To prevent the port from being placed in the unauthorized state, assign MAB authentication a higher priority than dot1x authentication. In that situation, if the client sends EAPOL start frames to the authentication manager, the authentication manager selects the first configured authentication method in the list, that is, dot1x, and compares the priority of the current authenticated method (that is, MAB) with the newly selected method (that is, dot1x). Because the priority for MAB authentication is higher than the priority for dot1x authentication, the authentication manager does not start dot1x authentication.

The CLI command to enable authentication is as follows.

```
(Netgear Switch)#configure
(Netgear Switch)(Config)#authentication enable
```

Configure a Dot1x, MAB, and Captive Portal Authentication Method List with Default Priority

Note: This section describes how to configure the authentication order and priority. For information about configuring the captive portal authentication method, see *Chapter 35, Captive Portals*.

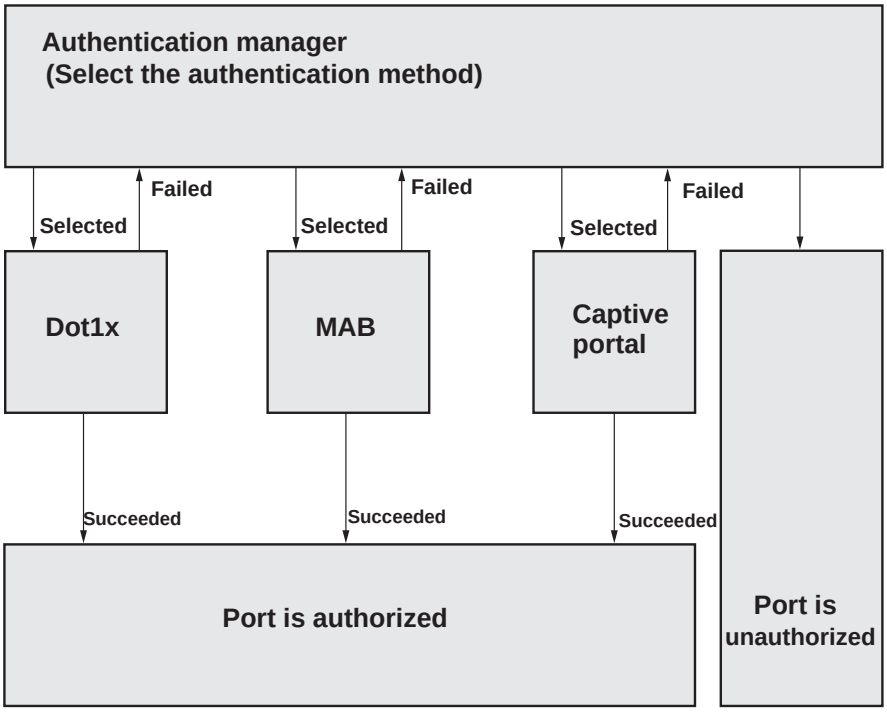


Figure 40. Dot1x, MAB, and captive portal authentication method list with default priority

In this example, a visiting client attempts to connect to a corporate network in which the authentication manager is enabled. In such a situation, configure the authentication method list in the order dot1x, followed by MAB, and followed by captive portal.

If the client is enabled for dot1x but fails to authenticate using dot1x, the authentication manager places the port in the unauthorized state and stops the process. If the client is not enabled for dot1x, the dot1x authentication process times out, and the authentication manager selects the next configured authentication method in the list, which is MAB. Because the client's MAC address is unknown in the corporate network, the MAB authentication process also times out.

The authentication manager selects the third configured authentication method in the list, which is captive portal. If the client can provide valid credentials for web authentication, the client is admitted to the network. If the client cannot provide valid credentials, the authentication manager starts a timer for reauthentication because no other authentication method is available in the list. At the expiration of the timer, the authentication manager restarts the authentication process for the first method in the list.

The CLI command to enable authentication is as follows.

```
(Netgear Switch)#configure
(Netgear Switch)(Config)#authentication enable
```

RADIUS Change of Authorization

Dynamic authorization as defined in RFC 5176 describes the Dynamic Authorization Server (DAS) and Dynamic Authorization Client (DAC). The DAC can send two types of messages: a disconnect message (DM) and a change of authorization (CoA) message. The DAS acts on these messages and sends an acknowledgment (ACK) message or a negative acknowledgment (NAK) message. The DM from the DAC can cause the user session to be terminated. The CoA message from the DAC causes the authorization status of the user session to be changed.

The various users such as dot1x-aware users, dot1x-unaware users (for example, phones and printers), and captive portal clients, as well as console, Telnet, SSH, HTTP, and HTTPS users can connect to the switch by authenticating themselves using the configured authentication method such as local authentication, RADIUS, or TACACS+. When such a user is authenticated through a RADIUS server and dynamic authorization is enabled, you can manage the user session from the DAC by generating a DM or CoA message. A NETGEAR switch can detect these messages on UDP port number 3799.

When a NETGEAR switch receives a disconnect message or a CoA message, the following occurs:

- In DM and CoA messages, all attributes are treated as mandatory attributes and one or more unsupported attributes causes a DM-NAK message or CoA-NAK message to be generated with an Error-Cause attribute as Unsupported Service.
- If the DAS does not perform the expected action for a session, it sends a CoA-NAK message with an Error-Cause attribute as Unsupported Service.

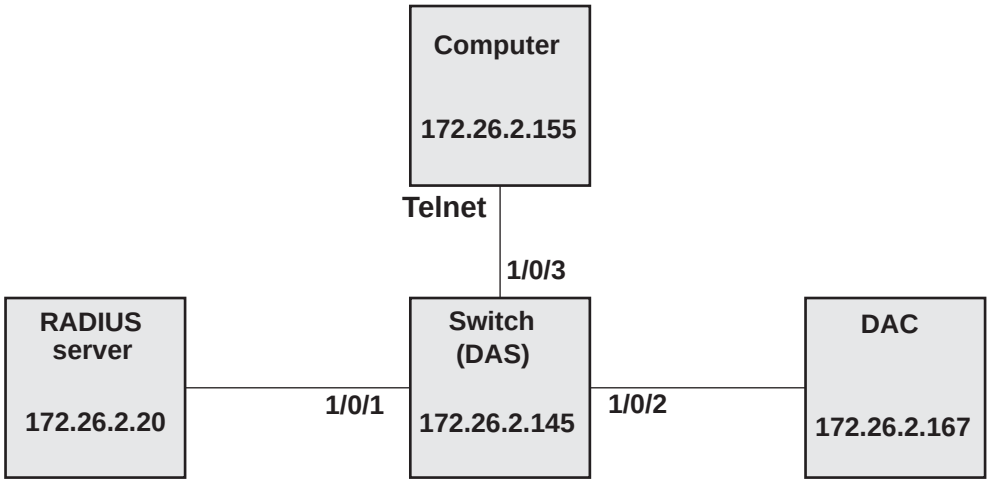


Figure 41. Configuration with a RADIUS server, DAS, and DAC

To configure RADIUS authentication, authenticate a user, and manually disconnect a user:

1. Configure the switch's IP address (172.26.2.145 on VLAN 1).

The switch functions as the Dynamic Authorization Server (DAS).

```
(Netgear Switch) #config
(Netgear Switch) (Config)#interface vlan 1
(Netgear Switch) (Interface vlan 1)#ip address 172.26.2.145 /24
```

2. Configure the RADIUS server.

```
(Netgear Switch) #config
(Netgear Switch) (Config)#radius server host auth 172.26.2.20
(Netgear Switch) (Config)#radius server key auth 172.26.2.20
Enter secret (64 characters max):12345678
Re-enter secret:12345678
```

3. Configure change of authorization (CoA).

```
(Netgear Switch) (Config)#aaa server radius dynamic-author
(Netgear Switch) (config-radius-da)#client 172.26.2.167
(Netgear Switch) (config-radius-da)#auth-type all
```

4. Configure RADIUS as the authentication method for Telnet.

```
(Netgear Switch) (Config)#aaa authentication login test1 radius
(Netgear Switch) (Config)#line telnet
(Netgear Switch) (Config-telnet)#login authentication test1
(Netgear Switch) (Config-telnet)#exit
(Netgear Switch) (Config)#exit
```

5. On the Dynamic Authorization Client (DAC), install a RADIUS client.

   The following example installs the FreeRADIUS client, which you can download from *http://freeradius.org/download.html* on a DAC that runs a Linux operating system.

```
[root@localhost root]# cd /usr/local/etc/raddb/
Create test.txt file using vi.
[root@localhost raddb]# vi test.txt
User-Name = "aaa"
Framed-IP-Address= "172.26.2.155"
```

6. Authenticate a Telnet user with RADIUS server credentials.

If the authentication is successful, the session displays in the output of the **show login sessions** command.

7. Disconnect the user from the DAC.

```
[root@localhost raddb]# cat /usr/local/etc/raddb/test.txt | radclient -x
172.26.2.145:3799  disconnect 12345678
```

IPv6 Stateless RA Guard

Spoof attacks can occur on routed protocols. When you operate an IPv6 network in a shared Layer 2 network segment, the network can receive and process rogue router advertisement (RA) messages that are generated with malicious intent or are caused by an incorrect configuration of routers that are connected to the segment.

If the IPv6 network segments are part of one or more managed switches and all traffic between the IPv6 end devices traverses through the managed switches, the IPv6 RA Guard feature can provide protection against rogue RA messages.

The IPv6 RA Guard feature lets you block or reject rogue RA messages that are received on a port. The IPv6 RA Guard feature analyzes the RA messages and compares the configuration on the switch with the information in the RA message. If the frame is validated, the RA message is forwarded to the unicast or multicast destination. If the RA message is not validated, the RA message is dropped by the switch.

The IPv6 RA Guard feature can operate in the following two modes:

- **Stateless**. The switch does not maintain any state and simply validates the RA messages as they are received against the configured match criteria.
- **Stateful**. The switch dynamically learns about valid RA senders and stores this information to allow subsequent RA messages. The switch listens to the RA messages that are received over a short period that you can configure manually. The switch then allows RA messages that are received only on the ports on which valid RA messages were received during the listening period.

Note: On a managed switch, the IPv6 RA Guard feature supports only the stateless mode.

To configure the IPv6 RA Guard feature, display the configuration, and display the dropped messages:

1. Configure the IPv6 RA Guard feature on port 1.

```
(Netgear Switch) (Config)#interface 1/0/1
(Netgear Switch) (Interface 1/0/1)#ipv6 nd raguard attach-policy
(Netgear Switch) (Interface 1/0/1)#exit
(Netgear Switch) (Config)#exit
```

2. Display the configuration of the IPv6 RA Guard feature on port 1/0/1.

```
(Netgear Switch) #show ipv6 nd raguard policy
Ipv6 RA-Guard Configured Interfaces
Interface    Role
---------    ------
1/0/1        Host
```

3. Display the router advertisement (RA) and redirect (REDIR) messages that were dropped by the IPv6 RA Guard feature.

```
(Netgear Switch) #Show ipv6 snooping counters
IPv6 Dropped Messages
RA(Router Advertisement - ICMP type 134)
REDIR(Router Redirect - ICMP type 137)
RA        Redir
---       -------
0            0
```

17 MAB

MAC Authentication Bypass

This chapter includes the following sections:

- *MAC Authentication Bypass Concepts*
- *Configure MAC Authentication Bypass on a Switch*
- *Configure a Network Policy Server on a Microsoft Windows Server 2008 R2 or Later Server*
- *Configure an Active Directory on a Microsoft Windows Server 2008 R2 or Later Server*
- *Reduce the MAB Authentication Time*

MAC Authentication Bypass Concepts

MAC Authentication Bypass (MAB) provides 802.1X-unaware clients controlled access to the network by using the MAC address of the client device as the identifier.

MAB has the following requirements:

- You must preconfigure the known and allowable MAC addresses and corresponding access rights in the authentication server.
- The port control mode of the port must be MAC-based.

You can configure MAB on a per-port basis. If you configure MAB on a port and the port receives a packet from an unknown MAC address, the following sequence of events can occur:

1. The authenticator sends an EAPOL Request ID packet to the supplicant and the switch starts a timer that is based on the guest VLAN period for the supplicant.
2. If the client does not respond when the timer expires, the switch treats the client as an 802.1X-unaware client.
3. The authenticator sends a request to the authentication server with the MAC address of the client in hhhhhhhhhhhh (nondotted decimal MAC format) format as the user name and the MD5 hash of the MAC address as the password.
4. The authentication server checks its preconfigured database for the authorized MAC addresses and returns either an Access-Accept or Access-Reject message, depending on whether the server can find the MAC address in its database.

   The switch can place the 802.1X-unaware client in a VLAN that is assigned by the RADIUS server or apply a specific filter ID to the client traffic.

MAB initiates only after the 802.1X guest VLAN period times out. If the client responds to any of the EAPOL identity requests, MAB does not initiate for that client. MAB and guest VLANs are mutually exclusive. If you configure a guest VLAN instead of MAB on a port and the 802.1X guest VLAN period times out, the switch places the client in the guest VLAN. If you do not configure a guest VLAN or MAB on a port and the 802.1X guest VLAN period times out, the switch denies the client access.

The following figure illustrates MAB operation.

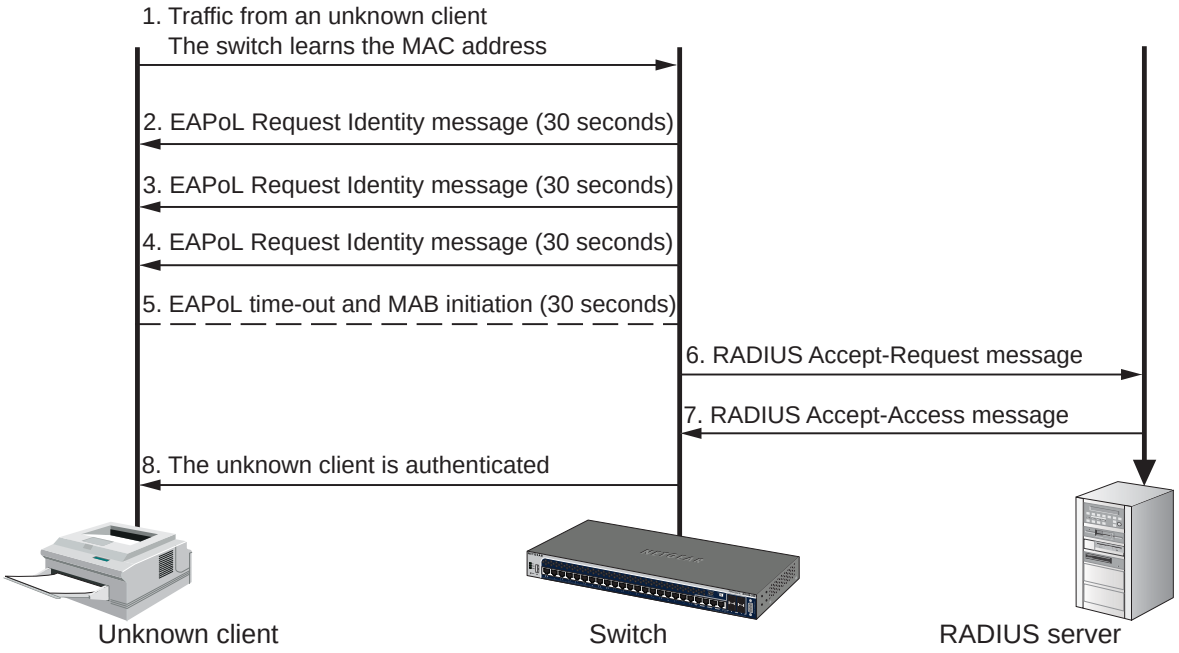


Figure 42. MAB operation

The following figure shows a switch that has MAB configured on port 1/0/1. The IP phone that is connected to this port can access the network after being authenticated successfully by the Microsoft network policy server.

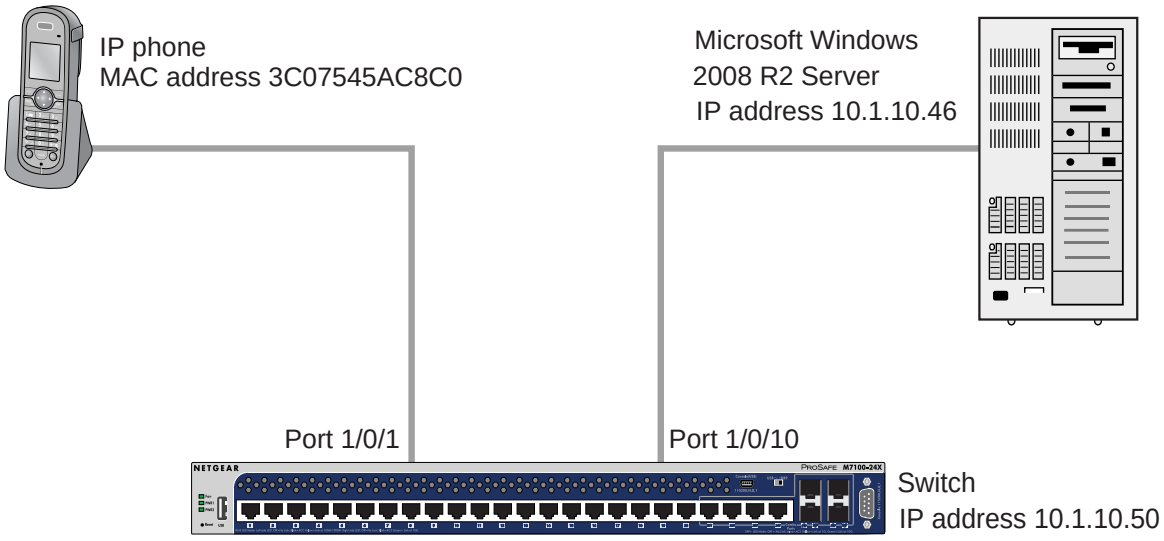


Figure 43. MAB topology with a switch, IP phone, and Microsoft server

Configure MAC Authentication Bypass on a Switch

This section provides an example of how to configure MAC Authentication Bypass (MAB) on a switch. The example is shown as CLI commands and as a web interface procedure.

CLI: Configure the Switch to Perform MAB with a Microsoft Network Policy Server

1. Enable 802.1X authentication on the switch.

```
(Netgear Switch) #config
(Netgear Switch) (Config)#dot1x system-auth-control
```

2. Configure RADIUS to authenticate 802.1X users.

```
 (Netgear Switch) (Config)#aaa authentication dot1x default radius
```

3. Configure the switch to communicate with the Microsoft network policy server.

   In this example, the Microsoft network policy server IP address is 10.1.10.46. The shared key on the switch and the RADIUS server must match.

```
(Netgear Switch) (Config)#radius server host auth 10.1.10.46
(Netgear Switch) (Config)#radius server key auth 10.1.10.46
 Enter secret (64 characters max):******
 Re-enter secret:******
(Netgear Switch) (Config)#radius server primary 10.1.10.46
```

4. Configure force-authorization on the port that connects to the Microsoft network policy server (port 1/0/1 in this example).

```
(Netgear Switch) (Config)#interface 1/0/1
(Netgear Switch) (Interface 1/0/1)#dot1x port-control force-authorized
(Netgear Switch) (Interface 1/0/1)#exit
```

5. Configure MAB on the port that connects to the IP phone (port 1/0/10 in this example).

```
(Netgear Switch) #config
(Netgear Switch) (Config)#interface 1/0/10
(Netgear Switch) (Interface 1/0/10)#dot1x port-control mac-based
(Netgear Switch) (Interface 1/0/10)#dot1x mac-auth-bypass
(Netgear Switch) (Interface 1/0/10)#exit
(Netgear Switch) (config)#exit
```

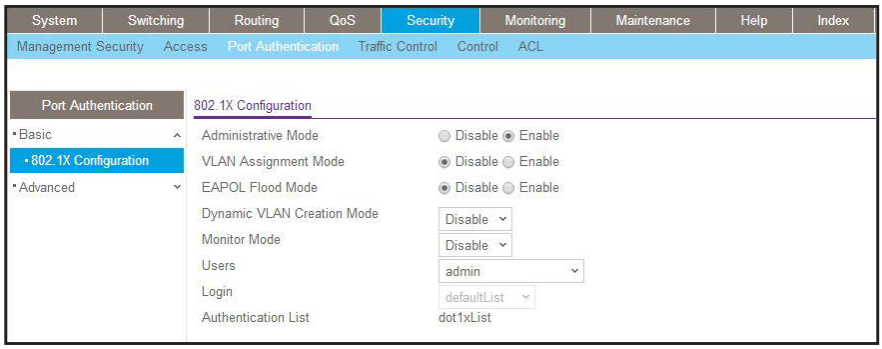
6. To reduce the MAB authentication time, decrease the time of guest VLAN period.

```
(Netgear Switch) #config
(Netgear Switch) (Config)#interface 1/0/10
(Netgear Switch) (Interface 1/0/10)#dot1x timeout guest-vlan-period 1
```

Web Interface: Configure the Switch to Perform MAB with a Microsoft Network Policy Server

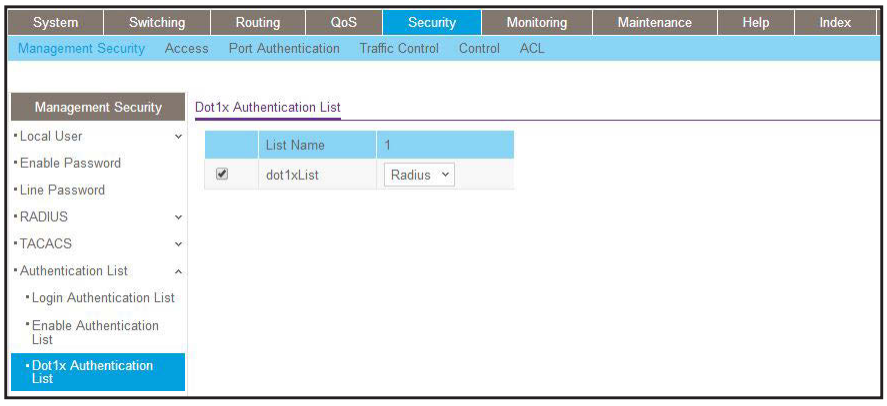
1. Enable 802.1X authentication on the switch:
   a. Select **Security > Port Authentication > Basic > 802.1X Configuration**.

      A screen similar to the following displays.



   b. Under 802.1X Configuration, next to Administrative Mode, select the **Enable** radio button.
   c. Click **Apply**.
2. Configure RADIUS to authenticate 802.1X users:
   a. Select **Security > Management Security > Authentication List > Dot1x Authentication List**.

      A screen similar to the following displays.



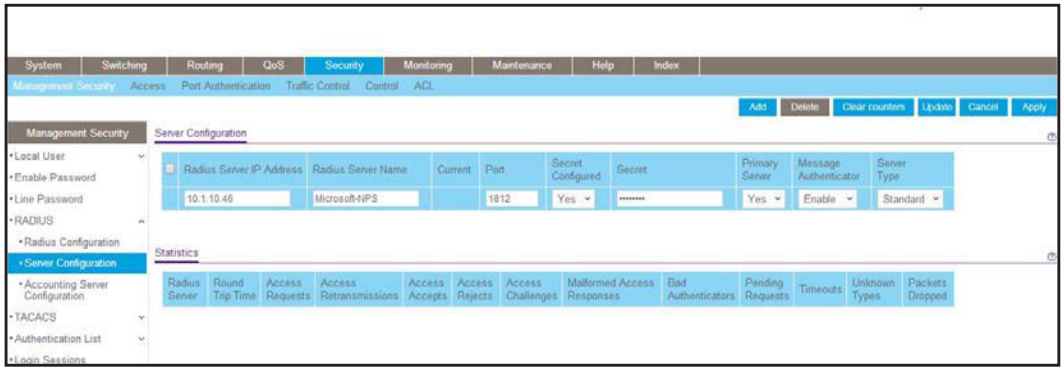
   b. Select the **dot1xList** check box.
   c. From the 1 menu, select **Radius**.
   d. Click **Apply**.

3. Configure the switch to communicate with the Microsoft network policy server.

   In this example, the IP address of the Microsoft network policy server is 10.1.10.46. The shared key between the switch and the server must match.

   a. Select **Security > Management Security > RADIUS > Server Configuration**.

      A screen similar to the following displays.



   b. Configure the following settings:

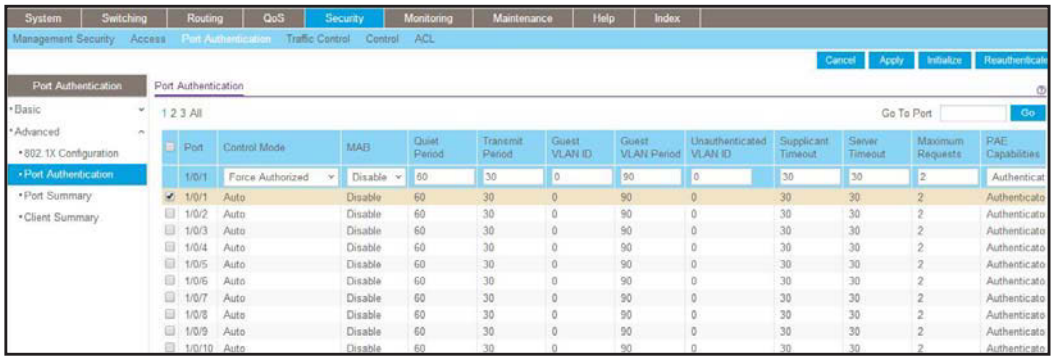
      - In the RADIUS Server IP Address field, enter **10.1.10.46**.
      - In the RADIUS Server Name field, enter **Microsoft-NPS.**
      - In the Port field, enter **1812.**
      - From the Secret Configured menu, select **Yes**.
      - In the Secret field, enter the secret key.
      - From the **Primary Server** menu, select **Yes**.
      - From the Message Authenticator menu, select **Enable**.
      - From the Server Type menu, select **Standard**.

   c. Click **Add**.

4. Configure the port that connects to the Microsoft network policy server (in this example, port 1/0/1) to be force-authorized:

   a. Select **Security > Port Authentication > Advance > Port Authentication**.

      A screen similar to the following displays.



   b. Select the check box that corresponds to port 0/1.

The table heading displays the information for port 0/1.

c. Configure the following settings:
   - From the Control Mode menu, select **Force Authorized**.
   - From the MAB menu, select **Disable**.

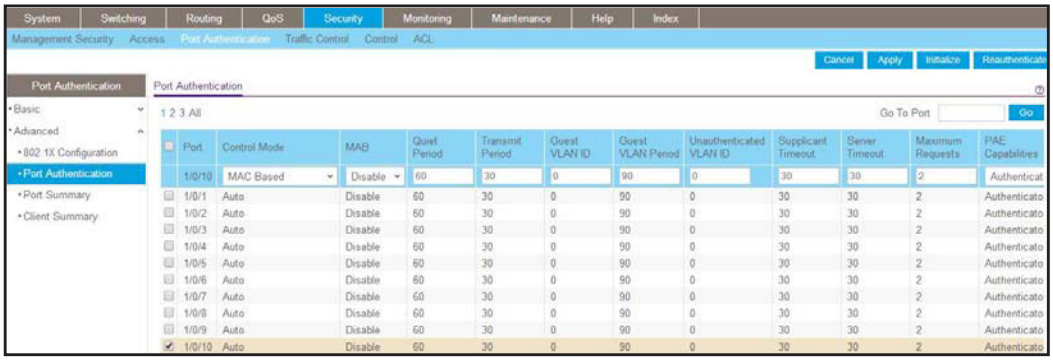
     Leave all other settings on the screen at their default value.

d. Click **Apply**.

5. Configure the port that connects to the IP phone (in this example, port 1/0/10) for MAB:

a. Select **Security > Port Authentication > Advance > Port Authentication**.

A screen similar to the following displays.



b. Select the check box that corresponds to port 0/10.

The table heading displays the information for port 0/10.

c. Configure the following settings:
   - From the Control Mode menu, select **MAC Based**.
   - From the MAB menu, select **Enable**.

     Leave all other settings on the screen at their default value.

d. Click **Apply**.

Note: For information about how to reduce the MAB authentication time, see *Reduce the MAB Authentication Time* on page 390.

Configure a Network Policy Server on a Microsoft Windows Server 2008 R2 or Later Server

1. Enable EAP-MD5 support.

   WARNING:

   Serious problems can occur if you modify the registry incorrectly by using the Registry Editor or by using another method. These problems might require that you reinstall your Microsoft operating system. Modify the registry at your own risk.

   To reenable EAP-MD5 support in Microsoft Windows Vista, add the following registry entries:

   ```
   HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\RasMan\PPP\EAP\4

   Value name: RolesSupported
   Value type: REG_DWORD
   Value data: 0000000a

   Value name: FriendlyName
   Value type: REG_SZ
   Value data: MD5-Challenge

   Value name: Path
   Value type: REG_EXPAND_SZ
   Value data: %SystemRoot%\System32\Raschap.dll

   Value name: InvokeUsernameDialog
   Value type: REG_DWORD
   Value data: 00000001

   Value name: InvokePasswordDialog
   Value type: REG_DWORD
   Value data: 00000001
   ```

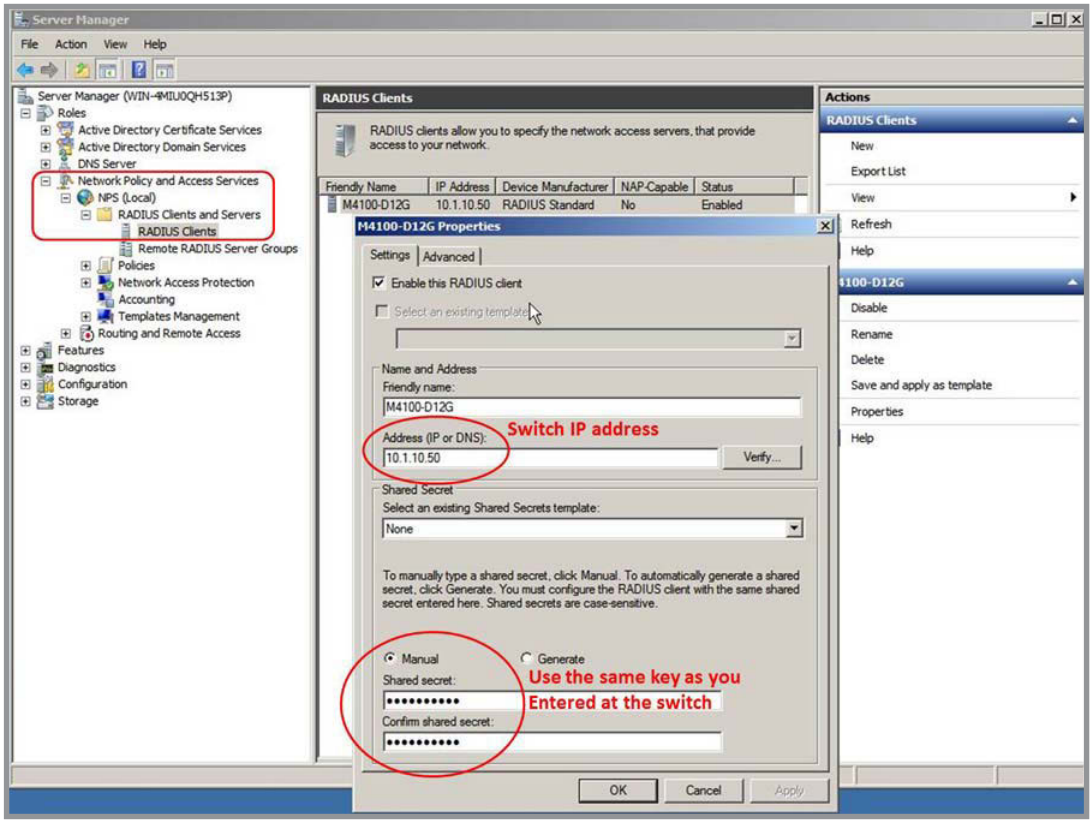
2. If your Windows server 2008 R2 does not have service pack 1 installed, download and install Microsoft hot fix KB981190 from the following Microsoft website:

   http://support.microsoft.com/kb/981190.

3. On the Windows server 2008 R2, configure the RADIUS client:

   a. Click **Network Policy and Access Services > NPS > RADIUS Clients and Servers > RADIUS Clients**.

      The server manager starts.



b. Configure the following settings:

- In the Friendly name field, enter the switch name (in this example, enter **M4100-D12G**).
- In the Address (IP or DNS) field, enter the IP address of the switch that connects to the network policy server (in this example, enter **10.1.10.50**.
- In the Shared secret field and Confirm shared secret field, enter the secret key.

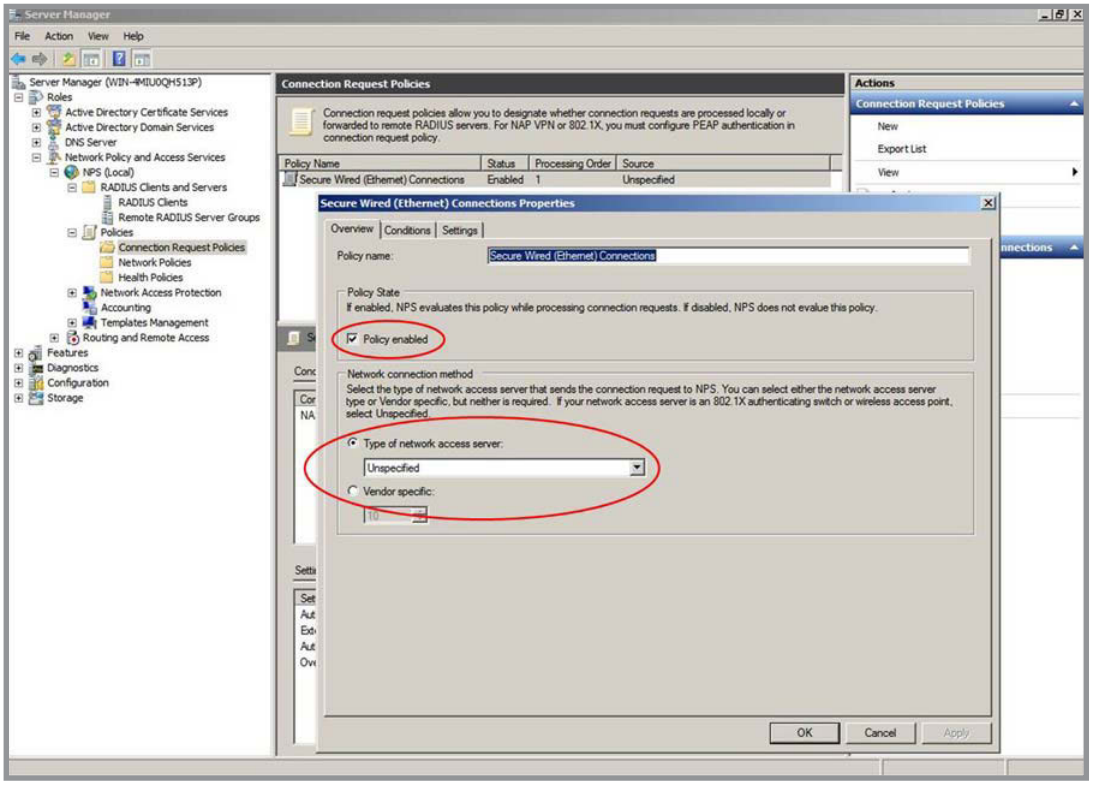
  The shared key between the switch and the server must match.

4. Configure the connection request policies for the network policy server:

   a. Click **Network Policy and Access Services > NPS > Policies > Connection Request Policies**.

   b. Double-click **Secured Wired (Ethernet) Connections**.

   The Secure Wired (Ethernet) Connections Properties pop-up screen displays with the Overview tab selected:



c. Select the **Policy enabled** check box.

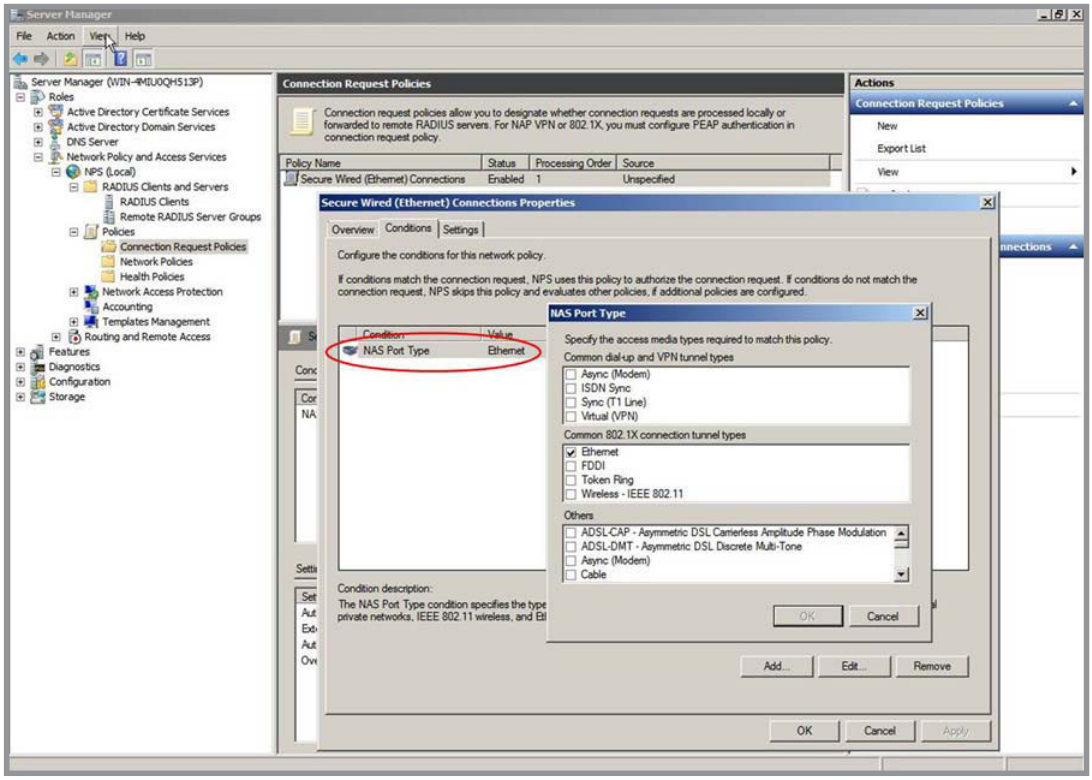
d. From the Type of network access server menu, select **Unspecified**.

Leave the Vendor specific radio button cleared.

e. Click the **Apply** button.

f. Click the **Conditions** tab.

The screen adjusts.

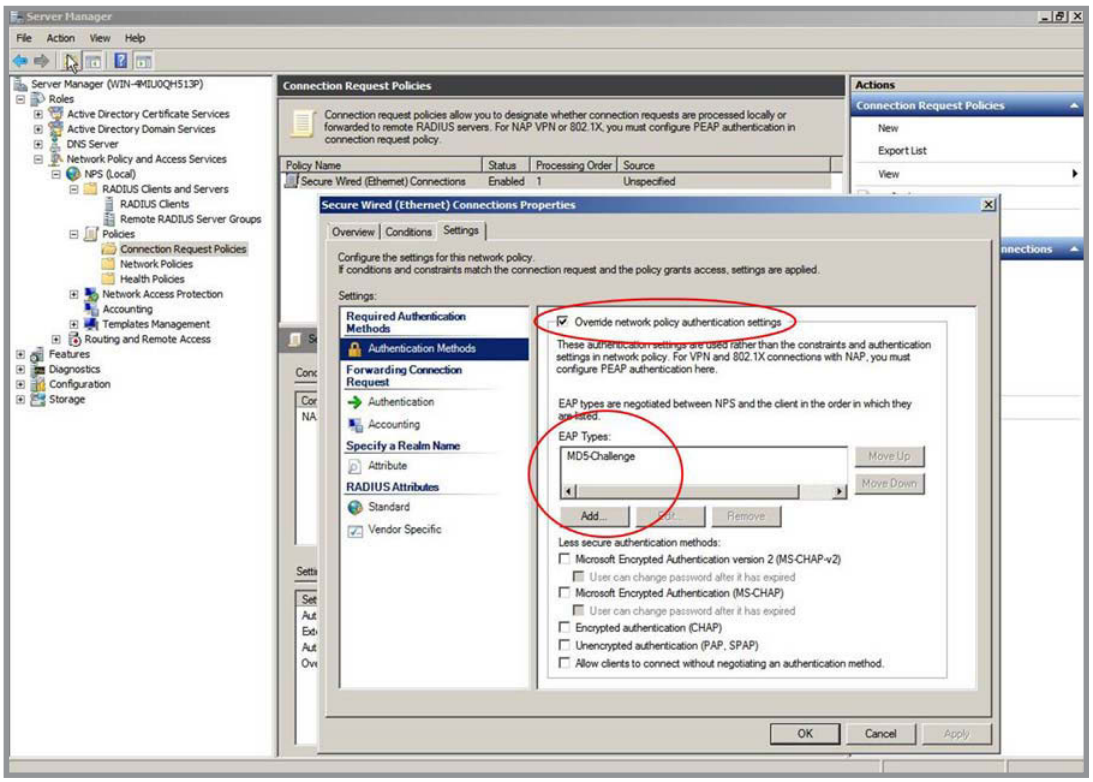


g. Configure the NAS Port Type field as Ethernet.

h. Click the **Apply** button.

i. Click the **Settings** tab.

The screen adjusts.



j. Select the **Override Network policy authentication settings** check box.

k. Under the EAP Types field, click the **Add** button.

l. From the menu, select **MD5-Challenge**.

m. Click the **OK** button.

MD5-Challenge is added to the EAP Types field.

n. From the EAP Types field, select **MD5-Challenge**.

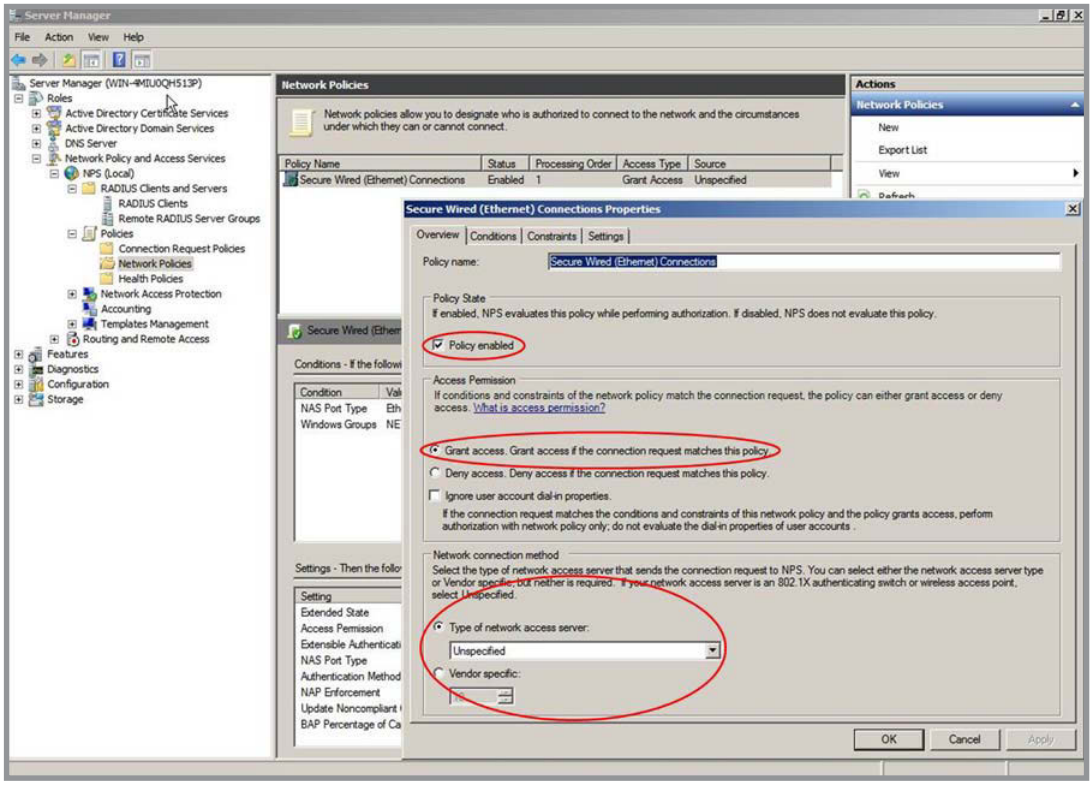
o. Click the **Apply** button.

5. Configure the network policies for the network policy server:

a. Click **Network Policy and Access Services > NPS > Policies > Network Policies**.

b. Double-click **Secured Wired (Ethernet) Connections**.

The Secure Wired (Ethernet) Connections Properties pop-up screen displays with the Overview tab selected:



c. Select the **Policy enabled** check box.

d. Select the **Grant access** radio button.

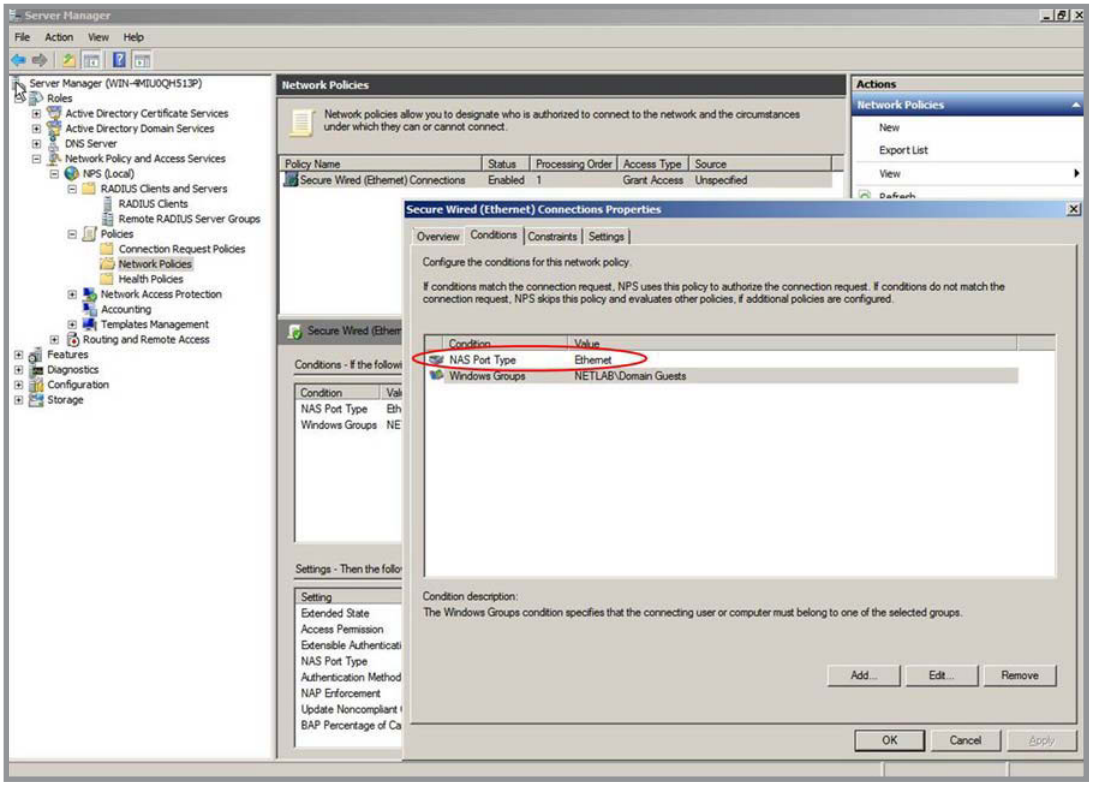
e. From the Type of network access server menu, select **Unspecified**.

Leave the Vendor specific radio button cleared.

f. Click the **Apply** button.

g. Click the **Conditions** tab.

The screen adjusts.

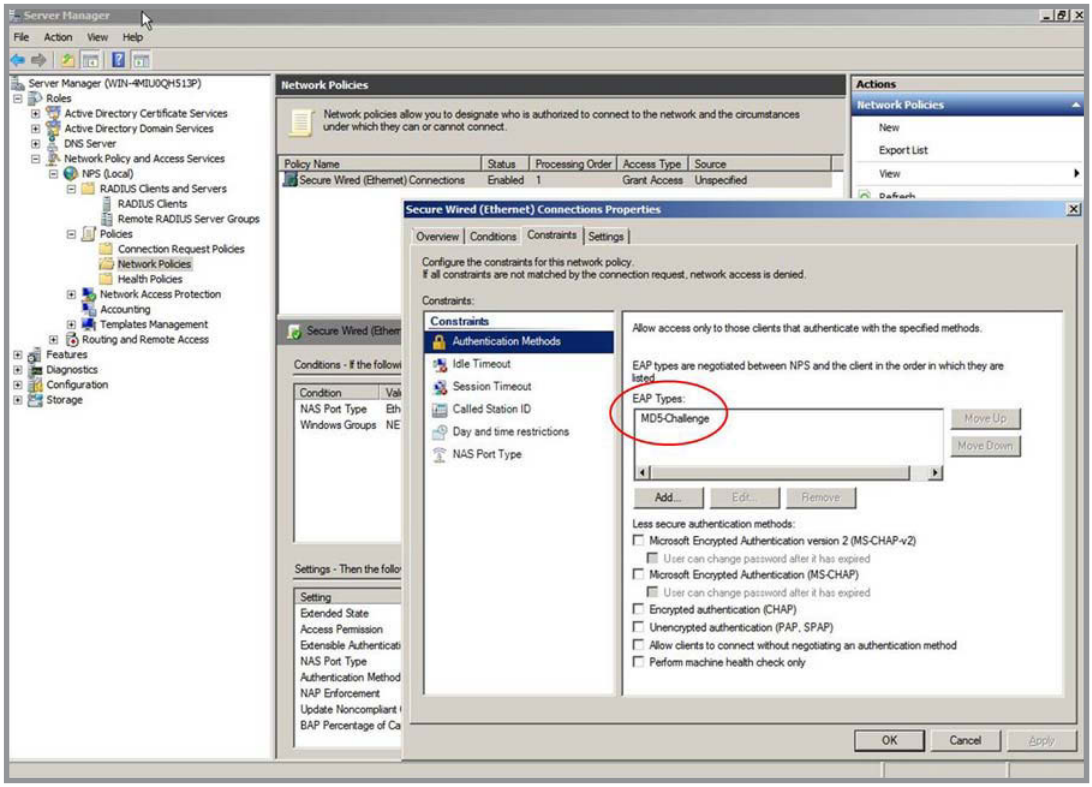


h. Configure the NAS Port Type field as Ethernet.

i. Click the **Apply** button.

j. Click the **Constraints** tab.

The screen adjusts.



k. Under the EAP Types field, click the **Add** button.

l. From the menu, select **MD5-Challenge**.

m. Click the **OK** button.

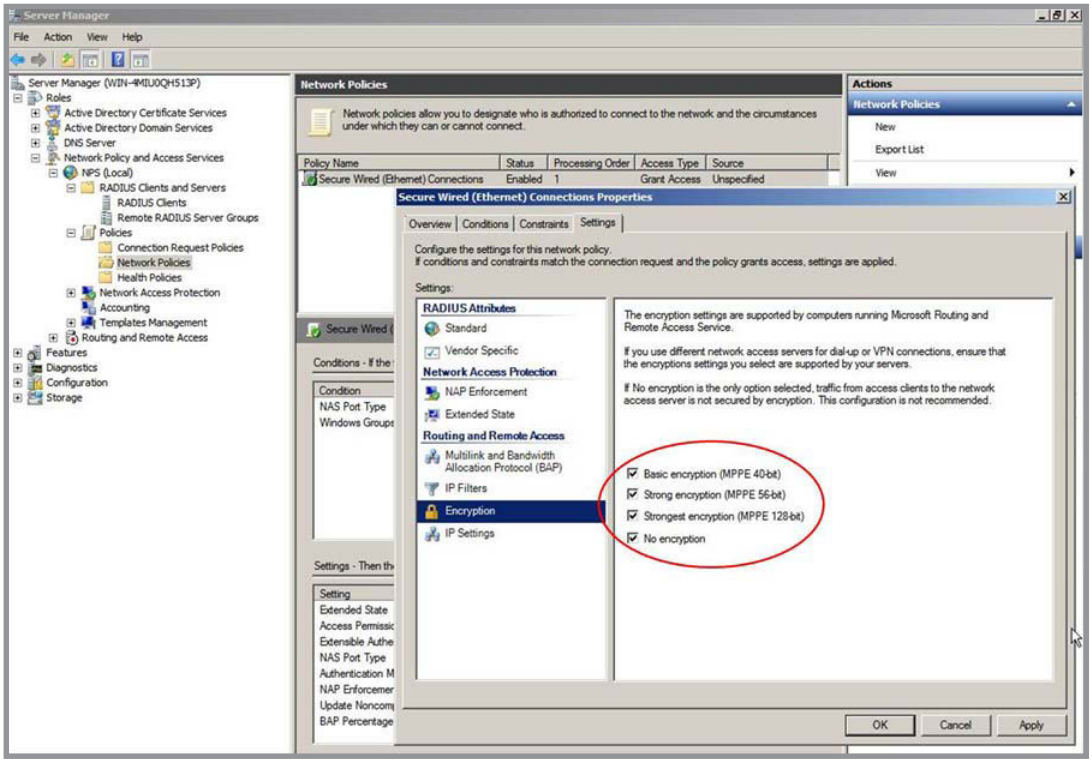
MD5-Challenge is added to the EAP Types field.

n. From the EAP Types field, select **MD5-Challenge**.

o. Click the **Apply** button.

p. Click the **Settings** tab.

The screen adjusts.

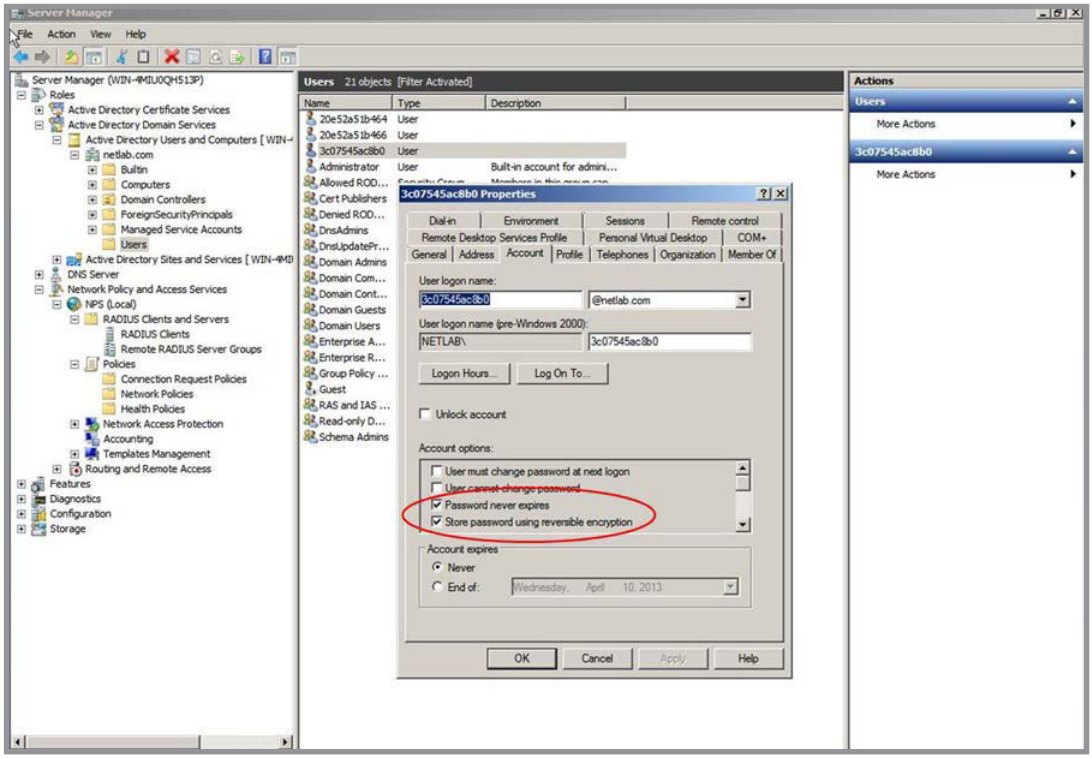


q. Select all four encryption check boxes, including the **No encryption** check box.

r. Click the **Apply** button.

Configure an Active Directory on a Microsoft Windows Server 2008 R2 or Later Server

1. Create a user account with the following settings:
   - **Logon name**. The MAC address of the device for which you want to allow a connection.
   - **Password**. Any temporary password.
2. Right-click the new user account name and select **Properties**.



3. Select the **Password never expires** check box.
4. Select the **Store password using reversible encryption** check box.
5. Click the **Apply** button.
6. Create a Password Settings Object (PSO) as described at the following Microsoft website:

   http://technet.microsoft.com/en-us/library/cc754461(v=ws.10).aspx.

   Use the default setting for all the attributes except for the following setting: msDS-PasswordComplexityEnabled = FALSE.
7. Apply PSO to the user account that you created in *Step 1*, as described at the following Microsoft website:

   http://technet.microsoft.com/en-us/library/cc731589(v=ws.10).aspx#BKMK_1.
8. Change the password for the user account that you created in *Step 1*.

   For the password, use the MAC address of the device for which you want to allow a connection, and use uppercase letters only.

Reduce the MAB Authentication Time

MAB waits for the expiration of the guest VLAN period before MAB sends a request to the authentication server with the MAC address as the user name and the MD5 hash as the password. To reduce the MAB authentication time, decrease the guest VLAN period. The default period for the guest VLAN period is 90 seconds.

CLI: Reduce the Authentication Time for MAB

Change the guest VLAN period timer to 10 seconds using the CLI:

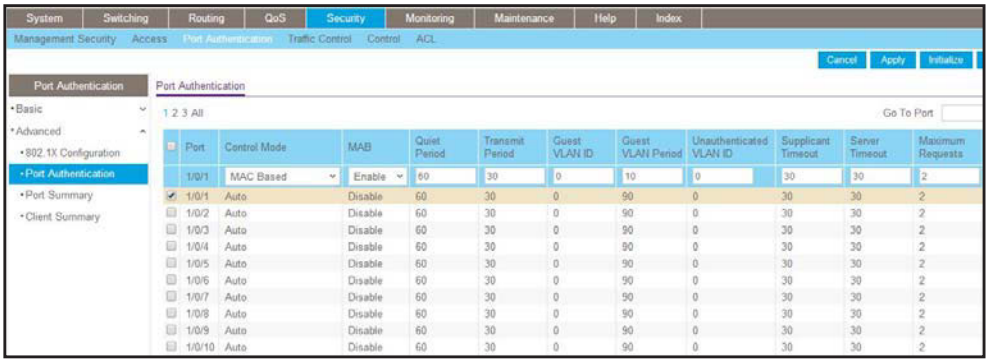
```
(Netgear Switch) #config
(Netgear Switch) (Config)# interface 1/0/1
(Netgear Switch) (Interface 1/0/1)#dot1x timeout guest-vlan-period 10
```

Web Interface: Reduce the Authentication Time for MAB

Change the guest VLAN period timer to 10 seconds using the web interface:

1. Select **Security > Port Authentication > Advanced > Port Authentication**.

   A screen similar to the following displays.



2. Select the check box that corresponds to port 0/1.

   The table heading displays the information for port 0/1.

3. In the Guest VLAN Period field, enter **10**

   Leave the other settings on the screen at the default value.

4. Click **Apply**.

SNTP

18

Simple Network Time Protocol

This chapter includes the following sections:

- *Simple Network Time Protocol Concepts*
- *Show SNTP (CLI Only)*
- *Configure SNTP*
- *Set the Time Zone (CLI Only)*
- *Set the Named SNTP Server*

Simple Network Time Protocol Concepts

Simple Network Time Protocol (SNTP) offers the following benefits:

- It can be used to synchronize network resources and for adaptation of NTP.
- SNTP provides synchronized network timestamp.
- It can be used in broadcast or unicast mode.
- It supports SNTP client implemented over UDP, which listens on port 123.

Show SNTP (CLI Only)

The following are examples of the commands used in the SNTP feature.

show sntp

```
(Netgear Switch) #show sntp?

<cr>      Press Enter to execute the command.
client    Display SNTP Client Information.
server    Display SNTP Server Information.
```

show sntp client

```
(Netgear Switch) #show sntp client

Client Supported Modes:    unicast broadcast
SNTP Version:              4
Port:                      123
Client Mode:               unicast
Unicast Poll Interval:     6
Poll Timeout (seconds):    5
Poll Retry:                1
```

show sntp server

```
(Netgear Switch) #show sntp server

Server IP Address:          81.169.155.234
Server Type:                ipv4
Server Stratum:             3
Server Reference Id:        NTP Srv: 212.186.110.32
Server Mode:                Server
Server Maximum Entries:     3
Server Current Entries:     1

SNTP Servers
------------

IP Address:                  81.169.155.234
Address Type:                IPV4
Priority:                    1
Version:                     4
Port:                        123
Last Update Time:            MAY 18 04:59:13 2005
Last Attempt Time:           MAY 18 11:59:33 2005
Last Update Status:          Other
Total Unicast Requests:      1111
Failed Unicast Requests:     361
```

Configure SNTP

The example is shown as CLI commands and as a web interface procedure.

CLI: Configure SNTP

NETGEAR switches do not have a built-in real-time clock. However, it is possible to use SNTP to get the time from a public SNTP/NTP server over the Internet. You may need permission from those public time servers. The following steps configure SNTP on the switch:

1. Configure the SNTP server IP address.

   The IP address can be either from the public NTP server or your own. You can search the Internet to locate the public server. The servers available could be listed in domain-name format instead of address format. In that case, use the `ping` command on the PC to find the server's IP address. The following example configures the SNTP server IP address to 208.14.208.19.

```
(Netgear Switch) (Config)#sntp server 208.14.208.19
```

2. After configuring the IP address, enable SNTP client mode.

   The client mode can be either broadcast mode or unicast mode. If the NTP server is not your own, you must use unicast mode.

```
(Netgear Switch) (Config)#sntp client mode unicast
```

   When the SNTP client mode is enabled, the client waits for the polling interval to send the query to the server. The default value is approximately 1 minute.

3. After this period, issue the show command to confirm that the time was received.

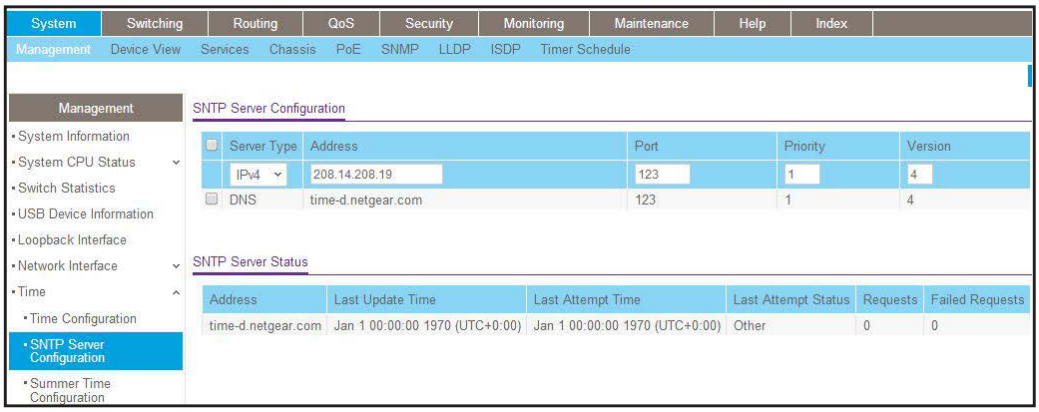
   The time will be used in all logging messages.

```
(Netgear Switch) #show sntp server
Server IP Address:                208.14.208.19
Server Type:                      ipv4
Server Stratum:                   4
Server Reference Id:              NTP Srv: 208.14.208.3
Server Mode:                      Server
Server Maximum Entries:           3
Server Current Entries:           1
SNTP Servers
------------

IP Address: 208.14.208.19
Address Type: IPV4
Priority: 1
Version: 4
Port: 123
Last Update Time: Mar 26 03:36:09 2006
Last Attempt Time: Mar 26 03:36:09 2006
Last Update Status: Success
Total Unicast Requests: 2
Failed Unicast Requests: 0
```

Web Interface: Configure SNTP

1. Configure the SNTP server.
   a. Select **System > Management >Time > SNTP Server Configuration**.

      A screen similar to the following displays.

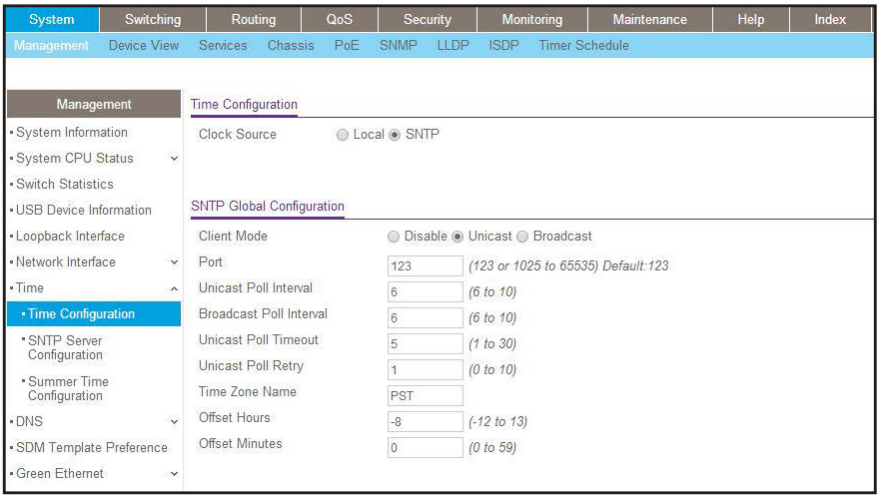


   b. Enter the following information:
      - In the **Server Type** field, select **IPV4**.
      - In the **Address** field, enter **208.14.208.19**.
      - In the **Port** field, enter **123**.
      - In the **Priority** field, enter **1**.
      - In the **Version** field, enter **4**.

   c. Click **Add**.

2. Configure SNTP globally.
   a. Select **System > Management > Time > SNTP Global Configuration**.

      A screen similar to the following displays.



b. Enter the following information:
   - For Client Mode, Select the **Unicast** radio button.
   - In the **Time Zone Name** field, enter **PST**.
   - In the **Offset Hours** field, enter **-8**.

c. Click **Apply**.

Set the Time Zone (CLI Only)

The SNTP/NTP server is set to Coordinated Universal Time (UTC) by default. The following example shows how to set the time zone to Pacific Standard Time (PST), which is 8 hours behind GMT/UTC.

```
(Netgear switch)(config)#clock timezone PST -8
```

Set the Named SNTP Server

The example is shown as CLI commands and as a web interface procedure.

CLI: Set the Named SNTP Server

NETGEAR provides SNTP servers accessible by NETGEAR devices. Because NETGEAR might change IP addresses assigned to its time servers, it is best to access an SNTP server by DNS name instead of using a hard-coded IP address. The public time servers available are time-a, time-b, and time-c.

Enable a DNS name server and access a time server with the following commands:

```
(Netgear switch) (config)#ip domain-lookup
(Netgear switch) (config)#ip name-server 192.168.1.1
(Netgear switch) (config)#sntp server time-a.netgear.com
```

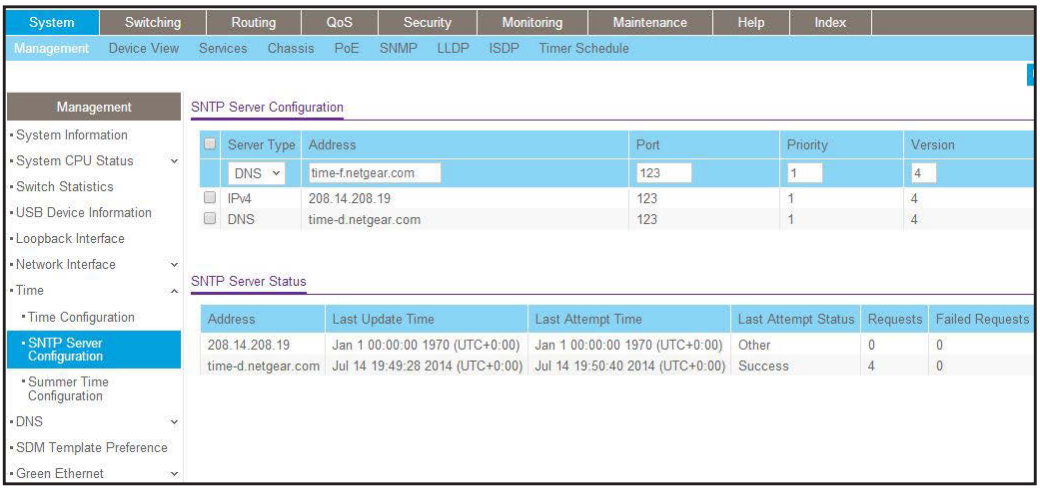
where *192.168.1.1* is the public network gateway IP address for your device.

This method of setting DNS name look-up can be used for any other applications that require a public IP address, for example, a RADIUS server.

Web Interface: Set the Named SNTP Server

1. Configure the SNTP server.
   a. Select **System > Management > Time > SNTP Server Configuration**.

      A screen similar to the following displays.

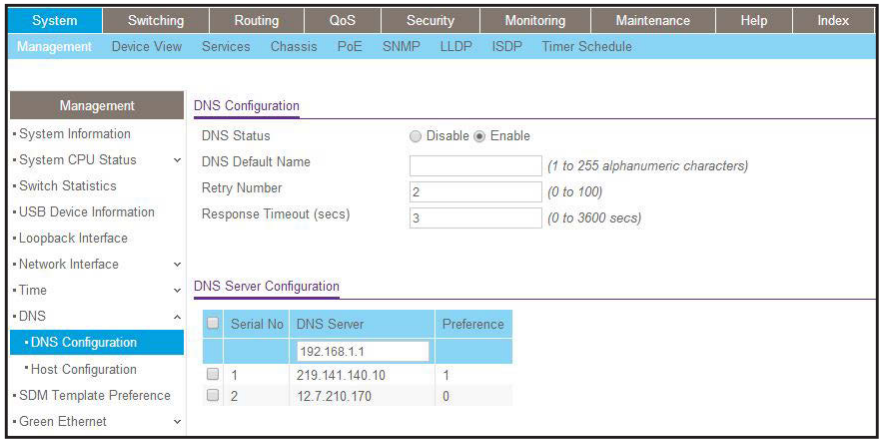


   b. Enter the following information:
      - In the **Server Type** list, select **DNS**.
      - In the **Address** field, enter **time-f.netgear.com**
      - In the **Port** field, enter **123**.
      - In the **Priority** field, enter **1**.
      - In the **Version** field, enter **4**.

   c. Click **Add**.

2. Configure the DNS server.
   a. Select **System > Management > DNS > DNS Configuration**.

      A screen similar to the following displays.



b. Enter the following information:

- For DNS Status, select the **Enable** radio button
- In the **DNS Server** field, enter **192.168.1.1**.

c. Click **Add**.

Tools

19

Tools to manage, monitor, and personalize the switch and network

This chapter includes the following sections:

- *Traceroute*
- *Configuration Scripting*
- *Pre-Login Banner*
- *Port Mirroring*
- *Remote SPAN*
- *Dual Image*
- *Outbound Telnet*
- *Error Disablement and Automatic Error Recovery*
- *Loop Protection*
- *Nondisruptive Configuration Management*
- *Full Memory Dump*

Traceroute

This section describes the traceroute feature. Use traceroute to discover routes that packets take when traveling on a hop-by-hop basis to their destination through the network.

- Traceroute maps network routes by sending packets with small time-to-live (TTL) values and watches the ICMP time-out announcements.
- The traceroute command displays all L3 devices.
- It can be used to detect issues on the network.
- Traceroute tracks up to 20 hops.
- The default UPD port is used 33343 unless you specify otherwise in the `traceroute` command.

The following shows an example of using the `traceroute` command to determine how many hops there are to the destination. The command output shows each IP address that the packet passes through and how long it takes for the packet to reach its destination. In this example, the packet takes 16 hops to reach its destination.

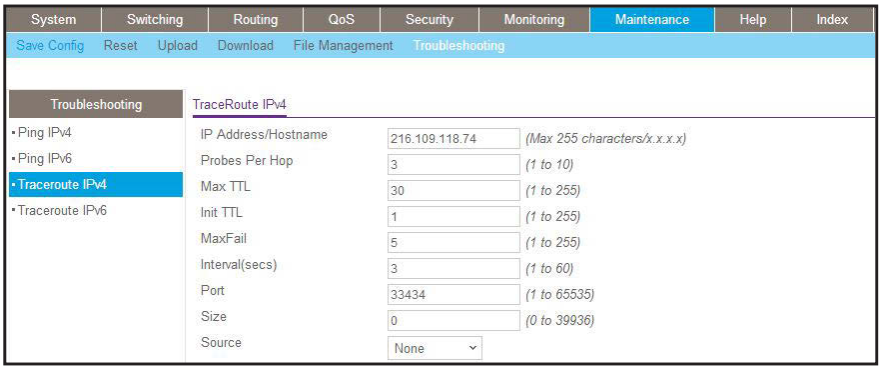
CLI: Traceroute

```
(Netgear Switch) #traceroute?
<ipaddr>      Enter IP address.

(Netgear Switch) #traceroute 216.109.118.74 ?
<cr>    Press Enter to execute the command.
<port>        Enter port no.

(Netgear Switch) #traceroute 216.109.118.74
tracing route over a maximum of 20 hops
 1  10.254.24.1        40 ms       9 ms      10 ms
 2  10.254.253.1       30 ms      49 ms      21 ms
 3  63.237.23.33       29 ms      10 ms      10 ms
 4  63.144.4.1         39 ms      63 ms      67 ms
 5  63.144.1.141       70 ms      50 ms      50 ms
 6  205.171.21.89      39 ms      70 ms      50 ms
 7  205.171.8.154      70 ms      50 ms      70 ms
 8  205.171.8.222      70 ms      50 ms      80 ms
 9  205.171.251.34     60 ms      90 ms      50 ms
10  209.244.219.181    60 ms      70 ms      70 ms
11  209.244.11.9       60 ms      60 ms      50 ms
12  4.68.121.146       50 ms      70 ms      60 ms
13  4.79.228.2         60 ms      60 ms      60 ms
14  216.115.96.185    110 ms      59 ms      70 ms
15  216.109.120.203    70 ms      66 ms      95 ms
16  216.109.118.74     78 ms     121 ms      69 ms
```

Web Interface: Traceroute

1. Select **Maintenance > Troubleshooting > Traceroute**.

   A screen similar to the following displays.



   Use this screen to specify that the switch must discover the routes that packets actually take when traveling to their destination through the network on a hop-by-hop basis. Once you click the Apply button, the switch sends three traceroute packets to each hop and the results are displayed in the result table.

2. In the **IP Address/Hostname** field, enter **216.109.118.74**.
3. Click the **Apply** button.

   Your settings are saved.

Configuration Scripting

This section provides the following examples:

- *script Command*
- *script list Command and script delete Command*
- *script apply running-config.scr Command*
- *Create a Configuration Script*
- *Upload a Configuration Script*

Configuration scripting:

- Allows you to generate text-formatted files.
- Provides scripts that can be uploaded and downloaded to the system.
- Provides flexibility to create command configuration scripts.
- Can be applied to several switches.
- Can save up to 10 scripts or 500 K of memory.
- Provides script format of one CLI command per line.

Consider the following:

- The total number of scripts stored is limited by the NVRAM/FLASH size.
- Application of scripts is partial if a script fails. For example, if the script executes 5 of 10 commands and the script fails, the script stops at 5.
- Scripts cannot be modified or deleted while being applied.
- Validation of scripts checks for syntax errors only. It does not validate that the script will run successfully.

script Command

```
(Netgear Switch) #script ?

apply       Applies configuration script to the switch.
delete      Deletes a configuration script file from the switch.
list        Lists all configuration script files present on the switch.
show        Displays the contents of configuration script.
validate    Validate the commands of configuration script.
```

script list Command and script delete Command

```
(Netgear Switch) #script list

Configuration Script Name        Size(Bytes)
-------------------------        -----------
basic.scr                        93
running-config.scr               3201

2 configuration script(s) found.
1020706 bytes free.

(Netgear Switch) #script delete basic.scr

Are you sure you want to delete the configuration script(s)? (y/n) y

1 configuration script(s) deleted.
```

script apply running-config.scr Command

```
(Netgear Switch) #script apply running-config.scr

Are you sure you want to apply the configuration script? (y/n) y

The system has unsaved changes.
Would you like to save them now? (y/n) y

Configuration Saved!
```

Create a Configuration Script

```
(Netgear Switch) #show running-config running-config.scr

Config script created successfully.

(Netgear Switch)                    #script list

Configuration Script Name        Size(Bytes)
-------------------------        ----------
running-config.scr               3201

1 configuration script(s) found.
1020799 bytes free.
```

Upload a Configuration Script

```
(Netgear Switch) #copy nvram: script running-config.scr
tftp://192.168.77.52/running-config.scr

Mode.........................        TFTP
Set TFTP Server IP...........        192.168.77.52
TFTP Path....................        ./
TFTP Filename................        running-config.scr
Data Type....................        Config Script
Source Filename..............        running-config.scr

Are you sure you want to start? (y/n) y

File transfer operation completed successfully.
```

Pre-Login Banner

Pre-login banner:

- Allows you to create message screens that display when a user logs in to the CLI.
- By default, no banner file exists.
- You can upload or download.
- File size cannot be larger than 2 K.

The Pre-Login Banner feature is only for the CLI interface.

Create a Pre-Login Banner

This command is provided for the CLI only.

1. On your computer, use Notepad to create a banner.txt file that contains the banner to be displayed.

```
Login Banner - Unauthorized access is punishable by law.
```

2. Transfer the file from the PC to the switch using TFTP.

```
(Netgear Switch) #copy tftp://192.168.77.52/banner.txt nvram:clibanner

Mode........................................... TFTP
Set TFTP Server IP............................. 192.168.77.52
TFTP Path...................................... ./
TFTP Filename.................................. banner.txt
Data Type...................................... Cli Banner

Are you sure you want to start? (y/n) y

CLI Banner file transfer operation completed successfully!

(Netgear Switch) #exit

(Netgear Switch) >logout

Login Banner - Unauthorized access is punishable by law.
User:
```

Note: The `no clibanner` command removes the banner from the switch.

Port Mirroring

The port mirroring feature:

- Allows you to monitor network traffic with an external network analyzer.
- Forwards a copy of each incoming and outgoing packet to a specific port.
- Is used as a diagnostic tool, debugging feature, or means of fending off attacks.
- Assigns a specific port to copy all packets to.
- Allows inbound or outbound packets to switch to their destination and to be copied to the mirrored port.

The example is shown as CLI commands and as a web interface procedure.

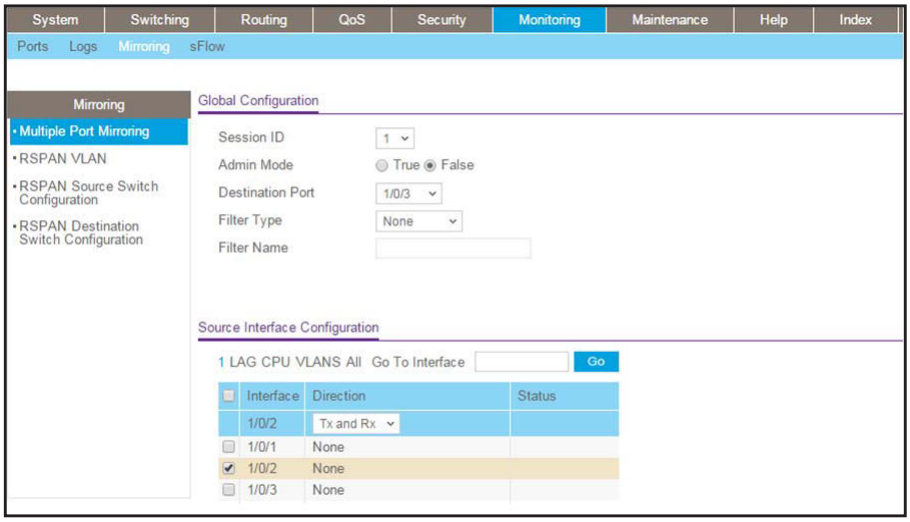
CLI: Specify the Source (Mirrored) Ports and Destination (Probe)

```
(Netgear Switch)#config
(Netgear Switch)(Config)#monitor session 1 mode
Enable mirror
(Netgear Switch)(Config)#monitor session 1 source interface 1/0/2
Specify the source interface.
(Netgear Switch)(Config)#monitor session 1 destination interface 1/0/3
Specify the destination interface.
(Netgear Switch)(Config)#exit
(Netgear Switch)#show monitor session 1
Session ID     Admin Mode    Probe Port    Mirrored Port
-------------      ---------------     -------------    ----------------
      1                      Enable              1/0/3             1/0/2
```

Web Interface: Specify the Source (Mirrored) Ports and Destination (Probe)

1. Select **Monitoring > Mirroring > Port Mirroring**.

   A screen similar to the following displays.



2. Next to **Admin Mode** field, select the **True** radio button.
3. From the **Destination Port** menu, select **1/0/3.**
4. Scroll down and select the check box to the left of interface **1/0/2**.

   1/0/2 displays in the Interface field of the table heading.

5. Click the **Apply** button.

   Your settings are saved.

Remote SPAN

Mirroring lets you monitor traffic to and from a port by copying the traffic to a probe port for analysis. Mirroring is usually limited to on one switch. With a remote switched port analyzer (RSPAN), you can extend mirroring to all participating switches.

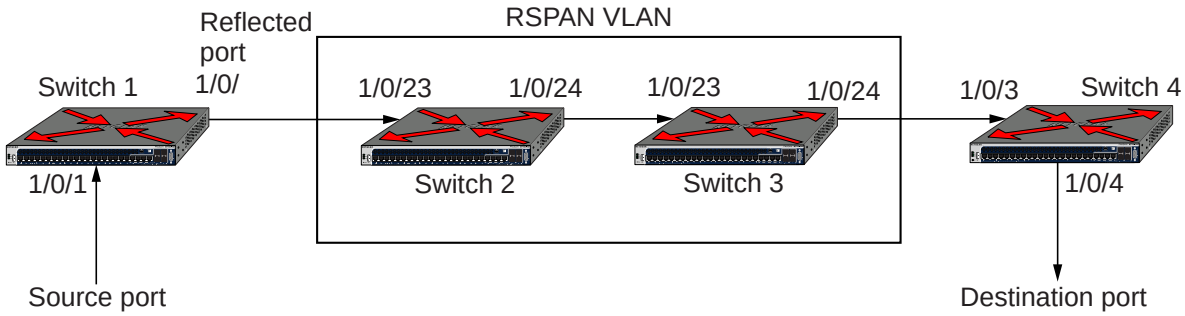


Figure 44. Example of an RSPAN topology

In the previous figure, Switch 1 is the source switch, Switch 2 and Switch 3 are intermediate switches, and Switch 4 is the destination switch.

You must configure the ports that are connected to the destination switch with tagging, with the VLAN ID as the RSPAN VLAN. You must also configure the ports on the intermediate switches that are connected to the source switch and destination switch with the RSPAN VLAN. Only one RSPAN VLAN is supported.

On the source switch, the traffic that is received on and transmitted from source port (1/0/1) is tagged with the RSPAN VLAN and transmitted on the configured reflector port. The reflector port (1/0/2) is the physical interface that carries the mirrored traffic to the destination switch.

The intermediate switches forward the incoming tagged traffic to the destination switch. Enable RSPAN VLAN egress tagging on the ports of the intermediate switches that are connected to the destination switch.

The destination switch accepts all the packets that are tagged with the RSPAN VLAN and mirrors the packets on the destination port to which you must connect a traffic analyzer.

The original tag is retained at the destination switch. Mirrored traffic has double tagging: The inner tag is the original VLAN ID and the outer tag is the RSPAN VLAN ID.

CLI: Enable RSPAN on a Switch

1. On the source switch (Switch 1), configure the following settings:
   - Source ports (the ports for which the traffic must be mirrored)
   - RSPAN VLAN (the destination for the mirrored traffic)
   - Reflector port (the port that is connected, through the intermediate switches, to the destination switch)
   - Tx/Rx (both egress and ingress traffic must be mirrored)

```
(Netgear Switch) #vlan database
(Netgear Switch) (Vlan)#vlan 5
(Netgear Switch) (Vlan)#exit
(Netgear Switch) #config
(Netgear Switch) (Config)#vlan 5
(Netgear Switch) (Config)(Vlan 5)#remote-span
(Netgear Switch) (Config)(Vlan 5)#exit
(Netgear Switch) (Config)#monitor session 1 mode
(Netgear Switch) (Config)#monitor session 1 source interface 1/0/1
(Netgear Switch) (Config)#monitor session 1 destination remote vlan 5 reflector-port
1/0/2
(Netgear Switch) (Config)#exit
(Netgear Switch) #show monitor session 1
Session Admin   Probe  Src  Mirrored Ref.   Src   Dst   Type  IP      MAC
ID      Mode    Port   VLAN Port     Port   RVLAN RVLAN       ACL     ACL
------- ------- ------ ---- -------- ------ ----- ----- ----- ------- -------
1       Enable              1/0/1    1/0/2        5     Rx,Tx
```

2. On the intermediate switches (Switch 2 and Switch 3), configure the ports that are connected to the source and destination switches as tagged members of the VLAN.

   Note: You do not need to configure RSPAN on the intermediate switches.

```
(Netgear Switch) #vlan database
(Netgear Switch) (Vlan)#vlan 5
(Netgear Switch) (Vlan)#exit
(Netgear Switch) #config
(Netgear Switch) (Config)#interface 1/0/23
(Netgear Switch) (Interface 1/0/23)#vlan participation include 5
(Netgear Switch) (Interface 1/0/23)#vlan tagging 5
(Netgear Switch) (Interface 1/0/23)#exit
(Netgear Switch) (Config)#interface 1/0/24
(Netgear Switch) (Interface 1/0/24)#vlan participation include 5
(Netgear Switch) (Interface 1/0/24)#vlan tagging 5
(Netgear Switch) (Interface 1/0/24)#exit
```

3. On the destination switch (Switch 4), configure the following settings:
   - RSPAN VLAN (the source of the mirrored traffic)
   - The probe port (the port that is connected, through the intermediate switches, to the source switch)

```
(Netgear Switch) #vlan database
(Netgear Switch) (Vlan)#vlan 5
(Netgear Switch) (Vlan)#exit
(Netgear Switch) #config
(Netgear Switch) (Config)#vlan 5
(Netgear Switch) (Config)(Vlan 5)#remote-span
(Netgear Switch) (Config)(Vlan 5)#exit
(Netgear Switch) (Config)#interface 1/0/3
(Netgear Switch) (Interface 1/0/3)#vlan participation include 5
(Netgear Switch) (Interface 1/0/3)#vlan tagging 5
(Netgear Switch) (Interface 1/0/3)#exit
(Netgear Switch) (Config)#monitor session 1 mode
(Netgear Switch) (Config)#monitor session 1 source remote vlan 5
(Netgear Switch) (Config)#monitor session 1 destination interface 1/0/4
(Netgear Switch) #show monitor session 1
Session Admin   Probe  Src  Mirrored Ref.   Src   Dst   Type  IP      MAC
ID      Mode    Port   VLAN Port     Port   RVLAN RVLAN       ACL     ACL
------- ------- ------ ---- -------- ------ ----- ----- ----- ------- -------
1       Enable  1/0/4                      5
```

Dual Image

Traditionally switches contain a single image in the permanent storage. This image is loaded into memory every time there is a reboot. The dual image feature allows switches to have two images in permanent storage. You can denote one of these images as an active image that will be loaded in subsequent reboots and the other image as a backup image. This feature provides for reduced down time for the switches, when the firmware is being upgraded or downgraded.

The images are stored in the file system with the file names *image1* and *image2*. These names are used in the CLI, Web, and SNMP interfaces. Each of the images can be associated with a textual description. The switch provides commands to associate and retrieve the text description for an image. A switch also provides commands to activate the backup image such that it is loaded in subsequent reboots. This activation command makes the current active image as the backup image for subsequent reboots.

On three successive errors executing the **active-image**, the switch attempts to execute the **backup-image**. If there are errors executing the **backup-image** as well, the bootloader will invoke the boot menu.

The Dual Image feature works seamlessly with the stacking feature. All members in the stack must be uniform in their support for the dual Image feature. The Dual Image feature works in the following way in a stack.

- When an image is activated, the management node notifies all the participating nodes. All nodes activate the specified image.

- When any node is unable to execute the **active-image** successfully, it attempts to execute the **backup-image**. Such cases will require user intervention to correct the problem, by using appropriate stacking commands.

