NETGEAR®

Configuration Example Guide

Fully Managed Switches M4250, M4300, and M4350 Series Configuration Examples for IT Installations

M4250: Firmware version 13.0.0 and later versions
M4300: Firmware version 12.0.8 and later versions
M4350: Firmware version 14.0.0 and later versions

July 2025
202-12617-01

NETGEAR, Inc.
350 East Plumeria Drive
San Jose, CA 95134, USA

Support and Community

Visit netgear.com/support to get your questions answered and access the latest downloads.

You can also check out our NETGEAR Community for helpful advice at community.netgear.com.

Regulatory and Legal

Si ce produit est vendu au Canada, vous pouvez accéder à ce document en français canadien à https://www.netgear.com/support/download/.

(If this product is sold in Canada, you can access this document in Canadian French at https://www.netgear.com/support/download/.)

For regulatory compliance information including the EU Declaration of Conformity, visit https://www.netgear.com/about/regulatory/.

See the regulatory compliance document before connecting the power supply.

For NETGEAR's Privacy Policy, visit https://www.netgear.com/about/privacy-policy.

By using this device, you are agreeing to NETGEAR's Terms and Conditions at https://www.netgear.com/about/terms-and-conditions. If you do not agree, return the device to your place of purchase within your return period.

This product is designed and warranted for indoor use only. Do not use this device outdoors. The PoE source is intended for intra building connection only.

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
202-12617-01	July 2025	Initial publication of this guide for the M4250, M4300 and M4350 series switches.

Chapter 1 Introduction and Documentation

Available documentation 21
Naming convention: slot/port or unit/slot/port 21

Chapter 2 VLANs

VLAN concepts. 25
Auto-Trunk 26
CLI: Enable the Auto-Trunk feature 27
Main UI: Enable the Auto-Trunk feature 27
Create three VLANs 28
CLI: Create three VLANs. 28
Main UI: Create three VLANs 28
Create two VLANs, assign ports to the VLANs, and assign one VLAN as a default VLAN for a port 30
Create two VLANs 30
CLI: Create two VLANs. 30
Main UI: Create two VLANs. 31
Assign ports to VLAN 2. 32
CLI: Assign ports to VLAN 2 32
Main UI: Assign ports to VLAN 2 32
Assign ports to VLAN 3. 33
CLI: Assign ports to VLAN 3 34
Main UI: Assign ports to VLAN 3 34
Assign a default VLAN to a port 35
CLI: Assign VLAN 3 as the default VLAN for port 1/0/2 35
Main UI: Assign VLAN 3 as the default VLAN for port 1/0/2 35
Create a MAC-based VLAN. 36
CLI: Create a MAC-based VLAN 36
Main UI: Assign a MAC-based VLAN 37
Create a protocol-based VLAN. 39
CLI: Create a protocol-based VLAN 39
Main UI: Create a protocol-based VLAN 41
Virtual VLANs: Create an IP subnet–based VLAN 44
CLI: Create an IP subnet–based VLAN 45
Main UI: Create an IP subnet–based VLAN 46
Voice VLANs. 47
Voice VLAN interoperation with Auto-VoIP 49
CLI: Configure a Voice VLAN and prioritize voice traffic 51
Main UI: Configure Voice VLAN and prioritize voice traffic 53
Configure GARP VLAN Registration Protocol. 58
CLI: Enable GVRP 59
Main UI: Configure GVRP on switch A 61
Main UI: Configure GVRP on Switch B 63
Private VLANs. 64
Assign private VLAN types (primary, isolated, community) 66
CLI: Assign private VLAN types (primary, isolated, community). . . 66
Main UI: Assign private VLAN types (primary, isolated,

community) 67
Configure a private VLAN association 68
CLI: Configure a private VLAN association 68
Main UI: Configure a private VLAN association 69
Configure the private VLAN port mode (promiscuous, host). 69
CLI: Configure the private VLAN port mode (promiscuous, host) 69
Main UI: Configure the private VLAN port mode (promiscuous, host) 70
Configure private VLAN host ports. 71
CLI: Configure private VLAN host ports 71
Main UI: Configure private VLAN host ports 71
Map a private VLAN promiscuous port 73
CLI: Map a private VLAN promiscuous port. 73
Main UI: Map a private VLAN promiscuous port 73
VLAN access ports and trunk ports 74
CLI: Configure a VLAN trunk 75
Main UI: Configure a VLAN trunk 76

Chapter 3 LAGs

Link aggregation concepts 82
Add ports to LAGs 83
CLI: Add ports to LAG. 83
Main UI: Add ports to LAGs 83
Auto-LAG 84
CLI: Enable the Auto-LAG feature. 85
Main UI: Enable the Auto-LAG feature 86

Chapter 4 Port Routing

Port routing concepts 88
Port routing configuration 88
Enable routing for the switch 89
CLI: Enable routing for the switch. 89
Main UI: Enable routing for the switch 90
Enable routing for ports on the switch 90
CLI: Enable routing for ports on the switch. 91
Main UI: Enable routing for ports on the switch 91
Add a default route 93
CLI: Add a default route 93
Main UI: Add a default route 94
Add a static route 94
CLI: Add a static route 95
Main UI: Add a static route. 95

Chapter 5 VLAN Routing

VLAN routing concepts. 98

Create two VLANs in preparation for VLAN routing 98
CLI: Configure two VLANs 99
Main UI: Configure two VLANs 100
Set up VLAN routing for VLANs and the switch 103
CLI: Set up VLAN routing for the VLANs and the switch 103
Main UI: Set up VLAN routing for the VLANs and the switch 104

Chapter 6 RIP

Routing Information Protocol concepts 106
Enable routing for the switch in preparation of RIP 107
CLI: Enable routing for the switch 107
Main UI: Enable routing for the switch 107
Enable routing for ports in preparation of RIP 108
CLI: Enable routing and assign IP addresses to ports 108
Main UI: Enable routing and assign IP addresses to ports 108
Enable RIP on the switch 110
CLI: Enable RIP on the Switch 110
Main UI: Enable RIP on the switch 110
Enable RIP for ports 111
CLI: Enable RIP for ports 1/0/2 and 1/0/3 111
Main UI: Enable RIP for ports 1/0/2 and 1/0/3 112
Configure VLAN routing with RIP support 113
CLI: Configure VLAN Routing with RIP support 113
Main UI: Configure VLAN Routing with RIP support 115

Chapter 7 OSPF

Open Shortest Path First concepts 119
Inter-area router 119
CLI: Configure an inter-area router 120
Main UI: Configure an inter-area router 122
OSPF on a switch that functions as a border router 125
CLI: Configure OSPF on a switch that functions as a border router 125
Main UI: Configure OSPF on a switch that functions as a border router 127
Stub areas 131
CLI: Configure Area 1 as a stub area on Switch A1 131
Main UI: Configure Area 1 as a stub area on Switch A1 133
CLI: Configure Area 1 as a stub area on Switch A2 136
Main UI: Configure Area 1 as a stub area on Switch A2 137
NSSA areas 140
CLI: Configure Area 1 as an NSSA area on Switch A1 140
Main UI: Configure Area 1 as an NSSA area on Switch A1 142
CLI: Configure Area 1 as an NSSA area on Switch A2 145
Main UI: Configure Area 1 as an NSSA area on Switch A2 147
VLAN routing with OSPF 151
CLI: Configure VLAN routing with OSPF 152

Main UI: Configure VLAN routing with OSPF 153
OSPFv3 156
CLI: Configure OSPFv3 156
Main UI: Configure OSPFv3 158

Chapter 8 PBR

Policy-based routing concepts 162
Route-map statements 162
PBR processing logic 163
PBR configurations 165
PBR example 165

Chapter 9 ARP

Proxy ARP concepts 169
Configure Proxy ARP on a port 169
CLI: Configure Proxy ARP on a port 169
Main UI: Configure Proxy ARP on a port 170

Chapter 10 VRRP

Virtual Router Redundancy Protocol concepts 172
Configure VRRP on a primary router 173
CLI: Configure VRRP on a primary router 173
Main UI: Configure VRRP on a primary router 174
Configure VRRP on a secondary router 175
CLI: Configure VRRP on a secondary router 175
Main UI: Configure VRRP on a secondary router 177

Chapter 11 ACLs

Access Control List concepts 180
MAC ACLs 180
IP ACLs 181
ACL configuration 181
Set up an IP ACL with two rules 181
CLI: Set up an IP ACL with two rules 182
Main UI: Set up an IP ACL with two rules 183
Configure one-way access using a TCP flag in an ACL 187
CLI: Configure one-way access using a TCP flag in an ACL 188
CLI Step 1: Configure VLANs, IP addresses, static routes, and ACLs on Switch A 188
CLI Step 2: Configure VLANs, IP addresses, and static routes on Switch B 190
Main UI: Configure one-way access using a TCP flag in an ACL 192
Main UI Step 1: Configure VLANs, IP addresses, static routes, and ACLs on Switch A 192
Main UI Step 2: Configure VLANs, IP addresses,

and static routes on Switch B 199
Use ACLs to isolate VLANs on a Layer 3 switch 202
CLI: Configure ACLs that isolate VLANs. 203
Main UI: Configure ACLs that isolate VLANs. 205
Set up a MAC ACL with two rules. 213
CLI: Set up a MAC ACL with two rules 213
Main UI: Set up a MAC ACL with two rules 214
Configure ACL mirroring 216
CLI: Configure ACL mirroring 217
Main UI: Configure ACL mirroring 218
Configure ACL redirection for a traffic stream 221
CLI: Configure an ACL that redirects a traffic stream. 222
Main UI: Configure an ACL that redirects a traffic stream 223
Add ACL remarks 226
Manage ACL rule sequences 227
CLI: Add an IP ACL with rules without specifying sequence numbers 228
CLI: Change sequence numbers and increments numbers for ACL rules. 229
Configure a management ACL. 231
CLI: Add an ACL to the CPU port, permitting any host to access the switch through Telnet or HTTP 232
CLI: Add an ACL to the CPU port, permitting a specific host to access the switch through SSH only. 232
Configure an IPv6 ACL. 233
CLI: Configure an IPv6 ACL 234
Main UI: Configure an IPv6 ACL 236

Chapter 12 CoS Queuing

CoS queuing concepts 242
CoS queue mapping 242
Trusted ports 242
Untrusted ports 243
CoS queue configuration 243
Show the trust mode for a class of service. 244
CLI: Show the trust mode for a class of service 244
Main UI: Show the trust mode for a class of service. 244
Set the trust mode for a class of service 244
CLI: Set the trust mode for a class of service 244
Main UI: Set the trust mode for a class of service. 245
Configure CoS queue minimum bandwidth and strict priority scheduler mode. 245
CLI: Configure CoS queue minimum bandwidth and strict priority scheduler mode 245
Main UI: Configure CoS queue minimum bandwidth and strict priority scheduler mode 245
Set the CoS trust mode for an interface 247
CLI: Set the CoS trust mode for an interface. 247

Main UI: Set the CoS trust mode for an interface 247
Configure traffic shaping 248
CLI: Configure traffic shaping 248
Main UI: Configure traffic shaping 248

Chapter 13 DiffServ

Differentiated services concepts 251
Configure DiffServ to allocate bandwidth 252
CLI: Configure DiffServ to allocate bandwidth 252
Main UI: Configure DiffServ to allocate bandwidth 255
Configure DiffServ for VoIP 267
CLI: Configure DiffServ for VoIP 268
Main UI: Diffserv for VoIP 270
Configure Auto VoIP 275
Protocol-based Auto VoIP 275
OUI-based Auto VoIP 276
Example 1: Enable protocol-based Auto VoIP 277
CLI: Enable protocol-based Auto VoIP 277
Main UI: Enable protocol-based Auto VoIP 278
Example 2: Change the queue of protocol-based Auto VoIP 278
CLI: Change the queue of protocol-based Auto VoIP 278
Main UI: Change the queue of protocol-based Auto VoIP 279
Example 3: Create an Auto VoIP VLAN 280
CLI: Create an Auto VoIP VLAN 280
Main UI: Change the Auto VoIP VLAN 281
DiffServ for IPv6 282
CLI: Configure DiffServ for IPv6 282
Main UI: Configure DiffServ for IPv6 284
Color conform policy 287
CLI: Configure a color conform policy 287
Main UI: Configure a color conform policy 288
Weighted random early detection 294

Chapter 14 IGMP Snooping and Querier

Internet Group Management Protocol concepts 297
Enable IGMP snooping 297
CLI: Enable IGMP snooping 297
Main UI: Enable IGMP snooping 298
Display the IGMP snooping configuration 299
CLI: Display the IGMP snooping configuration 299
Main UI: Display the IGMP snooping configuration 299
Display the IGMP snooping group information 300
CLI: Display the IGMP snooping group table 300
Main UI: Display the IGMP snooping group table 300
Multicast router interface 301
CLI: Configure a multicast router interface 301

Main UI: Configure a multicast router interface 301
Multicast router VLAN 302
CLI: Configure a multicast router VLAN 302
Main UI: Configure a multicast router VLAN 302
IGMP Querier concepts 303
Enable the IGMP querier 304
CLI: Enable the IGMP querier 304
Main UI: Enable the IGMP Querier 304
Display the IGMP querier status 306
CLI: Display the IGMP querier status 306
Main UI: Display IGMP querier status 307

Chapter 15 MVR

Multicast VLAN registration 309
Configure MVR in compatible mode 310
CLI: Configure MVR in compatible mode 311
Main UI: Configure MVR in compatible mode 313
Configure MVR in dynamic mode 317
CLI: Configure MVR in dynamic mode 317
Main UI: Configure MVR in dynamic mode 320