CLI: Download a Backup Image and Make It Active

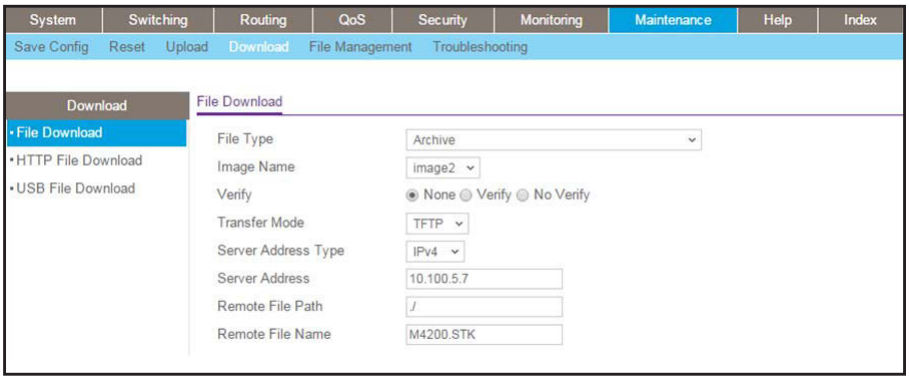
```
(Netgear Switch) #copy tftp://192.168.0.1/switch.stk image2
Mode..................................... TFTP
Set Server IP.............................. 192.168.0.1
Path..................................... ./
Filename................................. switchs.stk
Data Type................................ Code
Destination Filename..................... image2
Management access will be blocked for the duration of the transfer Are you sure you
want to start? (y/n) y


TFTP code transfer starting
101888 bytes transferred...277504 bytes transferred...410112 bytes
transferred...628224 bytes transferred...803328 bytes transferred...978944 bytes
transferred...1154560 bytes transferred...1330176 bytes transferred...1505280 bytes
transferred...1680896 bytes transferred...1861632 bytes transferred...2040320 bytes
transferred...2215936 bytes transferred...2391040 bytes transferred...2566656 bytes
transferred...2741760 bytes transferred...2916864 bytes transferred...3092992 bytes
transferred...3268096 bytes transferred...3443712 bytes transferred...3619328 bytes
transferred...3794432 bytes transferred...3970048 bytes transferred...4145152 bytes
transferred...4320768 bytes transferred...4496384 bytes transferred...4669952 bytes
transferred...4849152 bytes transferred...5027840 bytes transferred...5202944 bytes
transferred...5378560 bytes transferred...5554176 bytes transferred...5729280 by
tes transferred...5904896 bytes transferred...6078976 bytes transferred...6255616
bytes transferred...6423040 bytes transferred...6606336 bytes transferred...6781952
bytes transferred...6957056 bytes transferred...7111168 bytes transferred...7307776
bytes transferred...7483392 bytes transferred...7658496 bytes transferred...
Verifying CRC of file in Flash File System
Distributing the code to the members of the stack!
File transfer operation completed successfully.
(Netgear Switch) #
(Netgear Switch) #show bootvar
Image Descriptions
 image1 : default image
 image2 :
```

```
 Images currently available on Flash
--------------------------------------------------------------------
unit    image1        image2      current-active        next-active
--------------------------------------------------------------------
1       5.11.2.51     8.0.0.2         image1              image1
(Netgear Switch) #boot system image2
Activating image image2 ..
(Netgear Switch) #show bootvar
Image Descriptions
image1 : default image
image2 :
Images currently available on Flash
--------------------------------------------------------------------
unit    image1        image2      current-active        next-active
--------------------------------------------------------------------
1       5.11.2.51     8.0.0.2         image1              image2
                                      Image2 will be executed after reboot.
```

Web Interface: Download a Backup Image and Make It Active

1. Download a backup image using tftp.
   a. Select **Maintenance > Download > File Download**.

      A screen similar to the following displays.

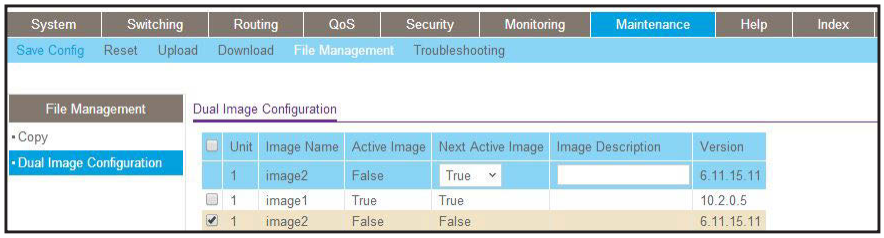


   b. From the **File Type** menu, select **Archive**.
   c. From the **Image Name** menu, select **image2**.
   d. From the **Transfer Mode** menu, select **TFTP**.
   e. From the **Server Address Type** menu, select **IPv4**.
   f. In the **Server Address** field, enter **10.100.5.17**(tftp server IP address).
   g. In the **Remote File Name**, enter **M4200.stk**.
   h. Click the **Apply** button.

      Your settings are saved.

2. Activate image2.
   a. Select **Maintenance > File Management > Dual Image Configuration**.

      A screen similar to the following displays.



   b. Under Dual Image Configuration, select the check box next image 2.

      The Image name field in the table heading displays image 2.

   c. From the **Next Active Image** menu, select **True**.
   d. Click the **Apply** button.

      Your settings are saved.

Outbound Telnet

In this section, the following examples are provided:

- *CLI: show network*
- *CLI: transport output telnet*
- *Web Interface: Configure Telnet*
- *CLI: Configure the Session Limit and Session Time-out*
- *Web Interface: Configure the Session Time-out*

Outbound Telnet:

- Establishes an outbound Telnet connection between a device and a remote host.
- A Telnet connection is initiated, each side of the connection is assumed to originate and terminate at a network virtual terminal (NVT).
- Server and user hosts do not maintain information about the characteristics of each other’s terminals and terminal handling conventions.
- Must use a valid IP address.

CLI: show network

```
(Netgear Switch) >telnet 192.168.77.151
Trying 192.168.77.151...
(Netgear Switch)
User:admin
Password:
(Netgear Switch)    >en
Password:

(Netgear Switch)    #show network

IP Address..............................  192.168.77.151
Subnet Mask.............................  255.255.255.0
Default Gateway.........................  192.168.77.127
Burned In MAC Address...................  00:10:18.82.04:E9
Locally Administered MAC Address.........  00:00:00:00:00:00
MAC Address Type........................  Burned In
Network Configuration Protocol Current...  DHCP
Management VLAN ID......................  1
Web Mode................................  Enable
Java Mode ..............................  Disable
```

CLI: show telnet

```
(Netgear Switch)#show telnet

Outbound Telnet Login Timeout (minutes)........  5
Maximum Number of Outbound Telnet Sessions.....  5
Allow New Outbound Telnet Sessions.............  Yes
```

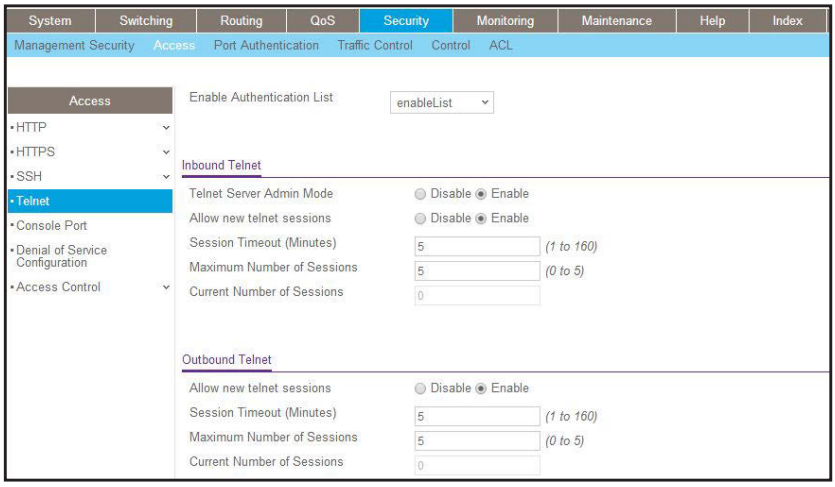
CLI: transport output telnet

```
(Netgear Switch) (Config)#lineconfig ?

<cr>                        Press Enter to execute the command.

(Netgear Switch) (Config)#lineconfig

(Netgear Switch) (Line)#transport ?

input                       Displays the protocols to use to connect to a
                            specific line of the router.
output                      Displays the protocols to use for outgoing
                            connections from a line.

(Netgear Switch) (Line)#transport output ?

telnet                      Allow or disallow new telnet sessions.

(Netgear Switch) (Line)#transport output telnet ?

<cr>                        Press Enter to execute the command.

(Netgear Switch) (Line)#transport output telnet

(Netgear Switch) (Line)#
```

Web Interface: Configure Telnet

1. Select **Security > Access > Telnet**.

   A screen similar to the following displays.



2. Under Outbound Telnet, for Admin Mode, select the **Enable** radio button.
3. Click the **Apply** button.

   Your settings are saved.

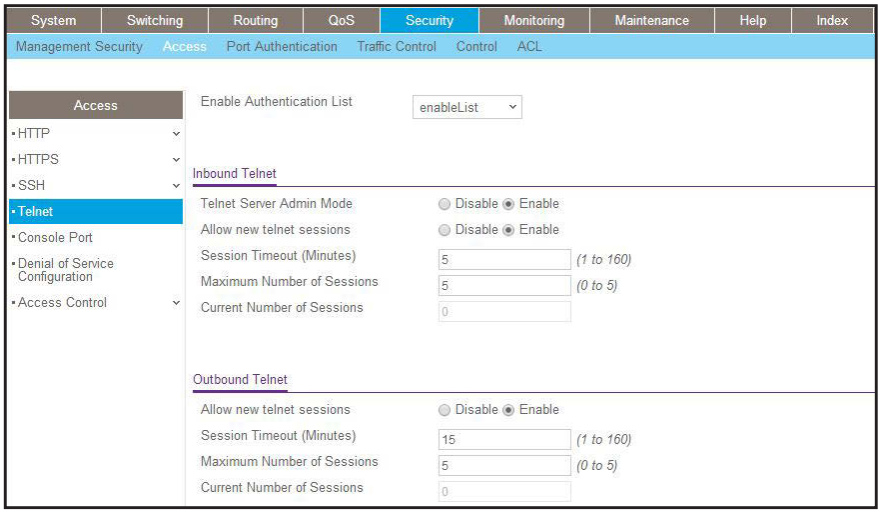
CLI: Configure the Session Limit and Session Time-out

```
(Netgear Switch) (Line)#session-limit ?
<0-5>                    Configure the maximum number of outbound telnet sessions
allowed.

(Netgear Switch) (Line)#session-limit 5

(Netgear Switch) (Line)#session-timeout ?

<1-160>                  Enter time in minutes.

(Netgear Switch) (Line)#session-timeout 15
```

Web Interface: Configure the Session Time-out

1. Select **Security > Access > Telnet**.

   A screen similar to the following displays.



2. Enter the following information:
   - In the **Session Timeout (Minutes)** field, enter **15**.
   - In the **Maximum Number of Sessions** field, enter **5**.
3. Click the **Apply** button.

   Your settings are saved.

Error Disablement and Automatic Error Recovery

The switch supports interface error disablement, also referred to as Diagnostic Disable (D-Disable), and error autorecovery of the disabled interface. If the switch detects an error condition for an interface, it places the interface in a diagnostic-disabled (error-disabled) state by shutting down the interface. The error-disabled interface does not allow any traffic until the interface is reenabled.

Either you can manually reenable the error-disabled interface or you can enable the error autorecovery feature, which automatically reenables the interface after the expiration of the time-out interval. The default time-out for autorecovery is 300 seconds. If an interface is reenabled but the reason that the interface was placed in the D-Disable state is not resolved, the interface is placed back in the D-Disable state.

The following features are supported by autorecovery:

- **Keepalive**. If loop protection is enabled, loop protection detects a loop, and the loop protection action is to disable the interface, the interface is placed in the D-Disable state. If autorecovery is enabled, the interface comes back up after the time-out interval expires.
- **BPDU storm**. If the number of BPDUs exceeds 15 for three consecutive seconds, the interface is placed in the D-Disable state. If autorecovery is enabled, the interface comes back up after the time-out interval expires.
- **BPDU guard**. The STP BPDU guard feature lets you enforce the STP domain borders and keep the active topology consistent and predictable. (Switches behind edge ports for which STP BPDU guard is enabled cannot influence the overall STP topology.) If the BPDU guard feature is enabled and a port receives BPDUs, the port is placed in the D-Disable state. If autorecovery is enabled, the port comes back up after the time-out interval expires.
- **Broadcast storm**. If broadcast storm control is enabled, the threshold value is exceeded, and the broadcast storm action is to disable the interface, the interface is placed in the D-Disable state. If autorecovery is enabled, the interface comes back up after the time-out interval expires.
- **Multicast storm**. If multicast storm control is enabled, the threshold value is exceeded, and the multicast storm action is to disable the interface, the interface is placed in the D-Disable state. If autorecovery is enabled, the interface comes back up after the time-out interval expires.
- **Unicast storm**. If unicast storm control is enabled, the threshold value is exceeded, and the unicast storm action is to disable the interface, the interface is placed in the D-Disable state. If autorecovery is enabled, the interface comes back up after the time-out interval expires.
- **Auto-DoS**. If auto-DoS is enabled and the switch detects a DoS attack, the interface is placed in the D-Disable state. If autorecovery is enabled, the interface comes back up after the time-out interval expires.
- **Port MAC address locking**. If dynamic MAC address locking is configured, the number of MAC addresses exceeds the threshold, and the port security violation action is to shut

down the port, the port is placed in the D-Disable state. If autorecovery is enabled, the port comes back up after the time-out interval expires.

- **Dynamic ARP inspection**. If dynamic ARP inspection (DAI) is enabled and the threshold value is reached, the interface is placed in the D-Disable state. If autorecovery is enabled, the interface comes back up after the time-out interval expires.
- **DHCP rate limiting**. If DHCP snooping is enabled and the incoming DHCP packet rate exceeds the threshold, the interface is placed in the D-Disable state. If autorecovery is enabled, the interface comes back up after the time-out interval expires.
- **UDLD**. If Unidirectional Link Detection (UDLD) is enabled and the unidirectional connection is detected, the interface is placed in the D-Disable state. If autorecovery is enabled, the interface comes back up after the time-out interval expires.

The following example shows how you can configure autorecovery for UDLD, change the time-out interval for autorecovery, and show the status of autorecovery for all features:

1. Enable autorecovery for UDLD.

```
(Netgear Switch) #config
(Netgear Switch) (Config)#errdisable recovery cause udld
```

2. Change the time-out interval for autorecovery.

```
(Netgear Switch) #config
(Netgear Switch) (Config) #errdisable recovery interval 30
```

3. Display the status of autorecovery for all features.

```
(Netgear Switch) #show errdisable recovery

Errdisable Reason      Auto-recovery Status
------------------     --------------------
dhcp-rate-limit           Enabled
arp-inspection            Enabled
udld                      Enabled
bcast-storm               Enabled
mcast-storm               Enabled
ucast-storm               Enabled
bpduguard                 Enabled
bpdustorm                 Enabled
keepalive                 Enabled
Port MAC Locking          Enabled
Denial Of Service         Enabled

Timeout for Auto-recovery from D-Disable state  30
```

Loop Protection

Loops inside a network are costly because they consume resources and reduce the performance of the network. Detecting loops manually can be cumbersome.

The switch can automatically identify loops in the network. You can enable loop protection per port or globally.

If loop protection is enabled, the switch sends predefined PDU packets to a Layer 2 multicast destination address (09:00:09:09:13:A6) on all ports for which the feature is enabled. You can selectively disable PDU packet transmission for loop protection on specific ports even while port loop protection is enabled. If the switch receives a packet with the previously mentioned multicast destination address, the source MAC address in the packet is compared with the MAC address of the switch. If the MAC address does not match, the packet is forwarded to all ports that are members of the same VLAN, just like any other multicast packet. The packet is not forwarded to the port from which it was received.

If the source MAC address matches the MAC address of the switch, the switch can perform one of the following actions, depending on how you configure the action:

- The port is shut down.
- A log message is generated. (If a syslog server is configured, the log message can be sent to the syslog server.)
- The port is shut down and a log message is generated.

If loop protection is disabled, the multicast packet is silently dropped.

You can configure the interval between two successive loop protection PDU packets with the **`transmit-interval`** command. The default interval parameter is 5 seconds. If the switch receives a loop protocol packet on a port for which the action is set to shut down the port, the port can no longer receive and send frames.

Loop protection operates at the port level, regardless of VLAN assignment and membership, detecting loops across VLANs. The protection uses the OUI-Extended Ethernet Type frame format (0x88b7), which is an IEEE-sanctioned format for vendor-specific packets.

Loop protection does not impact end nodes and is not intended for ports that serve as uplinks between spanning tree–aware switches. Loop protection can coexist with Spanning Tree Protocol (STP). You can enable both loop protection and STP on a port because these features function independently of each other. STP does not bring a port down when a loop is detected but keeps the port in blocking state. Because PDUs are allowed in a blocking state, loop protection packets are received and loop protection brings down the port that is involved in the loop (if the configured action is to shut down the port).

The following example shows how you can enable loop protection on ports 1/0/1 and 1/0/2:

1. Enable loop protection globally.

```
(Netgear Switch) (Config) #keepalive
```

Enable loop protection on ports 1/0/1 and 1/0/2 and set the violation action to shutting down the port and logging a message.

```
(Netgear Switch) (Config)#interface 1/0/1,1/0/2
(Netgear Switch) (Interface 1/0/1-1/0/2)#keepalive
(Netgear Switch) (Interface 1/0/1-1/0/2)#keepalive action both
```

Nondisruptive Configuration Management

If you are managing a large network with thousands of switches, the best way to change the switch configuration is to provide a new startup configuration file to the switch and let the switch gracefully resolve any differences between the running configuration and the new configuration by using the Nondisruptive Configuration Management feature.

For example, if VLANs 10, 20, and 30 are configured on the switch while the new configuration includes VLANs 10, 20, and 40, the switch must delete VLAN 30, create VLAN 40, and leave traffic that is being forwarded on VLANs 10 and 20 undisturbed.

To apply a new switch configuration without using the Nondisruptive Configuration Management feature, you must either restart the switch or send a delta configuration to the switch. Restarting the switch is disruptive, and managing delta configurations on a large scale can be difficult.

The following example shows how you can install a new configuration on a switch by using the Nondisruptive Configuration Management feature:

1. Download the file with the new configuration to switch.

```
(Netgear Switch) # Copy tftp://172.26.2.21/new_config.scr nvram:script new_config.scr
```

2. Merge the new configuration with the current configuration.

```
(Netgear Switch) # Reload configuration new_config.scr
```

3. Save the changes.

```
(Netgear Switch) #save
```

Full Memory Dump

The full memory dump feature provides the ability to retrieve the state of a crashed system and load it into a debugger to recreate the crashed state. This capability is useful when the switch encounters a crash.

The following example shows how to enable this feature and dump the information from a switch.

1. Select the way to transfer the exception dump.

   You can select NFS, TFTP, or USB. If you select NFS, you need an NFS share mount point on the network. Similarly, for TFTP mode, you need a TFTP server on the network. For USB mode, you need a USB sticker plugged into the USB slot on the front panel.

```
(Netgear Switch) (Config) #exception protocol tftp
```

2. Configure the IP address for the NFS or TFTP server.

```
(Netgear Switch) (Config) #exception dump tftp-server 172.26.2.100
```

3. Change the name of the dump file.

   The file name is formed as follows:

   - If hostname is selected: `file-name-prefix_hostname_Time_Stamp.bin`
   - If hostname is not selected: `file-name-prefix_MAC_Address_Time_Stamp.bin`

   By default, the file name is `core`, but you can change it with the following command:

```
(Netgear Switch) (Config) #exception core-file mydump
```

4. (Optional) Enable the switch-chip-register.

   This dumps the register value in the chipset.

```
(Netgear Switch) (Config) #exception switch-chip-register enable
```

Syslog

20

System logging

This chapter includes the following sections:

- *Syslog Concepts*
- *Show Logging*
- *Show Logging Buffered*
- *Show Logging Traplogs*
- *Show Logging Hosts*
- *Configure Logging for a Port*
- *Email Alerting*

Syslog Concepts

The syslog feature:

- Allows you to store system messages and errors.
- Can store to local files on the switch or a remote server running a syslog daemon.
- Provides a method of collecting message logs from many systems.

The following illustration explains how to interpret log files.

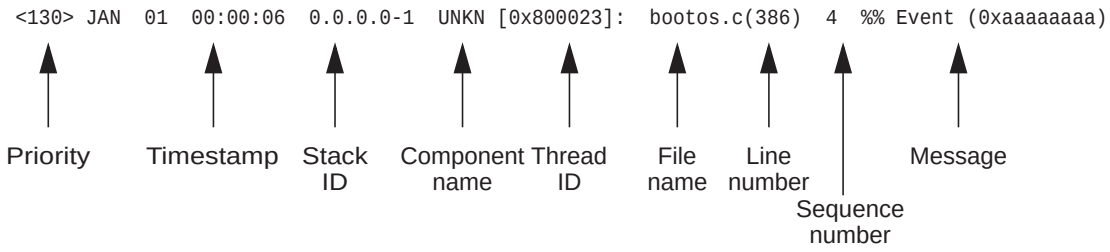


Figure 45. Log Files

Show Logging

The example is shown as CLI commands and as a web interface procedure.

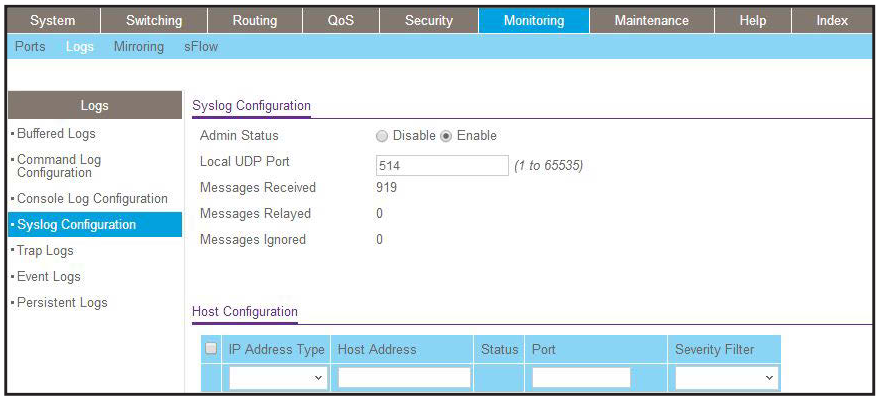
CLI: Show Logging

```
(Netgear Switch) #show logging

Logging Client Local Port       :    514
CLI Command Logging             :    disabled
Console Logging                 :    disabled
Console Logging Severity Filter :    alert
Buffered Logging                :    enabled

Syslog Logging                  :    enabled

Log Messages Received           :    66
Log Messages Dropped            :    0
Log Messages Relayed            :    0
Log Messages Ignored            :    0
```

Web Interface: Show Logging

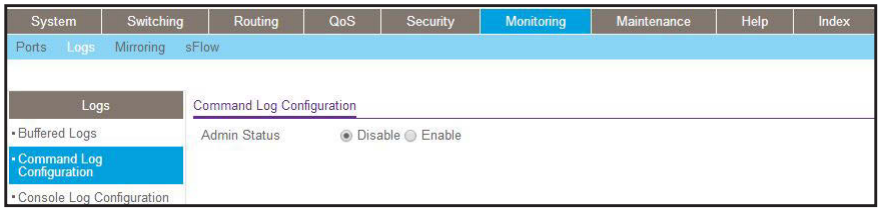
1. Configure the syslog.
   a. From the main menu, select **Monitoring > Logs > Sys Log Configuration**.

      A screen similar to the following displays.



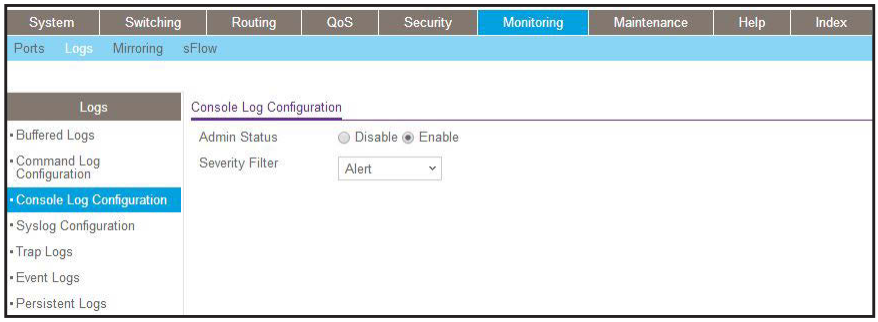
   b. In the Syslog Configuration, next to the Admin Status**,** select the **Enable** radio button.
   c. Click **Apply**.
2. Configure the command log.
   a. Select **Monitoring > Logs > Command Log**.

      A screen similar to the following displays.



   b. Under Command Log, for Admin Status, select the **Disable** radio button.
   c. Click **Apply**.
3. Configure the console log.
   a. **Select Monitoring > Logs > Console Log**.

      A screen similar to the following displays.



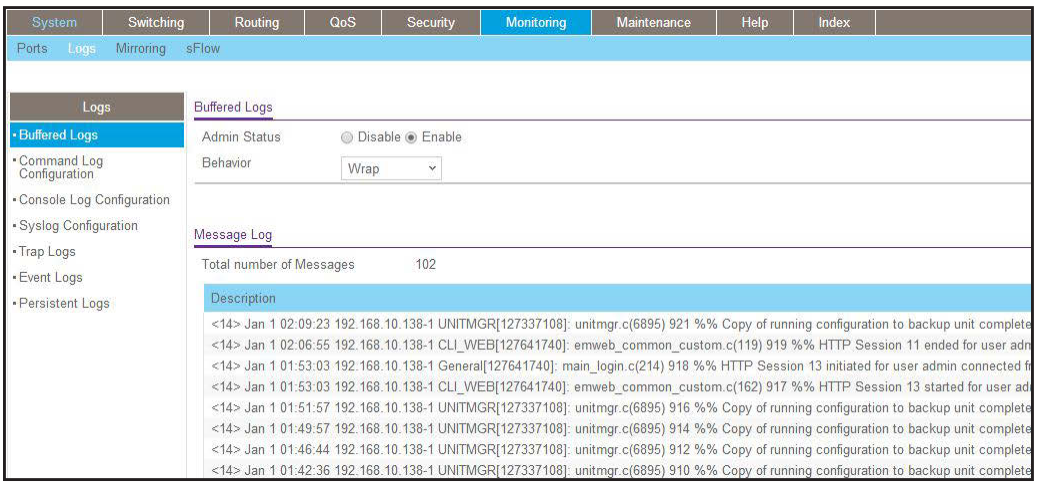
b. Under Console Log Configuration, for Admin Status**,** select the **Disable** radio button.

c. Click **Apply**.

4. Configure the buffer logs.

a. Select **Monitoring > Logs > Buffer Logs**.

A screen similar to the following displays.



b. Under Buffer Logs, for Admin Status**,** select the **Enable** radio button.

c. Click **Apply**.

Show Logging Buffered

The example is shown as CLI commands and as a web interface procedure.

CLI: Show Logging Buffered

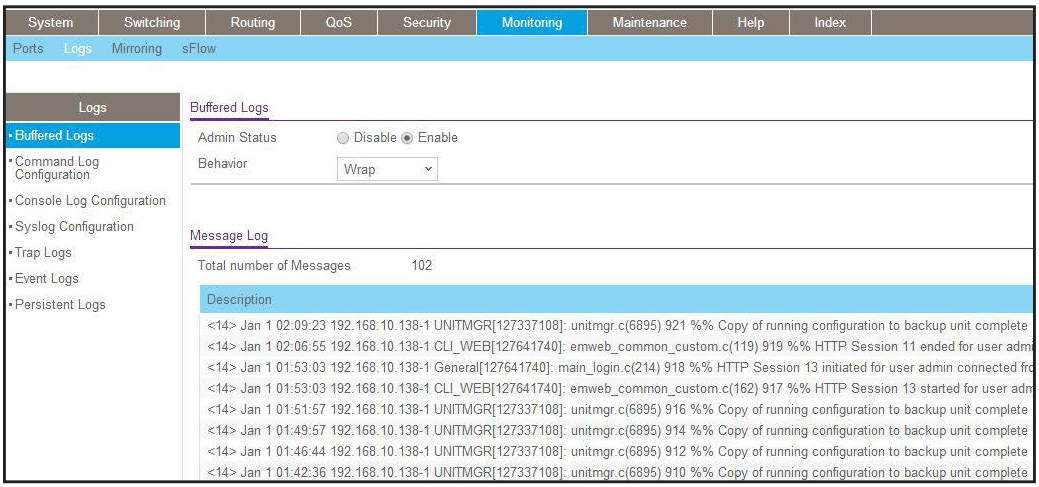
```
(Netgear Switch) #show logging buffered ?

<cr>    Press Enter to execute the command.

(Netgear Switch) #show logging buffered

Buffered (In-Memory) Logging        : enabled
Buffered Logging Wrapping Behavior  : On
Buffered Log Count                  : 3949

<14> Jan 13 00:42:58 172.26.2.129-1 CLI_WEB[101123540]: emweb_common_custom.c(119)
6497 %% HTTP Session 11 ended for user admin connected from 10.120.5.28
<14> Jan 13 00:36:21 172.26.2.129-1 UNITMGR[102633148]: unitmgr.c(6898) 6496 %% Copy
of running configuration to backup unit complete
<14> Jan 13 00:34:21 172.26.2.129-1 UNITMGR[102633148]: unitmgr.c(6898) 6494 %% Copy
of running configuration to backup unit complete
<13> Jan 13 00:33:45 172.26.2.129-1 TRAPMGR[102518604]: traputil.c(701) 6492 %% Link
Up: tunnel0
<13> Jan 13 00:33:44 172.26.2.129-1 TRAPMGR[102518604]: traputil.c(701) 6491 %% Link
Down: tunnel0
<13> Jan 13 00:33:44 172.26.2.129-1 TRAPMGR[102518604]: traputil.c(701) 6490 %% Link
Up: tunnel0
```

The priority (that is, the number that is stated in angle brackets before each logging message, for example, <14> in the previous example) is calculated by multiplying the facility number by 8 and adding the numerical value of the severity. If you know the priority, you can determine the facility and severity in the following ways:

- Facility = Priority divided by 8. The whole number is the facility. For example, if the priority is 14, divide 14 by 8. The result is 1.75. The whole number is 1, which is the facility.
- Severity = Priority minus 8. For example, if the priority is 14, subtract 8 from 14. The result is 6, which is the severity.

Web Interface: Show Logging Buffered

Select **Monitoring > Logs > Buffer Logs**. A screen similar to the following displays.



Show Logging Traplogs

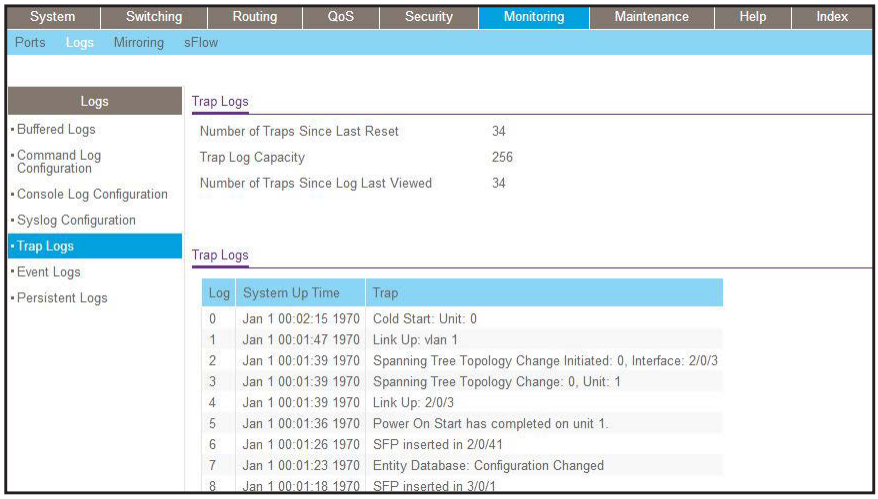
The example is shown as CLI commands and as a web interface procedure.

CLI: Show Logging Traplogs

```
(Netgear Switch)                    #show logging traplogs         ?
<cr>    Press Enter to execute the command.
(Netgear Switch)                    #show logging traplogs
Number of Traps Since Last Reset..... 6
Trap Log Capacity.....................256
Number of Traps Since Log Last Viewed....... 6

Log System Up Time         Trap
--- --------------         ------------------------------------------
0   0 days 00:00:46        Link Up: Unit: 3 Slot: 0 Port: 2
1   0 days 00:01:01        Cold Start: Unit: 0
2   0 days 00:21:33        Failed User Login: Unit: 1 User ID: admin
3   0 days 18:33:31        Failed User Login: Unit: 1 User ID: \
4   0 days 19:27:05        Multiple Users: Unit: 0     Slot: 3 Port: 1
5   0 days 19:29:57        Multiple Users: Unit: 0     Slot: 3 Port: 1
```

Web Interface: Show Logging Trap Logs

Select **Monitoring > Logs > Trap Logs**. A screen similar to the following displays.



Show Logging Hosts

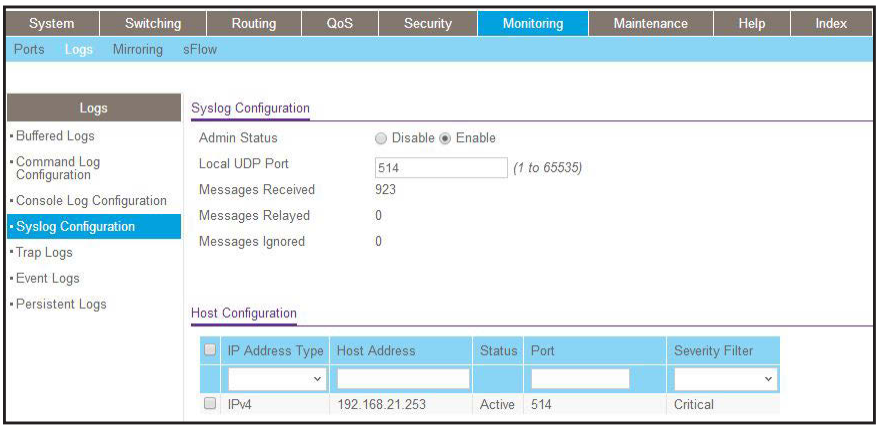
The example is shown as CLI commands and as a web interface procedure.

CLI: Show Logging Hosts

```
(Netgear Switch) #show logging hosts ?

<cr>                        Press Enter to execute the command.

(Netgear Switch) #show logging hosts

Index  IP Address          Severity    Port  Status
-----  -----------------   ----------  ----  -------------
1      192.168.21.253      critical    514   Active
```

Web Interface: Show Logging Hosts

Select **Monitoring > Logs > Sys Log Configuration**. A screen similar to the following displays.



Configure Logging for a Port

The example is shown as CLI commands and as a web interface procedure.

CLI: Configure Logging for the Port

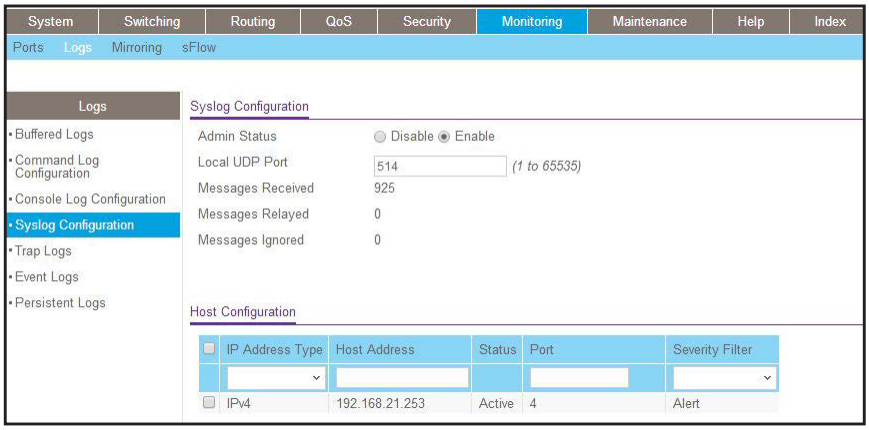
```
(Netgear Switch)     #config

(Netgear Switch) (Config)#logging ?

buffered           Buffered (In-Memory) Logging Configuration.
cli-command        CLI Command Logging Configuration.
console            Console Logging Configuration.
host               Enter IP Address for Logging Host
syslog             Syslog Configuration.

(Netgear Switch) (Config)#logging host ?
<hostaddress>          Enter Logging Host IP Address
reconfigure            Logging Host Reconfiguration
remove                  Logging Host Removal
(Netgear Switch) (Config)#logging host 192.168.21.253 ?

<cr>               Press Enter to execute the command.
<port>             Enter Port Id
```

```
(Netgear Switch) (Config)#logging host 192.168.21.253 4 ?

<cr>             Press Enter to execute the command.
<severitylevel>  Enter Logging Severity Level (emergency|0, alert|1, critical|2,
error|3, warning|4, notice|5, info|6, debug|7).

(Netgear Switch) (Config)#logging host 192.168.21.253 4 1 ?

<cr>             Press Enter to execute the command.

(Netgear Switch) (Config)#logging host 192.168.21.253 4 1

(Netgear Switch) #show logging hosts

Index  IP Address          Severity    Port  Status
-----  ------------------  ----------  ----  -------------
1      192.168.21.253      alert       4     Active
```

Web Interface: Configure Logging for the Port

1. Select **Monitoring > Logs > Sys Log Configuration**.

   A screen similar to the following displays.



2. Enter the following information:
   - In the **Host Address** field, enter your host address **192.168.21.253**.
   - In the **Port** field, enter **4**.
   - In the **Severity Filter** list, select **Alert**.
3. Click **Add**.

Email Alerting

Email alerting is an extension of the logging system. The logging system allows you to configure a set of destinations for log messages. This feature adds the email configuration, through which the log messages are sent to a configured SMTP server such that an administrator can receive the log in an email account of their choice.

This feature is enabled globally. When email alerting is enabled, selected log messages are sent to an SMTP server. Log messages are divided into three groups by severity level: urgent, nonurgent, and never.

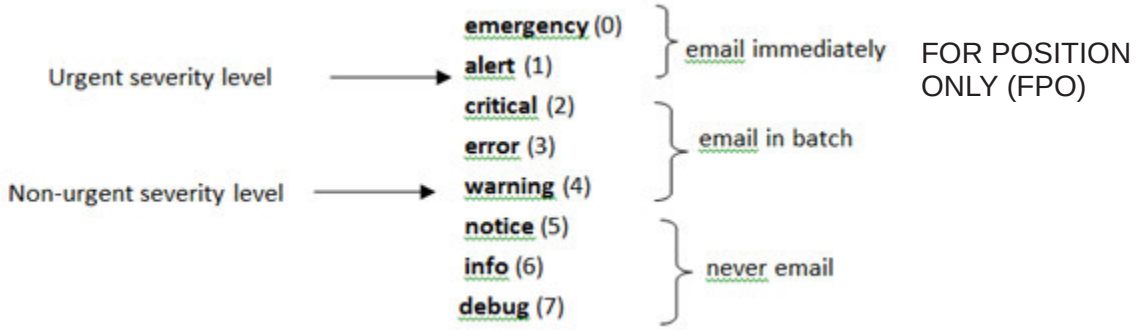


Figure 46. Log message severity levels

The network administrator can adjust the urgent and non-urgent severity levels. These levels are global and apply to all destination email addresses. Log messages in the urgent group are sent immediately to the SMTP server with each log message in a separate mail. After a delay period that you can configure, log messages in the nonurgent group are placed in a batch in a single email message.

Email alerting also provides a configuration option that allows the network administrator to specify the severity level at which SNMP traps are logged. Using this option, the administrator can put traps in the urgent group, the non-urgent group, or the never group for emailing. Traps are not emailed by default. For traps to be emailed, the network administrator has to either increase the severity at which traps are logged, or lower the severity level of log messages that are emailed.

The network administrator can configure multiple destination email addresses, and for each email address, specify whether to deliver urgent log messages, nonurgent log messages, or both.

When the log buffer is full, an exception occurs to how messages are sent to the SMTP server. When the log buffer is full before the periodic timer expires, the periodic timer is ignored and all log messages that were not sent previously are immediately forwarded to the SMTP server.

CLI: Send Log Messages to admin@switch.com Using Account aaaa@netgear.com

1. Configure an SMTP server, for example, smtp.netgear.com. Before you configure the SMTP server, you need to have an account on SMTP server.

```
(Netgear Switch) (Config)#mail-server "smtp.netgear.com" port 465
(Netgear Switch) (Mail-Server)#security tlsv1
(Netgear Switch) (Mail-Server)# username  aaaa
(Netgear Switch) (Mail-Server)# password  xxxxxx
(Netgear Switch) (Mail-Server)#exit
```

2. Configure logging mail. The from-addr is the source address of the email and the to-addr is the destination address of the email.

```
(Netgear Switch) (Config)#logging email
(Netgear Switch) (Config)#logging email from-addr aaaa@netgear.com
(Netgear Switch) (Config)#logging email message-type urgent to-addr
admin@switch.com
(Netgear Switch) (Config)#logging email message-type non-urgent to-addr
admin@switch.com
```

3. Increase the severity of traps to 3 (error). By default, it is 6 (informational).

```
(Netgear Switch) (Config)#logging traps 3
```

Switch Stacks

21

Manage switch stacks

This chapter describes the concepts and recommended operating procedures to manage NETGEAR stackable managed switches that are running release 12.0 or a newer release.

This chapter includes the following sections:

- *Switch Stack Management and Connectivity*
- *Stack Master and Stack Members*
- *Install and Power-up a Stack*
- *Switch Firmware and Firmware Mismatch*
- *Stack Switches Using a 10G Copper Port*
- *Add, Remove, or Replace a Stack Member*
- *Switch Stack Configuration Files*
- *Preconfigure a Switch*
- *Renumber Stack Members*
- *Move the Stack Master to a Different Unit*

Note: Switch stacking is available on the M4300 series switches only.

Switch Stack Management and Connectivity

You manage the switch stack through the stack master. You cannot manage stack members on an individual basis. To access the stack master, use either a serial connection to the switch master's console port or a Telnet connection to the IP address of the stack.

You can use these methods to manage switch stacks:

- Web management interface.
- CLI (over a serial connection).
- A network management application through SNMP.

Stack Master and Stack Members

A switch stack is a set of up to eight switches that are connected through their stack ports. The switch that controls the operation of the stack is the stack master. The stack master and the other switches in the stack are stack members. Stack members use stacking technology to behave and work together as a unified system. Layer 2 and Layer 3 protocols present the entire switch stack as a single entity to the network.

The following figure shows an example of switches that are interconnected to form a stack.

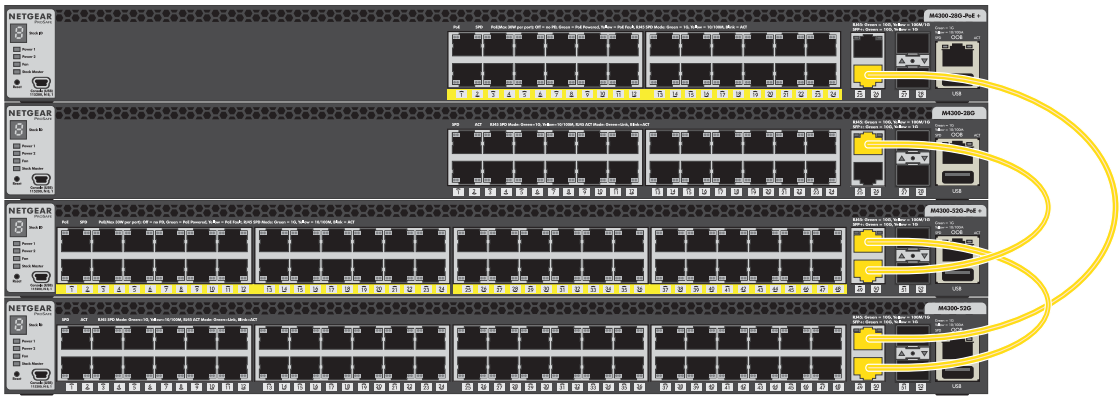


Figure 47. Stacked switches

Stack Master

The stack master is the single point of stack-wide management. From the stack master, you can configure:

- System-level (global) features that apply to all stack members
- Interface-level features for all interfaces on any stack member

A switch stack is identified in the network by its network IP address. The network IP address is assigned according to the MAC address of the stack master. Every stack member is uniquely identified by its own stack member number.

The stack master contains the saved and running configuration files for the switch stack. The configuration files include the system-level settings for the switch stack and the interface-level settings for all stack members. Each stack member retains a copy of the saved file for backup purposes. If the master is removed from the stack, another member is elected master, and then runs from that saved configuration.

All stack members are eligible stack masters. If the stack master becomes unavailable, the remaining stack members participate in electing a new stack master. A set of factors determine which switch is elected the stack master. The stack master is elected or re-elected based on one of these factors and in the order listed:

1. The switch that is currently the stack master
2. The switch with the highest stack member priority value

Note: NETGEAR recommends assigning the highest priority value to the switch that you prefer to be the stack master. This ensures that the switch is re-elected as stack master if a re-election occurs.

3. The switch with the higher MAC address

A stack master retains its role unless one of these events occurs:

- The stack master is removed from the switch stack.
- The stack master is reset or powered off.
- The stack master fails.
- The switch stack membership is increased by adding powered-on standalone switches or switch stacks.

In the case of a master re-election, the new stack master becomes available after a few seconds. In the meantime, the switch stack uses the forwarding tables in memory to minimize network disruption. The physical interfaces on the other available stack members are not affected while a new stack master is elected. If a new stack master is elected and the previous stack master becomes available, the previous stack master does not resume its role as stack master.

Stack Members

A switch stack can include up to eight stack members connected through their stack ports. A switch stack always includes one stack master.

A standalone switch is a switch stack with one stack member that also operates as the stack master. You can connect one standalone switch to another to create a switch stack containing two stack members, with one of them being the stack master. You can connect standalone switches to an existing switch stack to increase the stack membership.

The operation of the switch stack continues uninterrupted during membership changes unless you remove the stack master or you add powered-on standalone switches or switch stacks.

Stack Member Numbers

A stack member number (1 to 8) identifies each member in the switch stack. The member number also determines the interface-level configuration that a stack member uses. You can display the stack member number by issuing the **`show switch user`** EXEC command.

A new, out-of-the-box switch (one that did not join a switch stack or was not manually assigned a stack member number) ships with a default stack member number of 1. When the switch joins a switch stack, the default stack member number of the switch changes to the lowest available member number in the stack.

Stack members in the same switch stack cannot be assigned the same stack member number. Every stack member, including a standalone switch, retains its member number until you manually change the number or unless the number is already being used by another member in the stack. Fore more information, see *Renumber Stack Members* on page 449.

Stack Member Priority Values

You can change a stack member priority. This is useful if you want to change the master of the stack. To change the stack member priority, issue the **`switch unit priority value`** command in the global config mode.

Install and Power-up a Stack

Many switch models include a *Hardware Installation Guide* with information about rack mounting and stack cabling.

Compatible Switch Models

NETGEAR stackable managed switches include the following models:

- M4300-28G
- M4300-52G

- M4300-28G-POE+
- M4300-52G-POE+
- M4300-8X8F
- M4300-12X12F
- M4300-24X24F

Install a Switch Stack

➢ **To install a switch stack:**

1. Install the switches in a rack.
2. Install all stacking cables, including the redundant stack link.

   NETGEAR highly recommends that you install a redundant link between the switches.
3. Identify the switch to be the master and power it up.
4. Monitor the console port.

   Allow the master switch to come up to the login prompt. If the switch has the default configuration, it should come up as unit #1, and automatically become a master switch. If not, renumber the units.
5. If you want to configure switches offline, preconfigure the other switches to be added to the stack.

   For more information, see *Preconfigure a Switch* on page 448.
6. Power on a second switch, making sure it is adjacent (that is, the next physical switch in the stack) to the switch already powered up.

   This ensures that the second switch comes up as a member of the stack, and not a master of a separate stack.
7. Monitor the master switch to make sure that the second switch joins the stack.

   You can issue the **`show switch`** command to determine when the switch joins the stack. It will be assigned a unit number (unit #2, if it has the default configuration).
8. As an option, renumber this stack member.

   For more information, see *Renumber Stack Members* on page 449.
9. To add more members to the stack, repeat steps *Step 6* through *Step 8*.

   Always power on a switch adjacent to the switches already in the stack.

Switch Firmware and Firmware Mismatch

All stack members must run the same firmware version to ensure full compatibility in the stack protocol version among the stack members.

If a stack member is running a different firmware version than the stack master, that stack member is not allowed to join the stack. To list the stack members and firmware versions, issue the **show switch** command.

If a switch is added to a stack and it does not run the same firmware version as the master, the following occurs:

- The new unit boots up and becomes a member of the stack.
- Ports on the added unit remain in the detached state.
- A message displays on the CLI indicating a code (firmware) mismatch with the newly added unit.

To enable the newly added unit to merge normally with the stack, issue the **copy xmodem | ymodem | zmodem | tftp://ip/filepath/filename** command. This command copies the firmware image from a stack member to the one with incompatible firmware. That switch automatically reloads and joins the stack as a fully functioning member.

Upgrade the Firmware

All stack members must run the same firmware version. Ports on stack members that do not match the master switch firmware version do not come up. In that situation, the output of the **show switch** command shows a code (firmware) mismatch error.

Note: NETGEAR recommends that you schedule the firmware upgrade when there is no excessive network traffic (such as a broadcast event).

➢ **To download new firmware to the master switch and other switches in the stack:**

1. Using TFTP or xmodem, issue the **copy** command on the master switch.

   After the firmware is successfully loaded onto the master switch, the firmware automatically propagates to the other units in the stack.

CAUTION:

To avoid errors during firmware propagation, do not move stack cables or reconfigure units.

2. If an error occurs during firmware propagation, do the following:
   a. Check to make sure the master switch is running the correct firmware.

b. Attempt again to copy the firmware to the units that did not get updated by issuing the **copy** command in stack configuration mode.

3. After the firmware is loaded to all members of the stack, reset all the switches

   The new firmware takes effect.

Migrate Configuration with a Firmware Upgrade

In some cases, a configuration might not be carried forward in a firmware update.

- **If a configuration is not carried forward in a firmware update, to download new firmware to the master switch and other switches in the stack:**

1. Save the current configuration by uploading it from the stack, using the **copy** command from the CLI.
2. Load new firmware onto the stack manager.
3. Reboot the stack.
4. Upon reboot, enter the boot menu and erase the configuration (that is, restore is to factory default settings).
5. Continue with the boot of the operational firmware.
6. After the stack is up, download the saved configuration to the master.

   This saved configuration is automatically propagated to all members of the stack.

Web Interface: Copy Master Firmware to a Stack Member

1. Select **Maintenance > File Management > Copy**.

   A screen similar to the following displays.

2. In the **Stack Member** menu, select **2**.
3. Click **Apply**.

Stack Switches Using a 10G Copper Port

This example shows how to stack two switches at close range.

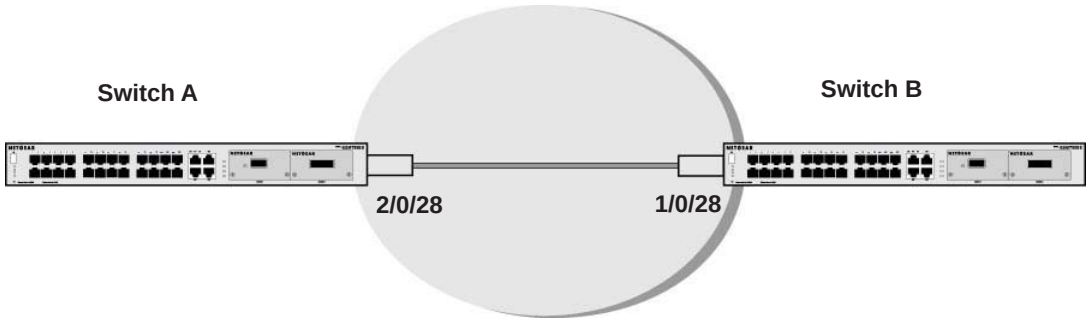


Figure 48. Connect switches through their 10G copper ports

➢ **To set up a stack between two switches:**

1. Using a Cat6e Ethernet cable, connect a 10G copper port on one switch with a 10G copper port on the other switch.
2. Configure the Switch A and Switch B as described in one of the following sections:
   - *CLI: Configure the 10G Copper Ports as Stack Ports* on page 441
   - *Web Interface: Copy Master Firmware to a Stack Member* on page 439

CLI: Configure the 10G Copper Ports as Stack Ports

1. On Switch A, configure the stack port and reboot the switch.

```
(Netgear Switch) #show stack-port

                     Configured Running
                     Stack      Stack      Link         Link
Unit Interface       Mode       Mode       Status       Speed (Gb/s)
---- --------------- ---------- ---------- ------------ ------------
2    0/25            Ethernet   Ethernet   Link Down    10
2    0/26            Ethernet   Ethernet   Link Down    10
2    0/27            Ethernet   Ethernet   Link Down    10
2    0/28            Ethernet   Ethernet   Link Down    10

(Netgear Switch) #
(Netgear Switch) #config
(Netgear Switch) (Config)#stack
(Netgear Switch) (Config-stack)#stack-port 2/0/28 stack
(Netgear Switch) (Config-stack)#exit
(Netgear Switch) (Config)#exit
(Netgear Switch)#exit
(Netgear Switch) #reload
Management switch has unsaved changes.
Would you like to save them now? (y/n) y
Config file 'startup-config' created successfully.
Configuration Saved!
Are you sure you want to reload the stack? (y/n)y
```

2. After Switch A reboots, check the stack port configuration.

```
(M4300-28G-PoE+) #show stack-port

                     Configured Running
                     Stack      Stack      Link         Link
Unit Interface       Mode       Mode       Status       Speed (Gb/s)
---- --------------- ---------- ---------- ------------ ------------
2    0/25            Ethernet   Ethernet   Link Down    10
2    0/26            Ethernet   Ethernet   Link Down    10
2    0/27            Ethernet   Ethernet   Link Down    10
2    0/28            Stack      Stack      Link Down    10
```

3. On Switch B, configure the stack port and reboot the switch.

```
(Netgear Switch) #show stack-port

                     Configured Running
                     Stack      Stack      Link         Link
Unit Interface       Mode       Mode       Status       Speed (Gb/s)
---- --------------- ---------- ---------- ------------ ------------
1    0/25            Ethernet   Ethernet   Link Down    10
1    0/26            Ethernet   Ethernet   Link Down    10
1    0/27            Ethernet   Ethernet   Link Down    10
1    0/28            Ethernet   Ethernet   Link Down    10

(Netgear Switch) #
(Netgear Switch) #config
(Netgear Switch) (Config)#stack
(Netgear Switch) (Config-stack)#stack-port 1/0/28 stack
(Netgear Switch) (Config-stack)#exit
(Netgear Switch) (Config)#exit
(Netgear Switch)#exit
(Netgear Switch) #reload
Management switch has unsaved changes.
Would you like to save them now? (y/n) y
Config file 'startup-config' created successfully.
Configuration Saved!
Are you sure you want to reload the stack? (y/n)y
```

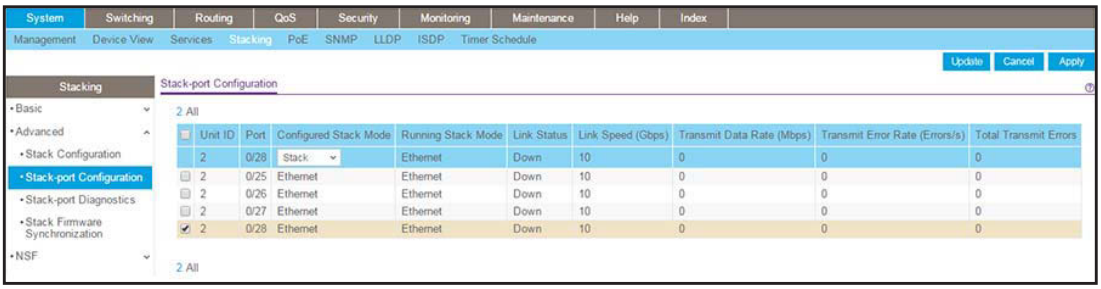
4. After Switch B reboots, check the stack port configuration.

```
(M4300-28G-PoE+) #show stack-port

                     Configured Running
                     Stack      Stack      Link         Link
Unit Interface       Mode       Mode       Status       Speed (Gb/s)
---- --------------- ---------- ---------- ------------ ------------
1    0/25            Ethernet   Ethernet   Link Down    10
1    0/26            Ethernet   Ethernet   Link Down    10
1    0/27            Ethernet   Ethernet   Link Down    10
1    0/28            Stack      Stack      Link Down    10
```

Web Interface: Configure the 10G Copper Ports as Stack Ports

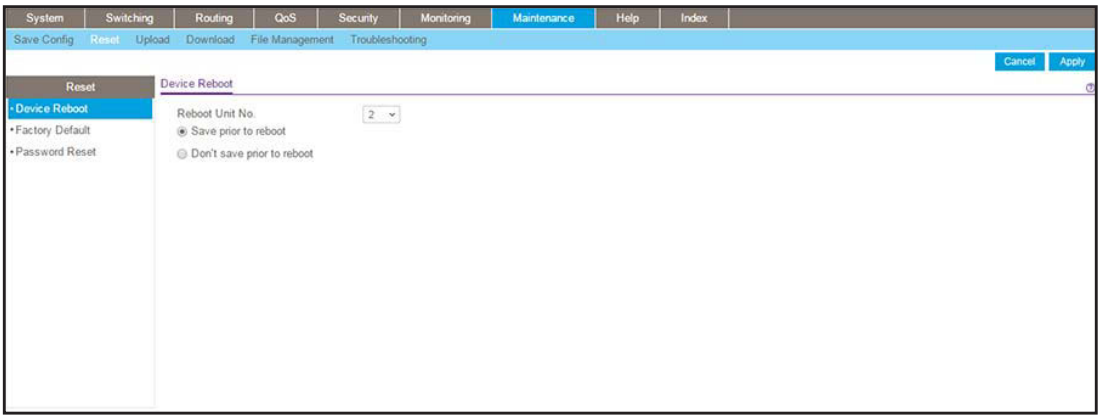
1. On Switch A, configure a stack port as an Ethernet port.
   a. Select **System > Stacking > Advanced > Stack Port Configuration**.

      A screen similar to the following displays.



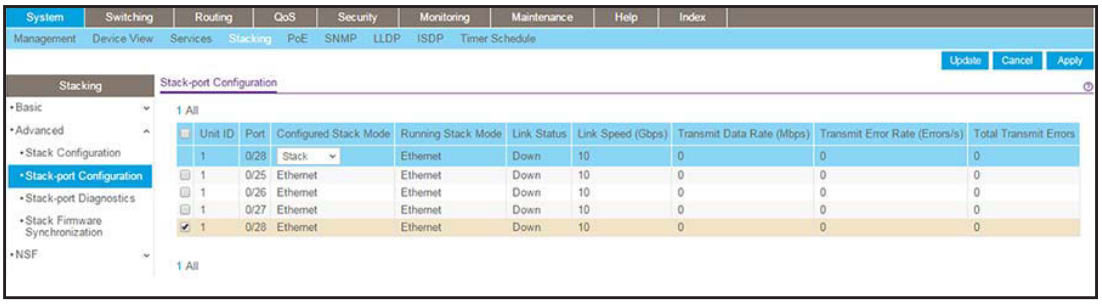
   b. Scroll down and select the **2/0/28** check box.
   c. In the **Configured Stack Mode** menu, select **Stack**.
   d. Click **Apply** to save the settings.
2. Reboot the switch.
   a. Select **Maintenance > Reset > Device Reboot**.

      A screen similar to the following displays.



   b. In the **Reboot Unit No.** menu, select **2**.
   c. Click **Apply**.
3. On Switch B, configure a stack port as an Ethernet port.
   a. Select **System > Stacking > Advanced > Stack Port Configuration**.

      A screen similar to the following displays.



b. Scroll down and select the **1/0/28** check box.

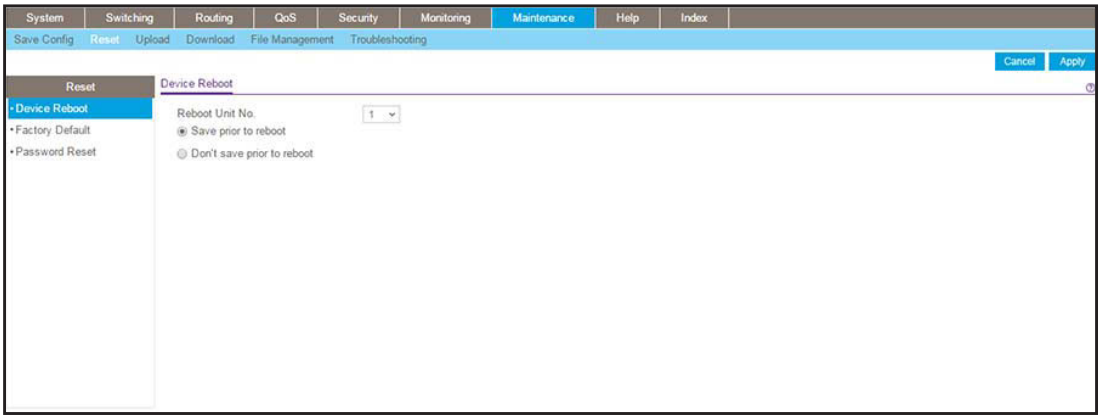
c. In the **Configured Stack Mode** menu, select **Stack**.

d. Click **Apply** to save the settings.

4. Reboot the switch.

a. Select **Maintenance > Reset > Device Reboot**.

A screen similar to the following displays.



b. In the **Reboot Unit No.** menu, select **1**.

c. Click **Apply**.

The switch reboots.

Add, Remove, or Replace a Stack Member

You can manage an operating stack.

Add Switches to an Operating Stack

➢ **To add new switches to an operating stack:**

1. Make sure that the redundant stack connection is functional.

   All stack members must be connected in a logical ring.

2. Preconfigure any new switches.
3. Power off all new switches that must join the stack.

CAUTION:

If you cable one or more powered-on switches to the stack, the existing stack and the new switches assume that two stacks are merging. They elect a single, new stack master, and you cannot specify which switch becomes the new master. All stack members assume the configuration that is based on the new stack master. Stack members change their stack member numbers to the lowest available numbers.

4. Install the new switches in the rack.

   This procedure assumes installation below the bottom-most switch, or above the top-most switch.

5. Disconnect the redundant stack cable that connects the last switch in the stack to the first switch in the stack at the position in the ring where you intend to insert the new switch.

Note: If you want to merge an operational stack into the this stack, add the switches as a group by unplugging one stacking cable in the operational stack and physically connecting all unpowered units at that point.

6. Connect this cable to the new switch, following the established order of stack-up to stack-down connections.
7. Power up the new switches one by one.
8. Verify, by monitoring the master switch console port, that the new switch joins the stack by issuing the **`show switch`** command. The new switch joins as a member (never as master; the existing master of the stack must not change).
9. If the firmware version of the newly added member is not the same as the existing stack, update the firmware (see *Upgrade the Firmware* on page 438.).

Remove a Switch from a Stack

➢ **To remove a switch from a stack:**

1. Make sure that the redundant stack connection is functional.

   All stack members must be connected in a logical ring.

2. Power down the switch that you want to remove.

CAUTION:

If the switch stack is not cabled correctly, removing powered-on stack members might cause the switch stack to divide (that is, partition) into two or more switch stacks, each with the same configuration. Make sure that the switch stack is cabled correctly.

3. Disconnect the stack cables.
4. If you do not intend to replace the switch, reconnect the stack cable from the stack member above to the stack member below the switch that you intend to remove.
5. Remove the switch from the rack.
6. To remove the switch not only from the stack but also from the stack configuration, issue the **no member** *unit-id* command.

   Note: If the switch stack divides, and you want the switch stacks to remain separate, change the IP address or addresses of the newly created switch stacks.

7. If the switch stack divides but you do not intend to partition the switch stack, do the following:
   a. Power off the newly created switch stacks.
   b. Reconnect them to the original switch stack through their stack ports.
   c. Power on the switches.

Replace a Stack Member

➢ **To replace a stack member:**

1. Make sure that the redundant stack connection is functional.

   All stack members must be connected in a logical ring.

2. Power down the switch that you intend to remove and disconnect its stack cables.
3. Remove the switch from the rack.
4. If you intend to install a different model switch, remove the unit from the configuration by issue the **no member** *unit-id* command.
5. Install the new switch in the rack:
   - If you are installing the same model switch, place the switch in the same position in the stack as the switch that you just removed.
   - If you are installing a different model switch, either place the switch in the same position as the previous switch, or at the bottom of the stack.
6. Cable the new switch, following the established order of stacking cables.
7. Power up the new switch.

Verify, by monitoring the master switch console port, that the new switch successfully joins the stack by issuing the **show switch** command. The new switch must join as a member (not as master; the existing master of the stack must not change).

8. If the firmware version of the newly added member is not the same as the existing stack, update the firmware (see *Upgrade the Firmware* on page 438).

Switch Stack Configuration Files

The configuration files include all global and interface-specific settings that define the operation of the stack and its individual members. If you issue the **save config** command, all stack members store a copy of the configuration settings. If a stack master becomes unavailable, the stack member that assumes the role of stack master operates from the saved configuration files.

When a new, out-of-box switch joins a switch stack, the switch uses the system-level settings of that switch stack. However, if you want the store to store this system level configuration, you must issue the **save config** command.

You can back up and restore the stack configuration by using the **copy** command in the same way as you back up and restore a standalone switch configuration.

The following table provides switch stack configuration scenarios. Most of the scenarios assume that at least two switches are connected through their stack ports.

Table 2. Switch stack master scenarios

Scenario	Action	Result
Stack master election specifically determined by existing stack masters. **Note:** NETGEAR does not recommend this scenario.	Connect two powered-on switch stacks through the stack ports.	Only one of the stack masters becomes the new stack master. No other stack members become the stack master.
Stack master election specifically determined by the stack member priority value.	• Connect two switches through their stack ports. • To set a stack member to a higher member priority value, issue the **switch stack-member-number priority new-priority-number** global configuration command. • Restart both stack members at the same time.	The stack member with the higher-priority value is elected stack master.
Stack master election specifically determined by the MAC address.	Assuming that both stack members have the same priority value and firmware image, restart both stack members at the same time.	The stack member with the higher MAC address is elected stack master.

Table 2. Switch stack master scenarios (continued)

Scenario	Action	Result
Add a stack member.	• Power off the new switch • Through their stack ports, connect the new switch to a powered-on switch stack. • Power on the new switch.	The stack master is retained. The new switch is added to the switch stack.
Stack master failure.	Remove (or power off) the stack master.	One of the remaining stack members becomes the new stack master. All other members in the stack remain stack members and do not reboot.

Preconfigure a Switch

You can preconfigure (that is, supply a configuration to) a new switch before it joins the switch stack. You can specify the stack member number, the switch type, and the interfaces that are associated with a switch that is not currently part of the stack.

Note: If you are replacing a switch with the same model in the same position in the stack, you do not need to preconfigure it. The new switch assumes the same configuration as the previous switch.

➢ **To preconfigure a switch:**

1. Issue the **member** *unit-id switchindex* command.
2. To view the supported unit types, use the **show supported switchtype** command.
3. Configure the unit that you defined in *Step 1*, just as if the unit were physically present.

   Ports for the preconfigured unit come up in a detached state.
4. To see the ports, use the **show port all** command.

   Now you can configure the detached ports for VLAN membership and any other port-specific configuration.

After you preconfigure a unit type for a specific unit number, attaching a unit with a different unit type for this unit number causes the switch to report an error. In this situation, the output of the **show switch** command indicates a configuration mismatch for the new unit and the ports on that unit do not come up. To resolve this situation, you can change the unit number of the mismatched unit or delete the preconfigured unit type by issuing the **no member** *unit-id* command.

When you add a preconfigured switch to the switch stack, the stack applies either the preconfigured configuration or the default configuration. The following table lists the events

that can occur when the switch stack compares the preconfigured configuration with the new switch.

Table 3. Preconfigured switches compared to stack configuration

Switch Type Is the Same	Stack Member Number	Result
Yes	Is the same	The switch stack applies the configuration to the preconfigured new switch and adds it to the stack.
Yes	Does not match	• The switch stack applies its default stack member number to the preconfigured switch and adds it to the stack. • The stack member number configuration in the preconfigured switch changes to reflect the new information.
	Is not found in the stack configuration	• The switch stack applies the default configuration to the new switch and adds it to the stack. • The preconfigured information is changed to reflect the new information.
	Is not found in the preconfigured switch	The switch stack applies the default configuration to the preconfigured switch and adds it to the stack.

Renumber Stack Members

This example is provided as CLI commands and a web interface procedure.

CLI: Renumber Stack Members

Note: When you issue a command such as **`move management`** or **`renumber`**, NETGEAR recommends that you wait until the command fully executes before issuing the next command. For example, after you issue a **`reset`** command for a stack member, issue the **`show port`** command to verify that the switch remerged with the stack and that all ports joined before you issue a next command.

- If specific numbering is required, NETGEAR recommends that you assign stack members their numbers when they are first installed and configured in the stack.
- If the stack unit number for a switch is unused, you can renumber the unit by issuing the **`switch <oldunit-id> renumber <newunit-id>`** global config mode command.
- If you preconfigured the new unit ID, you might need to remove the new unit ID from the configuration before renumbering the unit.
- If you need to reassign multiple existing stack unit numbers, the configuration could become mismatched. To avoid this situation, NETGEAR recommends that you power down all switches except the master, and then add them back one at a time (see *Add Switches to an Operating Stack* on page 444).

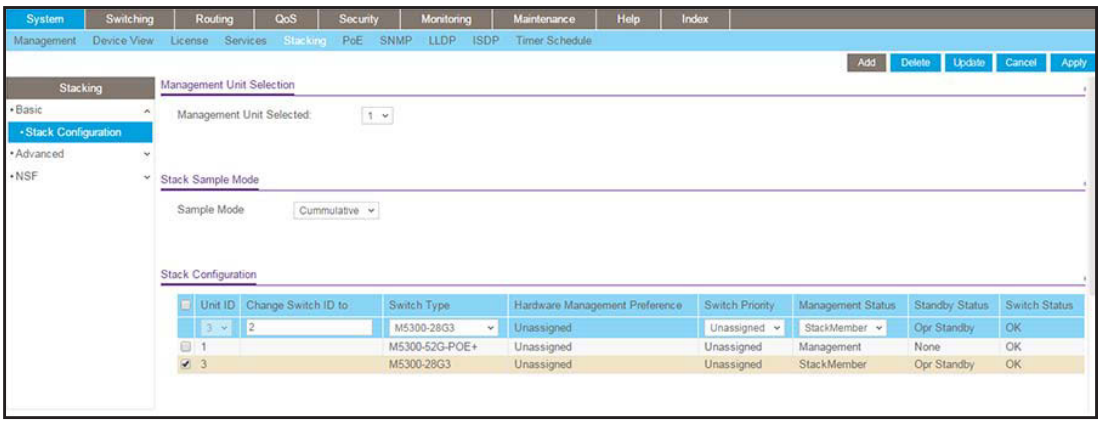
To renumber stack members, issue the following CLI command:

```
(Netgear Switch) (Config)#switch 3 renumber 2
All the switches in the stack will be reset to perform Manager unit renumbering and
the configuration of Manager switch interfaces will be cleared.
Are you sure you want to renumber? (y/n) y
```

Web Interface: Renumber Stack Members

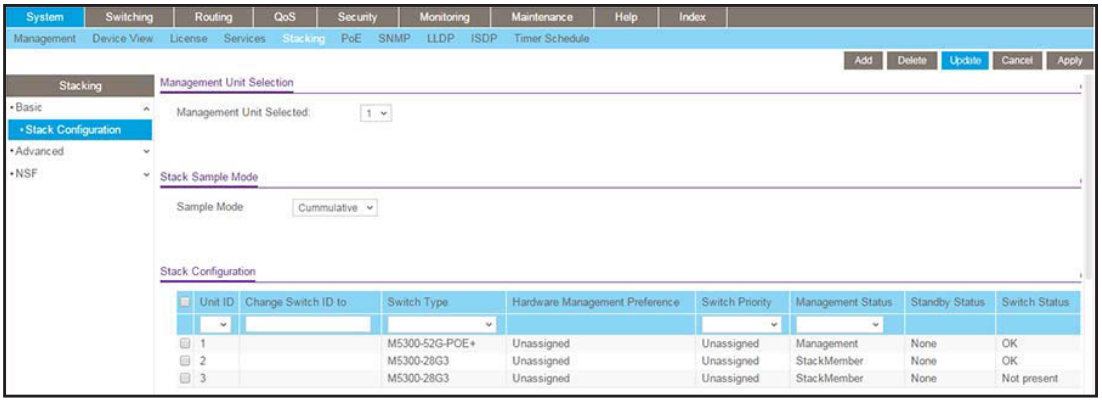
1. Renumber the stacking member's ID from 3 to 2.
   a. Select **System > Management > Basic > Stack Configuration**.

      A screen similar to the following displays.



   b. Scroll down and select the **3** check box.
   c. In the **Change Switch ID to** field, enter **2**.
   d. Click **Apply** to save the settings.

      Now, the unit ID of the stacking member is 2.



Move the Stack Master to a Different Unit

This example is provided as CLI commands and a Web interface procedure.

CLI: Move the Stack Master to a Different Unit

1. To mover the stack master to a different unit number, issue the **movemanagement** *<fromunit-id>* *<tounit-id>* command.

   The operation takes between 30 seconds and 3 minutes, depending on the stack size and configuration.
2. Make sure that you can log in on the console that is attached to the new master.
3. To verify that all units rejoined the stack, issue the **show switch** command.
4. Reset the stack by issuing the **reload** command.

To mover the stack master to a different unit number, issue the following CLI command:

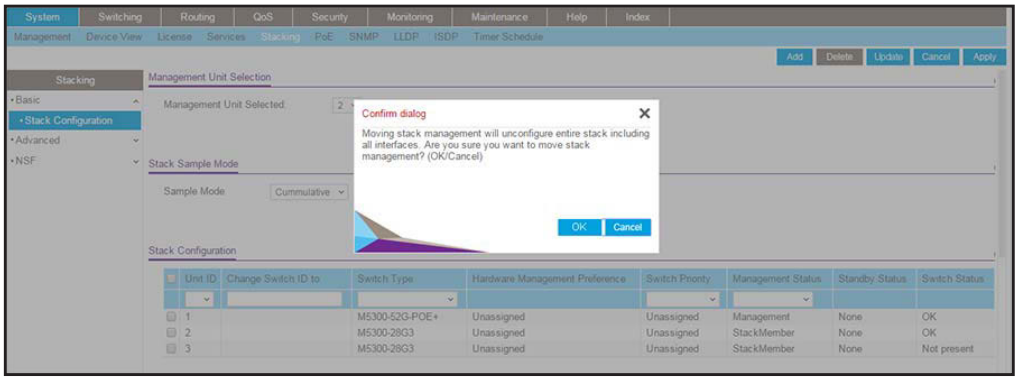
```
(Netgear Switch) (Config)#stack
(Netgear Switch) (Config-stack)#movemanagement 1 2
```

Web Interface: Move the Stack Master to a Different Unit

1. Select **System > Management > Basic > Stack Configuration**.

   A screen similar to the following displays.
2. In the **Management Unit Selected** menu, select **2**.

   A warning window displays.



3. Click the **OK** button.
4. Click **Apply** to save the settings.

Note: If the master receives its IP address from a DHCP server and you move the master to a different unit, its IP address might change and you could lose the connection to the switch.

SNMP

22

Simple Network Management Protocol

This chapter includes the following sections:

- *Add a New Community*
- *Enable SNMP Trap*
- *SNMP Version 3*
- *sFlow*
- *Time-Based Sampling of Counters with sFlow*

Add a New Community

The example is shown as CLI commands and as a web interface procedure.

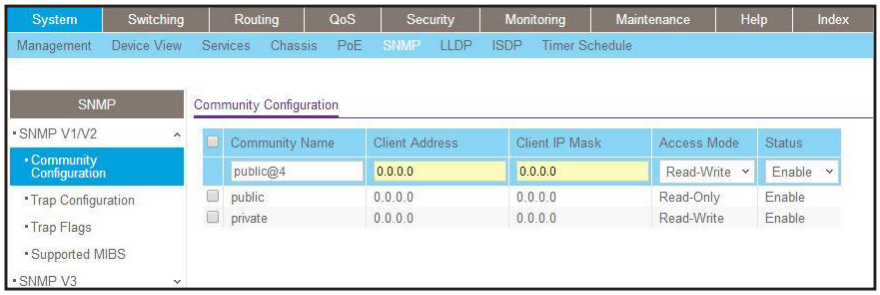
CLI: Add a New Community

```
(Netgear switch) #config
(Netgear switch) (Config)#snmp-server community rw public@4
```

Web Interface: Add a New Community

1. Select **System > SNMP > SNMP V1/V2 > Community Configuration**.

   A screen similar to the following displays.



2. In the **Community Name** field, enter **public@4**.
3. In the **Client Address** field, enter **0.0.0.0**.
4. In the **Client IP Mask** field, enter **0.0.0.0**.
5. In the **Access Mode** field, select **Read/Write**.
6. In the **Status** field, select **Enable**.
7. Click **Add**.

Enable SNMP Trap

The example is shown as CLI commands and as a web interface procedure.

CLI: Enable SNMP Trap

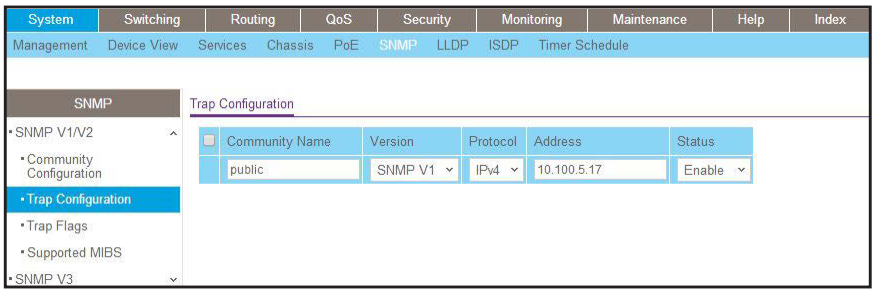
This example shows how to send SNMP trap to the SNMP server.

```
(Netgear switch) #config
(Netgear switch) (Config)# snmptrap public 10.100.5.17
                                        Enable send trap to SNMP server 10.100.5.17
(Netgear switch) (Config)#snmp-server traps linkmode
                                        Enable send link status to the SNMP server
when link status changes.
```

Web Interface: Enable SNMP Trap

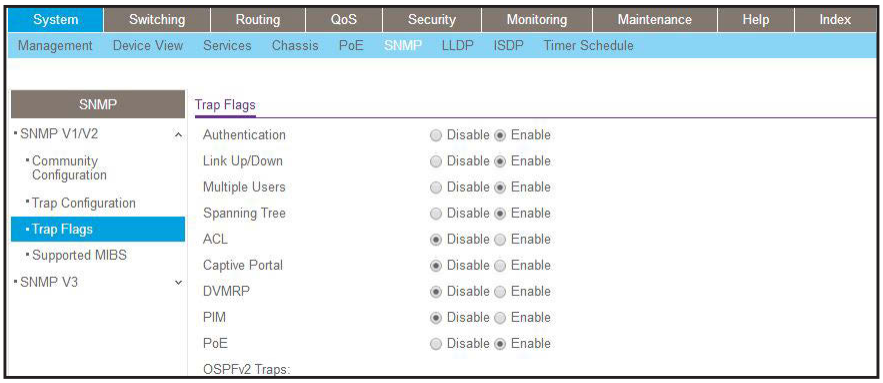
1. Enable SNMP trap for the server 10.100.5.17.
   a. Select **System > SNMP > SNMP V1/V2 > Trap Configuration**.

      A screen similar to the following displays.



   b. In the **Community Name** field, enter **public**.
   c. In the **Version** list, select **SNMPv1**.
   d. In the **Address** field, enter **10.100.5.17**.
   e. In the **Status** field, select **Enable**.
   f. Click the **Add** button.
2. Set the Link Up/Down flag.
   a. Select **System > SNMP > SNMP V1/V2 > Trap Flags**.

A screen similar to the following displays.



b. For Link Up/Down, select the **Enable** radio button.

c. Click **Apply**.

SNMP Version 3

The example is shown as CLI commands and as a web interface procedure.

CLI: Configure SNMPv3

```
(Netgear Switch) #config
(Netgear Switch) (Config)#users passwd admin
Enter old password:
Enter new password:12345678
Confirm new password:12345678
Password Changed!
change the password to “12345678”
(Netgear Switch) (Config)#users snmpv3 authentication admin md5
Set the authentication mode to md5
(Netgear Switch) (Config)#users snmpv3 encryption admin des 12345678
Set the encryption mode to des and the key is “12345678”
```

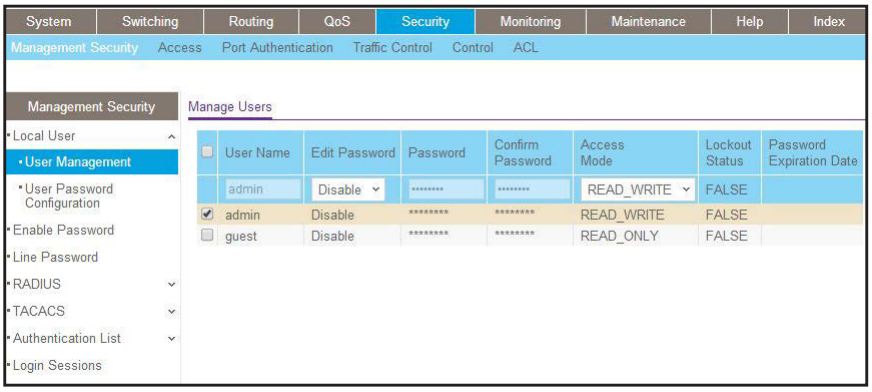
Web Interface: Configure SNMPv3

1. Change the user password.

   If you set the authentication mode to MD5, you must make the length of password longer than 8 characters.

   a. Select **Security > Management Security > User Configuration > User Management**.

      A screen similar to the following displays.



   b. Under User Management, scroll down and select the User Name **admin** check box. Now admin appears in the User Name field at the top.

   c. In the **Password** field, enter **12345678**.

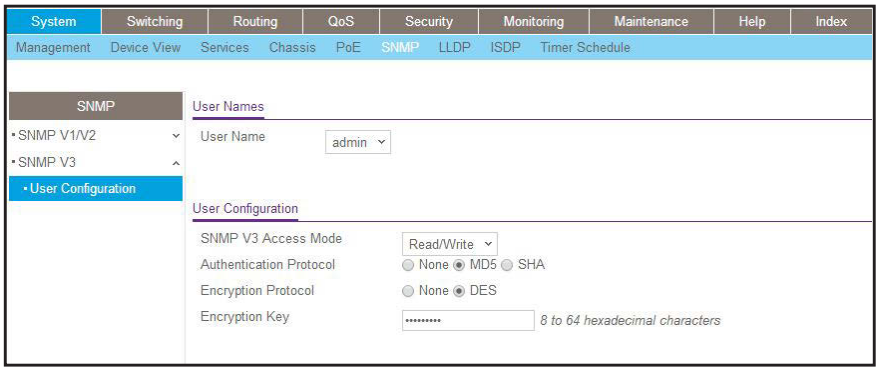
   d. In the **Confirm Password** field, enter **12345678**.

   e. Click **Apply** to save the settings.

2. Configure the SNMP V3 user.

   a. Select **System > Management > User Configuration**.

      A screen similar to the following displays.



   b. In the **User Name** field, select the **admin**.

   c. For Authentication Protocol, select the **MD5** radio button.

   d. For Encryption Protocol, select the **DES** radio button.

   e. In the **Encryption Key** field, enter **12345678**.

   f. Click **Apply** to save the settings.

sFlow

sFlow is the standard for monitoring high-speed switched and routed networks. sFlow technology is built into network equipment and gives complete visibility into network activity, enabling effective management and control of network resources.

The sFlow monitoring system consists of an sFlow agent (embedded in a switch or router or in a standalone probe) and a central sFlow collector. The sFlow agent uses sampling technology to capture traffic statistics from the device it is monitoring. The sFlow datagrams are used to immediately forward the sampled traffic statistics to an sFlow collector for analysis.

The sFlow agent uses two forms of sampling: statistical packet-based sampling of switched or routed packet flows, and time-based sampling of counters.

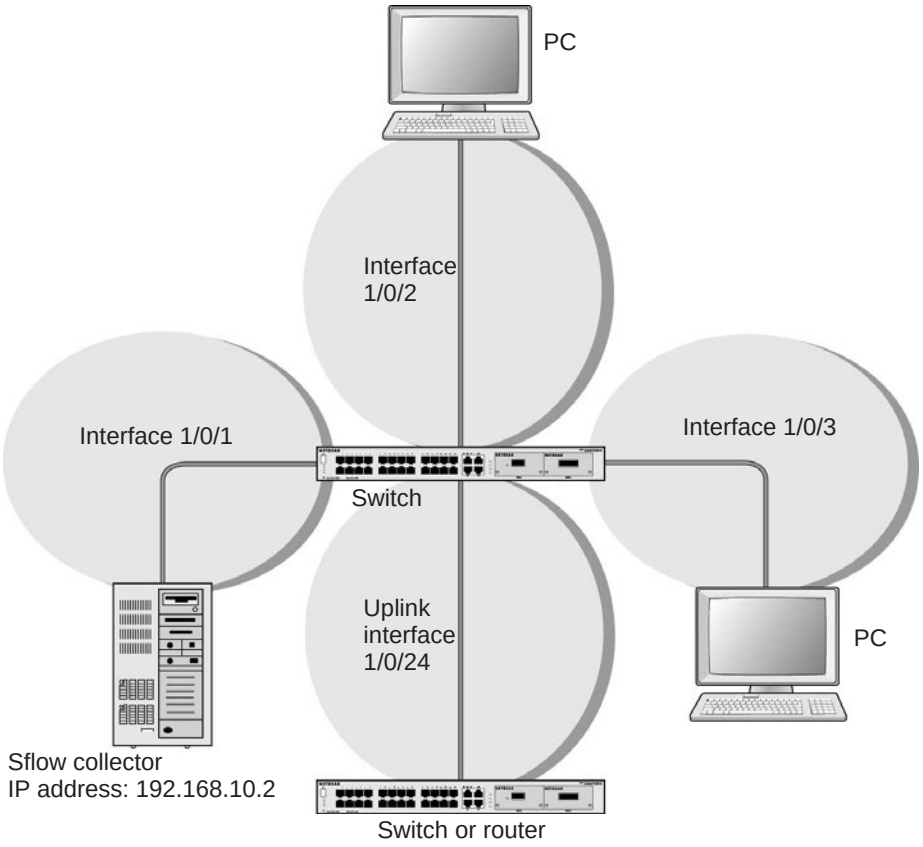


Figure 49. sFlow

CLI: Configure Statistical Packet-Based Sampling of Packet Flows with sFlow

1. Configure the sFlow receiver (sFlow collector) IP address. In this example, sFlow samples will be sent to the destination address 192.168.10.2.

```
(Netgear Switch) (Config)# sflow receiver 1 ip 192.168.10.2
```

2. Configure the sFlow receiver timeout. Here sFlow samples will be sent to this receiver for the duration of 31536000 seconds. That is approximately 1 year.

```
(Netgear Switch) (Config)# sflow receiver 1 owner NetMonitor timeout 31536000
```

3. Here, the default maximum datagram size is 1400. It can be modified to a value between 200 and 9116 using the command `sflow receiver 1 maxdatagram <size>`.

```
(Netgear Switch) #show sflow receivers

Receiver Owner    Time out   Max Datagram Port  IP Address
Index    String              Size
-------- -------- ---------- ------------ ----- -------------------------
1        NetMonit 31535988   1400         6343  192.168.10.2
2                 0          1400         6343  0.0.0.0
3                 0          1400         6343  0.0.0.0
4                 0          1400         6343  0.0.0.0
5                 0          1400         6343  0.0.0.0
6                 0          1400         6343  0.0.0.0
7                 0          1400         6343  0.0.0.0
8                 0          1400         6343  0.0.0.0
```

4. Configure the sampling port sFlow receiver index, sampling rate, and sampling maximum header size. You need to repeat these for all the ports to be sampled.

```
(Netgear Switch) (Config)# interface 1/0/1
(Netgear Switch) (Interface 1/0/1)# sflow sampler 1
(Netgear Switch) (Interface 1/0/1)# sflow sampler rate 1024
(Netgear Switch) (Interface 1/0/1)# sflow sampler maxheadersize 64
```

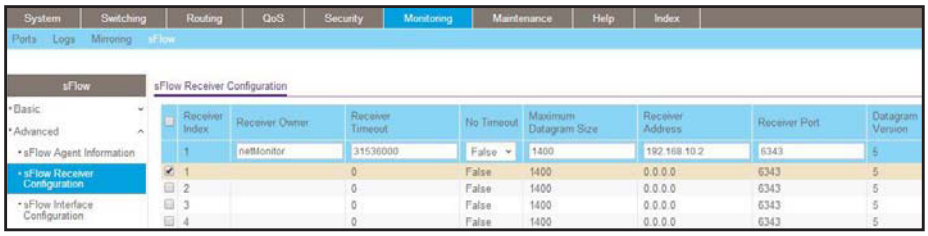
5. View the sampling port configurations.

```
(Netgear Switch)) #show sflow samplers
Sampler            Receiver                Packet         Max Header
Data Source        Index                 Sampling Rate       Size
-----------       ---------------     -----------------  ------------------
1/0/1                    1                1024                 64
```

Web Interface: Configure Statistical Packet-based Sampling with sFlow

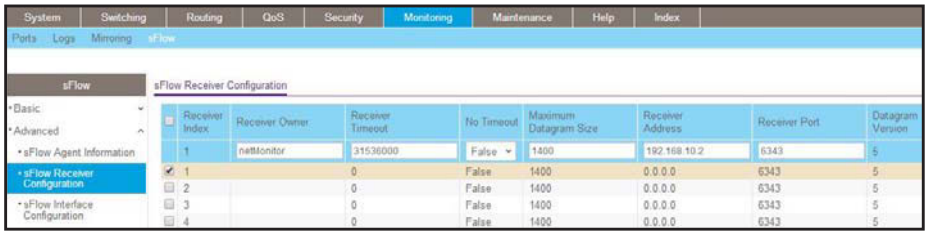
1. Configure the sFlow receiver IP address.
   a. Select **Monitoring > sFlow > Advanced > sFlow Receiver Configuration**.
   b. Select the **1** check box.
   c. In the **Receiver Owner** field, enter **NetMonitor**.
   d. In the **Receiver Timeout** field, enter **31536000**.
   e. In the **Receiver Address** field, enter **192.168.10.2**.

   A screen similar to the following displays.



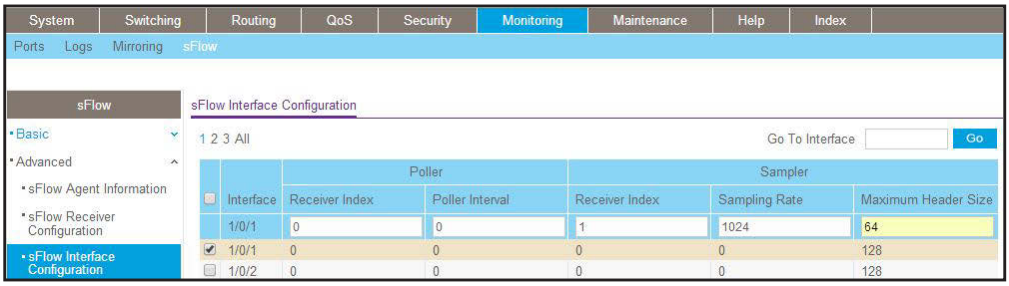
   f. Click **Apply**.

   A screen similar to the following displays.



2. Configure the sampling ports sFlow receiver index, sampling rate, and sampling maximum header size.
   a. Select **Monitoring > sFlow > Advanced > sFlow Interface Configuration**.

A screen similar to the following displays.



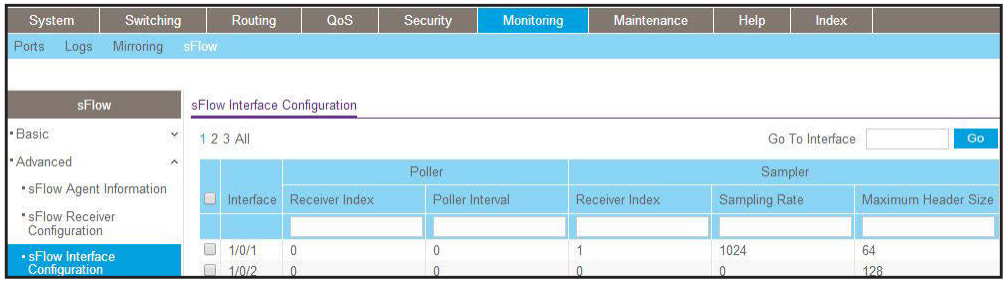
b. Select the Interface **1/0/1** check box.

c. In the **Sampling Rate** field, enter **1024**.

d. In the **Maximum Header Size** field, enter 64.

e. Click **Apply**.

A screen similar to the following displays.



Time-Based Sampling of Counters with sFlow

CLI: Configure Time-Based Sampling of Counters with sFlow

1. Configure the sampling port sFlow receiver index, and polling interval. You need to repeat this for all the ports to be polled.

```
(Netgear Switch) (Config)# interface 1/0/1
(Netgear Switch) (Interface 1/0/1)# sflow poller 1
(Netgear Switch) (Interface 1/0/1)# sflow poller interval  300
```

2. View the polling port configurations.

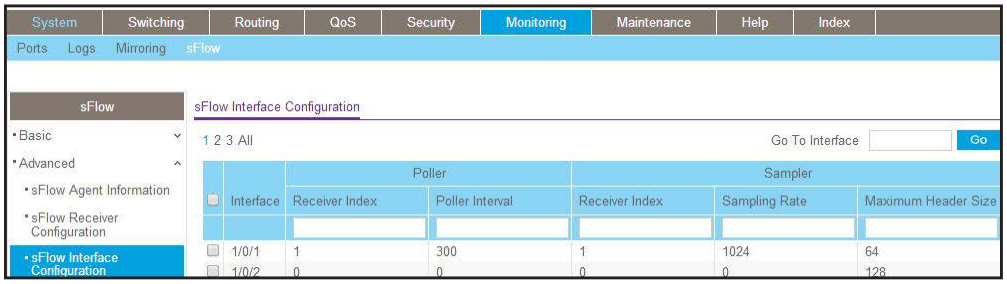
```
(Netgear Switch) #show sflow pollers
Poller            Receiver            Poller
Data Source       Index               Interval
----------        ---------           ---------
1/0/1             1                   300
```

Web Interface: Configure Time-Based Sampling of Counters with sFlow

Configure the sampling ports sFlow receiver index, and polling interval:

1. Select **Monitoring > sFlow > Advanced > sFlow Interface Configuration**.
2. Select the Interface **1/0/1** check box.
3. In the **Poller Interval** field, enter **300**.

   A screen similar to the following displays.



4. Click **Apply**.

DNS

23

Domain Name System

This chapter includes the following sections:

- *Domain Name System Concepts*
- *Specify Two DNS Servers*
- *Manually Add a Host Name and an IP Address*

Domain Name System Concepts

The Domain Name System (DNS) protocol maps a host name to an IP address, allowing you to replace the IP address with the host name for IP commands such as a ping and a traceroute, and for features such as RADIUS, DHCP relay, SNTP, SNMP, TFTP, SYSLOG, and UDP relay.

You can obtain the DNS server IP address from your ISP or public DNS server list. DNS is used to resolve the host's IP address. It enables a static host name entry to be used to resolve the IP address. The following are examples of how the DNS feature is used.

Specify Two DNS Servers

The following example shows how to specify two DNS servers (that is, two IP addresses for DNS servers) and to resolve an IP address using the DNS server. The example is shown as CLI commands and as a web interface procedure.

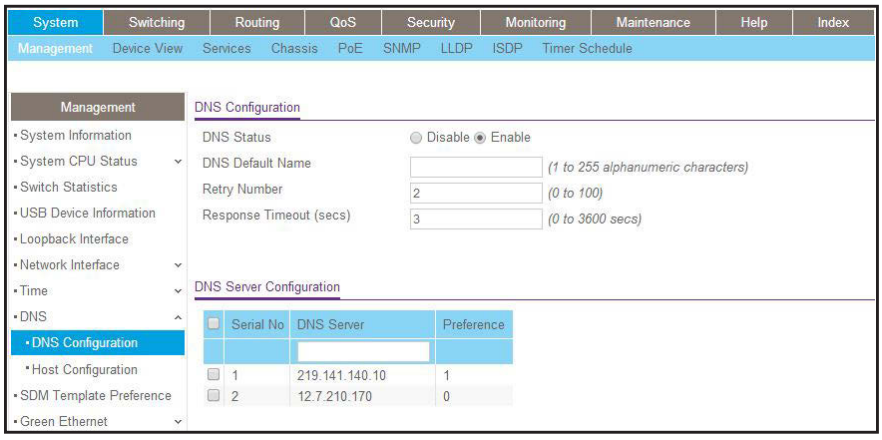
CLI: Specify Two DNS Servers

```
(Netgear Switch)#config
(Netgear Switch) (Config)#ip name-server 12.7.210.170 219.141.140.10
(Netgear Switch) (Config)#ip domain-lookup
(Netgear Switch) (Config)#exit
(Netgear Switch)#ping www.netgear.com

Send count=3, Receive count=3 from 206.82.202.46
```

Web Interface: Specify Two DNS Servers

1. Select **System > Management > DNS > DNS Configuration**.

   A screen similar to the following displays.



2. Under DNS Server Configuration, in the **DNS Server** field, enter **12.7.210.170**.
3. Click **Add**.
4. In the **DNS Server** field, enter **219.141.140.10**.
5. Click **Add**.

Both DNS servers now show in the DNS Server Configuration table.

Manually Add a Host Name and an IP Address

The following example shows commands to add a static host name entry to the switch so that you can use this entry to resolve the IP address. The example is shown as CLI commands and as a web interface procedure.

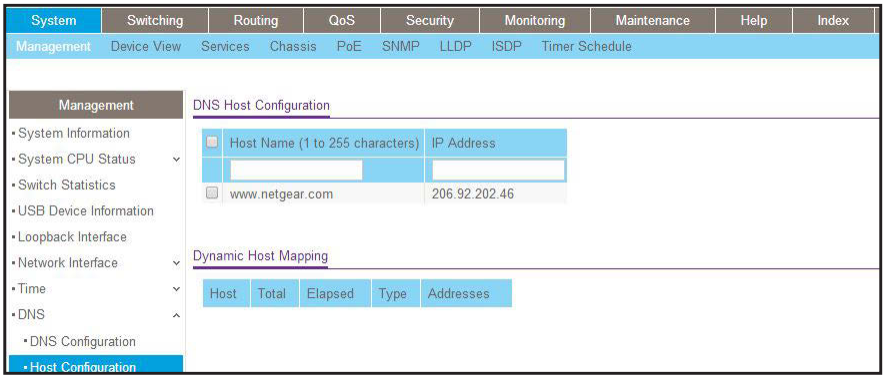
CLI: Manually Add a Host Name and an IP Address

```
(Netgear Switch)#config
(Netgear Switch) (Config)#ip host www.netgear.com 206.82.202.46
(Netgear Switch) (Config)#ip domain-lookup
(Netgear Switch) (Config)#ping www.netgear.com

Send count=3, Receive count=3 from 206.82.202.46
```

Web Interface: Manually Add a Host Name and an IP Address

1. Select **System > Management > DNS > Host Configuration**.

   A screen similar to the following displays.



2. Under DNS Host Configuration, enter the following information:
   - In the **Host Name** field, enter **www.netgear.com**.
   - In the **IP Address** field, enter **206.82.202.46**.
3. Click **Add**.

The host name and IP address now show in the DNS Host Configuration table.

DHCP Server

24

Dynamic Host Configuration Protocol Server

This chapter includes the following sections:

- *Dynamic Host Configuration Protocol Concepts*
- *Configure a DHCP Server in Dynamic Mode*
- *Configure a DHCP Server that Assigns a Fixed IP Address*

Dynamic Host Configuration Protocol Concepts

When a client sends a request to a Dynamic Host Configuration Protocol (DHCP) server, the DHCP server assigns the IP address from address pools that are specified on the switch. The network in the DHCP pool must belong to the same subnet.

A DHCP server allows the switch to dynamically assign an IP address to a DHCP client that is attached to the switch. It also enables the IP address to be assigned based on the client's MAC address. The following are examples of how the DHCP Server feature is used.

Configure a DHCP Server in Dynamic Mode

The following example shows how to create a DHCP server with a dynamic pool. The example is shown as CLI commands and as a web interface procedure.

CLI: Configure a DHCP Server in Dynamic Mode

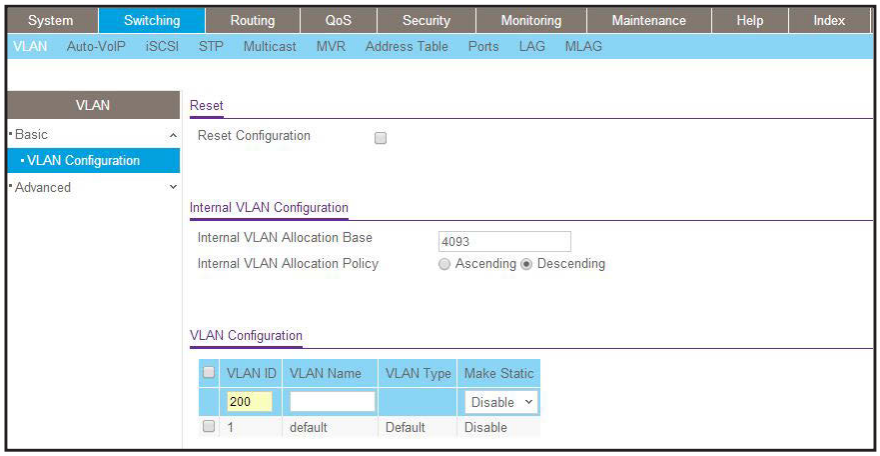
```
(Netgear Switch) #vlan database
(Netgear Switch) (Vlan)#vlan 200
(Netgear Switch) (Vlan)#vlan routing 200
(Netgear Switch) (Vlan)#exit
(Netgear Switch) (Config)#interface 1/0/1
(Netgear Switch) (Interface 1/0/1)#vlan participation include 200
(Netgear Switch) (Interface 1/0/1)#vlan pvid 200
(Netgear Switch) (Interface 1/0/1)#exit
(Netgear Switch) (Config)#interface vlan 200
(Netgear Switch) (Interface-vlan 200)#routing
(Netgear Switch) (Interface-vlan 200)#ip address 192.168.100.1 255.255.255.0
(Netgear Switch) #config
(Netgear Switch) (Config)#service dhcp
(Netgear Switch) (Config)#ip dhcp pool pool_dynamic
(Netgear Switch) (Config)#network 192.168.100.0 255.255.255.0
```

Note: If there is no DHCP L3 relay between client PC and DHCP server, there must be an active route whose subnet is the same as the DHCP dynamic pool's subnet.

Web Interface: Configure a DHCP Server in Dynamic Mode

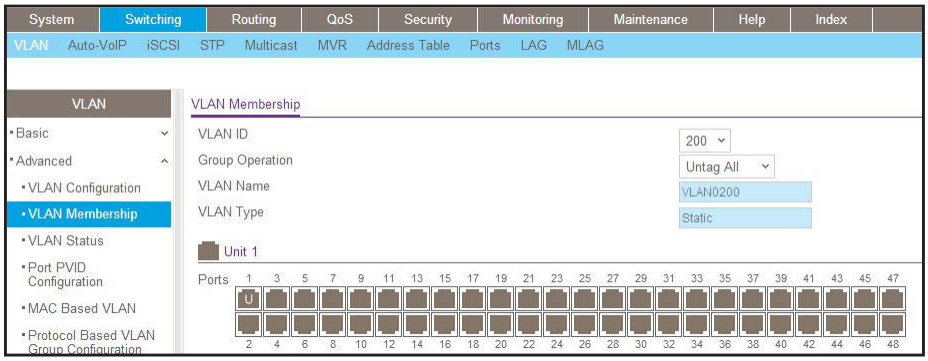
1. Create VLAN 200.
   a. Select **Switching > VLAN > Basic > VLAN Configuration**.

      A screen similar to the following displays.



   b. Under VLAN Configuration, in the **VLAN ID** field, enter **200**.
   c. Click **Add**.
2. Add port 1/0/1 to VLAN 200.
   a. Select **Switching > VLAN >Advanced > VLAN Membership**.

      A screen similar to the following displays.

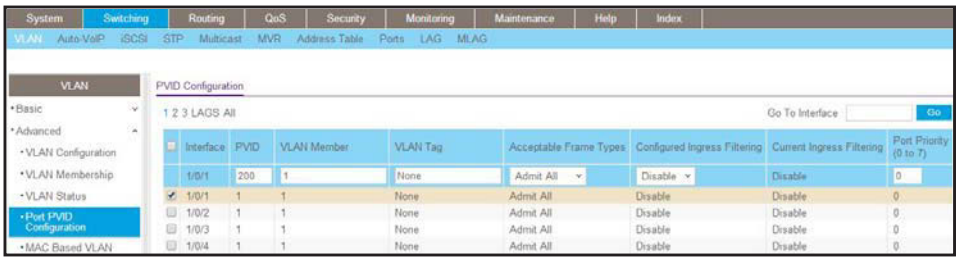


   b. In the **VLAN ID** field, select **200**.
   c. Click **Unit 1**. The ports display.
   d. Click the gray boxes under ports **1** and **24** until **U** displays.

      The U specifies that the egress packet is untagged for the port.

   e. Click **Apply**.
3. Assign PVID to the VLAN 200.
   a. Select **Switching > VLAN> Advanced > Port PVID Configuration**.

A screen similar to the following displays.



b. Under Port PVID Configuration, scroll down and select the **1/0/1** check box.

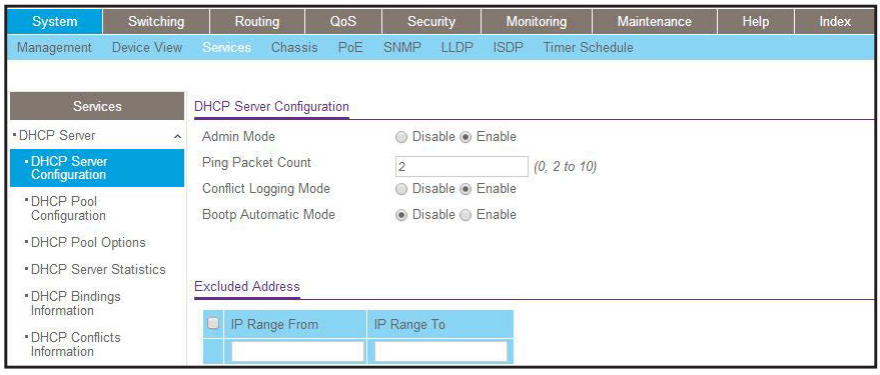
c. In the **PVID (1 to 4093)** field, enter **200**.

d. Click **Apply** to save the settings.

4. Create a new DHCP pool.

a. Select **System > Services > DHCP Server > DHCP Server Configuration**.

A screen similar to the following displays.

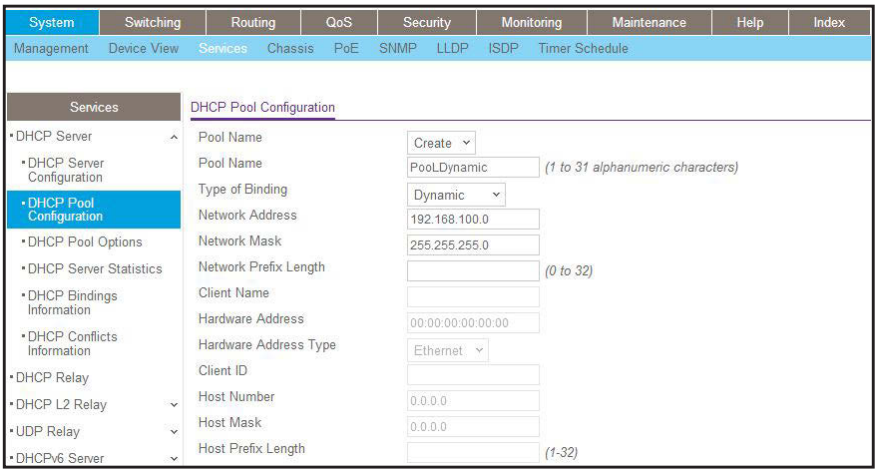


b. For Admin Mode, select the **Enable** radio button.

c. Click **Apply** to enable the DHCP service.

d. Select **System > Services > DHCP Server > DHCP Pool Configuration**.

A screen similar to the following displays.



e. Under DHCP Pool Configuration, enter the following information:
   - In the **Pool Name** list, select **Create**.
   - In the **Pool Name** field, enter **pool_dynamic**.
   - In the **Type of Binding** list, select **Dynamic**.
   - In the **Network Number** field, enter **192.168.100.0**.
   - In the **Network Mask** field, enter **255.255.255.0**. As an alternate, you can enter **24** in the **Network Prefix Length** field. Do not fill in both the Network Mask field and Network Prefix Length fields.
   - In the **Days** field, enter **1**.

f. Click **Add**.

The pool_dynamic name is now added to the Pool Name drop-down list.

Configure a DHCP Server that Assigns a Fixed IP Address

The following example shows how to set up a DHCP server with an IP address pool and let the DHCP server assign a fixed IP address based on a MAC address. The example is shown as CLI commands and as a Web interface procedure.

CLI: Configure a DHCP Server that Assigns a Fixed IP Address

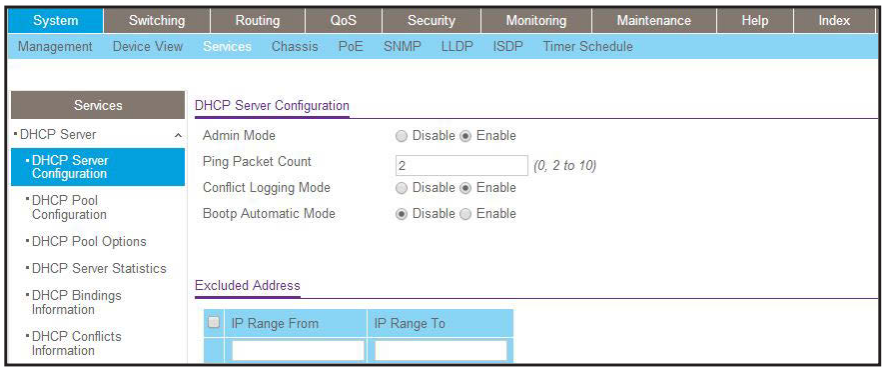
```
(Netgear Switch)#config
(Netgear Switch) (Config)#service dhcp
(Netgear Switch) (Config)#ip dhcp pool pool_manual
(Netgear Switch) (Config)#client-name dhcpclient
(Netgear Switch) (Config)#hardware-address 00:01:02:03:04:05
(Netgear Switch) (Config)#host 192.168.200.1 255.255.255.0
(Netgear Switch) (Config)#client-identifier 01:00:01:02:03:04:05
```

Note: The unique identifier is a concatenation of the media type and MAC addresses. For example, the Microsoft client identifier for Ethernet address c8:19:24:88:f1:77 is 01:c8:19:24:88:f1:77, where 01 represents the Ethernet media type. For more information, see the “Address Resolution Protocol Parameters” section of RFC 1700.

Web Interface: Configure a DHCP Server that Assigns a Fixed IP Address

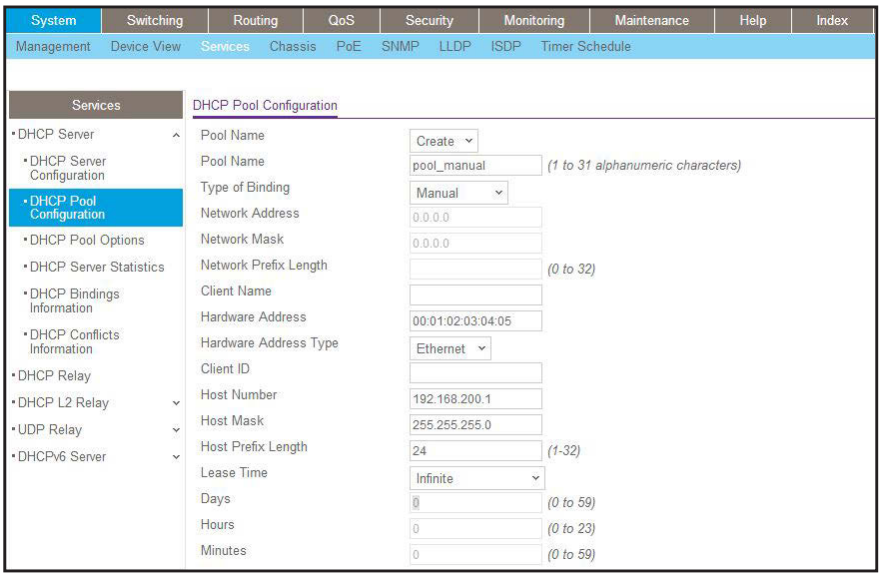
1. Select **System > Services > DHCP Server > DHCP Server Configuration**.

   A screen similar to the following displays.



2. For Admin Mode, select the **Enable** radio button.
3. Click **Apply** to enable the DHCP service.
4. Select **System > Services > DHCP Server > DHCP Pool Configuration**.

   A screen similar to the following displays.



5. Under DHCP Pool Configuration, enter the following information:
   - In the **Pool Name** list, select **Create**.
   - In the **Pool Name** field, enter **pool_manual**.
   - In the **Type of Binding** list, select **Manual**.
   - In the **Client Name** field, enter **dhcpclient**.
   - In the **Hardware Address** field, enter **00:01:02:03:04:05**.

- In the **Hardware Type** list, select **ethernet**.
- In the **Host Number** field, enter **192.168.200.1**.
- In the **Network Mask** field, enter **255.255.255.0**. As an alternate, you can enter **24** in the **Network Prefix Length** field.
- In the **Days** field, enter **1**.

6. Click **Add**. The pool_manual name is now added to the Pool Name drop-down list.

25 DHCPv6 Server

Dynamic Host Configuration Protocol version 6 Server

This chapter includes the following sections:

- *Dynamic Host Configuration Protocol Version 6 Concepts*
- *CLI: Configure DHCPv6 Prefix Delegation*
- *Web Interface: Configure DHCPv6 Prefix Delegation*
- *Configure a Stateless DHCPv6 Server*
- *Configure a Stateful DHCPv6 Server*
- *CLI: Set Up a Configuration With a DHCPv6 Server and DHCPv6 Relay*

Dynamic Host Configuration Protocol Version 6 Concepts

Dynamic Host Configuration Protocol version 6 (DHCPv6) for IPv6 is used to assign IPv6 addresses statefully and distribute other configuration information such as domain name or DNS server.

DHCPv6 supports stateful address allocation, prefix delegation, and stateless services. This chapter describes how to configure the prefix delegation mode using a DHCPv6 pool. When you create a DHCPv6 pool, you need to assign a prefix to the client DHCP unique identifier (DUID).

DUID is used to identify the client's unique DUID value. The format is xx:xx:xx:xx:xx:xx. RFC3315 defines three types:

- Link-layer address plus time:
  - 00:01:hardware type:time:link-layer address
  - Hardware type - 16 bit hardware type reserved by IANA. 1 means an Ethernet device.
  - Time: 32-bit unsigned integer. The time in seconds when this DUID was generated since 00:00:00 1/1/2000.
  - Link-layer address - The link layer address of a device generating the DUID.
- Vendor-assigned unique ID based on Enterprise Number:
  - 00:02:enterprise-number:identifier
  - Enterprise-number - 32-bit integer reserved by IANA.
  - Identifier - Variable length data for each vendor
- Link-layer address:
  - 00:03:hardware type:link-layer address
  - Hardware type - 16 bit hardware type reserved by IANA. 1 means an Ethernet device.
  - Link-layer address - The link layer address of a device generating the DUID.

In the following case, the CPE router requests prefix from the PE router. The PE router chooses prefix (2001:1::/64) for delegation, and responds with the prefix to the requesting CPE router. The CPE router subnets the prefix and assigns the longer prefixes to links in the user's network. The CPE router is then responsible to assign the 2001:1:1::/96 to one user's network and 2001:1:2::/96 to another user's network.

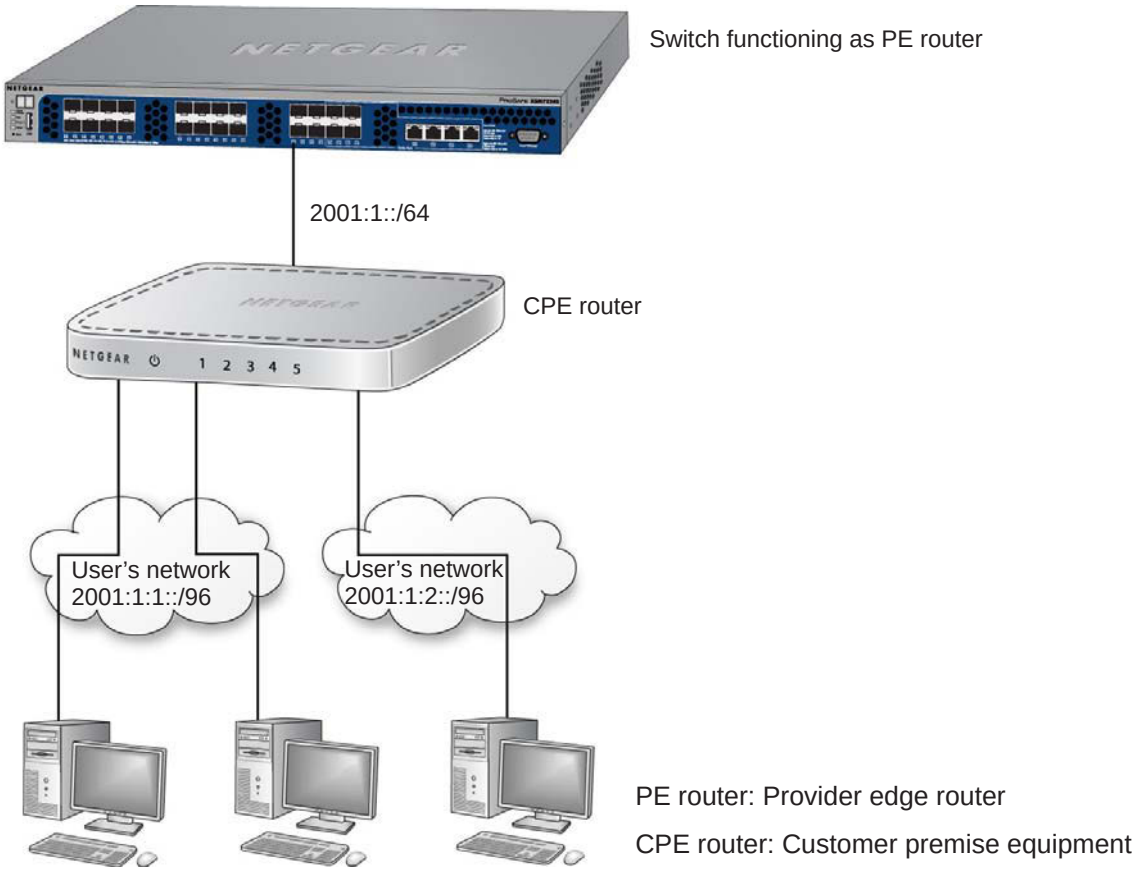


Figure 50. DHCPv6 stateful IPv6 address assignment

CLI: Configure DHCPv6 Prefix Delegation

1. Enable IPv6 routing.

```
(Netgear Switch) #configure
(NETGEAR SWITCH) (Config)#ip routing
(NETGEAR SWITCH) (Config)#ipv6 unicast routing
```

2. Create a DHCPv6 pool and enable DHCP service.

```
(NETGEAR SWITCH) (Config)#service dhcpv6
(NETGEAR SWITCH) (Config)#ipv6 dhcp pool pool1
(NETGEAR SWITCH) (Config dhcp6 pool)#domain name netgear.com
(NETGEAR SWITCH) (Config dhcp6s pool)#prefix delegation 2001:1::/64
00:01:00:01:15:40:14:4f:00:00:00:4d:aa:d0
(NETGEAR SWITCH) (Config dhcp6s pool)#exit
```

3. Enable DHCPv6 service on port 1/0/9.

```
(NETGEAR SWITCH) (Config)#interface 1/0/9
(NETGEAR SWITCH) (Interface 1/0/9)#routing
(NETGEAR SWITCH) (Interface 1/0/9)#ipv6 address 2001:1::1/64
(NETGEAR SWITCH) (Interface 1/0/9)#ipv6 enable
(NETGEAR SWITCH) (Interface 1/0/9)#ipv6 dhcp server pool1 preference 20
(NETGEAR SWITCH) (Interface 1/0/9)#exit
```

4. Show DHCPv6 binding.

```
(NETGEAR SWITCH) #show ipv6 dhcp binding
Client Address.............................. FE80::200:FF:FE4D:AAD0
Client Interface............................ 1/0/9
Client DUID.................................
00:01:00:01:15:40:14:4f:00:00:00:4d:aa:d0
Identity Association ID..................... 5090000
Binding Prefix Address/Length............... 2001:1::/64
Binding Prefix Type ........................ IA_PD
Binding Expiration (secs)................... 4294967284
Binding Prefix Valid Lifetime (secs)........ infinite
Binding Prefix Preferred Lifetime (secs)..... infinite
```

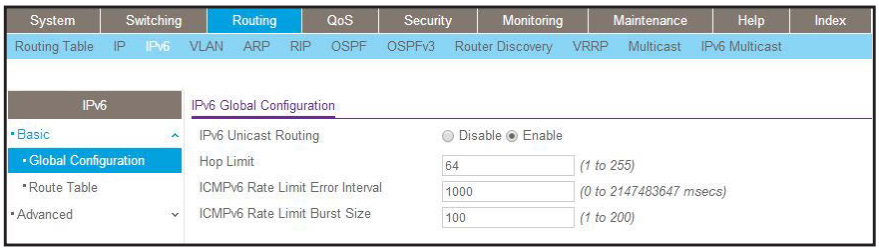
Web Interface: Configure DHCPv6 Prefix Delegation

1. Enable IP routing globally.
   a. Select **Routing > IP > Basic > IP Configuration**.

      A screen similar to the following displays.

   b. For Routing Mode, select the **Enable** radio button.
   c. Click **Apply** to save the settings.
2. Enable IPv6 unicast globally.
   a. Select **Routing > IPv6 > Basic > Global Configuration**.

A screen similar to the following displays.



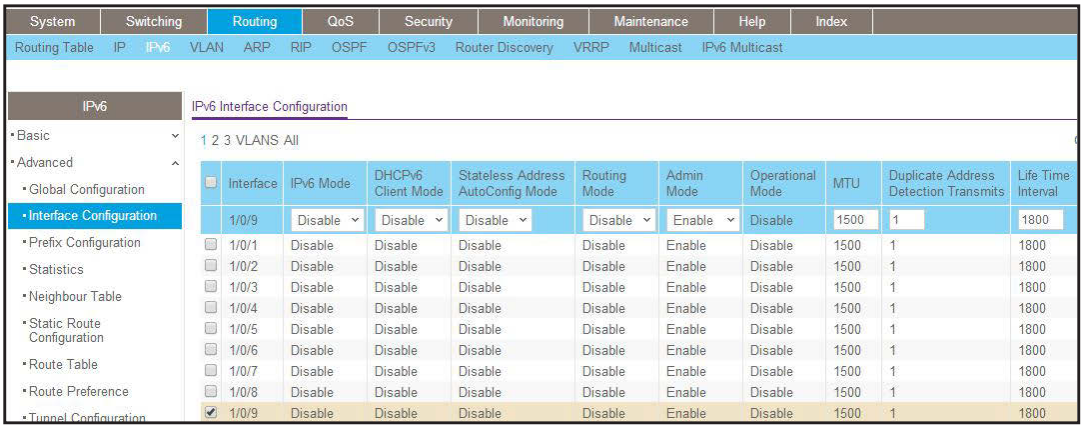
b. For IPv6 Unicast Routing, select the **Enable** radio button.

c. Click **Apply** to save the settings.

3. Enable IPv6 address on interface 1/0/9.

a. Select **Routing > IPv6 > Advanced > Interface Configuration**.

A screen similar to the following displays.



b. Scroll down and select the interface **1/0/9** check box to the left of the Interface column.

1/0/9 displays in the Interface field of the table heading.

c. Enter the following information:

- In the **IPv6 Mode** field, select **Enable**.
- In the **Routing Mode** field, select **Enable**.

d. Click **Apply** to apply the settings.

4. Configure the prefix on interface 1/0/9.

a. Select **Routing > IPv6 > Advanced > Prefix Configuration**.

A screen similar to the following displays.

b. In the **Interface** list, select interface **1/0/9**.

c. In the **Ipv6 Prefix** field, enter **2001:1::1**.

d. In the **Prefix Length** field, select **64**.

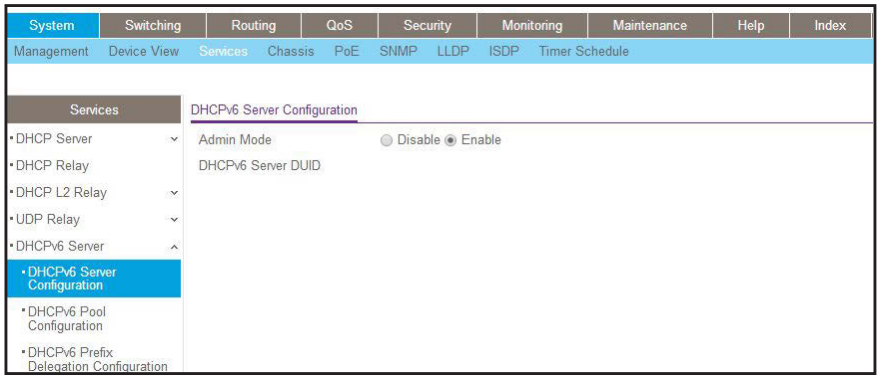
e. Click **Add.**

The IPv6 prefix for interface 1/0/9 is created.

5. Enable the DHCPv6 server configuration.

a. Select **System > Services > DHCPv6 Server > DHCPv6 Server Configuration**.

A screen similar to the following displays.



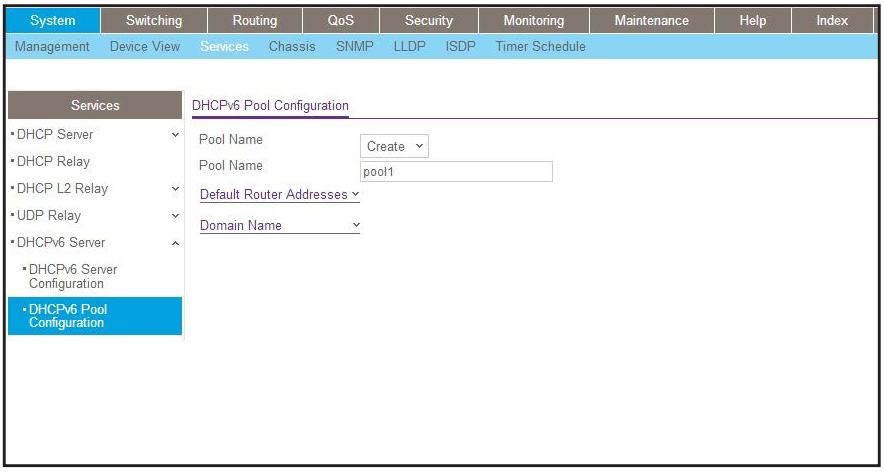
b. For Admin Mode, select the **Enable** radio button.

c. Click **Apply** to save the settings.

6. Create a DHCPv6 pool named pool1.

a. Select **System > Services > DHCP Server > DHCPv6 Pool Configuration**.

A screen similar to the following displays.



b. In the **Pool Name** list, select **Create**.

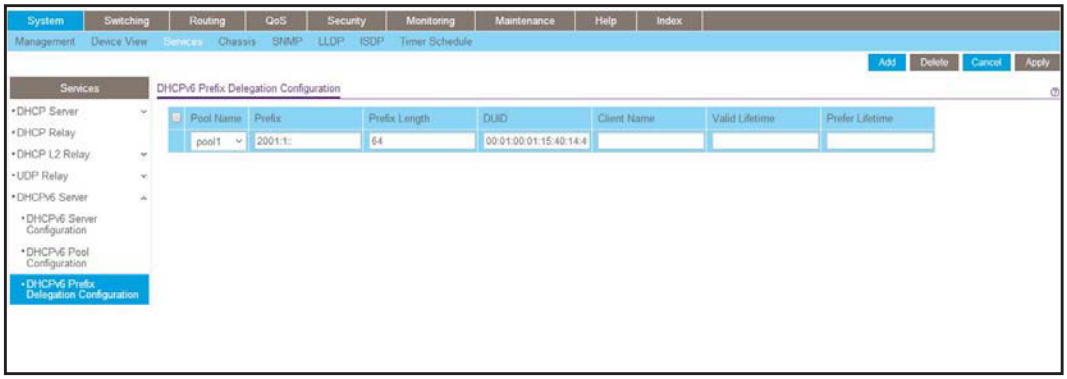
c. In the **Pool Name** field, enter **pool1**.

d. Click **Apply** to save the settings.

7. Configure the prefix in the pool1.

a. Select **System > Services > DHCPv6 Server > DHCPv6 Pool Configuration**.

A screen similar to the following displays.



b. In the **Pool Name** field, select **pool1**.

c. In the **Prefix** field, enter **2001:1::**.

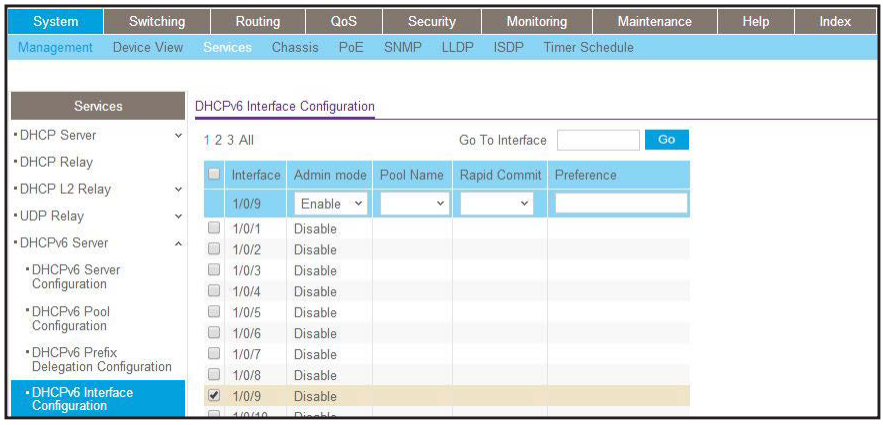
d. In the **Prefix Length** field, enter **64**.

e. Click **Apply** to save the settings.

8. Configure DHCPv6 on interface 1/0/9.

a. Select **System > Services > DHCPv6 Server > DHCPv6 Interface Configuration**.

A screen similar to the following displays.



b. Scroll down and select the interface **1/0/9** check box to the left of the Interface column.

1/0/9 displays in the Interface field of the table heading.

c. In the **Admin mode** field, select **Enable**.

d. In the **Pool Name** field, select **pool1**.

e. Click **Apply** to save the settings.

Configure a Stateless DHCPv6 Server

This example show how you can use a DHCPv6 server to pass on information about a DNS server to clients that receive an IPv6 address in autoconfiguration mode or manual mode. The configured DHCP pool does not contain a prefix pool but contains information about the DNS server. The **`ipv6 nd other-config-flag`** command must be enabled on the IPv6 interface.

The following sections show how to configure a DNS server for clients with a stateless IPv6 address using a DHCPv6 server.

CLI: Configure a Stateless DHCPv6 Server

1. Enable IPv6 routing.

```
(Netgear Switch) (Config)#ipv6 unicast-routing
```

2. Create an IPv6 pool with a DNS server and enable the DHCPv6 service.

```
(Netgear Switch) (Config)#ipv6 dhcp pool ipv6_server
(Netgear Switch) (Config-dhcp6s-pool)#dns-server 2011:9:18::1
(Netgear Switch) (Config-dhcp6s-pool)#exit
(Netgear Switch) (Config)#service dhcpv6
```

3. Enable the IPv6 DHCP server on interface 2/0/21.

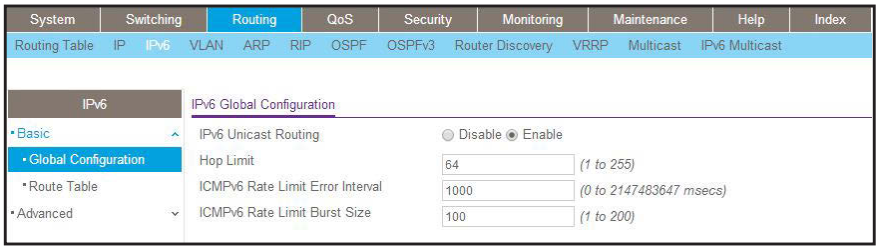
Note: In this case, you must configure the **`ipv6 nd other-config-flag`** command on the interface, otherwise the host cannot update the DNS server.

```
(Netgear Switch) (Config)#interface 2/0/21
(Netgear Switch) (Interface 2/0/21)#routing
(Netgear Switch) (Interface 2/0/21)#ipv6 address 2003:1000::1/64
(Netgear Switch) (Interface 2/0/21)#ipv6 enable
(Netgear Switch) (Interface 2/0/21)#ipv6 nd other-config-flag
(Netgear Switch) (Interface 2/0/21)#ipv6 dhcp server ipv6_server
(Netgear Switch) (Interface 2/0/21)#exit
```

Web Interface: Configure a Stateless DHCPv6 Server

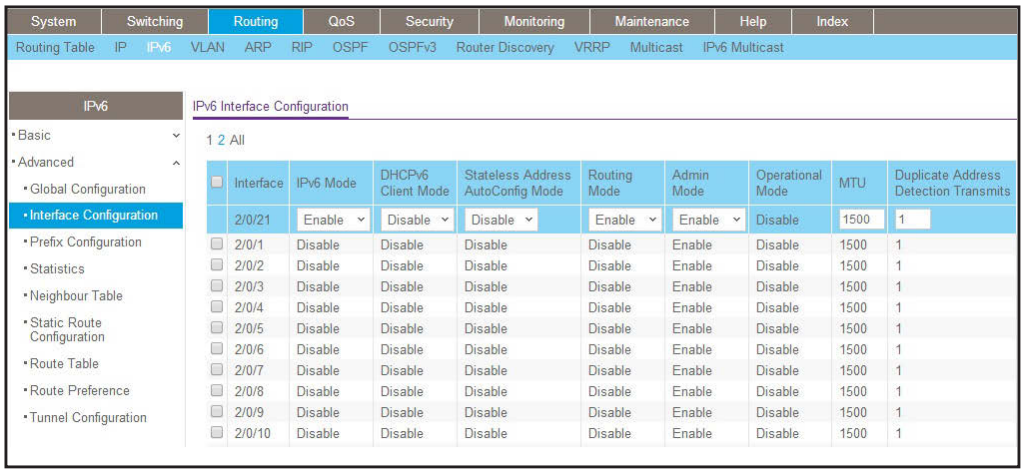
1. Enable ipv6 routing.
   a. Select **Routing > IPv6 > Basic > Global Configuration**.

      A screen similar to the following displays.



   b. For IPv6 Unicast Routing, select the **Enable** radio button.
   c. Click **Apply** to save the settings.
2. Enable IPv6 routing on interface 2/0/21.
   a. Select **Routing > IPv6 > Advanced > Interface Configuration**.

A screen similar to the following displays.



b. Scroll down and select the **2/0/21** check box to the left of the Interface column.

2/0/21 displays in the Interface field of the table heading.

c. In the **IPv6 Mode** field, select **Enable**.

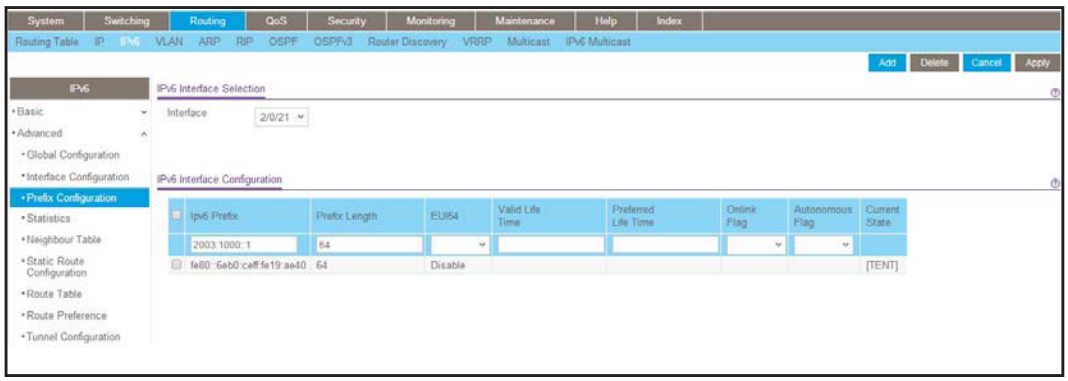
d. In the **Routing Mode** field, select **Enable**.

e. Click **Apply** to save the settings.

3. Configure IPv6 address on interface 2/0/21.

a. Select **Routing > IPv6 > Advanced > Prefix Configuration**.

A screen similar to the following displays.



b. In the **Interface** list, select **1/0/21**.

c. In the **IPv6 Prefix** field, enter **2003:1000::1**.

d. In the **Prefix Length** field, enter **64**.

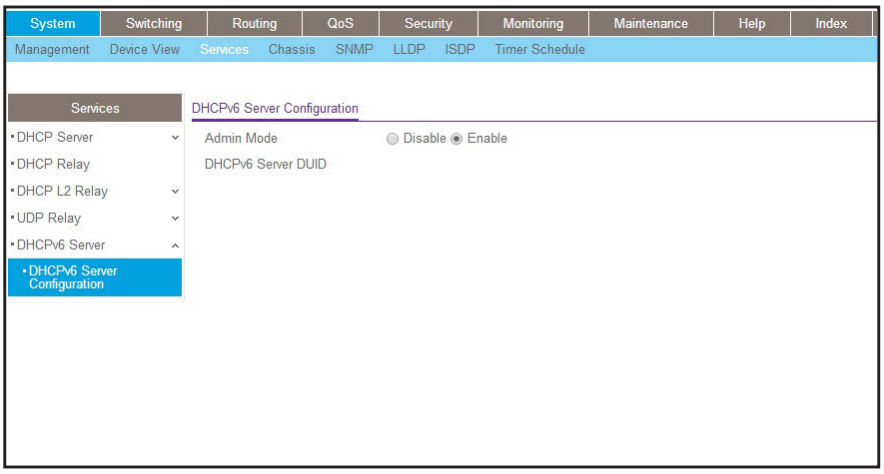
e. In the **EUI64** field, select **Disable**.

f. Click **Add**.

4. Enable DHCPv6 service.

a. Select **System > Services > DHCPv6 Server > DHCPv6 Server Configuration**.

A screen similar to the following displays.



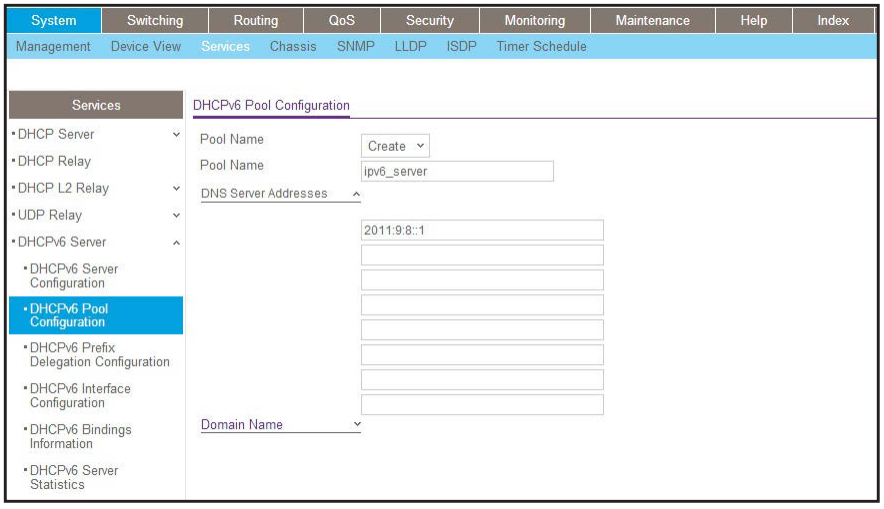
b. For Admin Mode, select the **Enable** radio button.

c. Click **Apply** to save the settings.

5. Create a DHCPv6 pool.

a. Select **System > Services > DHCP Server > DHCPv6 Pool Configuration**.

A screen similar to the following displays.



b. From the **Pool Name** list, select **Create**.

c. In the **Pool Name** field, enter **ipv6_server**.

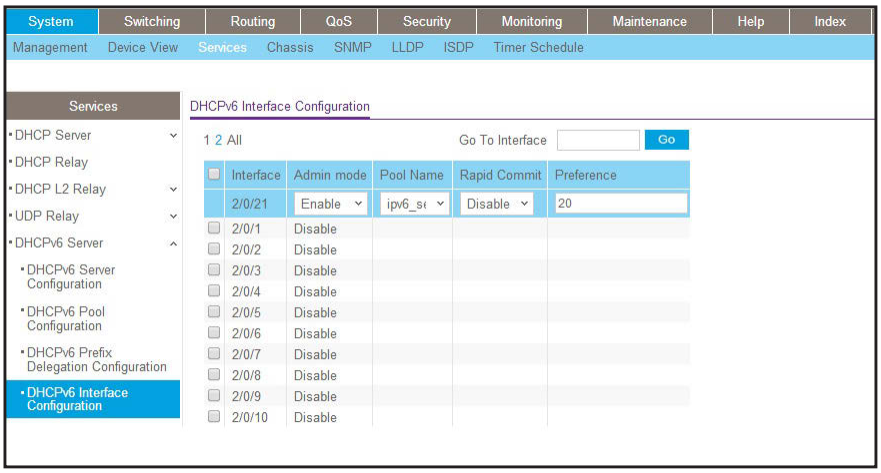
d. In the **DNS Server Addresses** fields, enter **20011:9:18::1** (which is the IPv6 address of the DNS server).

e. Click **Apply** to save the settings.

6. Enable DHCPv6 pool on interface 2/0/21.

a. Select **System > Services > DHCPv6 Server > DHCPv6 Interface Configuration**.

A screen similar to the following displays.



b. Select the **2/0/21** check box to the left of the Interface column.

2/0/21 displays in the Interface field of the table heading.

c. In the **Admin mode** field, select **Enable**.

d. In the **Pool Name** field, select **ipv6_server**.

e. Click **Apply** to save the settings.

Configure a Stateful DHCPv6 Server

This example shows how you can use a DHCPv6 server to assign an IPv6 address directly to a client in the same way that an IPv4 DHCPv4 server assigns an IPv4 address to an IPv4 client. A stateful DHCPv6 server assigns the IPv6 address to a client based on the configured IPv6 prefix in the DHCPv6 pool.

The following sections show how to configure a DHCPv6 server that functions in stateful mode.

CLI: Configure a Stateful DHCPv6 Server

1. Enable IPv6 routing.

```
(Netgear Switch) (Config)#ipv6 unicast-routing
```

2. Create an IPv6 pool with a DNS server and enable the DHCPv6 service.

```
(Netgear Switch) (Config)#ipv6 dhcp pool ipv6_server
(Netgear Switch) (Config-dhcp6s-pool)#address prefix 2001:1:2::/64
(Netgear Switch) (Config-dhcp6s-pool)#exit
(Netgear Switch) (Config)#service dhcpv6
```

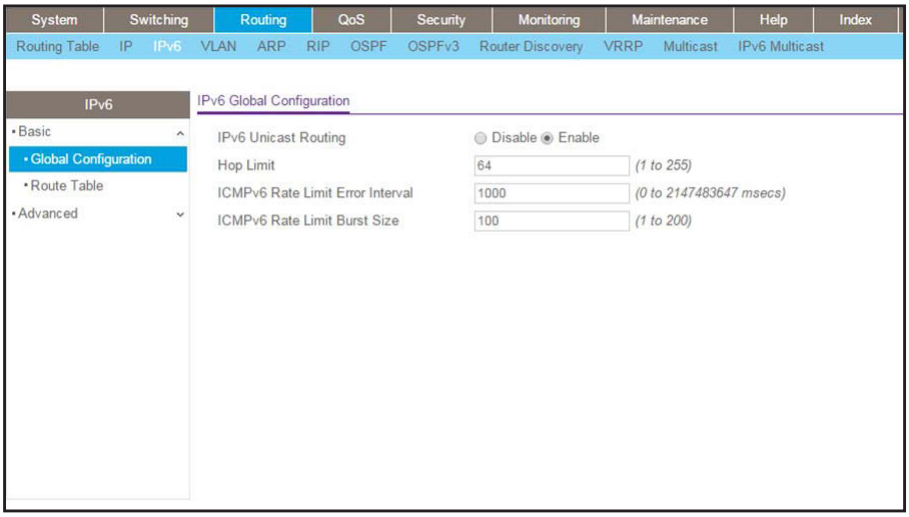
3. Enable the IPv6 DHCP server on interface 1/0/1.

```
(Netgear Switch) (Config)#interface 1/0/1
(Netgear Switch) (Interface 1/0/1)#routing
(Netgear Switch) (Interface 1/0/1)#ipv6 address 2001:1:2::1/64
(Netgear Switch) (Interface 1/0/1)#ipv6 enable
(Netgear Switch) (Interface 1/0/1)#ipv6 dhcp server ipv6_server
(Netgear Switch) (Interface 1/0/1)#exit
```

Web Interface: Configure a Stateful DHCPv6 Server

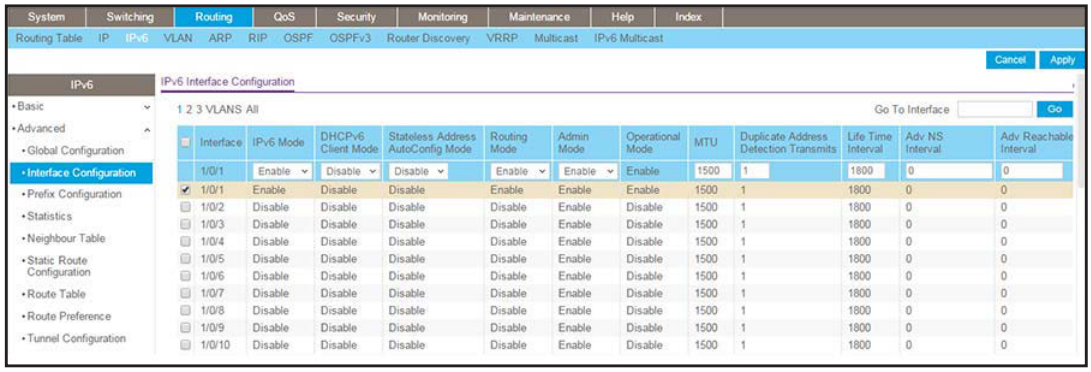
1. Enable ipv6 routing.
   a. Select **Routing > IPv6 > Basic > Global Configuration**.

      A screen similar to the following displays.



   b. For IPv6 Unicast Routing, select the **Enable** radio button.
   c. Click **Apply** to save the settings.
2. Enable IPv6 routing on interface 1/0/1.
   a. Select **Routing > IPv6 > Advanced > Interface Configuration**.

A screen similar to the following displays.



b. Select the **1/0/1** check box to the left of the Interface column.

1/0/1 displays in the Interface field of the table heading.

c. In the **IPv6 Mode** field, select **Enable**.

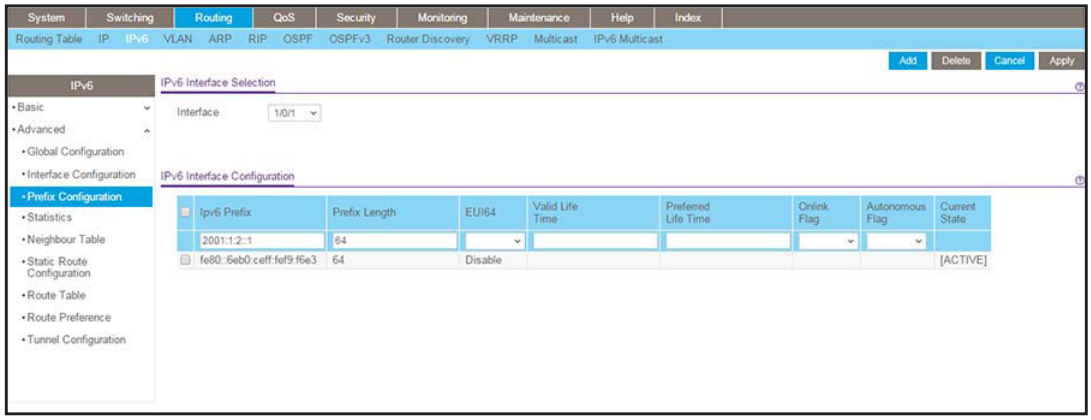
d. In the **Routing Mode** field, select **Enable**.

e. Click **Apply** to save the settings.

3. Configure the IPv6 address on interface 1/0/1.

a. Select **Routing > IPv6 > Advanced > Prefix Configuration**.

A screen similar to the following displays.



b. In the **Interface** list, select **1/0/1**.

c. In the **IPv6 Prefix** field, enter **2001:1:2::1**.

d. In the **Length** field, enter **64**.

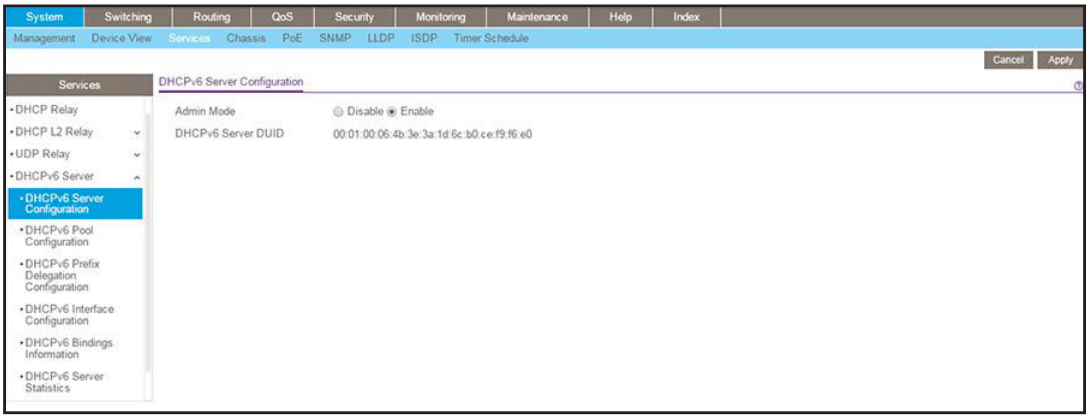
e. In the **EUI64** field, select **Disable**.

f. Click **Add**.

4. Enable the DHCPv6 service.

a. Select **System > Services > DHCPv6 Server > DHCPv6 Server Configuration**.

A screen similar to the following displays.



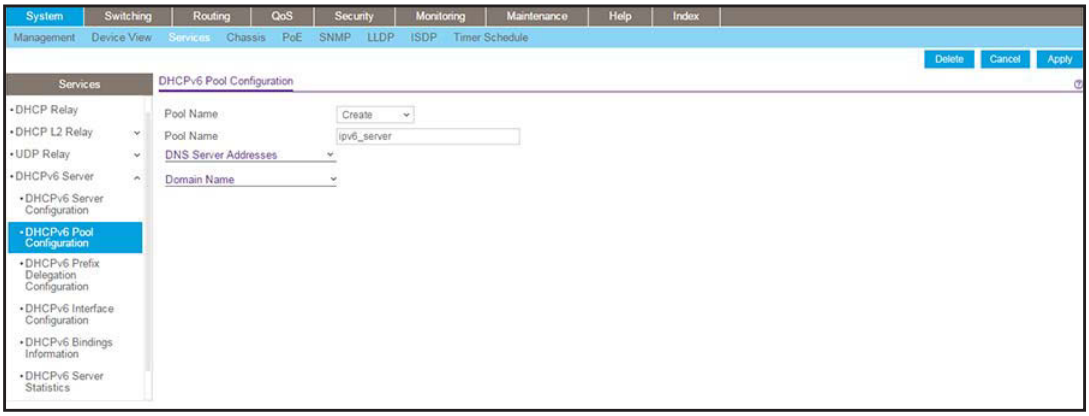
b. For Admin Mode, select the **Enable** radio button.

c. Click **Apply** to save the settings.

5. Create the DHCPv6 pool.

a. Select **System > Services > DHCP Server > DHCPv6 Pool Configuration**.

A screen similar to the following displays.



b. In the **Pool Name** list, select **Create**.

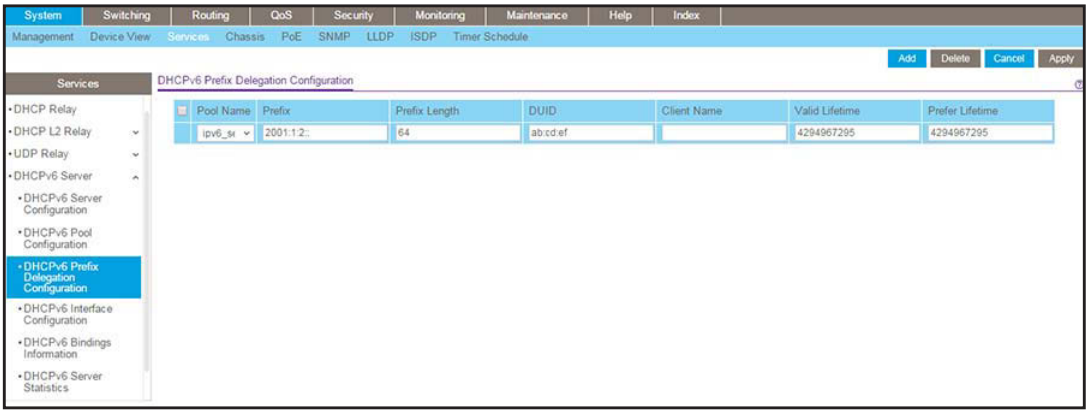
c. In the **Pool Name** field, enter **ipv6_server**.

d. Click **Apply** to save the settings.

6. Configure the prefix for the DHCPv6 pool.

a. Select **System > Services > DHCPv6 Prefix Delegation Configuration > DHCPv6 Prefix Delegation Configuration**.

A screen similar to the following displays.



b. In **Pool Name** list, select **ipv6_server**.

c. In the **Prefix** field, enter **2001:1:2::**.

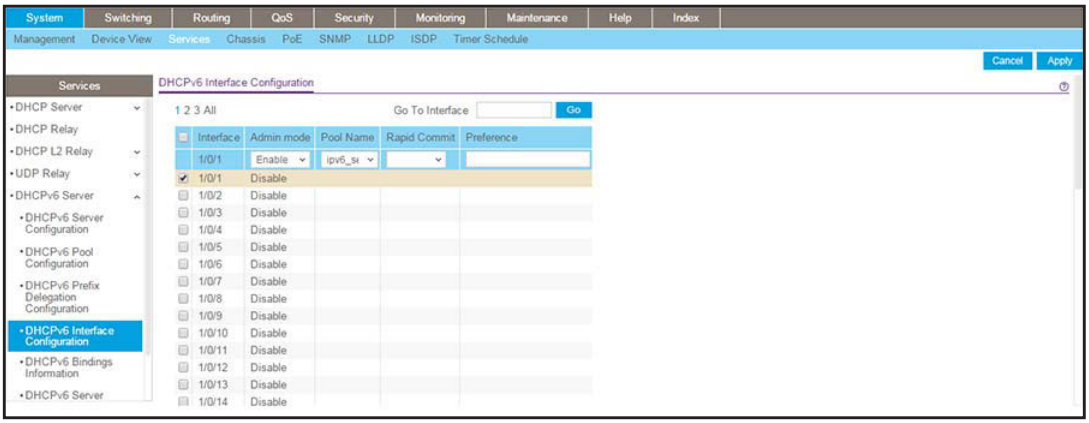
d. In the **Prefix Length** field, enter **64**.

e. Click **Add**.

7. Enable the DHCPv6 pool on interface 1/0/1.

a. **Select System > Services > DHCPv6 Server > DHCPv6 Interface Configuration**.

A screen similar to the following displays.



b. Select the interface **1/0/1** check box to the left of the Interface column.

1/0/1 displays in the Interface field of the table heading.

c. In the **Admin mode** field, select **Enable**.

d. In the **Pool Name** field, enter **ipv6_server**.

e. Click **Apply** to save the settings.

CLI: Set Up a Configuration With a DHCPv6 Server and DHCPv6 Relay

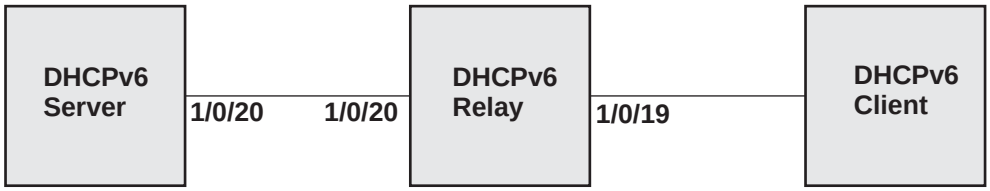


Figure 51. Configuration with a DHCPv6 server and DHCPv6 relay

This is a two-step process:

- *Configure the DHCPv6 Server*
- *Configure the DHCPv6 Relay*

Configure the DHCPv6 Server

1. Enable IPv6 routing.

```
(Netgear Switch) (Config)#ipv6 dhcp pool ipv6_server
(Netgear Switch) (Config)#ip routing
```

2. Create a DHCPv6 pool and enable DHCP service.

```
(Netgear Switch) (Config)#service dhcpv6
(Netgear Switch) (Config)#ipv6 dhcp pool pool1
(Netgear Switch) (Config-dhcp6s-pool)#domain-name netgear.com
(Netgear Switch) (Config-dhcp6s-pool)#address prefix 2001:2::/64
(Netgear Switch) (Config-dhcp6s-pool)#exit
```

3. Enable DHCPv6 service on VLAN 1.

```
(Netgear Switch) (Config)#interface vlan 1
(Netgear Switch) (Interface vlan 1)#ipv6 address 2001:1::1/64
(Netgear Switch) (Interface vlan 1)#ipv6 enable
(Netgear Switch) (Interface vlan 1)#ipv6 dhcp server pool1 preference 20
(Netgear Switch) (Interface vlan 1)#exit

(Netgear Switch) (Config)#interface 1/0/20
(Netgear Switch) (Interface 1/0/20)#vlan pvid 1
(Netgear Switch) (Interface 1/0/20)#vlan participation include 1
(Netgear Switch) (Interface 1/0/20)#exit
```

4. Configure a static route for 2001:2::/64.

```
(Netgear Switch) (Config)#ipv6 route 2001:2::/64 2001:1::2
(Netgear Switch) (Config)#exit
```

Configure the DHCPv6 Relay

1. Enable IPv6 routing.

```
(Netgear Switch) (Config)#ip routing
(Netgear Switch) (Config)#ipv6 unicast-routing
```

2. On the DHCPv6 relay, configure the interface that is connected to the DHCPv6 server.

```
(Netgear Switch) (Config)#interface vlan 1
(Netgear Switch) (Interface vlan 1)#ipv6 address 2001:1::2/64
(Netgear Switch) (Interface vlan 1)#ipv6 enable
(Netgear Switch) (Interface vlan 1)#exit

(Netgear Switch) (Config)#interface 1/0/20
(Netgear Switch) (Interface 1/0/20)#vlan pvid 1
(Netgear Switch) (Interface 1/0/20)#vlan participation include 1
(Netgear Switch) (Interface 1/0/20)#exit
```

3. On the DHCPv6 relay, configure the interface that is connected to the DHCPv6 client.

```
(Netgear Switch) #vlan data
(Netgear Switch) (Vlan)#vlan 2
(Netgear Switch) (Vlan)#vlan routing 2
(Netgear Switch) (Vlan)#exit

(Netgear Switch) (Config)#interface vlan 2
(Netgear Switch) (Interface vlan 2)#ipv6 address 2001:2::1/64
(Netgear Switch) (Interface vlan 2)#ipv6 dhcp relay destination 2001:1::2
(Netgear Switch) (Interface vlan 2)#ipv6 enable
(Netgear Switch) (Interface vlan 2)#exit

(Netgear Switch) (Config)#interface 1/0/19
(Netgear Switch) (Interface 1/0/19)#vlan pvid 2
(Netgear Switch) (Interface 1/0/19)#vlan participation include 2
(Netgear Switch) (Interface 1/0/19)#ipv6 enable
(Netgear Switch) (Interface 1/0/19)#exit
```

4. Enable DHCPv6.

```
(Netgear Switch) (Config)#service dhcpv6
```

5. Display the DHCPv6 binding information.

```
(Netgear Switch) #show ipv6 dhcp binding

Total number of bindings : 1

Client Address.............................. fe80::6458:f6b:e2b:a0c3
Client Interface............................ vlan 2
Client DUID.................................
00:01:00:01:1d:c5:22:15:00:21:cc:70:0b:bf
Identity Association ID..................... 83894732
Binding Prefix Address...................... 2001:2::1
Binding Prefix Type ........................ IA_NA
Binding Expiration (secs)................... 4294967255
Binding Prefix Valid Lifetime (secs)........... infinite
Binding Prefix Preferred Lifetime (secs)....... infinite
```

DVLANs and Private VLANs

26

Double VLANS and private VLAN groups

This chapter includes the following sections:

- *Double VLANs*
- *Private VLAN Groups*

Double VLANs

This section describes how to enable the double DVLAN feature. Double VLANs pass traffic from one customer domain to another through the metro core. Custom VLAN IDs are preserved and a provider service VLAN ID is added to the traffic so the traffic can pass the metro core in a simple and cost-effective manner. You can use VLANs to specify customer ports and a service provider port. In this example, the switches have the same configuration.

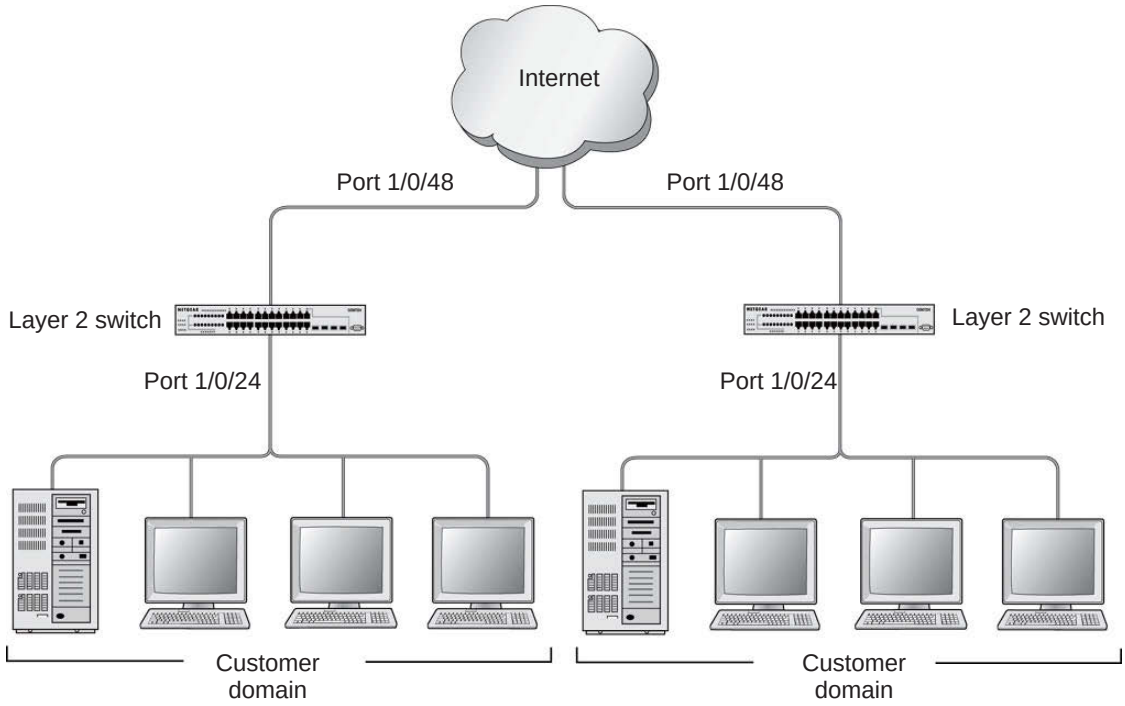


Figure 52. Double VLANS

The following example shows how to configure the NETGEAR switch shown in the preceding figure to add a double VLAN tag for traffic going from the subnet domain connected to port 1/0/24. This example assumes that a Layer 2 switch connects all these devices in your domain. The Layer 2 switch tags the packet going to the NETGEAR switch port 1/0/24. The example is shown as CLI commands and as a web interface procedure.

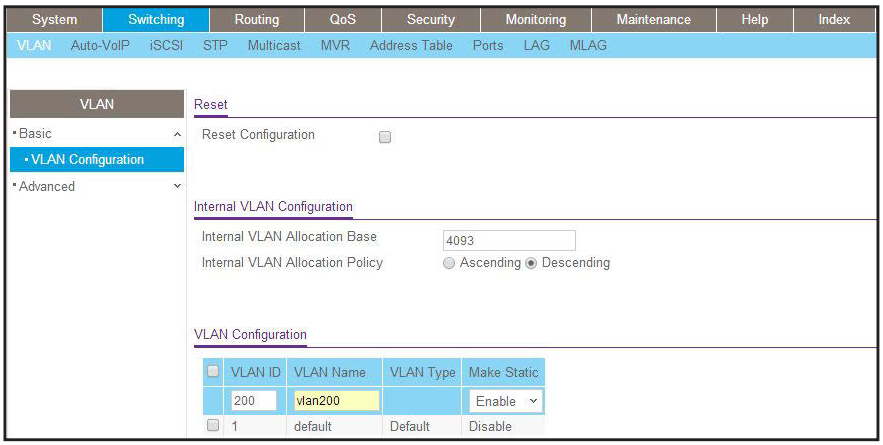
CLI: Enable a Double VLAN

```
Create a VLAN 200.
(Netgear Switch)#vlan database
(Netgear Switch) (Vlan)#vlan 200
(Netgear Switch) (Vlan)#exit

Add interface 1/0/24 to VLAN 200, add pvid 200 to port.
(Netgear Switch) #config
(Netgear Switch) (Config)#interface 1/0/24
(Netgear Switch) (Interface 1/0/24)#vlan pvid 200
(Netgear Switch) (Interface 1/0/24)#vlan participation include 200
(Netgear Switch) (Interface 1/0/24)#exit

Add interface 1/0/48 to the VLAN 200 in a tagging mode.
(Netgear Switch) (Config)#interface 1/0/48
(Netgear Switch) (Interface 1/0/48)#vlan participation include 200
(Netgear Switch) (Interface 1/0/48)#vlan tagging 200
(Netgear Switch) (Interface 1/0/48)#exit

Select interface 1/0/48 as the provider port.
(Netgear Switch) (Config)#
(Netgear Switch) (Config)#interface 1/0/48
(Netgear Switch) (Interface 1/0/48)#mode dvlan-tunnel
(Netgear Switch) (Interface 1/0/48)#exit
```

Web Interface: Enable a Double VLAN

1. Create static VLAN 200:
   a. Select **Switching > VLAN > Basic > VLAN Configuration**.

      A screen similar to the following displays.



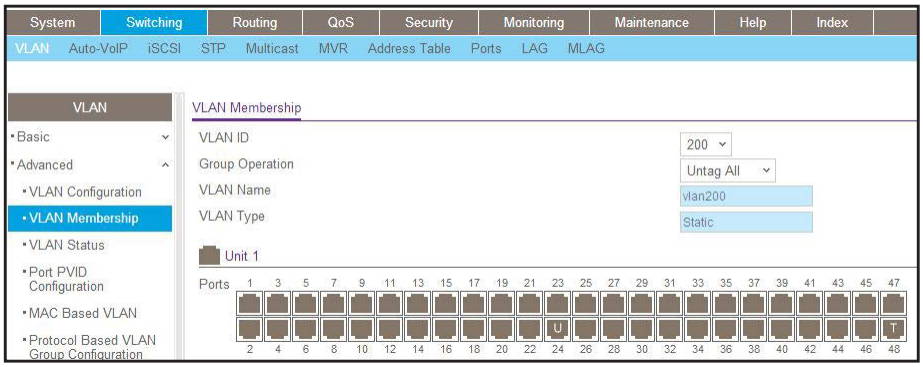
b. Under VLAN Configuration, enter the following information:
   - In the **VLAN ID** field, enter **200**.
   - In the **VLAN Name** field, enter **vlan200**.
   - In the **VLAN Type** field, select **Static**.

c. Click **Add**.

2. Add ports 24 and 48 to VLAN 200.

a. Select **Switching > VLAN > Advanced > VLAN Membership**.

A screen similar to the following displays.



b. Under VLAN Membership, in the **VLAN ID** field, select **200**.

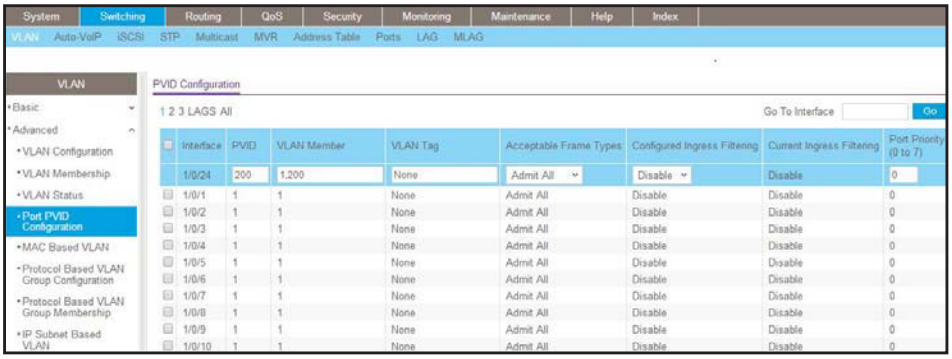
c. Click **Unit 1**. The ports display:
   - Click the gray box under port **24** twice until **U** displays. The U specifies that the egress packet is untagged for the port.
   - Click the gray box under port **48** once until **T** displays. The T specifies that the egress packet is tagged for the port.

d. Click **Apply** to save the settings.

3. Change the port VLAN ID (PVID) of port 24 to 200:

a. Select **Switching > VLAN > Advanced > Port PVID Configuration**.

A screen similar to the following displays.



b. Scroll down and select the Interface **1/0/24** check box. Now 1/0/24 appears in the Interface field at the top.

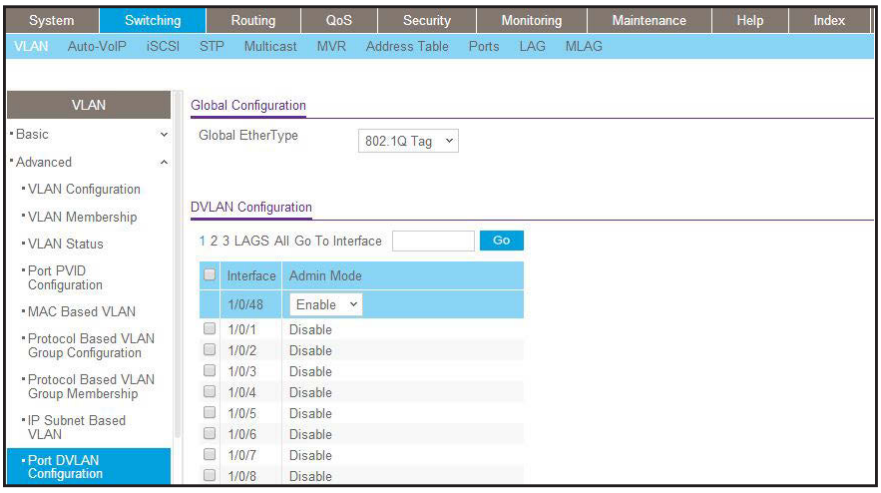
c. In the **PVID (1 to 4093)** field, enter **200**.

d. Click **Apply** to save the settings.

4. Configure port 48 as the provider service port:

a. Select **Switching > VLAN > Advanced > Port DVLAN Configuration**.

A screen similar to the following displays.



b. Scroll down and select the Interface **1/0/48** check box. Now 1/0/48 appears in the Interface field at the top.

c. In the **Admin Mode** field, select **Enable**.

d. Click **Apply** to save the settings.

Private VLAN Groups

The private VLAN group allows you to create groups of users within a VLAN that cannot communicate with members in different groups but only within the same group. There are two modes for the private group. The mode can be either isolated or community. When in isolated mode, the member port in the group cannot forward its egress traffic to any other members in the same group. the default mode is community, in which each member port can forward traffic to other members in the same group, but not to members in other groups. The following examples show how to create a private group.

The following example creates two groups. Group 1 is in community mode, and Group 2 is in isolated mode.

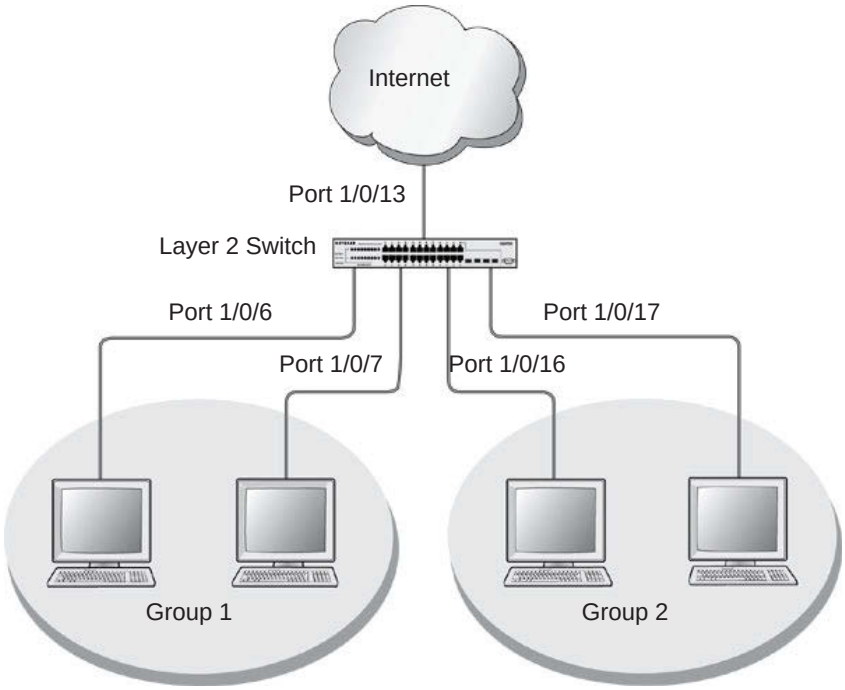


Figure 53. Private VLAN groups in community mode and isolated mode

CLI: Create a Private VLAN Group

1. Enter the following commands.

```
(Netgear Switch) #
(Netgear Switch) #vlan data
(Netgear Switch) (Vlan)#vlan 200
(Netgear Switch) (Vlan)#exit

(Netgear Switch) #config
(Netgear Switch) (Config)#interface 1/0/6
(Netgear Switch) (Interface 1/0/6)#vlan participation include 200
(Netgear Switch) (Interface 1/0/6)#vlan pvid 200
(Netgear Switch) (Interface 1/0/6)#exit

(Netgear Switch) (Config)#interface 1/0/7
(Netgear Switch) (Interface 1/0/7)#vlan participation include 200
(Netgear Switch) (Interface 1/0/7)#vlan pvid 200
(Netgear Switch) (Interface 1/0/7)#exit
(Netgear Switch) (Config)#interface 1/0/16
(Netgear Switch) (Interface 1/0/16)#vlan participation include 200
(Netgear Switch) (Interface 1/0/16)#vlan participation pvid 200
(Netgear Switch) (Interface 1/0/16)#exit

(Netgear Switch) (Config)#interface 1/0/17
(Netgear Switch) (Interface 1/0/17)#vlan participation include 200
(Netgear Switch) (Interface 1/0/17)#vlan pvid 200
(Netgear Switch) (Interface 1/0/17)#exit
```

2. Create a VLAN 200 and include 1/0/6,1/0/7, 1/0/16, and 1/0/17.

```
(Netgear Switch) (Config)#
(Netgear Switch) (Config)#private-group name group1 1 mode community
```

3. Create a private group in community mode.

```
(Netgear Switch) (Config)#private-group name group2 2 mode isolated
```

4. Create a private group in isolated mode.

```
(Netgear Switch) (Config)#interface range 1/0/6-1/0/7
(Netgear Switch) (conf-if-range-1/0/6-1/0/7)#switchport private-group 1
(Netgear Switch) (conf-if-range-1/0/6-1/0/7)#exit
```

5. Add 1/0/16 and 1/0/7 to the private group 1.

```
(Netgear Switch) (Config)#interface range 1/0/16-1/0/17
(Netgear Switch) (conf-if-range-1/0/16-1/0/17)#switchport private-group 2
```

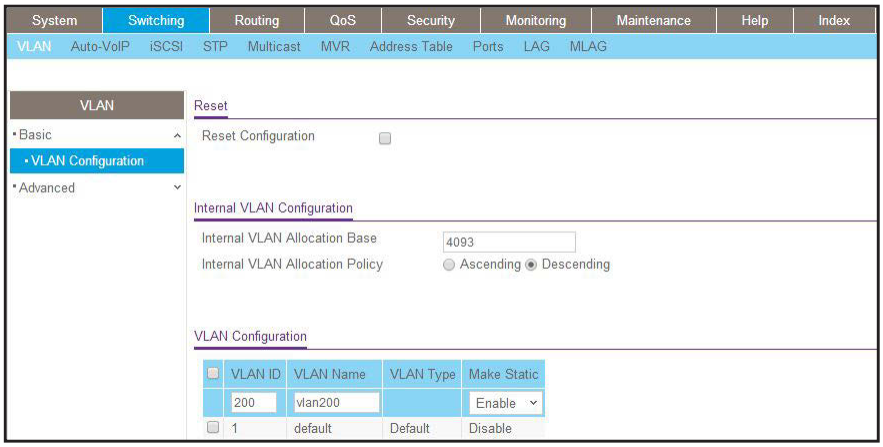
6. Add 1/0/16 and 1/0/7 to the private group 2.

```
(Netgear Switch) (conf-if-range-1/0/16-1/0/17)#exit
```

Web Interface: Create a Private VLAN Group

1. Create VLAN 200.
   a. Select **Switching > VLAN > Basic > VLAN Configuration**.

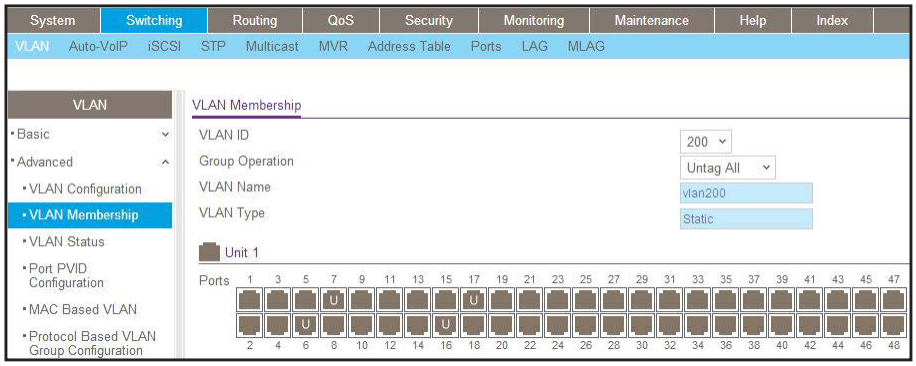
      A screen similar to the following displays.



   b. Enter the following information:
      - In the **VLAN ID** field, enter **200**.
      - In the **VLAN Name** field, enter **VLAN200**.
      - In the **VLAN Type** field, select **Static**.

   c. Click **Add**.
2. Add ports 1/0/6, 1/0/7, 1/0/16, and 1/0/17 to VLAN 200.
   a. Select **Switching > VLAN > Advanced > VLAN Membership**.