Chapter 16 MAB

MAC Authentication Bypass concepts 325
MAB and authentication servers 326
Configure MAC authentication bypass on a switch 327
CLI: Configure the switch to perform MAB with a RADIUS server . . . 327
Main UI: Configure the switch to perform MAB with a RADIUS server 329

Chapter 17 Security Management

Port security concepts 333
Set dynamic and static MAC address limits on a port 334
CLI: Set the dynamic and static MAC address limits on a port 334
Main UI: Set the dynamic and static MAC address limits on a port . . 335
Convert dynamically learned MAC addresses to static addresses 336
CLI: Convert dynamically learned MAC addresses to static addresses 336
Main UI: Convert dynamically learned MAC addresses to static addresses 336
Create a static MAC address 337
CLI: Create a static MAC address 337
Main UI: Create a static MAC address 337
Protected ports 338
CLI: Configure protected ports to isolate ports on the switch 339
Main UI: Configure protected ports to isolate ports on the switch . . 340
802.1x port security 344
CLI: Authenticate dot1x users through a RADIUS server 345

Main UI: Authenticate dot1x users through a RADIUS server 346
Create a guest VLAN 349
CLI: Create a guest VLAN. 351
Main UI: Create a guest VLAN. 353
Assign VLANs using RADIUS 356
CLI: Assign VLANS using RADIUS. 357
Main UI: Assign VLANS using RADIUS. 359
Dynamic ARP inspection 361
CLI: Configure Dynamic ARP inspection 362
Main UI: Configure Dynamic ARP inspection 364
Static mapping for dynamic ARP inspection 366
CLI: Configure static mapping for dynamic ARP inspection 366
Main UI: Configure static mapping for dynamic ARP inspection. . . . 367
DHCP snooping 368
CLI: Configure DHCP snooping 369
Main UI: Configure DHCP snooping 370
Find a rogue DHCP server. 371
CLI: Find a rogue DHCP server 371
Main UI: Find a rogue DHCP server 373
Enter a static binding into the binding database 375
CLI: Enter a static binding into the binding database. 375
Main UI: Enter a static binding into the binding database 375
Maximum rate of DHCP messages 376
CLI: Configure the maximum rate of DHCP messages 376
Main UI: Configure the maximum rate of DHCP messages 377
IP Source Guard 377
CLI: Configure IP Source Guard 378
Main UI: Configure IP Source Guard 380
Command authorization for the CLI 382
CLI Example 1: Configure command authorization by a TACACS+ server 382
CLI Example 2: Configure command authorization by a RADIUS server 385
Privileged Exec Command mode authorization for the CLI 388
CLI Example 1: Configure EXEC authorization by a TACACS+ server 388
CLI Example 2: Configure EXEC authorization by a RADIUS server . 391
Accounting. 393
CLI: Configure Telnet command accounting by a TACACS+ server 393
CLI: Configure Telnet EXEC accounting by a RADIUS server. 394
Use the authentication manager to set up an authentication method list 395
Dot1x MAB authentication method lists 396
Dot1x MAB authentication method list with MAB dot1x priority. . . . 396
Dot1x, MAB, and captive portal authentication method list with default priority 397
RADIUS change of authorization 398

IPv6 Stateless RA Guard 400
CLI: Configure IPv6 RA Guard 401
Change SSH and Telnet login authentication to RADIUS 402
CLI: Change the SSH and Telnet login authentication to RADIUS . . . 402
Main UI: Change the SSH and Telnet login authentication to RADIUS 403

Chapter 18 NTP

Network Time Protocol concepts 407
Show commands for NTP in the CLI 407
show ntp 407
show ntp authentication-keys 407
show ntp information 408
show ntp packets 408
show ntp servers 408
show ntp status 409
Configure NTP 409
CLI: Configure an NTP server and an NTP source interface 409
Main UI: Configure an NTP server and an NTP source interface 410
Set the time zone 412
CLI: Set the time zone 412
Main UI: Set the time zone 412
Configure a NETGEAR NTP server using its DNS address 413
CLI: Configure a NETGEAR NTP server using its DNS address 413
Main UI: Configure a NETGEAR NTP server using its DNS address . 413

Chapter 19 SNTP

Simple Network Time Protocol concepts 416
Show commands for SNTP in the CLI 416
show sntp 416
show sntp client 416
show sntp server 417
show sntp source-interface 417
Configure SNTP and set the time zone 417
CLI: Configure SNTP and set the time zone 418
Main UI: Configure SNTP and set the time zone 419
Configure a NETGEAR SNTP server using its DNS address 420
CLI: Configure a NETGEAR SNTP server using its DNS address 421
Main UI: Configure a NETGEAR SNTP server using its DNS address 421

Chapter 20 Tools

Trace a route 424
CLI: Trace a route 424
Main UI: Trace a route 425
Configuration scripting (CLI only) 425
Pre-login banner (CLI only) 426

Create a Pre-login banner and upload it to the switch 426
Port mirroring. 427
CLI: Specify a source port and a destination port 427
Main UI: Specify a source port and a destination port 428
Remote SPAN 428
CLI: Enable RSPAN on source, intermediate, and destination switches 429
CLI: Configure the source switch (Switch 1). 429
CLI: Configure the intermediate switches (Switch 2 and Switch 3). 430
CL:I: Configure the destination switch (Switch 4) 431
Main UI: Enable RSPAN on source, intermediate, and destination switches 432
Main UI: Configure the source switch (Switch 1). 432
Main UI: Configure the intermediate switches (Switch 2 and Switch 3). 435
Main UI: Configure the destination switch (Switch 4). 436
Dual Image feature 438
CLI: Download a backup image and make it active 439
Main UI: Download a backup image and make it active. 440
Outbound Telnet. 441
Configure outbound Telnet 442
CLI: Configure outbound Telnet 442
Main UI: Configure outbound Telnet 442
Configure the outbound Telnet session limit and session time-out . 443
CLI: Configure the outbound Telnet session limit and session time-out 443
Main UI: Configure the outbound Telnet session limit and session time-out 443
Error disablement and automatic error recovery (CLI only). 444
Loop protection 446
CLI: Enable loop protection. 447
Main UI: Enable loop protection. 448
Nondisruptive Configuration Management feature (CLI only). 449
Full memory dump 449
CLI: Perform a full memory dump. 450
Main UI: Perform a full memory dump. 451

Chapter 21 Syslog

Syslog concepts 453
Syslog message logging 453
CLI: Configure the syslog settings and display the syslog messages 454
Main UI: Configure the syslog settings and display the syslog messages 455
Trap logs. 457
CLI: Display the trap logs 458
Main UI: Display the trap logs 458

Logging 459
CLI: Configure logging for a port and display the syslog server 459
Main UI: Configure logging for a port and display the syslog server 460
Email alerting (CLI only) 460

Chapter 22 Switch Stacks

Switch stack management and connectivity 464
Stack management switch and stack members 464
Stack management switch 465
Stack members 466
Stack member numbers 466
Stack member priority values 467
Install a switch stack 467
Stack switches using 10G Ethernet ports 468
CLI: Configure 10G Ethernet ports as stack ports 469
Main UI: Configure 10G Ethernet ports as stack ports 471
Switch firmware and firmware mismatch 472
Upgrade the firmware 473
Migrate configuration with a firmware upgrade 474
Manually copy the firmware of the stack management switch to a stack member 474
CLI: Copy the firmware of the stack management switch to a stack member 475
Main UI: Copy the firmware of the stack management switch to a stack member 475
Add, remove, or replace a stack member 475
Add switches to an operating stack 475
Remove a switch from a stack 476
Replace a stack member 477
Switch stack configuration files 478
Preconfigure a switch 479
Renumber stack members 480
CLI: Renumber stack members 481
Main UI: renumber stack members 481
Make a different unit the stack management switch 482
CLI: Make a different unit the stack management switch 482
Main UI: Make a different unit the stack management switch 483

Chapter 23 SNMP and sFlow

Add a new SNMP community 485
CLI: Add a new SNMP community 485
Main UI: Add a new SNMP community 485
Enable an SNMP trap 486
CLI: Enable an SNMP trap 486
Main UI: Enable an SNMP trap 486
SNMPv3 users 487
CLI: Add an SNMPv3 user 487

Main UI: Add an SNMPv3 user 488
sFlow 488
CLI: Configure statistical packet-based sampling of packet flows with sFlow 489
Main UI: Configure statistical packet-based sampling with sFlow . . 491
Time-based sampling of counters with sFlow 492
CLI: Configure time-based sampling of counters with sFlow 492
Main UI: Configure time-based sampling of counters with sFlow. . . 492

Chapter 24 DNS

Domain Name System concepts 495
Specify two DNS servers 495
CLI: Specify two DNS servers and ping a DNS name 495
Main UI: Specify two DNS servers and ping a DNS name 496
Manually add a host name and an IP address 497
CLI: Manually add a host name and an IP address and ping a DNS name 497
Main UI: Manually add a host name and an IP address and ping a DNS name 498

Chapter 25 DHCP Server

Dynamic host configuration protocol concepts 500
Configure a DHCP server in dynamic mode 500
CLI: Configure a DHCP server in dynamic mode 500
Main UI: Configure a DHCP server in dynamic mode 501
Configure a DHCP server that assigns a fixed IP address 504
CLI: Configure a DHCP server that assigns a fixed IP address 504
Main UI: Configure a DHCP server that assigns a fixed IP address . . 505

Chapter 26 DHCPv6 Server

DHCPv6 concepts 508
Configure DHCPv6 prefix delegation 509
CLI: Configure DHCPv6 prefix delegation 509
Main UI: Configure DHCPv6 prefix delegation. 511
Configure a stateless DHCPv6 server 515
CLI: Configure a stateless DHCPv6 server. 515
Main UI: Configure a stateless DHCPv6 server. 516
Configure a stateful DHCPv6 server 519
CLI: Configure a stateful DHCPv6 server. 519
Main UI: Configure a stateful DHCPv6 server 520
Set up a configuration with a DHCPv6 server and DHCPv6 relay. 523
CLI: Set up a configuration with a DHCPv6 server and DHCPv6 relay 524
CLI: Configure the DHCPv6 server, add a static route, and display the IPv6 binding information 524
CLI: Configure the DHCPv6 relay 525

Main UI: Set up a configuration with a DHCPv6 server and DHCPv6 relay 526
Main UI: Configure the DHCPv6 server, add a static route, and display the IPv6 binding information 527
Main UI: Configure the DHCPv6 relay 531

Chapter 27 DVLANs and Private VLANs

Double VLANs 538
CLI: Create and enable a double VLAN 539
Main UI: Create and enable a double VLAN 540
Private VLAN groups 542
CLI: Create private VLAN groups 543
Main UI: Create private VLAN groups 544

Chapter 28 STP

Spanning Tree Protocol concepts 549
Configure Classic STP (802.1d) 549
CLI: Configure Classic STP (802.1d) 549
Main UI: Configure Classic STP (802.1d) 550
Configure Rapid STP (802.1w) 551
CLI: Configure Rapid STP (802.1w) 551
Main UI: Configure Rapid STP (802.1w) 551
Configure Multiple STP (802.1s) 552
CLI: Configure Multiple STP (802.1s) 552
Main UI: Configure Multiple STP (802.1s) 553
Configure PVSTP and PVRSTP 555
CLI: Configure PVSTP 556
CLI: Configure PVSTP on Switch 1 557
CLI: Configure PVSTP on Switch 2 558
Main UI: Configure PVSTP 558
Main UI: Configure PVSTP on Switch 1 559
Main UI: Configure PVSTP on Switch 2 561

Chapter 29 IPv6 Interface Configuration

Create an IPv6 routing interface 564
CLI: Create an IPv6 routing interface 564
Main UI: Create an IPv6 routing interface 565
Create an IPv6 routing VLAN 567
CLI: Create an IPv6 routing VLAN 567
Main UI: Create an IPv6 VLAN routing Interface 569
Configure DHCPv6 mode on a routing interface 572
CLI: Configure DHCPv6 mode on a routing interface 573
Main UI: Configure DHCPv6 mode on a routing Interface 574

Chapter 30 Tunnels for IPv6

IPv6 tunnel concepts 577

Create a 6in4 tunnel 577
CLI: Create a 6in4 tunnel 578
CLI: Create a 6in4 tunnel on Switch 1 578
CLI: Create a 6in4 tunnel on Switch 2 579
Main UI: Create a 6in4 tunnel 580
Main UI: Create a 6in4 tunnel on Switch 1 580
Main UI: Create a 6in4 tunnel on Switch 2 582
Create a 6to4 tunnel. 583
CLI: Create a 6to4 tunnel 584
CLI: Create a 6to4 tunnel on Switch 1. 584
CLI: Create a 6to4 tunnel on Switch 2. 586
CLI: Create a 6to4 tunnel on Switch 3. 587
Main UI: Create a 6to4 tunnel 589
Main UI: Create a 6to4 tunnel on Switch 1 589
Main UI: Create a 6to4 tunnel on Switch 2 594
Main UI: Create a 6to4 tunnel on Switch 3 597

Chapter 31 PIM

Protocol Independent Multicast concepts. 603
PIM-DM. 603
CLI: Configure PIM-DM 605
CLI: Configure PIM-DM on Switch A 605
CLI: Configure PIM on Switch B 606
CLI: Configure PIM-DM on Switch C 607
CLI: Configure PIM-DM on Switch D 608
CLI: Display the multicast route table on Switches A, B, C, and D 609
Main UI: Configure PIM-DM. 610
Main UI: Configure PIM-DM on Switch A 610
Main UI: Configure PIM-DM on Switch B 615
Main UI: Configure PIM-DM on Switch C 618
Main UI: Configure PIM-DM on Switch D 622
PIM-SM 627
CLI: Configure PIM-SM 628
CLI: Configure PIM-SM on Switch A 628
CLI: Configure PIM-SM and RP and BSR candidate configurations on Switch B 629
CLI: Configure PIM-SM and RP and BSR candidate configurations on Switch C 630
CLI: Configure PIM-SM, RP and BSR candidate configurations, and IGMP on Switch D. 631
CLI: Display the Multicast Route Table on Switches, A, B, C, and D 633
Main UI: Configure PIM-SM 634
Main UI: Configure PIM-SM on Switch A. 634
Main UI: Configure PIM-SM and RP and BSR candidate configurations on Switch B 638
Main UI: Configure PIM-SM and RP and BSR candidate configurations

on Switch C 642
Main UI: Configure PIM-SM, RP and BSR candidate configurations, and IGMP on Switch D 647