A screen similar to the following displays.



b. Under VLAN Membership, in the **VLAN ID** list, select **200**.

c. Click **Unit 1.** The ports display.

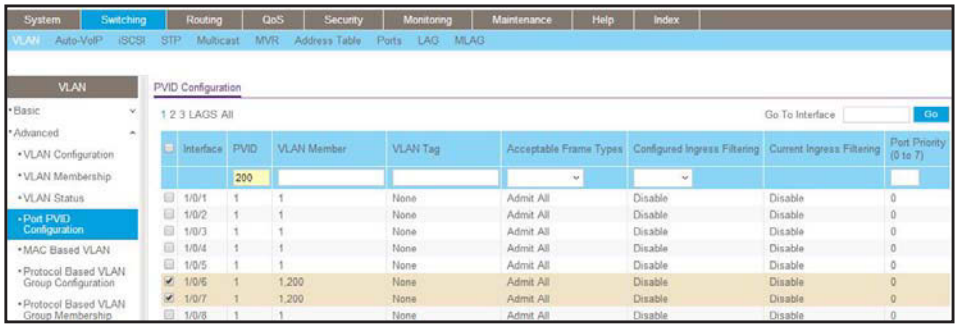
d. Click the gray boxes under ports **6**, **7**, **16** and **17** until **U** displays. The U specifies that the egress packet is untagged for the port.

e. Click **Apply**.

3. Specify the PVID on ports 1/0/6, 1/0/7, 1/0/16, and 1/0/17.

a. Select **Switching > VLAN > Advanced > Port PVID Configuration**.

A screen similar to the following displays.



b. Under PVID Configuration, scroll down and select the Interface **1/0/6**,**1/0/7**,**1/0/16**, and **1/0/17** check boxes.

c. In the **PVID (1 to 4093)** field, enter **200**.

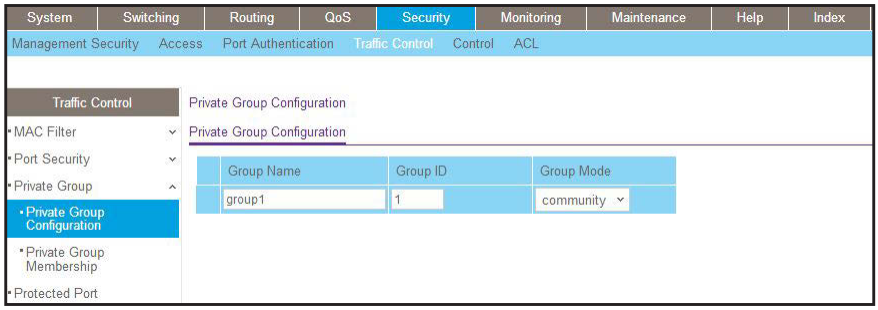
d. In the **Acceptable Frame Type** list, select **Admit All**.

e. Click **Apply** to save the settings.

4. Create a private group, group1.

a. Select **Security > Traffic Control > Private Group VLAN > Private Group VLAN > Private Group Configuration**.

A screen similar to the following displays.



b. In the **Group Name** field, enter **group1**.

c. In the **Group ID** field, enter **1**.

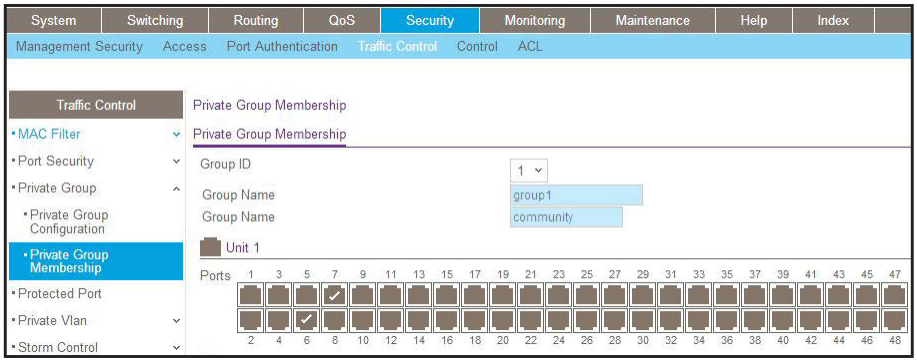
d. In the **Group Mode** list, select **community**.

e. Click **Add**.

5. Add port 6 and 7 to group1.

a. Select **Security > Traffic Control > Private Group VLAN >Private Group Membership**.

A screen similar to the following displays.



b. In the **Group ID** list, select **1**.

c. Click **Unit 1.** The ports display.

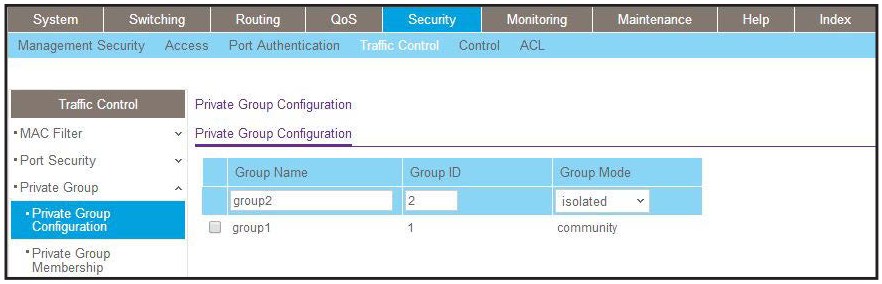
d. Click the gray boxes under ports **6** and **7**. A check mark displays in each box.

e. Click **Apply.**

6. Create a private group, group2.

a. Select **Security > Traffic Control > Private Group VLAN > Private Group Configuration**.

A screen similar to the following displays.



b. In the **Group Name** field, enter **group2**.

c. In the **Group ID** field, enter **2**.

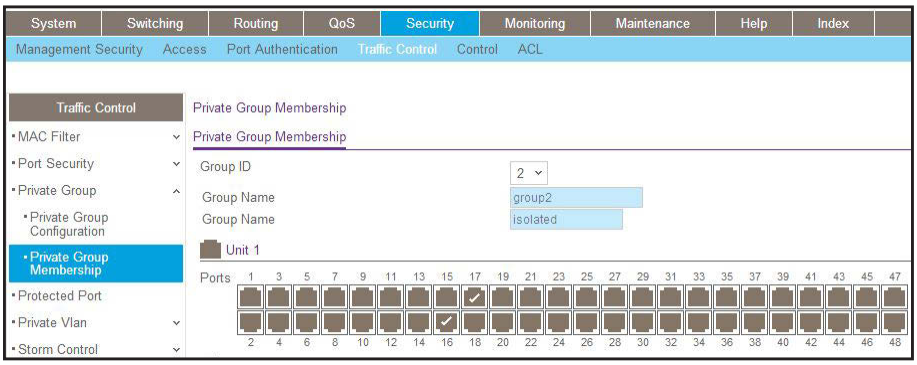
d. In the **Group Mode** field, select **isolated**.

e. Click **Add**.

7. Add ports 16 and 17 to group2.

a. Select **Security > Traffic Control > Private Group VLAN > Private Group VLAN > Private Group Membership**.

A screen similar to the following displays.



b. In the **Group ID** list, select **2**.

c. Click **Unit 2.** The ports display.

d. Click the gray boxes under ports **16** and **17,** and a check mark displays in each box.

e. Click **Apply**.

STP

27

Spanning Tree Protocol

This chapter includes the following sections:

- *Spanning Tree Protocol Concepts*
- *Configure Classic STP (802.1d)*
- *Configure Rapid STP (802.1w)*
- *Configure Multiple STP (802.1s)*
- *Configure PVSTP and PVRSTP*

Spanning Tree Protocol Concepts

The purpose of the Spanning Tree Protocol (STP) is to eliminate loops in the switch system. There are three STPs: Classic STP (802.1d), Rapid STP (RSTP, 802.1w), and Multiple STP (MSTP, 802.1s).

While STP can take 30 to 50 seconds to respond to a topology change, RSTP is typically able to respond to changes within a few seconds. RSTP can revert back to 802.1d in order to interoperate with legacy bridges on a per-port basis. This drops the benefits it introduces.

In Multiple Spanning Tree Protocol (MSTP), each Spanning Tree instance can contain several VLANs. Each Spanning Tree instance is independent of other instances. This approach provides multiple forwarding paths for data traffic, enabling load balancing, and reducing the number of Spanning Tree instances required to support a large number of VLANs.

Configure Classic STP (802.1d)

The example is shown as CLI commands and as a web interface procedure.

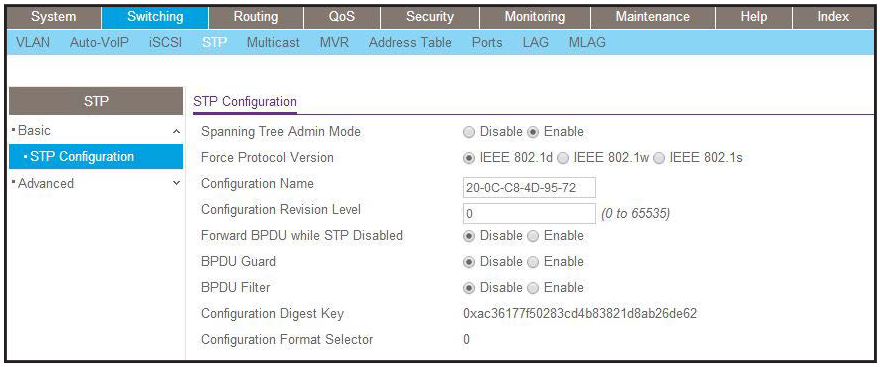
CLI: Configure Classic STP (802.1d)

```
(Netgear Switch) (Config)# spanning-tree
(Netgear Switch) (Config)# spanning-tree mode stp
(Netgear switch) (Interface 1/0/3)# spanning-tree port mode
```

Web Interface: Configure Classic STP (802.1d)

1. Enable 802.1d on the switch.
   a. Select **Switching > STP > STP Configuration**.

      A screen similar to the following displays.



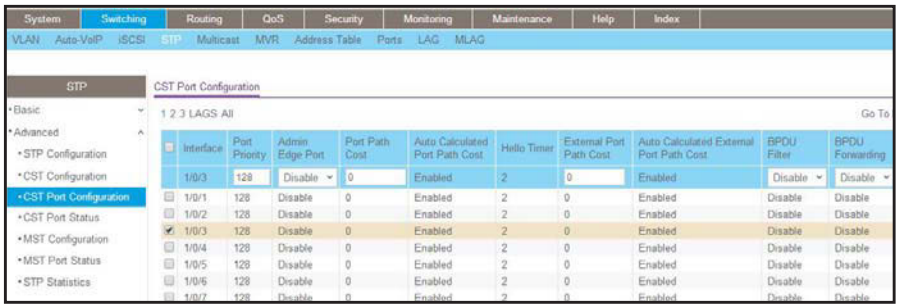
b. Enter the following information:
   - For Spanning Tree Admin Mode, select the **Enable** radio button.
   - For Force Protocol Version, select the **IEEE 802.1d** radio button.

c. Click **Apply**.

2. Configure the CST port.

a. Select **Switching > STP > CST Port Configuration**.

A screen similar to the following displays.



b. Under CST Port Configuration, scroll down and select the Interface **1/0/3** check box. Now 1/0/3 appears in the Interface field at the top.

c. In the **Port Mode** field, select **Enable**.

d. Click **Apply**.

Configure Rapid STP (802.1w)

The example is shown as CLI commands and as a web interface procedure.

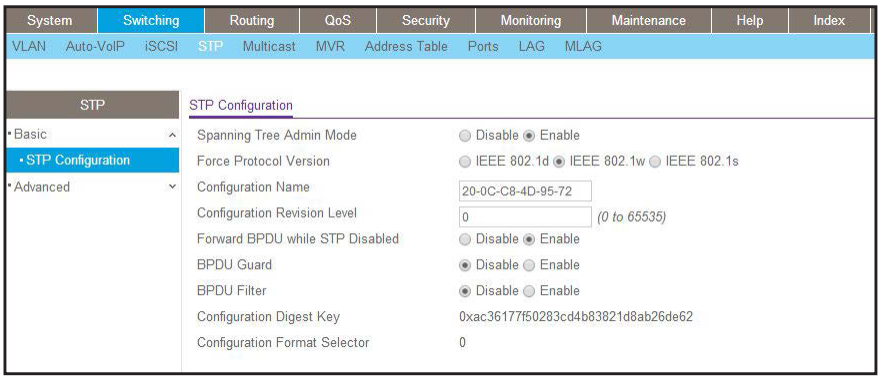
CLI: Configure Rapid STP (802.1w)

```
(Netgear switch) (Config)# spanning-tree
(Netgear switch) (Config)# spanning-tree mode rstp
(Netgear switch) (Interface 1/0/3)# spanning-tree port mode
```

Web Interface: Configure Rapid STP (802.1w)

1. Enable 802.1w on the switch:
   a. Select **Switching > STP > STP Configuration**.

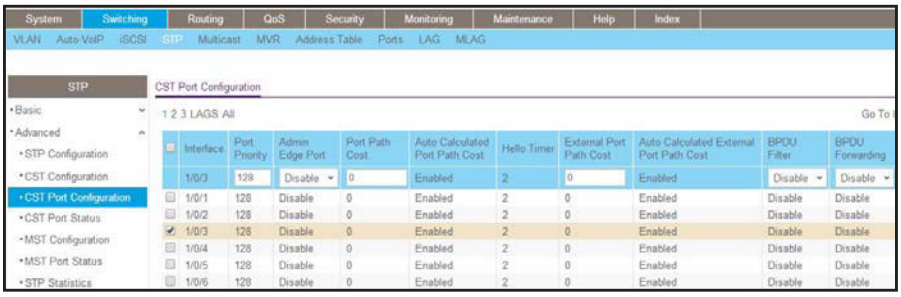
      A screen similar to the following displays.



   b. Enter the following information:
      - For Spanning Tree Admin Mode, select the **Enable** radio button.
      - For Force Protocol Version, select the **IEEE 802.1w** radio button.

   c. Click **Apply.**
2. Configure the CST port.
   a. Select **Switching > STP > CST Port Configuration**.

      A screen similar to the following displays.



   b. Under CST Port Configuration, scroll down and select the Interface **1/0/3** check box.

      Now 1/0/3 appears in the Interface field at the top.

   c. In the **Port Mode** field, select **Enable**.
   d. Click **Apply**.

Configure Multiple STP (802.1s)

The example is shown as CLI commands and as a web interface procedure.

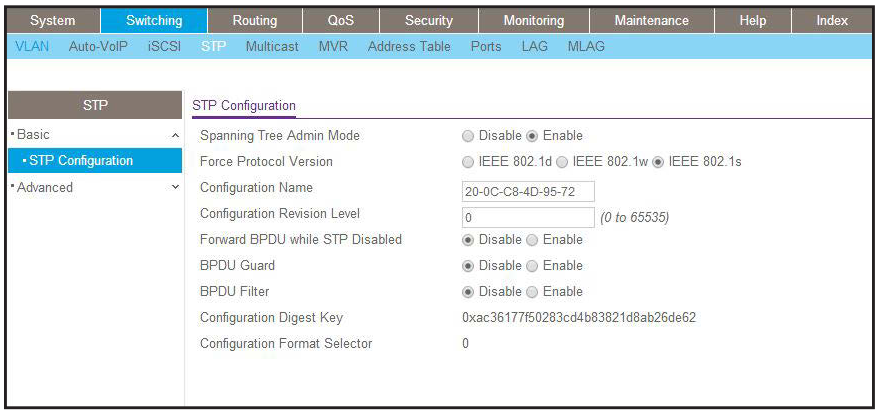
CLI: Configure Multiple STP (802.1s)

```
(Netgear switch) (Config)# spanning-tree
(Netgear switch) (Config)# spanning-tree mode mst
(Netgear Switch) (Config)#spanning-tree configuration name mstp_1
(Netgear Switch) (Config)#spanning-tree configuration revision 0

Configure an MSTP region name and revision for the switches in the same MSTP region.
The switches in the same MSTP region must be configured with the same region name
and revision.

Create a mst instance 1:
(Netgear switch) (Config)# spanning-tree mst instance 1

Associate the mst instance 1 with the VLAN 2 and 3:
(Netgear switch) (Config)# spanning-tree mst priority 1 4096
(Netgear switch) (Config)# spanning-tree mst vlan 1 2
(Netgear switch) (Config)# spanning-tree mst vlan 1 3

Create a mst instance 2:
(Netgear switch) (Config)# spanning-tree mst instance 2

Associate the mst instance 2 with the VLAN 11 and 12:
(Netgear switch) (Config)# spanning-tree mst priority 2 4096
(Netgear switch) (Config)# spanning-tree mst vlan 2 11
(Netgear switch) (Config)# spanning-tree mst vlan 2 12

Configure the priority and cost on port 1/0/3:
(Netgear switch) (Interface 1/0/3)# spanning-tree mst 1 port-priority 128
(Netgear switch) (Interface 1/0/3)# spanning-tree mst 1 cost 0
```

Web Interface: Configure Multiple STP (802.1s)

1. Enable 802.1s on the switch.
   a. Select **Switching > STP > STP Configuration**.

      A screen similar to the following displays.



   b. Enter the following information:
      - For Spanning Tree Admin Mode, select the **Enable** radio button.
      - For Force Protocol Version, select the **IEEE 802.1s** radio button.
      - In the **Configuration Name** field, enter **mstp_1**.
      - In the **Configuration Revision Level** field, enter **0**.

   c. Click **Apply**.
2. Configure MST.
   a. Select **Switching > STP > MST Configuration**.

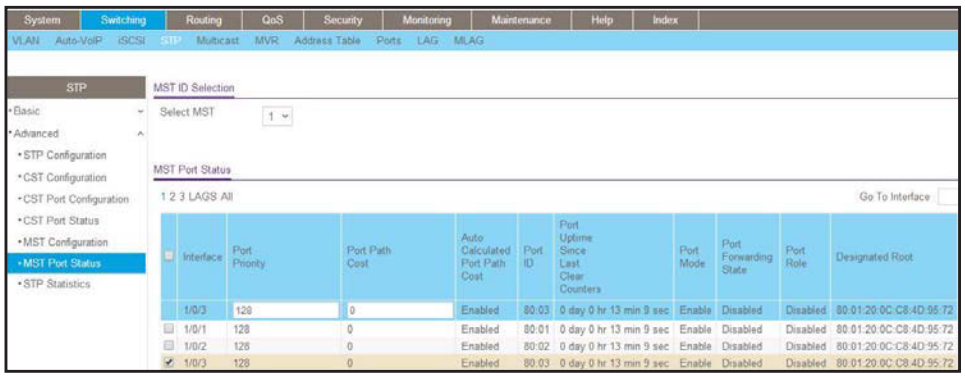
      A screen similar to the following displays.

   b. Configure MST ID 1.
      - In the **MST ID** field, enter **1**.
      - In the **Priority** field, enter **4096**.
      - In the **VLAN Id** field, enter **2**.
      - Click **Add**.
      - In the **VLAN Id** field, enter **3**.
      - Click **Apply**.

c. Configure MST ID 2.
   - In the **MST ID** field, enter **2**.
   - In the **Priority** field, enter **4096**.
   - In the **VLAN Id** field, enter **11**.
   - Click **Add**.
   - In the **VLAN Id** field, enter **12**.
   - Click **Apply**.

3. Configure the MST port.
   a. Select **Switching > STP > MST Port Status**.

      A screen similar to the following displays.



4. Under MST Port Configuration, scroll down and select the Interface **1/0/3** check box.

   Now 1/0/3 appears in the Interface field at the top.

5. Enter the following information:
   - In the **Port Priority** field, enter **128**.
   - In the **Port Path Cost** field, enter **0**.
6. Click **Apply**.

Configure PVSTP and PVRSTP

Per VLAN Rapid Spanning Tree Protocol (PVRSTP) is similar to Rapid Spanning Tree Protocol (RSTP) as defined by IEEE 802.1w but with one main difference: PVRSTP runs one instance per VLAN. That is, each configured VLAN runs an independent instance of PVRSTP and each instance elects a root bridge independent of another instance. A region can include as many root bridges as there are VLANs that are configured for PVRSTP. PVRSTP is equivalent to Cisco's RPVST+ and can interoperate with it.

Per VLAN Spanning Tree Protocol (PVSTP) is similar to the Spanning Tree Protocol (STP) as defined by IEEE 802.1d, but with one main difference: PVSTP runs one instance per VLAN. The protocol is equivalent to Cisco's PVST+ and can interoperate with it.

If you enable PVSTP or PVRSTP on a switch, all other spanning tree modes on the switch become disabled. The difference between Multiple Spanning Tree Protocol (MSTP) and PVSTP or PVRSTP lies primarily in the way that the protocol maps spanning tree instances to VLANs: PVSTP or PVRSTP creates a spanning tree instance for each VLAN, whereas MSTP maps one or more VLANs to each Multiple Spanning Tree (MST) instance.

If a switch that runs PVRSTP receives PVSTP Bridge Protocol Data Units (BPDUs), the switch falls back from PVRSTP to PVSTP after its migration-delay timer expires.

A switch that runs PVSTP or PVRSTP transmits IEEE spanning tree BPDUs along with Shared Spanning Tree Protocol (SSTP) BPDUs. The SSTP BPDU are transmitted as untagged packets on an access or native VLAN and transmitted as tagged packets on other VLANs. If a switch that runs PVSTP or PVRSTP receives IEEE spanning tree BPDUs, the switch include them in an access VLAN instance or native VLAN instance.

The Per VLAN Spanning Tree (PVST) behavior is as follows:

- An access port sends IEEE spanning tree BPDUs.
- A trunk port sends IEEE spanning tree BPDUs and SSTP BPDUs on the native VLAN. For other VLANs, the trunk port transmits SSTP BPDUs as tagged packets with the respective VLAN. If the trunk port receives IEEE spanning tree BPDUs, the received BPDUs are processed by the instance that is mapped to the native VLAN. The SSTP BPDUs are processed by instances to which the respective VLANs are mapped.

If a switch that is running an IEEE standard spanning tree protocol (such as STP, RSTP, or MSTP) receives SSTP BPDUs, the switch does not treat them as standard BPDUs. Instead, the incoming SSTP BPDUs are flooded to all the ports of the corresponding VLAN. As a comparison, incoming STP BPDUs are multicasted over the region.

A switch that runs an IEEE standard spanning tree protocol uses its Common and Internal Spanning Tree (CIST) to communicate with a switch that runs PVSTP or PVRSTP. On the other hand, a switch that runs PVSTP or PVRSTP uses an access VLAN instance or native VLAN instance to communicate with a switch that runs an IEEE standard spanning tree protocol.

PVRSTP embeds support for the FastUplink feature to speed up the selection of a new root and the FastBackbone feature to speed up the selection of indirect ports. You do not need to configure these features for RVRSTP. However, for PVSTP, you need to configure these features:

- **FastUplink**. This feature allows for a quick selection of a port with the lowest cost after the root port fails. That is, FastUplink reduces the converge time after a link fails. This feature is similar to Cisco’s UplinkFast feature. If the primary link fails, FastUplink creates an alternate path immediately, speeding up the transition from the failed primary link to the backup link.
- **FastBackbone**. This feature allows for faster convergence time when an indirect link to the root fails. If a root port or blocked port receives an inferior BPDU from the designated switch, the switch acts as if an indirect link to the root failed. To speed up the convergence time, the switch expires the maximum age timer immediately and forces the port through the Listening and Learning states.

The following diagram shows a simple PVSTP configuration.

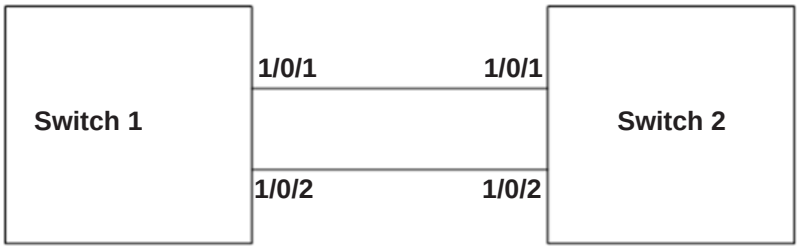


Figure 54. PVSTP configuration

CLI: Configure PVSTP

You must configure PVSTP on Switch 1 and Switch 2. This example assumes that all switches can support PVSTP.

CLI: Configure PVSTP on Switch 1

1. Ensure that ports 1/0/1 and 1/0/2 are in VLAN 1002 in tagged mode because BPDU packets for PVSTP are transmitted in tagged packets.
2. Enable PVSTP.

```
(Netgear Switch) #config
(Netgear Switch) (Config)#spanning-tree mode pvst
```

Note: After you enable PVSTP (or PVRSTP) globally, PVSTP (or PVRSTP) is applied to VLANs automatically.

3. Verify the PVSTP status.

```
(Netgear Switch) #show spanning-tree vlan 1002
VLAN 1002
 Spanning-tree enabled protocol pvst
 RootID    Priority        33770
           Address         6C:B0:CE:19:AE:3D
           Cost            20000
           Port            1(1/0/1  )
           Hello Time 2 Sec Max Age 20 sec Forward Delay 15 sec
 BridgeID  Priority        33770 (priority 32768 sys-id-ext 1002)
           Address         6C:B0:CE:F9:F6:E0
           Hello Time 2 Sec Max Age 20 sec Forward Delay 15 sec
           Aging Time 300 sec

Interface  Role        Sts            Cost         Prio.Nbr
---------  ----------  -------------  -----------  --------
1/0/1      Root        Forwarding     20000        128.1
1/0/2      Alternate   Discarding     20000        128.2
```

4. Enable the FastUplink and FastBackbone features to speed up the selection of a new root and indirect ports, respectively.

```
(Netgear Switch) (Config)#spanning-tree uplinkfast
(Netgear Switch) (Config)#spanning-tree backbonefast
```

5. To enable the switch to be elected as the root in VLAN 1000, set the PVSTP priority to 0.

```
(Netgear Switch) (Config)#spanning-tree vlan 1000 priority 0
```

CLI: Configure PVSTP on Switch 2

1. Ensure that ports 1/0/1 and 1/0/2 are in VLAN 1002 in tagged mode because BPDU packets for PVSTP are transmitted in tagged packets.
2. Enable PVSTP.

```
(Netgear Switch) #config
(Netgear Switch) (Config)#spanning-tree mode pvst
```

3. Verify the PVSTP status.

```
(Netgear Switch) #show spanning-tree vlan 1002

VLAN 1002
 Spanning-tree enabled protocol pvst
 RootID    Priority        33770
           Address         6C:B0:CE:19:AE:3D
           Cost            0
           Port            This switch is the root
           Hello Time 2 Sec Max Age 20 sec Forward Delay 15 sec
 BridgeID  Priority        33770 (priority 32768 sys-id-ext 1002)
           Address         6C:B0:CE:19:AE:3D
           Hello Time 2 Sec Max Age 20 sec Forward Delay 15 sec
           Aging Time 300 sec

Interface  Role        Sts            Cost         Prio.Nbr
---------  ----------  -------------  -----------  --------
1/0/1      Designated  Forwarding     20000        128.1
1/0/2      Designated  Forwarding     20000        128.
```

4. Enable the FastUplink and FastBackbone features to speed up the selection of a new root and indirect ports, respectively.

```
(Netgear Switch) (Config)#spanning-tree uplinkfast
(Netgear Switch) (Config)#spanning-tree backbonefast
```

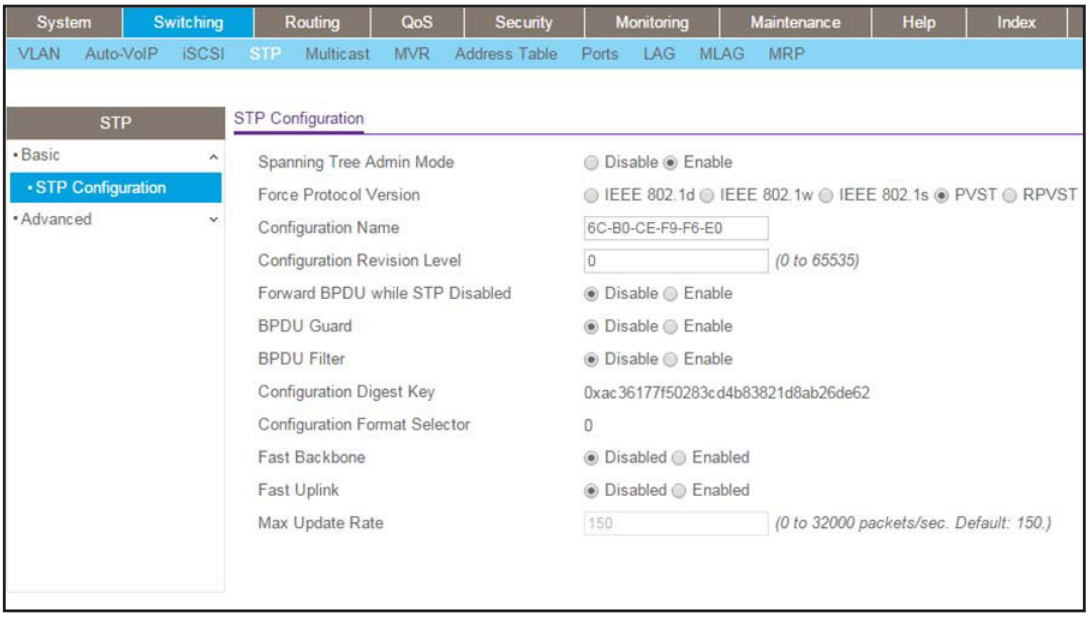
Web Interface: Configure PVSTP

You must configure PVSTP on Switch 1 and Switch 2. This example assumes that all switches can support PVSTP.

Web Interface: Configure PVSTP on Switch 1

1. Ensure that ports 1/0/1 and 1/0/2 are in VLAN 1002 in tagged mode because BPDU packets for PVSTP are transmitted in tagged packets.
2. Enable PVSTP.
   a. Select **Switching > STP > Basic > STP Configuration**.

      A screen similar to the following displays.



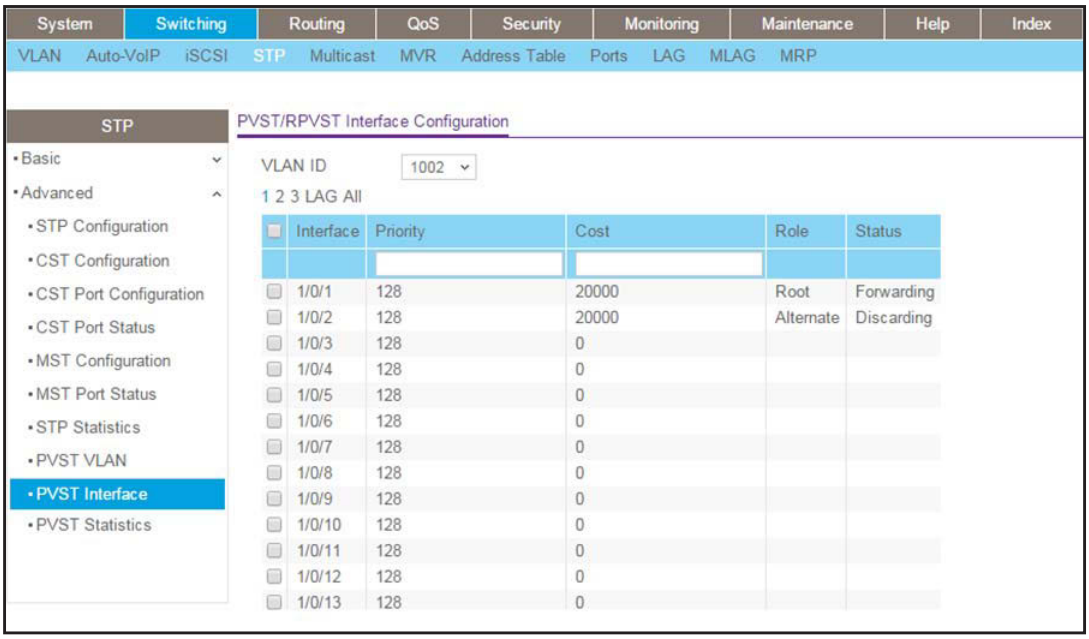
   b. Configure the following settings:
      - For Spanning Tree Admin Mode, select the **Enable** radio button.
      - For Force Protocol Version, select the **PVST** radio button.

   c. Click **Apply**.

   Note: After you enable PVST globally, PVST is applied to VLANs automatically.

3. Display the PVST status for port 1/0/1 and 1/0/2 in VLAN 1002.
   a. Select **Switching > STP > Advanced > PVST Interface**.

      A screen similar to the following displays.



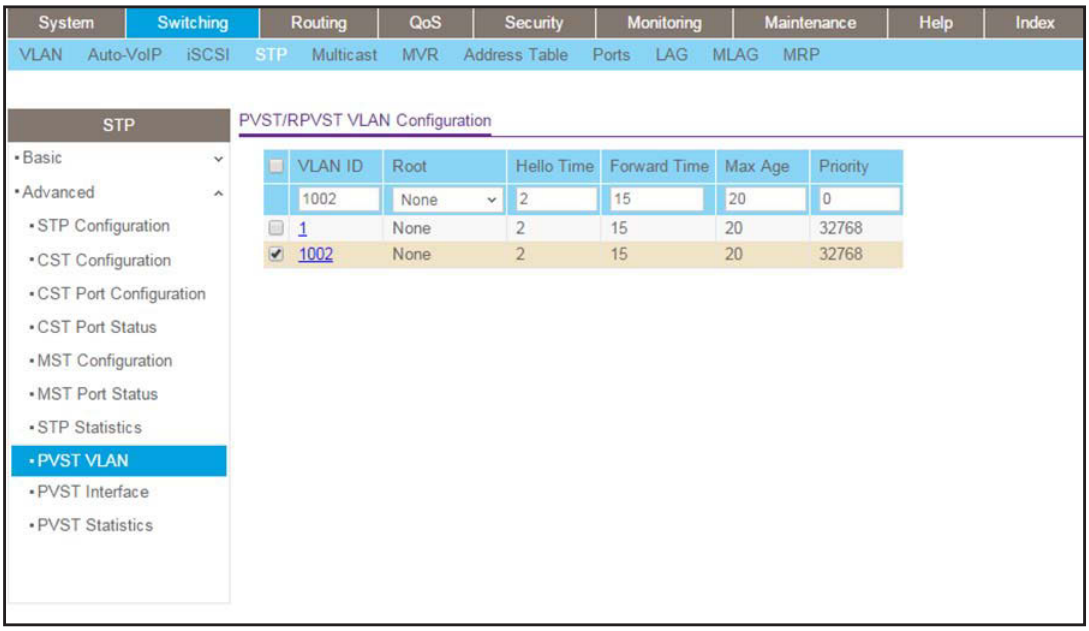
b. From the **VLAN ID** menu, select **1002**.

The roles of ports 1/0/1 and 1/0/2 display.

4. To enable the switch to be elected as the root, change the PVST priority to lower value (for example, 0).

a. Select **Switching > STP > Advanced > PVST VLAN**.

A screen similar to the following displays.



b. Select the **1002** check box for VLAN ID 1002.

The settings for VLAN ID 1002 display in the fields in the table heading.

c. In the **Priority** field, enter **0**.

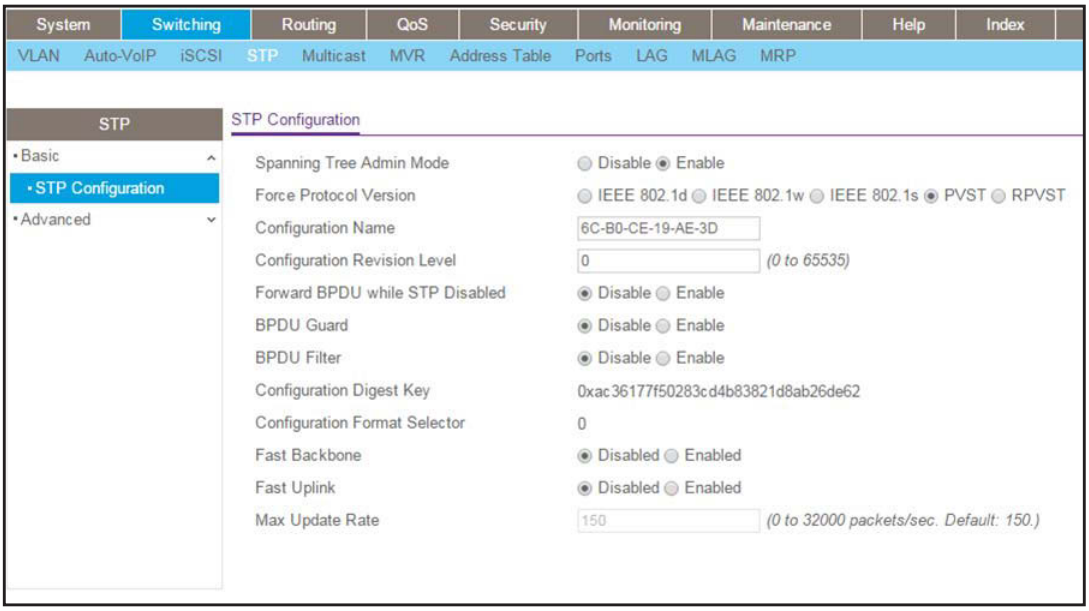
d. Click **Apply**.

Web Interface: Configure PVSTP on Switch 2

1. Ensure that ports 1/0/1 and 1/0/2 are in VLAN 1002 in tagged mode because BPDU packets for PVSTP are transmitted in tagged packets.
2. Enable PVSTP.

   a. Select **Switching > STP > Basic > STP Configuration**.

   A screen similar to the following displays.



   b. Configure the following settings:
      - For Spanning Tree Admin Mode, select the **Enable** radio button.
      - For Force Protocol Version, select the **PVST** radio button.

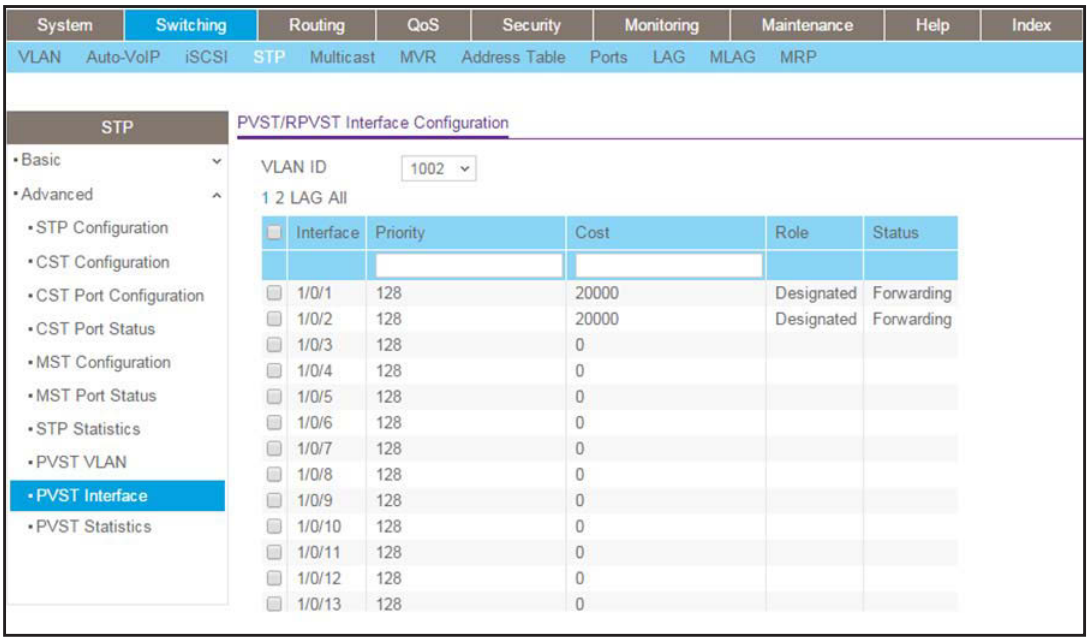
   c. Click **Apply**.

   Note: After you enable PVST globally, PVST is applied to VLANs automatically.

3. Display the PVST status for ports 1/0/1 and 1/0/2 in VLAN 1002.

   a. Select **Switching > STP > Advanced > PVST Interface**.

   A screen similar to the following displays.



b. From the **VLAN ID** menu, select **1002**.

The roles of ports 1/0/1 and 1/0/2 display.

Tunnels for IPv6

28

6in4 tunnels and 6to4 tunnels

This chapter includes the following sections:

- *Tunnel Concepts*
- *Create a 6in4 Tunnel*
- *Create a 6to4 Tunnel*

Tunnel Concepts

Two methods exist for IPv6 sites to communicate with each other over the IPv4 network: 6in4 tunnel and 6to4 tunnel. The 6in4 tunnel encapsulates IPv6 traffic over an explicitly configured IPv4 destination or end port of the tunnel with the IP protocol number set to 41. The 6to4 tunnel IPv6 prefix is constructed by prepending 2002 (hexadecimal) to the global IPv4 address. For example, if the IPv4 address is 4.4.4.1, the tunnel IPv6 prefix would be 2002:404:401::/16.

The 6to4 tunnels are automatically formed IPv4 tunnels carrying IPv6 traffic. The automatic tunnel's IPv4 destination address is derived from the 6to4 IPv6 address of the tunnel's next hop. A 6to4 tunnel supports the functionality of a 6to4 border router that connects a 6to4 site to a 6to4 domain. With 6to4 tunnels, routers in a 6to4 domain, including other 6to4 border routers and 6to4 relay routers, can send and receive tunneled traffic from each other.

Create a 6in4 Tunnel

In the example, you create a 6in4 tunnel between Switch 1 and Switch 2. The tunnel carries IPv6 packets over IPv4 packets.

Figure 55. 6in4 tunnel configuration

CLI: Create a 6in4 Tunnel

You must configure Switch 1 and Switch 2.

CLI: Create a 6in4 Tunnel on Switch 1

```
(Netgear Switch) #config
(Netgear Switch) (Config)#ip routing
(Netgear Switch) (Config)#ipv6 unicast-routing
(Netgear Switch) (Config)#interface 1/0/1
(Netgear Switch) (Interface 1/0/1)#routing
(Netgear Switch) (Interface 1/0/1)#ip address 192.168.1.1 255.255.255.0
(Netgear Switch) (Interface 1/0/1)#exit
(Netgear Switch) (Config)#interface tunnel 0
(Netgear Switch) (Interface tunnel 0)#ipv6 enable
(Netgear Switch) (Interface tunnel 0)#ipv6 address 2000::1/64
(Netgear Switch) (Interface tunnel 0)#tunnel mode ipv6ip
(Netgear Switch) (Interface tunnel 0)#tunnel source 192.168.1.1
(Netgear Switch) (Interface tunnel 0)#tunnel destination 192.1.168.1.2
(Netgear Switch) (Interface tunnel 0)#exit
(Netgear Switch) (Config)#exit
(Netgear Switch) #show interface tunnel 0

Interface Link Status..... Up
IPv6 is enabled
IPv6 Prefix is ..... FE80::C0A8:101/128
                                          2000::1/64
MTU size..... 1280 bytes

(Netgear Switch) #show interface tunnel

TunnelId    Interface    TunnelMode           SourceAddress     DestinationAddress
--------    ---------    -----------------    -------------     ------------------
0   tunnel    0            6 in 4 Configured    192.168.1.1       192.168.1.2

(Netgear Switch) # ping ipv6 2000::2
Send count=3, Receive count=3 from 2000::2
Average round trip time = 1.00 ms
```

CLI: Create a 6in4 Tunnel on Switch 2

```
(Netgear Switch) #config
(Netgear Switch) (Config)#ip routing
(Netgear Switch) (Config)#ipv6 unicast-routing
(Netgear Switch) (Config)#interface 1/0/13
(Netgear Switch) (Interface 1/0/13)#routing
(Netgear Switch) (Interface 1/0/13)#ip address 192.168.1.2 255.255.255.0
(Netgear Switch) (Interface 1/0/13)#exit

(Netgear Switch) (Config)#interface tunnel 0
(Netgear Switch) (Interface tunnel 0)#ipv6 enable
(Netgear Switch) (Interface tunnel 0)#ipv6 address 2000::2/64
(Netgear Switch) (Interface tunnel 0)#tunnel mode ipv6ip
(Netgear Switch) (Interface tunnel 0)#tunnel source 192.168.1.2
 (Netgear Switch) (Interface tunnel 0)#tunnel destination 192.168.1.1
(Netgear Switch) (Interface tunnel 0)#exit
(Netgear Switch) (Config)#exit
(Netgear Switch) #show interface tunnel

TunnelId  Interface  TunnelMode         SourceAddress   DestinationAddress
--------  ---------  -----------------  -------------   ------------------
0 tunnel  0          6 in 4 Configured  192.168.1.2     192.168.1.1
```

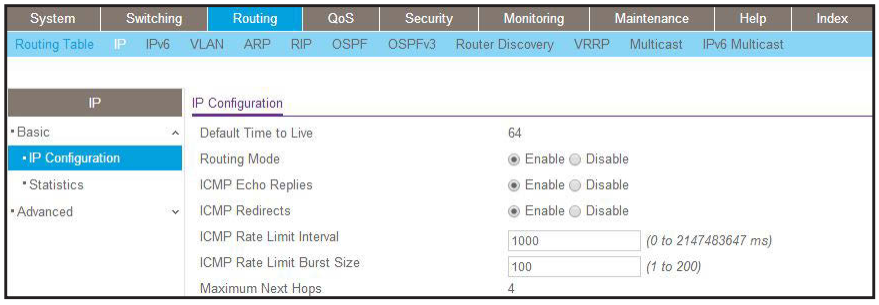
Web Interface: Create a 6in4 Tunnel

You must configure Switch 1 and Switch 2.

Web Interface: Create a 6in4 Tunnel on Switch 1

1. Enable IP routing on the switch.
   a. Select **Routing > IP > Basic > IP Configuration**.

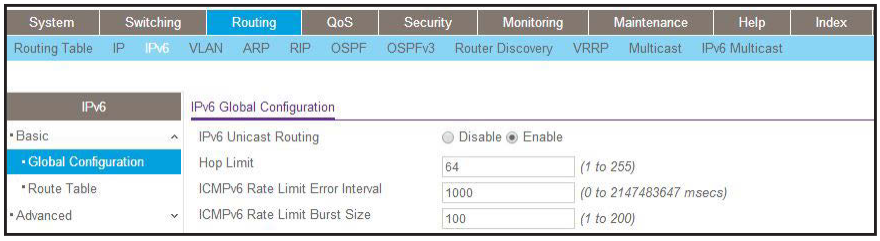
      A screen similar to the following displays.



   b. For Routing Mode, select the **Enable** radio button.
   c. Click **Apply**.

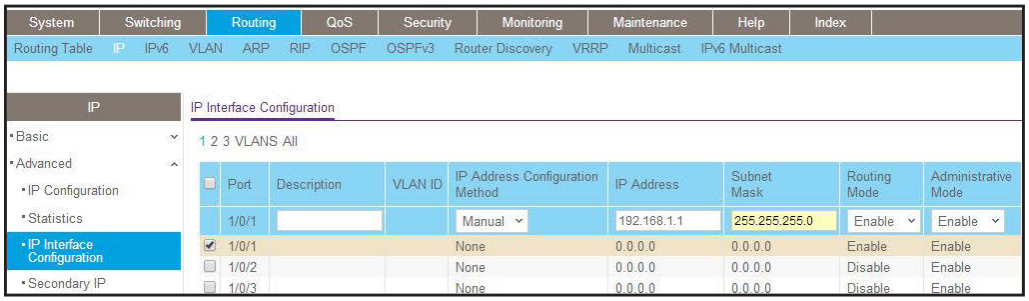
2. Enable IPv6 forwarding and unicast routing on the switch.
   a. Select **Routing > IPv6 > Basic> Global Configuration**.

      A screen similar to the following displays.



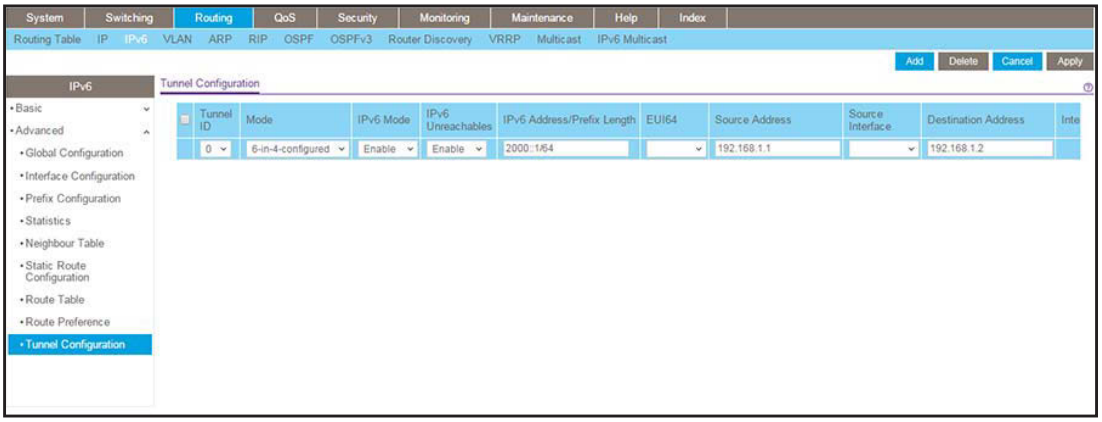
   b. For IPv6 Unicast Routing, select the **Enable** radio button.
   c. For IPv6 Forwarding, select the **Enable** radio button.
   d. Click **Apply**.
3. Create a routing interface and assign an IP address to it.
   a. Select **Routing > IP > Advanced > IP Interface Configuration**.

      A screen similar to the following displays.



   b. Under IP Interface Configuration, scroll down and select the Port **1/0/1** check box. Now 1/0/1 appears in the Interface field at the top.
      - In the **IP Address** field, enter **192.168.1.1**.
      - In the **Subnet Mask** field, enter **255.255.255.0**.
      - In the **Routing Mode** field, select **Enable**.
   c. Click **Apply**.
4. Create a 6-in-4 tunnel interface.
   a. Select **Routing > IPv6 > Advanced > Tunnel Configuration**.

A screen similar to the following displays.



b. In the **Tunnel ID** list, select **0**.

c. In the **Mode** field, select **6-in-4-configured**.

d. In the **Source Address** field, enter **192.168.1.1**.

e. In the **IPv6 Mode** field, select **Enable**.

f. In the **IPv6 Address/Prefix Length** field, enter **2000::1/64**.

g. In the **Destination Address** field, enter **192.168.1.2**.

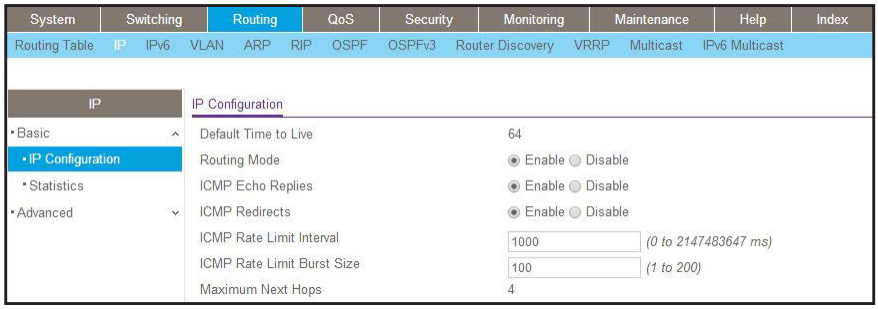
h. Click **Apply**.

Web Interface: Create a 6in4 Tunnel on Switch 2

1. Enable IP routing on the switch.

   a. Select **Routing > IP > Basic > IP Configuration**.

   A screen similar to the following displays.



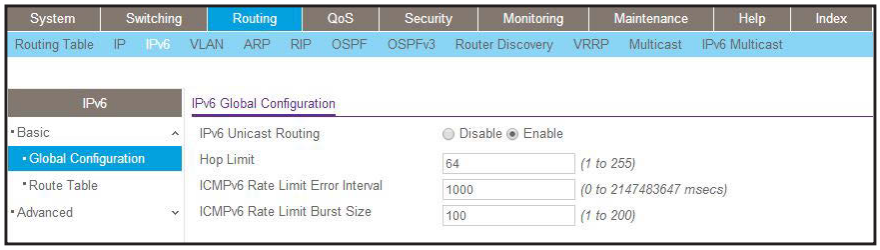
   b. For Routing Mode, select the **Enable** radio button.

   c. Click **Apply**.

2. Enable IPv6 forwarding and unicast routing on the switch.

   a. Select **Routing > IPv6 > Basic > Global Configuration**.

A screen similar to the following displays.



b. For IPv6 Unicast Routing, select the **Enable** radio button.

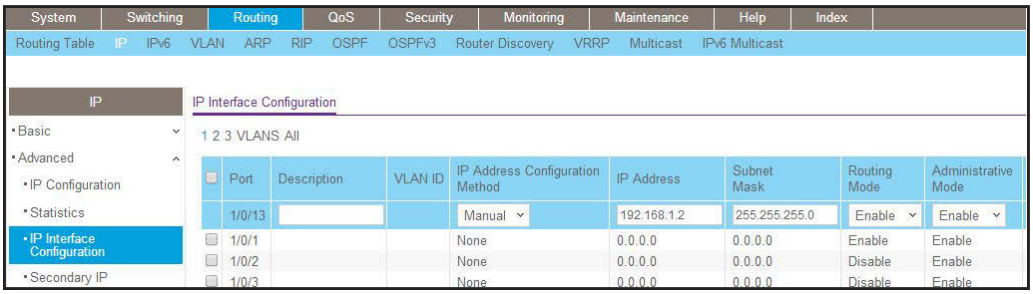
c. For IPv6 Forwarding, select the **Enable** radio button.

d. Click **Apply**.

3. Create a routing interface and assign an IP address to it.

a. Select **Routing > IP > Advanced > IP Interface Configuration**.

A screen similar to the following displays.



b. Under IP Interface Configuration, scroll down and select the Port **1/0/13** check box. Now 1/0/1 appears in the Port field at the top.

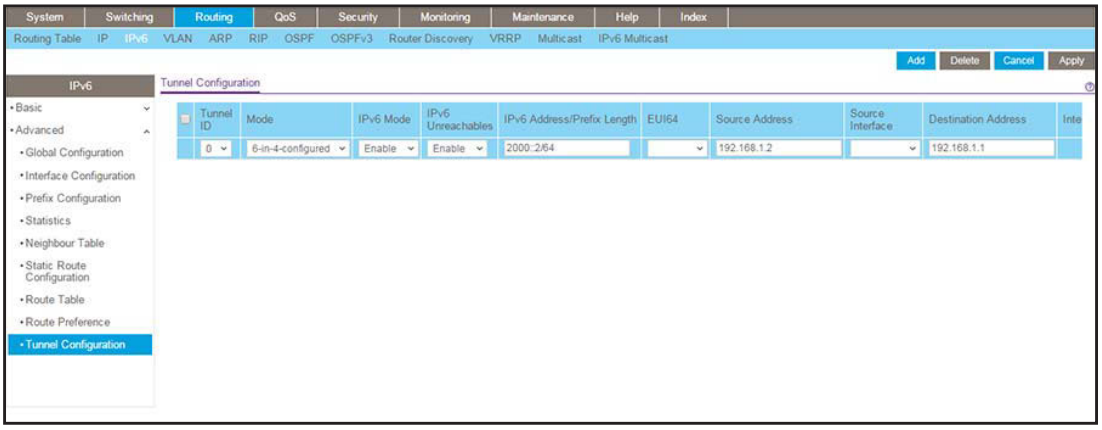
- In the **IP Address** field, enter **192.168.1.2**.
- In the **Subnet Mask** field, enter **255.255.255.0**.
- In the **Routing Mode** field, select **Enable**.

c. Click **Apply**.

4. Create a 6-in-4 tunnel interface.

a. Select **Routing > IPv6 > Advanced > Tunnel Configuration**.

A screen similar to the following displays.



b. In the **Tunnel Id** list, select **0**.

c. In the **Mode** list, select **6-in-4-configured**.

d. In the **IPv6 Address/Prefix Length** field, enter **2000::2/64**.

e. In the **Source Address** field, enter **192.168.1.2**.

f. In the **Destination Address** field, enter **192.168.1.1**.

g. Click **Apply**.

Create a 6to4 Tunnel

An IPv6 tunnel in 6to4 mode connects an isolated IPv6 domain (that is, an 6to4 island) over an IPv4 domain to remote IPv6 domains or to another 6to4 island. An IPv6 tunnel in 6to4 mode is also called an automatic 6to4 tunnel. Unlike a 6in4 tunnel, which is a point-to-point tunnel, a 6to4 tunnel is a point-to-multipoint tunnel. In a 6to4 tunnel, the IPv6 tunnel destination is determined by the IPv4 address, which is extracted from IPv6 destination address with the prefix 2002::V4ADDR::/48.

A NETGEAR switch behaves as a 6to4 border router that connects 6to4 islands (in the following figure, Switch 1 and Switch 2) to an IPv6 domain (in the following figure, Switch 3). This means the following:

The NETGEAR switch forwards traffic from an IPv6 domain (with a non-2002:: address) to a 6to4 island (with a 2002:: address) and the other way around. (In the following figure, this type of forwarding refers to the traffic between Switch 1 and Switch 3 and the traffic between Switch 2 and Switch 3).

The NETGEAR switch forwards traffic from one 6to4 island to another 6to4 island (in the following figure, the traffic between Switch 1 and Switch 2).

The NETGEAR switch does not forward traffic from one IPv6 domain (with a non-2002:: address) to other IPv6 domain (also with a non-2002:: address).

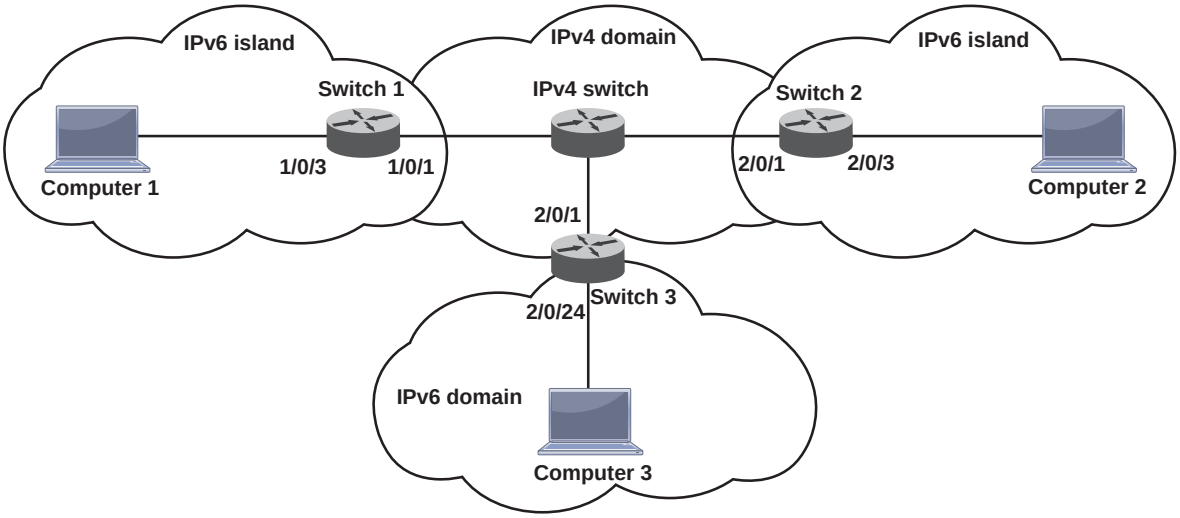


Figure 56. 6to4 tunnel configuration

Note: The following examples do not include the configuration of the IPv4 switch because the 6to4 configuration occurs only in the IPv6 island. The switch in IPv4 domain does not require any special configuration.

CLI: Create a 6to4 Tunnel

You must configure Switch1, Switch2, and Switch 3.

CLI: Create a 6to4 Tunnel on Switch 1

1. Enable routing and IPv6 routing on Switch 1.

```
(Netgear Switch) # config
(Netgear Switch) (Config)#ipv6 unicast-routing
(Netgear Switch) (Config)#ip routing
```

2. Configure IPv4 address on routing port 1/0/1**.**

```
(Netgear Switch) (Config)#interface 1/0/1
(Netgear Switch) (Interface 1/0/1)#routing
(Netgear Switch) (Interface 1/0/1)#ip address 195.1.3.2 255.255.255.0
(Netgear Switch) (Interface 1/0/1)#exit
```

3. Configure the IPv6 address on the 6to4 tunnel in the format 2002:V4ADDR::Host/16, in which where V4ADDR is the source IPv4 address of the tunnel. The prefix length for the tunnel must be 16.

```
(Netgear Switch) (Config)#interface tunnel 0
(Netgear Switch) (Interface tunnel 0)#ipv6 address 2002:c301:302::1/16
(Netgear Switch) (Interface tunnel 0)#ipv6 enable
(Netgear Switch) (Interface tunnel 0)#tunnel mode ipv6ip 6to4
(Netgear Switch) (Interface tunnel 0)#tunnel source 195.1.3.2
(Netgear Switch) (Interface tunnel 0)#exit
```

4. Configure the IPv6 address for routing port 1/0/3. The IPv6 address format is 2002:V4ADDR:Subnet::Host/64, in which V4ADDR is the source IPv4 address of the tunnel and Subnet is the subnet of 2002:V4ADDR::/64.

```
(Netgear Switch) (Config)#interface 1/0/3
(Netgear Switch) (Interface 1/0/3)#routing
(Netgear Switch) (Interface 1/0/3)#ipv6 address 2002:c301:302:1::1/64
(Netgear Switch) (Interface 1/0/3)#ipv6 enable
(Netgear Switch) (Interface 1/0/3)#exit
```

5. Create a static IPv4 route to ensure that Switch 1 can reach Switch 2 and Switch 3. You can also use a routing protocol such as RIP or OSPF to let Switch 1 learn the routes from Switch 2 and Switch 3.

```
(Netgear Switch) (Config)#ip route 195.1.4.0 255.255.255.0 195.1.3.1
(Netgear Switch) (Config)#ip route 195.1.5.0 255.255.255.0 195.1.3.1
```

6. Because Switch 1 cannot detect the route for IPv6 address 8888::/16 (of port 2/0/24 on Switch 3), create a static IPv6 route for Switch 1 with the tunnel address of Switch 3 as the next hop.

```
(Netgear Switch) (Config)#ipv6 route 8888::/16 2002:c301:502::1
```

7. Verify the configuration.

```
(Netgear Switch) #show ipv6 route
IPv6 Routing Table - 5 entries
Codes: C - connected, S - static, 6To4 - 6to4 Route, B - BGP Derived
       O - OSPF Intra, OI - OSPF Inter, OE1 - OSPF Ext 1, OE2 - OSPF Ext 2
       ON1 - OSPF NSSA Ext Type 1, ON2 - OSPF NSSA Ext Type 2
C    2002::/16 [0/0]
      via ::,   tunnel 0
C    2002:c301:302:1::/64 [0/0]
      via ::,   1/0/3
6To4 2002:c301:402::/48 [1/0]
      via fe80::c301:301,   01h:25m:23s,  tunnel 0
6To4 2002:c301:502::/48 [1/0]
      via fe80::c301:301,   00h:44m:11s,  tunnel 0
S    8888::/16 [1/0]
      via 2002:c301:502::1,   tunnel 0
```

CLI: Create a 6to4 Tunnel on Switch 2

1. Enable routing and IPv6 routing on Switch 2.

```
(Netgear Switch) # config
(Netgear Switch) (Config)#ipv6 unicast-routing
(Netgear Switch) (Config)#ip routing
```

2. Configure the IPv4 address on routing port 2/0/1.

```
(Netgear Switch) (Config)# interface 2/0/1
(Netgear Switch) (Interface 2/0/1)#routing
(Netgear Switch) (Interface 2/0/1)#ip address 195.1.4.2 255.255.255.0
(Netgear Switch) (Interface 2/0/1)#exit
```

3. Configure the IPv6 address on the 6to4 tunnel in the format 2002:V4ADDR::Host/16, in which where V4ADDR is the source IPv4 address of the tunnel. The prefix length for the tunnel must be 16.

```
(Netgear Switch) (Config)#interface tunnel 0
(Netgear Switch) (Interface tunnel 0)#ipv6 address 2002:c301:402::1/16
(Netgear Switch) (Interface tunnel 0)#ipv6 enable
(Netgear Switch) (Interface tunnel 0)#tunnel mode ipv6ip 6to4
(Netgear Switch) (Interface tunnel 0)#tunnel source 195.1.4.2
(Netgear Switch) (Interface tunnel 0)#exit
```

4. Configure the IPv6 address for routing port 2/0/3. The IPv6 address format is 2002:V4ADDR:Subnet::Host/64, in which V4ADDR is the source IPv4 address of the tunnel and Subnet is the subnet of 2002:V4ADDR::/64.

```
(Netgear Switch) (Config)#interface 2/0/3
(Netgear Switch) (Interface 2/0/3)#routing
(Netgear Switch) (Interface 2/0/3)#ipv6 address 2002:c301:402:1::1/64
(Netgear Switch) (Interface 2/0/3)#ipv6 enable
(Netgear Switch) (Interface 2/0/3)#exit
```

5. Create a static IPv4 route to ensure that Switch 2 can reach Switch 1. You can also use a routing protocol such as RIP or OSPF to let Switch 2 learn the route from Switch 1.

```
(Netgear Switch) (Config)#ip route 195.1.3.0 255.255.255.0 195.1.4.1
```

6. Verify the configuration.

```
(Netgear Switch) #show ipv6 route
IPv6 Routing Table - 3 entries
Codes: C - connected, S - static, 6To4 - 6to4 Route, B - BGP Derived
       O - OSPF Intra, OI - OSPF Inter, OE1 - OSPF Ext 1, OE2 - OSPF Ext 2
       ON1 - OSPF NSSA Ext Type 1, ON2 - OSPF NSSA Ext Type 2
C    2002::/16 [0/0]
      via ::,   tunnel 0
6To4 2002:c301:302::/48 [1/0]
      via fe80::c301:401,   01h:32m:28s,  tunnel 0
C    2002:c301:402:1::/64 [0/0]
      via ::,   2/0/3
```

CLI: Create a 6to4 Tunnel on Switch 3

1. Enable routing and IPv6 routing on Switch 3.

```
(Netgear Switch) # config
(Netgear Switch) (Config)#ipv6 unicast-routing
(Netgear Switch) (Config)#ip routing
```

2. Configure IPv4 address on routing port 2/0/1.

```
(Netgear Switch) (Config)# interface 2/0/1
(Netgear Switch) (Interface 2/0/1)#routing
(Netgear Switch) (Interface 2/0/1)#ip address 195.1.5.2 255.255.255.0
(Netgear Switch) (Interface 2/0/1)#exit
```

3. Configure the IPv6 address on the 6to4 tunnel in the format 2002:V4ADDR::Host/16, in which where V4ADDR is the source IPv4 address of the tunnel. The prefix length for the tunnel must be 16.

```
(Netgear Switch) (Config)#interface tunnel 0
(Netgear Switch) (Interface tunnel 0)#ipv6 address 2002:c301:502::1/16
(Netgear Switch) (Interface tunnel 0)#ipv6 enable
(Netgear Switch) (Interface tunnel 0)#tunnel mode ipv6ip 6to4
(Netgear Switch) (Interface tunnel 0)#tunnel source 195.1.5.2
(Netgear Switch) (Interface tunnel 0)#exit
```

4. Configure a global IPv6 address on routing port 2/0/1.

```
(Netgear Switch) (Config)#interface 2/0/24
(Netgear Switch) (Interface 2/0/24)#routing
(Netgear Switch) (Interface 2/0/24)#ipv6 address 8888::1/64
(Netgear Switch) (Interface 2/0/24)#ipv6 enable
(Netgear Switch) (Interface 2/0/24)#exit
```

5. Create a static IPv4 route to ensure that Switch 3 can reach Switch 1. You can also use a routing protocol such as RIP or OSPF to let Switch 3 learn the route from Switch 1.

```
(Netgear Switch) (Config)#ip route 195.1.3.0 255.255.255.0 195.1.5.1
```

6. Verify the configuration.

```
(Netgear Switch) #show ipv6 route
IPv6 Routing Table - 3 entries
Codes: C - connected, S - static, 6To4 - 6to4 Route, B - BGP Derived
       O - OSPF Intra, OI - OSPF Inter, OE1 - OSPF Ext 1, OE2 - OSPF Ext 2
       ON1 - OSPF NSSA Ext Type 1, ON2 - OSPF NSSA Ext Type 2
C    2002::/16 [0/0]
      via ::,   tunnel 0
6To4 2002:c301:302::/48 [1/0]
      via fe80::c301:501,   00h:50m:06s,  tunnel 0
C    8888::/64 [0/0]
      via ::,   2/0/24
```

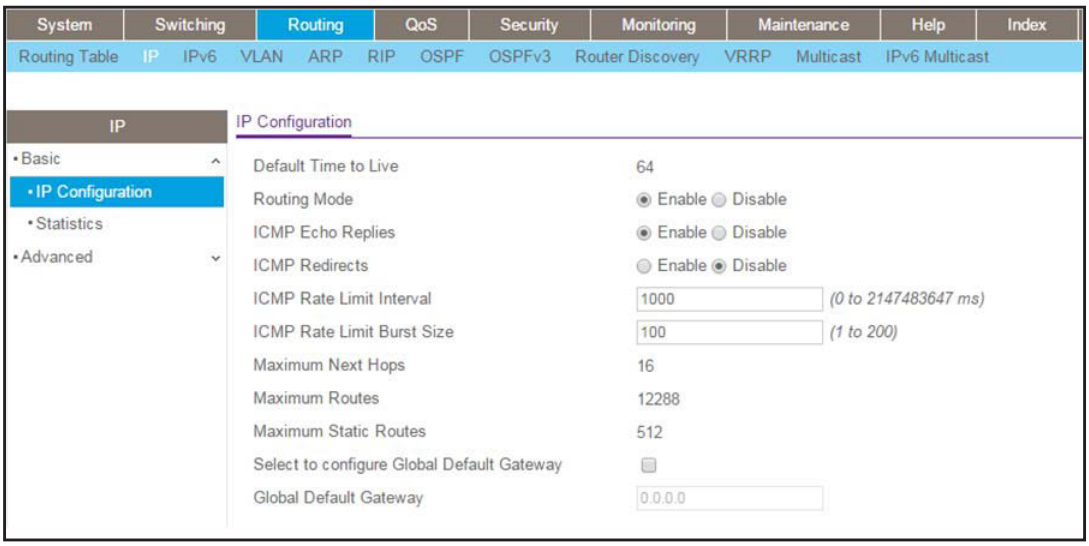
Web Interface: Create a 6to4 Tunnel

You must configure Switch1, Switch2, and Switch 3.

Web Interface: Create a 6to4 Tunnel on Switch 1

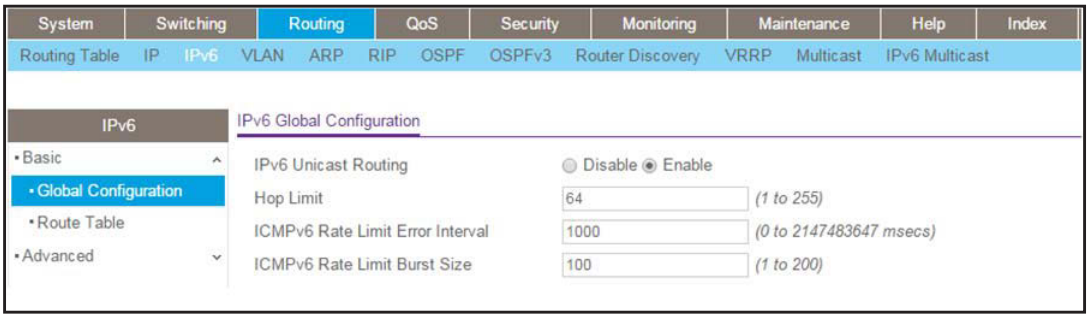
1. Enable IP routing on Switch 1.
   a. Select **Routing > IP > Basic > IP Configuration**.

      A screen similar to the following displays.



   b. For Routing Mode, select the **Enable** radio button.
   c. Click **Apply**.
2. Enable IPv6 forwarding and unicast routing on Switch 1.
   a. Select **Routing > IPv6 > Basic> Global Configuration**.

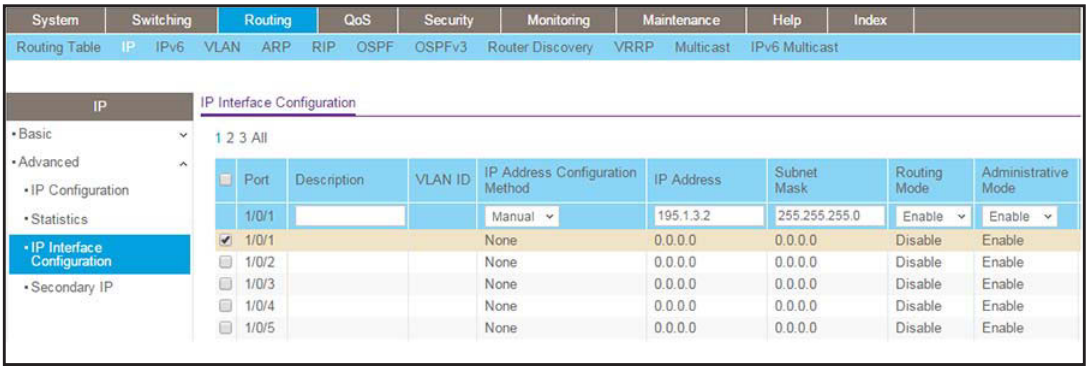
      A screen similar to the following displays.



   b. For IPv6 Unicast Routing, select the **Enable** radio button.
   c. Click **Apply**.

3. Create a routing interface and assign an IP address to it.
   a. Select **Routing > IP > Advanced > IP Interface Configuration**.

      A screen similar to the following displays.



   b. Select the **1/0/1** check box for port 1/0/1.

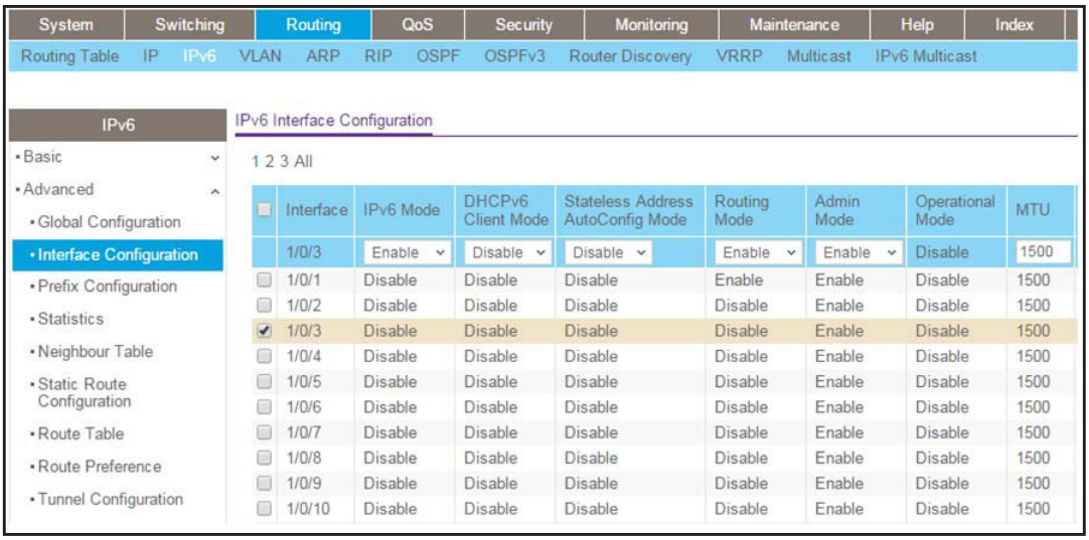
      The settings for port 1/0/1 display in the fields in the table heading.

   c. Configure the following settings:
      - In the **IP Address Configuration Method** field, select **Manual**.
      - In the **IP Address** field, enter **195.1.3.2**.
      - In the **Subnet Mask** field, enter **255.255.255.0**.
      - In the **Routing Mode** field, select **Enable**.

   d. Click **Apply**.

4. Create an IPv6 routing interface.
   a. Select **Routing > IPv6 > Advanced > Interface Configuration**.

      A screen similar to the following displays.



   b. Select the **1/0/3** check box for port 1/0/3.

The settings for port 1/0/3 display in the fields in the table heading.

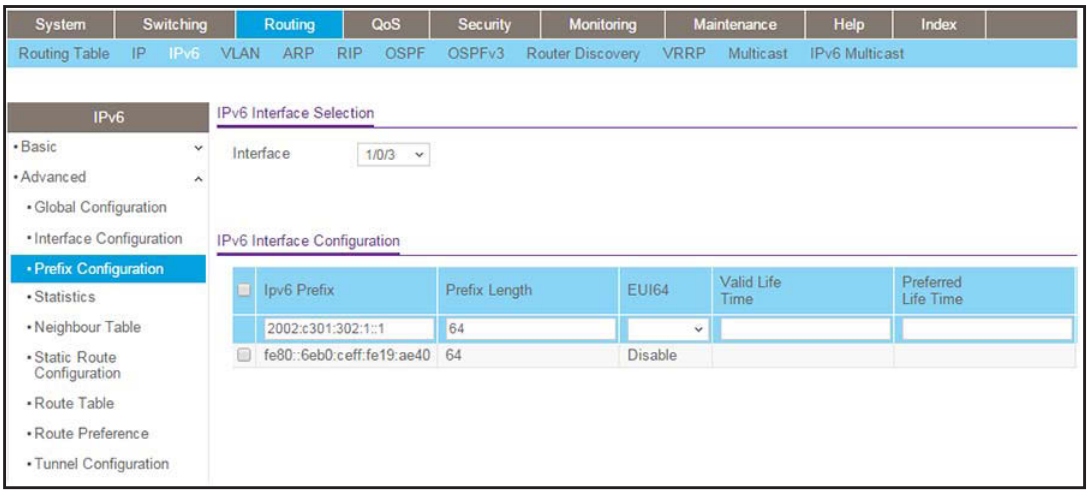
c. Configure the following settings:
   - In the **IPv6 Mode** field, select **Enable**.
   - In the **Routing Mode** field, select **Enable**.

d. Click **Apply**.

5. Configure the IPv6 address for IPv6 routing interface 1/0/3.

a. Select **Routing > IPv6 > Advanced > Prefix Configuration**.

A screen similar to the following displays.



b. From the **Interface** menu, select **1/0/3**.

The settings for port 1/0/3 display in the fields in the table heading.

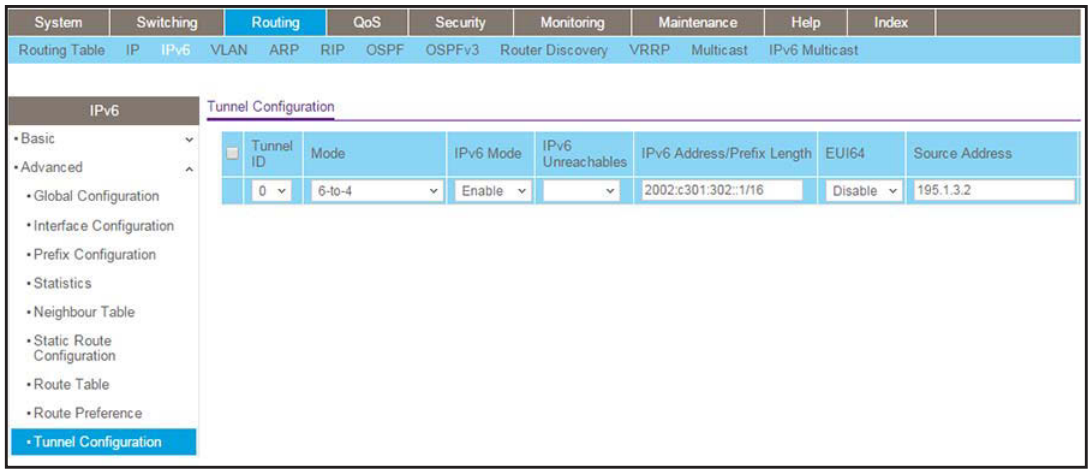
c. Configure the following settings:
   - In the **Ipv6 Prefix** field, enter **2002:c301:302:1::1**.
   - In the **Prefix Length** field, enter **64**.
   - In the **EUI64** field, select **Disable**.

d. Click **Add**.

6. Create a 6to4 tunnel interface.

a. Select **Routing > IPv6 > Advanced > Tunnel Configuration**.

A screen similar to the following displays.



b. Configure the following tunnel settings:

- In the **Tunnel ID** field, select **0**.
- In the **Mode** field, select **6-to-4**.
- In the **IPv6 Mode** field, select **Enable**.
- In the **IPv6 Address/Prefix Length** field, enter **2002:c301:302::1/16**.
- In the **EUI64** field, select **Disable**.
- In the **Source Address** field, enter **195.1.3.2**.

c. Click **Add**.

7. Create a default route for nonnative IPv6 addresses.

a. Select **Routing > IPv6 > Advanced > Static Route Configuration**.

A screen similar to the following displays.

b. Configure the following route settings:

- In the **IPv6 Prefix** field, enter **8888::**.
- In the **Prefix Length** field, enter **16**.

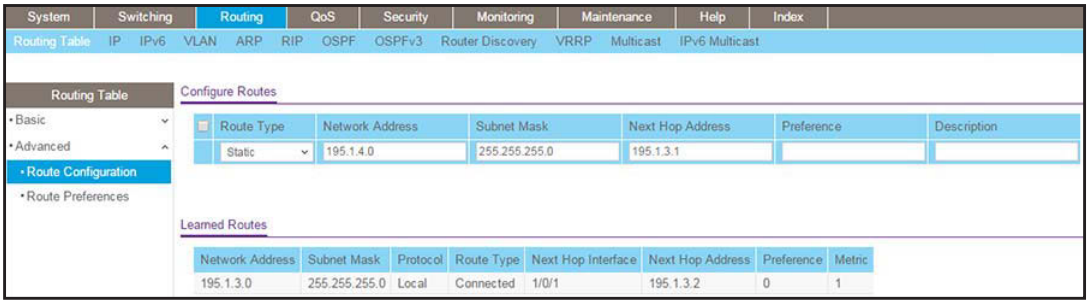
- In the **Next Hop IPv6 Address Type** field, select **Global**.
- In the **Next Hop IPv6 Address** field, enter **2002:c301:502::1**.

c. Click **Add**.

8. Create a static route for subnet 195.1.4.0/24.

a. Select **Routing > Routing Table > Advanced > Route Configuration**.

A screen similar to the following displays.



b. Configure the following route settings:

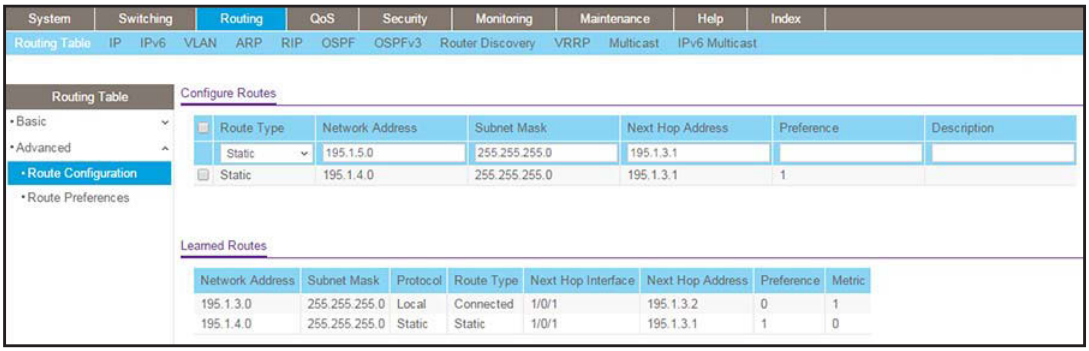
- In the **Network Address** field, enter **195.1.4.0**.
- In the **Subnet Mask** field, enter **255.255.255.0**.
- In the **Next Hop Address** field, enter **195.1.3.1**.

c. Click **Add**.

9. Create a static route for 195.1.5.0/24.

a. Select **Routing > Routing Table > Advanced > Route Configuration**.

A screen similar to the following displays.



b. Configure the following route settings:

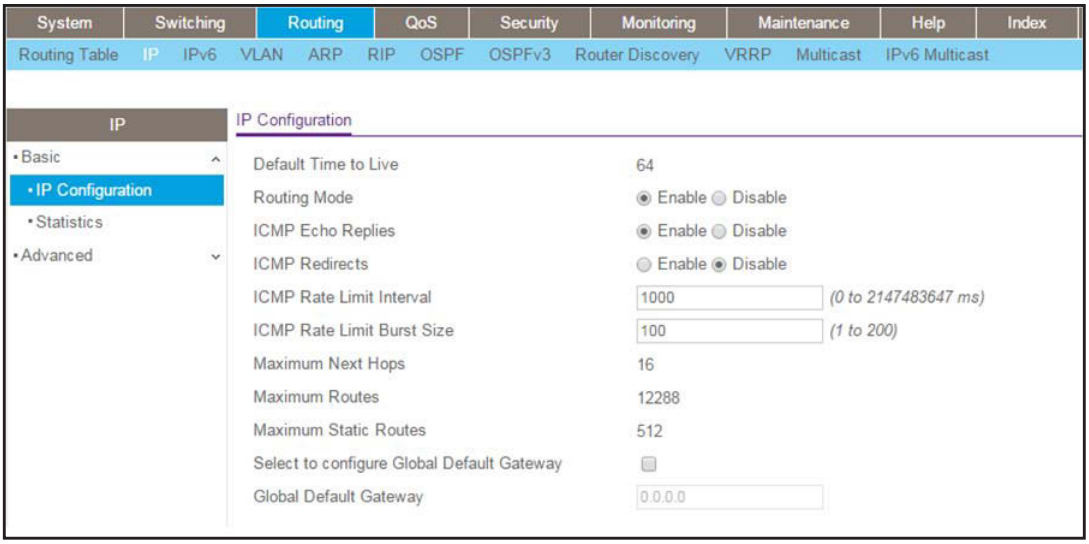
- In the **Network Address** field, enter **195.1.5.0**.
- In the **Subnet Mask** field, enter **255.255.255.0**.
- In the **Next Hop Address** field, enter **195.1.3.1**.

c. Click **Add**.