Chapter 32 DHCP L2 Relay and L3 Relay

DHCP L2 relay 655
CLI: Configure DHCP L2 relay 656
Main UI: Configure DHCP L2 relay 657
DHCP L3 relay 660
CLI: Configure DHCP L3 Relay 661
Main UI: Configure DHCP L3 relay 662

Chapter 33 MLD

Multicast Listener Discovery concepts 666
Configure MLD 666
CLI: Configure MLD. 667
CLI: Configure MLD on Switch A 667
CLI: Configure MLD on Switch B 668
Main UI: Configure MLD. 670
Main UI: Configure MLD on Switch A 670
Main UI: Configure MLD on Switch B 674
Configure MLD snooping 679
CLI: Configure MLD snooping. 680
Main UI: Configure MLD snooping. 681

Chapter 34 DVMRP

Distance Vector Multicast Routing Protocol concepts 685
Configure DVMRP. 685
CLI: Configure DVMRP 686
CLI: Configure DVMRP on Switch A. 686
CLI: Configure DVMRP on Switch B. 688
CLI: Configure DVMRP on Switch C 690
Main UI: Configure DVMRP 693
Main UI: Configure DVMRP on Switch A. 693
Main UI: Configure DVMRP on Switch B. 696
Main UI: Configure DVMRP on Switch C. 698

Chapter 35 PTP End-to-End Transparent Clock

PTP concepts 704
PTP time stamp operation 705
PTP transparent clock concepts 705
Manage the PTP end-to-end transparent clock 706
CLI: Manage the PTP end-to-end transparent clock 706
CLI: Globally disable the PTP end-to-end transparent clock. . . . 707
CLI: Disable the PTP end-to-end transparent clock for an interface 707

CLI: Globally reenable the PTP end-to-end transparent clock . . 707
CLI: Reenable the PTP end-to-end transparent clock for an interface 707
CLI: Display the PTP end-to-end transparent clock status 708
Main UI: Manage the PTP end-to-end transparent clock 709
Main UI: Globally disable the PTP end-to-end transparent clock 709
Main UI: Disable the PTP end-to-end transparent clock for an interface 710
Main UI: Globally reenable the PTP end-to-end transparent clock 711
Main UI: Reenable the PTP end-to-end transparent clock for an interface and display the clock status 712

Chapter 36 Audio Video Bridging

AVB concepts 714
MRP 714
MMRP 715
MVRP 715
MSRP 715
802.1AS 716
Enable AVB on the switch and configure AVB on interfaces 717
CLI: Enable AVB on the switch and configure AVB on interfaces . . . 717
Main UM: Enable AVB on the switch and configure AVB on interfaces 718

Chapter 37 Link Dependency

Link Dependency concepts 722
Create a link state group 723
CLI: Create a link state group 723
Main UI: Create a link state group 724

Chapter 38 Captive Portals

Captive portal concepts 727
Captive portal client concepts 728
Enable a captive portal 728
CLI: Enable a captive portal 728
Main UI: Enable a captive portal 729
Block a captive portal instance 730
CLI: Block a captive portal instance 730
Main UI: Block a captive portal instance 731
Create users and groups for local authentication 731
CLI: Create a group and a user and add the user to the group 732
Main UI: Create a group and a user and add the user to the group . 733
RADIUS user configuration 734
CLI: Configure RADIUS as the verification mode for a captive portal 735

Main UI: Configure RADIUS as the verification mode for a captive portal 735
SSL certificate concepts 735

Chapter 39 iSCSI

iSCSI concepts 738
Enable iSCSI awareness with a VLAN priority tag 739
CLI: Enable iSCSI awareness with a VLAN priority tag 739
Main UI: Enable iSCSI awareness with a VLAN priority tag 739
Enable iSCSI awareness with DSCP 740
CLI: Enable iSCSI awareness with DSCP 740
Main UI: Enable iSCSI awareness with DSCP 740
Set the iSCSI target port 741
CLI: Set the iSCSI target port 741
Main UI: Set the iSCSI target port 741
Display iSCSI sessions 742
CLI: Display iSCSI sessions 742
Main UI: Display iSCSI sessions 743

Chapter 40 Override Factory Defaults

About overriding the factory default configuration file 745
Install another factory default configuration file 745

Chapter 41 NETGEAR SFP

Connect a NETGEAR SFP transceiver module to a third-party switch . . 748

Index

1

Introduction and Documentation

This Configuration Example Guide for IT is for the Fully Managed Switches M4250, M4300, and M4350 Series and covers all M4250, M4300, and M4350 switch models.

This guide is specifically for IT installations (as opposed to ProAV installations).

The guide provides selected configuration examples for the command-line interface (CLI) and main user interface (main UI).

This chapter includes the following sections:

- Available documentation
- Naming convention: slot/port or unit/slot/port

For each chapter in this guide, the supported switch series is stated for the feature that is described in the chapter, using the following color coding:

- Green: **This feature is supported on the M4250 series switches**
- Red: **This feature is supported on the M4300 series switches**
- Blue: **This feature is supported on the M4350 series switches**

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

Note: Firmware updates with new features and bug fixes are made available from time to time at netgear.com/support/download/. 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 does not match what is described in this guide, you might need to update your firmware.

Available documentation

You can download the following guides and manuals for the Fully Managed Switches M4250, M4300, and M4350 Series:

- Hardware Installation Guide
- Main User Manual
- Audio Video User Manual
- CLI Command Reference Manual
- Configuration Example Guide (this manual)

For more information, and depending on your model, visit one of the following sites:

- **M4250 series**: netgear.com/support/product/m4250/#docs
- **M4300 series**: netgear.com/support/product/m4300/#docs
- **M4350 series**: netgear.com/support/product/m4350#docs

Naming convention: slot/port or unit/slot/port

An M4250 series switch references physical entities such as ports by using a *slot/port* naming convention because stacking is not supported.

An M4300 or M4350 series switch references physical entities such as ports by using a *unit/slot/port* naming convention because stacking is supported. The *unit* parameter indicates the stack unit number.

The switch also uses this convention to identify certain logical entities, such as port channel interfaces (link aggregation groups, abbreviated as LAGs).

The port identifies the specific physical port or logical interface.

Table 1. Types of ports

Port Type	Description
M4250 series switch: Physical interfaces	The physical interface number consists of the slot number (which is always 0) followed by a forward slash, and the port number, which is a sequential number starting from 1. Examples: • port 1 is 0/1 • port 2 is 0/2 • port 3 is 0/3 • and so on for other ports

Table 1. Types of ports

Port Type	Description
M4300 and M4350 series switch: Physical interfaces	The physical interface number consists of the switch unit number (from 1 to 8) followed by a forward slash, the slot number (which is always 0) followed by a forward slash, and the port number, which is a sequential number starting from 1. Examples: • **Standalone switch**: For a switch that is not a member of a stack (that is, a standalone switch), port 1 is 1/0/1, port 2 is 1/0/2, port 3 is 1/0/3, and so on. • **Stacked switch**: For a switch that is a member of a stack, the port numbering is as follows: - Stack unit 2: port 1 is 2/0/1, port 2 is 2/0/2, port 3 is 2/0/3, and so on - Stack unit 3: port 1 is 3/0/1, port 2 is 3/0/2, port 3 is 3/0/3, and so on - and so on for other stack units, up to stack unit number 8
Logical Interfaces	• Port-channel or Link Aggregation Group (LAG) interfaces are logical interfaces that are used only for bridging functions. • VLAN routing interfaces are used only for routing functions. • Loopback interfaces are logical interfaces that are always up. • For an M4250 or M4300 series switch only, tunnel interfaces are logical point-to-point links that carry encapsulated packets. **Note:** In the CLI, loopback interfaces do not use the slot/port format (M4250 series switches) or unit/slot/port (M4300 and M4350 series switches) format. To specify a loopback interface, you use the loopback ID. **Note:** For an M4250 series switch only, in the CLI, tunnel interfaces do not use the slot/port format (M4250 series switches). To specify a tunnel interface, you use the tunnel ID.
CPU ports	CPU ports are handled by the driver as one or more physical entities.
Routing VLAN interfaces	This is an interface used for routing functionality: Examples: • VLAN 1 • VLAN 2 • VLAN 3 • and so on

Note: About the interface designation in the examples in this guide:

Most examples in this guide use the *unit/slot/port* interface designation, in which *port* is the interface number. This is the designation that the M4300 and M4350 series switches use. However, for the M4250 series switches, adjust the example to use the *slot/port* designation, in which *port* is the interface number.

Note: About the figures in the main UI examples in this guide:

Each figure that displays a main UI page is preceded by the following text: “A page similar to the following figure displays.” The reason is that different switch series, and within a switch series, different models support different features.
In some figures, menu options that are now supported are not displayed. In other figures, menu options that are no longer supported are displayed. However, each figure effectively covers the configuration example that it is illustrating. Therefore you can ignore any differences between a main UI page on your model and a figure in an example.

2

VLANs

Virtual LANs

This feature is supported on the M4250 series switches

This feature is supported on the M4300 series switches

This feature is supported on the M4350 series switches

This chapter includes the following sections:

- VLAN concepts
- Auto-Trunk
- Create three VLANs
- Create two VLANs, assign ports to the VLANs, and assign one VLAN as a default VLAN for a port
- 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
- 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, which NETGEAR calls the Private 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 following diagram shows a Layer 3 switch with three ports configured to handle the traffic for two VLANs (VLAN 10 and VLAN 20). Ports 1/0/1 and 1/0/2 are part of a link aggregation group (LAG) for fault tolerance and increased throughput, and the LAG is a member of VLAN 10. Port 1/0/3 is a member of VLAN 20.

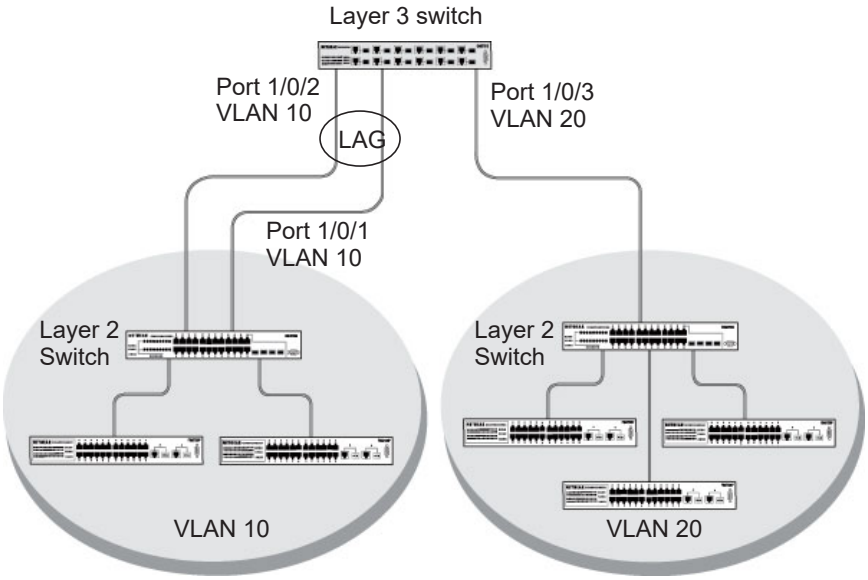


Figure 1. Layer 3 switch with three ports configured for traffic from two VLANs

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

Auto-Trunk

Auto-trunk is a feature that lets the switch automatically enable Trunk mode on capable physical links and LAG interfaces between partner devices. A trunk can carry all active VLANs. By default, the Auto-Trunk feature is enabled on the switch.

If the switch automatically configures a port as a trunk (that is, an Auto-Trunk), all VLANs on the switch become part of the trunk, allowing automatic configuration of all VLANs on the switch and on the partner device with which the trunk is established.

Before the switch configures an Auto-Trunk, the switch first detects the physical links with the partner device that also supports the Auto-Trunk feature, and then automatically configures the ports that are connected and capable of forming a trunk at both ends.

A trunk carries multiple VLANs and accepts both tagged and untagged packets. Typically, a connection between the switch and a partner device such as a router, access point, or another switch functions as a trunk.

For the switch to form an Auto-Trunk with a partner device, the following are required:

- The Auto-Trunk feature must be supported and globally enabled on the switch and the partner device. (On all M4250 and M4350 series switch models, the Auto-Trunk feature is enabled by default; On all M4300 series switch models, the Auto-Trunk feature is disabled by default.)
- The interconnected ports on both the switch and the partner device must be enabled. (On all M4250, M4300, and M4350 series switch models, all ports are enabled by default.)
- The PVID on the interconnected ports must be set to the management VLAN. (On all M4250, M4300, and M4350 series switch models, the management VLAN is VLAN 1 by default).
- LLDP must be enabled on the interconnected ports on both the switch and the partner device. (On all M4250, M4300, and M4350 series switch models, LLDP is enabled by default on all ports.)
- The interconnected ports on the switch and the partner device must be in the default switch port mode, which is the General mode. If the ports are in the Access mode or already in the Trunk mode, an Auto-Trunk cannot be formed on an Auto-LAG.

For an Auto-Trunk, the PVID is automatically set to the management VLAN. If you want to change the PVID for an Auto-Trunk, change the management VLAN.

The Auto-Trunk feature functions together with the Auto-LAG feature (see Auto-LAG on page 84). After an Auto-LAG is formed, the switch automatically applies trunk mode (that is, an Auto-Trunk) to the LAG at both ends. In other words, after an Auto-LAG is formed, the mode for the ports that participate in an Auto-LAG is automatically changed from the default switch port mode to the trunk port mode, and the Auto-LAG then becomes an Auto-Trunk.

After a port or an Auto-LAG becomes an Auto-Trunk, all VLANs on the switch become part of the trunk, and all VLANs on the switch and the partner device can be configured automatically.

CLI: Enable the Auto-Trunk feature

By default, the Auto-Trunk feature is enabled. If you disable it, you can enable it again.

To use the CLI to enable the Auto-Trunk feature:

```
(Netgear Switch)#config
(Netgear Switch)(Config)#switchport mode auto
(Netgear Switch)(Config)#exit
(Netgear Switch)#
```

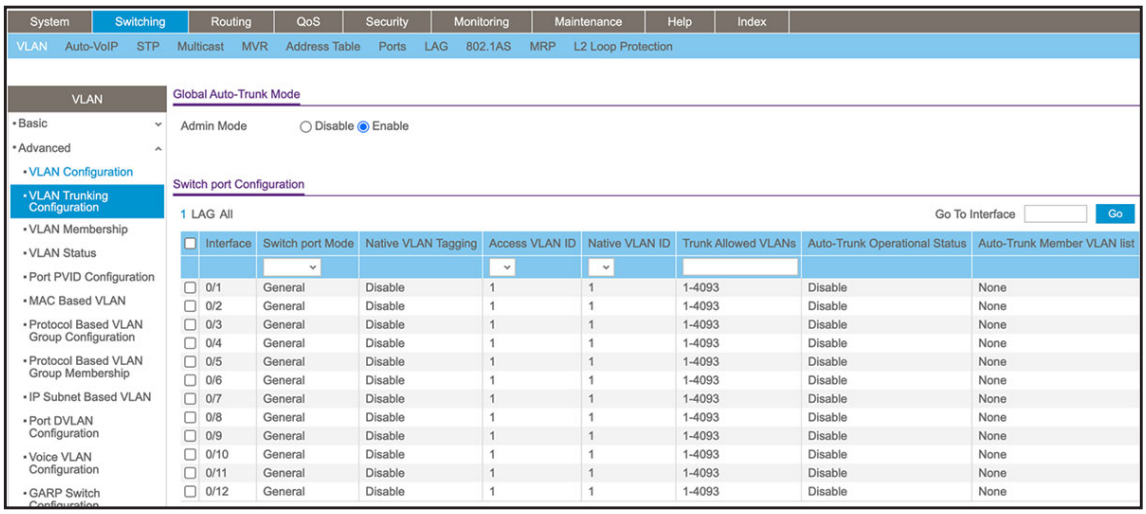
Main UI: Enable the Auto-Trunk feature

By default, the Auto-Trunk feature is enabled. If you disable it, you can enable it again.

To use the main UI to enable the Auto-Trunk feature:

1. Select **Switching > VLAN > Advanced > VLAN Trunking Configuration**.

   A page similar to the following figure displays.



2. Select the Admin Mode **Enable** radio button.

   By default, the Auto-Trunk feature is globally enabled.

3. Click the **Apply** button. Your settings are saved.

Create three VLANs

The following sections describe how to create two VLANs and assign ports to one VLAN.

The example is shown as CLI commands and as a main UI procedure.

CLI: Create three VLANs

To use the CLI to create three VLANs and to assign the VLAN IDs while leaving the names blank:

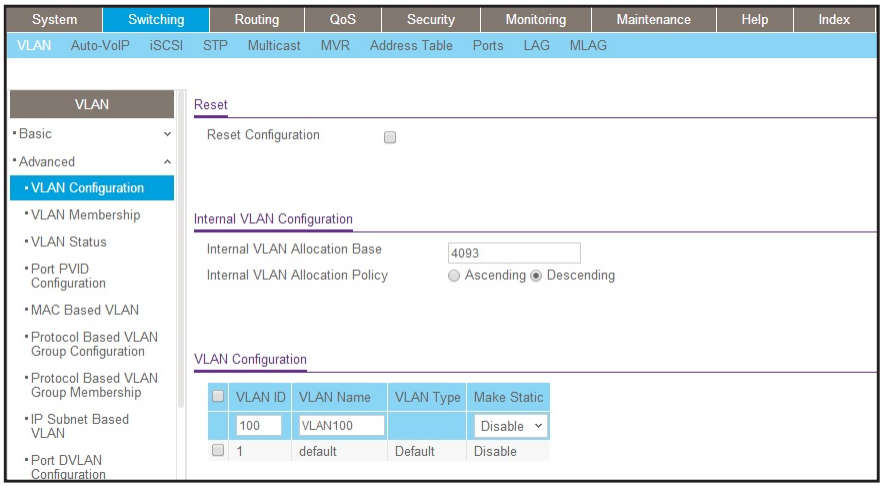
```
(Netgear Switch) #vlan database
(Netgear Switch) (Vlan)#vlan 100
(Netgear Switch) (Vlan)#vlan 101
(Netgear Switch) (Vlan)#vlan 102
(Netgear Switch) (Vlan)#exit
```

Main UI: Create three VLANs

To use the main UI to create three VLANs and to assign the VLAN IDs while leaving the names blank:

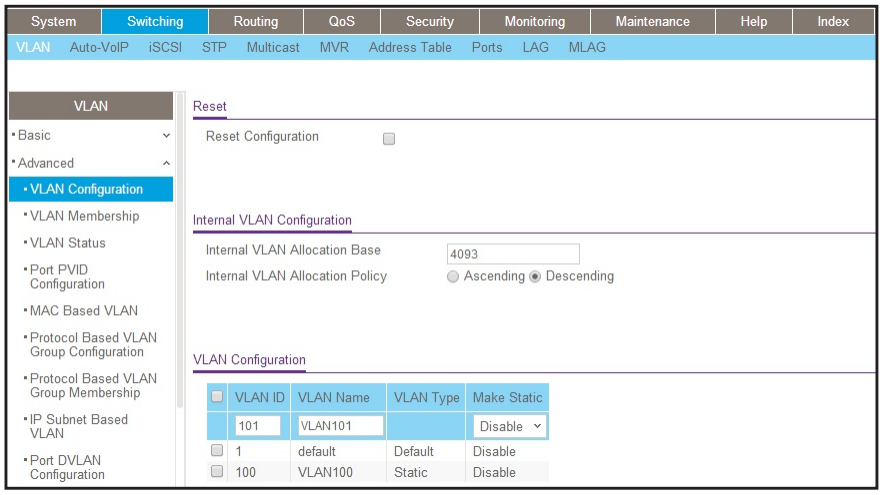
1. Create VLAN 100.
   a. Select **Switching > VLAN > Basic > VLAN Configuration**.

      A page similar to the following figure displays.

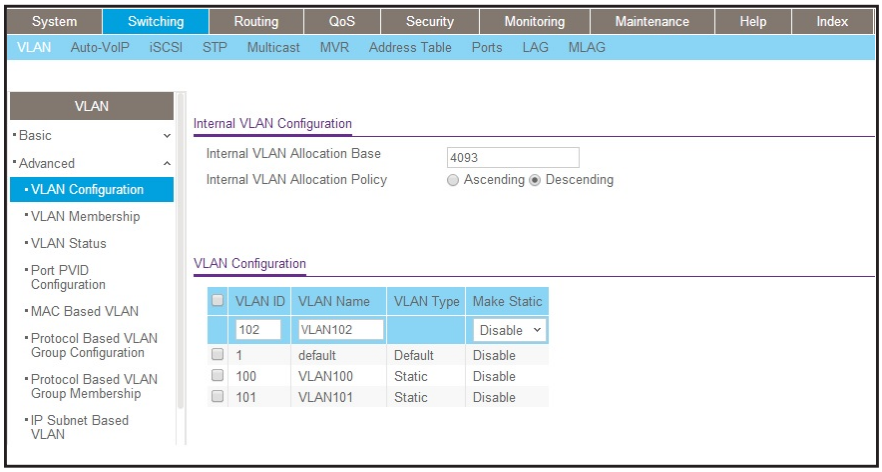


   b. In the **VLAN ID** field, enter **100**.
   c. In the **VLAN Name** field, enter **VLAN100**.
   d. Click the **Add** button. Your settings are saved.

2. Create VLAN 101.
   a. Remain on the same page.



   b. In the **VLAN ID** field, enter **101**.
   c. In the **VLAN Name** field, enter **VLAN101**.
   d. Click the **Add** button. Your settings are saved.
3. Create VLAN 102.
   a. Remain on the same page.



   b. In the **VLAN ID** field, enter **102**.
   c. In the **VLAN Name** field, enter **VLAN102**.
   d. Click the **Add** button. Your settings are saved.

Create two VLANs, assign ports to the VLANs, and assign one VLAN as a default VLAN for a port

The following sections describe how to create VLAN 2 and VLAN 3, how to assign ports to each VLAN, and how to assign VLAN 3 as the default VLAN for a port.

The examples are shown as CLI commands and as main UI procedures.

Create two VLANs

CLI: Create two VLANs

To use the CLI to create VLAN 2 and VLAN 3:

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

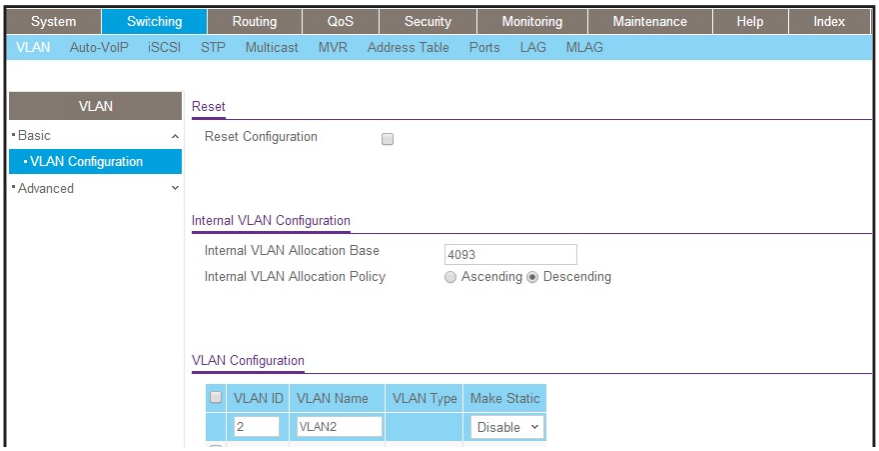
```
(Netgear Switch) #vlan database
(Netgear Switch) (Vlan)#vlan 2
(Netgear Switch) (Vlan)#vlan 3
(Netgear Switch) (Vlan)#exit
```

Main UI: Create two VLANs

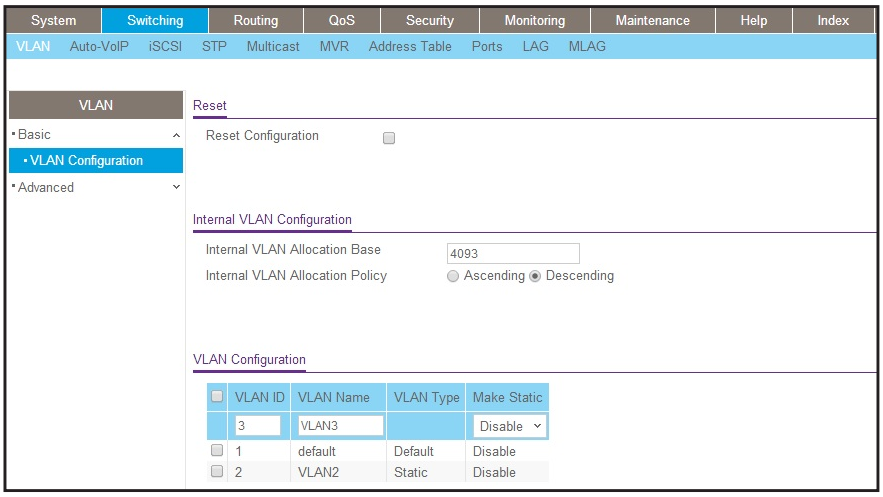
To use the main UI to create VLAN 2 and VLAN 3:

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

      A page similar to the following figure displays.



   b. In the **VLAN ID** field, enter **2**.
   c. In the **VLAN Name** field, enter **VLAN2**.
   d. Click the **Add** button. Your settings are saved.
2. Create VLAN 3.
   a. Remain on the same page.



   b. In the **VLAN ID** field, enter **3**.
   c. In the **VLAN Name** field, enter **VLAN3**.
   d. Click the **Add** button. Your settings are saved.