Web Interface: Create a 6to4 Tunnel on Switch 2

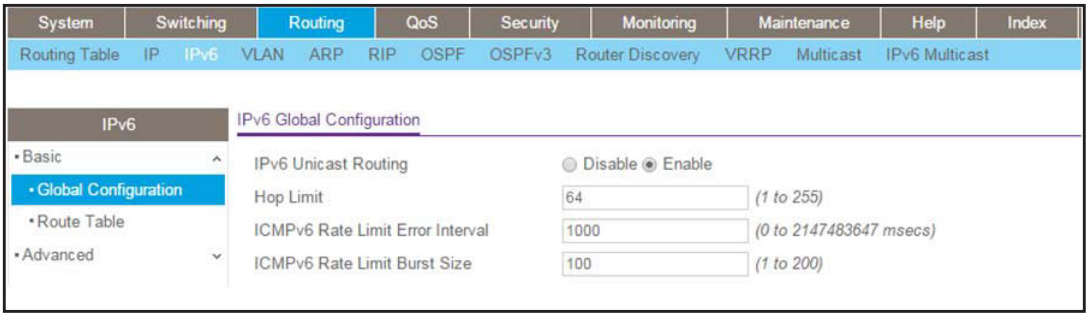
1. Enable IP routing on Switch 2.
   a. Select **Routing > IP > Basic > IP Configuration**.

      A screen similar to the following displays.



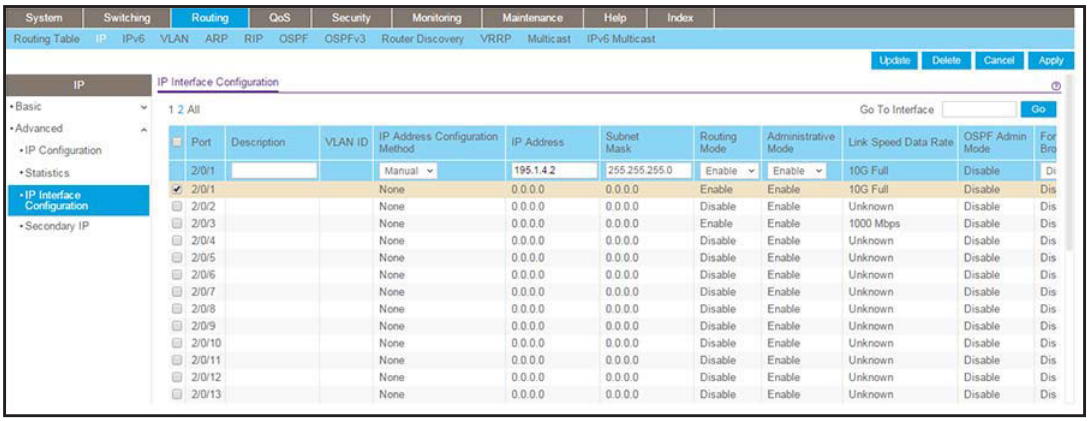
   b. For Routing Mode, select the **Enable** radio button.
   c. Click **Apply**.
2. Enable IPv6 forwarding and unicast routing on Switch 2.
   a. Select **Routing > IPv6 > Basic> Global Configuration**.

      A screen similar to the following displays.



   b. For IPv6 Unicast Routing, select the **Enable** radio button.
   c. Click **Apply**.
3. Create a routing interface and assign an IP address to it.
   a. Select **Routing > IP > Advanced > IP Interface Configuration**.

      A screen similar to the following displays.



b. Above the table heading, Under IP Interface Configuration, click **2**.

c. Select the **2/0/1** check box for port 2/0/1.

The settings for port 2/0/1 display in the fields in the table heading.

d. Configure the following settings:

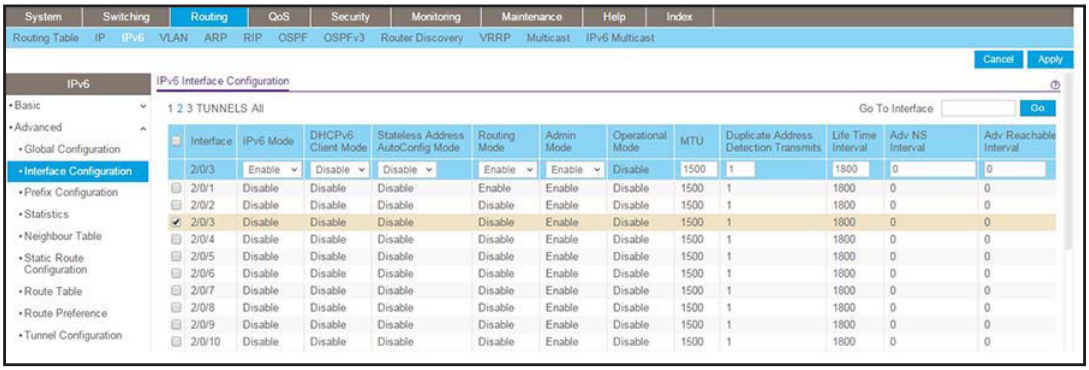
- In the **IP Address Configuration Method** field, select **Manual**.
- In the **IP Address** field, enter **195.1.4.2**.
- In the **Subnet Mask** field, enter **255.255.255.0**.
- In the **Routing Mode** field, select **Enable**.

e. Click **Apply**.

4. Create an IPv6 routing interface.

a. Select **Routing > IPv6 > Advanced > Interface Configuration**.

A screen similar to the following displays.



b. Above the table heading, Under IP Interface Configuration, click **2**.

c. Select the **2/0/3** check box for port 2/0/3.

The settings for port 2/0/3 display in the fields in the table heading.

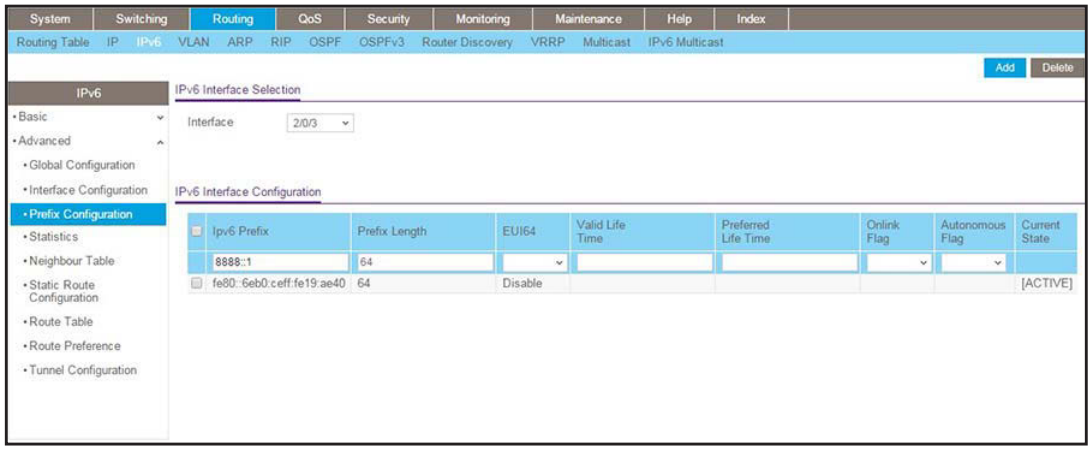
d. Configure the following settings:
   - In the **IPv6 Mode** field, select **Enable**.
   - In the **Routing Mode** field, select **Enable**.

e. Click **Apply**.

5. Configure an IPv6 address for routing interface 2/0/3.

a. Select **Routing > IPv6 > Advanced > Prefix Configuration**.

A screen similar to the following displays.



b. From the **Interface** menu, select **2/0/3**.

The settings for port 2/0/3 display in the fields in the table heading.

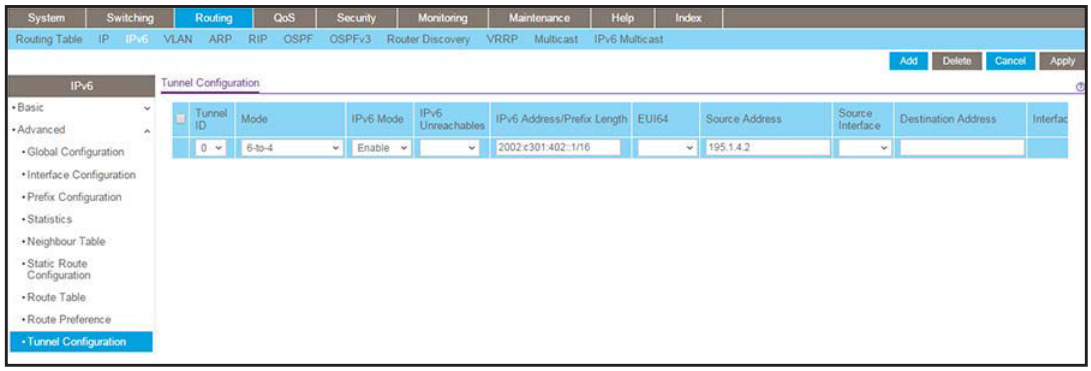
c. Configure the following settings:
   - In the **Ipv6 Prefix** field, enter **2002:c301:402:1::1**.
   - In the **Prefix Length** field, enter **64**.
   - In the **EUI64** field, select **Disable**.

d. Click **Add**.

6. Create a 6to4 tunnel interface.

a. Select **Routing > IPv6 > Advanced > Tunnel Configuration**.

A screen similar to the following displays.



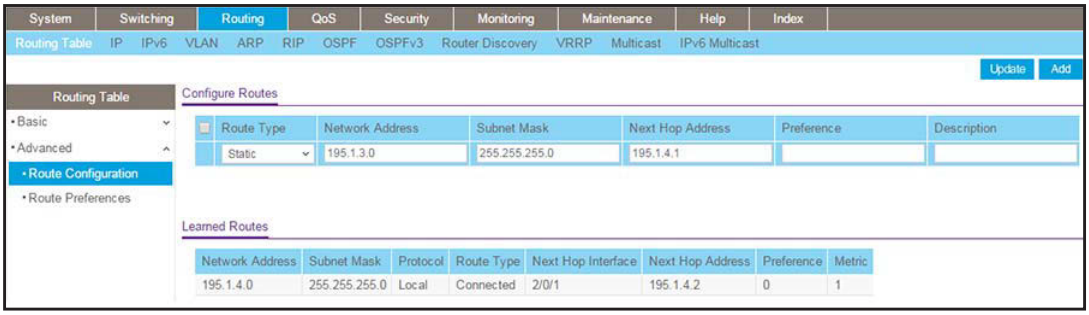
b. Configure the following tunnel settings:
   - In the **Tunnel ID** field, select **0**.
   - In the **Mode** field, select **6-to-4**.
   - In the **IPv6 Mode** field, select **Enable**.
   - In the **IPv6 Address/Prefix Length** field, enter **2002:c301:402::1/16**.
   - In the **EUI64** field, select **Disable**.
   - In the **Source Address** field, enter **195.1.4.2**.

c. Click **Add**.

7. Create a static route for subnet 195.1.3.0/24.

a. Select **Routing > Routing Table > Advanced > Route Configuration**.

A screen similar to the following displays.



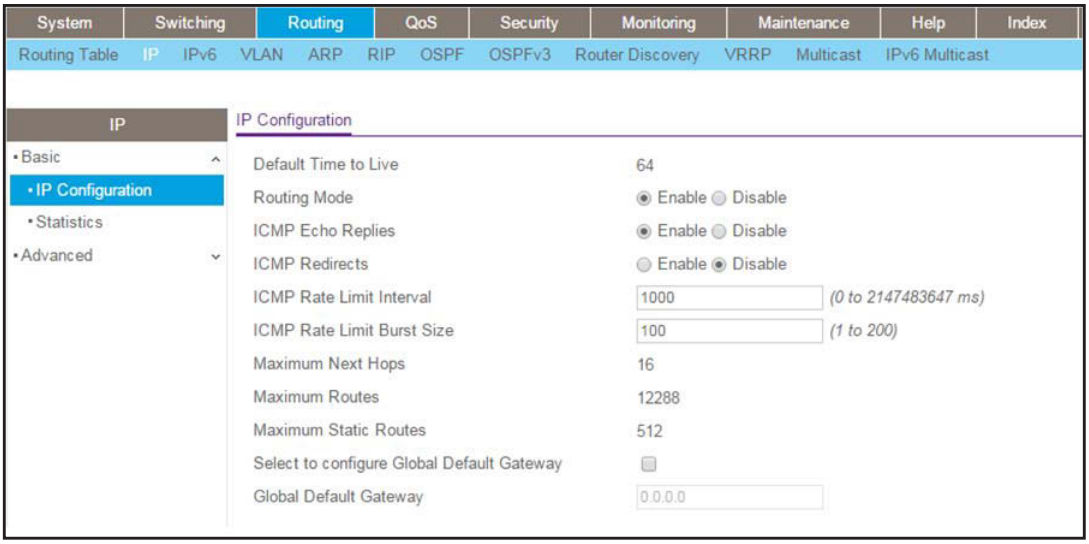
b. Configure the following route settings:
   - In the **Network Address** field, enter **195.1.3.0**.
   - In the **Subnet Mask** field, enter **255.255.255.0**.
   - In the **Next Hop Address** field, enter **195.1.4.1**.

c. Click **Add**.

Web Interface: Create a 6to4 Tunnel on Switch 3

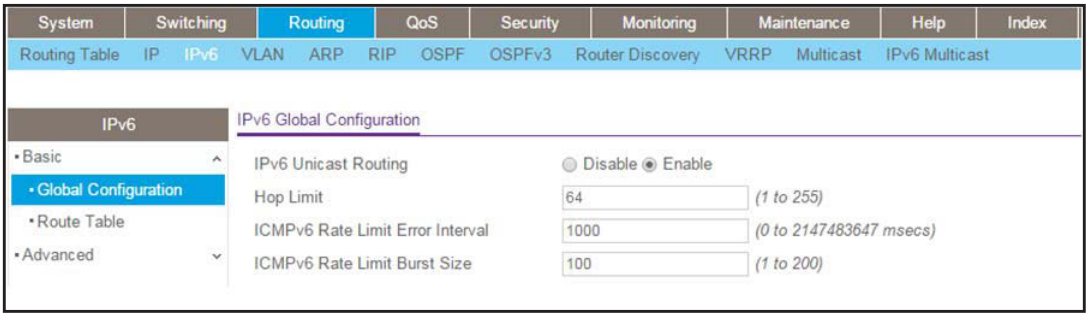
1. Enable IP routing on Switch 3.
   a. Select **Routing > IP > Basic > IP Configuration**.

      A screen similar to the following displays.



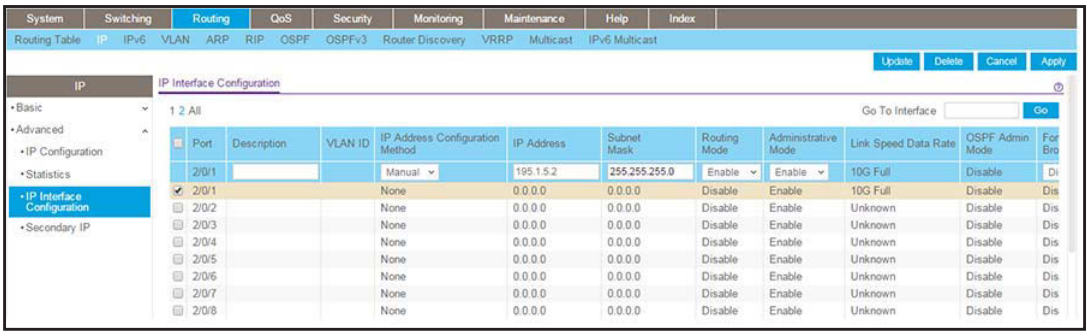
   b. For Routing Mode, select the **Enable** radio button.
   c. Click **Apply**.
2. Enable IPv6 forwarding and unicast routing on Switch 3.
   a. Select **Routing > IPv6 > Basic> Global Configuration**.

      A screen similar to the following displays.



   b. For IPv6 Unicast Routing, select the **Enable** radio button.
   c. Click **Apply**.
3. Create a routing interface and assign an IP address to it.
   a. Select **Routing > IP > Advanced > IP Interface Configuration**.

      A screen similar to the following displays.



b. Above the table heading, Under IP Interface Configuration, click **2**.

c. Select the **2/0/1** check box for port 2/0/1.

The settings for port 2/0/1 display in the fields in the table heading.

d. Configure the following settings:

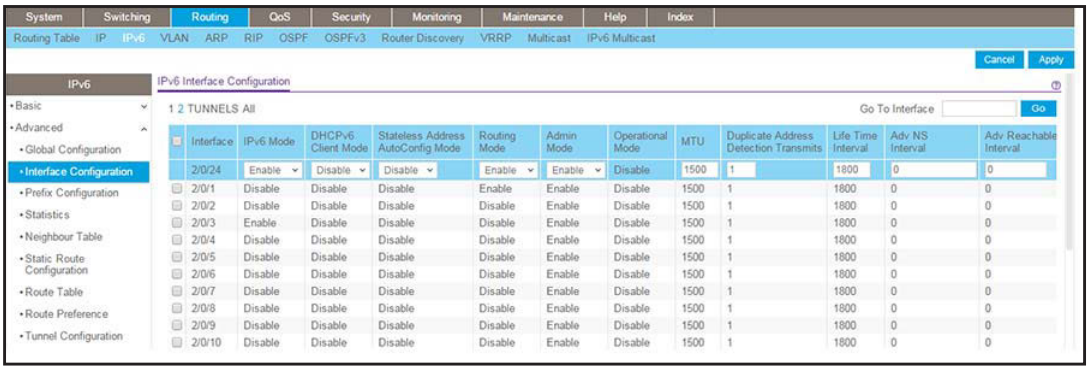
- In the **IP Address Configuration Method** field, select **Manual**.
- In the **IP Address** field, enter **195.1.5.2**.
- In the **Subnet Mask** field, enter **255.255.255.0**.
- In the **Routing Mode** field, select **Enable**.

e. Click **Apply**.

4. Create an IPv6 routing interface.

a. Select **Routing > IPv6 > Advanced > Interface Configuration**.

A screen similar to the following displays.



b. Above the table heading, Under IP Interface Configuration, click **2**.

c. Select the **2/0/24** check box for port 2/0/24.

The settings for port 2/0/24 display in the fields in the table heading.

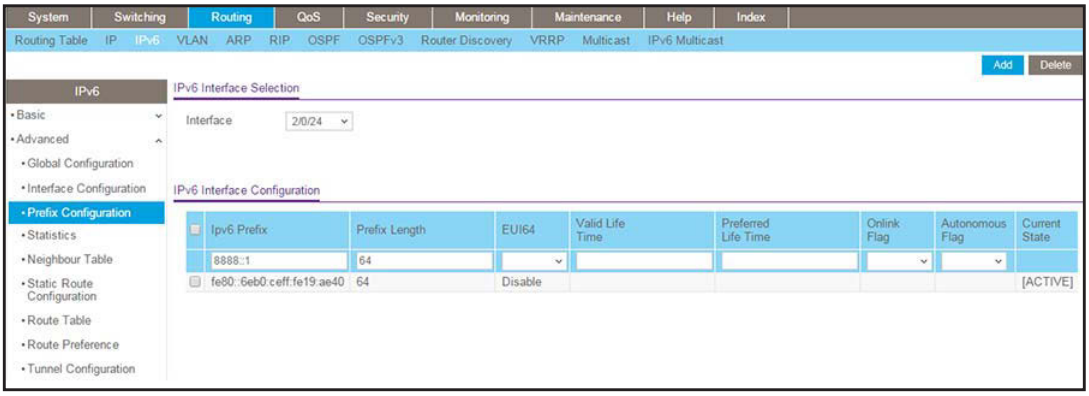
d. Configure the following settings:

- In the **IPv6 Mode** field, select **Enable**.
- In the **Routing Mode** field, select **Enable**.

e. Click **Apply**.

5. Configure the IPv6 address for the IPv6 routing interface 2/0/24.
   a. Select **Routing > IPv6 > Advanced > Prefix Configuration**.

      A screen similar to the following displays.



   b. From the **Interface** menu, select **2/0/24**.

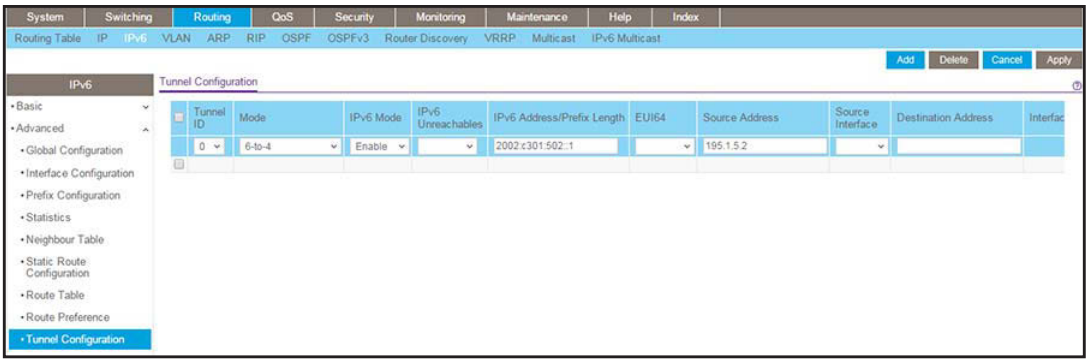
      The settings for port 2/0/24 display in the fields in the table heading.

   c. Configure the following settings:
      - In the **Ipv6 Prefix** field, enter **8888::1**.
      - In the **Prefix Length** field, enter **64**.
      - In the **EUI64** field, select **Disable**.

   d. Click **Add**.

6. Create a 6to4 tunnel interface.
   a. Select **Routing > IPv6 > Advanced > Tunnel Configuration**.

      A screen similar to the following displays.



   b. Configure the following tunnel settings:
      - In the **Tunnel ID** field, select **0**.
      - In the **Mode** field, select **6-to-4**.
      - In the **IPv6 Mode** field, select **Enable**.
      - In the **IPv6 Address/Prefix Length** field, enter **2002:c301:402::1/16**.

- In the **EUI64** field, select **Disable**.
- In the **Source Address** field, enter **195.1.4.2**.

c. Click **Add**.

d. Configure the following tunnel settings:

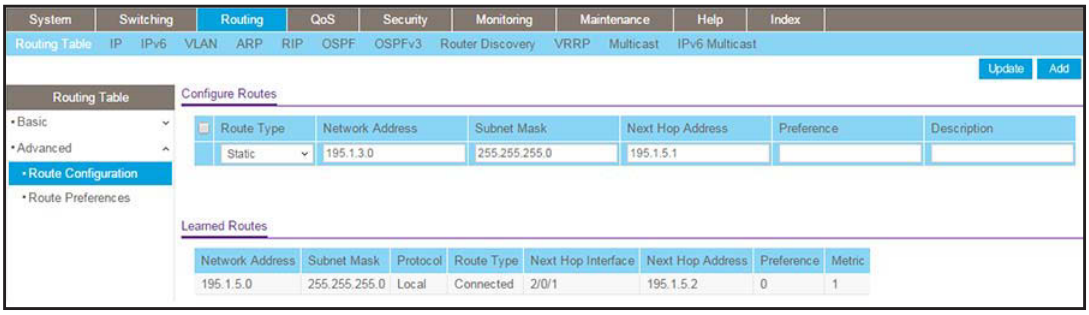
- In the **Tunnel ID** field, select **0**.
- In the **Mode** field, select **6-to-4**.
- In the **IPv6 Mode** field, select **Enable**.
- In the **IPv6 Address/Prefix Length** field, enter **2002:c301:502::1/16**.
- In the **EUI64** field, select **Disable**.
- In the **Source Address** field, enter **195.1.5.2**.

e. Click **Add**.

7. Create a static route for subnet 195.1.3.0/24.

a. Select **Routing > Routing Table > Advanced > Route Configuration**.

A screen similar to the following displays.



b. Configure the following route settings:

- In the **Network Address** field, enter **195.1.3.0**.
- In the **Subnet Mask** field, enter **255.255.255.0**.
- In the **Next Hop Address** field, enter **195.1.5.1**.

c. Click **Add**.

29 IPv6 Interface Configuration

IPv6 routing and routing VLANs

This chapter includes the following sections:

- *Create an IPv6 Routing Interface*
- *Create an IPv6 Routing VLAN*
- *Configure DHCPv6 Mode on the Routing Interface*

Create an IPv6 Routing Interface

The example is shown as CLI commands and as a web interface procedure.

CLI: Create an IPv6 Routing Interface

1. Enable IPV6 forwarding and unicast routing on the switch.

```
(Netgear Switch) (Config)#ipv6 forwarding
(Netgear Switch) (Config)#ipv6 unicast-routing
```

2. Assign an IPv6 address to interface 1/0/1.

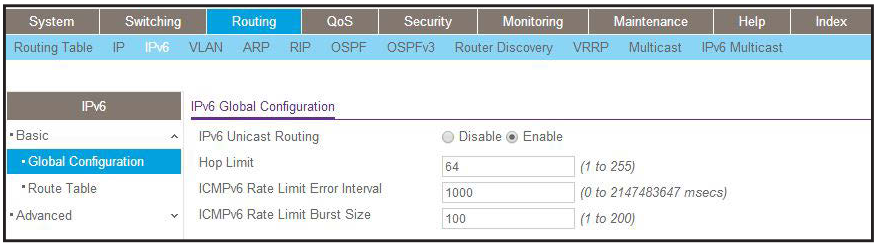
```
(Netgear Switch) (Config)#interface 1/0/1
(Netgear Switch) (Interface 1/0/1)#ipv6 enable
(Netgear Switch) (Interface 1/0/1)#ipv6 address 2000::2/64
(Netgear Switch) (Interface 1/0/1)#routing
(Netgear Switch) (Interface 1/0/1)#exit
(Netgear Switch) #ping ipv6 2000::2
Send count=3, Receive count=3 from 2000::2
Average round trip time = 1.00 ms
(Netgear Switch) #show ipv6 brief
IPv6 Forwarding Mode..... Enable
IPv6 Unicast Routing Mode..... Enable
IPv6 Hop Limit..... 0
ICMPv6 Rate Limit Error Interval..... 1000 msec
ICMPv6 Rate Limit Burst Size..... 100 messages
Maximum Routes..... 12
```

```
(Netgear Switch) #show ipv6 interface 1/0/1
IPv6 is enabled
IPv6 Prefix is ............................... FE80::21E:2AFF:FED9:249B/128
                                                       2000::2/64 [TENT]
Routing Mode.................................. Enabled
Administrative Mode........................... Enabled
IPv6 Routing Operational Mode................. Enabled
Bandwidth..................................... 1000000  kbps
Interface Maximum Transmit Unit............... 1500
Router Duplicate Address Detection Transmits... 1
Router Advertisement NS Interval.............. 0
Router Advertisement Lifetime................. 1800
Router Advertisement Reachable Time........... 0
Router Advertisement Interval................. 600
Router Advertisement Managed Config Flag...... Disabled
Router Advertisement Other Config Flag........ Disabled
Router Advertisement Suppress Flag............ Disabled
IPv6 Destination Unreachables................. Enabled

Prefix 2000::2/64
Preferred Lifetime............................ 604800
Valid Lifetime................................ 2592000
Onlink Flag................................... Enabled
Autonomous Flag............................... Enabled
```

Web Interface: Create an IPv6 Routing Interface

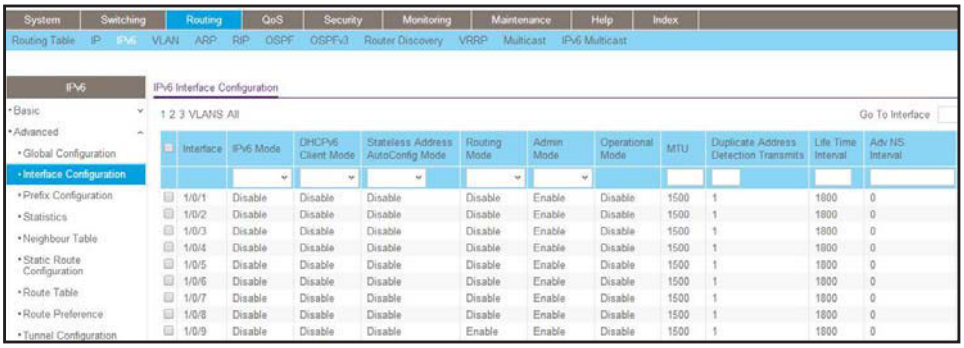
1. Enable IPv6 forwarding and unicast routing on the switch.
   a. Select **Routing > IPv6 > Basic > Global Configuration**.

      A screen similar to the following displays.



   b. For IPv6 Unicast Routing, select the **Enable** radio button.
   c. For IPv6 Forwarding, select the **Enable** radio button.
   d. Click **Apply**.
2. Enable IPv6 routing on interface 1/0/1.
   a. Select **Routing > IPv6 > Advanced > Interface Configuration**.

A screen similar to the following displays.



b. Under IPv6 Interface Configuration, scroll down and select the Interface **1/0/1** check box.

Now 1/0/1 appears in the Interface field at the top.

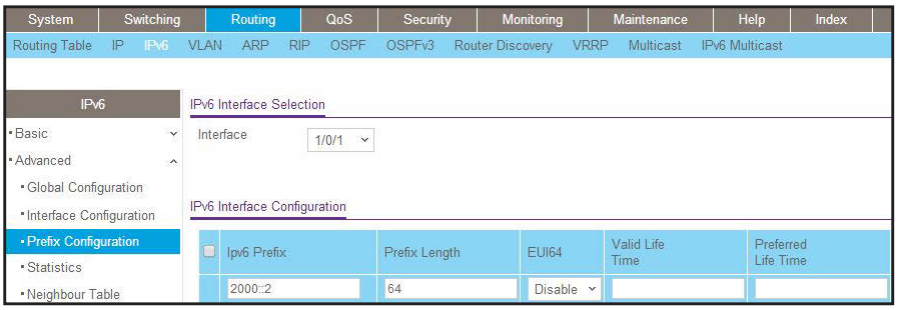
c. In the IPv6 Mode field, select **Enable**.

d. Click **Apply** to save the settings.

3. Assign an IPv6 address to the routing interface.

a. Select **Routing > IPv6 > Advanced > Prefix Configuration**.

A screen similar to the following displays.



b. In the Interface list, select **1/0/1**.

c. In the IPv6 Prefix field, enter **2000::2**.

d. In the Length field, enter **64**.

e. In the EUI64 field, select **Disable**.

f. Click **Add**.

Create an IPv6 Routing VLAN

The example is shown as CLI commands and as a web interface procedure.

CLI: Create an IPv6 Routing VLAN

1. Create a routing VLAN with VLAN ID 500.

```
Netgear Switch) (Vlan)#vlan 500
(Netgear Switch) (Vlan)#vlan routing 500
(Netgear Switch) (Vlan)#exit
```

2. Add interface 1/0/1 to VLAN 500.

```
(Netgear Switch) #config
(Netgear Switch) (Config)#interface 1/0/1
(Netgear Switch) (Interface 1/0/1)#vlan participation include 500
(Netgear Switch) (Interface 1/0/1)#vlan participation pvid 500
(Netgear Switch) (Interface 1/0/1)#exit
```

3. Assign IPv6 address 2000::1/64 to VLAN 500 and enable IPv6 routing.

```
(Netgear Switch) (Config)#interface vlan 0/4/1
(Netgear Switch) (Interface 0/4/1)#routing
(Netgear Switch) (Interface 0/4/1)#ipv6 enable
(Netgear Switch) (Interface 0/4/1)#ipv6 address 2000::1/64
(Netgear Switch) (Interface 0/4/1)#exit
```

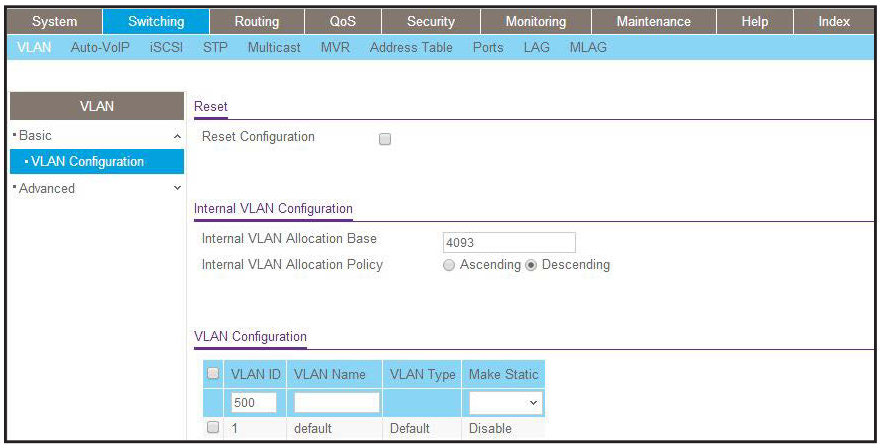
4. Enable IPV6 forwarding and unicast routing on the switch.

```
(Netgear Switch) (Config)#ipv6 forwarding
(Netgear Switch) (Config)#ipv6 unicast-routing
(Netgear Switch) #ping ipv6 2000::2
Send count=3, Receive count=3 from 2000::2
Average round trip time = 1.00 ms
(Netgear Switch) #show ipv6 brief
IPv6 Forwarding Mode..................... Enable
IPv6 Unicast Routing Mode................ Enable
IPv6 Hop Limit........................... 0
ICMPv6 Rate Limit Error Interval......... 1000 msec
ICMPv6 Rate Limit Burst Size............. 100 messages
Maximum Routes........................... 128
(Netgear Switch) #show ipv6 interface 0/4/1
IPv6 is enabled
IPv6 Prefix is .......................... FE80::21E:2AFF:FED9:249B/128
                                                  2000::1/64
Routing Mode............................. Enabled
Administrative Mode...................... Enabled
IPv6 Routing Operational Mode............ Enabled
Bandwidth................................ 10000  kbps
Interface Maximum Transmit Unit.......... 1500
Router Duplicate Address Detection Transmits... 1
Router Advertisement NS Interval......... 0
Router Advertisement Lifetime............ 1800
Router Advertisement Reachable Time...... 0
Router Advertisement Interval............ 600
Router Advertisement Managed Config Flag....... Disabled
Router Advertisement Other Config Flag......... Disabled
Router Advertisement Suppress Flag............. Disabled
IPv6 Destination Unreachables............ Enabled
Prefix 2000::1/64
Preferred Lifetime....................... 604800
Valid Lifetime........................... 2592000
Onlink Flag.............................. Enabled
Autonomous Flag.......................... Enabled
```

Web Interface: Create an IPv6 VLAN Routing Interface

1. Create VLAN 500.
   a. Select **Switching > VLAN > Basic > VLAN Configuration**.

      A screen similar to the following displays.

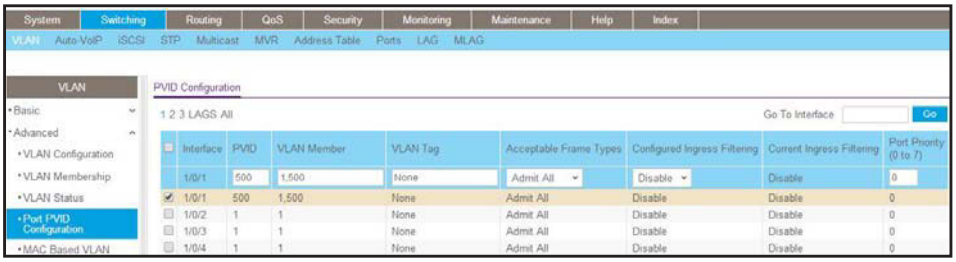


   b. In the **VLAN ID** field, enter **500**.
   c. In the **VLAN Type** field, select **Static**.
   d. Click **Add**.
2. Add ports to VLAN 500.
   a. Select **Switching > VLAN > Advanced > VLAN Membership**.

      A screen similar to the following displays.

   b. In the **VLAN ID** list, select **500**.
   c. Click **Unit 1**. The ports display.
   d. Click the gray box under port **1** until **U** displays, indicating that the egress packet is untagged for the port.
   e. Click **Apply**.
3. Specify the PVID on port 1/0/1.
   a. Select **Switching > VLAN > Advanced > Port PVID Configuration**.

A screen similar to the following displays.



b. Under PVID Configuration, scroll down and select the Interface **1/0/1** check box.

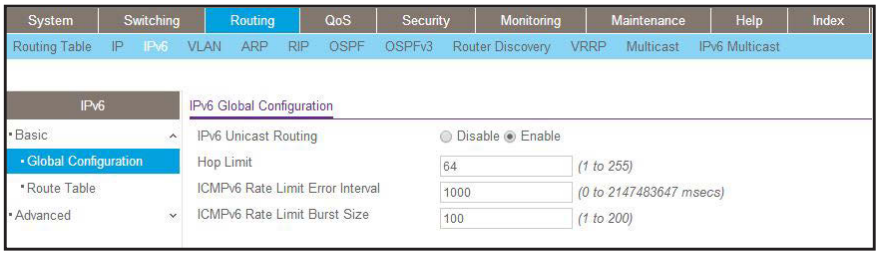
c. In the **PVID (1 to 4093)** field, enter **500**.

d. Click **Apply** to save the settings.

4. Enable IPv6 forwarding and unicast routing on the switch.

a. Select **Routing > IPv6 > Basic > Global Configuration**.

A screen similar to the following displays.



b. For IPv6 Unicast Routing, select the **Enable** radio button.

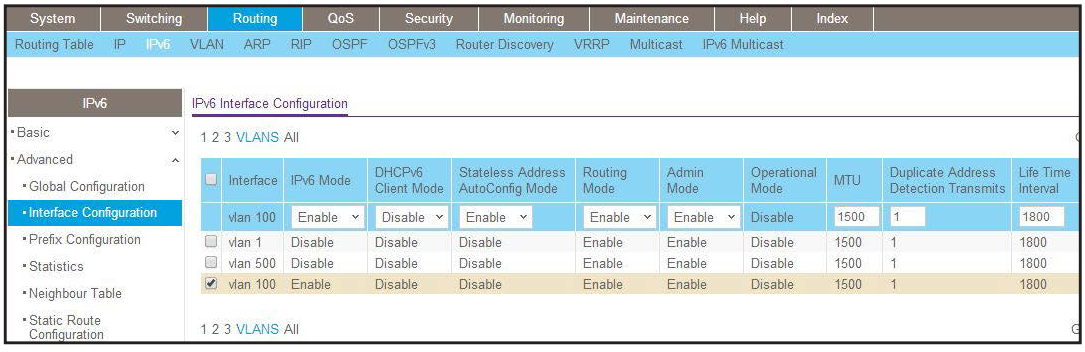
c. For IPv6 Forwarding, select the **Enable** radio button.

d. Click **Apply**.

5. Enable IPv6 routing on the VLAN.

a. Select **Routing > IPv6 > Advanced > Interface Configuration**.

A screen similar to the following displays.



b. Click VLANS. The logical VLAN interface 0/4/2 displays.

c. Select the **0/4/2** check box.

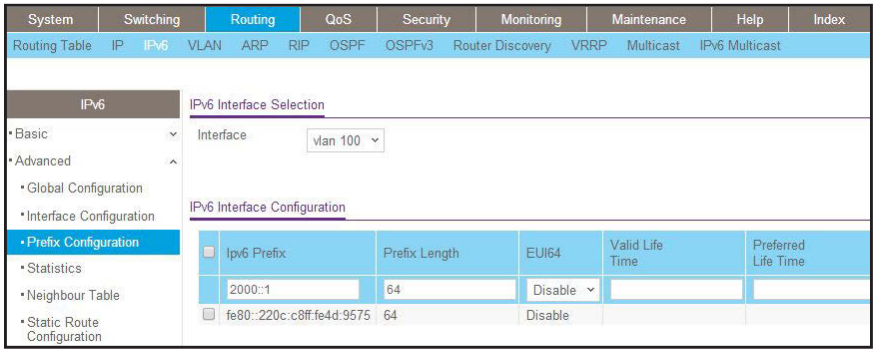
d. Under IPv6 Interface Configuration, in the **IPv6 Mode** field, select **Enable**.

e. Click **Apply**.

6. Assign an IPv6 address to the routing VLAN.

a. Select **Routing > IPv6 > Advanced > Prefix Configuration**.

A screen similar to the following displays.



b. In the **Interface** field, select **0/4/2**.

c. In the **IPv6 Prefix** field, enter **2000::1**.

d. In the **Length** field, enter **64**.

e. In the **EUI64** field, select **Disable**.

f. Click **Add**.

Configure DHCPv6 Mode on the Routing Interface

The routing interface supports DHCPv6 mode, which can get the IPv6 address from a DHCPv6 server (address allocation).

Note: Before you enable DHCPv6 mode, you must disable IPv6 unicast mode globally.

CLI: Configure DHCPv6 mode on routing interface

1. Enable IPv6 unicast globally.

```
(Netgear Switch) (Config)#ipv6 unicast-routing
```

2. Enable DHCPv6 on the interface 1/0/23.

```
(Netgear Switch) (Config)#interface 1/0/23
(Netgear Switch) (Interface 1/0/23)#routing
(Netgear Switch) (Interface 1/0/23)#ipv6 enable
(Netgear Switch) (Interface 1/0/23)#ipv6 address dhcp
(Netgear Switch) (Interface 1/0/23)
```

3. Show the ipv6 address assigned from 1/0/23.

```
(Netgear Switch) #show ipv6 interface 1/0/23
IPv6 is enabled
IPv6 Prefix is ............................... FE80::E291:F5FF:FE06:2BF6/128
                                               2000::1D5C:7CFE:828F:8144/128 [DHCP]
Routing Mode.................................. Enabled
IPv6 Enable Mode.............................. Enabled
Administrative Mode........................... Enabled
IPv6 Operational Mode......................... Enabled
Bandwidth..................................... 1000000  kbps
Interface Maximum Transmit Unit............... 1500
Router Duplicate Address Detection Transmits... 1
Address DHCP Mode............................. Enabled
Router Advertisement NS Interval.............. 0
Router Advertisement Lifetime................. 1800
Router Advertisement Reachable Time........... 0
Router Advertisement Interval................. 600
Router Advertisement Managed Config Flag...... Disabled
Router Advertisement Other Config Flag........ Disabled
Router Advertisement Router Preference........ medium
Router Advertisement Suppress Flag............ Disabled
IPv6 Destination Unreachables................. Enabled
```

Web Interface: Configure DHCPv6 mode on routing interface

1. Enable IPv6 unicast globally.
   a. Select **Routing > IPv6 > Basic > Global Configuration**.

A screen similar to the following displays.

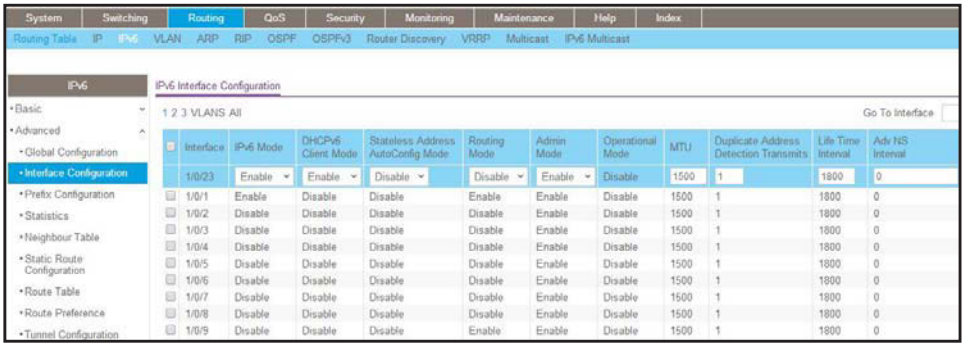
b. For IPv6 Unicast Routing, select the **Enable** radio button.

c. Click **Apply** to apply the setting.

2. Enable DHCPv6 on the interface 1/0/23.

a. Select **Routing > IPv6 > Advanced > Interface Configuration**.

A screen similar to the following displays.



b. Scroll down and select the **interface 1/0/23** check box.

Now 1/0/23 appears in the Interface field at the top.

c. Enter the following information:

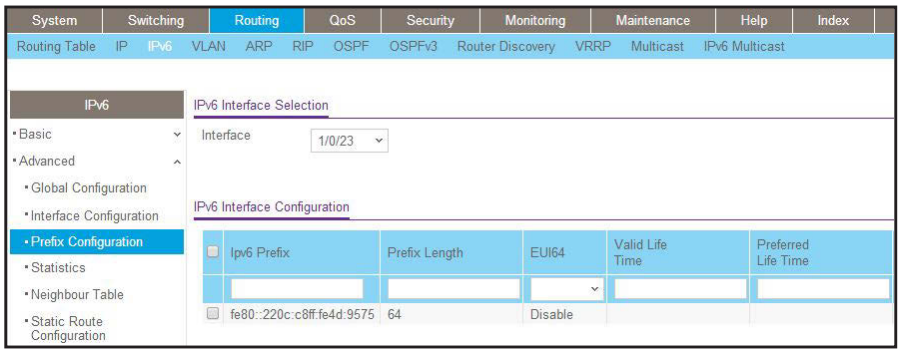
- In the IPv6 Mode field, select **Enable**.
- In the Routing Mode field, select **Enable**.
- In the DHCPv6 Client Mode field, select **Enable**.

d. Click **Apply** to apply the settings.

3. Show the ipv6 address assigned from 1/0/23.

a. Select **Routing > IPv6 > Advanced > Prefix Configuration**.

A screen similar to the following displays.



b. Scroll down and select the i**nterface 1/0/23**. You can see the IPv6 address assigned by the DHCPv6 server.

PIM

30

Protocol Independent Multicast

This chapter includes the following sections:

- *Protocol Independent Multicast Concepts*
- *PIM-DM*
- *PIM-SM*

Note: PIM is available on the M4300 series switches only.

Protocol Independent Multicast Concepts

The PIM protocol can be configured to operate on IPv4 and IPv6 networks. Separate CLI commands are provided for IPv4 and IPv6 operation; however, most configuration options are common to both protocols. Therefore, this section describes only IPv4 configuration; IPv6 configuration is similar to IPv4.

Multicast protocols are used to deliver multicast packets from one source to multiple receivers. They facilitate better bandwidth utilization, and use less host and router processing, making them ideal for usage in applications such as video and audio conferencing, whiteboard tools, and stock distribution tickers. PIM is a widely used multicast routing protocol. Protocol Independent Multicast (PIM) is a standard multicast routing protocol that provides scalable inter-domain multicast routing across the Internet, independent of the mechanisms provided by any particular unicast routing protocol. There are two types of PIM:

- PIM-Dense Mode (PIM-DM)
- PIM-Sparse Mode (PIM-SM)

PIM-DM

PIM-DM is appropriate for:

- Densely distributed receivers
- A ratio of few senders to many receivers (due to frequent flooding)
- High volume of multicast traffic
- Constant stream of traffic

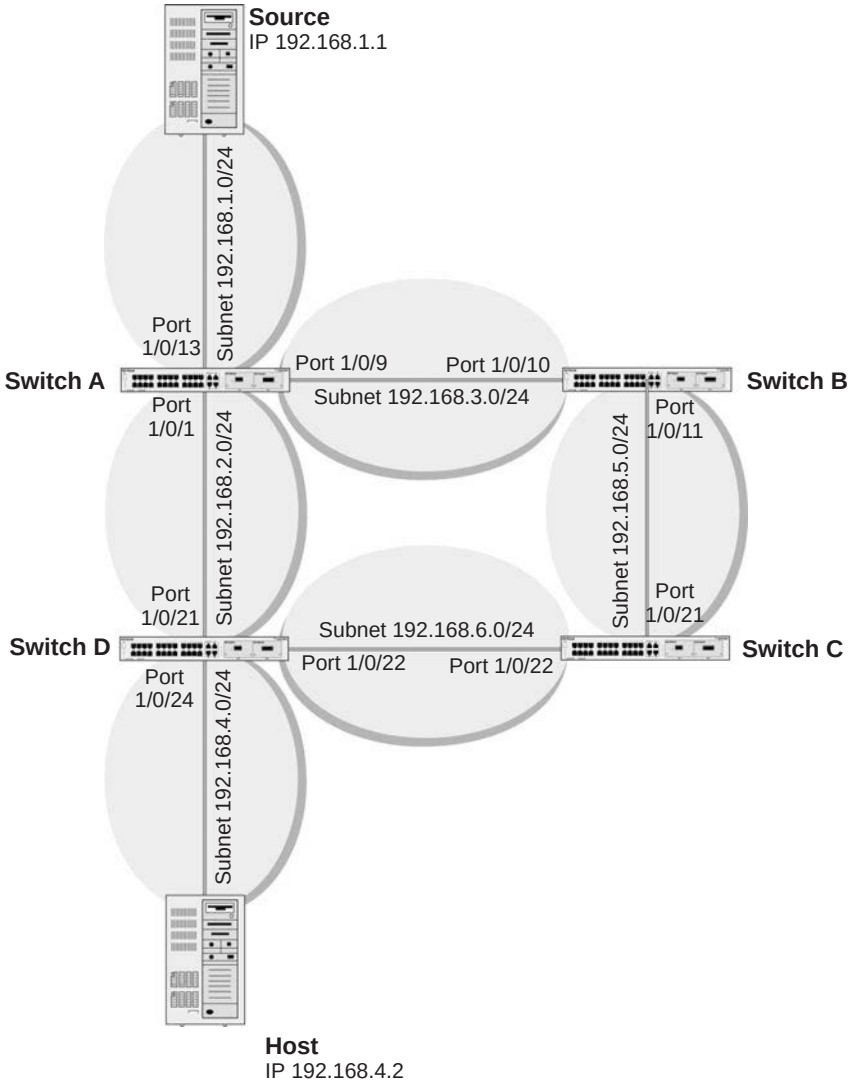


Figure 57. Configuring and Using PIM-DM

PIM-DM uses the existing unicast routing table and join, prune, and graft mechanism to build a tree. PIM-DM creates source-based shortest-path distribution trees that use reverse path forwarding (RPF). PIM-DM cannot be used to build a shared distribution tree, as PIM-SM can. PIM-DM assumes that when a sender starts sending data, all downstream routers and hosts want to receive a multicast datagram. PIM-DM initially floods multicast traffic throughout the network. Routers that do not have any downstream neighbors prune back the unwanted traffic. Apart from prune messages, PIM-DM uses two other types of messages: graft messages and assert messages. Graft messages are used whenever a new host wants to join the group. Assert messages are used to shut off duplicate flows onto the same multi-access network.

To minimize the repeated flooding of datagrams and subsequent pruning associated with a particular (S,G) pair, PIM-DM uses a state refresh message. This message is sent by the routers directly connected to the source and is propagated throughout the network. When

received by a router on its RPF interface, the state refresh message causes an existing prune state to be refreshed. State refresh messages are generated periodically by the router directly attached to the source. There are two versions of PIM-DM. Version 2 does not use IGMP messages; instead, it uses a message that is encapsulated in IP packets with protocol number 103. In version 2, the Hello message is introduced in place of the query message.

CLI: Configure PIM-DM

PIM-DM on Switch A

1. Enable IP routing on the switch.

```
(Netgear Switch) #configure
(Netgear Switch) (Config)#ip routing
```

2. Enable pimdm on the switch.

```
(Netgear Switch) (Config)#ip pim dense
```

3. Enable IP multicast forwarding on the switch.

```
(Netgear Switch) (Config)#ip multicast
```

4. Enable RIP to build the unicast IP routing table.

```
(Netgear Switch) (Config)#interface 1/0/1
(Netgear Switch) (Interface 1/0/1)#routing
(Netgear Switch) (Interface 1/0/1)#ip address 192.168.2.2  255.255.255.0
(Netgear Switch) (Interface 1/0/1)#ip rip
```

5. Enable PIM-DM on the interface.

```
(Netgear Switch) (Interface 1/0/1)#ip pim
(Netgear Switch) (Interface 1/0/1)#exit

(Netgear Switch) (Config)#interface 1/0/9
(Netgear Switch) (Interface 1/0/9)#routing
(Netgear Switch) (Interface 1/0/9)#ip address  192.168.3.1  255.255.255.0
(Netgear Switch) (Interface 1/0/9)#ip rip
(Netgear Switch) (Interface 1/0/9)#ip pim
(Netgear Switch) (Interface 1/0/9)#exit

(Netgear Switch) (Config)#interface 1/0/13
(Netgear Switch) (Interface 1/0/13)#routing
(Netgear Switch) (Interface 1/0/13)#ip address  192.168.1.2  255.255.255.0
(Netgear Switch) (Interface 1/0/13)#ip rip
(Netgear Switch) (Interface 1/0/13)#ip pim
(Netgear Switch) (Interface 1/0/13)#exit
```

PIM-DM on Switch B

```
(Netgear Switch) #configure
(Netgear Switch) (Config)#ip routing
(Netgear Switch) (Config)#ip pim
(Netgear Switch) (Config)#ip multicast
(Netgear Switch) (Config)#interface 1/0/10
(Netgear Switch) (Interface 1/0/10)#routing
(Netgear Switch) (Interface 1/0/10)#ip address 192.168.3.2  255.255.255.0
(Netgear Switch) (Interface 1/0/10)#ip rip
(Netgear Switch) (Interface 1/0/10)#ip pim
(Netgear Switch) (Interface 1/0/10)#exit
(Netgear Switch) (Config)#interface 1/0/11
(Netgear Switch) (Interface 1/0/11)#routing
(Netgear Switch) (Interface 1/0/11)#ip address 192.168.5.1  255.255.255.0
(Netgear Switch) (Interface 1/0/11)#ip rip
(Netgear Switch) (Interface 1/0/11)#ip pim
(Netgear Switch) (Interface 1/0/11)#exit
```

PIM-DM on Switch C

```
(Netgear Switch) #configure
(Netgear Switch) (Config)#ip routing
(Netgear Switch) (Config)#ip pim dense
(Netgear Switch) (Config)#ip multicast
(Netgear Switch) (Config)#interface 1/0/21
(Netgear Switch) (Interface 1/0/21)#routing
(Netgear Switch) (Interface 1/0/21)#ip address 192.168.5.2  255.255.255.0
(Netgear Switch) (Interface 1/0/21)#ip rip
(Netgear Switch) (Interface 1/0/21)#ip pim
(Netgear Switch) (Interface 1/0/21)#exit
(Netgear Switch) (Config)#interface 1/0/22
(Netgear Switch) (Interface 1/0/22)#routing
(Netgear Switch) (Interface 1/0/22)#ip address 192.168.6.1  255.255.255.0
(Netgear Switch) (Interface 1/0/22)#ip rip
(Netgear Switch) (Interface 1/0/22)#ip pim
(Netgear Switch) (Interface 1/0/22)#exit
```

PIM-DM on Switch D

1. Enable IGMP on the switch.

```
(Netgear Switch) #configure
(Netgear Switch) (Config)#ip routing
(Netgear Switch) (Config)#ip pim dense
(Netgear Switch) (Config)#ip igmp
```

```
(Netgear Switch) (Config)#ip multicast
(Netgear Switch) (Config)#interface 1/0/21
(Netgear Switch) (Interface 1/0/21)#routing
(Netgear Switch) (Interface 1/0/21)#ip address 192.168.2.1  255.255.255.0
(Netgear Switch) (Interface 1/0/21)#ip rip
(Netgear Switch) (Interface 1/0/21)#ip pim
(Netgear Switch) (Interface 1/0/21)#exit

(Netgear Switch) (Config)#interface 1/0/22
(Netgear Switch) (Interface 1/0/22)#routing
(Netgear Switch) (Interface 1/0/22)#ip address 192.168.6.2  255.255.255.0
(Netgear Switch) (Interface 1/0/22)#ip rip
(Netgear Switch) (Interface 1/0/22)#ip pim
(Netgear Switch) (Interface 1/0/22)#exit
```

2. Enable IGMP on port 1/0/24.

```
(Netgear Switch) (Config)#interface 1/0/24
(Netgear Switch) (Interface 1/0/24)#routing
(Netgear Switch) (Interface 1/0/24)#ip pim
(Netgear Switch) (Interface 1/0/24)#ip igmp
(Netgear Switch) (Interface 1/0/24)#ip rip
(Netgear Switch) (Interface 1/0/24)#ip address 192.168.4.1  255.255.255.0
(Netgear Switch) (Interface 1/0/24)#exit
```

3. PIM-DM builds the multicast routes table on each switch.

```
(A) #show ip mcast mroute summary
                  Multicast Route Table Summary
                                        Incoming      Outgoing
Source IP     Group IP     Protocol     Interface     Interface List
-----------   ----------   ----------   ---------    ---------------
192.168.1.1   225.1.1.1    PIMDM         1/0/13       1/0/1

(B) #show ip mcast mroute summary
                  Multicast Route Table Summary
                                        Incoming       Outgoing
Source IP     Group IP     Protocol     Interface      Interface List
-----------   ---------    ----------   ---------     ---------------
192.168.1.1   225.1.1.1    PIMDM        1/0/10
(C) #show ip mcast mroute summary
                  Multicast Route Table Summary
                                        Incoming       Outgoing
Source IP     Group IP     Protocol     Interface      Interface List
-----------   ---------    --------     ---------     ---------------
192.168.1.1   225.1.1.1    PIMDM        1/0/21

(D) #show ip mcast mroute summary
                  Multicast Route Table Summary
                                        Incoming        Outgoing
Source IP    Group IP       Protocol    Interface       Interface List
----------   ---------      --------    ----------      ---------------
192.168.1.1  225.1.1.1      PIMDM       7/0/21           7/0/24
```

Web Interface: Configure PIM-DM

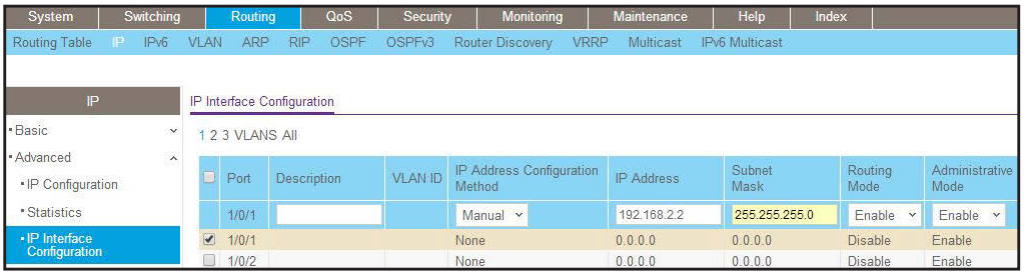
PIM-DM on Switch A

1. Enable IP routing on the switch.
   a. Select **Routing > IP > Basic > IP Configuration**.

      A screen similar to the following displays.

   b. For Routing Mode, select the **Enable** radio button.
   c. Click **Apply**.
2. Configure 1/0/1 as a routing port and assign an IP address to it.
   a. Select **Routing > IP > Advanced > IP Interface Configuration**.

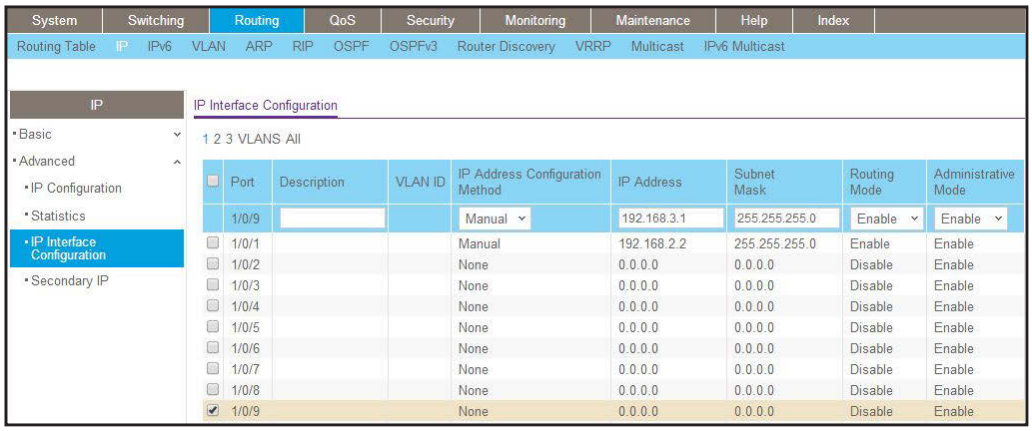
      A screen similar to the following displays.



   b. Under IP Interface Configuration, scroll down and select the Port **1/0/1** check box.

      Now 1/0/1 appears in the Port field at the top.
   c. Enter the following information:
      - In the **IP Address** field, enter **192.168.2.2**.
      - In the **Subnet Mask** field, enter **255.255.255.0**.
      - In the **Routing Mode** field, select **Enable**.
   d. Click **Apply** to save the settings.
3. Configure 1/0/9 as a routing port and assign an IP address to it.
   a. Select **Routing > IP > Advanced > IP Interface Configuration**.

A screen similar to the following displays.



b. Scroll down and select the Port **1/0/9** check box.

Now 1/0/9 appears in the Port field at the top.

c. Enter the following information:

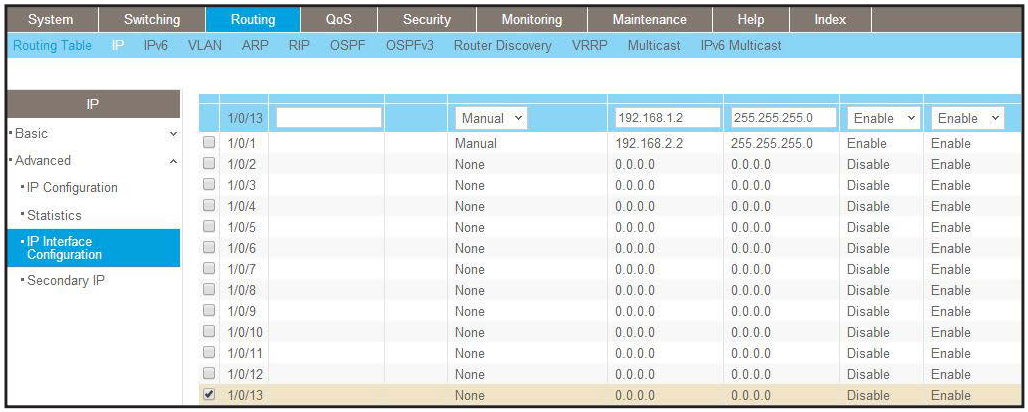
- In the **IP Address** field, enter **192.168.3.1**.
- In the **Subnet Mask** field, enter **255.255.255.0**.
- In the **Routing Mode** field, select **Enable**.

d. Click **Apply**.

4. Configure 1/0/13 as a routing port and assign an IP address to it.

a. Select **Routing > IP > Advanced > IP Interface Configuration**.

A screen similar to the following displays.



b. Under IP Interface Configuration, scroll down and select the Port **1/0/13** check box.

Now 1/0/13 appears in the Port field at the top.

c. Enter the following information:

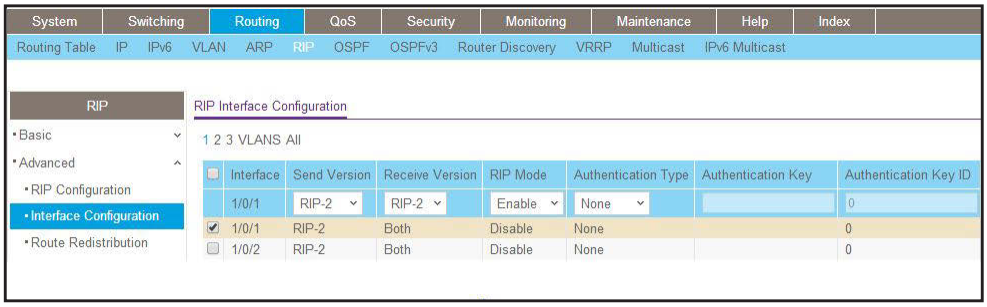
- In the **IP Address** field, enter **192.168.1.2**.
- In the **Subnet Mask** field, enter **255.255.255.0**.
- In the **Routing Mode** field, select **Enable**.

d. Click **Apply** to save the settings.

5. Enable RIP on the interface 1/0/1.

a. Select **Routing > RIP > Advanced > Interface Configuration**.

A screen similar to the following displays.



b. In the **Interface** list, select **1/0/1**.

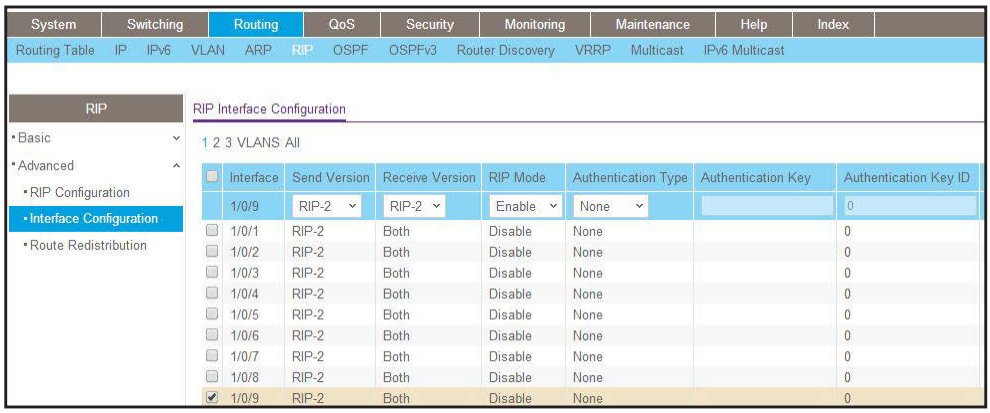
c. For RIP Admin Mode, select the **Enable** radio button.

d. Click **Apply**.

6. Enable RIP on interface 1/0/9.

a. Select **Routing > RIP > Advanced > Interface Configuration**.

A screen similar to the following displays.



b. In the **Interface** field, select **1/0/9**.

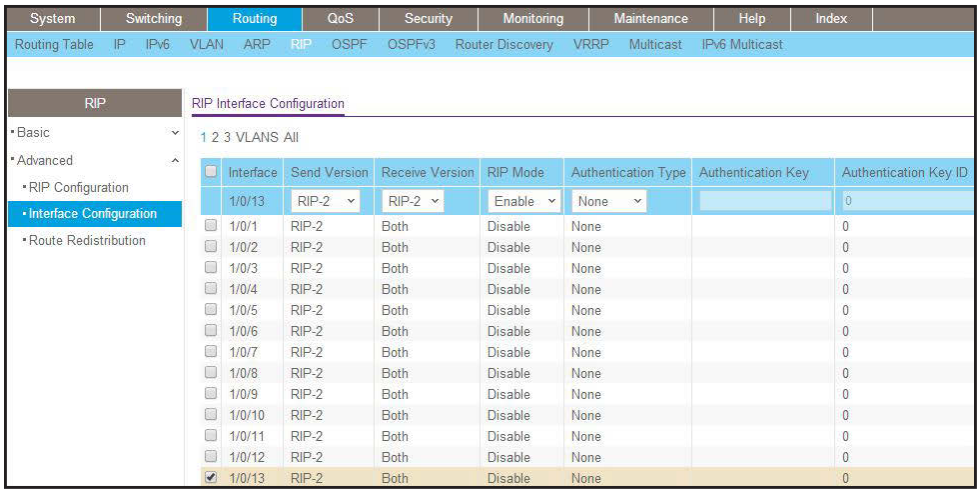
c. For RIP Admin Mode, select the **Enable** radio button.

d. Click **Apply**.

7. Enable RIP on interface 1/0/13.

a. Select **Routing > RIP > Advanced > Interface Configuration**.

A screen similar to the following displays.



b. In the **Interface** list, select **1/0/13**.

c. For RIP Admin Mode, select the **Enable** radio button.

d. Click **Apply**.

8. Enable multicast globally.

a. Select **Routing > Multicast > Global Configuration**.

A screen similar to the following displays.

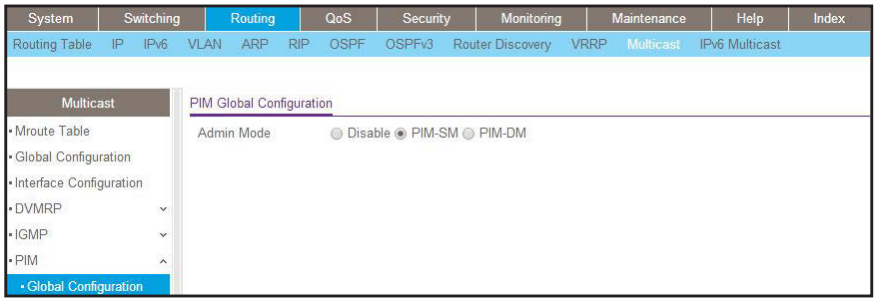
b. For Admin Mode, select the **Enable** radio button.

c. Click **Apply**.

9. Enable PIM-DM globally.

a. Select **Routing > Multicast > PIM > Global Configuration**.

A screen similar to the following displays.



b. For PIM Protocol Type, select the **PIM-DM** radio button.

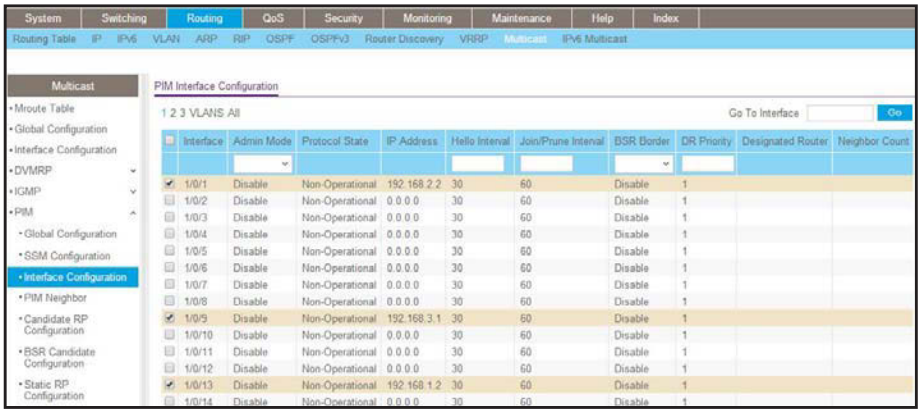
c. For Admin Mode, select the **Enable** radio button.

d. Click **Apply**.

10. Enable PIM-DM on interfaces 1/0/1,1/0/9, and 1/0/13.

a. Select **Routing > Multicast > PIM > Interface Configuration**.

A screen similar to the following displays.



b. Under PIM Interface Configuration, scroll down and select the **1/0/1**, **1/0/9**, and **1/0/13** check boxes.

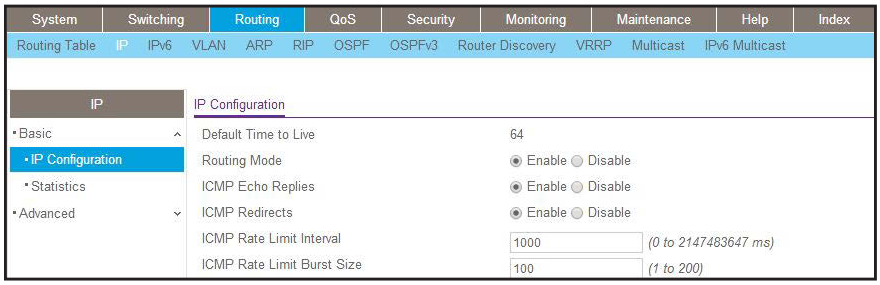
c. In the **Admin Mode** field, select **Enable**.

d. Click **Apply** to save the settings.

PIM-DM on Switch B:

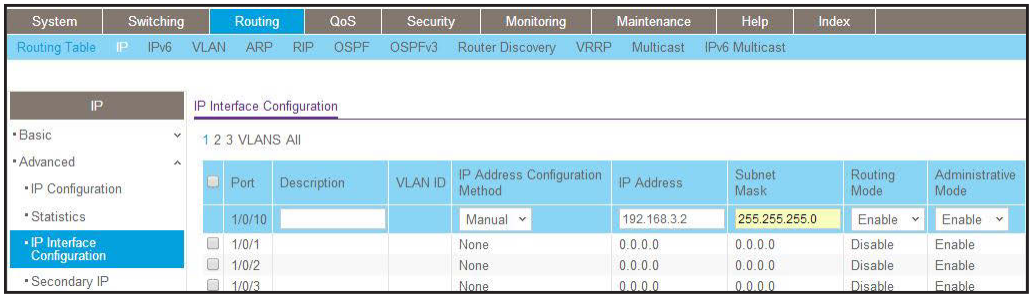
1. Enable IP routing on the switch.
   a. Select **Routing > IP > Basic > IP Configuration**.

      A screen similar to the following displays.



   b. For Routing Mode, select the **Enable** radio button.
   c. Click **Apply**.
2. Configure 1/0/10 as a routing port and assign an IP address to it.
   a. Select **Routing > IP > Advanced > IP Interface Configuration**.

      A screen similar to the following displays.

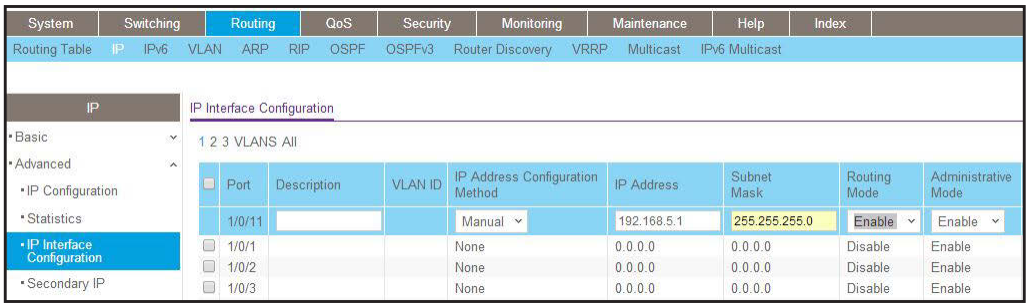


   b. Scroll down and select the Port **1/0/10** check box.

      Now 1/0/10 appears in the Port field at the top.

   c. Enter the following information:
      - In the **IP Address** field, enter **192.168.3.2**.
      - In the **Subnet Mask** field, enter **255.255.255.0**.
      - In the **Routing Mode** field, select **Enable**.
   d. Click **Apply** to save the settings.
3. Configure 1/0/11 as a routing port and assign an IP address to it.
   a. Select **Routing > IP > Advanced > IP Interface Configuration**.

A screen similar to the following displays.



b. Under IP Interface Configuration, scroll down and select the Port **1/0/11** check box.

Now 1/0/11 appears in the Port field at the top.

c. Enter the following information:

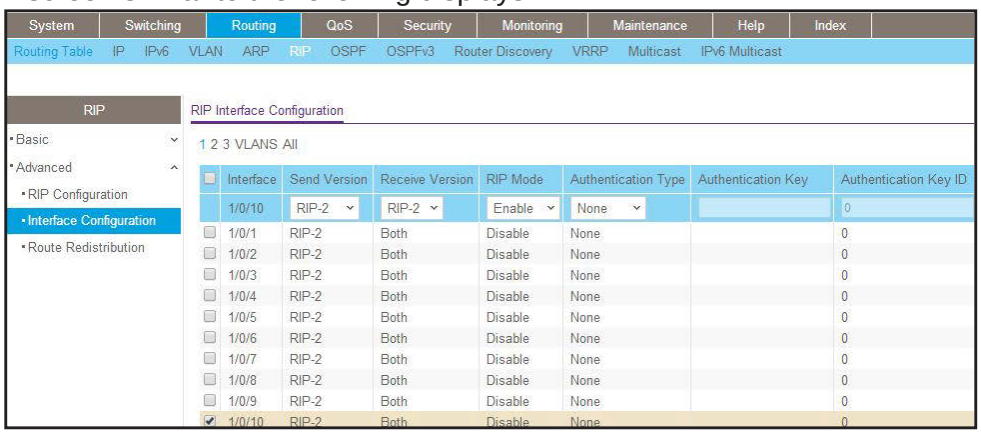
- In the **IP Address** field, enter **192.168.5.1**.
- In the **Subnet Mask** field, enter **255.255.255.0**.
- In the **Routing Mode** field, select **Enable**.

d. Click **Apply** to save the settings.

4. Enable RIP on interface 1/0/10.

a. Select **Routing >RIP > Advanced > Interface Configuration**.

A screen similar to the following displays.



b. In the **Interface** list, select **1/0/10**.

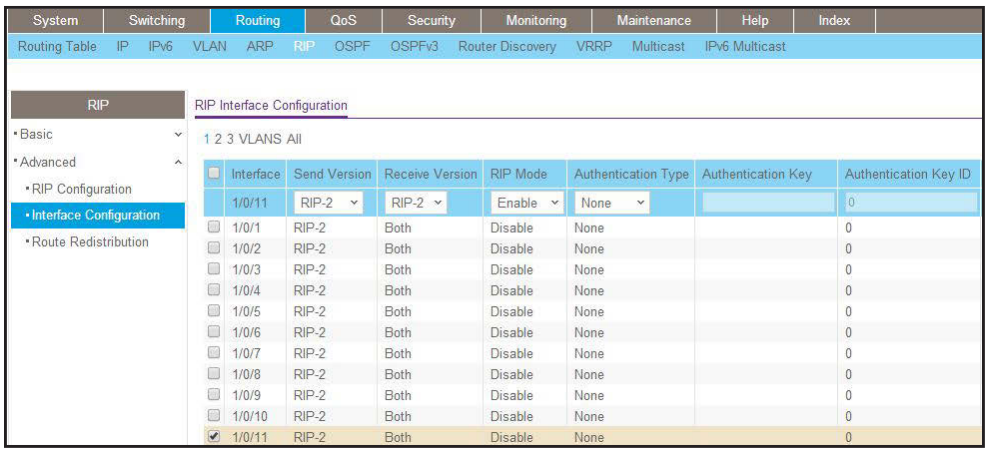
c. For RIP Admin Mode, select the **Enable** radio button.

d. Click **Apply**.

5. Enable RIP on interface 1/0/11.

a. Select **Routing > RIP > Advanced > Interface Configuration**.

A screen similar to the following displays.



b. In the **Interface** list, select **1/0/11**.

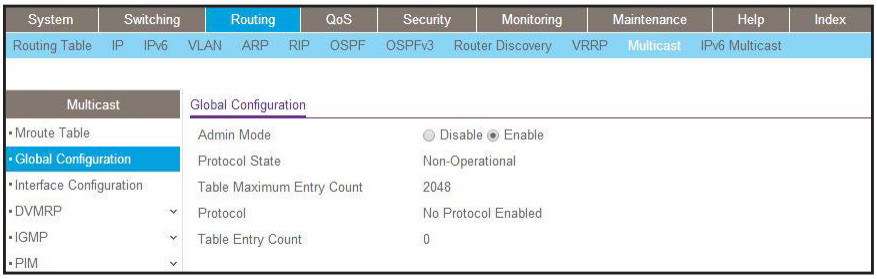
c. For RIP Admin Mode, select the **Enable** radio button.

d. Click **Apply**.

6. Enable multicast globally.

a. Select **Routing > Multicast > Global Configuration**.

A screen similar to the following displays.



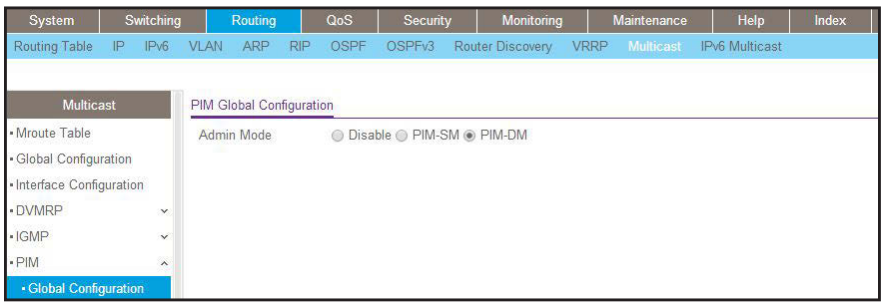
b. For Admin Mode, select the **Enable** radio button.

c. Click **Apply**.

7. Enable PIM-DM globally.

a. Select **Routing > Multicast > PIM > Global Configuration**.

A screen similar to the following displays.



b. For PIM Protocol Type, select the **PIM-DM** radio button.

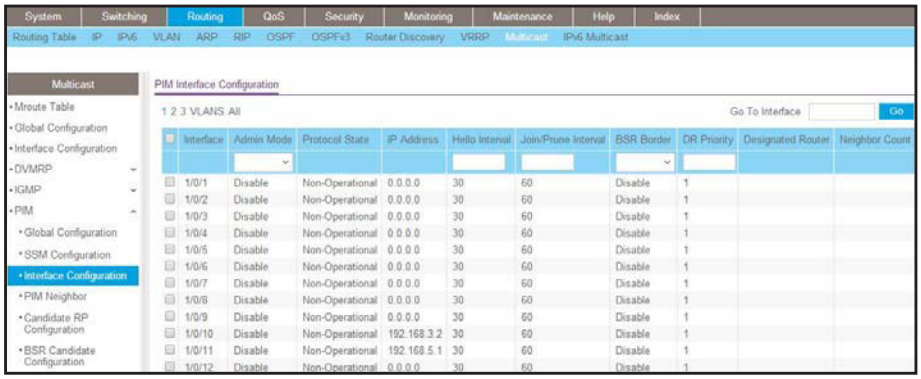
c. For Admin Mode, select the **Enable** radio button.

d. Click **Apply**.

8. Enable PIM-SM on interfaces 1/0/10 and 1/0/11.

a. Select **Routing > Multicast > PIM > Interface Configuration**.

A screen similar to the following displays.



b. Scroll down and select the Interface **1/0/10** and **1/0/11** check box.

c. In the **Admin Mode** field, select **Enable**.

d. Click **Apply** to save the settings.

PIM-DM on Switch C

1. Enable IP routing on the switch.

a. Select **Routing > IP > Basic > IP Configuration**.

A screen similar to the following displays.

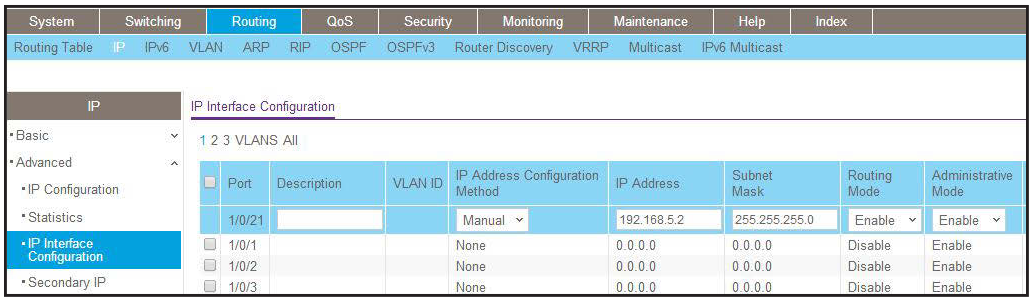
b. For Routing Mode, select the **Enable** radio button.

c. Click **Apply**.

2. Configure 1/0/21 as a routing port and assign an IP address to it.

a. Select **Routing > IP > Advanced > IP Interface Configuration**.

A screen similar to the following displays.



b. Scroll down select the Port **1/0/21** check box.

Now 1/0/21 appears in the Interface field at the top.

c. Enter the following information:

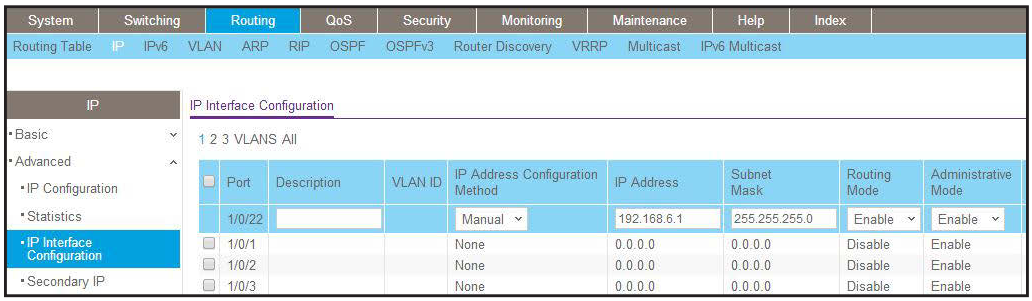
- In the **IP Address** field, enter **192.168.5.2**.
- In the **Subnet Mask** field, enter **255.255.255.0**.
- In the **Routing Mode** field, select **Enable**.

d. Click **Apply** to save the settings.

3. Configure 1/0/22 as a routing port and assign an IP address to it.

a. Select **Routing > IP > Advanced > IP Interface Configuration**.

A screen similar to the following displays.



b. Scroll down and select the Port **1/0/22** check box.

Now 1/0/22 appears in the Port field at the top.

c. Enter the following information:

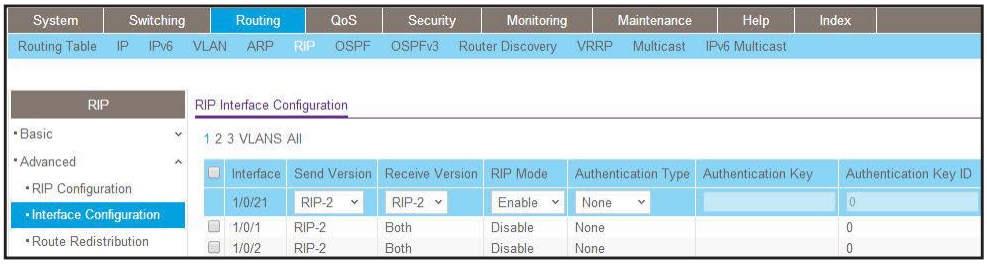
- In the **IP Address** field, enter **192.168.6.1**.
- In the **Subnet Mask** field, enter **255.255.255.0**.
- In the **Routing Mode** field, select **Enable**.

d. Click **Apply** to save the settings.

4. Enable RIP on interface 1/0/21.

a. Select **Routing > RIP > Advanced > Interface Configuration**.

A screen similar to the following displays.



b. In the **Interface** list, select **1/0/21**.

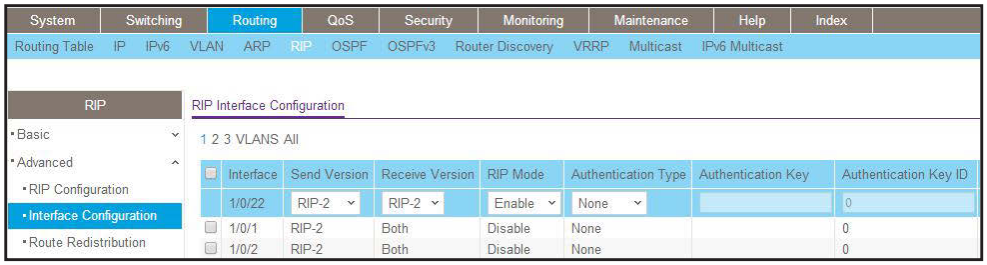
c. For RIP Admin Mode, select the **Enable** radio button.

d. Click **Apply**.

5. Enable RIP on interface 1/0/22.

a. Select **Routing > RIP > Advanced > Interface Configuration**.

A screen similar to the following displays.



b. In the **Interface** list, select **1/0/22**.

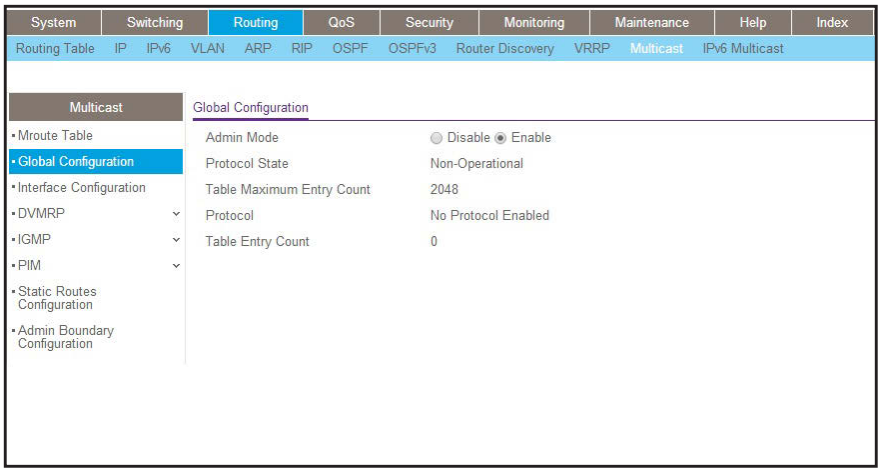
c. For RIP Admin Mode, select the **Enable** radio button.

d. Click **Apply**.

6. Enable mulicast globally.

a. Select **Routing > Multicast > Global Configuration**.

A screen similar to the following displays.



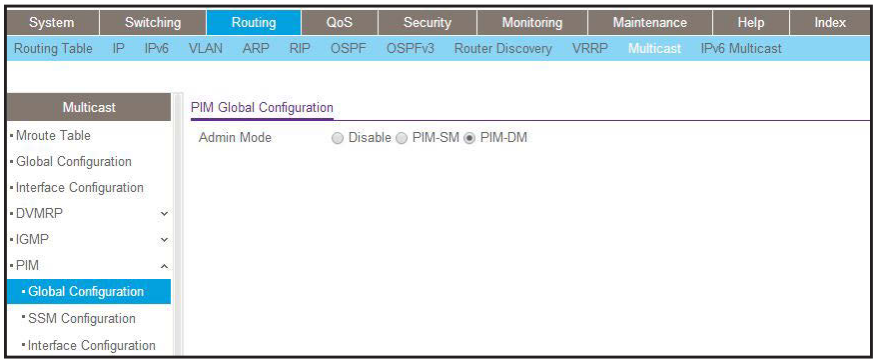
b. For Admin Mode, select the **Enable** radio button.

c. Click **Apply**.

7. Enable PIM-DM globally.

a. Select **Routing > Multicast > PIM > Global Configuration**.

A screen similar to the following displays.



b. For PIM Protocol Type, select the **PIM-DM** radio button.

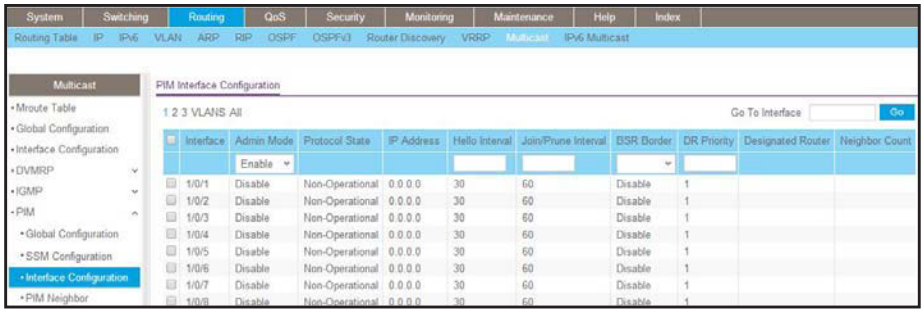
c. For Admin Mode, select the **Enable** radio button.

d. Click **Apply**.

8. Enable PIM-DM on interfaces 1/0/21 and 1/0/22.

a. Select **Routing > Multicast > PIM > Interface Configuration**.

A screen similar to the following displays.



b. Scroll down and select the **1/0/21** and **1/0/22** check boxes.

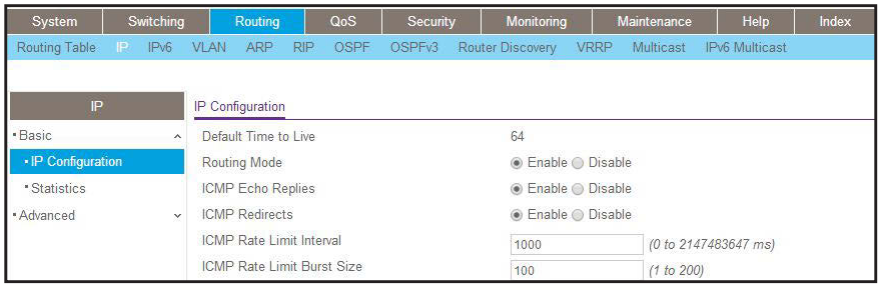
c. In the PIM Interface Configuration, in the **Admin Mode** field, select **Enable**.

d. Click **Apply** to save the settings.

PIM-DM on Switch D:

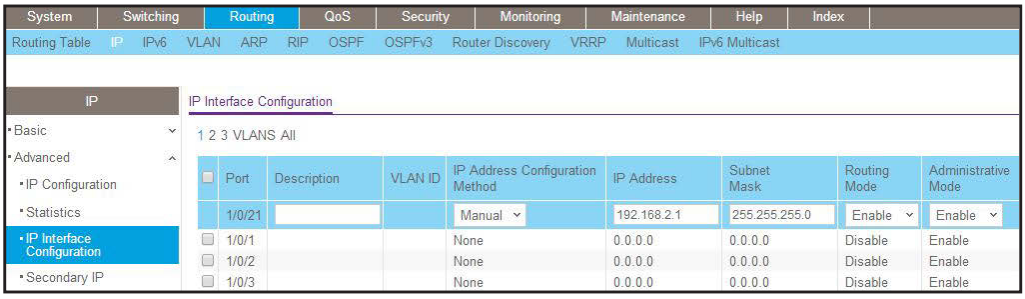
1. Enable IP routing on the switch.
   a. Select **Routing > IP > Basic > IP Configuration**.

      A screen similar to the following displays.



   b. For Routing Mode, select the **Enable** radio button.
   c. Click **Apply**.
2. Configure 1/0/21 as a routing port and assign an IP address to it.
   a. Select **Routing > IP > Advanced > IP Interface Configuration**.

      A screen similar to the following displays.



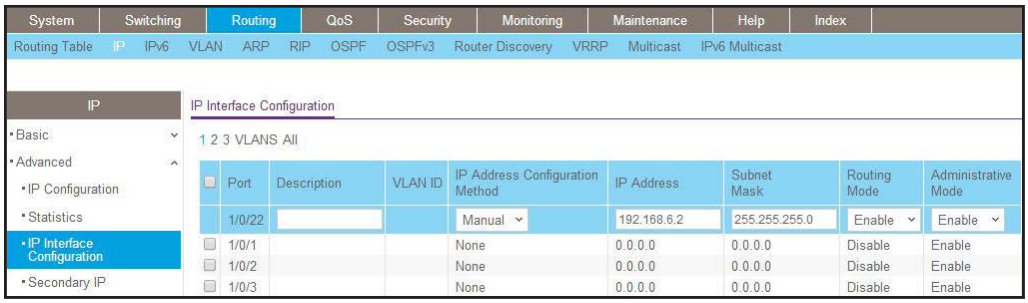
   b. Scroll down and select the Port **1/0/21** check box.

      Now 1/0/21 appears in the Port field at the top.

   c. Enter the following information in the IP Interface Configuration.
      - In the **IP Address** field, enter **192.168.2.1**.
      - In the **Subnet Mask** field, enter **255.255.255.0**.
      - In the **Routing Mode** field, select **Enable**.

   d. Click **Apply** to save the settings.
3. Configure 1/0/22 as a routing port and assign an IP address to it.
   a. Select **Routing > IP > Advanced > IP Interface Configuration**.

A screen similar to the following displays.



b. Scroll down and select the Port **1/0/22** check box.

Now 1/0/22 appears in the Interface field at the top.

c. Enter the following information:

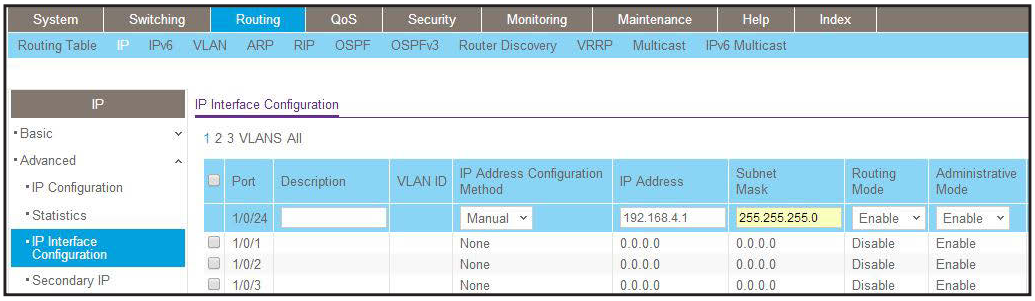
- In the **IP Address** field, enter **192.168.6.2**.
- In the **Subnet Mask** field, enter **255.255.255.0**.
- In the **Routing Mode** field, select **Enable**.

d. Click **Apply** to save the settings.

4. Configure 1/0/24 as a routing port and assign an IP address to it.

a. Select **Routing > IP > Advanced > IP Interface Configuration**.

A screen similar to the following displays.



b. Scroll down and select the Port **1/0/24** check box.

Now 1/0/24 appears in the Interface field at the top.

c. Enter the following information:

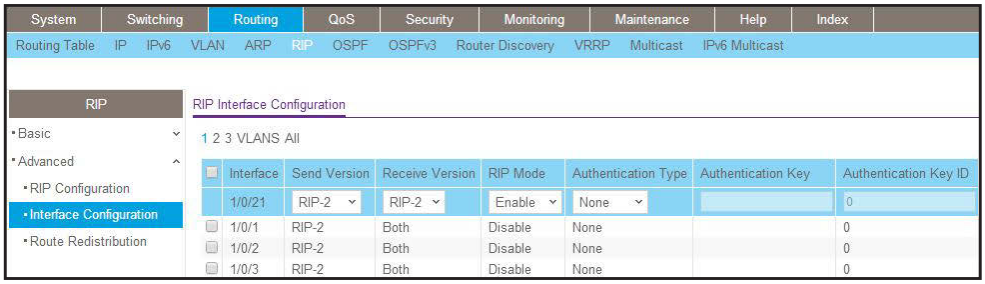
- In the **IP Address** field, enter **192.168.4.1**.
- In the **Subnet Mask** field, enter **255.255.255.0**.
- In the **Routing Mode** field, select **Enable**.

d. Click **Apply** to save the settings.

5. Enable RIP on interface 1/0/21.

a. Select **Routing > RIP > Advanced > Interface Configuration**.

A screen similar to the following displays.



b. In the **Interface** list, select t **1/0/21**.

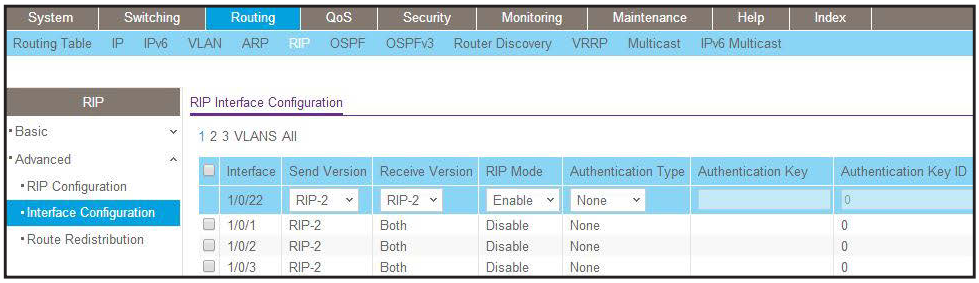
c. For RIP Admin Mode, select the **Enable** radio button.

d. Click **Apply**.

6. Enable RIP on interface 1/0/22.

a. Select **Routing > RIP > Advanced > Interface Configuration**.

A screen similar to the following displays.



b. In the **Interface** list, select **1/0/22**.

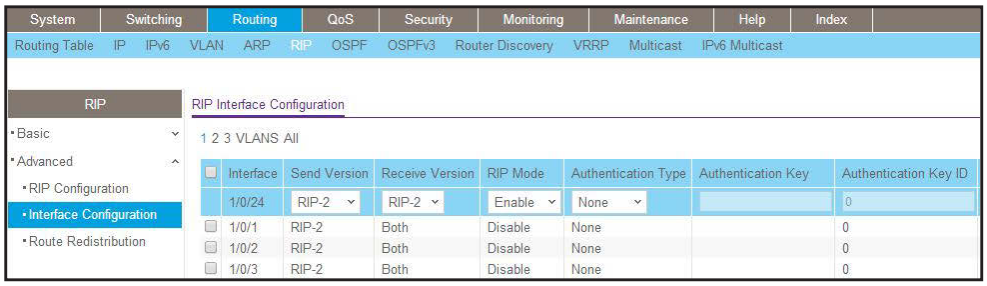
c. For RIP Admin Mode, select the **Enable** radio button.

d. Click **Apply**.

7. Enable RIP on interface 1/0/24.

a. Select **Routing > RIP > Advanced > Interface Configuration**.

A screen similar to the following displays.



b. In the **Interface** list, select **1/0/24**.

c. For RIP Admin Mode, select the **Enable** radio button.

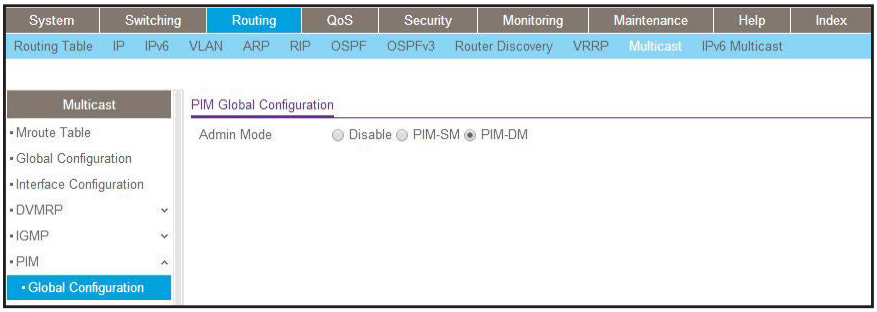
d. Click **Apply**.

8. Enable multicast globally.
   a. Select **Routing > Multicast > Global Configuration**.

      A screen similar to the following displays.

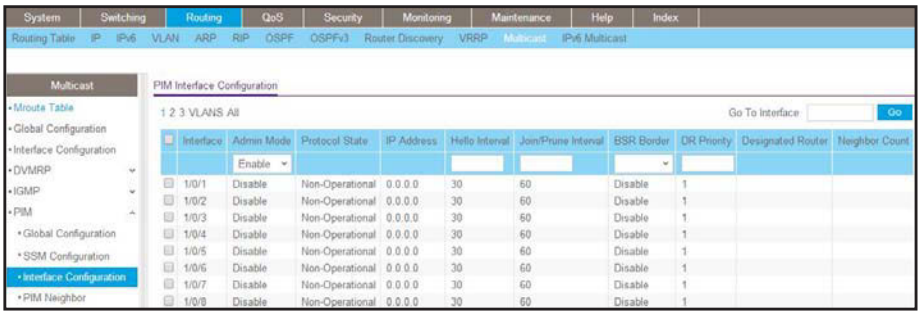
   b. For Admin Mode, select the **Enable** radio button.
   c. Click **Apply**.
9. Enable PIM-DM globally.
   a. Select **Routing > Multicast > PIM > Global Configuration**.

      A screen similar to the following displays.



   b. For PIM Protocol Type, select the **PIM-SM** radio button.
   c. For Admin Mode, select the **Enable** radio button.
   d. Click **Apply**.
10. Enable PIM-DM on interfaces 1/0/21,1/0/22, and 1/0/24.
   a. Select **Routing > Multicast > PIM > Interface Configuration**.

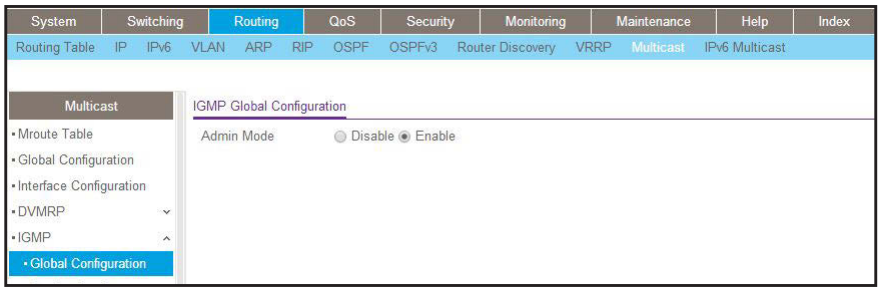
      A screen similar to the following displays.



b. Scroll down and select the Interface **1/0/21**, **1/0/22**, and **1/0/24** check boxes.
c. In the **Admin Mode** field, select **Enable**.
d. Click **Apply** to save the settings.

11. Enable IGMP globally.
    a. Select **Routing > Multicast > IGMP > Global Configuration**.

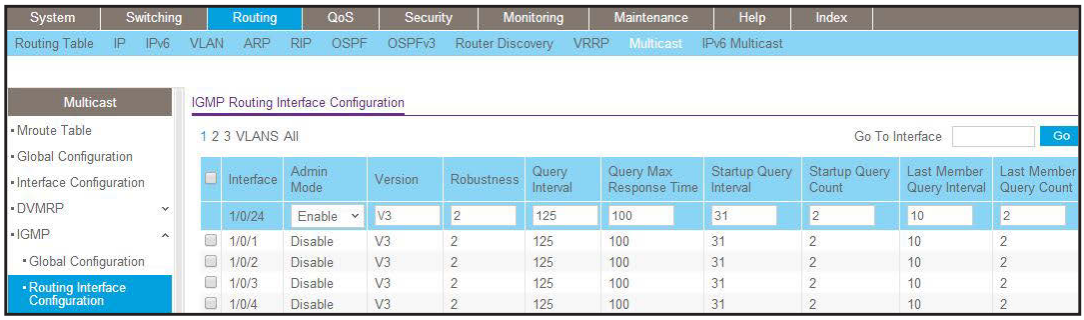
       A screen similar to the following displays.



    b. For Admin Mode, select the **Enable** radio button.
    c. Click **Apply**.

12. Enable IGMP on interface 1/0/24.
    a. Select **Routing > Multicast > IGMP > Interface Configuration**.

       A screen similar to the following displays.



    b. Scroll down and select the interface **1/0/24** check box.
    c. In the **Admin Mode** field, select **Enable**.
    d. Click **Apply** to save the settings.

PIM-SM

Protocol-independent multicast sparse mode (PIM-SM) is used to efficiently route multicast traffic to multicast groups that can span wide area networks where bandwidth is a constraint.

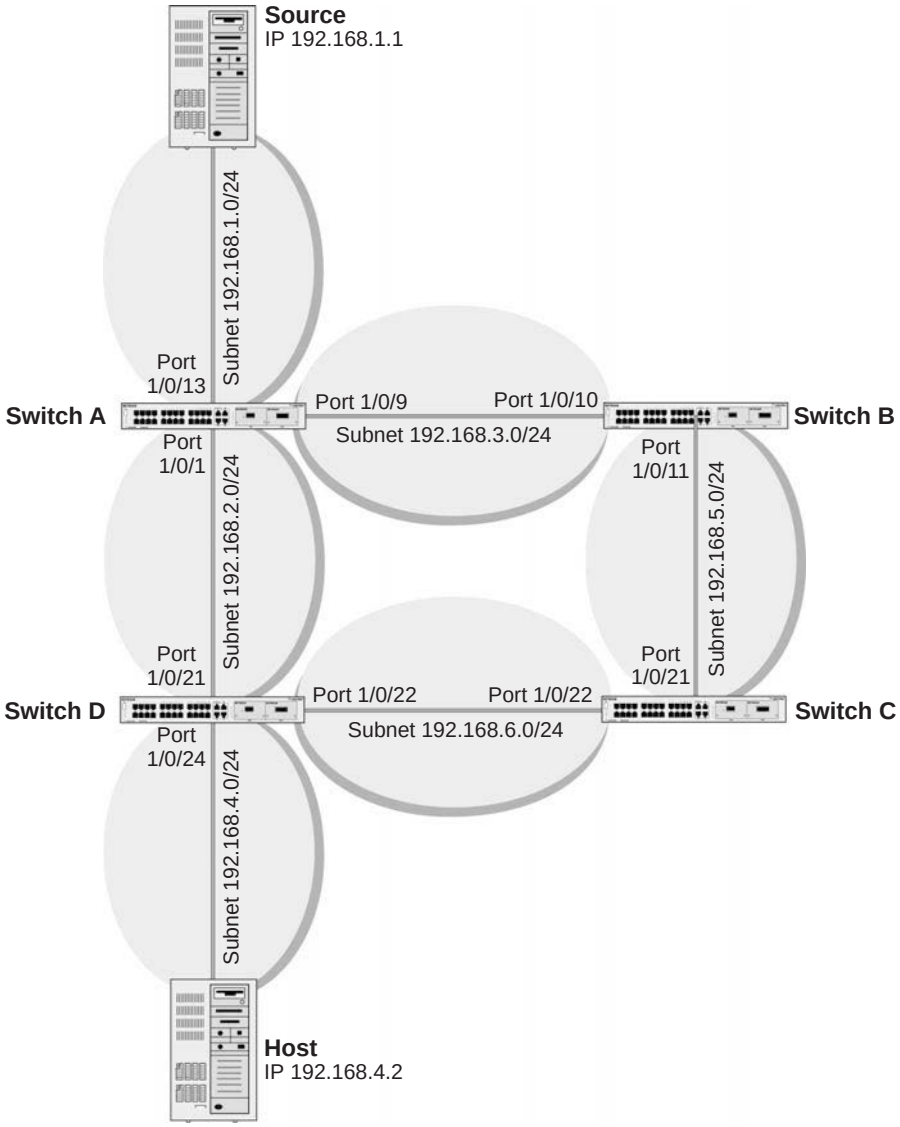


Figure 58. PIM-SM

PIM-SM uses shared trees by default and implements source-based trees for efficiency; it assumes that no hosts want the multicast traffic unless they specifically ask for it. It creates a shared distribution tree centered on a defined rendezvous point (RP). Traffic from this source is relayed to the receivers. Senders first send the multicast data to the RP, which in turn sends the data down the shared tree to the receivers. Shared trees centered on an RP do not necessarily provide the shortest, most optimal path. In such cases PIM-SM provides a means to switch to more efficient source-specific trees. A data threshold rate is defined for toggling between trees. PIM-SM uses a bootstrap router (BSR), which advertises information to other

multicast routers about the RP. In a given network, a set of routers can be administratively enabled as candidate bootstrap routers. If it is not apparent which router should be the BSR, the candidates flood the domain with advertisements. The router with the highest priority is elected. If all the priorities are equal, then the candidate with the highest IP address becomes the BSR. PIM-SM is defined in RFC 4601.

The following example describes how to configure and use PIM-SM. In this case, set the switch B,C,D as RP-candidate and BSR-candidate. Switch B will become the BSR because it has the highest priority. Switch D will become the RP after RP election.

CLI: Configure PIM-SM

PIM-SM on Switch A

1. Enable IP routing on the switch.

```
(Netgear Switch)#configure
(Netgear Switch) (Config)#ip routing
```

2. Enable PIM-SM on the switch.

```
(Netgear Switch) (Config)#ip pim sparse
```

3. Enable IP multicast forwarding on the switch.

```
(Netgear Switch) (Config)#ip multicast
```

4. Enable RIP to build a unicast IP routing table.

```
(Netgear Switch) (Config)#interface 1/0/1
(Netgear Switch) (Interface 1/0/1)#routing
(Netgear Switch) (Interface 1/0/1)#ip address 192.168.2.2  255.255.255.0
(Netgear Switch) (Interface 1/0/1)#ip rip
```

```
(Netgear Switch) (Interface 1/0/1)#ip pim
(Netgear Switch) (Interface 1/0/1)#exit

(Netgear Switch) (Config)#interface 1/0/9
(Netgear Switch) (Interface 1/0/9)#routing
(Netgear Switch) (Interface 1/0/9)#ip address 192.168.3.1  255.255.255.0
(Netgear Switch) (Interface 1/0/9)#ip rip
(Netgear Switch) (Interface 1/0/9)#ip pim
(Netgear Switch) (Interface 1/0/9)#exit

(Netgear Switch) (Config)#interface 1/0/13
(Netgear Switch) (Interface 1/0/13)#routing
(Netgear Switch) (Interface 1/0/13)#ip address  192.168.1.2  255.255.255.0
(Netgear Switch) (Interface 1/0/13)#ip rip
(Netgear Switch) (Interface 1/0/13)#ip pim
(Netgear Switch) (Interface 1/0/1)#exit
```

PIM-SM on Switch B

1. Enable the switch to advertise itself as a PIM candidate rendezvous point (RP) to the bootstrap router (BSR).

```
(Netgear Switch)#configure
(Netgear Switch) (Config)#ip routing
(Netgear Switch) (Config)#ip pim spars
(Netgear Switch) (Config)#ip multicast
(Netgear Switch) (Config)#ip pim rp-candidate interface 1/0/11 225.1.1.1
255.255.255.0
```

2. Enable the switch to announce its candidacy as a bootstrap router (BSR).

```
(Netgear Switch) (Config)#ip pim bsr-candidate interface 1/0/10 30  7

(Netgear Switch) (Config)#interface 1/0/10
(Netgear Switch) (Interface 1/0/10)#routing
(Netgear Switch) (Interface 1/0/10)#ip address 192.168.3.2  255.255.255.0
(Netgear Switch) (Interface 1/0/10)#ip rip
(Netgear Switch) (Interface 1/0/10)#ip pim
(Netgear Switch) (Interface 1/0/10)#exit

(Netgear Switch) (Config)#interface 1/0/11
(Netgear Switch) (Interface 1/0/11)#routing
(Netgear Switch) (Interface 1/0/11)#ip address 192.168.5.1  255.255.255.0
(Netgear Switch) (Interface 1/0/11)#ip rip
(Netgear Switch) (Interface 1/0/11)#ip pim
(Netgear Switch) (Interface 1/0/11)#exit
```

PIM-SM on Switch C

```
(Netgear Switch)#configure
(Netgear Switch) (Config)#ip routing
(Netgear Switch) (Config)#ip pim sparse
(Netgear Switch) (Config)#ip multicast
(Netgear Switch) (Config)#ip pim rp-candidate interface 1/0/22 225.1.1.1
255.255.255.0
(Netgear Switch) (Config)#ip pim bsr-candidate interface 1/0/21  30  5
(Netgear Switch) (Config)#interface 1/0/21
(Netgear Switch) (Interface 1/0/21)#routing
(Netgear Switch) (Interface 1/0/21)#ip address  192.168.5.2  255.255.255.0
(Netgear Switch) (Interface 1/0/21)#ip rip
(Netgear Switch) (Interface 1/0/21)#ip pim
(Netgear Switch) (Interface 1/0/21)#exit
(Netgear Switch) (Config)#interface 1/0/22
(Netgear Switch) (Interface 1/0/22)#routing
(Netgear Switch) (Interface 1/0/22)#ip address  192.168.6.1  255.255.255.0
(Netgear Switch) (Interface 1/0/22)#ip rip
(Netgear Switch) (Interface 1/0/22)#ip pim
(Netgear Switch) (Interface 1/0/22)#exit
```

PIM-SM on Switch D

```
(Netgear Switch)#configure
(Netgear Switch) (Config)#ip multicast
(Netgear Switch) (Config)#ip routing
(Netgear Switch) (Config)#ip igmp
(Netgear Switch) (Config)#ip pim
(Netgear Switch) (Config)#ip pim rp-candidate interface 1/0/22 225.1.1.1
255.255.255.0
(Netgear Switch) (Config)#ip pim bsr-candidate interface 1/0/22  30   3
(Netgear Switch) (Config)#interface 1/0/21
(Netgear Switch) (Interface 1/0/21)#routing
(Netgear Switch) (Interface 1/0/21)#ip address  192.168.2.1  255.255.255.0
(Netgear Switch) (Interface 1/0/21)#ip rip
(Netgear Switch) (Interface 1/0/21)#ip pim
(Netgear Switch) (Interface 1/0/21)#exit
(Netgear Switch) (Config)#interface 1/0/22
(Netgear Switch) (Interface 1/0/22)#routing
(Netgear Switch) (Interface 1/0/22)#ip address  192.168.6.2  255.255.255.0
(Netgear Switch) (Interface 1/0/22)#ip rip
(Netgear Switch) (Interface 1/0/22)#ip pim
(Netgear Switch) (Interface 1/0/22)#exit
```

```
(Netgear Switch) (Config)#interface 1/0/24
(Netgear Switch) (Interface 1/0/24)#routing
(Netgear Switch) (Interface 1/0/24)#ip address 192.168.4.1 255.255.255.0
(Netgear Switch) (Interface 1/0/24)#ip rip
(Netgear Switch) (Interface 1/0/24)#ip igmp
(Netgear Switch) (Interface 1/0/24)#ip pim
(Netgear Switch) (Interface 1/0/24)#exit
```

PIM-SM builds the multicast route table on each switch. The following tables show the routes that are built after PIM-SM switches to the source-specific tree from the shared tree.

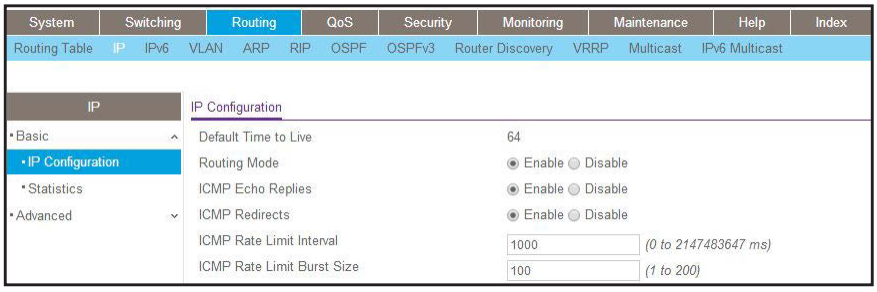
```
(A) #show ip mcast mroute summary
                  Multicast Route Table Summary
                                          Incoming     Outgoing
Source IP       Group IP     Protocol     Interface    Interface List
-----------     ---------    ---------    ---------    ---------------
192.168.1.1     225.1.1.1    PIMSM         1/0/13        1/0/1

(B) #show ip mcast mroute summary
                   Multicast Route Table Summary
                                         Incoming      Outgoing
Source IP       Group IP      Protocol    Interface     Interface List
-----------     ----------   ---------   ---------      ---------------
192.168.1.1     225.1.1.1     PIMSM       1/0/10

(C) #show ip mcast mroute summary
                  Multicast Route Table Summary
                                        Incoming      Outgoing
Source IP       Group IP     Protocol    Interface     Interface List
------------    ---------   ----------   ---------    ---------------
    *           225.1.1.1    PIMSM        1/0/22
192.168.1.1     225.1.1.1    PIMSM        1/0/21

(D) #show ip mcast mroute summary
                  Multicast Route Table Summary
                                        Incoming      Outgoing
Source IP       Group IP      Protocol    Interface    Interface List
----------    -----------    ----------  ---------    ---------------
    *           225.1.1.1       PIMSM    1/0/22          1/0/24
192.168.1.1     225.1.1.1       PIMSM    1/0/21          1/0/24
```

Web Interface: Configure PIM-SM

PIM-SM on Switch A

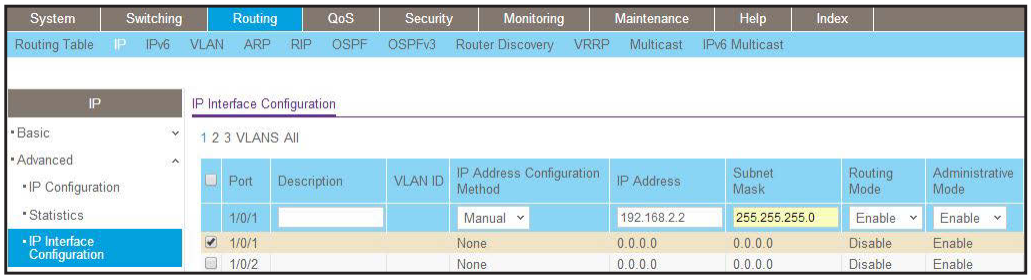
1. Enable IP routing on the switch.
   a. Select **Routing > IP > Basic > IP Configuration**.

      A screen similar to the following displays.



   b. For Routing Mode, select the **Enable** radio button.
   c. Click **Apply**.
2. Configure 1/0/1 as a routing port and assign an IP address to it.
   a. Select **Routing > IP > Advanced > IP Interface Configuration**.

      A screen similar to the following displays.

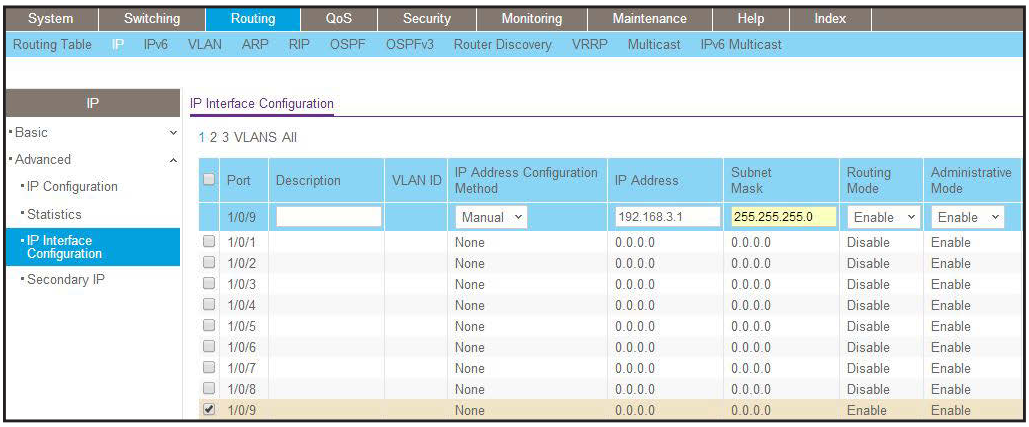


   b. Scroll down and select the interface **1/0/1** check box.

      Now 1/0/1 appears in the Interface field at the top.

   c. Enter the following information:
      - In the **IP Address** field, enter **192.168.2.2**.
      - In the **Subnet Mask** field, enter **255.255.255.0**.
      - In the **Routing Mode** field, select **Enable**.
   d. Click **Apply** to save the settings.
3. Configure 1/0/9 as a routing port and assign an IP address to it.
   a. Select **Routing > IP > Advanced > IP Interface Configuration**.

A screen similar to the following displays.



b. Scroll down and select the interface **1/0/9** check box.

Now 1/0/9 appears in the Interface field at the top.

c. Enter the following information:

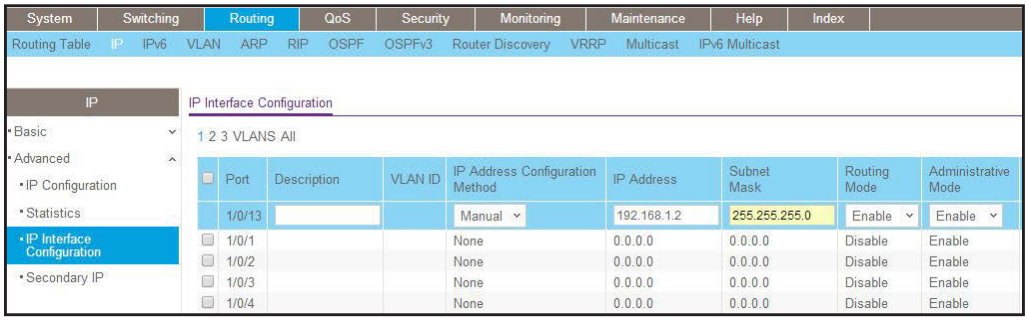
- In the **IP Address** field, enter **192.168.3.1**.
- In the **Subnet Mask** field, enter **255.255.255.0**.
- In the **Routing Mode** field, select **Enable**.

d. Click **Apply**.

4. Configure 1/0/13 as a routing port and assign an IP address to it.

a. Select **Routing > IP > Advanced > IP Interface Configuration**.

A screen similar to the following displays.



b. Scroll down and select the interface **1/0/13** check box.

Now 1/0/13 appears in the Interface field at the top.

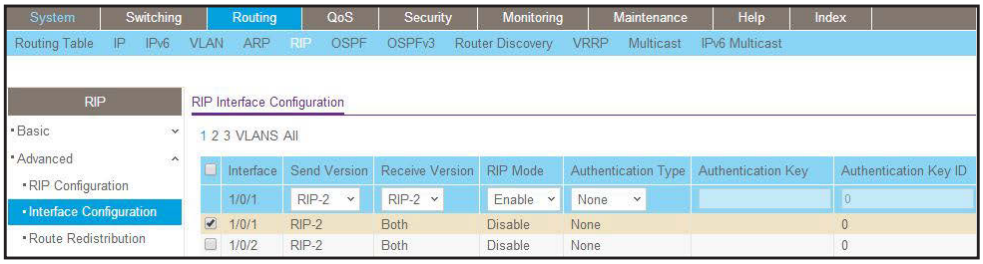
c. Enter the following information:

- In the **IP Address** field, enter **192.168.1.2**.
- In the **Subnet Mask** field, enter **255.255.255.0**.
- In the **Routing Mode** field, select **Enable**.

d. Click **Apply** to save the settings.

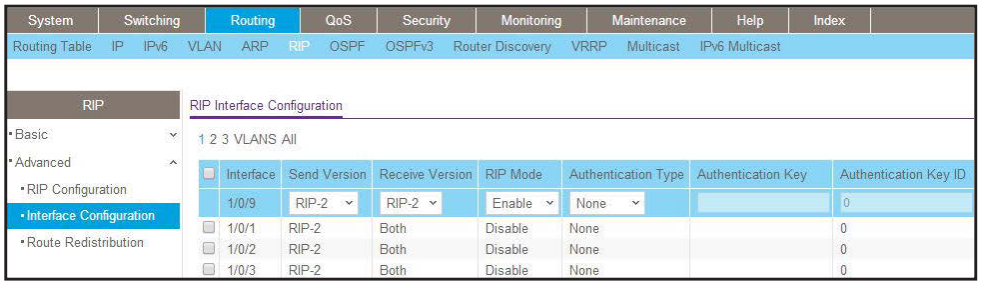
5. Enable RIP on interface 1/0/1.
   a. Select **Routing > RIP > Advanced > Interface Configuration**.

      A screen similar to the following displays.



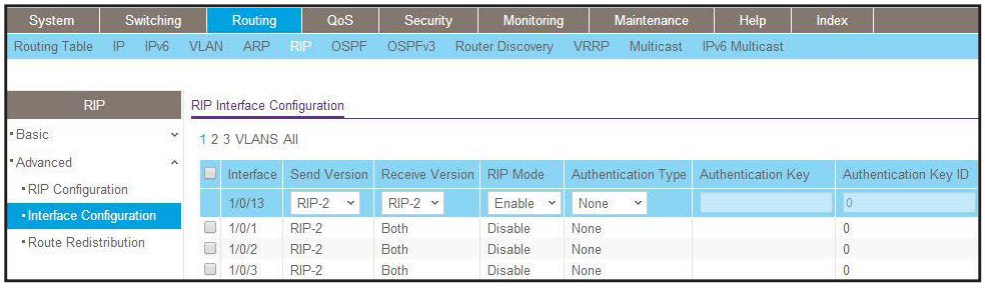
   b. In the **Interface** field, select **1/0/1**.
   c. For RIP Admin Mode, select the **Enable** radio button.
   d. Click **Apply**.
6. Enable RIP on interface 1/0/9.
   a. Select **Routing > RIP > Advanced > Interface Configuration**.

      A screen similar to the following displays.



   b. In the **Interface** field, select **1/0/9**.
   c. For RIP Admin Mode, select the **Enable** radio button.
   d. Click **Apply**.
7. Enable RIP on interface 1/0/13.
   a. Select **Routing > RIP > Advanced > Interface Configuration**.

      A screen similar to the following displays.



   b. Select **1/0/13** in the **Interface** field.
   c. For RIP Admin Mode, select the **Enable** radio button.

d. Click **Apply**.

8. Enable multicast globally.

a. Select **Routing > Multicast > Global Configuration**.

A screen similar to the following displays.

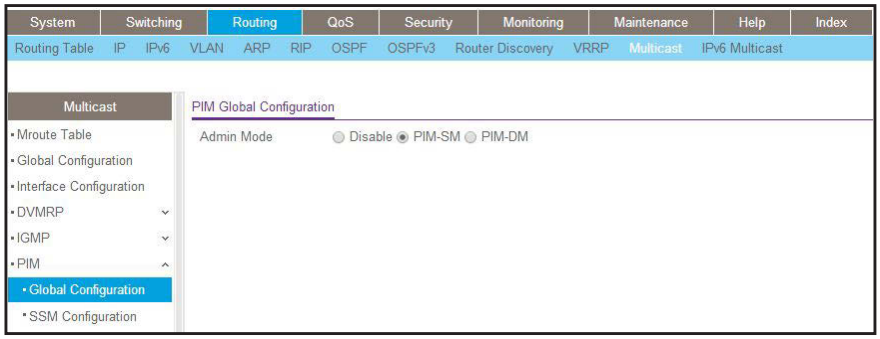
b. For Admin Mode, select the **Enable** radio button.

c. Click **Apply**.

9. Enable PIM-SM globally.

a. Select **Routing > Multicast > PIM > Global Configuration**.

A screen similar to the following displays.



b. For PIM Protocol Type, select the **PIM-SM** radio button.

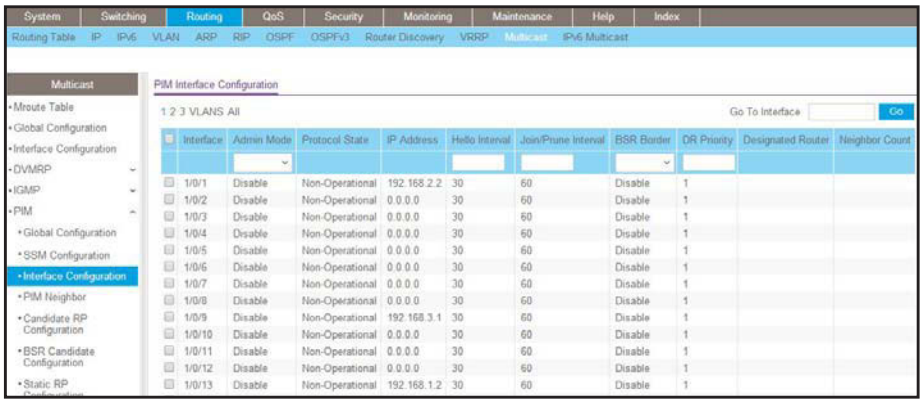
c. For Admin Mode, select the **Enable** radio button.

d. Click **Apply**.

10. Enable PIM-SM on interfaces 1/0/1,1/0/9, and 1/0/13.

a. Select **Routing > Multicast > PIM > Interface Configuration**.

A screen similar to the following displays.



b. Scroll down and select the Interface **1/0/1**, **1/0/9**, and **1/0/13** check boxes.

c. In the **Admin Mode** field, select **Enable**.

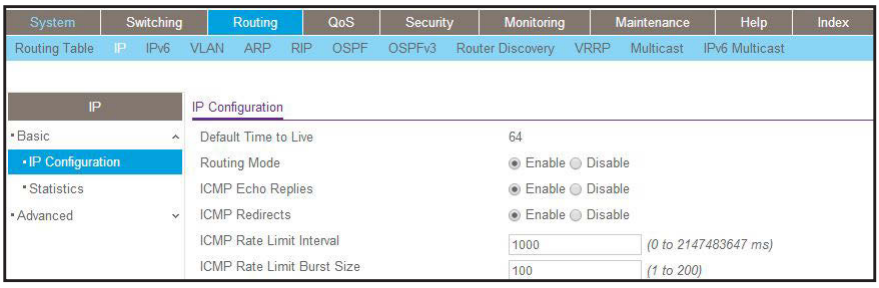
d. Click **Apply** to save the settings.

PIM-SM on Switch B:

1. Enable IP routing on the switch.

a. Select **Routing > IP > Basic > IP Configuration**.

A screen similar to the following displays.



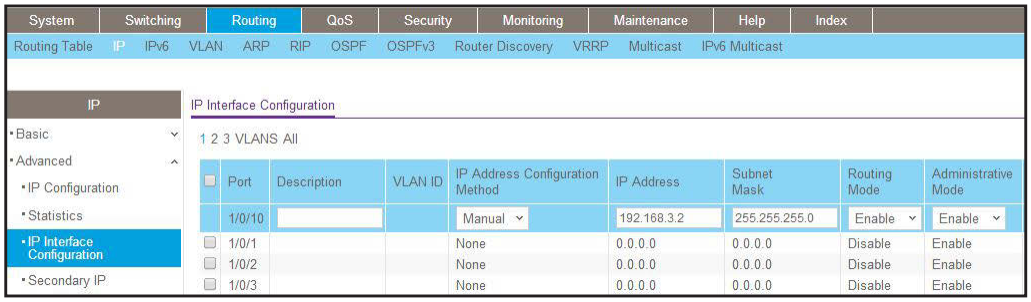
b. For Routing Mode, select the **Enable** radio button.

c. Click **Apply**.

2. Configure 1/0/10 as a routing port and assign an IP address to it.

a. Select **Routing > IP > Advanced > IP Interface Configuration**.

A screen similar to the following displays.



b. Scroll down and select the interface **1/0/10** check box.

Now 1/0/10 appears in the Interface field at the top.

c. Enter the following information:

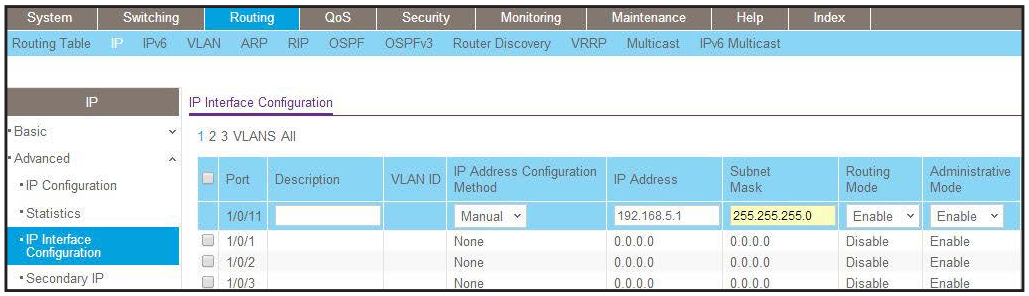
- In the **IP Address** field, enter **192.168.3.2**.
- In the **Subnet Mask** field, enter **255.255.255.0**.
- In the **Routing Mode** field, select **Enable**.

d. Click **Apply** to save the settings.

3. Configure 1/0/11 as a routing port and assign an IP address to it.

a. Select **Routing > IP > Advanced > IP Interface Configuration**.

A screen similar to the following displays.



b. Scroll down and select the Port **1/0/11** check box.

Now 1/0/11 appears in the Port field at the top.

c. Enter the following information:

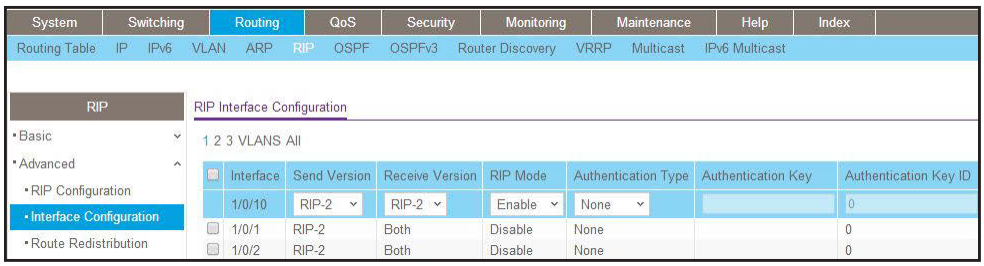
- In the **IP Address** field, enter **192.168.5.1**.
- In the **Subnet Mask** field, enter **255.255.255.0**.
- In the **Routing Mode** field, select **Enable**.

d. Click **Apply** to save the settings.

4. Enable RIP on interface 1/0/10.

a. Select **Routing > RIP > Advanced > Interface Configuration**.

A screen similar to the following displays.



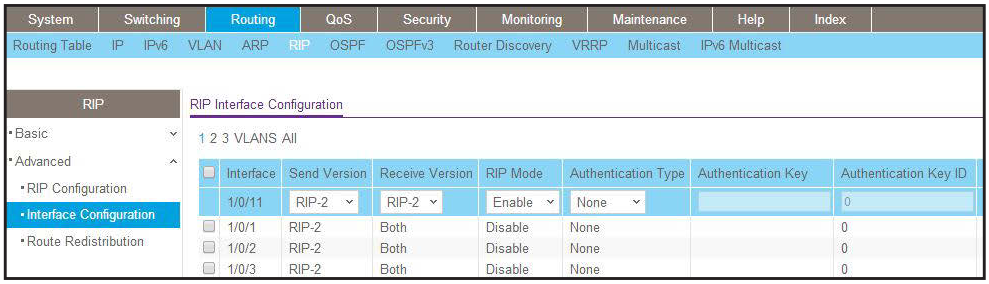
b. In the **Interface** field, select **1/0/10**.

c. For RIP Admin Mode, select the **Enable** radio button.

d. Click **Apply**.

5. Enable RIP on interface 1/0/11.
   a. Select **Routing > RIP > Advanced > Interface Configuration**.

      A screen similar to the following displays.

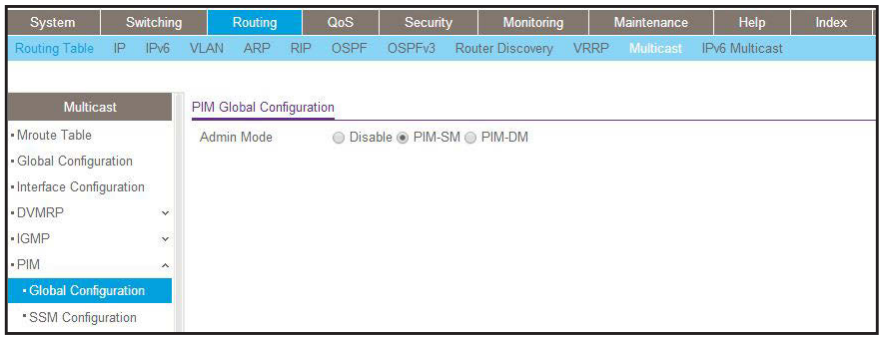


   b. In the **Interface** list, select **1/0/11**.
   c. For RIP Admin Mode, select the **Enable** radio button.
   d. Click **Apply**.
6. Enable multicast globally.
   a. Select **Routing > Multicast > Global Configuration**.

      A screen similar to the following displays.

   b. For Admin Mode, select the **Enable** radio button.
   c. Click **Apply**.
7. Enable PIM-SM globally.
   a. Select **Routing > Multicast > PIM > Global Configuration**.

      A screen similar to the following displays.



b. For PIM Protocol Type, select the **PIM-SM** radio button.

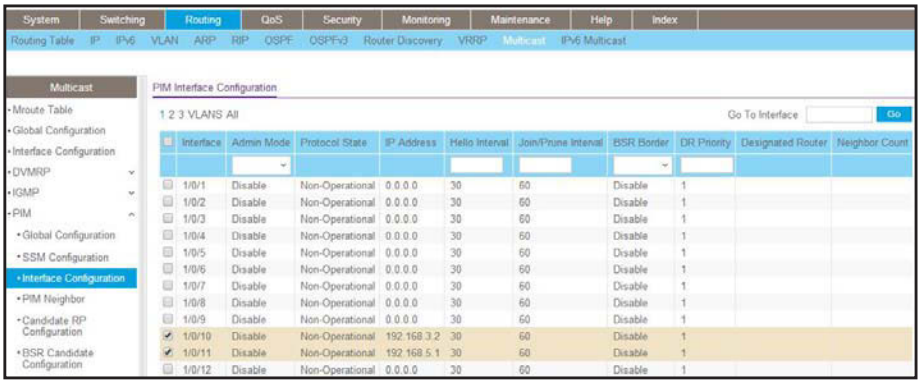
c. For Admin Mode, select the **Enable** radio button.

d. Click **Apply**.

8. Enable PIM-SM on interfaces 1/0/10 and 1/0/11.

a. Select **Routing > Multicast > PIM > Interface Configuration**.

A screen similar to the following displays.



b. Scroll down and select the Interface **1/0/10** and **1/0/11** check boxes.

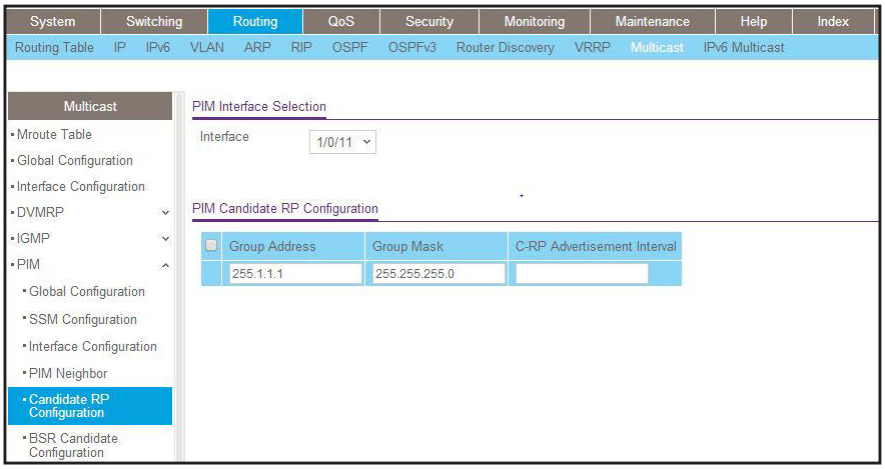
c. In the **Admin Mode** field, select **Enable**.

d. Click **Apply** to save the settings.

9. Set up the candidate RP configuration.

a. Select **Routing > Multicast > PIM > Candidate RP Configuration**.

A screen similar to the following displays.



b. In the **Interface** list, select **1/0/11**.

c. In the **Group IP** field, enter **225.1.1.1**.

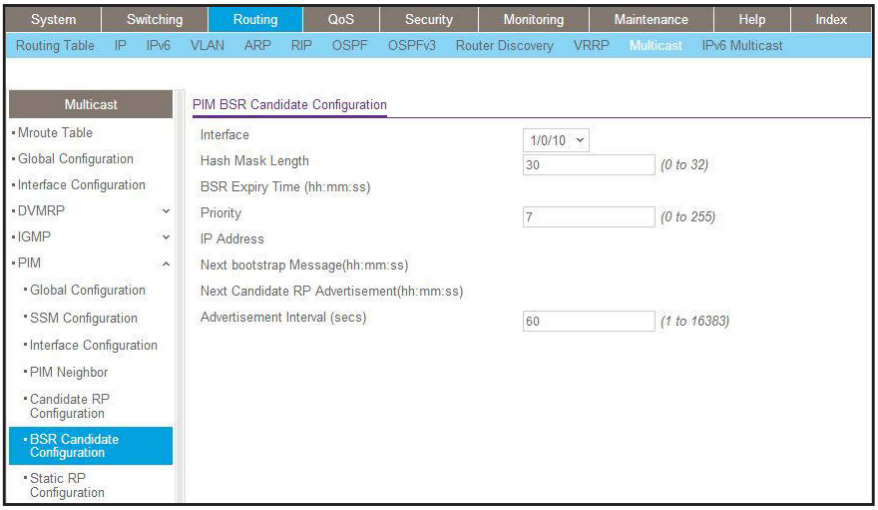
d. In the **Group Mask** field, enter **255.255.255.0**.

e. Click **Add**.

10. Set up the BSR candidate configuration.

a. Select **Routing > Multicast > PIM > BSR Candidate Configuration**.

A screen similar to the following displays.



b. In the **Interface** list, select the **1/0/10**.

c. In the **Hash Mask Length** field, enter **30**.

d. In the **Priority** field, enter **7**.

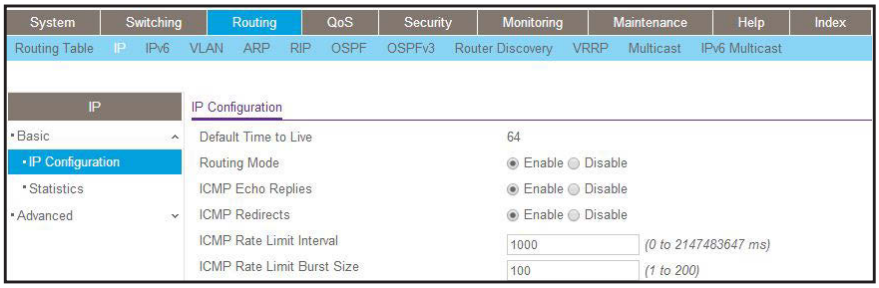
e. Click **Apply**.

PIM-SM on Switch C:

1. Enable IP routing on the switch.

a. Select **Routing > IP > Basic > IP Configuration**.

A screen similar to the following displays.



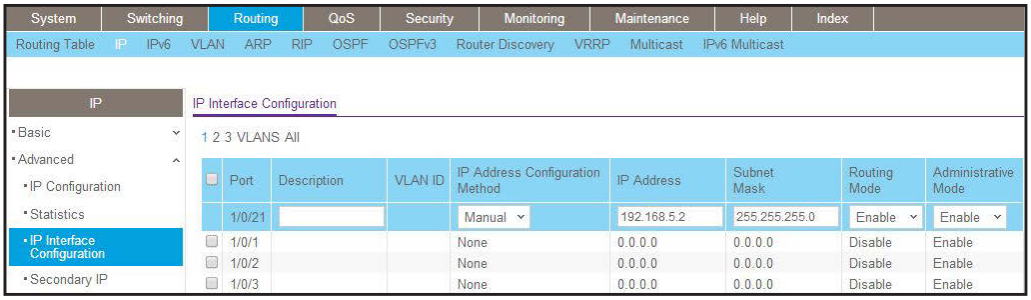
b. For Routing Mode, select the **Enable** radio button.

c. Click **Apply**.

2. Configure 1/0/21 as a routing port and assign an IP address to it.

a. Select **Routing > IP > Advanced > IP Interface Configuration**.

A screen similar to the following displays.



b. Scroll down and select the Port **1/0/21** check box.

Now 1/0/21 appears in the Interface field at the top.

c. Enter the following information:

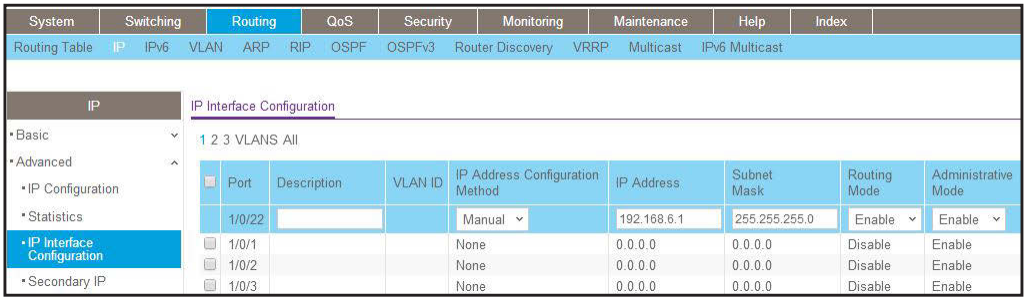
- In the **IP address**, enter **192.168.5.2**.
- In the **Subnet Mask** field, enter **255.255.255.0**.
- In the **Routing Mode** field, select **Enable**.

d. Click **Apply** to save the settings.

3. Configure 1/0/22 as a routing port and assign an IP address to it.

a. Select **Routing > IP > Advanced > IP Interface Configuration**.

A screen similar to the following displays.



b. Scroll down and select the **1/0/22** check box.

Now 1/0/22 appears in the Interface field at the top.

c. Enter the following information:

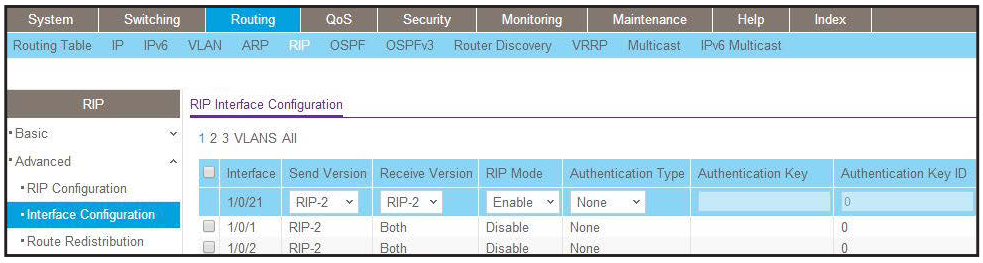
- In the **IP Address** field, enter **192.168.6.1**.
- In the **Subnet Mask** field, enter **255.255.255.0**.
- In the **Routing Mode** field, select **Enable**.

d. Click **Apply** to save the settings.

4. Enable RIP on the interface 1/0/21.

a. Select **Routing > RIP > Advanced > Interface Configuration**.

A screen similar to the following displays.



b. In the **Interface** field, select **1/0/21**.

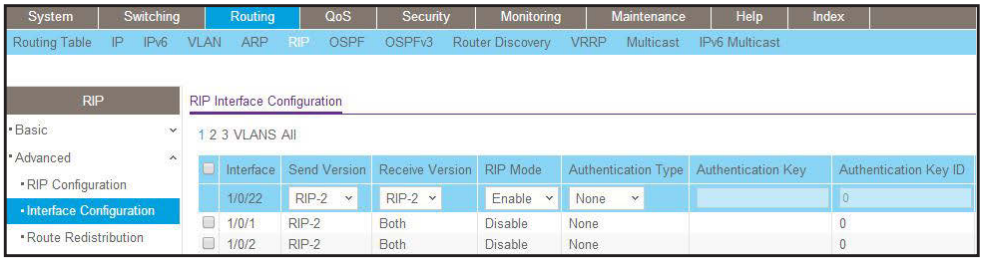
c. For RIP Admin Mode, select the **Enable** radio button.

d. Click **Apply**.

5. Enable RIP on interface 1/0/22.

a. Select **Routing > RIP > Advanced > Interface Configuration**.

A screen similar to the following displays.



b. In the **Interface** list, select **1/0/22**.

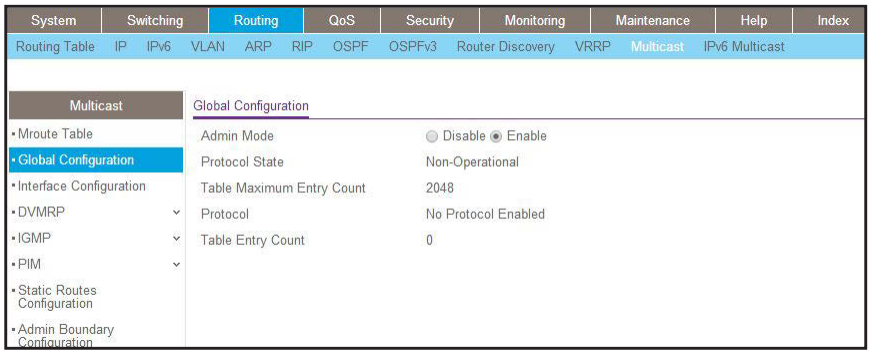
c. For RIP Admin Mode, select the **Enable** radio button.

d. Click **Apply**.

6. Enable multicast globally.

a. Select **Routing > Multicast > Global Configuration**.

A screen similar to the following displays.

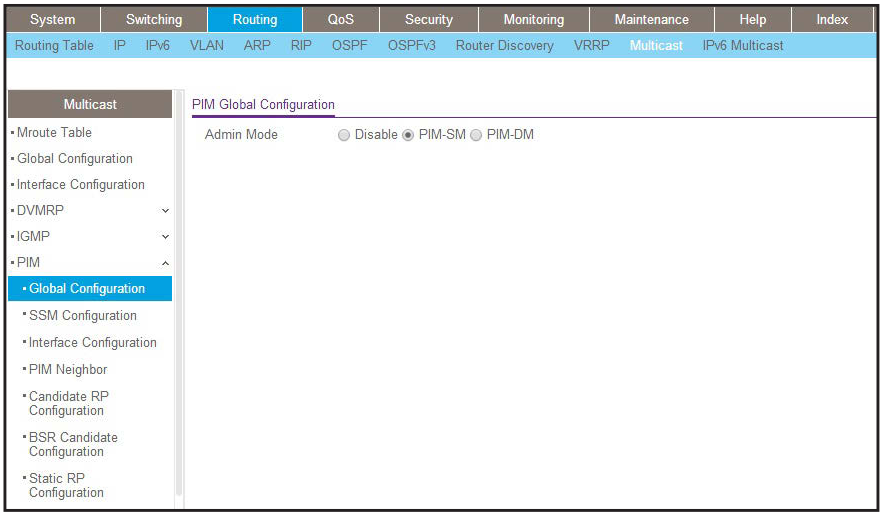


b. For Admin Mode, select the **Enable** radio button.

c. Click **Apply**.

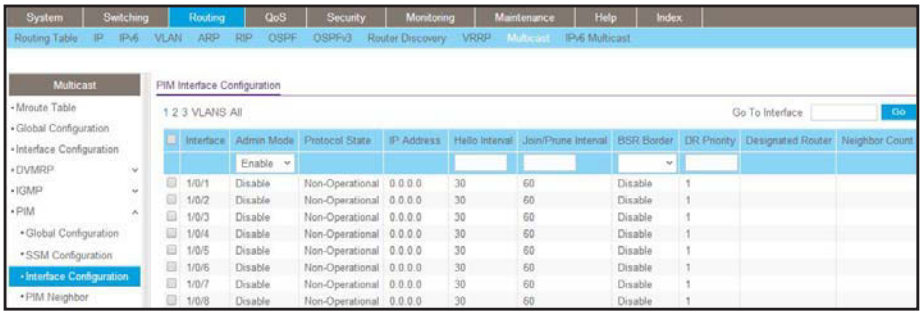
7. Enable PIM-SM globally.
   a. Select **Routing > Multicast > PIM > Global Configuration**.

      A screen similar to the following displays.



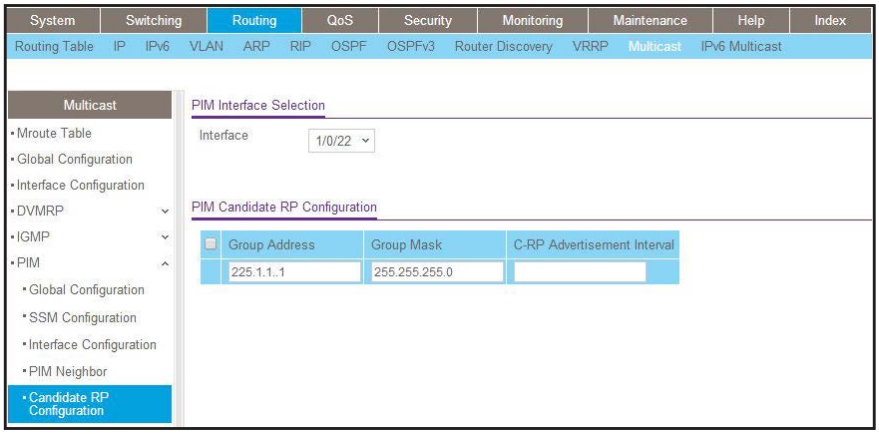
   b. For PIM Protocol Type, select the **PIM-SM** radio button.
   c. For Admin Mode, select the **Enable** radio button.
   d. Click **Apply**.
8. Enable PIM-SM on interfaces 1/0/21 and 1/0/22.
   a. Select **Routing > Multicast > PIM > Interface Configuration**.

      A screen similar to the following displays.



   b. Scroll down and select the Interface **1/0/21** and **1/0/22** check boxes.
   c. In the **Admin Mode** field, select **Enable**.
   d. Click **Apply** to save the settings.
9. Candidate RP Configuration.
   a. Select **Routing > Multicast > PIM > Candidate RP Configuration**.

A screen similar to the following displays.



b. In the **Interface** list, select **1/0/22**.

c. In the **Group IP** field, enter **225.1.1.1**.

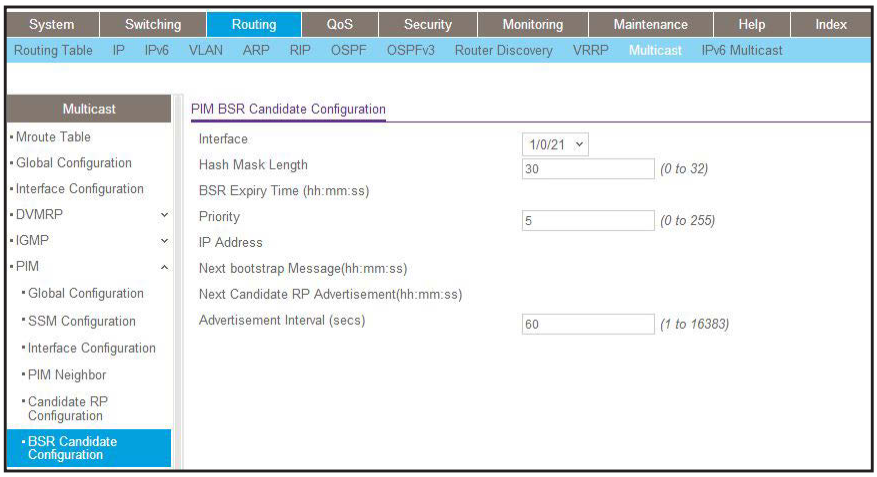
d. In the **Group Mask** field, enter **255.255.255.0**.

e. Click **Add**.

10. BSR Candidate Configuration.

a. Select **Routing > Multicast > PIM > BSR Candidate Configuration**.

A screen similar to the following displays.



b. In the **Interface** list, select the **1/0/21**.

c. In the **Hash Mask Length** field, enter **30**.

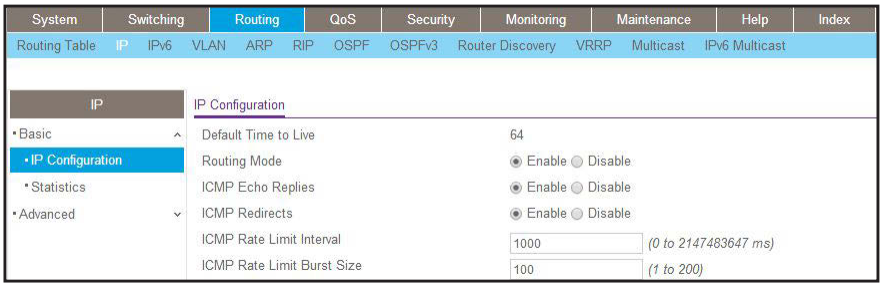
d. In the **Priority** field, enter **5**.

e. Click **Apply**.

PIM-SM on Switch D

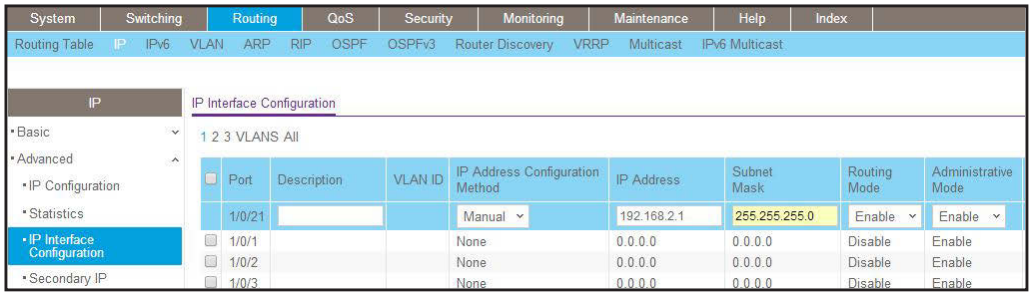
1. Enable IP routing on the switch.
   a. Select **Routing > IP > Basic > IP Configuration**.

      A screen similar to the following displays.



   b. For Routing Mode, select the **Enable** radio button.
   c. Click **Apply**.
2. Configure 1/0/21 as a routing port and assign an IP address to it.
   a. Select **Routing > IP > Advanced > IP Interface Configuration**.

      A screen similar to the following displays.



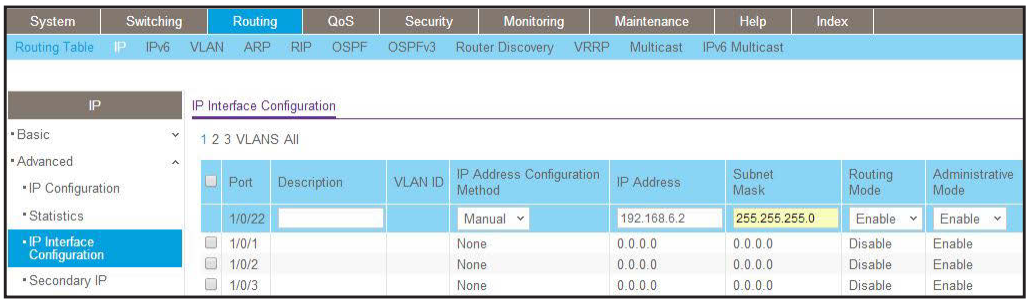
   b. Scroll down and select the Interface **1/0/21** check box.

      Now 1/0/21 appears in the Interface field at the top.

   c. Enter the following information:
      - In the **IP Address** field, enter **192.168.2.1**.
      - In the **Subnet Mask** field, enter **255.255.255.0**.
      - In the **Routing Mode** field, select **Enable**.

   d. Click **Apply** to save the settings.
3. Configure 1/0/22 as a routing port and assign an IP address to it.
   a. Select **Routing > IP > Advanced > IP Interface Configuration**.

A screen similar to the following displays.



b. Scroll down and select the Port **1/0/22** check box.

Now 1/0/22 appears in the Port field at the top.

c. Enter the following information:

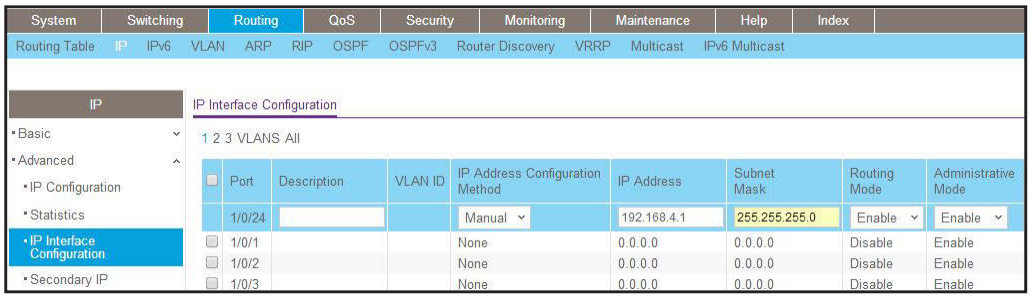
- In the **IP Address** field, enter **192.168.6.2**.
- In the **Subnet Mask** field, enter **255.255.255.0**.
- In the **Routing Mode** field, select **Enable**.

d. Click **Apply** to save the settings.

4. Configure 1/0/24 as a routing port and assign an IP address to it.

a. Select **Routing > IP > Advanced > IP Interface Configuration**.

A screen similar to the following displays.



b. Scroll down and select the Interface **1/0/24** check box.

Now 1/0/24 appears in the Interface field at the top.

c. Enter the following information:

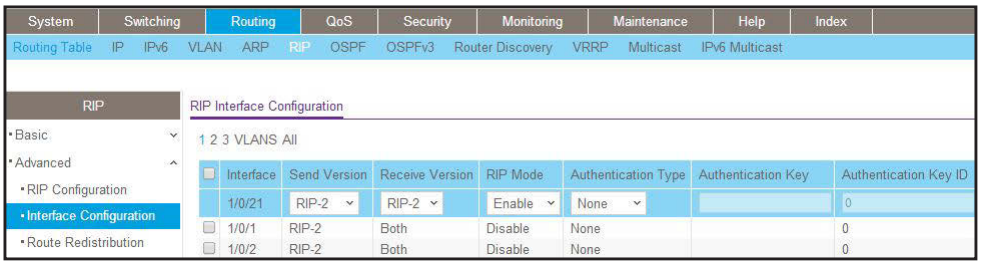
- In the **IP Address** field, enter **192.168.4.1**.
- In the **Subnet Mask** field, enter **255.255.255.0**.
- In the **Routing Mode** field, select **Enable**.

d. Click **Apply** to save the settings.

5. Enable RIP on interface 1/0/21.

a. Select **Routing > RIP > Advanced > Interface Configuration**.

A screen similar to the following displays.



b. In the **Interface** list, select **1/0/21**.

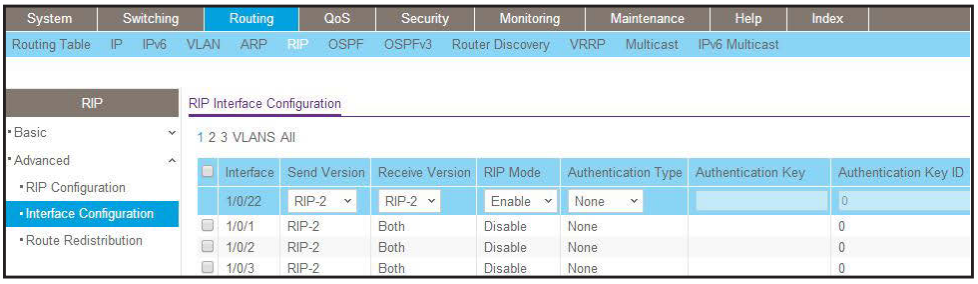
c. For RIP Admin Mode, select the **Enable** radio button.

d. Click **Apply**.

6. Enable RIP on interface 1/0/22.

a. Select **Routing > RIP > Advanced > Interface Configuration**.

A screen similar to the following displays.



b. In the **Interface** list, select **1/0/22**.

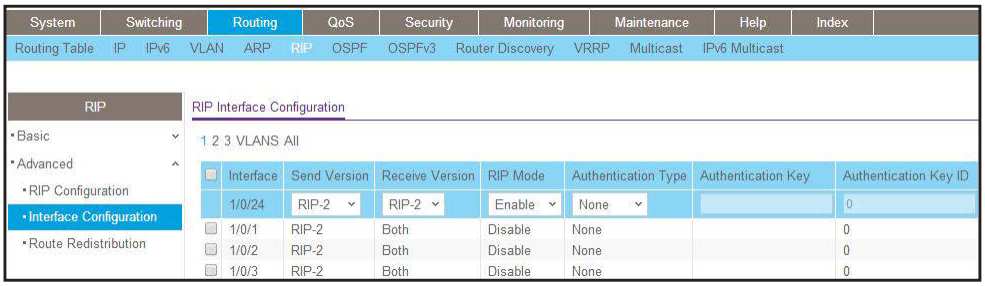
c. For RIP Admin Mode, select the **Enable** radio button.

d. Click **Apply**.

7. Enable RIP on interface 1/0/24.

a. Select **Routing > RIP > Advanced > Interface Configuration**.

A screen similar to the following displays.



b. In the **Interface** list, select **1/0/24**.

c. For RIP Admin Mode, select the **Enable** radio button.

d. Click **Apply**.

8. Enable multicast globally.

a. Select **Routing > Multicast > Global Configuration**.

A screen similar to the following displays.

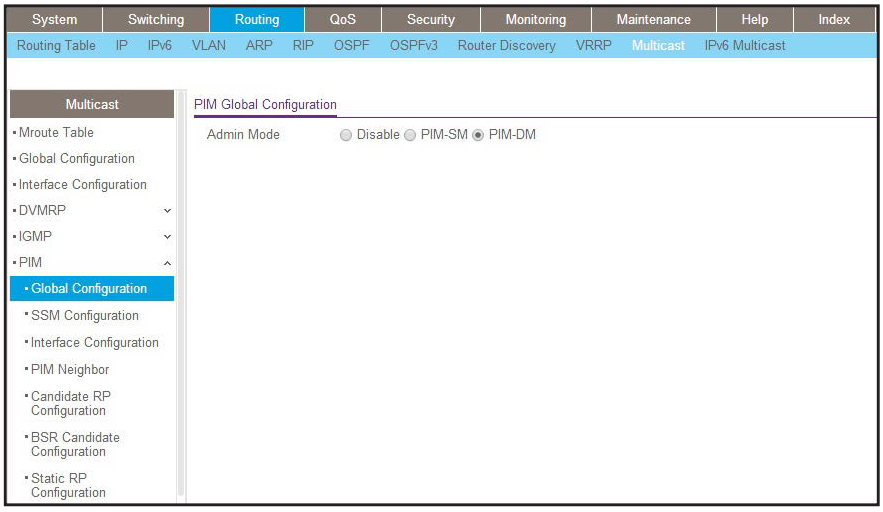
b. For Admin Mode, select the **Enable** radio button.

c. Click **Apply**.

9. Enable PIM-SM globally.

a. Select **Routing > Multicast > PIM > Global Configuration**.

A screen similar to the following displays.



b. For PIM Protocol Type, select the **PIM-SM** radio button.

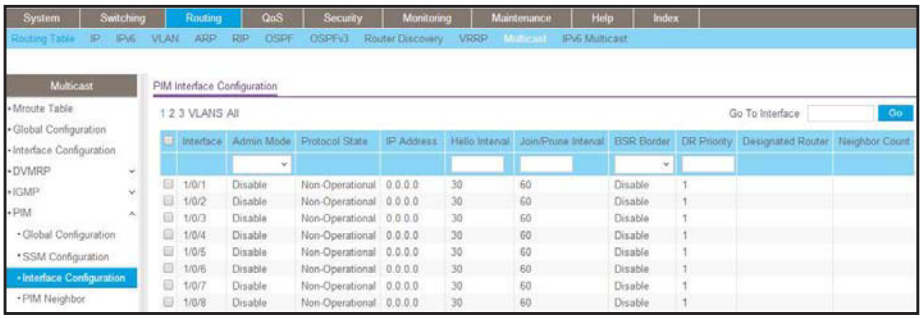
c. For Admin Mode, select the **Enable** radio button.

d. Click **Apply**.

10. Enable PIM-SM on interfaces 1/0/21, 1/0/22, and 1/0/24.

a. Select **Routing > Multicast > PIM > Interface Configuration**.

A screen similar to the following displays.



b. Scroll down and select the Interface **1/0/21, 1/0/22**, and **1/0/24** check boxes.

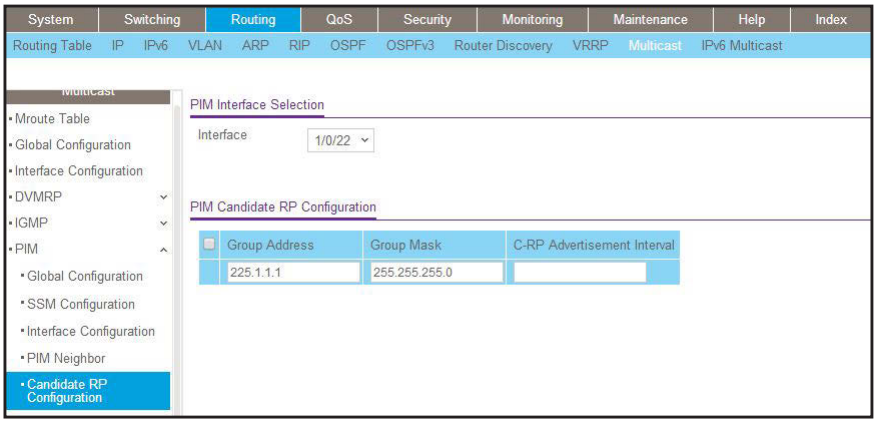
c. In the **Admin Mode** field, select **Enable**.

d. Click **Apply** to save the settings.

11. Set up Candidate RP configuration.

a. Select **Routing > Multicast > PIM > Candidate RP Configuration**.

A screen similar to the following displays.



b. In the **Interface** list, select **1/0/22**.

c. In the **Group IP** field, enter **225.1.1.1**.

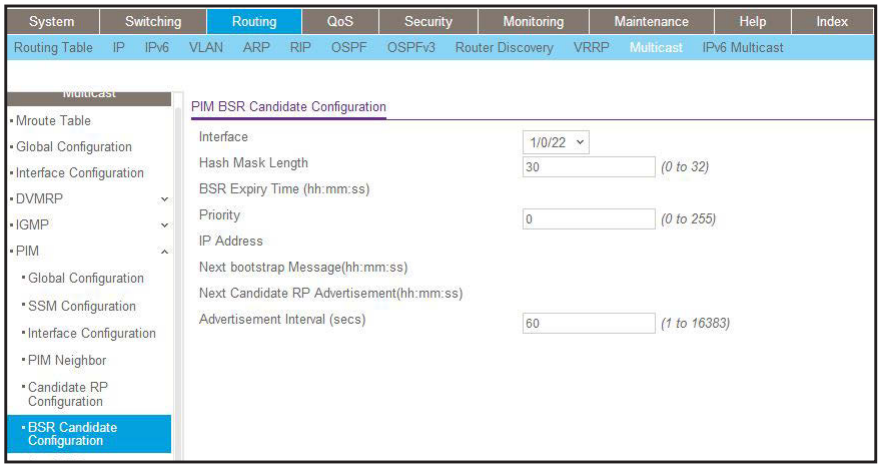
d. In the **Group Mask** field, enter **255.255.255.0**.

e. Click **Add**.

12. Set up BSR Candidate configuration.

a. Select **Routing > Multicast > PIM > BSR Candidate Configuration**.

A screen similar to the following displays.



b. In the **Interface** list, select **1/0/22**.

c. In the **Hash Mask Length** field, enter **30**.

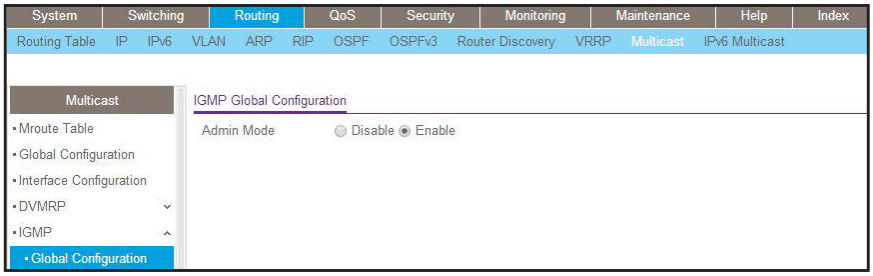
d. In the **Priority** field, enter **3**.

e. Click **Apply**.

13. Enable IGMP globally.

a. Select **Routing > Multicast > IGMP > Global Configuration**.

A screen similar to the following displays.



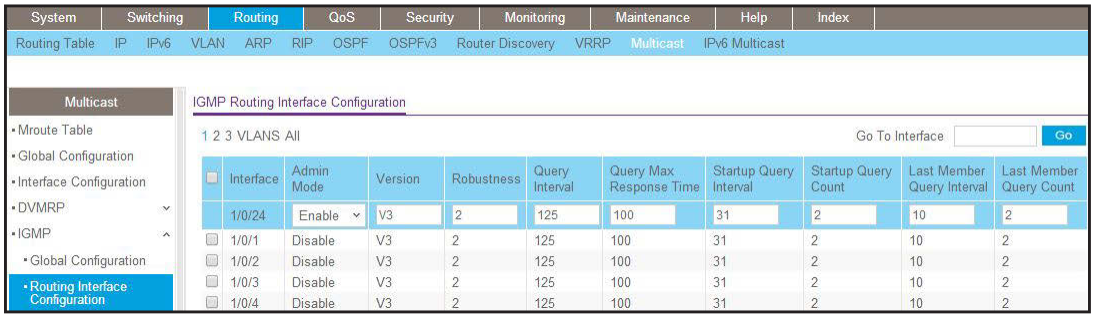
b. For Admin Mode, select the **Enable** radio button.

c. Click **Apply**.

14. Enable IGMP on interface 1/0/24.

a. Select **Routing > Multicast > IGMP > Interface Configuration**.

A screen similar to the following displays.



b. Under IGMP Routing Interface Configuration, scroll down and select the Interface **1/0/24** check box.

c. In the **Admin Mode** field, select **Enable**.

d. Click **Apply** to save the settings.

DHCP L2 Relay and L3 Relay

31

Dynamic Host Configuration Protocol relays

This chapter includes the following sections:

- *DHCP L2 Relay*
- *DHCP L3 Relay*
- *Configure a DHCP L3 Switch*

DHCP L2 Relay

DHCP relay agents eliminate the need to have a DHCP server on each physical network. Relay agents populate the `giaddr` field and also append the `Relay Agent Information` option to the DHCP messages. DHCP servers use this option for IP addresses and other parameter assignment policies. These DHCP relay agents are typically IP routing-aware devices and are referred to as Layer 3 relay agents.

In some network configurations, Layer 2 devices can append the relay agent Information option as they are closer to the end hosts.

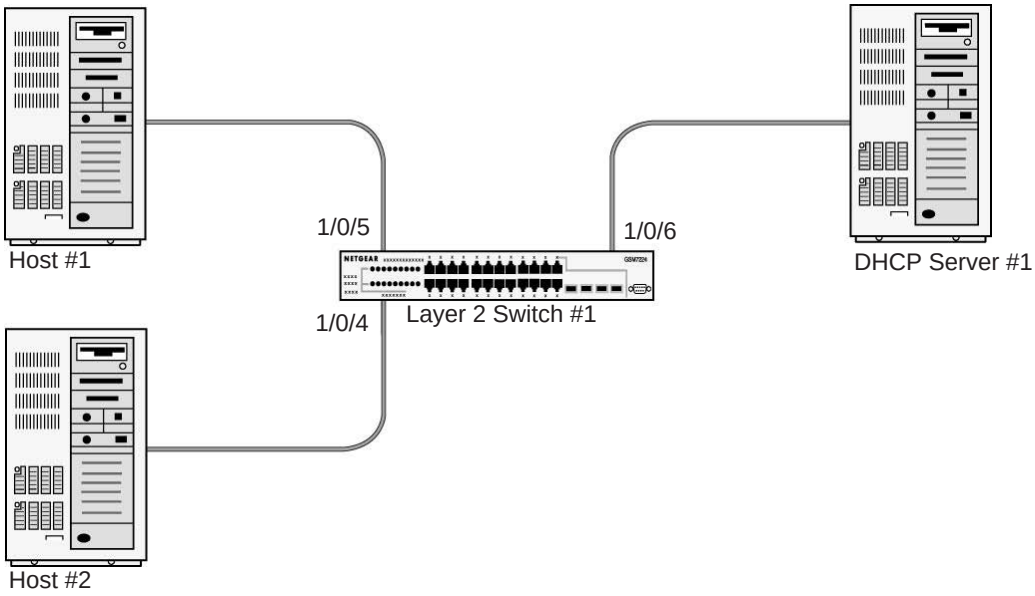


Figure 59. DHCP L2 relay

These Layer 2 devices typically operate only as bridges for the network and might not have an IPv4 address on the network. Lacking a valid IPv4 source address, they cannot relay packets directly to a DHCP server on another network. These Layer 2 devices append the Relay agent information option and broadcast the DHCP message. This section provides information about where a Layer 2 relay agent fits in and how it is used.