Assign ports to VLAN 2

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

CLI: Assign ports to VLAN 2

To use the CLI to assign ports to VLAN 2:

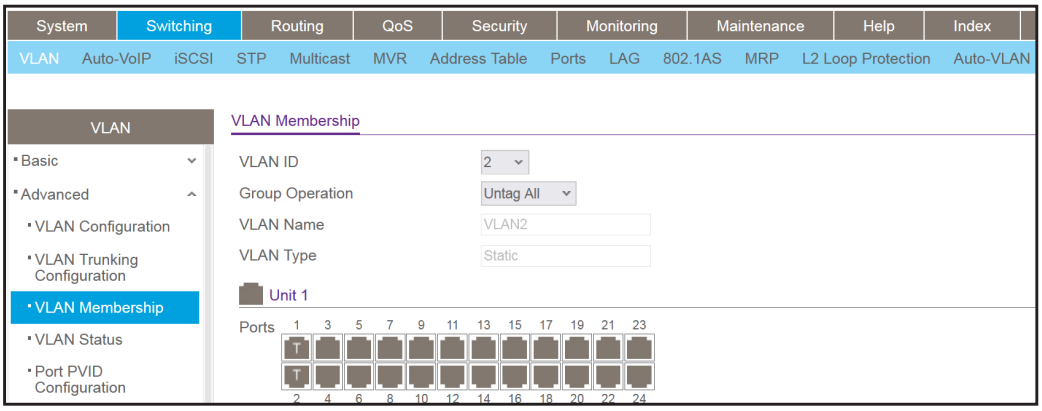
```
(Netgear Switch) #config
(Netgear Switch) (Config)#interface range 1/0/1-1/0/2
(Netgear Switch) (conf-if-range-1/0/1-1/0/2)#vlan participation include 2
(Netgear Switch) (conf-if-range-1/0/1-1/0/2)#vlan acceptframe vlanonly
(Netgear Switch) (conf-if-range-1/0/1-1/0/2)#vlan pvid 2
(Netgear Switch)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

Main UI: Assign ports to VLAN 2

To use the main UI to assign ports to VLAN 2:

1. Assign ports to VLAN 2.
   a. Select **Switching > VLAN > Advanced > VLAN Membership**.

      A page similar to the following figure displays.

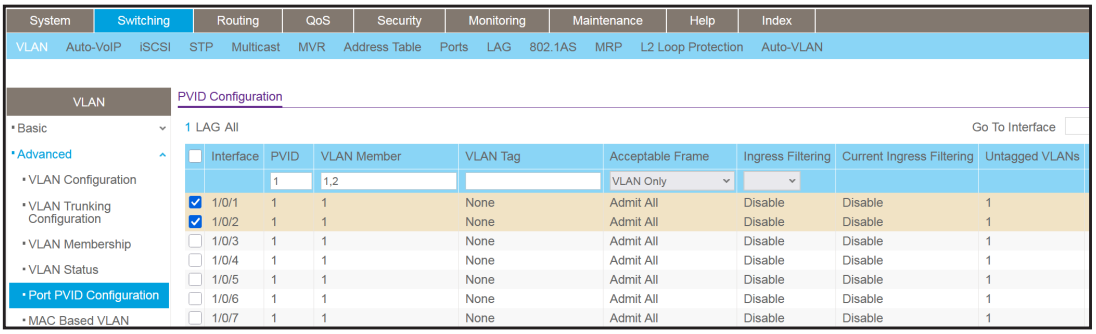


   b. In the **VLAN ID** menu, select **2**.
   c. Click the gray boxes under ports **1** and **2** until T displays, which specifies that the egress packets are tagged for the ports.

      If your switch is a member of a stack, be sure that you select the ports in the correct unit.
   d. Click the **Apply** button. Your settings are saved.

2. Specify that only tagged frames are accepted on ports 1/0/1 and 1/0/2.
   a. Select **Switching > VLAN > Advanced > Port PVID Configuration**.

      A page similar to the following figure displays.



   b. Select the Interface **1/0/1** check box and the Interface **1/0/2** check box.
   c. In the **PVID** field, enter **2**.
   d. In the **Acceptable Frame** menu, select **VLAN Only**.
   e. Click the **Apply** button. Your settings are saved.

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

To use the CLI to assign ports to VLAN 3:

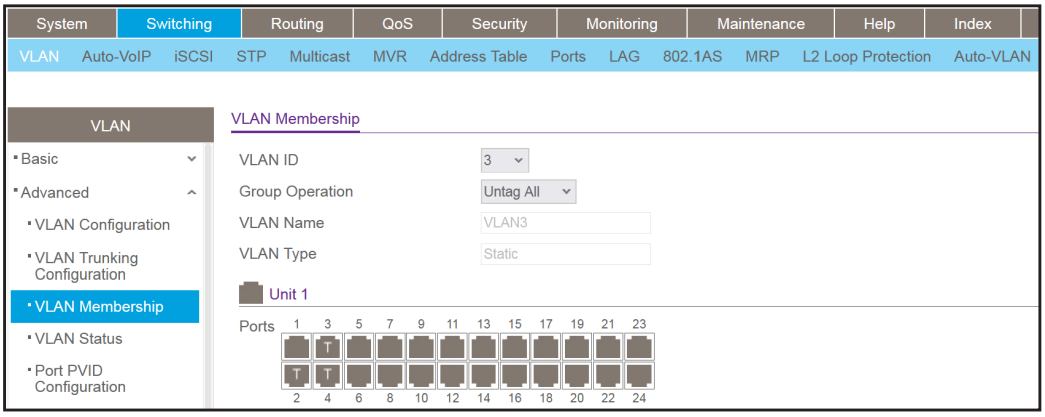
```
(Netgear Switch) (Config)#interface range 1/0/2-1/0/4
(Netgear Switch) (conf-if-range-1/0/2-1/0/4)#vlan participation include 3
(Netgear Switch) (conf-if-range-1/0/2-1/0/4)#exit
(Netgear Switch) (Config)#interface 1/0/4
(Netgear Switch) (Interface 1/0/4)#vlan acceptframe all
(Netgear Switch) (Interface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

Main UI: Assign ports to VLAN 3

To use the main UI to assign ports to VLAN 3:

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

      A page similar to the following figure displays.

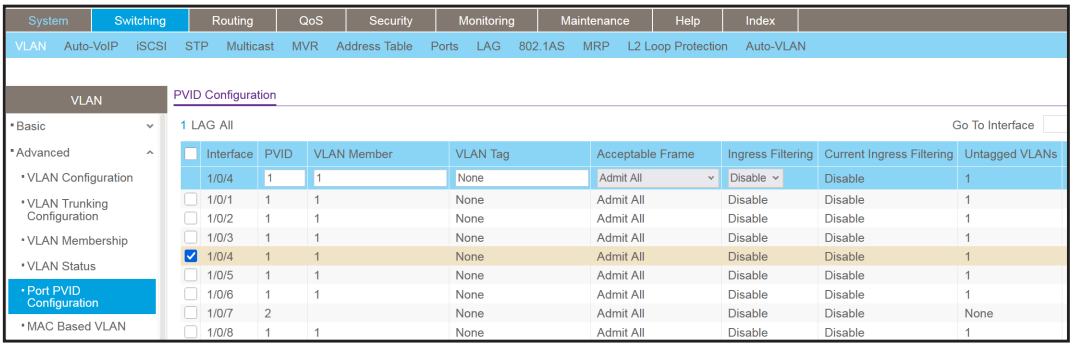


   b. In the **VLAN ID** menu, select **3**.
   c. Click the gray boxes under ports **2**, **3**, and **4** until T displays, which specifies that the egress packets are tagged for the ports.

      If your switch is a member of a stack, be sure that you select the ports in the correct unit.

   d. Click the **Apply** button. Your settings are saved.
2. Specify that untagged frames are accepted on port 1/0/4.
   a. Select **Switching > VLAN > Advanced > Port PVID Configuration**.

A page similar to the following figure displays.



b. Select the Interface **1/0/4** check box.

c. In the **Acceptable Frame** menu, select **Admit All**.

d. Click the **Apply** button. Your settings are saved.

Assign a default VLAN to a port

CLI: Assign VLAN 3 as the default VLAN for port 1/0/2

To use the CLI to assign VLAN 3 as the default VLAN for port 1/0/2:

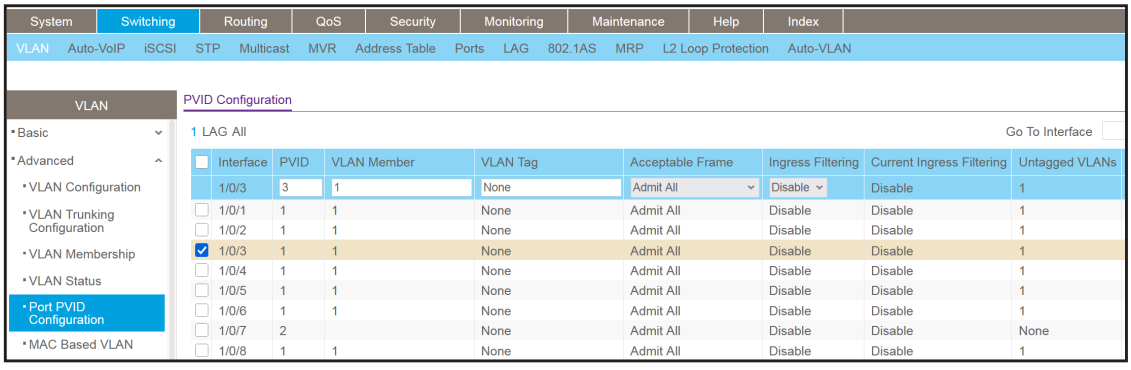
```
(Netgear Switch) #config
(Netgear Switch) (Config)#interface 1/0/2
(Netgear Switch) (Interface 1/0/2)#vlan pvid 3
(Netgear Switch) (Interface 1/0/2)#exit
(Netgear Switch) (Config)#exit
```

Main UI: Assign VLAN 3 as the default VLAN for port 1/0/2

To use the main UI to assign VLAN 3 as the default VLAN for port 1/0/2:

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

   A page similar to the following figure displays.



2. Select the Interface **1/0/2** check box.

3. In the **PVID** field, enter **3**.
4. Click the **Apply** button. Your settings are saved.

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 is 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 switch.

CLI: Create a MAC-based VLAN

To use the CLI to 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.

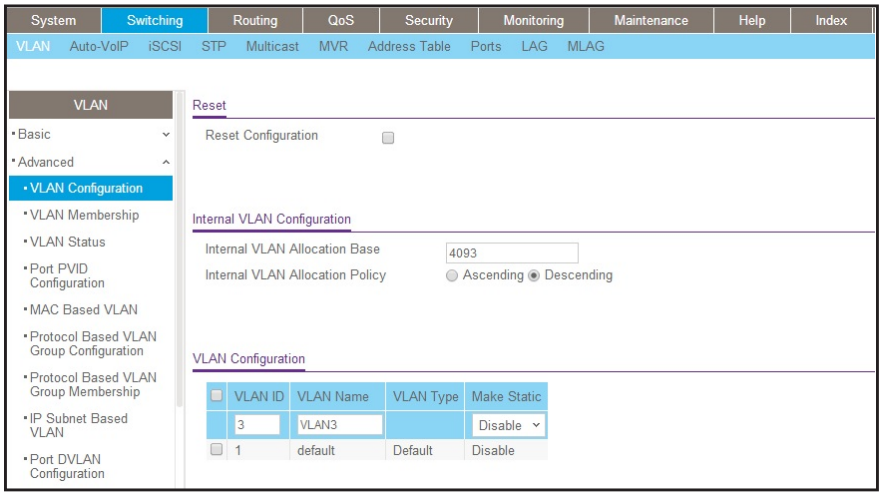
```
(Netgear Switch)#config
(Netgear Switch)(Config)#interface range 1/0/1-1/0/28
(Netgear Switch)(conf-if-range-1/0/1-1/0/28)#vlan participation include 3
(Netgear Switch)(conf-if-range-1/0/1-1/0/28)#exit
(Netgear Switch)(Config)#exit
```

Main UI: Assign a MAC-based VLAN

To use the main UI to create a MAC-based VLAN:

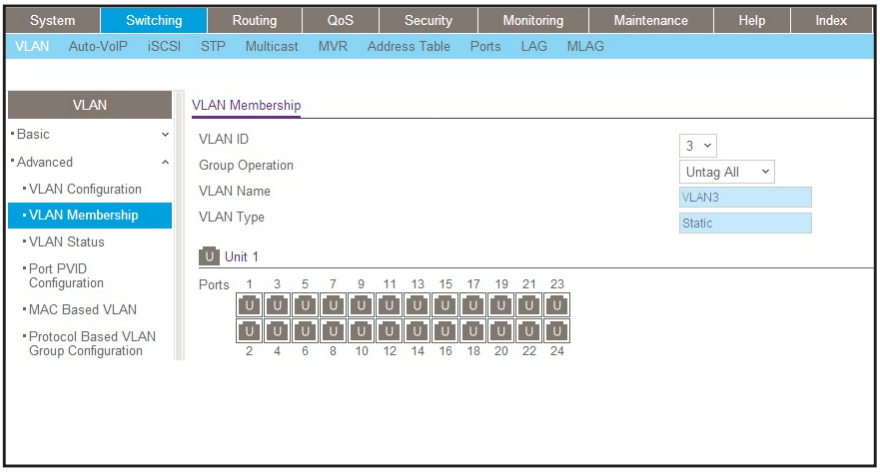
1. Create VLAN3.
   a. Select **Switching > VLAN > Basic > VLAN Configuration**.

      A page similar to the following figure displays.



   b. In the **VLAN ID** field, enter **3**.
   c. In the **VLAN Name** field, enter **VLAN3**.
   d. Click the **Add** button. Your settings are saved.
2. Assign ports to VLAN3.
   a. Select **Switching > VLAN > Advanced > VLAN Membership**.

A page similar to the following figure displays.



b. In the **VLAN ID** menu, select **3**.

c. Click the gray **Ports** box, or for an M4350 series switch that is a member of a stack, the gray **Unit** box, until **U** displays.