CLI: Enable DHCP L2 Relay

1. Enter the following commands:

```
(Netgear Switch)#vlan database
(Netgear Switch)(Vlan)#vlan 200
(Netgear Switch)(Vlan)#exit
```

2. Enable the DHCP L2 relay on the switch.

```
(Netgear Switch) (Config)#dhcp l2relay
(Netgear Switch) (Config)#dhcp l2relay vlan 200
```

3. Enable the Option 82 Circuit ID field.

```
(Netgear Switch) (Config)#dhcp l2relay circuit-id vlan 200
```

4. Enable the Option 82 Remote ID field.

```
(Netgear Switch) (Config)#dhcp l2relay remote-id rem_id vlan 200
```

5. Enable DHCP L2 relay on port 1/0/4.

```
(Netgear Switch) (Config)#interface 1/0/4
(Netgear Switch) (Interface 1/0/4)# dhcp l2relay
```

```
(Netgear Switch) (Interface 1/0/4)# vlan pvid 200
(Netgear Switch) (Interface 1/0/4)# vlan participation include 200
(Netgear Switch) (Interface 1/0/4)# exit
```

6. Enable DHCP L2 relay on port 1/0/5.

```
(Netgear Switch) (Config)#interface 1/0/5
(Netgear Switch) (Interface 1/0/5)# dhcp l2relay
(Netgear Switch) (Interface 1/0/5)# vlan pvid 200
(Netgear Switch) (Interface 1/0/5)# vlan participation include 200
(Netgear Switch) (Interface 1/0/5)# exit
```

7. Enable DHCP L2 relay on port 1/0/6.

```
(Netgear Switch) (Config)#interface 1/0/6
(Netgear Switch) (Interface 1/0/6)# dhcp l2relay
```

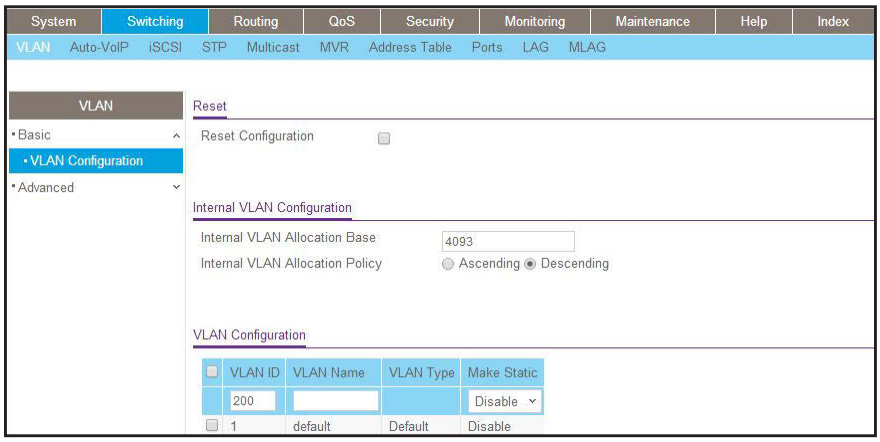
8. Trust packets with option 82 received on port 1/0/6.

```
(Netgear Switch) (Interface 1/0/6)# dhcp l2relay trust
(Netgear Switch) (Interface 1/0/6)# vlan pvid 200
(Netgear Switch) (Interface 1/0/6)# vlan participation include 200
(Netgear Switch) (Interface 1/0/6)# exit
```

Web Interface: Enable DHCP L2 Relay

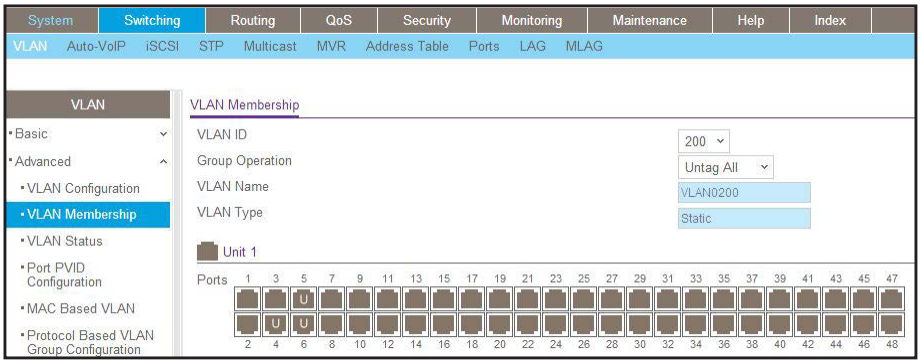
1. Create VLAN 200.
   a. Select **Switching > VLAN > Basic > VLAN Configuration**.

      A screen similar to the following displays.



   b. In the **VLAN ID** field, enter **200**.
   c. In the **VLAN Type** field, select **Static**.
   d. Click **Add**.
2. Add ports to VLAN 200.
   a. Select **Switching > VLAN > Advanced > VLAN Membership**.

      A screen similar to the following displays.

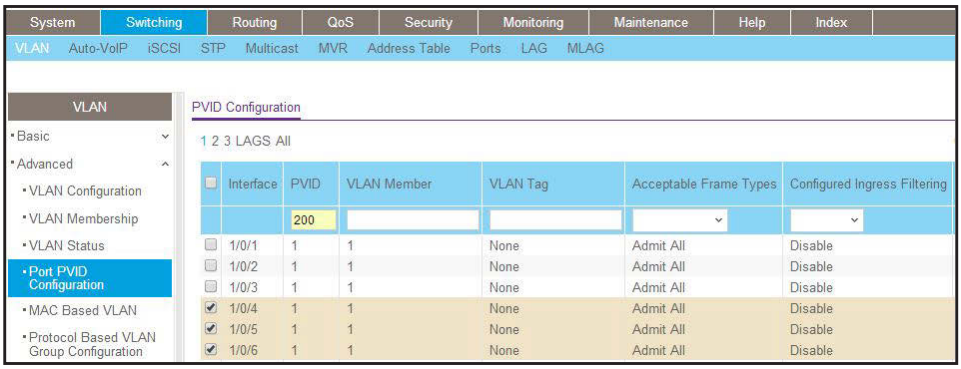


   b. In the **VLAN ID** field, select **200**.
   c. Click **Unit 1**. The ports display.
   d. Click the gray boxes under ports **4**, **5**, and **6** until **U** displays.

      The U specifies that the egress packet is untagged for the port.

   e. Click **Apply**.
3. Specify the PVID on ports 1/0/4, 1/0/5 and 1/0/6.
   a. Select **Switching > VLAN > Advanced > Port PVID Configuration**.

A screen similar to the following displays.



b. Scroll down and select the Interface **1/0/4**, **1/0/5**, and **1/0/6** check boxes.

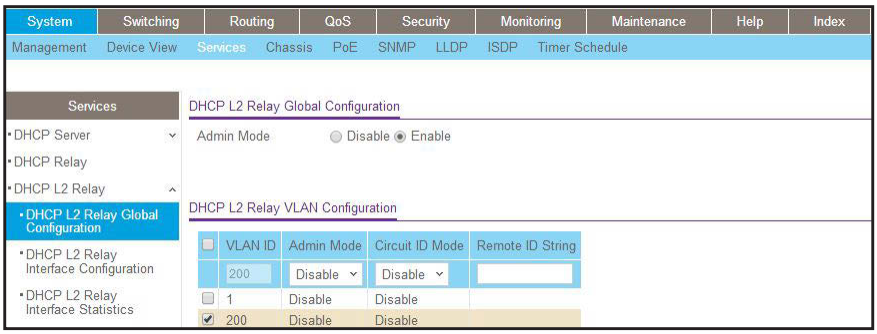
c. In the **PVID (1 to 4093)** field, enter **200**.

d. Click **Apply** to save the settings.

4. Enable DHCP L2 relay on VLAN 200.

a. Select **System > Services > DHCP L2 Relay > DHCP L2 Relay Configuration**.

A screen similar to the following displays.



b. For Admin Mode, select the **Enable** radio button.

c. Scroll down and select the VLAN ID **200** check box.

d. Enter the following information:

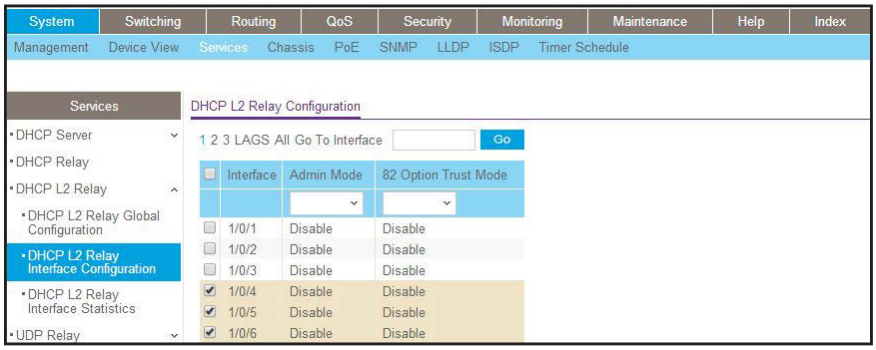
- In the **Admin Mode** field, select **Enable**.
- In the **Circuit ID Mode** field, select **Enable**.
- In the **Remote ID String** field, enter **rmt_id**.

e. Click **Apply** to save the settings.

5. Enable DHCP L2 Relay on interfaces 1/0/4,1/0/5, and 1/0/6.

a. Select **System > Services > DHCP L2 Relay > DHCP L2 Relay Interface Configuration**.

A screen similar to the following displays.



b. Scroll down and select the **1/0/4**, **1/0/5**, and **1/0/6** check boxes.

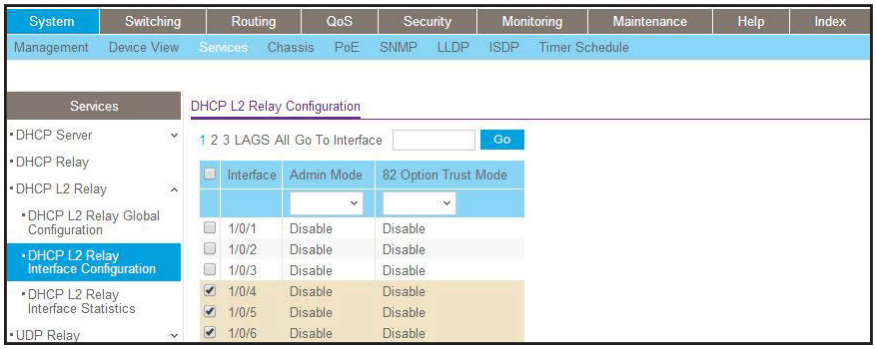
c. In the **Admin Mode** field, select **Enable**.

d. Click **Apply** to save the settings.

6. Enable DHCP L2 relay trust on interface 1/0/6.

a. Select **System > Services > DHCP L2 Relay > DHCP L2 Relay Interface Configuration**.

A screen similar to the following displays.



b. Under DHCP L2 Relay Configuration, scroll down and select the Interface **1/0/6** check box.

c. In the **82 Option Trust Mode** field, select **Enable**.

d. Click **Apply** to save the settings.

DHCP L3 Relay

This example consists of two steps:

- Use a Windows Server operating system to configure a DHCP L3 server.
- Use the CLI to configure a DHCP L3 relay through which a DHCP client can receive an IP address from a DHCP server.

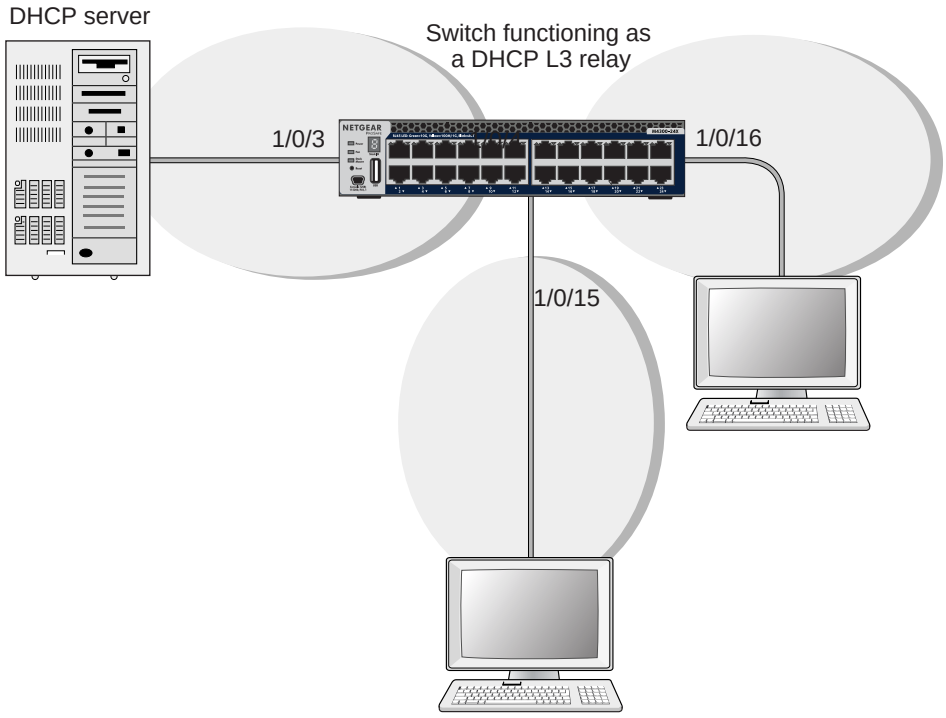
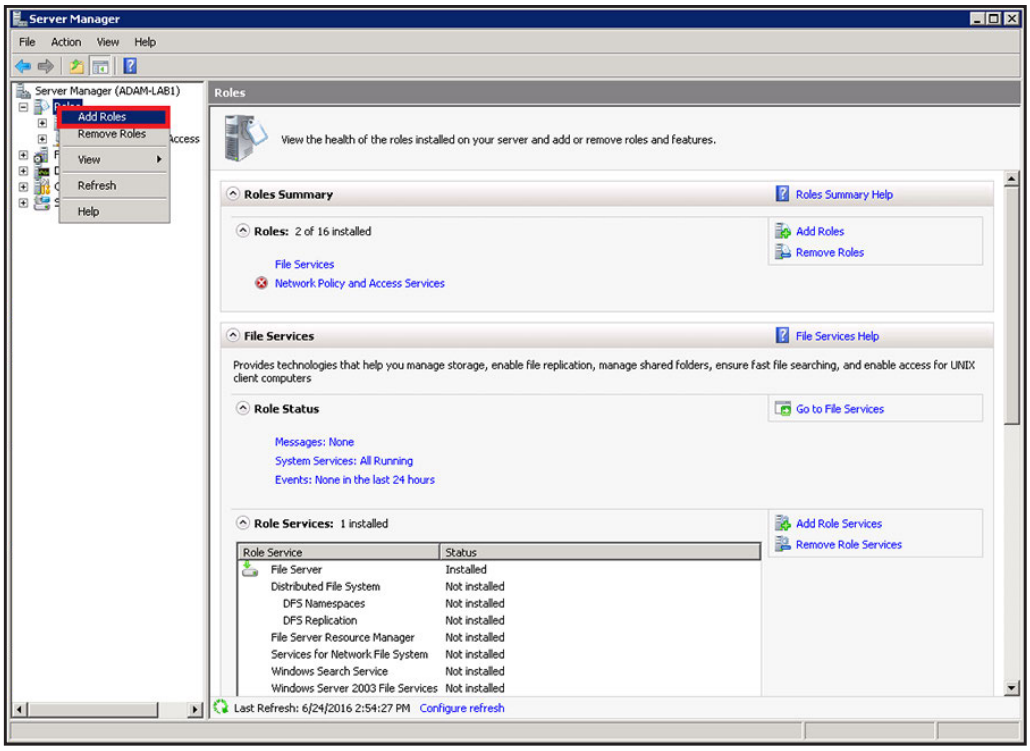


Figure 60. DHCP L3 relay

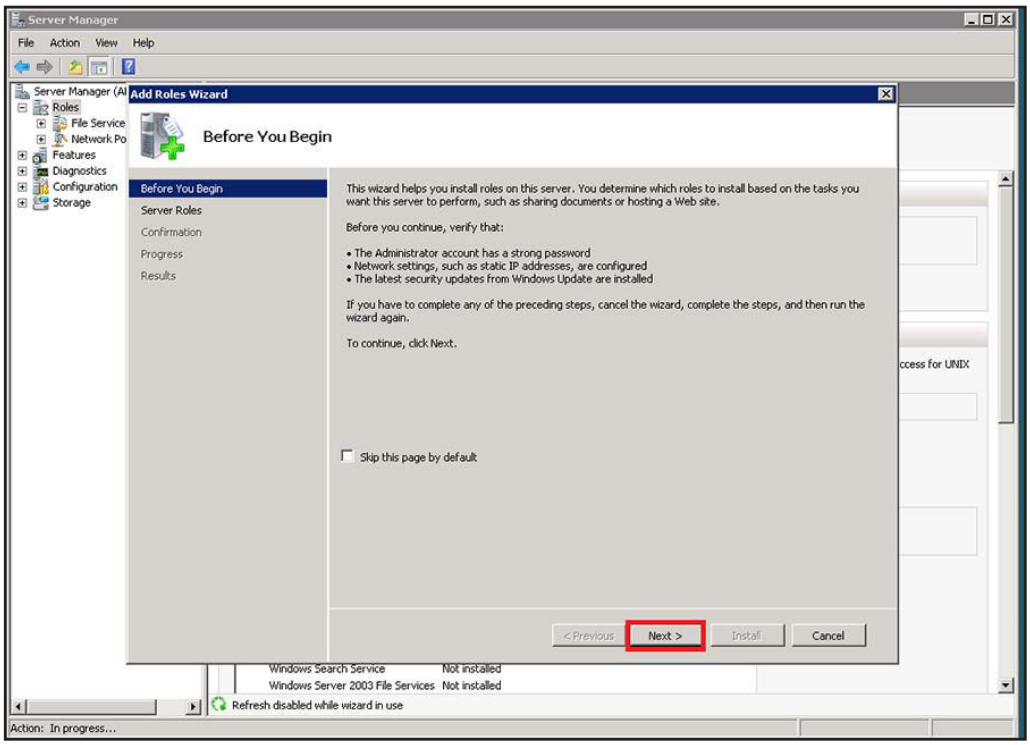
Configure the DHCP L3 Server in a Windows Server Operating System

1. In the Windows Server operating system, open the Server Manager.
2. In the menu tree on the left, click **Roles**.

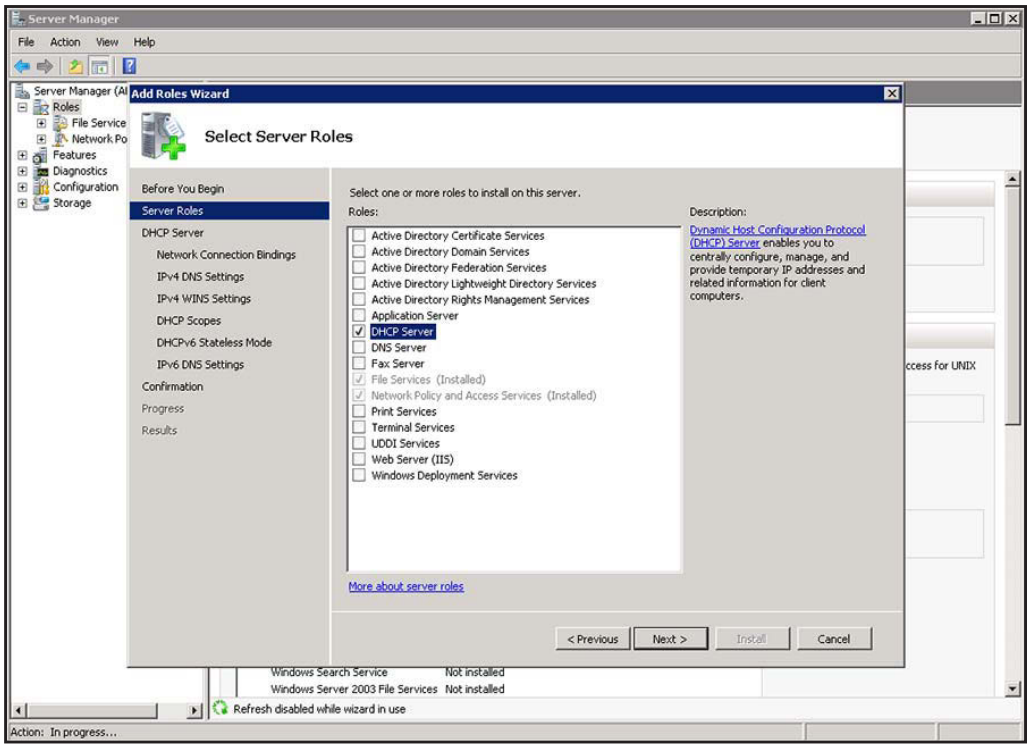


3. In the pop-up menu, select **Add Roles**.

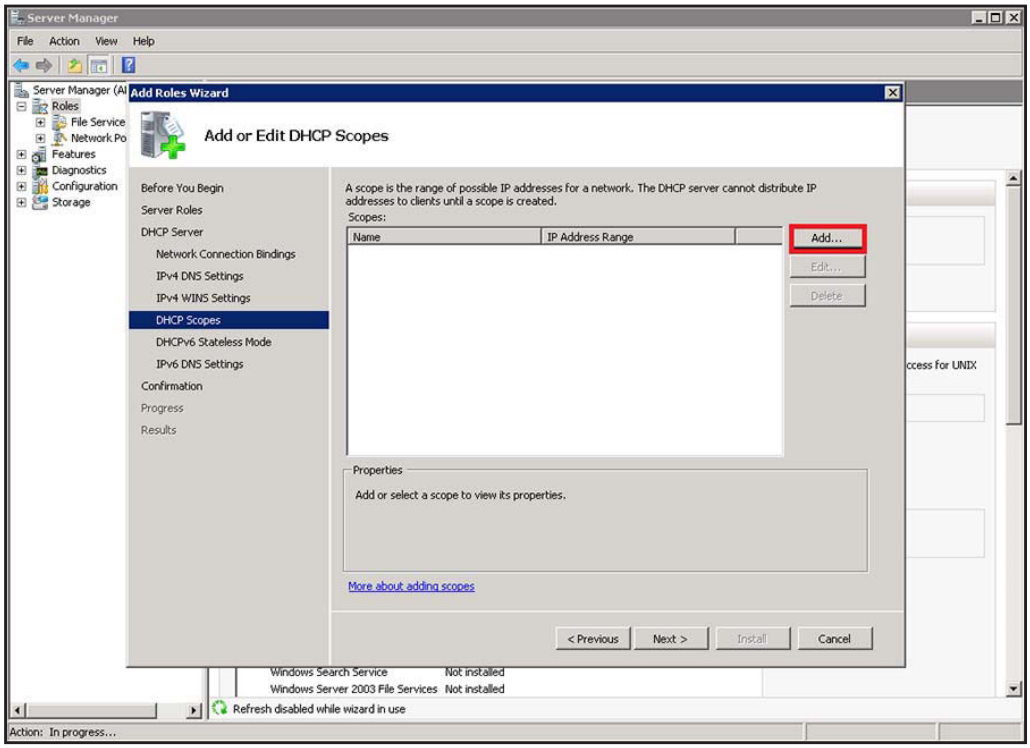
   The Add Roles Wizard starts.



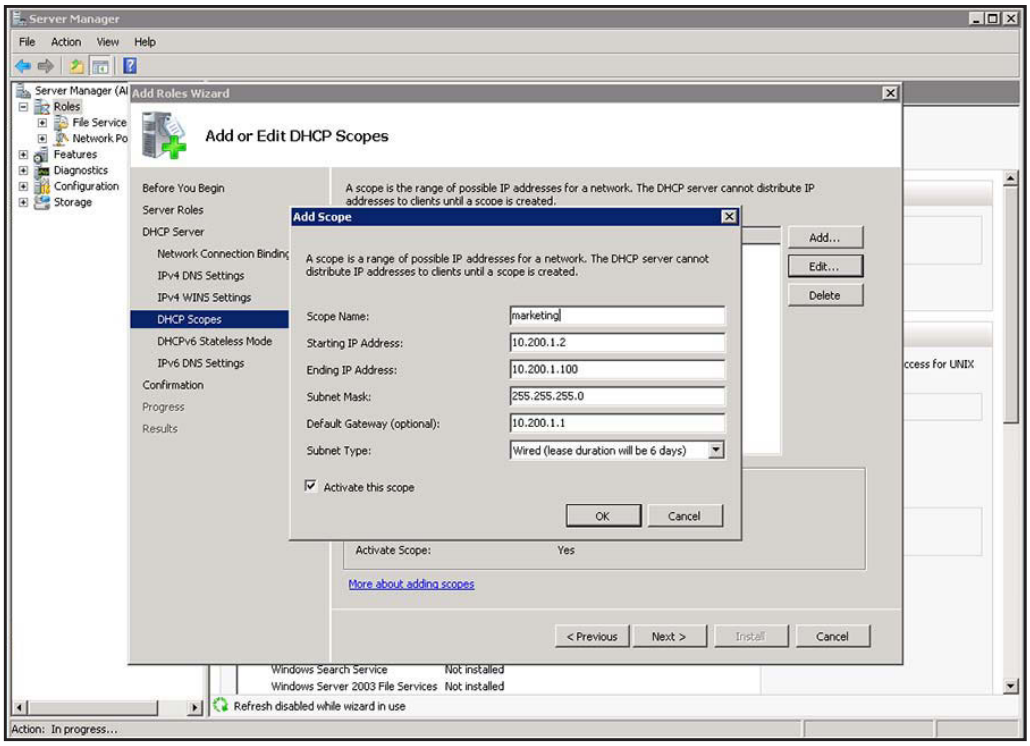
4. Click the **Next** button.



5. Select the **DHCP Server** check box.
6. Click the **Next** button.
7. From the menu on the left, select **DHCP scopes**.



8. Click the **Add** button.



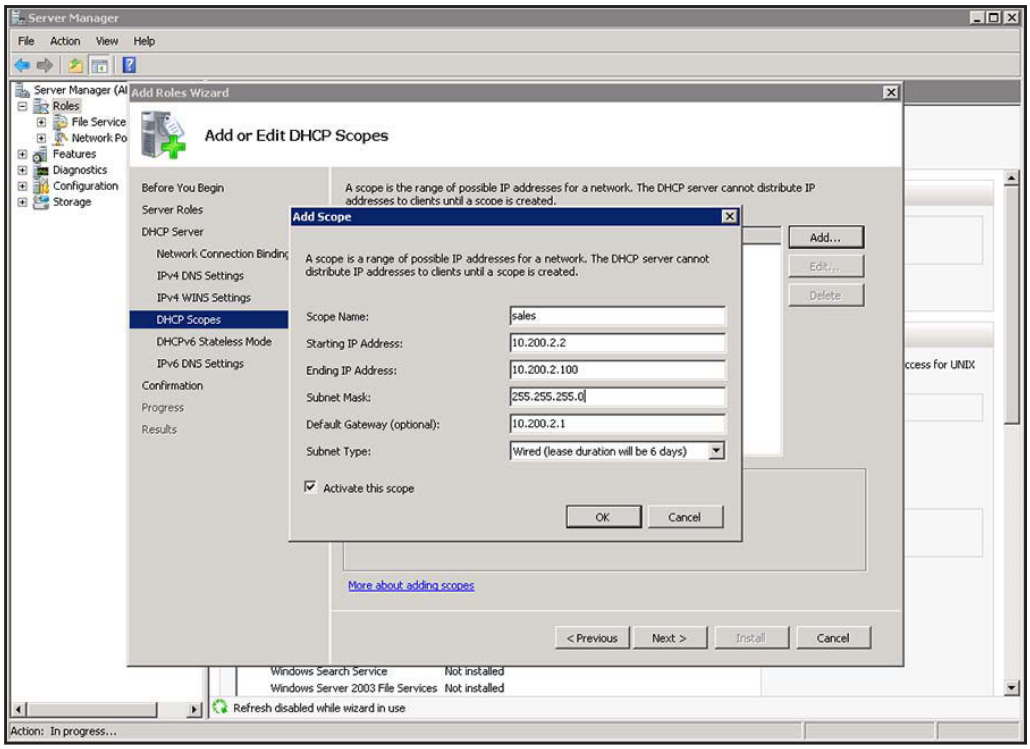
9. In the Add Scope pop-up window, enter the IP address scope information for a marketing scope.

   In this example, an IP address range of 10.200.1.2–10.200.1.100 is used. In the **Default Gateway (optional)** field, an IP address of 10.200.1.1 is used, which is the IP address of the gateway for the DHCP client.

10. Click the **OK** button.

    The scope information is saved.

11. Click the **Add** button.

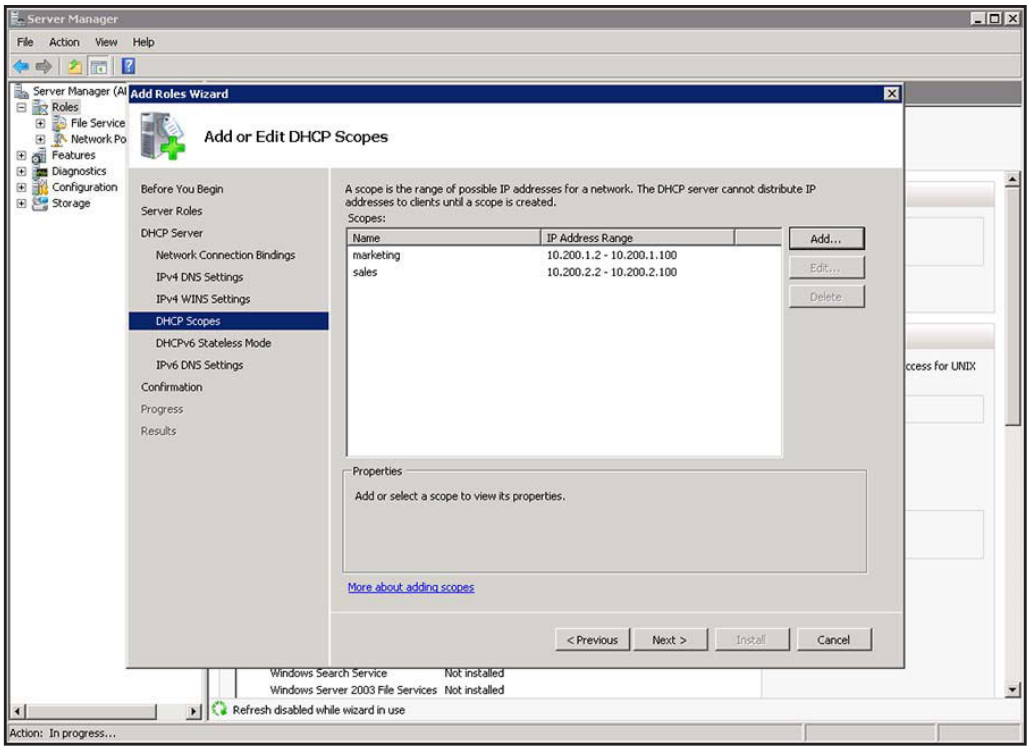


12. In the Add Scope pop-up window, enter the IP address scope information for a sales scope.

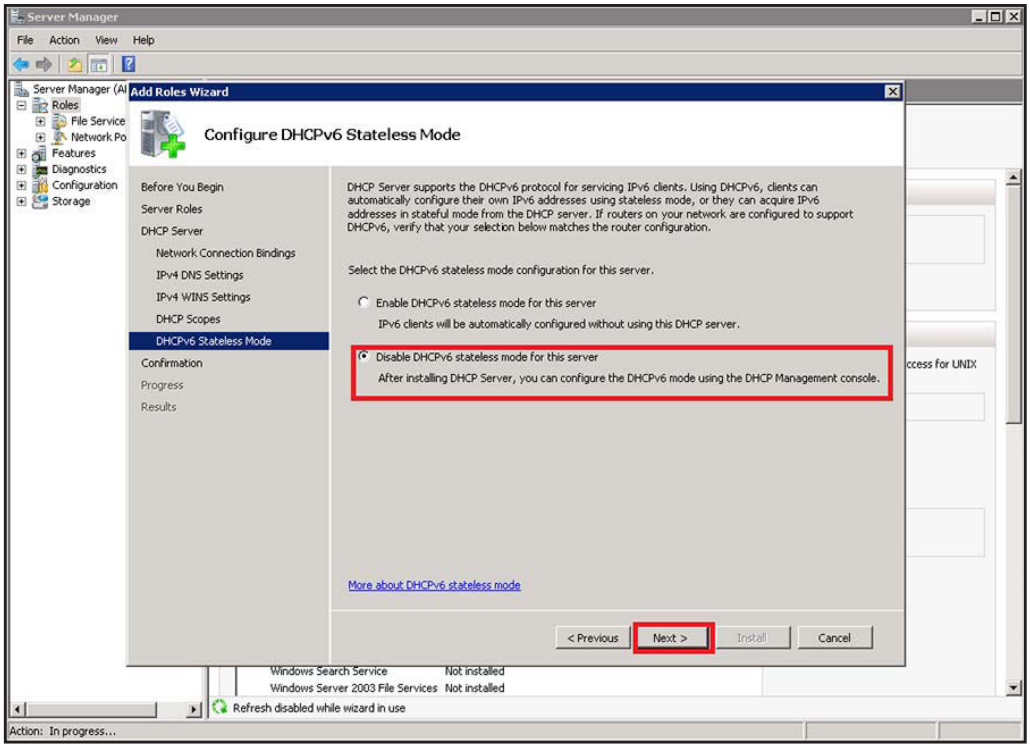
    In this example, an IP address range of 10.200.2.2–10.200.2.100 is used. In the **Default Gateway (optional)** field, an IP address of 10.200.2.1 is used, which is the gateway for the DHCP client.

13. Click the **OK** button.

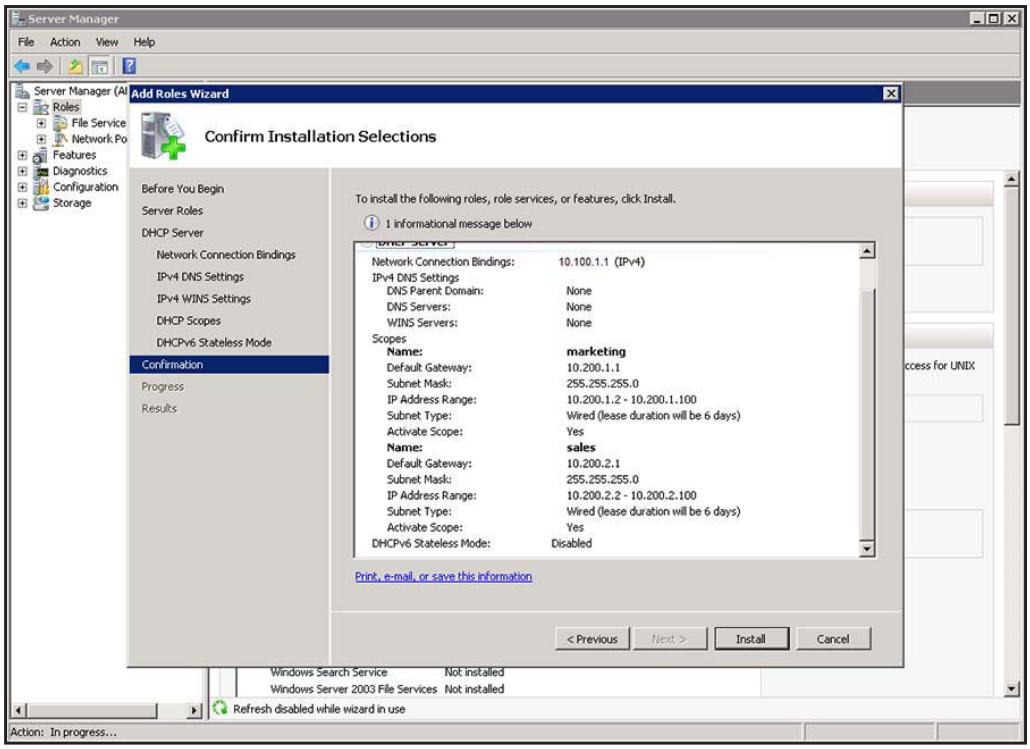
    The scope information is saved.



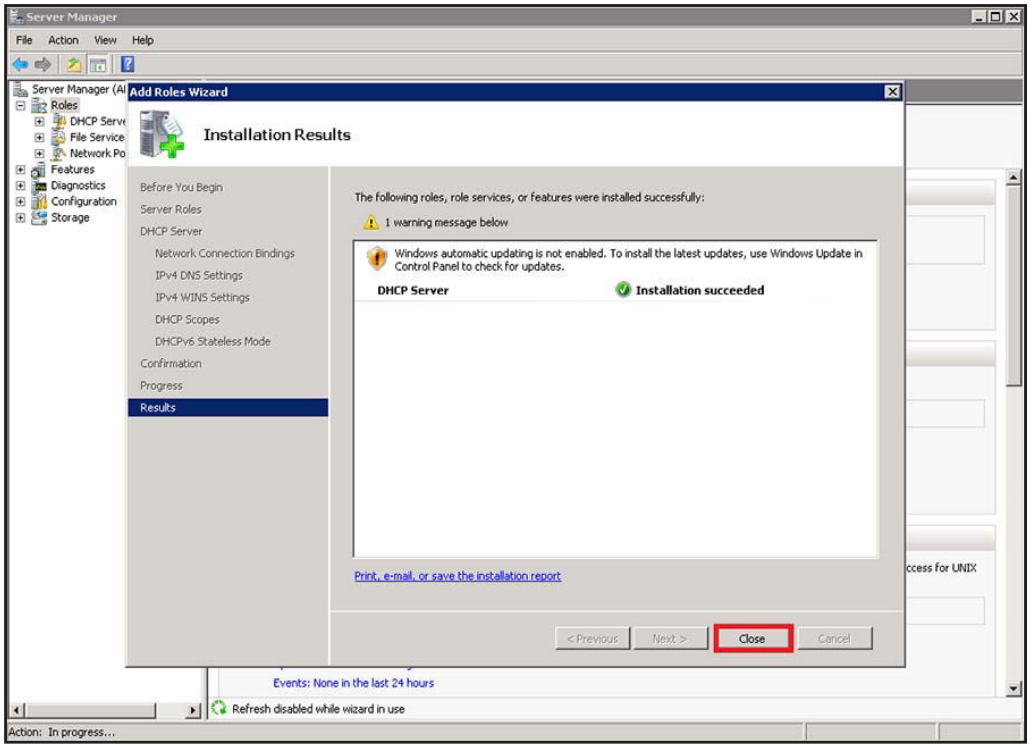
14. Click the **Next** button.



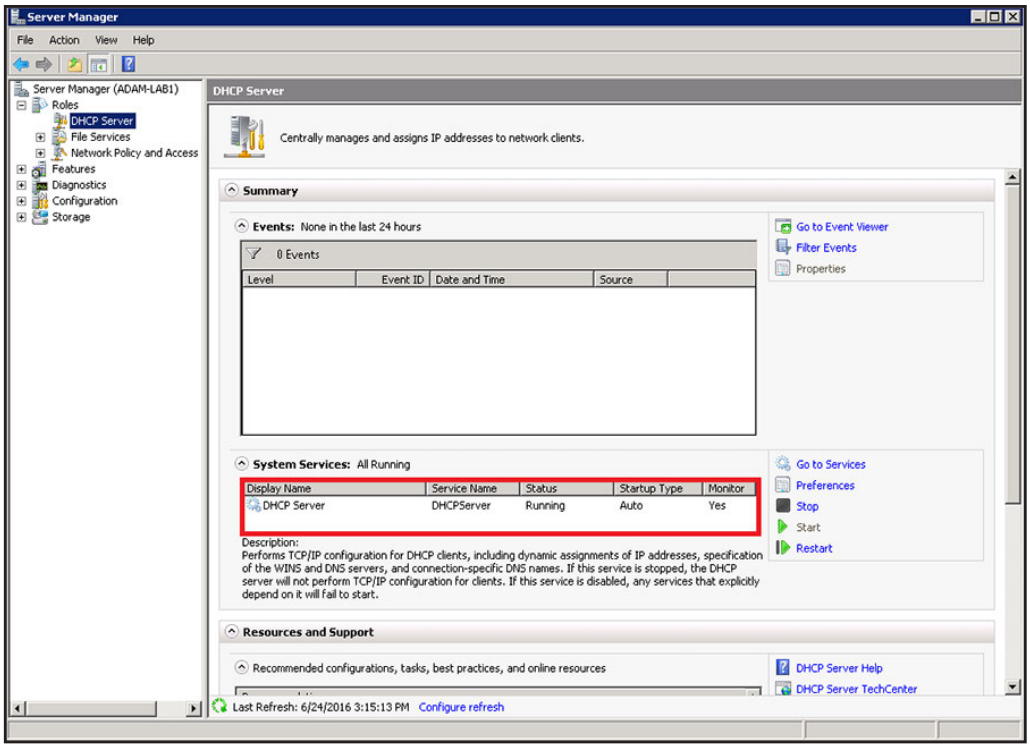
15. Select the **Disable DHCPv6 stateless mode for this server** radio button.
16. Click the **Next** button.



17. Click the **Install** button.



18. Wait for the DHCP server to be installed and the installation process to finish.
19. Click the **Close** button.

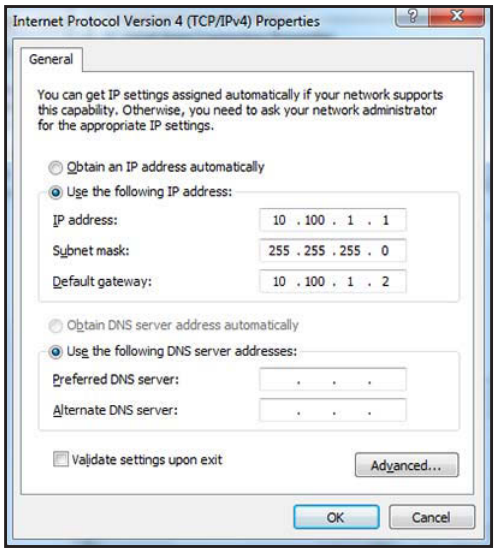


20. Make sure that in the Status column, the field for the DHCP server states Running.

If a computer in the network must receive an IP address in the marketing scope or sales scope, the computer must include a static IP address configuration with the IP address, subnet mask, and gateway address of the gateway that is used for the marketing scope or sales scope.

- **To enable a computer with a Windows operating system to receive an IP address from the gateway for the marketing scope or sales scope, do the following:**

1. Navigate to the properties of the network interface card.
2. Open the Internet Protocol Version 4 (TCP/IPv4) Properties pop-up window.
3. Select the **Use the following IP address** radio button.
4. Configure the IP address, subnet mask, and gateway address for the marketing or sales scope.



Configure a DHCP L3 Switch

CLI: Configure a DHCP L3 Relay

1. Enable routing on the switch.

```
(Netgear Switch) #config
(Netgear Switch) (Config)#ip routing
(Netgear Switch) (Config)#
```

2. Create a routing interface and assign subnet 10.100.1.2/24 to it.

```
(Netgear Switch) (Config)#
(Netgear Switch) (Config)#interface 1/0/4
(Netgear Switch) (Interface 1/0/4)#routing
(Netgear Switch) (Interface 1/0/4)#ip address 10.100.1.2 255.255.255.0
(Netgear Switch) (Interface 1/0/4)#exit
```

3. Create a routing interface connecting to the client.

```
(Netgear Switch) (Config)#
(Netgear Switch) (Config)#Interface 1/0/15
(Netgear Switch) (Interface 1/0/15)#routing
(Netgear Switch) (Interface 1/0/15)#ip address 10.200.1.1 255.255.255.0
(Netgear Switch) (Interface 1/0/15)#exit
(Netgear Switch) (Config)#
(Netgear Switch) (Config)#interface 1/0/16
(Netgear Switch) (Interface 1/0/16)#routing
(Netgear Switch) (Interface 1/0/16)#ip address 10.200.2.1 255.255.255.0
(Netgear Switch) (Interface 1/0/16)#exit
```

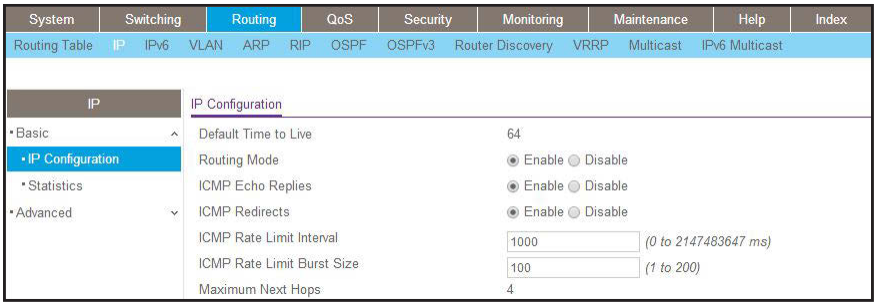
4. Configure the DHCP Server IP address and enable the DHCP L3 relay.

```
(Netgear Switch) (Config)#ip helper-address 10.100.1.1 dhcp
(Netgear Switch) (Config)#ip helper enable
```

Web Interface: Configure a DHCP L3 Relay

1. Enable routing mode on the switch.
   a. Select **Routing > IP > Basic > IP Configuration**.

      A screen similar to the following displays.



   b. For Routing Mode, select the **Enable** radio button.
   c. Click **Apply**.
2. Create a routing interface and assign 10.100.1.2/24 to it.
   a. Select **Routing > IP > Advanced > IP Interface Configuration**.

A screen similar to the following displays.

b. Scroll down and select the Port **1/0/4** check box.

c. In the **IP Address** field, enter **10.100.1.2**.

d. In the **Subnet Mask** field, enter **255.255.255.0**.

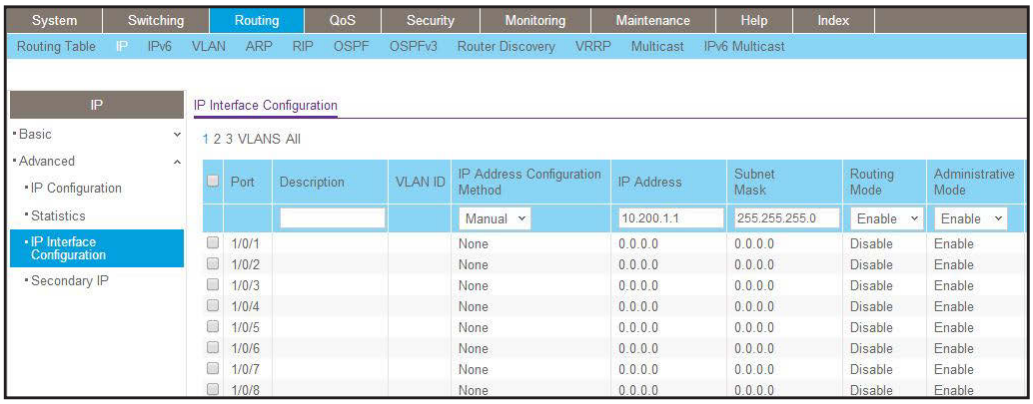
e. In the **Routing Mode** field, select **Enable**.

f. Click **Apply** to save the settings.

3. Create a routing interface and assign 10.200.1.1/24 to it.

a. Select **Routing > IP > Advanced > IP Interface Configuration**.

A screen similar to the following displays.



b. Under IP Interface Configuration, scroll down and select the Port **1/0/15** check box.

c. In the **IP Address Configuration Method** field, enter **Manual**.

d. In the **IP Address** field, enter **10.200.1.1**.

e. In the **Subnet Mask** field, enter **255.255.255.0**.

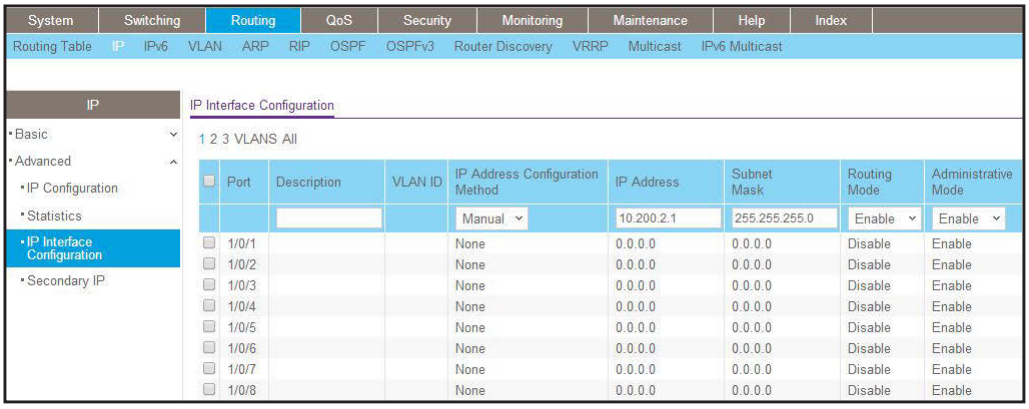
f. In the **Routing Mode** field, select **Enable**.

g. Click **Apply** to save the settings.

4. Create a routing interface and assign 10.200.2.1/24 to it.

a. Select **Routing > IP > Advanced > IP Interface Configuration**.

A screen similar to the following displays.



b. Under IP Interface Configuration, scroll down and select the Port **1/0/16** check box.

c. In the IP Address Configuration Method field, enter **Manual**.

d. In the IP Address field, enter **10.200.2.1**.

e. In the Subnet Mask field, enter **255.255.255.0**.

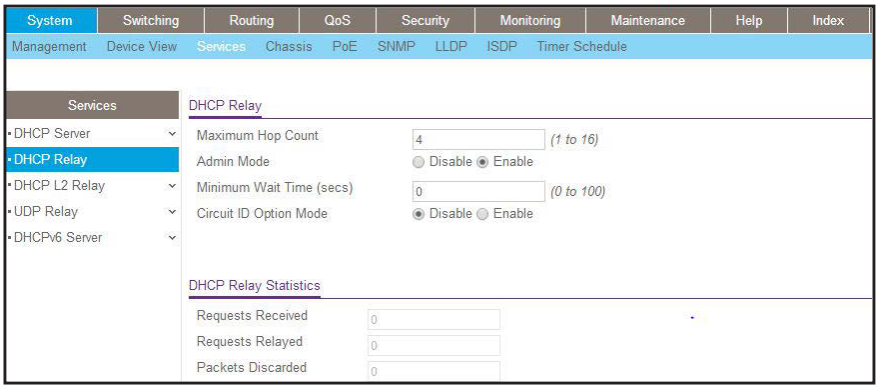
f. In the Routing Mode field, select **Enable**.

g. Click **Apply** to save the settings.

5. Enable DHCP L3 relay.

a. Select **System > Services > DHCP Relay**.

A screen similar to the following displays.



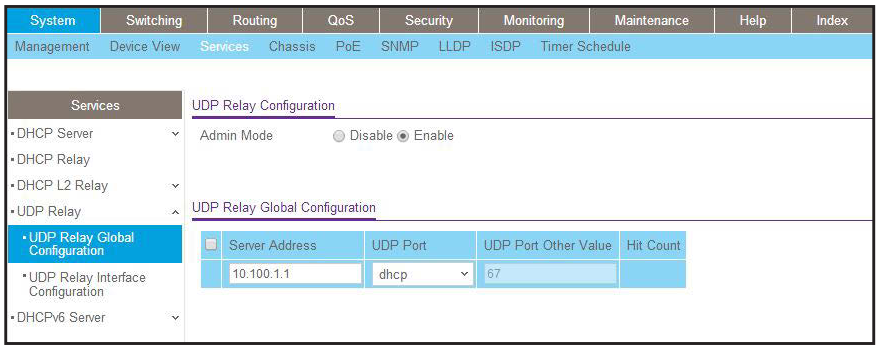
b. For Admin Mode, select the **Enable** radio button.

c. Click **Apply** to save the settings.

6. Configure the DHCP server IP address.

a. Select **System > Services > UDP Relay**.

A screen similar to the following displays.



b. In the **Server Address** field, enter **10.100.1.1**.

c. In the **UDP Port** field, enter **dhcp**.

d. Click **Add** to save the settings.

MLD

32

Multicast Listener Discovery

This chapter includes the following sections:

- *Multicast Listener Discovery Concepts*
- *Configure MLD*
- *MLD Snooping*

Note: MLD is available on the M4300 series switches only.

Multicast Listener Discovery Concepts

Multicast Listener Discovery (MLD) protocol enables IPv6 routers to discover multicast listeners, the nodes that are configured to receive multicast data packets, on its directly attached interfaces. The protocol specifically discovers which multicast addresses are of interest to its neighboring nodes and provides this information to the active multicast routing protocol that determines the flow of multicast data packets.

Periodically, the multicast router sends general queries requesting multicast address listener information from systems on an attached network. These queries are used to build and refresh the multicast address listener state on the attached networks. In response to the queries, multicast listeners reply with membership reports. These membership reports specify their multicast addresses listener state and their desired set of sources with current-state multicast address records.

The multicast router also processes unsolicited filter- mode-change records and source-list-change records from systems that want to indicate interest in receiving or not receiving traffic from particular sources.

Configure MLD

In this case, PIM-DM is enabled on Switch A and Switch B, and MLD is enabled on Switch B’s port 1/0/24 to discover the multicast listeners.

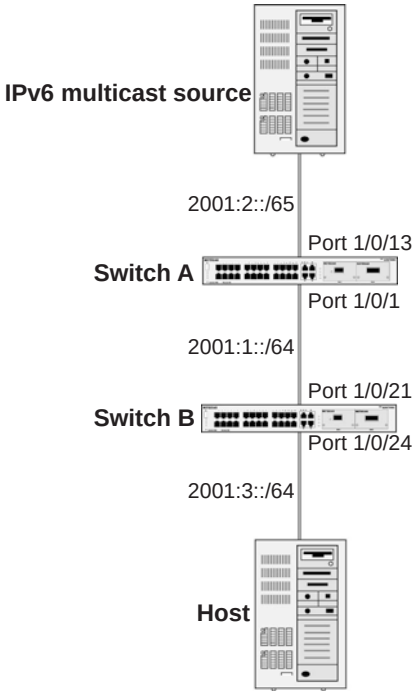


Figure 61. Configure MLD

CLI: Configure MLD

MLD on Switch A

```
(Netgear Switch) #configure
(Netgear Switch) (Config)#ipv6 router ospf
(Netgear Switch) (Config-rtr)#router-id 1.1.1.1
(Netgear Switch) (Config)#exit
```

```
(Netgear Switch) (Config)#ipv6 unicast-routing
(Netgear Switch) (Config)#ipv6 pim dense
(Netgear Switch) (Config)#ip routing
(Netgear Switch) (Config)#ip multicast
(Netgear Switch) (Config)#interface 1/0/1
(Netgear Switch) (Interface 1/0/1)#routing
(Netgear Switch) (Interface 1/0/1)#ipv6 address 2001:1::1/64
(Netgear Switch) (Interface 1/0/1)#ipv6 enable
(Netgear Switch) (Interface 1/0/1)#ipv6 pim
(Netgear Switch) (Interface 1/0/1)#ipv6 ospf
(Netgear Switch) (Interface 1/0/1)#exit

(Netgear Switch) (Config)#interface 1/0/13
(Netgear Switch) (Interface 1/0/13)#routing
(Netgear Switch) (Interface 1/0/13)#ipv6 address 2001:2::1/64
(Netgear Switch) (Interface 1/0/13)#ipv6 enable
(Netgear Switch) (Interface 1/0/13)#ipv6 pim
(Netgear Switch) (Interface 1/0/13)#ipv6 ospf
(Netgear Switch) (Interface 1/0/13)#exit
```

MLD on Switch B

1. Enable OSPFv3 to build a unicast route table.

```
(Netgear Switch)#configure
(Netgear Switch) (Config)#ipv6 router ospf
(Netgear Switch) (Config-rtr)#router-id 2.2.2.2
(Netgear Switch) (Config)#exit
```

2. Enable IPV6 unicast routing on the switch.

```
(Netgear Switch) (Config)#ipv6 unicast-routing
```

3. Enable IPV6 MLD on the switch.

```
(Netgear Switch) (Config)#ipv6 mld router
```

4. Enable IPV6 PIM-DM on the switch.

```
(Netgear Switch) (Config)#ipv6 pim dense
```

5. Enable IP multicast forwarding on the switch.

```
(Netgear Switch) (Config)#ip routing
(Netgear Switch) (Config)#ip multicast
```

6. Enable MLD on interface 1/0/24.

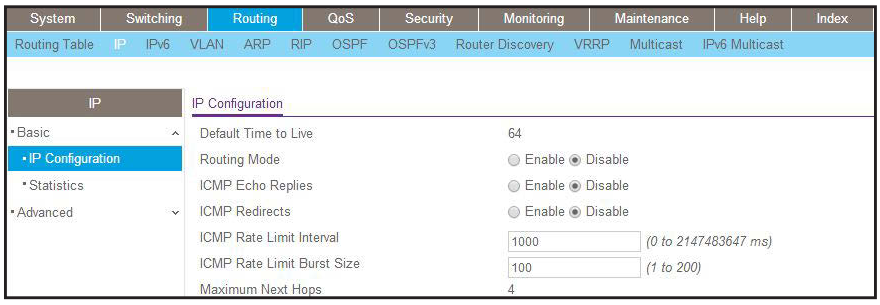
```
(Netgear Switch) (Config)#interface 1/0/21
(Netgear Switch) (Interface 1/0/21)#routing
(Netgear Switch) (Interface 1/0/21)#ipv6 address 2001:1::2/64
(Netgear Switch) (Interface 1/0/21)#ipv6 enable
(Netgear Switch) (Interface 1/0/21)#ipv6 pim
(Netgear Switch) (Interface 1/0/21)#ipv6 ospf
(Netgear Switch) (Interface 1/0/21)#exit

(Netgear Switch) (Config)#interface 1/0/24
(Netgear Switch) (Interface 1/0/24)#routing
(Netgear Switch) (Interface 1/0/24)#ipv6 address 2001:3::1/64
(Netgear Switch) (Interface 1/0/24)#ipv6 enable
(Netgear Switch) (Interface 1/0/24)#ipv6 mld router

(Netgear Switch) (Interface 1/0/24)#ipv6 pim
(Netgear Switch) (Interface 1/0/24)#exit

The MLD group information on switch B:
(B) #show ipv6 mld groups ff32::1

Interface..................................... 71/1/24
Group Address................................. FF32::1
Last Reporter................................. FE80::200:4FF:FEE8:5EFC
Up Time (hh:mm:ss)............................ 00:00:18
Expiry Time (hh:mm:ss)........................ ------
Filter Mode................................... Include
Version1 Host Timer........................... ------
Group compat mode............................. v2
Source Address    ExpiryTime
-----------------  -----------
  2001:2::2       00:04:02
```

Web Interface: Configure MLD

MLD on Switch A

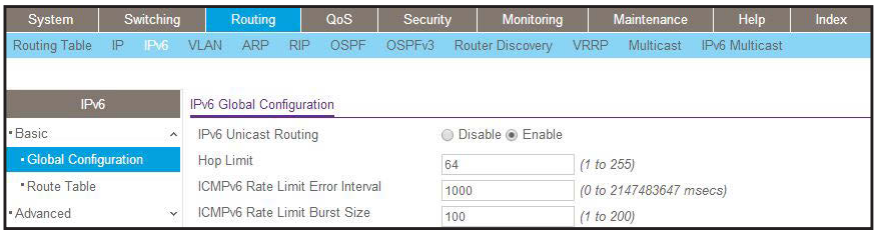
1. Enable IP routing on the switch.
   a. Select **Routing > IP > Basic > IP Configuration**.

      A screen similar to the following displays.



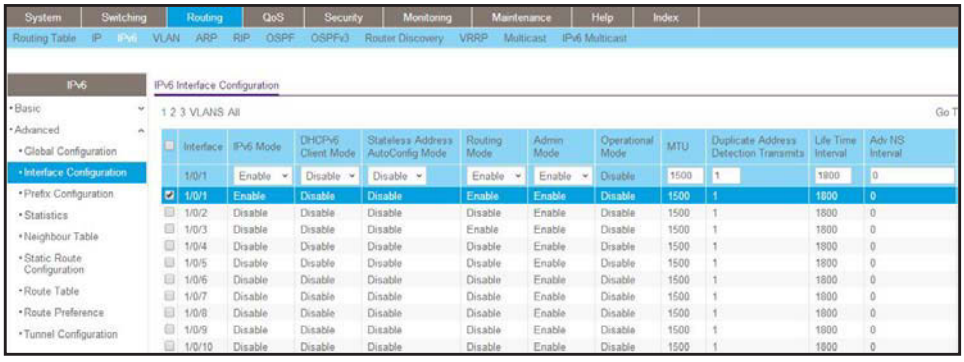
   b. For Routing Mode, select the **Enable** radio button.
   c. Click **Apply**.
2. Enable IPv6 unicast routing on the switch.
   a. Select **Routing > IPv6 > Basic > Global Configuration**.

      A screen similar to the following displays.



   b. For IPv6 Unicast Routing, select the **Enable** radio button.
   c. Click **Apply**.
3. Configure 1/0/1 and 1/0/13 as a IPv6 routing ports.
   a. Select **Routing > IPv6 > Advanced > Interface Configuration**.

      A screen similar to the following displays.



b. Scroll down and select the Interface **1/0/1** and **1/0/13** check boxes.

c. Enter the following information:

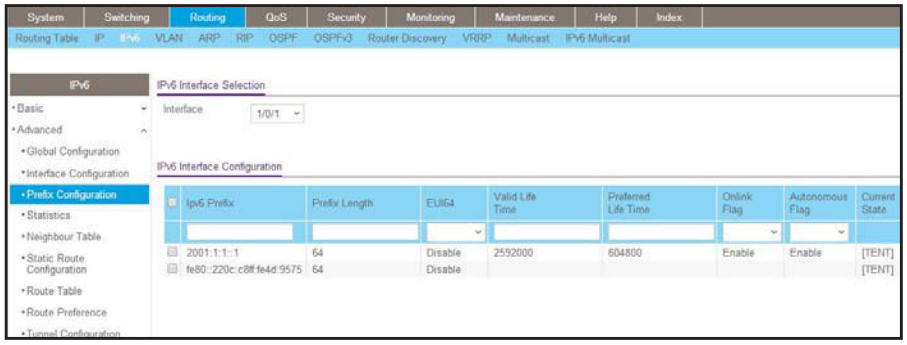
- In the **IPv6 Mode** field, select **Enable**.
- In the **Routing Mode** field, select **Enable**.
- In the **Admin Mode** field, select **Enable**.

d. Click **Apply** to save the settings.

4. Assign an IPv6 address to 1/0/1.

a. Select **Routing > IPv6 > Advanced > Prefix Configuration**.

A screen similar to the following displays.



b. In the Interface field, select **1/0/1**.

c. Enter the following information:

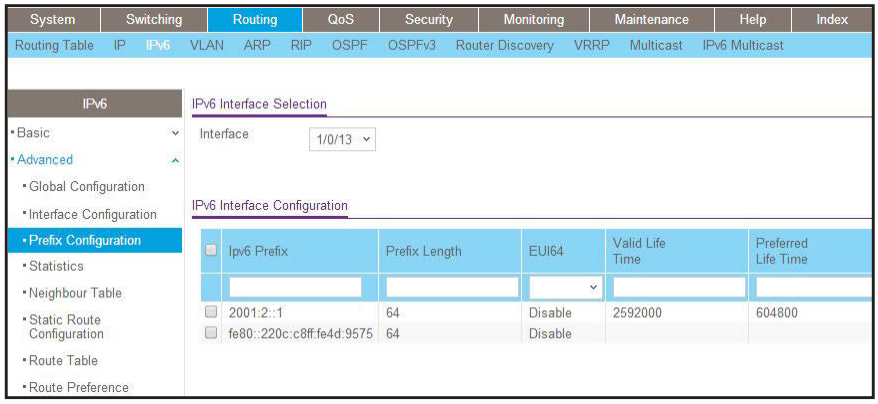
- In the **IPv6 Prefix** field, enter **2001:1::1**.
- In the **Prefix Length** field, enter **64**.
- In the **EUI64** field, select **Disable**.

d. Click **Add** to save the settings.

5. Assign an IPv6 address to 1/0/13.

a. Select **Routing > IPv6 > Advanced > Prefix Configuration**.

A screen similar to the following displays.



b. Select Interface **1/0/13**.

c. Enter the following information:
   - In the **IPv6 Prefix** field, enter **2001:2::1**.
   - In the **Prefix Length** field, enter **64**.
   - In the **EUI64** field, select **Disable**.

d. Click **Add** to save the settings.

6. Configure the router ID of OSPFv3.

a. Select **Routing > OSPFv3 > Basic > OSPFv3 Configuration**.

A screen similar to the following displays.

b. In the **Router ID** field, enter **1.1.1.1**.

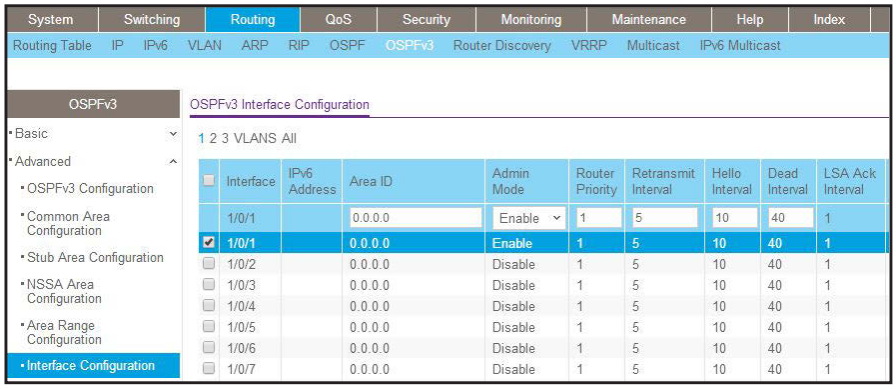
c. For Admin Mode, select the **Enable** radio button.

d. Click **Apply**.

7. Enable OSPFv3 on interfaces 1/0/1 and 1/0/13.

a. Select **Routing > OSPFv3 > Advanced > Interface Configuration**.

A screen similar to the following displays.



b. Scroll down and select the Interface **1/0/1** and **1/0/13** check boxes.

c. In the **Admin Mode** field, select **Enable**.

d. Click **Apply** to save the settings.

8. Enable multicast globally.

a. Select **Routing > Multicast > Global Configuration**.

A screen similar to the following displays.

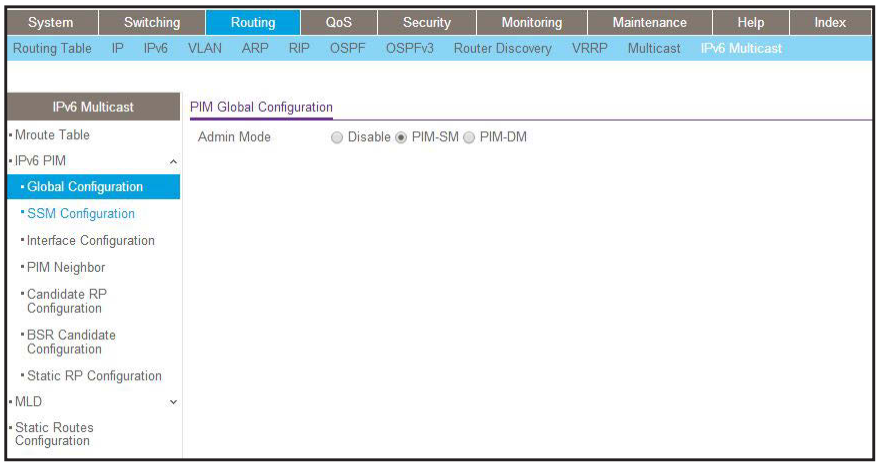
b. For Admin Mode, select the **Enable** radio button.

c. Click **Apply**.

9. Enable PIM-DM globally.

a. Select **Routing > IPv6 Multicast > IPv6 PIM > Global Configuration**.

A screen similar to the following displays.



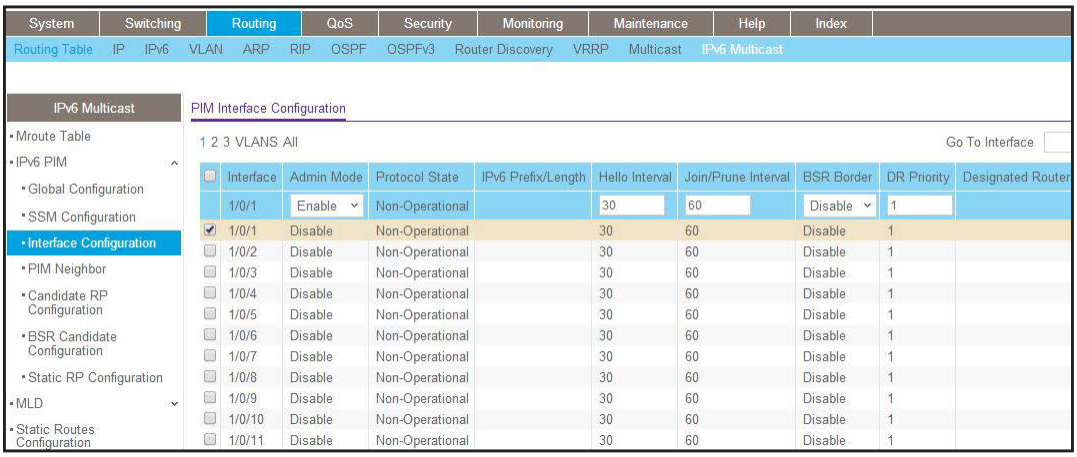
b. For Admin Mode, select the **Enable** radio button.

c. Click **Apply**.

10. Enable PIM-DM on interfaces 1/0/1 and 1/0/13.

a. Select **Routing > IPv6 Multicast > IPv6 PIM > Interface Configuration**.

A screen similar to the following displays.



b. Scroll down and select the Interface **1/0/1** and **1/0/13** check boxes.

c. In the **Admin Mode** field, select **Enable**.

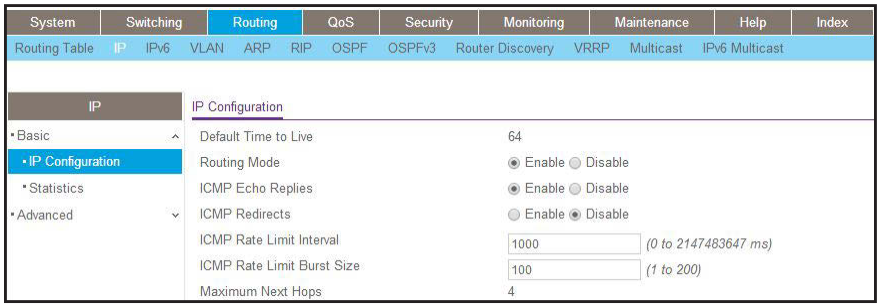
d. Click **Apply** to save the settings.

MLD on Switch B

1. Enable IP routing on the switch.

   a. Select **Routing > IP > Basic > IP Configuration**.

   A screen similar to the following displays.



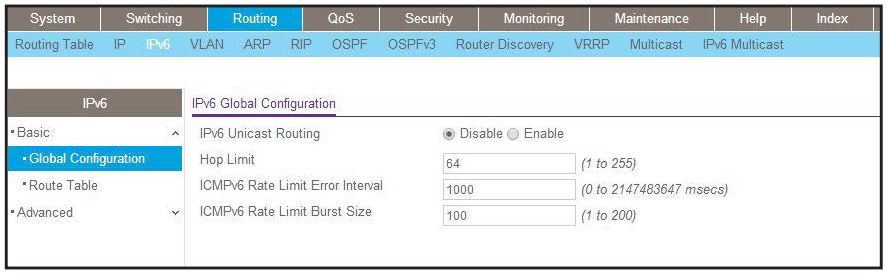
   b. For Routing Mode, select the **Enable** radio button.

   c. Click **Apply**.

2. Enable IPv6 unicast routing on the switch.

   a. Select **Routing > IPv6 > Basic > Global Configuration**.

A screen similar to the following displays.



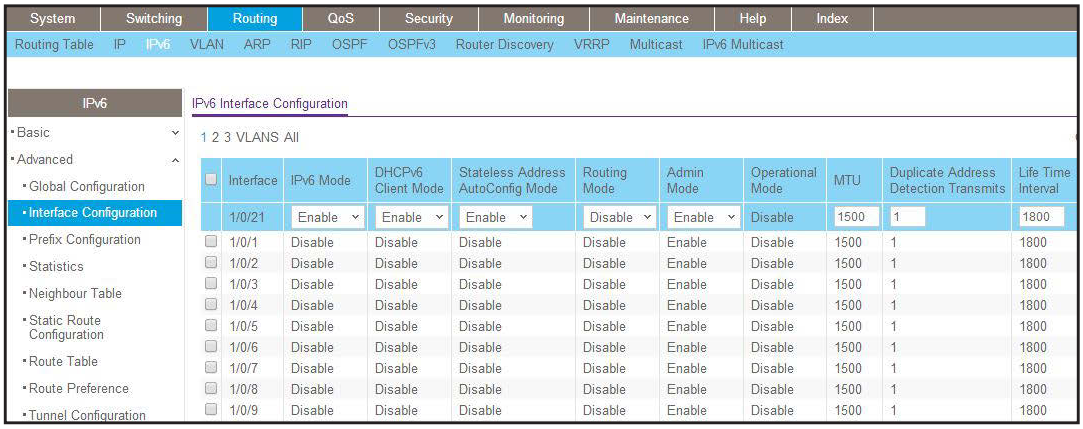
b. For IPv6 Unicast Routing, select the **Enable** radio button.

c. Click **Apply**.

3. Configure 1/0/21 and 1/0/24 as IPv6 routing ports.

a. Select **Routing > IPv6 > Advanced > Interface Configuration**.

A screen similar to the following displays.



b. Scroll down and select the Interface **1/0/21** and **1/0/24** check boxes.

c. Enter the following information:

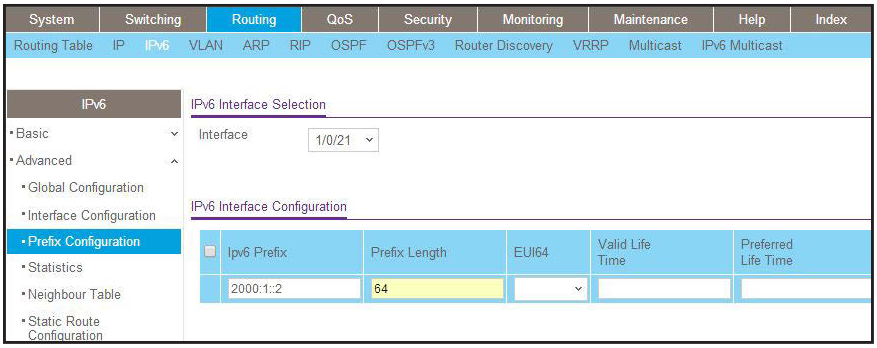
- In the I**Pv6 Mode** field, select **Enable**.
- In the **Routing Mode** field, select **Enable**.
- In the **Admin Mode** field, select **Enable**.

d. Click **Apply** to save the settings.

4. Assign an IPv6 address to 1/0/21.

a. Select **Routing > IPv6 > Advanced > Prefix Configuration**.

A screen similar to the following displays.



b. In the Interface field, select **1/0/21**.

c. Enter the following information:

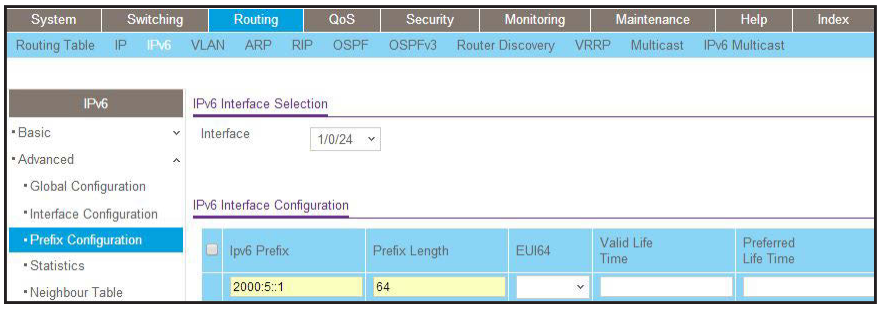
- In the **IPv6 Prefix** field, enter **2001:1::2**.
- In the **Prefix Length** field, enter **64**.
- In the **EUI64** field, select **Disable**.

d. Click **Add** to save the settings.

5. Assign an IPv6 address to 1/0/24.

a. Select **Routing > IPv6 > Advanced > Prefix Configuration**.

A screen similar to the following displays.



b. Under IPv6 Interface Selection, in the **Interface** field, select **1/0/24**.

c. Enter the following information:

- In the **IPv6 Prefix** field, enter **2001:3::1**.
- In the **Prefix Length** field, enter **64**.
- In the **EUI64** field, select **Disable**.

d. Click **Add** to save the settings.

6. Configure the router ID of OSPFv3.

a. Select **Routing > OSPFv3 > Basic > OSPFv3 Configuration**.

A screen similar to the following displays.

b. In the **Router ID** field, enter **2.2.2.2**.

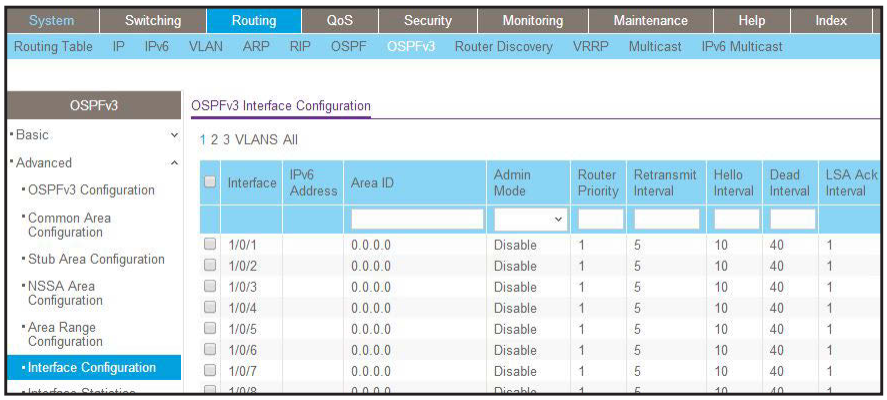
c. For Admin Mode, select the **Enable** radio button.

d. Click **Apply**.

7. Enable OSPFv3 on interfaces 1/0/21 and 1/0/24.

a. Select **Routing > OSPFv3 > Advanced > Interface Configuration**.

A screen similar to the following displays.



b. Under OSPFv3 Interface Configuration, scroll down and select the Interface **1/0/21** and **1/0/24** check boxes.

c. In the OSPFv3 Interface Configuration, in the **Admin Mode** field, select **Enable**.

d. Click **Apply** to save the settings.

8. Enable multicast globally.

a. Select **Routing > Multicast > Global Configuration**.

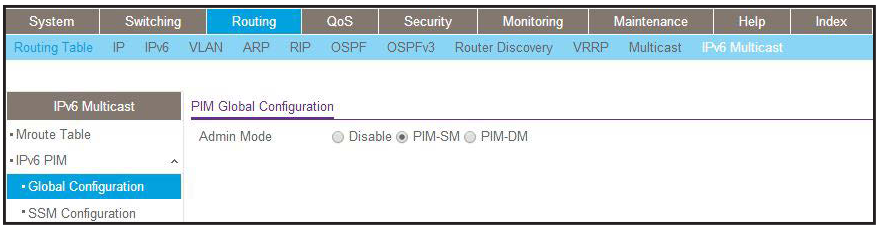
A screen similar to the following displays.

b. For Admin Mode, select the **Enable** radio button.

c. Click **Apply**.

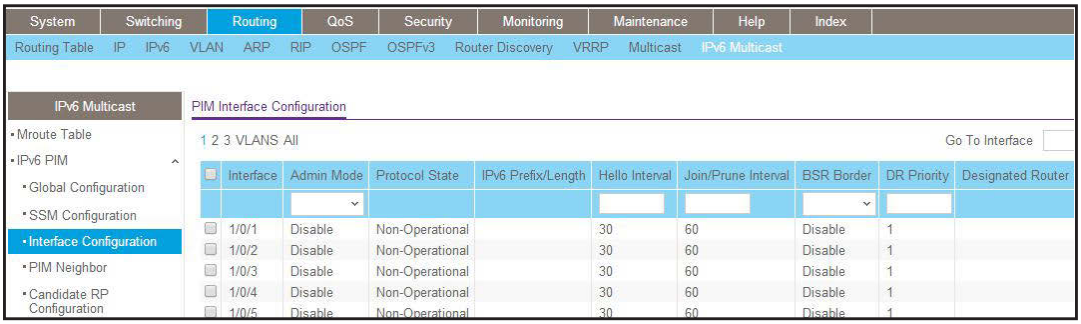
9. Enable PIM-DM globally.
   a. Select **Routing > IPv6 Multicast > IPv6PIM > Global Configuration**.

      A screen similar to the following displays.



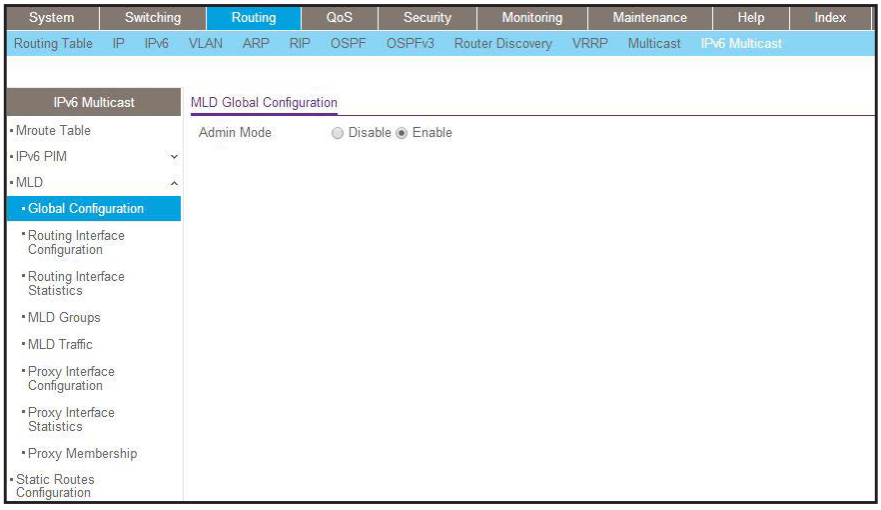
   b. For Admin Mode, select the **Enable** radio button.
   c. Click **Apply**.
10. Enable PIM-DM on interfaces 1/0/21 and 1/0/24.
   a. Select **Routing > IPv6 Multicast > IPv6 PIM > Interface Configuration**.

      A screen similar to the following displays.



   b. Under PIM Interface Configuration, scroll down select the Interface **1/0/21** and **1/0/24** check boxes.
   c. In the **Admin Mode** field, select **Enable**.
   d. Click **Apply** to save the settings.
11. Enable MLD on the switch.
   a. Select **Routing > IPv6 Multicast > MLD > Global Configuration**.

A screen similar to the following displays.



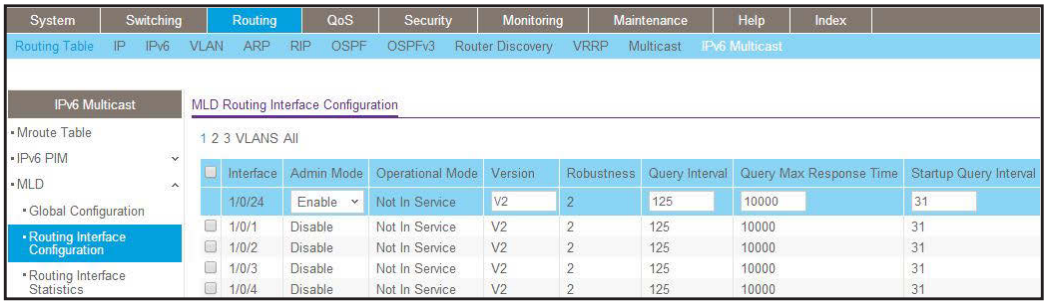
b. For Admin Mode, select the **Enable** radio button.

c. Click **Apply**.

12. Enable MLD on interface 1/0/24.

a. Select **Routing > IPv6 Multicast > MLD > Routing Interface Configuration**.

A screen similar to the following displays.



b. Under MLD Routing Interface Configuration, scroll down and select the **1/0/24** check box.

Now 1/0/24 appears in the Interface field at the top.

c. In the **Admin Mode** field, select **Enable**.

d. Click **Apply**.

MLD Snooping

In IPv4, Layer 2 switches can use IGMP snooping to limit the flooding of multicast traffic by dynamically configuring Layer 2 interfaces so that multicast traffic is forwarded to only those interfaces associated with IP multicast address. In IPv6, MLD snooping performs a similar function. With MLD snooping, IPv6 multicast data is selectively forwarded to a list of ports

that want to receive the data, instead of being flooded to all ports in a VLAN. This list is constructed by snooping IPv6 multicast control packets.

MLD is a protocol used by IPv6 multicast routers to discover the presence of multicast listeners (nodes configured to receive IPv6 multicast packets) on its directly attached links and to discover which multicast packets are of interest to neighboring nodes. MLD is derived from IGMP; MLD version 1 (MLDv1) is equivalent to IGMPv2, and MLD version 2 (MLDv2) is equivalent to IGMPv3. MLD is a subprotocol of Internet Control Message Protocol version 6 (ICMPv6), and MLD messages are a subset of ICMPv6 messages, identified in IPv6 packets by a preceding Next Header value of 58.

The switch can snoop on both MLDv1 and MLDv2 protocol packets and bridge IPv6 multicast data based on destination IPv6 multicast MAC addresses. The switch can be configured to perform MLD snooping and IGMP snooping simultaneously.

CLI: Configure MLD Snooping

1. Enter the following commands.

```
(Netgear Switch) #vlan da
(Netgear Switch) (Vlan)#vlan 300
(Netgear Switch) (Vlan)#exit
(Netgear Switch) #config
(Netgear Switch) (Config)#interface 1/0/1
(Netgear Switch) (Interface 1/0/1)#vlan participation include 300
(Netgear Switch) (Interface 1/0/1)#vlan pvid 300
(Netgear Switch) (Interface 1/0/1)#exit
(Netgear Switch) (Config)#interface 1/0/24
(Netgear Switch) (Interface 1/0/24)#vlan participation include 300
(Netgear Switch) (Interface 1/0/24)#vlan pvid 300
(Netgear Switch) (Interface 1/0/24)#exit
(Netgear Switch) (Config)#exit
(Netgear Switch) (Config)#set mld
(Netgear Switch) (Config)#exit
(Netgear Switch) #vlan database
(Netgear Switch) (Vlan)#set mld 300
(Netgear Switch) (Vlan)#exit
```

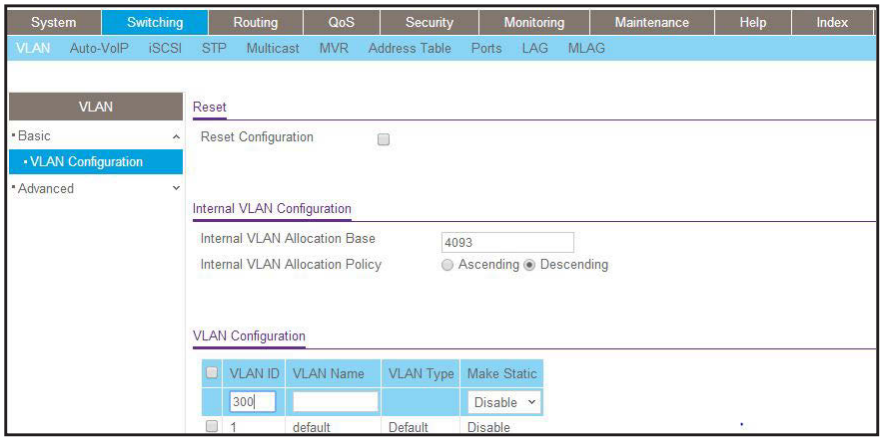
2. Enable MLD snooping on VLAN 300.

```
(Netgear Switch) #show mldsnooping
Admin Mode..................................... Enable
Multicast Control Frame Count.................. 0
Interfaces Enabled for MLD Snooping............ None
VLANs enabled for MLD snooping................. 300
(Netgear Switch) #
```

Web Interface: Configure MLD Snooping

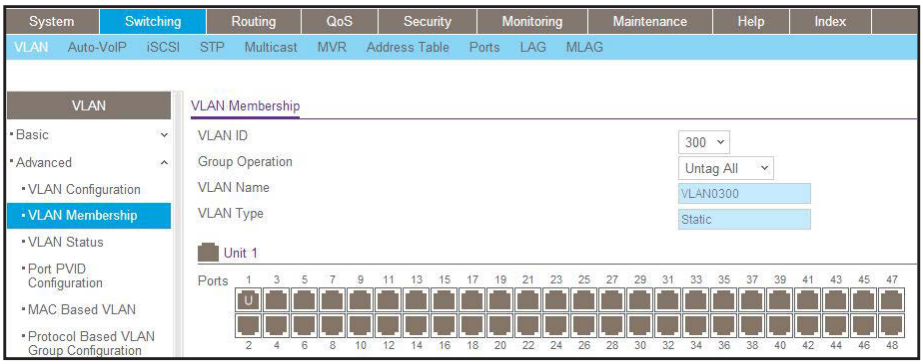
1. Create VLAN 300.
   a. Select **Switching > VLAN > Basic > VLAN Configuration**.