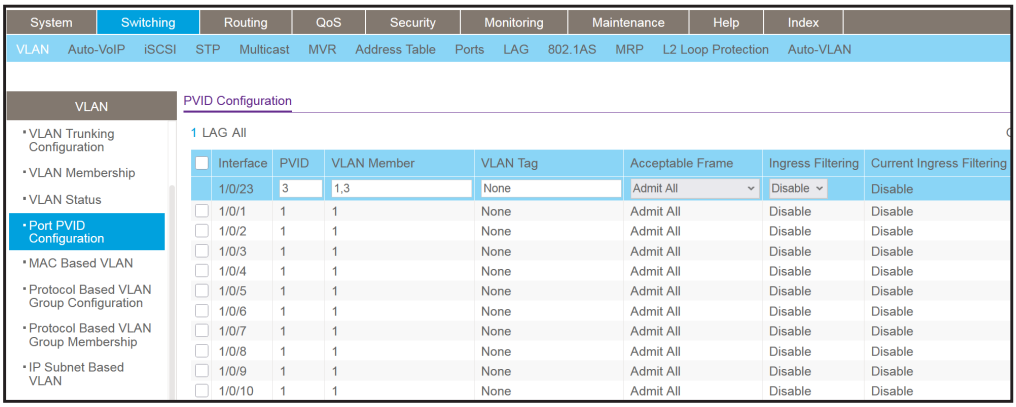
If your switch is a member of a stack, be sure that you select the ports in the correct unit.

d. Click the **Apply** button. Your settings are saved.

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

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

A page similar to the following figure displays.



b. Select the Interface **1/0/23** check box.

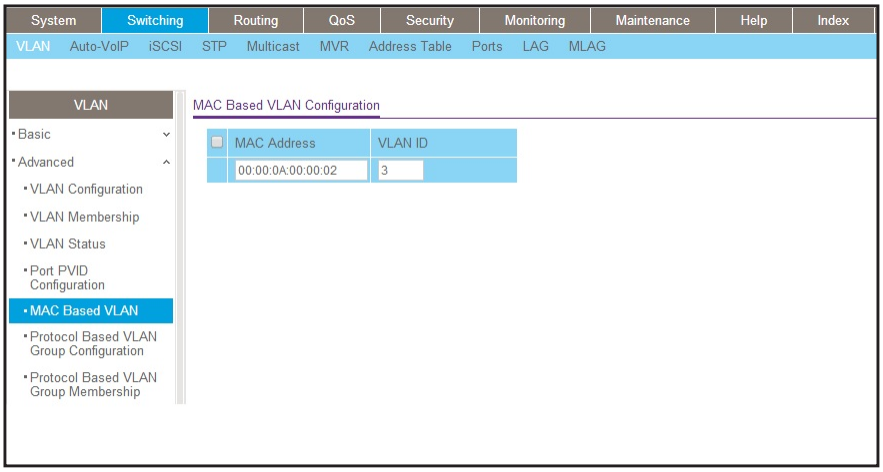
c. In the **PVID** field, enter **3**.

d. Click the **Apply** button. Your settings are saved.

4. Map the specific MAC to VLAN3.

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

A page similar to the following figure displays.



b. In the **MAC Address** field, enter **00:00:0A:00:00:02**.

c. In the **VLAN ID** field, enter **3**.

d. Click the **Add** button. Your settings are saved.

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

To use the CLI to create a protocol-based VLAN:

1. Create a VLAN protocol group1 with the name “vlan_ipx” that is based on Internetwork Packet Exchange (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 2 “vlan_ip” that is based on the IP and ARP protocols.

```
(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 an interface.

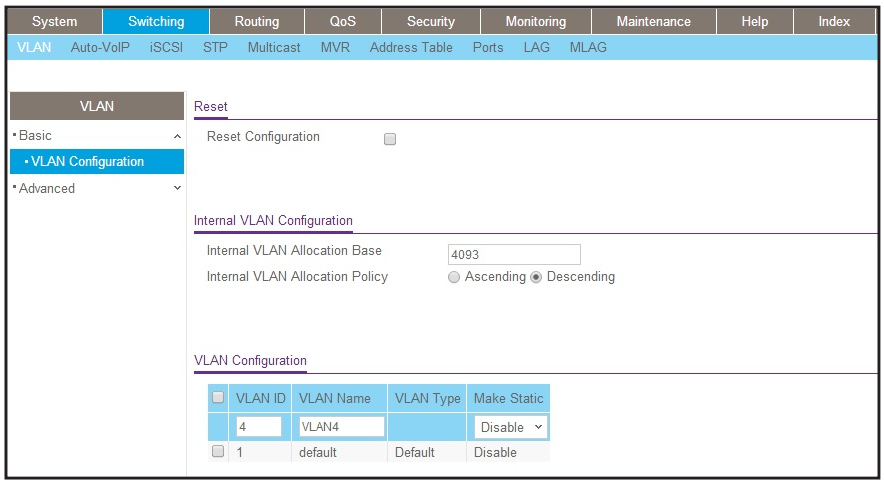
```
(Netgear Switch)(Vlan)#exit
(Netgear Switch)#config
(Netgear Switch)(Config)#interface 1/0/11
(Netgear Switch)(Interface 1/0/11)#protocol vlan group 1
(Netgear Switch)(Interface 1/0/11)#protocol vlan group 2
(Netgear Switch)(Interface 1/0/11)#exit
```

Main UI: Create a protocol-based VLAN

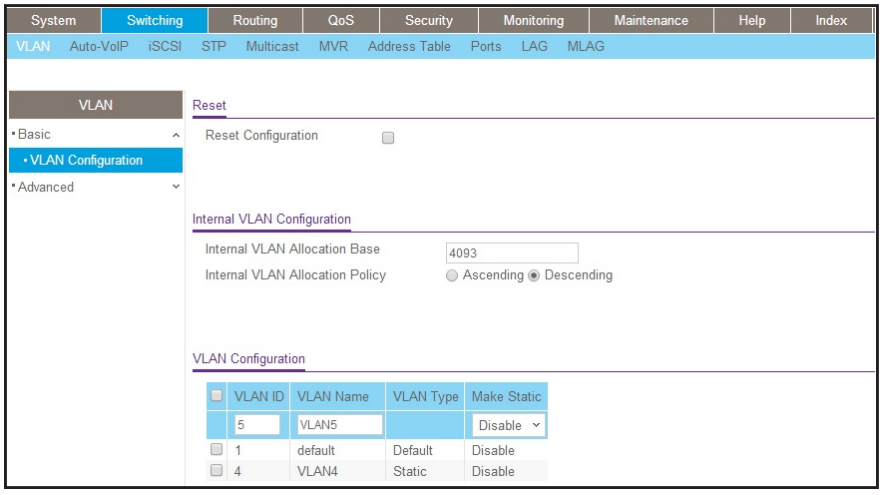
To use the main UI to create a protocol-based VLAN:

1. Create VLAN 4:
   a. Select **Switching > VLAN > Basic > VLAN Configuration**.

      A page similar to the following figure displays.



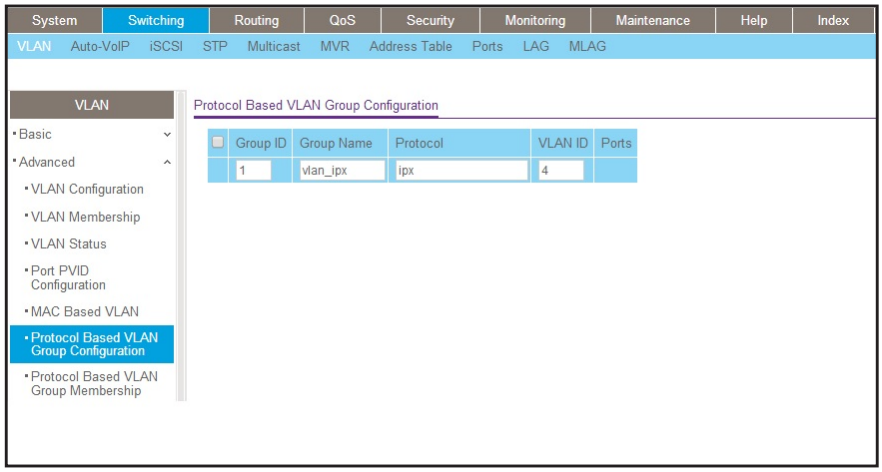
   b. In the **VLAN ID** field, enter **4**.
   c. In the **VLAN Name** field, enter **VLAN4**.
   d. Click the **Add** button. Your settings are saved.
2. Create VLAN 5:
   a. Remain on the same page.



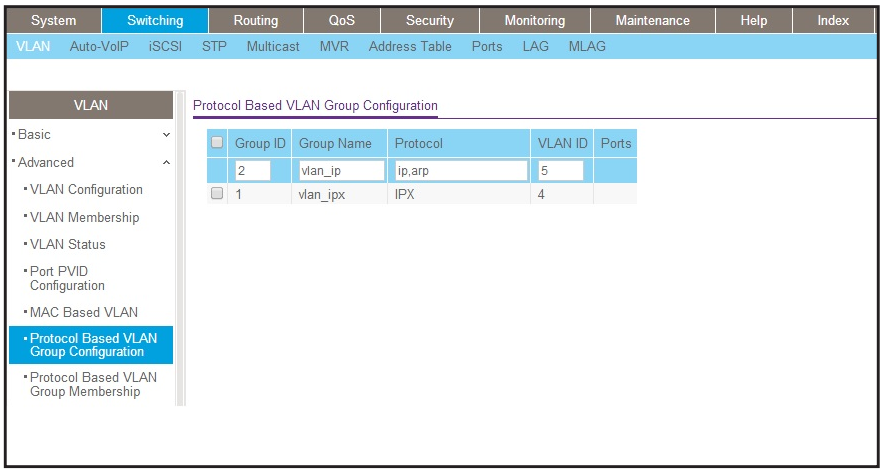
   b. In the **VLAN ID** field, enter **5**.
   c. In the **VLAN Name** field, enter **VLAN5**.
   d. Click the **Add** button. Your settings are saved.

3. Create the protocol-based VLAN group 1 with the name “vlan_ipx” that is based on Internetwork Packet Exchange (IPX) protocol.
   a. Select **Switching > VLAN > Advanced > Protocol Based VLAN Group Configuration**.

      A page similar to the following figure displays.



   b. In the **Group ID** field, enter **1**.
   c. In the **Group Name** field, enter **vlan_ipx**.
   d. In the **Protocol** menu, enter **IPX**.
   e. In the **VLAN ID** field, enter **4.**
   f. Click the **Add** button. Your settings are saved.
4. Create the protocol-based VLAN group vlan_ip.
   a. Remain on the same page.



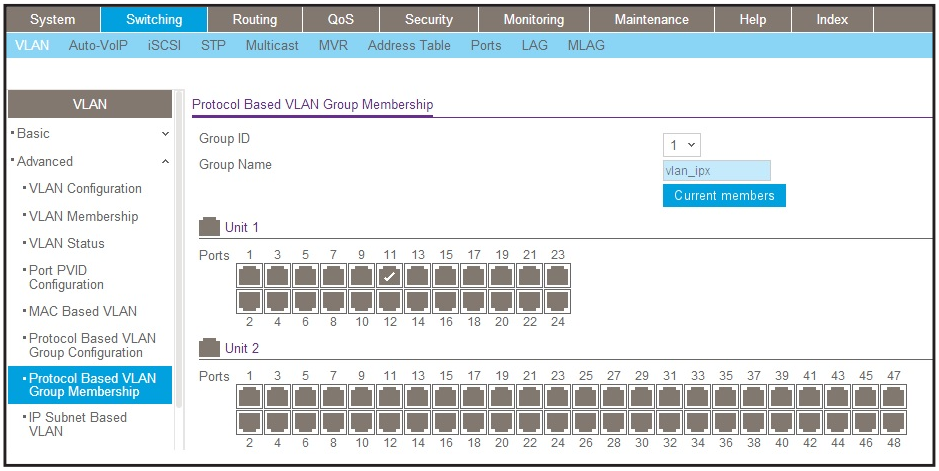
   b. In the **Group ID** field, enter **2**.
   c. In the **Group Name** field, enter **vlan_ip**.
   d. In the **Protocol** menu, enter **IP,ARP**.
   e. In the **VLAN ID** field, enter **5**.

f. Click the **Add** button. Your settings are saved.

5. Add port 11 to the group vlan_ipx.

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

A page similar to the following figure displays.



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

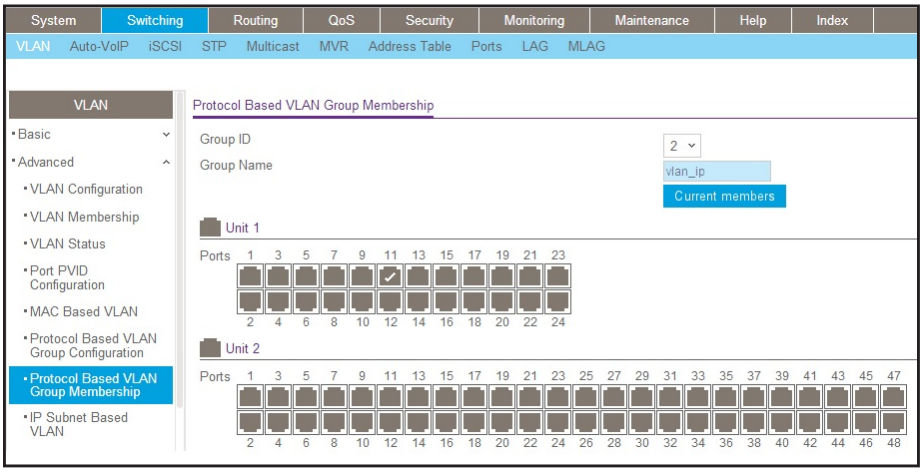
c. Click the gray box under port **11**. A check mark displays in the box.

If your switch is a member of a stack, be sure that you select the port in the correct unit.

d. Click the **Apply** button.

6. Add port 11 to the group vlan_ip.

a. Remain on the same page.



b. In the **Group ID** menu, select **2**.

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

If your switch is a member of a stack, be sure that you select the port in the correct unit.

d. Click the **Apply** button. Your settings are saved.

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.

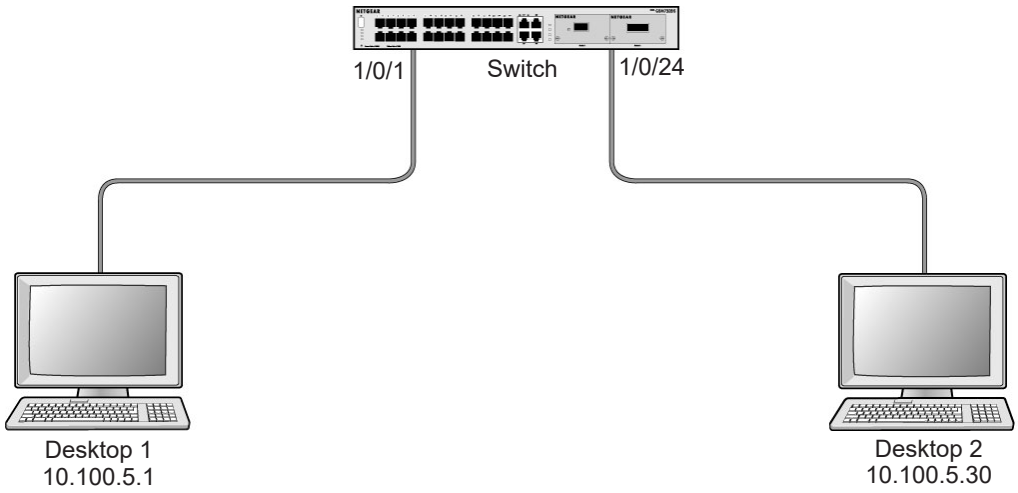


Figure 2. IP subnet–based VLAN

CLI: Create an IP subnet–based VLAN

To use the CLI to create an IP subnet-based VLAN:

1. Create an IP subnet–based VLAN 2000.