      A screen similar to the following displays.



   b. In the **VLAN ID** field, enter **300**.
   c. Click **Add**.
2. Assign all of the ports to VLAN 300.
   a. Select **Switching > VLAN > Advanced > VLAN Membership**.

      A screen similar to the following displays.

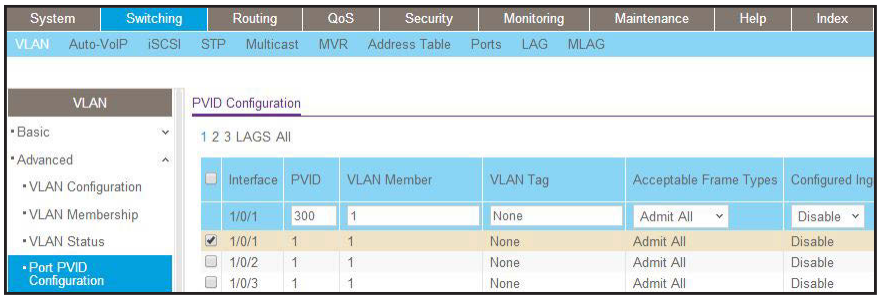


   b. In the **VLAN ID** list, select **300**.
   c. Click **Unit 1**. The ports display.
   d. Click the gray boxes under ports **1** and **24** until **U** displays.

      The U specifies that the egress packet is untagged for the port.

   e. Click **Apply**.
3. Assign PVID to ports 1/0/1 and 1/0/24.
   a. Select **Switching > VLAN > Advanced > Port PVID Configuration**.

A screen similar to the following displays.



b. Scroll down and select the interface **1/0/1** and 1/0/24 check boxes.

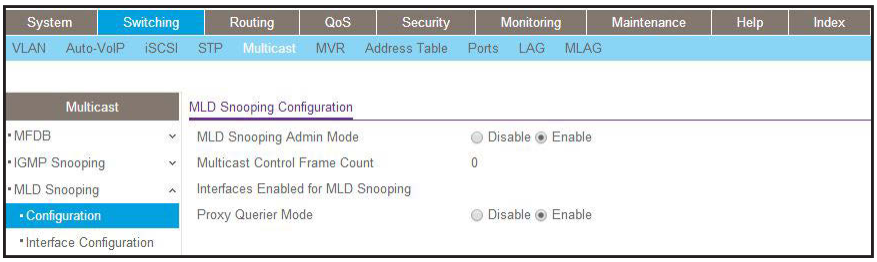
c. In the **PVID (1 to 4093)** field, enter **300**.

d. Click **Apply** to save the settings.

4. Enable MLD snooping on the switch.

a. Select **Routing > Multicast > MLD Snooping > Configuration**.

A screen similar to the following displays.



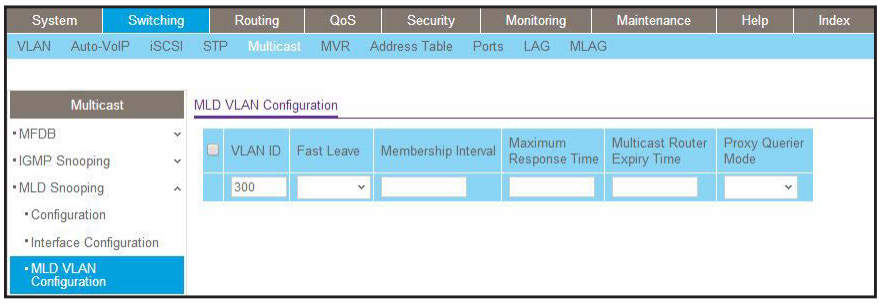
b. For MLD Snooping Admin Mode, select the **Enable** radio button.

c. Click **Apply**.

5. Enable MLD snooping on the VLAN 300.

a. Select **Routing > Multicast > MLD Snooping > MLD VLAN Configuration**.

A screen similar to the following displays.



b. Enter the following information:

- In the **VLAN ID** field, enter **300**.
- In the **Admin Mode** field, select **Enable**.

6. Click **Add**.

DVMRP

33

Distance Vector Multicast Routing Protocol

This chapter includes the following sections:

- *Distance Vector Multicast Routing Protocol Concepts*
- *CLI: Configure DVMRP*
- *Web Interface: Configure DVMRP*

Note: DVMRP is available on the M4300 series switches only.

Distance Vector Multicast Routing Protocol Concepts

The Distance Vector Multicast Routing Protocol (DVMRP) is used for multicasting over IP networks without routing protocols to support multicast. The DVMRP is based on the RIP protocol but more complicated than RIP. DVRMP maintains a link-state database to keep track of the return paths to the source of multicast packages.

The DVMRP operates as follows:

- The first message for any source-group pair is forwarded to the entire multicast network, with respect to the time-to-live (TTL) of the packet.
- TTL restricts the area to be flooded by the message.
- All the leaf routers that do not have members on directly attached subnetworks send back prune messages to the upstream router.
- The branch that transmitted a prune message is deleted from the delivery tree.
- The delivery tree, which is spanning to all the members in the multicast group, is constructed.

In this example, DVMRP is running on switches A, B, and C. IGMP is also running on Switch C, which is connected to the host directly. After the host sends an IGMP report to switch C, multicast streams are sent from the multicast resource to the host along the path built by DVMRP.

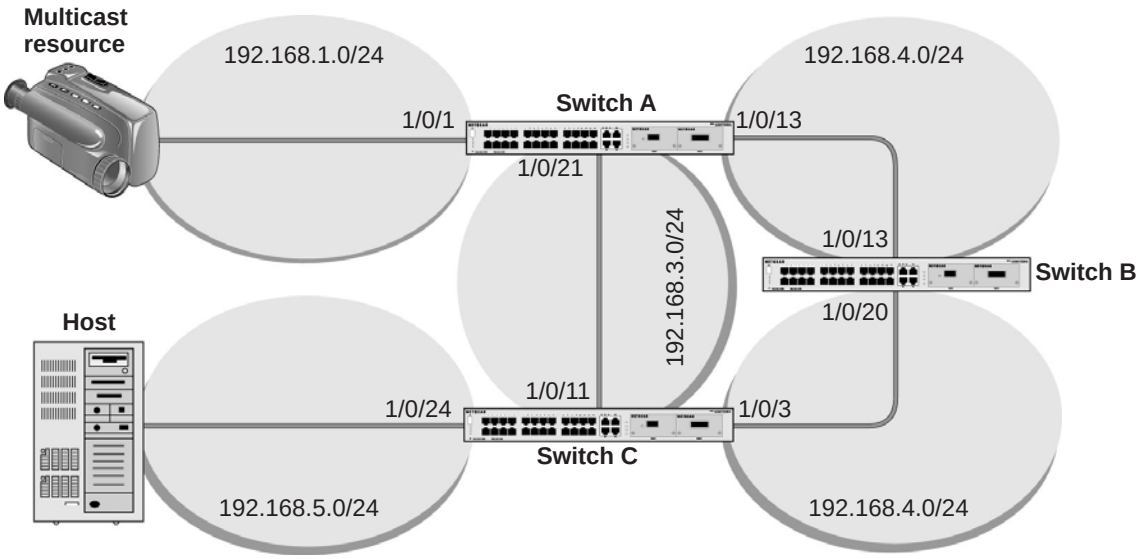


Figure 62. DVMRP

CLI: Configure DVMRP

DVRMP on Switch A

1. Create routing interfaces 1/0/1, 1/0/13, and 1/0/21.

```
(Netgear Switch) #config
(Netgear Switch) (Config)#ip routing
(Netgear Switch) (Config)#interface 1/0/1
(Netgear Switch) (Interface 1/0/1)#routing
(Netgear Switch) (Interface 1/0/1)#ip address 192.168.1.1  255.255.255.0
(Netgear Switch) (Interface 1/0/1)#exit
(Netgear Switch) (Config)#interface 1/0/13
(Netgear Switch) (Interface 1/0/13)#routing
(Netgear Switch) (Interface 1/0/13)#ip address 192.168.2.1 255.255.255.0
(Netgear Switch) (Interface 1/0/13)#exit
(Netgear Switch) (Config)#interface 1/0/21
(Netgear Switch) (Interface 1/0/21)#routing
(Netgear Switch) (Interface 1/0/21)#ip address 192.168.3.2 255.255.255.0
(Netgear Switch)(Interface 1/0/21)#exit
```

2. Enable IP multicast forwarding on the switch.

```
(Netgear Switch) (Config)#ip multicast
```

3. Enable DVMRP protocol on the switch.

```
(Netgear Switch) (Config)#ip dvmrp
```

4. Enable DVMRP mode on the interfaces 1/0/1, 1/0/13, and 1/0/21.

```
(Netgear Switch) (Config)#interface 1/0/1
(Netgear Switch) (Interface 1/0/1)#ip dvmrp
(Netgear Switch) (Interface 1/0/1)#exit
(Netgear Switch) (Config)#interface 1/0/13
(Netgear Switch) (Interface 1/0/13)#ip dvmrp
(Netgear Switch) (Interface 1/0/13)#exit
(Netgear Switch) (Config)#interface 1/0/21
(Netgear Switch) (Interface 1/0/21)#ip dvmrp
(Netgear Switch) (Interface 1/0/21)#exit
(Netgear Switch) #show ip dvmrp neighbor
Interface ..................................... 1/0/13
Neighbor IP Address ........................... 192.168.2.2
State ......................................... Active
Up Time (hh:mm:ss) ............................ 00:02:40
Expiry Time (hh:mm:ss) ........................ 00:00:25
Generation ID ................................. 1116347719
Major Version ................................. 3
Minor Version ................................. 255
Capabilities .................................. Prune GenID Missing 11441
Received Routes ............................... 0
Received Bad Packets .......................... 0
Received Bad Routes ........................... 0
Interface ..................................... 1/0/21
Neighbor IP Address ........................... 192.168.3.1
State ......................................... Active
Up Time (hh:mm:ss) ............................ 00:01:44
Expiry Time (hh:mm:ss) ........................ 00:00:28
Generation ID ................................. 1116595047
Major Version ................................. 3
Minor Version ................................. 255
 More Entries or quit(q)
Capabilities .................................. Prune GenID Missing 11441
Received Routes ............................... 0
Received Bad Packets .......................... 0
Received Bad Routes ........................... 0
```

```
(Netgear Switch) #show ip mcast mroute summary

             Multicast Route Table Summary
                                              Incoming      Outgoing
Source IP       Group IP       Protocol      Interface   Interface List
-------------  ------------   ----------    ---------   ---------------
192.168.1.2     225.0.0.1       DVMRP       1/0/1          1/0/21
```

DVRMP on Switch B

1. Create routing ports 1/0/13 and 1/0/20.

```
(Netgear Switch) #config
(Netgear Switch) (Config)#ip routing
(Netgear Switch) (Config)#interface 1/0/13
(Netgear Switch) (Interface 1/0/13)#routing
(Netgear Switch) (Interface 1/0/13)#ip address 192.168.2.2 255.255.255.0
(Netgear Switch) (Interface 1/0/13)#exit
(Netgear Switch) (Config)#interface 1/0/20
(Netgear Switch) (Interface 1/0/20)#routing
(Netgear Switch) (Interface 1/0/20)#ip address 192.l.168.4.1 255.255.255.0
(Netgear Switch) (Interface 1/0/20)#exit
(Netgear Switch) (Config)#exit
```

2. Enable IP multicast forwarding on the switch.

```
(Netgear Switch) (Config)#ip multicast
```

3. Enable DVMRP protocol on the switch.

```
(Netgear Switch) (Config)#ip dvmrp
```

4. Enable DVMRP mode on interfaceS 1/0/13 and 1/0/20.

```
(Netgear Switch) (Config)#interface 1/0/13
(Netgear Switch) (Interface 1/0/13)#ip dvmrp
(Netgear Switch) (Interface 1/0/13)#ex
(Netgear Switch) (Config)#interface 1/0/20
(Netgear Switch) (Interface 1/0/20)#ip dvmrp
(Netgear Switch) (Interface 1/0/20)#exit
(Netgear Switch) (Config)#exit
```

```
(Netgear Switch) #show ip dvmrp neighbor
Interface ..................................... 1/0/13
Neighbor IP Address ........................... 192.168.2.1
State ......................................... Active
Up Time (hh:mm:ss) ............................ 00:02:26
Expiry Time (hh:mm:ss) ........................ 00:00:20
Generation ID ................................. 88091
Major Version ................................. 3
Minor Version ................................. 255
Capabilities .................................. Prune GenID Missing 11441
Received Routes ............................... 0
Received Bad Packets .......................... 0
Received Bad Routes ........................... 0
Interface ..................................... 1/0/20
Neighbor IP Address ........................... 192.168.4.2
State ......................................... Active
Up Time (hh:mm:ss) ............................ 00:01:44
Expiry Time (hh:mm:ss) ........................ 00:00:29
Generation ID ................................. 1116595033
Major Version ................................. 3
Minor Version ................................. 255
Capabilities .................................. Prune GenID Missing 11441
Received Routes ............................... 0
Received Bad Packets .......................... 0
Received Bad Routes ........................... 0

(Netgear Switch) #show ip mcast mroute detail summary

                  Multicast Route Table Summary
                                          Incoming       Outgoing
Source IP       Group IP      Protocol    Interface   Interface List

--------------  ------------  ----------  ---------   --------------

192.168.1.2      225.0.0.1       DVMRP      1/0/13
```

DVRMP on Switch C:

1. Create routing interfaceS 1/0/11, 1/0/3, and 1/0/24.

```
(Netgear Switch) #config
(Netgear Switch) (Config)#ip routing
(Netgear Switch) (Config)#ip interface 1/0/11
(Netgear Switch) (Interface 1/0/11)#ip routing
(Netgear Switch) (Interface 1/0/11)#ip address 192.168.3.1 255.255.255.0
(Netgear Switch) (Interface 1/0/11)#exit
(Netgear Switch) (Config)#interface 1/0/3
(Netgear Switch) (Interface 1/0/3)#routing
(Netgear Switch) (Interface 1/0/3)#ip address 192.168.4.2 255.255.255.0
(Netgear Switch) (Interface 1/0/3)#exit
(Netgear Switch) (Config)#interface 1/0/24
(Netgear Switch) (Interface 1/0/24)#routing
(Netgear Switch) (Interface 1/0/24)#ip address 192.168.5.1 255.255.255.0
(Netgear Switch) (Interface 1/0/24)#exit
```

2. Enable IP multicast forwarding on the switch.

```
(Netgear Switch) (Config)#ip multicast
```

3. Enable IP DVMRP protocol on the switch.

```
(Netgear Switch) (Config) #ip dvmrp
```

4. Enable DVMRP mode on interfaces 1/0/3, 1/0/11, and 1/0/24.

```
(Netgear Switch) (Config)#interface 1/0/3
(Netgear Switch) (Interface 1/0/3)#ip dvmrp
(Netgear Switch) (Interface 1/0/3)#exit
(Netgear Switch) (Config)#interface 1/0/11
(Netgear Switch) (Interface 1/0/11)#ip dvmrp
(Netgear Switch) (Interface 1/0/11)#exit
(Netgear Switch) (Config)#interface 1/0/24
(Netgear Switch) (Interface 1/0/24)#ip dvrmp
(Netgear Switch) (Interface 1/0/24)#exit
```

5. Enable IGMP protocol on the switch.

```
(Netgear Switch) (Config)# ip igmp
```

6. Enable IGMP mode on the interface 1/0/24.

```
(Netgear Switch) (Config)#interface 1/0/24
(Netgear Switch) (Interface 1/0/24)#ip igmp
(Netgear Switch) (Interface 1/0/24)#exit
```

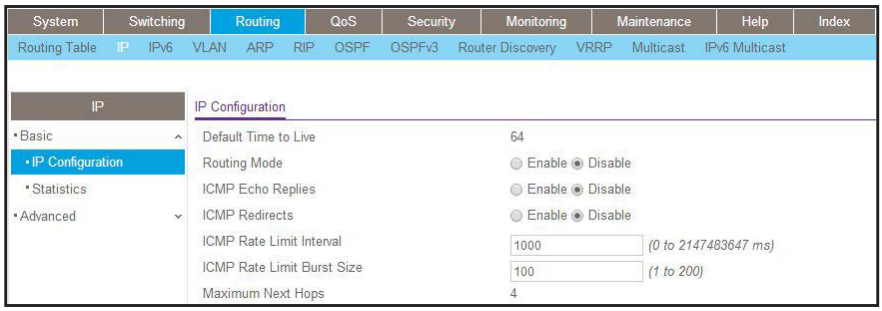
```
(Netgear Switch) #show ip dvmrp neighbor
Interface ..................................... 1/0/11
Neighbor IP Address ........................... 192.168.3.2
State ......................................... Active
Up Time (hh:mm:ss) ............................ 00:01:03
Expiry Time (hh:mm:ss) ........................ 00:00:24
Generation ID ................................. 88099
Major Version ................................. 3
Minor Version ................................. 255
Capabilities .................................. Prune GenID Missing 11441
Received Routes ............................... 0
Received Bad Packets .......................... 0
Received Bad Routes ........................... 0
Interface ..................................... 1/0/3
Neighbor IP Address ........................... 192.168.4.1
State ......................................... Active
Up Time (hh:mm:ss) ............................ 00:01:17
Expiry Time (hh:mm:ss) ........................ 00:00:23
Generation ID ................................. 1116347728
Major Version ................................. 3
Minor Version ................................. 255

More Entries or quit(q)
Capabilities .................................. Prune GenID Missing 11441
Received Routes ............................... 0
Received Bad Packets .......................... 0
Received Bad Routes ........................... 0
(Netgear Switch) #show ip mcast mroute detail summary

                  Multicast Route Table Summary
                                              Incoming      Outgoing
Source IP       Group IP        Protocol    Interface   Interface List
-------------   ------------   ----------   ---------   ---------------
 192.168.1.2     225.0.0.1       DVMRP      1/0/11      1/0/24
```

Web Interface: Configure DVMRP

DVMRP on Switch A

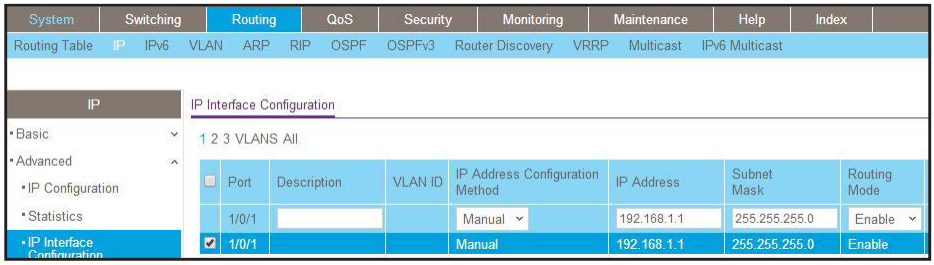
1. Enable IP routing on the switch.
   a. Select **Routing > IP > Basic >IP Configuration**.

      A screen similar to the following displays.



   b. For Routing Mode, select the **Enable** radio button.
   c. Click **Apply**.
2. Configure 1/0/1 as a routing port and assign an IP address to it.
   a. Select **Routing > IP > Advanced > IP Interface Configuration**.

      A screen similar to the following displays.

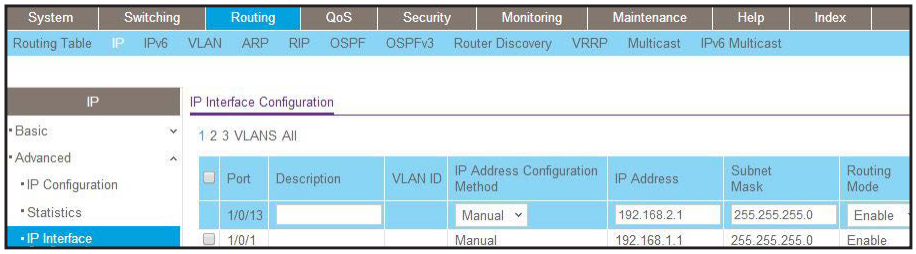


   b. Scroll down and select the Port **1/0/1** check box.

      Now 1/0/1 appears in the Port field at the top.

   c. Enter the following information:
      - In the **IP Address** field, enter **192.168.1.1**.
      - In the **Subnet Mask** field, enter **255.255.255.0**.
      - In the **Routing Mode** field, select **Enable**.
   d. Click **Apply** to save the settings.
3. Configure 1/0/13 as a routing port and assign an IP address to it.
   a. Select **Routing > IP > Advanced > IP Interface Configuration**.

A screen similar to the following displays.



b. Scroll down and select the Port **1/0/13** check box.

Now 1/0/13 appears in the Port field at the top.

c. Enter the following information:

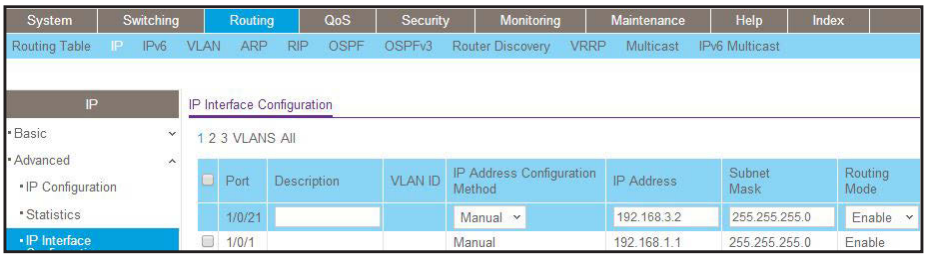
- In the **IP Address** field, enter **192.168.2.1**.
- In the **Subnet Mask** field, enter **255.255.255.0**.
- In the **Routing Mode** field, select **Enable**.

d. Click **Apply** to save the settings.

4. Configure 1/0/21 as a routing port and assign an IP address to it.

a. Select **Routing > IP > Advanced > IP Interface Configuration**.

A screen similar to the following displays.



b. Scroll down and select the Port **1/0/13** check box.

Now 1/0/13 appears in the Port field at the top.

c. Enter the following information:

- In the **IP Address** field, enter **192.168.3.2**.
- In the **Subnet Mask** field, enter **255.255.255.0**.
- In the **Routing Mode** field, select **Enable**.

d. Click **Apply** to save the settings.

5. Enable IP multicast on the switch.

a. Select **Routing > Multicast > Global Configuration**.

A screen similar to the following displays.

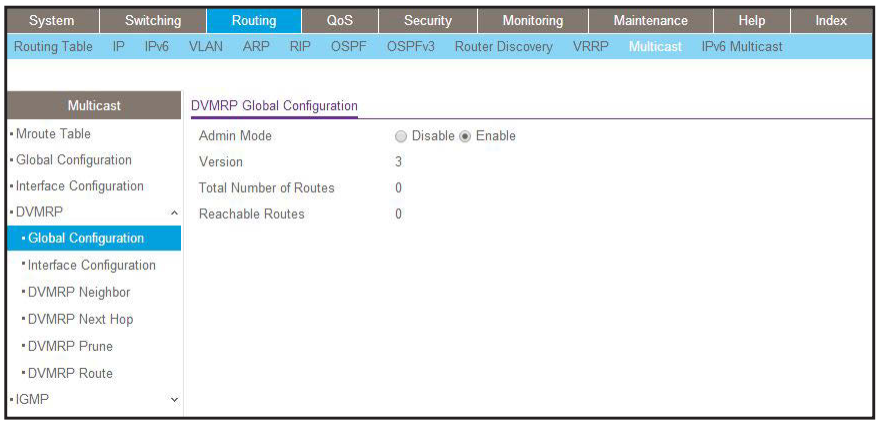
b. For Admin Mode, select the **Enable** radio button.

c. Click **Apply**.

6. Enable DVMRP on the switch.

a. Select **Routing > Multicast > DVMRP > Global Configuration**.

A screen similar to the following displays.



b. For Admin Mode, select the **Enable** radio button.

c. Click **Apply**.

7. Enable DVMRP on the interface.

a. Select **Routing > Multicast > DVMRP > Interface Configuration**.

A screen similar to the following displays.

b. Scroll down select the Interface **1/0/1**, **1/0/13**, and **1/0/21** check boxes.

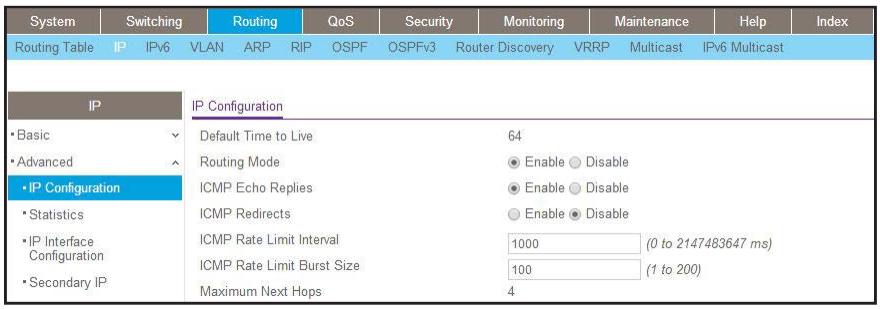
c. In the **Interface Mode** field, select **300**.

d. Click **Apply** to save the settings.

DVMRP on Switch B

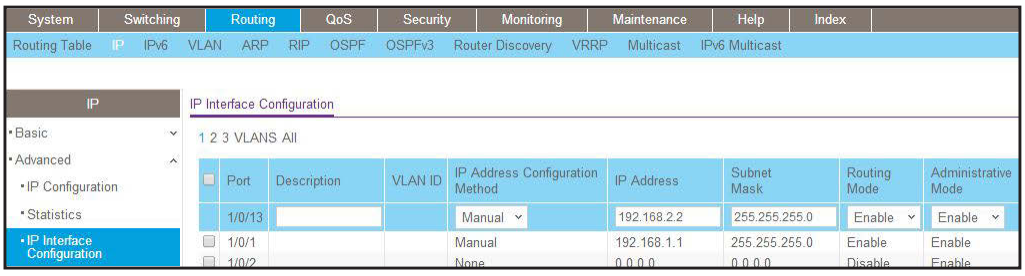
1. Enable IP routing on the switch.
   a. Select **Routing > IP > Basic > IP Configuration**.

      A screen similar to the following displays.



   b. For Routing Mode, select the **Enable** radio button.
   c. Click **Apply**.
2. Configure 1/0/13 as a routing port and assign and IP address to it.
   a. Select **Routing > IP > Advanced > IP Interface Configuration**.

      A screen similar to the following displays.

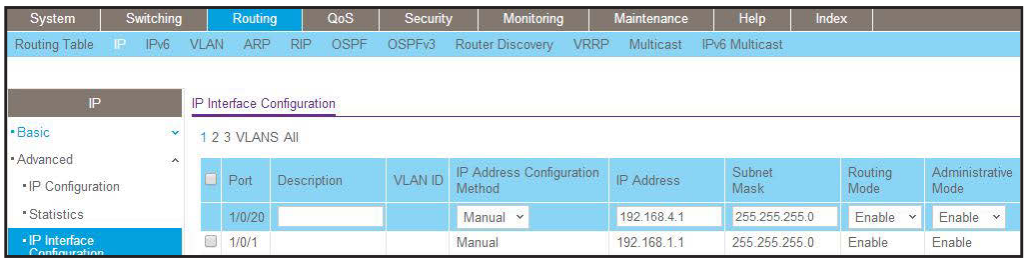


   b. Scroll down and select the Port **1/0/13** check box.

      Now 1/0/13 appears in the Port field at the top.

   c. Enter the following information in the IP Interface Configuration.
      - In the **IP Address** field, enter **192.168.2.2**.
      - In the **Subnet Mask** field, enter **255.255.255.0**.
      - In the **Routing Mode** field, select **Enable**.
   d. Click **Apply** to save the settings.
3. Configure 1/0/20 as a routing port and assign an IP address to it.
   a. Select **Routing > IP > Advanced > IP Interface Configuration**.

A screen similar to the following displays.



b. Scroll and select the Port **1/0/20** check box.

Now 1/0/20 appears in the Interface field at the top.

c. Enter the following information:

- In the **IP Address** field, enter **192.168.4.1**.
- In the **Subnet Mask** field, enter **255.255.255.0**.
- In the **Routing Mode** field, select **Enable**.

d. Click **Apply** to save the settings.

4. Enable IP multicast on the switch.

a. Select **Routing > Multicast > Global Configuration**.

A screen similar to the following displays.

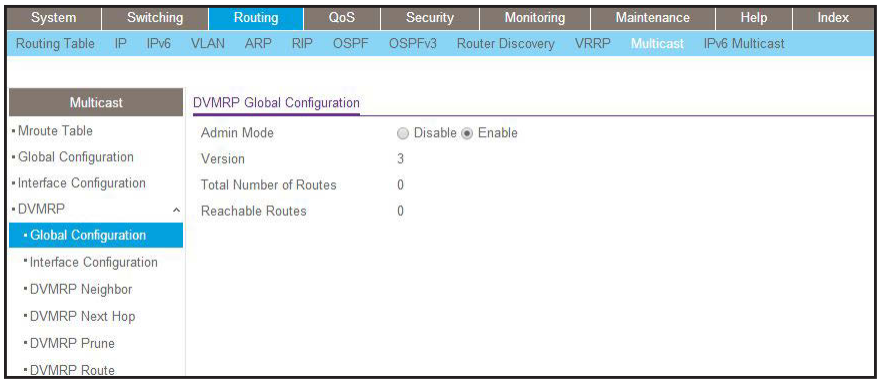
b. For Admin Mode, select the **Enable** radio button.

c. Click **Apply**.

5. Enable DVMRP on the switch.

a. Select **Routing > Multicast > DVMRP> Global Configuration**.

A screen similar to the following displays.



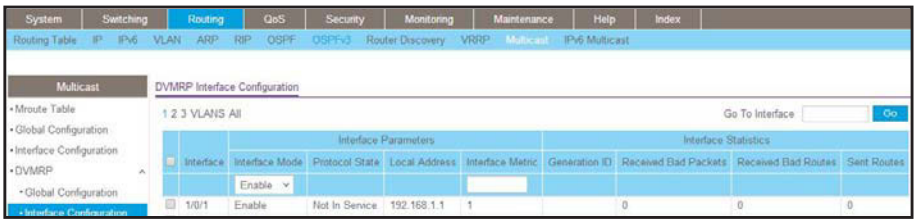
b. For Admin Mode, select the **Enable** radio button.

c. Click **Apply**.

6. Enable DVMRP on the interface.

a. Select **Routing > Multicast > DVMRP > Interface Configuration**.

A screen similar to the following displays.



b. Scroll down and select the Interface **1/0/13** and **1/0/20** check boxes.

c. In the **Interface Mode** field, select **Enable**.

d. Click **Apply** to save the settings.

DVMRP on Switch C

1. Enable IP routing on the switch.

a. Select **Routing > IP > Basic > IP Configuration**.

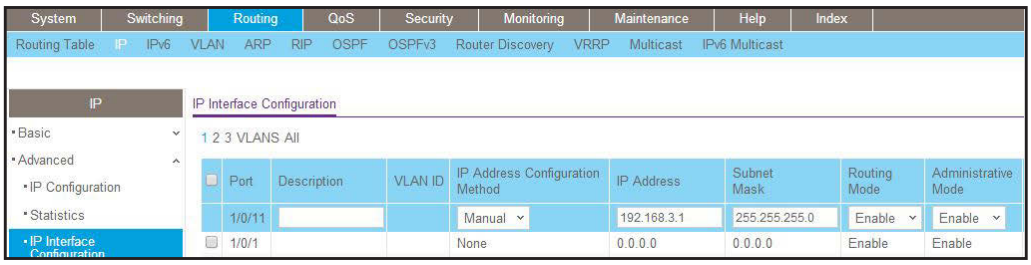
A screen similar to the following displays.

b. For Routing Mode, select the **Enable** radio button.

c. Click **Apply**.

2. Configure 1/0/11 as a routing port and assign an IP address to it.
   a. Select **Routing > IP > Advanced > IP Interface Configuration**.

      A screen similar to the following displays.



   b. Scroll down and select the Port **1/0/11** check box.

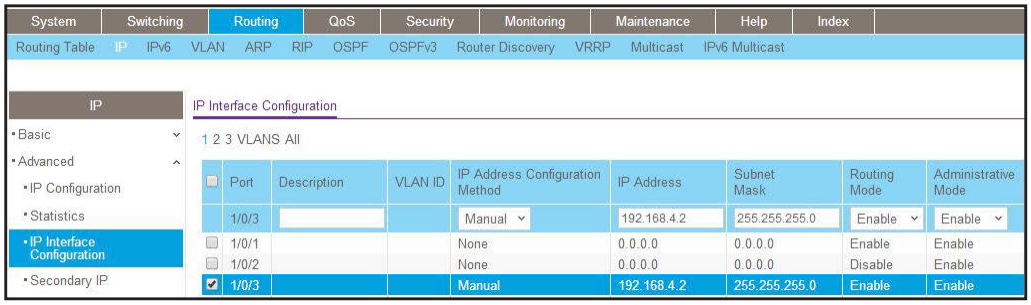
      Now 1/0/11 appears in the Port field at the top.

   c. Enter the following information:
      - In the **IP Address** field, enter **192.168.3.1**.
      - In the **Subnet Mask** field, enter **255.255.255.0**.
      - In the **Routing Mode** field, select **Enable**.

   d. Click **Apply** to save the settings.

3. Configure 1/0/3 as a routing port and assign an IP address to it.
   a. Select **Routing > IP > Advanced > IP Interface Configuration**.

      A screen similar to the following displays.



   b. Scroll down and select the Port **1/0/3** check box.

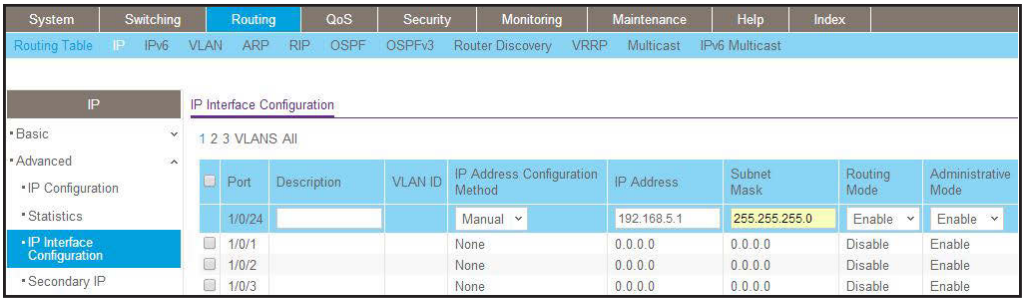
      Now 1/0/3 appears in the Port field at the top.

   c. Enter the following information:
      - In the **IP Address** field, enter **192.168.4.2**.
      - In the **Subnet Mask** field, enter **255.255.255.0**.
      - In the **Routing Mode** field, select **Enable**.

   d. Click **Apply** to save the settings.

4. Configure 1/0/24 as a routing port and assign an IP address to it.
   a. Select **Routing > IP > Advanced > IP Interface Configuration**.

A screen similar to the following displays.



b. Scroll down and select the Port **1/0/24** check box.

Now 1/0/24 appears in the Port field at the top.

c. Enter the following information:

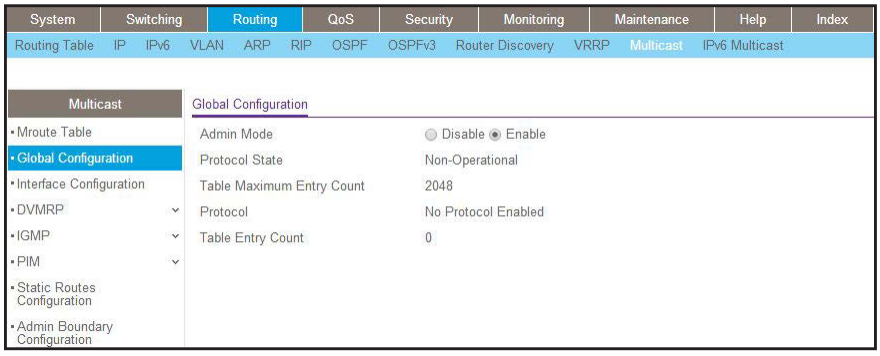
- In the **IP Address** field, enter **192.168.5.1**.
- In the **Subnet Mask** field, enter **255.255.255.0**.
- In the **Routing Mode** field, select **Enable**.

d. Click **Apply** to save the settings.

5. Enable IP multicast on the switch.

a. Select **Routing > Multicast >Global Configuration**.

A screen similar to the following displays.



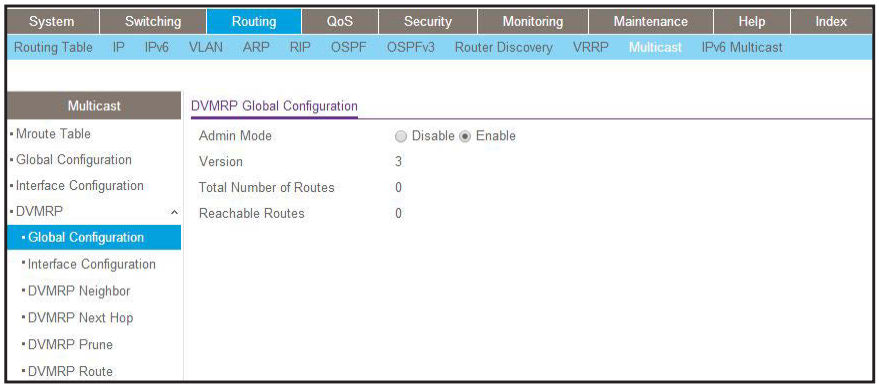
b. For Admin Mode, select the **Enable** radio button.

c. Click **Apply**.

6. Enable DVMRP on the switch.

a. Select **Routing > Multicast > DVMRP > Global Configuration**.

A screen similar to the following displays.



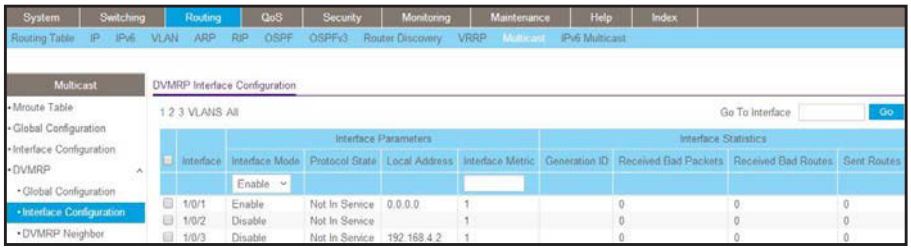
b. For Admin Mode, select the **Enable** radio button.

c. Click **Apply**.

7. Enable DVMRP on the interface.

a. Select **Routing > Multicast > DVMRP > Interface Configuration**.

A screen similar to the following displays.



b. Scroll down and select the Interface **1/0/3**, **1/0/11**, and **1/0/24** check boxes.

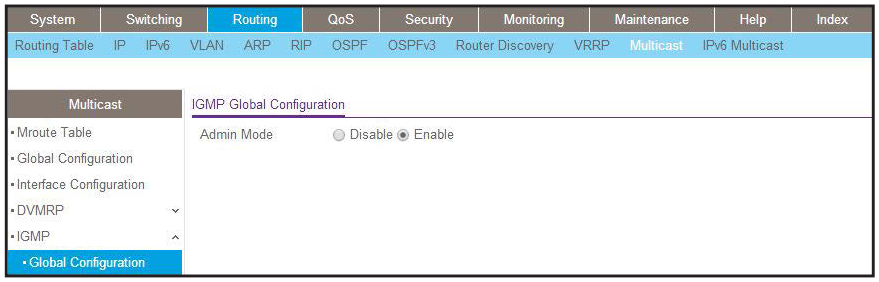
c. Select **Enable** in the **Interface Mode** field.

d. Click **Apply** to save the settings.

8. Enable IGMP on the switch.

a. Select **Routing > Multicast > IGMP > Global Configuration**.

A screen similar to the following displays.

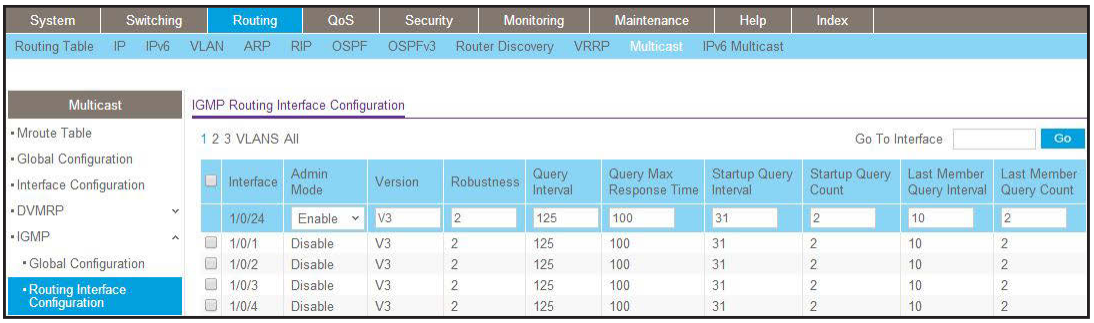


b. For Admin Mode, select the **Enable** radio button.

c. Click **Apply**.

9. Enable IGMP on the interface.
   a. Select **Routing > Multicast > IGMP > Routing Interface Configuration**.

      A screen similar to the following displays.



   b. Scroll down and select the Interface **1/0/24** check box.

      Now 1/0/24 appears in the Interface field at the top.

   c. In the **Admin Mode** field, select **Enable**.
   d. Click **Apply** to save the settings.

Link Dependency

34

Configure Link State Groups

This chapter includes the following sections:

- *Link Dependency Concepts*
- *CLI: Create a Link State Group*
- *Web Interface: Create a Link State Group*

Link Dependency Concepts

Link dependency enables or disables ports in a group based on the link state of other ports in the same group. That is, the link state of some ports depends on the link state of other ports.

For example, if port A depends on port B and the switch detects link loss on B, the switch automatically brings down the link on port A. When the link is restored to port B, the switch automatically restores the link to port A. You can specify whether link A is brought up or brought down, depending on the state of link B. The ports that are participating in link dependency can be among different members of a stack.

To establish link dependency, you must define a link state group. A link state group is identified by a group number and consists of an upstream interface list, a downstream interface list, and an action (up or down) that is associated with the group. One or more link aggregation group (LAG) interfaces, one or more physical interfaces, or a combination of both LAG interfaces and physical interfaces can be members of the upstream and downstream interface list. If all the members of a link state group's upstream interface list go down, all the downstream interfaces in the link state group are either brought down or brought up, depending on the action that is associated with the group.

Note the following characteristics and limitations of link dependency:

- If you add an interface to the downstream list of a link state group, the interface remains down until you add an upstream interface to the list. The link status of the downstream interface is then determined by the link state of the upstream interface, as defined by the action that is associated with the link state group. To prevent downstream interfaces from remaining down in a link state group, configure upstream interfaces in the group before you configure downstream interfaces in the group.
- If the configured action for a link group is up and if any configured upstream interface is down, then upon configuring the downstream interfaces, all downstream interfaces are immediately brought down.
- When a physical interface is configured as an upstream or downstream interface for a link state group and you make the physical interface a member of a LAG interface, the physical interface continues to be an upstream or downstream interface for the link state group.
- An interface that is defined as an upstream interface in a link state group cannot be defined as a downstream interface in the same link state group.
- Link dependencies cannot be circular. That is, an interface that is defined as an upstream interface in one link state group cannot be defined as a downstream interface in another link state group if such a configuration causes circular dependencies between groups.

CLI: Create a Link State Group

1. Create a link state group with group number 1.

```
(Netgear Switch) (Config)#link state group 1 action down
```

2. Configure port 1/0/1 as an upstream link.

```
(Netgear Switch) (Config)#interface 1/0/1
(Netgear Switch) (Interface 1/0/1)#link state group 1 upstream
```

3. Configure port 1/0/5 as a downstream link.

```
(Netgear Switch) (Interface 1/0/1)#interface 1/0/5
(Netgear Switch) (Interface 1/0/5)#link state group 1 downstream
(Netgear Switch) (Interface 1/0/5)#exit
```

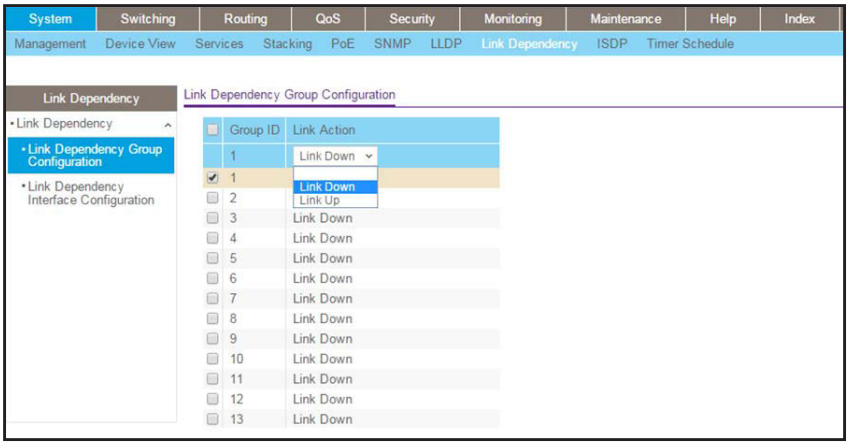
4. Display the status of the link state group with group number 1.

```
(Netgear Switch) #show link state group 1
GroupId  Downstream Interfaces   Upstream Interfaces   Link Action   Group State
-------  ----------------------  --------------------  ------------  -----------
1        1/0/5                   1/0/1                 Link Down     Up
```

Web Interface: Create a Link State Group

1. Configure the action for link state group with group number 1.
   a. Select **System > Link Dependency > Link Dependency Group Configuration**.

   A screen similar to the following displays.



b. Select the check box for Group ID 1.

   1 displays in the Group ID field of the table heading.

c. From the **Link Action** menu, select **Link Down**.

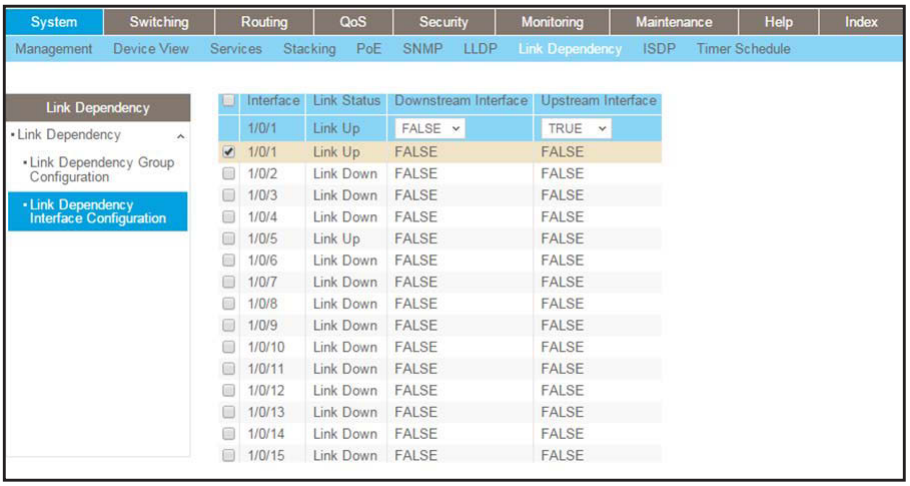
d. Click the **Apply** button.

   Your settings are saved.

2. Configure port 1/0/1 as an upstream port.

a. Select **System > Link Dependency > Link Dependency Interface Configuration**.

   A screen similar to the following displays.



b. Select the check box to the left of interface 1/0/1.

   1/0/1 displays in the Interface field of the table heading.

c. From the **Upstream Interface** menu, select **True**.

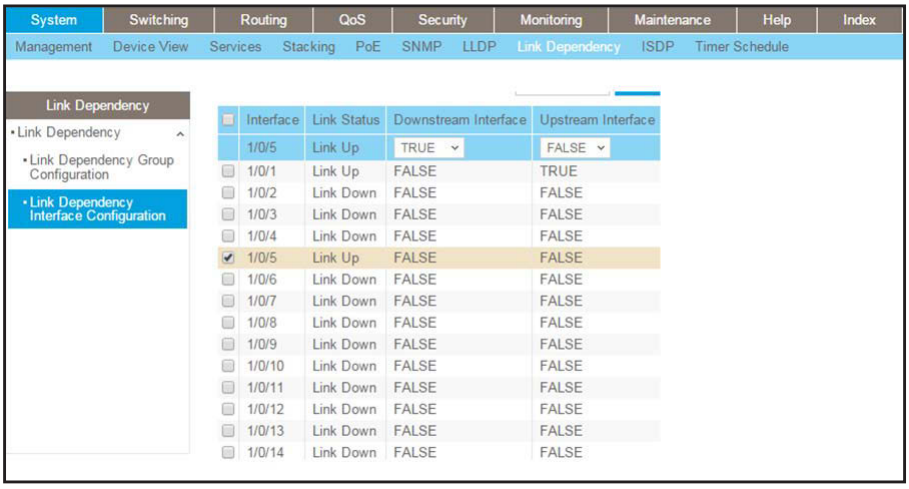
d. Click the **Apply** button.

   Your settings are saved.

3. Configure port 1/0/1 as an upstream port.

a. Select **System > Link Dependency > Link Dependency Interface Configuration**.

A screen similar to the following displays.



b. Select the check box to the left of interface 1/0/5.

1/0/5 displays in the Interface field of the table heading.

c. From the **Downstream Interface** menu, select **True**.

d. Click the **Apply** button.

Your settings are saved.

Captive Portals

35

Captive portals and client authentication

This chapter includes the following sections:

- *Captive Portal Concepts*
- *Captive Portal Configuration Concepts*
- *Enable a Captive Portal*
- *Client Access, Authentication, and Control*
- *Block a Captive Portal Instance*
- *Local Authorization, Create Users and Groups*
- *Remote Authorization (RADIUS) User Configuration*
- *SSL Certificates*

Captive Portal Concepts

The captive portal feature is a software implementation that blocks clients from accessing the network until user verification has been established. You can set up verification to allow access for both guests and authenticated users. Authenticated users must be validated against a database of authorized captive portal users before access is granted.

The authentication server supports both HTTP and HTTPS web connections. In addition, you can configure a captive portal to use an optional HTTP port (in support of HTTP proxy networks). If configured, this additional port is then used exclusively by the captive portal. This optional port is in addition to the standard HTTP port 80, which is being used for all other web traffic.

The captive portal for wired interfaces allows the clients directly connected to the switch to be authenticated using a captive portal mechanism before the client is given access to the network. When you enable the captive portal feature on a wired physical port, the port is set in captive-portal- enabled state such that all the traffic coming to the port from the unauthenticated clients is dropped except for the ARP, DHCP, DNS, and NETBIOS packets. The switch forwards these packets so that unauthenticated clients can get an IP address and resolve the hostname or domain names. Data traffic from authenticated clients goes through, and the rules do not apply to these packets.

All the HTTP/HTTPS packets from unauthenticated clients are directed to the CPU on the switch for all the ports for which you enabled the captive portal feature. When an unauthenticated client opens a web browser and tries to connect to network, the captive portal redirects all the HTTP/HTTPS traffic from unauthenticated clients to the authenticating server on the switch. A captive portal web page is sent back to the unauthenticated client. The client can authenticate. If the client successfully authenticates, the client is given access to port.

You can enable the captive portal feature on all the physical ports on the switch. It is not supported for VLAN interfaces, loopback interfaces, or logical interfaces. The captive portal feature uses MAC-address based authentication and not port-based authentication. This means that all the clients connected to the captive portal interface must be authenticated before they can get access to the network.

Clients connecting to the captive portal interface have three states; unknown, unauthenticated, and authenticated.

- **Unknown**. In the unknown state, the captive portal does not redirect HTTP/S traffic to the switch, but instead asks the switch whether the client is authenticated or unauthenticated.
- **Unauthenticated**. The captive portal directs the HTTP/S traffic to the switch so that the client can authenticate with the switch.
- **Authenticated**. After successful authentication, the client is placed in authenticated state. In this state, all the traffic emerging from the client is forwarded through the switch.

Captive Portal Configuration Concepts

This chapter introduces the objects that make up the captive portal and describes the interaction between the captive portal and the network administrator. It explains what configurations are visible to the network administrator and enumerates the events.

All the configurations included in this section are managed using the CLI, the web interface, and SNMP, with one exception; to customize the captive portal web page, you must use the web interface.

The captive portal configuration provides the network administrator control over verification and authentication, assignment to interfaces, client sessions, and web page customization.

You can create multiple captive portal configuration instances. Each captive portal configuration contains various flags and definitions used to control client access and content to customize the user verification web page. A captive portal configuration can be applied to one or more interfaces. An interface can only be a physical port on the switch. Software release 8.0 and newer versions can contain up to 10 captive portal configurations.

Enable a Captive Portal

CLI: Enable a Captive Portal

1. Enable captive portal on the switch.

```
(Netgear Switch) (config)#captive-portal
(Netgear Switch) (Config-CP)#enable
```

2. Enable captive portal instance 1.

```
(Netgear Switch) (Config-CP)#configuration 1
(Netgear Switch) (Config-CP 1)#enable
```

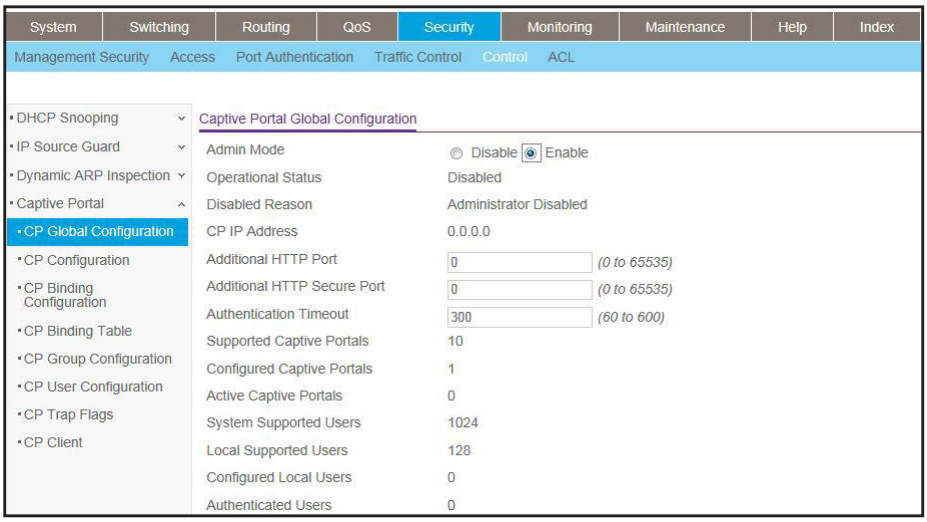
3. Enable captive portal instance 1 on port 1/0/1.

```
(Netgear Switch) (Config-CP 1)#interface 1/0/1
```

Web Interface: Enable a Captive Portal

1. Enable captive portal on the switch.
   a. Select **Security > Control > Captive Portal > CP Global Configuration**.

      A screen similar to the following displays.



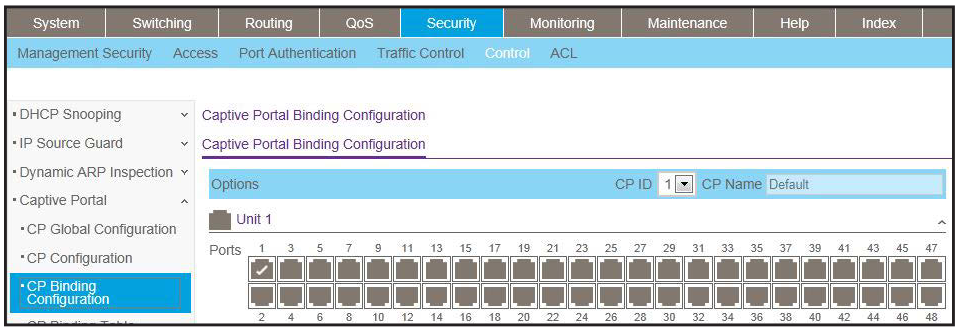
   b. For Admin Mode, Select the **Enable** radio button.
   c. Click **Apply**.
2. Enable captive portal instance 1 on the switch.
   a. Select **Security > Control > Captive Portal > CP Configuration**.

      A screen similar to the following displays.

   b. Scroll down and select the CP **1** check box.

      Now CP 1 appears in the CP ID field at the top.
   c. In the **Admin Mode** field, select **Enable**.
   d. Click **Apply** to save the settings.
3. Enable CP 1 on interface 1/0/1.
   a. Select **Security > Controls > Captive Portal > CP Binding Configuration**.

A screen similar to the following displays.



b. In the **CP ID** list, select **1**.

c. Click **Unit 1**. The ports display.

d. Click the gray box under port **1**.

e. Click **Apply**.

Client Access, Authentication, and Control

User verification can be configured to allow access for guest users—users who do not have assigned user names and passwords. User verification can also be configured to allow access for authenticated users. Authenticated users are required to enter a valid user name and password that must first be validated against the local database or a RADIUS server. Network access is granted once user verification has been confirmed. The administrator can block access to a captive portal configuration. When an instance is blocked, no client traffic is allowed through any interfaces associated with that captive portal configuration. Blocking a captive portal instance is a temporary command executed by the administrator and not saved in the configuration.

Block a Captive Portal Instance

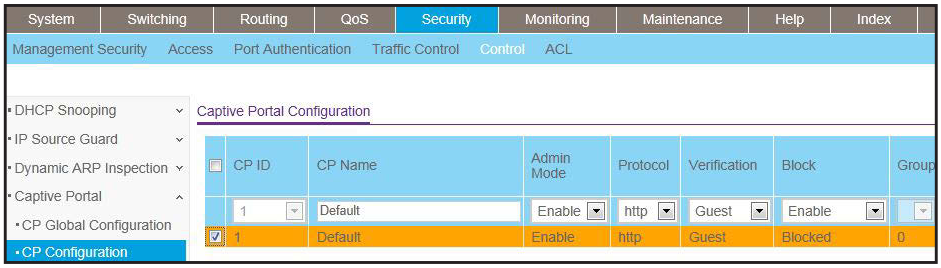
CLI: Block a Captive Portal Instance

```
(Netgear Switch)(Config-CP 1)#block
```

Web Interface: Block a Captive Portal Instance

1. Select **Security > Control > Captive Portal > CP Configuration**.

   A screen similar to the following displays.



2. Under Captive Portal Configuration, scroll down and select the CP **1** check box. Now CP 1 appears in the CP ID field at the top.
3. In the **Block** field, select **Enable**.
4. Click **Apply** to save the settings.

Local Authorization, Create Users and Groups

When using local authentication, the administrator provides user identities for captive portal by adding unique user names and passwords to the local user database. This configuration is global to the captive portal component and can contain up to 128 user entries (a RADIUS server should be used if more users are required). A local user can belong to one or more groups. There is one group created by default with the group name *Default* to which all new users are assigned. All new captive portal instances are also assigned to the Default group. You can create new groups and modify the user/group association to allow only a subset of users access to a specific captive portal instance. Network access is granted upon successful user name, password, and group verification.

CLI: Create Users and Groups

1. Create a group whose group ID is 2.

```
(Netgear Switch) #config
(Netgear Switch) (config)#captive-portal
(Netgear Switch)(Config-CP)# user group 2
```

2. Create a user whose name is user1.

```
(Netgear Switch) (Config-CP)#user 2 name user1
```

3. Configure the user's password.

```
(Netgear Switch) (Config-CP)#user 2 password
Enter password (8 to 64 characters): 12345678
Re-enter password: 12345678
```

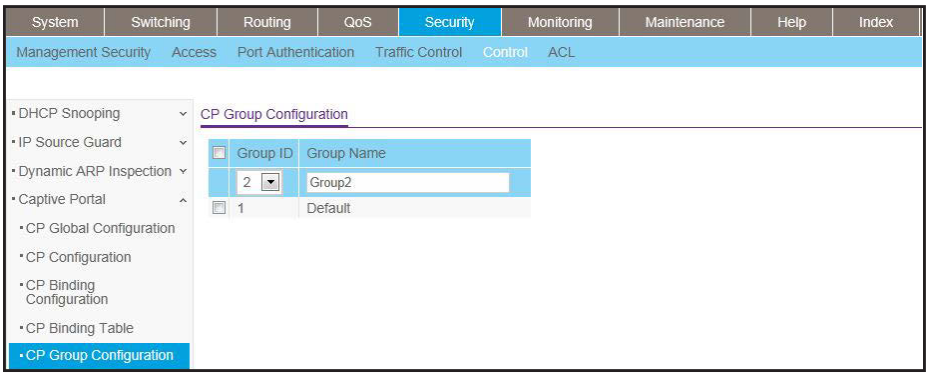
4. Add the user to the group.

```
(Netgear Switch) (Config-CP)#user 2 group 2
```

Web Interface: Create Users and Groups

1. Create a group.
   a. Select **Security > Control > Captive Portal > CP Group Configuration**.

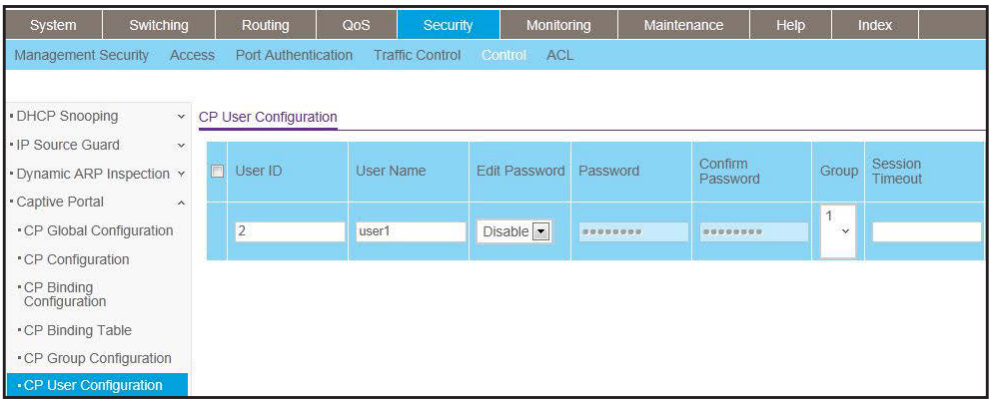
      A screen similar to the following displays.



   b. Enter the following information:
      - In the **Group ID** field, select **2**.
      - In the **Group Name** field, enter **Group2**.

   c. Click **Add**.
2. Create a user.
   a. Select **Security > Control > Captive Portal > CP User Configuration**.

A screen similar to the following displays.



b. Enter the following information:

- In the **User ID** Field, enter **2**.
- In the **User Name** field, enter **user1**.
- In the **Password** field, enter **12345678**.
- In the **Confirm Password** field, enter **12345678**.
- In the **Group** field, select **2**.

c. Click **Add**.

Remote Authorization (RADIUS) User Configuration

A remote RADIUS server can be used for client authentication. In software release 8.0 (or newer), the RADIUS authentication and accounting servers are configured separate from the captive portal configuration. In order to perform authentication and accounting using RADIUS, you configure one or more RADIUS servers and then references the servers using their names in the captive portal configuration. Each captive portal instance can be assigned one RADIUS authentication server and one RADIUS accounting server.

If RADIUS is enabled for a captive portal configuration and no RADIUS servers are assigned, the captive portal activation status will indicate that the instance is disabled with an appropriate reason code.

The following table indicates the RADIUS attributes that are used to configure captive portal users. The table indicates both RADIUS attributes and vendor specific attributes (VSA) that are used to configure captive portal. VSAs are denoted in the ID column and are comma delimited (vendor ID, attribute ID).

Table 4. RADIUS Attributes for Configuring Captive Portal Users

RADIUS Attribute	No.	Description	Range	Usage	Default
User-Name	1	User name to be authorized.	1–32 characters	Required	None
User-Password	2	User password.	8–64 characters	Required	None
Session-Timeout	27	Logout once session timeout is reached (seconds). If the attribute is 0 or not present, use the value configured for the captive portal.	Integer (seconds)	Optional	0
Idle-Timeout	28	Log out once idle timeout is reached (seconds). If the attribute is 0 or not present, use the value configured for the captive portal.	Integer (seconds)	Optional	0
WISPr-Max-Bandwidth-Up	14122, 7	Maximum client transmit rate (b/s). Limits the bandwidth at which the client can send data into the network. If the attribute is 0 or not present, use the value configured for the captive portal.	Integer	Optional	0
WISPr-Max-Bandwidth-Down	14122, 8	Maximum client receive rate (b/s). Limits the bandwidth at which the client can receive data from the network. If the attribute is 0 or not present, use the value configured for the captive portal.	Integer	Optional	0

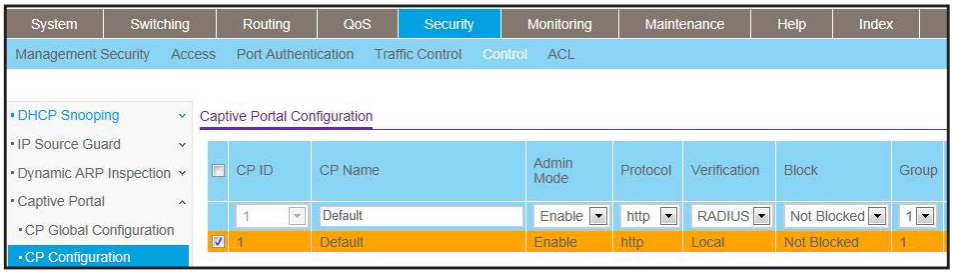
CLI: Configure RADIUS as the Verification Mode

```
(Netgear Switch) (Config-CP 1)#radius-auth-server Default-RADIUS-Server
(Netgear Switch) (Config-CP 1)#verification radius
```

Web Interface: Configure RADIUS as the Verification Mode

1. Select **Security > Control > Captive Portal > CP Configuration**.

   A screen similar to the following displays.



2. Scroll down and select the CP **1** check box. Now CP 1 appears in the CP ID field at the top.
3. Enter the following information:
   - In the **Verification** field, select **RADIUS**.
   - In the **Radius Auth Server** field, enter the RADIUS server name **Default-RADIUS-Server**.
4. Click **Apply**.

SSL Certificates

A captive portal instance can be configured to use the HTTPS protocol during its user verification process. The connection method for HTTPS uses the Secure Sockets Layer (SSL) protocol, which requires a certificate to provide encryption. The certificate is presented to the user at connection time.

In software release 8.0 (or newer), the captive portal uses the same certificate that is used for secure HTTP connections. You can generate this certificate using a CLI command. If a captive portal instance is configured for the HTTPS protocol and there is not a valid certificate present on the system, the captive portal instance status will show Disabled with an appropriate reason code.

iSCSI

Internal Small Computer System Interface

36

This chapter includes the following sections:

- *iSCSI Concepts*
- *Enable iSCSI Awareness with VLAN Priority Tag*
- *Enable iSCSI Awareness with DSCP*
- *Set the iSCSI Target Port*
- *Show iSCSI Sessions*

iSCSI Concepts

The Internal Small Computer System Interface (iSCSI) feature is used in networks containing iSCSI initiators and targets where the administrator desires to protect the iSCSI traffic from interruption by giving the traffic preferential QoS treatment. The dynamically generated classifier rules are used to direct the iSCSI data traffic to queues that can be given the desired preference characteristics over other data transiting the switch. This can avoid session interruptions during times of congestion that would otherwise cause iSCSI packets to be dropped.

The administrator can select VLAN priority tag (VPT) or DSCP mapping for the QoS preferential treatment. iSCSI flows are assigned by default to the highest VPT/DSCP queue not used for chassis management or voice VLAN. The administrator should also take care of configuring the relevant Class of Service parameters for the queue chosen in order to complete the setting.

The following figure shows an example of iSCSI implementation.

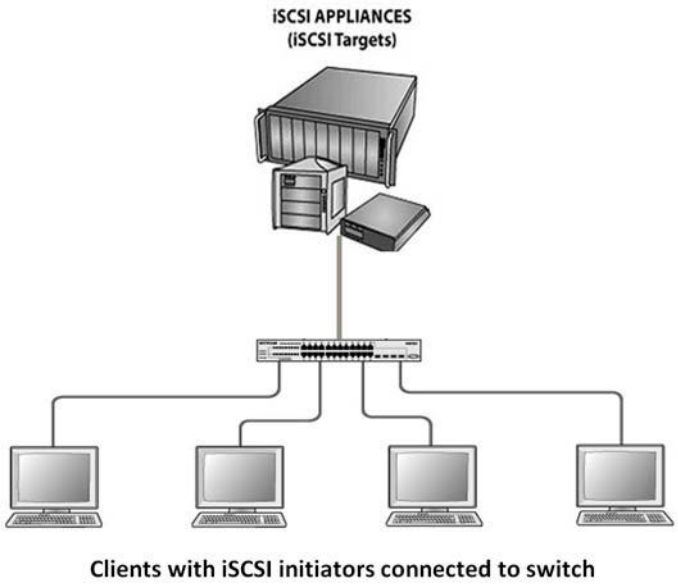


Figure 63. Sample iSCSI implementation

Enable iSCSI Awareness with VLAN Priority Tag

The example is shown as CLI commands and as web interface procedure.

CLI: Enable iSCSI Awareness with VLAN Priority Tag

Use the following commands to enable iSCSI awareness, select VPT, and set VLAN number and aging time.

```
(Netgear Switch) #config
(Netgear Switch) (Config) #iscsi enable
(Netgear Switch) (Config) #iscsi cos vpt 5
(Netgear Switch) (Config) #iscsi aging time 10
(Netgear Switch) (Config) #exit
```

Web Interface: Enable iSCSI Awareness with VLAN Priority Tag

1. Enable iSCSI awareness, select VPT, and set VLAN number and aging time.
   a. Select **Switching > iSCSI > Basic**.

      A screen similar to the following displays.

   b. Enter the following information:
      - Next to iSCSI Status, select the **Enable** radio button.
      - Next to QoS Profile, select the **VLAN Priority Tag** radio button.
      - From the VLAN Priority Tag menu, select **5** (the default value).
      - Next to Remark, select the **Enable** radio button (the default value).
      - In the iSCSI Aging Time field, enter **10** (the default value).
   c. Click **Apply** to save the settings.

Enable iSCSI Awareness with DSCP

The example is shown as CLI commands and as web interface procedure.

CLI: Enable iSCSI Awareness with DSCP

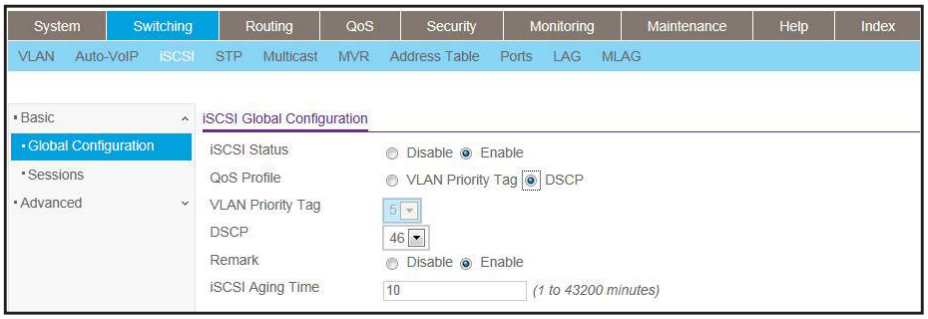
Use the following commands to enable iSCSI awareness, select DSCP, and set DSCP queue number and aging time.

```
(Netgear Switch) #config
(Netgear Switch) (Config) #iscsi enable
(Netgear Switch) (Config) #iscsi cos dscp 46
(Netgear Switch) (Config) #iscsi aging time 10
(Netgear Switch) (Config) #exit
```

Web Interface: Enable iSCSI Awareness with DSCP

1. Enable iSCSI awareness, select DSCP, and set the DSCP queue number and aging time.
   a. Select **Switching > iSCSI > Basic**.

      A screen similar to the following displays.



   b. Enter the following information:
      - Next to iSCSI Status, select the **Enable** radio button.
      - Next to QoS Profile, select the **DSCP** radio button.
      - From the DSCP menu, select **46** (the default value).
      - Next to Remark, select the **Enable** radio button (the default value).
      - In the iSCSI Aging Time field, enter **10** (the default value).
2. Click **Apply** to save the settings.

Set the iSCSI Target Port

When working with iSCSI that does not use the standard IANA assigned iSCSI ports (3260/860), NETGEAR recommends that you specify the target IP address. Then, the switch snoops frames only if the TCP destination port is one of the configured TCP ports and the destination IP address is the target IP address. This configuration improves the performance of the switch by preventing the CPU from processing non-iSCSI flows.

The example is shown as CLI commands and as web interface procedure.

CLI: Set iSCSI Target Port

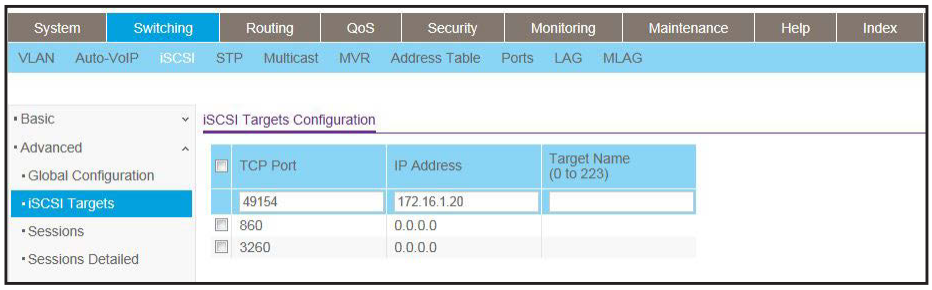
Use the following commands to set iSCSI target port to 49154 at IP address 172.16.1.20.

```
(Netgear Switch) #config
(Netgear Switch) (Config) #iscsi target port 49154 address 172.16.1.20
(Netgear Switch) (Config) #exit
```

Web Interface: Set iSCSI Target Port

1. Configure the iSCSI target port.
   a. Select **Switching > iSCSI > Advanced > iSCSI Targets**.

      A screen similar to the following displays.



   b. Enter the following information:
      - In the TCP Port field, enter **49154**.
      - In the IP Address field, enter **172.16.1.20**.

   c. Click **Apply** to save the settings.

Show iSCSI Sessions

The example is shown as CLI commands and as web interface procedure

CLI: Show iSCSI Sessions

Use the following commands to show iSCSI sessions and session details:

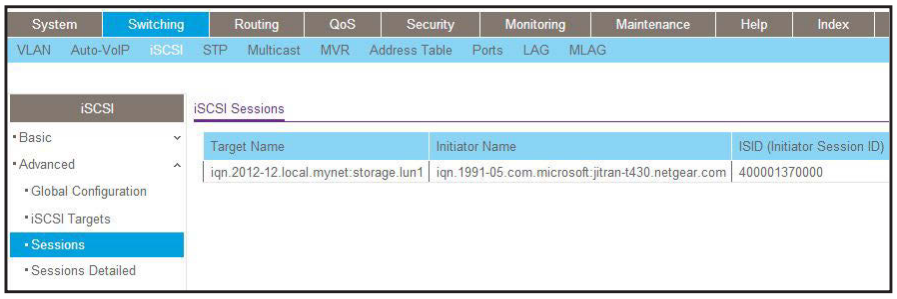
```
(Netgear Switch)  #show iscsi sessions

Session 0:
-------------------------------------------------------------------------------
Target: iqn.2012-08.com.example:storage.lun1
Initiator: iqn.1991-05.com.microsoft:netgear-think
ISID: 400001370000

(Netgear Switch)  #show iscsi sessions detailed

Session 0:
-------------------------------------------------------------------------------

Target: iqn.2012-08.com.example:storage.lun1
Initiator: iqn.1991-05.com.microsoft:netgear-think
Up Time: 00:00:04:11 (DD:HH:MM:SS)
Time for aging out: 382 secs
ISID: 400001370000

Initiator             Initiator       Target                Target
IP Address            TCP Port        IP Address            TCP Port
-------------------   -------------   -------------------   -------------
192.168.10.107        57965           192.168.10.116        3260

(Netgear Switch) #
```

The command shows that there is an active iSCSI session. The initiator is at IP address 192.168.10.107 and the Target is at IP address 192.168.10.116

Web Interface: Show iSCSI Sessions

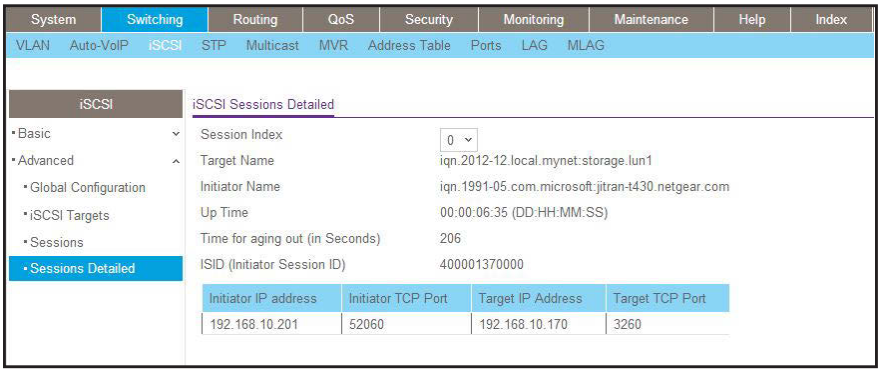
1. Show iSCSI sessions.
   a. Select **Switching > iSCSI > Advanced > Sessions**.

      A screen similar to the following displays.



2. Click **Refresh**.
3. Show the iSCSI session details.
   a. Select **Switching > iSCSI > Advanced > Sessions detailed**.

      A screen similar to the following displays.



4. Click **Refresh**.

37 Override Factory Defaults

Use another factory default configuration file

This chapter includes one section:

- *Override the Factory Default Configuration File*

Override the Factory Default Configuration File

NETGEAR managed switches support a single set of default configurations and scaling parameters, which are hard-coded in the factory default configuration file. To enable you to use a different set of default configurations and scaling parameters, you can override the factory default configuration file and specify that another file in the file system must be regarded as the factory defaults. After you issue the **clear config** privileged EXEC command, the switch uses the new factory defaults.

CLI: Install Another Factory Defaults Configuration File

1. Create a new factory default configuration file.

   The file format must be the same as the format of the startup configuration file.

2. Disable STP and LLDP MED on all interfaces.

   If the switch is not configured for STP and LLDP MED, you can skip this step.

```
(Netgear Switch) #configure
(Netgear Switch) (Config)#no spanning-tree
(Netgear Switch) (Config)#no lldp med all
```

3. Save the new factory default configuration file as a text file named factory_default.txt.
4. Download the factory_default.txt file to the switch.

```
(Netgear Switch) #copy tftp://172.26.2.100/factory_default.txt nvram:factory-defaults

Mode........................................... TFTP
Set Server IP.................................. 172.26.2.100
Path........................................... ./
Filename....................................... factory_default.txt
Data Type...................................... Text Configuration
Download configuration file. Configuration will be applied upon next reboot.
Management access will be blocked for the duration of the transfer
Are you sure you want to start? (y/n) y
File transfer in progress. Management access will be blocked for the duration of the
transfer. please wait...
File transfer successful..
```

CLI: Erase the Old Factory Default Configuration File

1. Erase the old factory default configuration file from the switch.

```
(Netgear Switch) #erase factory-default
```

2. Reload the switch.

   The new factory default configuration file (that is, the factory_default.txt. file) takes effect.

NETGEAR SFP

Small form-factor pluggable

38

This chapter includes one section:

- *Connect with NETGEAR SFP AGM731F*

Connect with NETGEAR SFP AGM731F

Cisco provides a way to support third-party small form-factor pluggables (SFPs). For example, you can get the NETGEAR SFP AGM731F to work between a Cisco switch and a NETGEAR switch.

1. Before connecting the NETGEAR switch to the Cisco switch, configure the following command on the Cisco switch.

```
service unsupported-transceiver
no errdisable detect cause gbic-invalid
```

2. Make sure that the autonegotiation mode is the same on both sides.

   The following supported AN mode can be configured on the NETGEAR switch and the Cisco switch.

XCM8944+AGM731F	CISCO+AGM731F	Result
Autonegotiate	No speed nonegotiate	Link is up
No Autonegotiate	speed nonegotiate	Link is up

Index

Numerics

6in4 tunnels 518
6to4 tunnels 524
802.1d (classic STP) 503
802.1s (MSTP) 506
802.1w (RSTP) 504
802.1x (port security) 315

A

access ports 61
accounting for commands 364
ACL mirroring 198
ACL redirection 204
ACLs (access control lists) 163
active directory (AD), MAB 389
ARP (Address Resolution Protocol)
    dynamic inspection 332
    proxy feature 152
authentication manager 366
authentication, captive portal 667
authorization
    privileged EXEC commands 359
auto VoIP 255
Automatic error recovery 417

B

backup router, VRRP 159
banner, pre-login 405
bindings, static 346
bootstrap router (BSR) 579
border routers, OSPF 108
BSR (bootstrap router) 579
buffered logs, syslog 426

C

captive portals 664
Change of authorization (CoA), RADIUS 370
class, DiffServ 231
classic STP 503
client access, captive portal 667
color conform policies, DiffServ 268
command accounting 364
compatibility, switch stack firmware 447
compatible mode, MVR 291
configuration files, switch stacks 447
configuration scripting 402
CoS (Class of Service) queuing 223

D

DAI (Dynamic ARP inspection) 332
default configuration file, overriding 681
default routes, port routing 77
dense mode, PIM 556
DHCP L2 relay 605
DHCP L3 relay 609
DHCP messages, maximum rate 347
DHCP reservation, configuring 469
DHCP servers
    configuring 466
    rogue, finding 343
DHCP snooping 339
DHCPv6 relay 488
DHCPv6 routing interface 551
DHCPv6 servers 473
Differentiated Services Code Point (DSCP)
    CoS queuing 223
    DiffServ 231
    iSCSI 674
DiffServ (Differentiated Services) 231
Distance Vector Multicast Routing Protocol ((DVMRP) 641
DNS (domain name system) 463
double VLANs (DVLANs) 492
DSCP (Differentiated Services Code Point)
    CoS queuing 223
    DiffServ 231
    iSCSI 674
dual images 410
DVLANs (double VLANs) 492
DVMRP (Distance Vector Multicast Routing Protocol)

641
Dynamic ARP inspection (DAI) 332
dynamic mode
DHCP server 466
MVR 297
dynamic port locking 305

E

edge device, DiffServ 231
email alerting, syslog 431
Error disablement 417
EXEC command authorization 359
Explicit Congestion Notification (ECN) 275

F

factory defaults, overriding 681
firmware and firmware mismatch, switch stacks 438

G

GARP (Generic Attribute Registration Protocol) 46
groups
captive portal 668
link state 658
guest VLANs 321
GVRP (GARP VLAN Registration Protocol) 46

H

host name, DNS 464
hosts, logging 428

I

IGMP (Internet Group Management Protocol) snooping and querying 279
installing, switch stacks 436
inter-area routers
IPv4 101
IPv6 475
interior node, DiffServ 231
IP ACLs 164
IP source guard 348
IPv6
ACLs 213
configuring interfaces 543
DHCPv6 servers 473
DiffServ 260
inter-area routers 475
tunnels 518
IPv6 stateless RA guard 372
iSCSI initiators and targets 674
isolated ports 52, 312
isolated VLANs 52, 184

L

LAGs (link aggregation groups) 68
levels of severity, syslog 431
limits, dynamic and static MAC addresses 306
link dependency 658
locking ports 305
Loop protection 419

M

MAB (MAC Authentication Bypass) 375
MAC ACLs 163
MAC addresses, static 308
MAC Authentication Bypass (MAB) 375
MAC-based VLANs 27
management ACLs 212
managing, switch stacks 444
mapping
CoS queues 223
static 337
master router, VRRP 157
master switch and member switches, switch stacks 434
migrating configuration, switch stacks 439
mirroring
ACLs 198
ports 406
MLD (multicast listener discovery) 624
monitoring, sFLow 457
moving, stack master 451
MSTP (multiple STP) 506
multicast routers 282
multicast VLAN registration (MVR) 290
MVR (multicast VLAN registration) 290

N

network policy server, MAB 381
Nondisruptive configuration management 420
NSSA areas, OSPF 123

O

organizationally unique identifier (OUI) 256
OSPF (Open Shortest Path First) 101

OUI-based auto VoIP 256
outbound Telnet 413

P

Per VLAN (Rapid) Spanning Tree Protocol (PV(R)STP) 508
PIM (Protocol Independent Multicast) 556
policy based routing (PBR) 146
policy server, MAB 381
policy, DiffServ 231
port analyzer 407
port mirroring 406
port routing 72
port security 305
preconfiguring, switch stack members 448
primary VLANs 52
priority values, switch stack members 436
private VLAN groups 496
private VLANs 52
promiscuous ports 52
protected ports 309
Protocol Independent Multicast (PIM) 556
protocol-based auto VoIP 255
protocol-based VLANs 31
PV(R)STP (Per VLAN (Rapid) Spanning Tree Protocol) 508

Q

queriers, IGMP 284
queues, CoS 224

R

RADIUS
  accounting server 365
  assigning VLANs 326
  captive portal authorization 670
RADIUS change of authorization (CoA) 370
redirection, ACLs 204
relay, DHCPv6 488
relays, DHCP L2 and DHCP L3 604
remote switched port analyzer (RSPAN) 407
renumbering, switch stack members 449
reverse path forwarding (RPF) 557
RIP (Routing Information Protocol) 88
rogue DHCP servers 343
route-map statement 146
routing interface, configuring for IPv6 544
routing, VLANs 81
RPF (reverse path forwarding) 557
RSPAN (remote switched port analyzer) 407
RSTP (rapid STP) 504
rules, ACLs 163

S

sampling, sFlow 460
SCCP (Skinny Call Control Protocol) 255
scheduler mode, strict priority 226
scripting, configuration 402
security, ports 305
service, DiffServ 231
Session Initiation Protocol (SIP) 255
session limit and time-out, Telnet 416
severity levels, syslog 431
sFlow monitoring 457
shaping traffic, CoS 229
Simple Network Time Protocol (SNTP) 393
SIP (Session Initiation Protocol) 255
Skinny Call Control Protocol (SCCP) 255
small form-factor pluggable (SFP) 684
SNMP (Simple Network Management Protocol) 452
snooping
  DHCP 339
  IGMP 279
  MLD 636
SNTP (Simple Network Time Protocol) 393
Spanning Tree Protocol (STP) 503
sparse mode, PIM 579
SSL certificates 672
stacking switches 433
stateful address assignment, IPv6 473
stateless DHCPv6 server 479, 483
stateless RA guard, IPv6 372
static bindings 346
static MAC addresses 308
static mapping 337
static port locking 305
static routes, port routing 78
STP (Spanning Tree Protocol) 503
strict priority schedule mode, CoS 226
stub areas, OSPF 114
subnet-based VLANs 35
switch port modes 61
switch stacks 433
system logging (syslog), logging, syslog 423

T

TACACS+ accounting server 364
target port, iSCSI 677
TCP flags, ACLs 169
Telnet, outbound 413
time zone, SNTP server 397
traceroute 401, 402
traffic shaping, CoS 229
traplogs, syslog 427
traps, SNMP 454
trunk ports 61
trust mode
    global, configuring 225
    interface, configuring for 228
trusted ports, CoS 223
tunnels, IPv6 518

U

untrusted ports, CoS 224
upgrading firmware, switch stacks 438
users, captive portal 668

V

Virtual Router Redundancy Protocol (VRRP)
    concepts and configuring 156
virtual VLANs 35
VLAN groups, private 496
VLAN priority tag (VPT) 674
VLAN routing
    concepts and configuring 81
    IPv6 547
    OSPF 134
    RIP 95
VLANs
    concepts and configuring 19
    double VLANs 492
    guest VLANs 321
    voice 38
voice VLANs 38
VoIP (voice over IP)
    auto 255
    DiffServ 248
VPTs (VLAN priority tag) 674
VRRP (Virtual Router Redundancy Protocol)
    concepts and configuring 156

W

WRED (weighted random early discard) 223
WRED explicit congestion notification 275