```
(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
```

2. Assign all the ports to 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)#
```

3. (Optionally) Display the MAC address table for VLAN 2000.

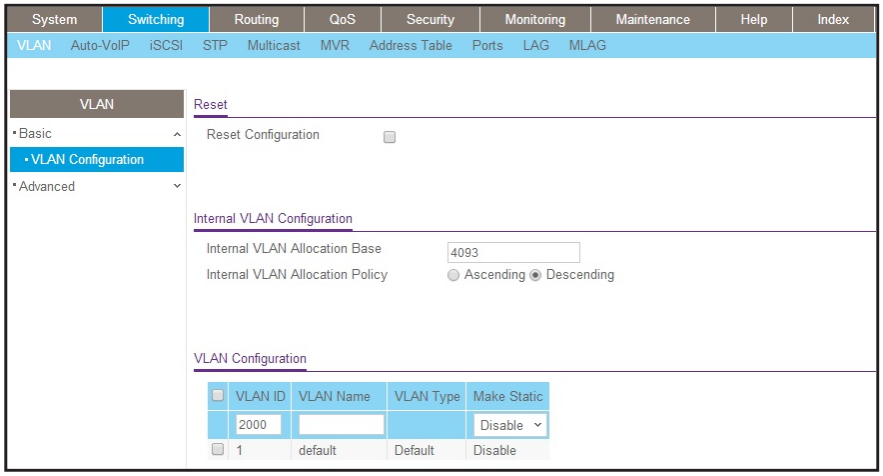
```
(Netgear Switch) #show mac-addr-table vlan 2000
MAC Address        Interface  Status
-----------------  ---------  ------------
00:00:24:58:F5:56  1/0/1      Learned
00:00:24:59:00:62  1/0/24     Learned
```

Main UI: Create an IP subnet-based VLAN

To use the main UI to create an IP subnet-based VLAN:

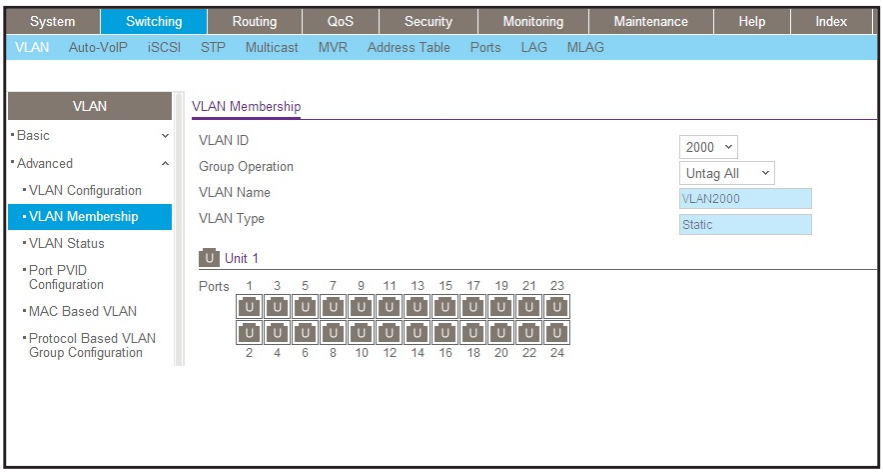
1. Create VLAN 2000.
   a. Select **Switching > VLAN > Basic > VLAN Configuration**.

      A page similar to the following figure displays.



   b. In the **VLAN ID** field, enter **2000**.
   c. Click the **Add** button. Your settings are saved.
2. Assign all the ports to VLAN 2000.
   a. Select **Switching > VLAN > Advanced > VLAN Membership**.

      A page similar to the following figure displays.



   b. In the **VLAN ID** menu, select **2000**.
   c. Click the gray **Ports** box, or for an M4350 series switch that is a member of a stack, the gray **Unit** box, until **U** displays.

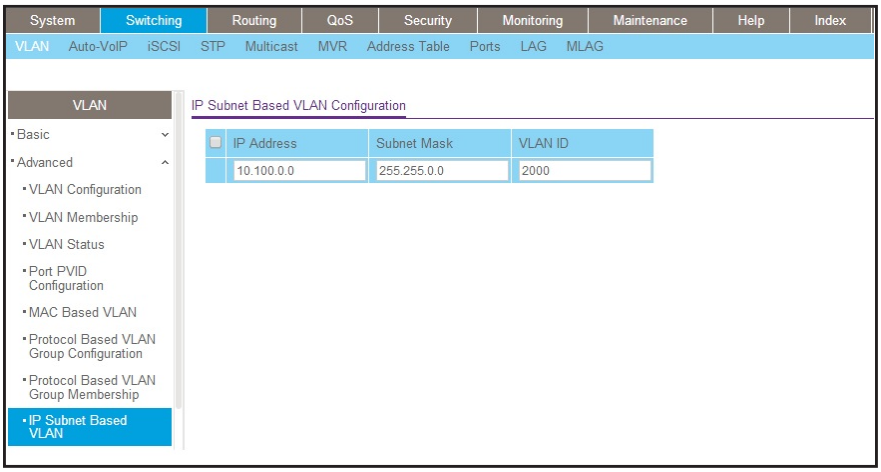
If your switch is a member of a stack, be sure that you select the ports in the correct unit.

d. Click the **Apply** button. Your settings are saved.

3. Associate the IP subnet with VLAN 2000.

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

A page similar to the following figure displays.



b. In the **IP Address** field, enter **10.100.0.0**.

c. In the **Subnet Mask** field, enter **255.255.0.0**.

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

e. Click the **Add** button. Your settings are saved.

Voice VLANs

The voice VLAN feature enables switch ports to carry voice traffic with a specific priority to enable separation of voice and data traffic coming onto port. A 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.

You can configure the switch to support a voice VLAN on a port connecting to a VoIP phone. When a VLAN is associated with the voice VLAN port, the VLAN ID information is passed on to the VoIP phone using LLDP-MED. The voice data coming from the VoIP phone is tagged with the exchanged VLAN ID, allowing regular data arriving on the switch to be assigned to the default PVID of the port, and the voice traffic to be received on a predefined VLAN. The two types of traffic are therefore segregated so that better service can be provided to the voice traffic.

When a dot1p priority is associated with the voice VLAN port instead of VLAN ID, the priority information is passed on to the VoIP phone using LLDP-MED. The voice data coming from

the VoIP phone is tagged with VLAN 0 and with the exchanged priority. Regular data arriving at the switch is assigned the default priority of the port (default 0), and the voice traffic is assigned a higher priority. This segregates the types of traffic and provides better service to the voice traffic.

You can configure the switch to override the data traffic CoS. This feature enables overriding the 802.1P priority of the data traffic packets arriving at a port that is enabled for a voice VLAN. In that way, a rogue client that is also connected to the voice VLAN port does not deteriorate the voice traffic.

The table below describes how the PVID and tagging are handled by a voice VLAN in the four modes.

Table 2. PVID and Tagging

Configure Voice VLAN = 4088 Data VLAN = 4000	Ingress VLAN Tag	Egress VLAN Tag	PVID	Comments
Disable: Default value	No	No	1	No voice VLAN,
None: Allow the IP phone to use its own configuration to send untagged voice traffic	No	No	1	No special priority for voice, but you must configure a data VLAN if it is not using default VLAN.
VLAN ID: Enter the Voice VLAN ID in the Value field.	Yes (VLAN= 4088, PRI=1)	Yes (VLAN= 4088, PRI=1)	4000	• The voice VLAN automatically becomes part of a tagged set for the port. VoIP traffic is received with this VLAN tag. • The voice VLAN sets egress tagging for voice VLAN (4088) automatically. • No priority is automatically assigned by the voice VLAN. If you want a higher priority for voice traffic, you must manually configure it. This priority (dot1p) is conveyed from the voice device as part of the VLAN tag in the VoIP traffic. You do not need to configure CoS on the port.
dot1p: Configure Voice VLAN 802.1p priority tagging for voice traffic. When this is selected, enter the dot1p value in the Value field.	Yes (VLAN=0, PRI=5)	Yes (VLAN=0, PRI=5)	4000	• You must configure a dot1p priority value (for example, 5). This value is communicated to the VoIP device over LLDP. • By default, the priority advertised is 0.
Untagged: Configure the phone to send untagged voice traffic	No	No	4088	• You do not need to set a PVID for voice but you might need to configure a data VLAN (VLAN 4000 in this example). VLAN ID 0 is communicated to the VoIP device.

Note: For the Voice VLAN feature, you can enable CoS override for a maximum of eight ports.

Voice VLAN interoperation with Auto-VoIP

This section describes a situation in which both the voice VLAN and Auto-VoIP are enabled on a port.

A voice VLAN configures the ingress port as tagged (in VLAN-ID mode) only if the switch can exchange LLDP-MED packets with the VoIP device. If the VoIP device is not LLDP-capable or LLDP is disabled on the switch port, the voice VLAN does not add the VLAN as tagged or untagged on the ingress port. That is, the voice VLAN does not really work if the LLDP-MED exchange does not occur.

Auto-VoIP requires a VLAN (the Auto-VoIP VLAN) to be configured on the switch. If you enable Auto-VoIP on a port, the switch automatically adds that port as an untagged port of the Auto-VoIP VLAN. This occurs because the switch expects to receive the voice packets as untagged packets. You also must configure the egress port as a member of the VLAN (untagged is fine). The switch forwards all untagged voice traffic from the VoIP device through the egress port as tagged packets with the Auto-VoIP VLAN (even if the Auto-VoIP VLAN is untagged on the port) and with the VLAN priority set to 6 (on the M4300 and M4350 series switches) or 7 (on the M4250 series switches). This allows the next hop to prioritize the traffic.

The following figure shows egress packets.

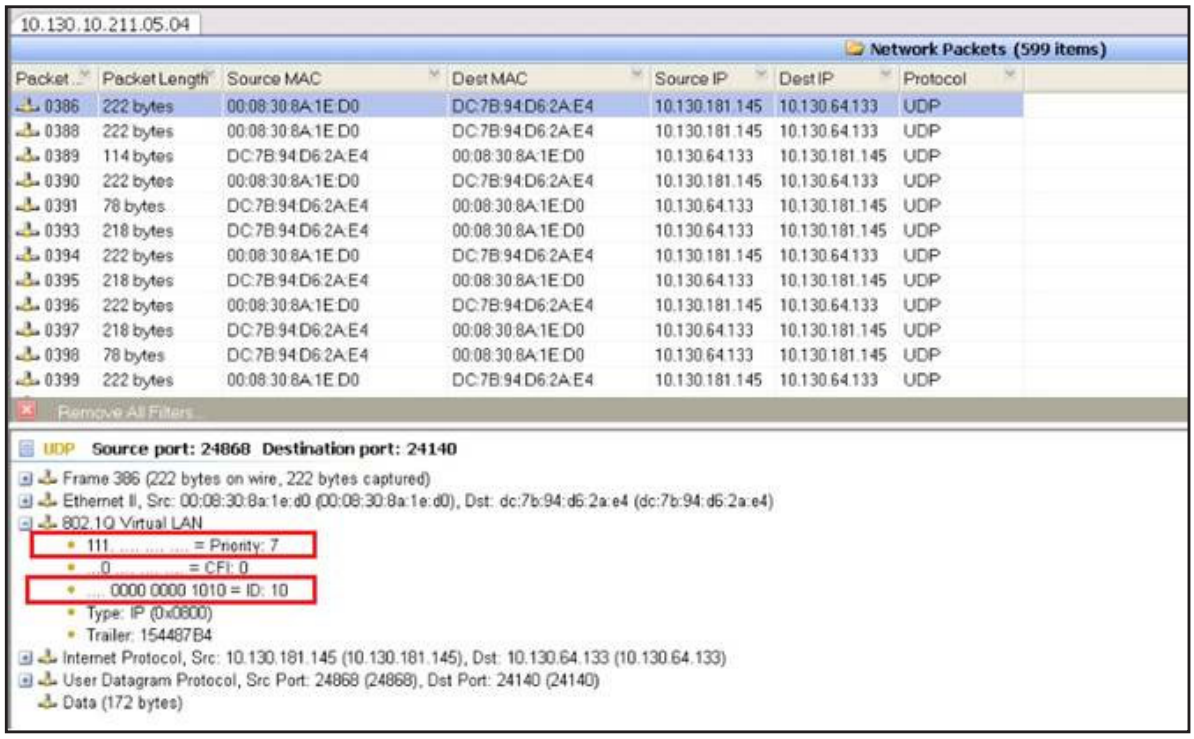


Figure 3. Egress packets

These packets were sent untagged from the VoIP device to the Auto-VoIP–enabled port. (The voice VLAN is also enabled on that port, but LLDP is disabled). Because the LLDP exchange did not occur, the voice VLAN is passive and the Auto-VoIP is active.

However, if you configure a port for both the voice VLAN and Auto-VoIP with the same VLAN ID for both VLANs, and LLDP-MED functions between the switch and VoIP device, the voice VLAN receives priority over Auto-VoIP. In that situation, the VoIP device sends tagged VoIP packets to the switch.

If you need a data VLAN, you must configure it separately because the voice VLAN and Auto-VoIP do not automatically create data a VLAN.

If you use a separate data VLAN, the voice VLAN supports segregation and separation of voice traffic from data traffic. The priority that is set in the VLAN header of the tagged VoIP traffic depends on the VoIP device.

The following figure shows the ingress port (voice VLAN 10) with traffic received from the VoIP device.

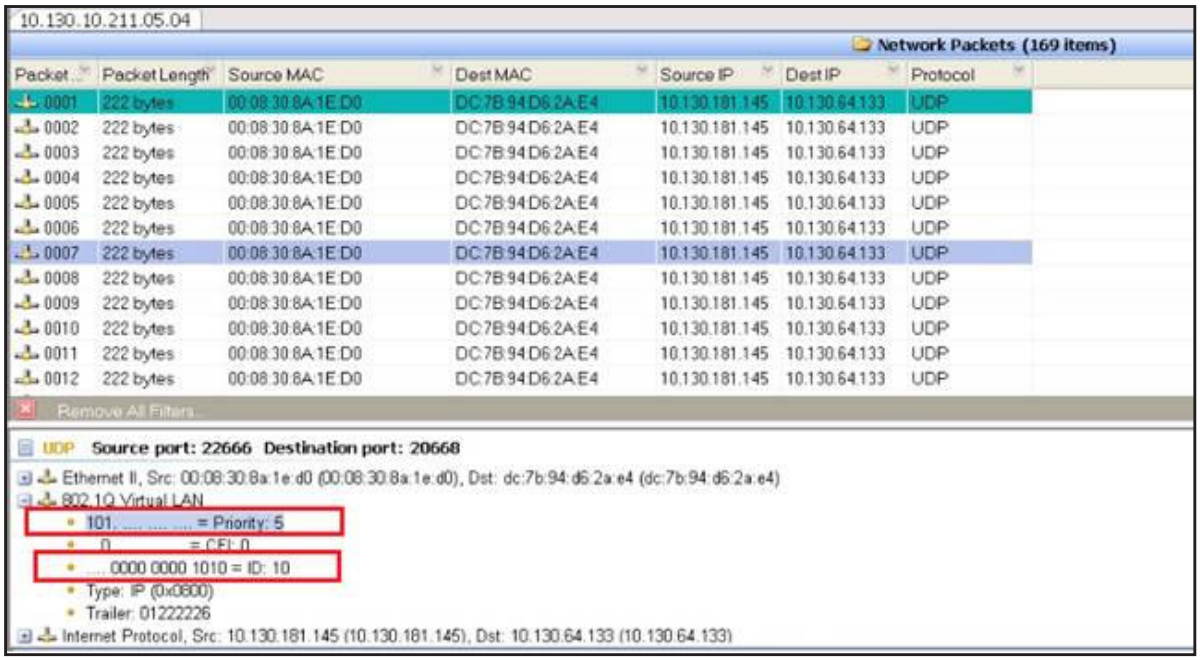


Figure 4. Ingress packets

You can use the CoS override aspect of the voice VLAN (that is, in the CLI you can use the **vlan priority** command) to lower the dot1p priority of the ingress port so that untagged data traffic is assigned a lower CoS queue.

You must configure the egress port with the voice VLAN as its member (untagged is fine) so that the traffic is forwarded with the voice VLAN tag and with the same priority as the incoming packet from VoIP device (5, in the previous figure). This enables the next hop to prioritize the VoIP traffic.

Note: For more information about voice VLANs, see Configure Auto VoIP on page 275.

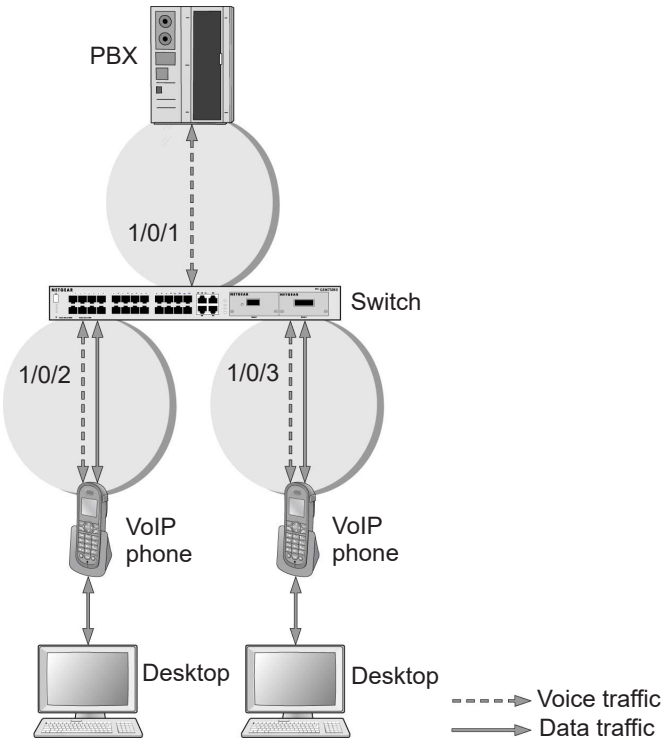


Figure 5. Voice VLAN

The example in the following sections shows how to configure Voice VLAN and prioritize the voice traffic. In the example, the Voice VLAN mode is in VLAN ID 10.

CLI: Configure a Voice VLAN and prioritize voice traffic

To use the CLI to configure a voice VLAN and a prioritize voice traffic:

1. Create VLAN 10.

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

2. Include 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 for 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
```

Note: Steps 5 through 9 are optional. These steps assign the packets with the VLAN ID 10 to a high priority queue.

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 the policy to interfaces 1/0/1 and 1/0/2.

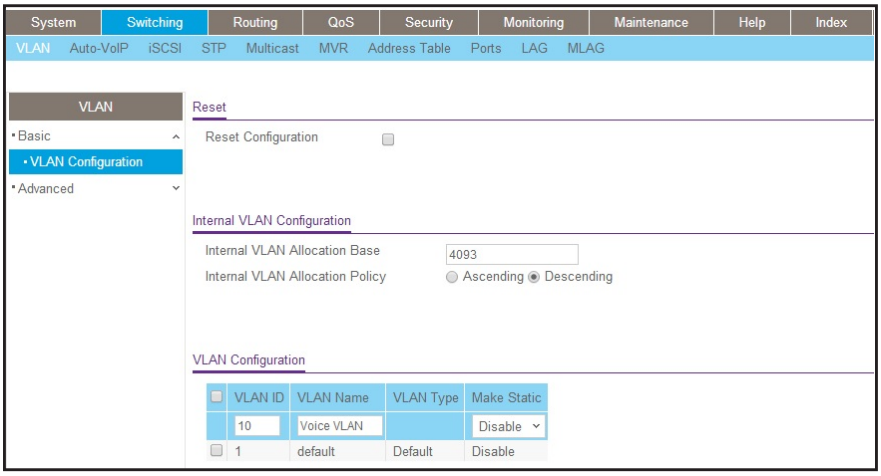
```
(Netgear Switch) (Config)#interface range 1/0/1-1/0/2
(Netgear Switch) (conf-if-range-1/0/1-1/0/2)# service-policy in PolicyVoiceVLAN
```

Main UI: Configure Voice VLAN and prioritize voice traffic

To use the main UI to configure a voice VLAN and a prioritize voice traffic:

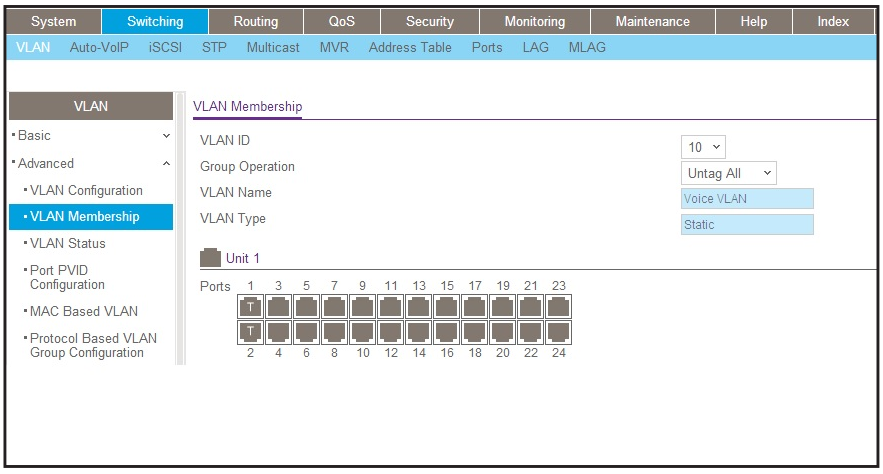
1. Create VLAN 10.
   a. Select **Switching > VLAN > Basic > VLAN Configuration**.

      A page similar to the following figure displays.



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

      A page similar to the following figure displays.



   b. In the **VLAN ID** menu, select **10**.
   c. Click the gray boxes under port **1** and port **2** until a T displays in the box, specifying that the ports are tagged.

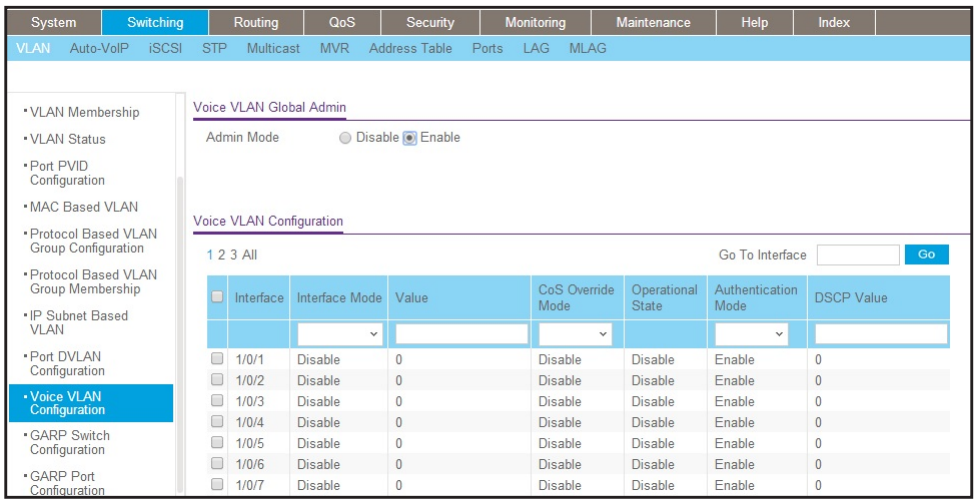
If your switch is a member of a stack, be sure that you select the ports in the correct unit.

d. Click the **Apply** button. Your settings are saved.

3. Configure Voice VLAN globally.

a. Select **Switching > VLAN > Advanced > Voice VLAN Configuration**.

A page similar to the following figure displays.

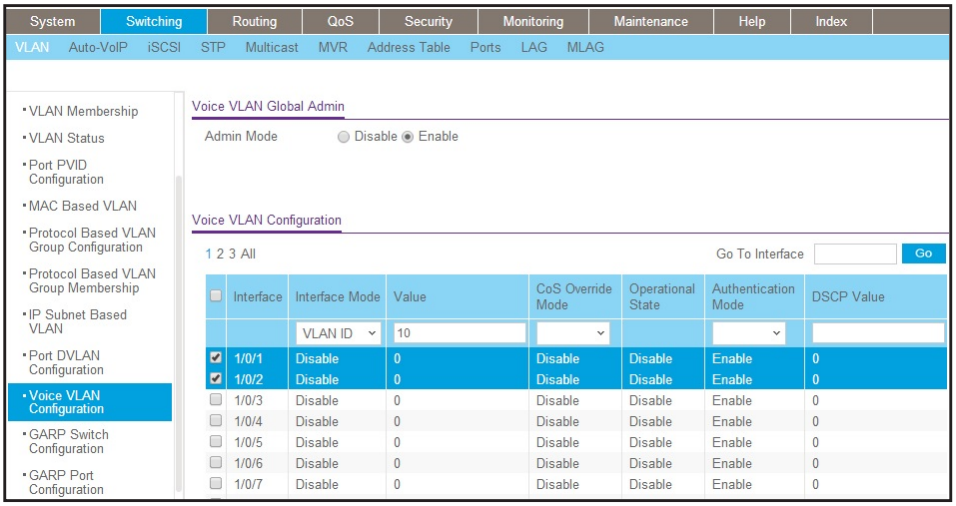


b. Select the Admin Mode **Enable** radio button.

c. Click the **Apply** button. Your settings are saved.

4. Configure Voice VLAN mode for interfaces 1/0/1 and 1/0/2.

a. Remain on the same page.



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

c. In the **Interface Mode** menu, select **VLAN ID**.

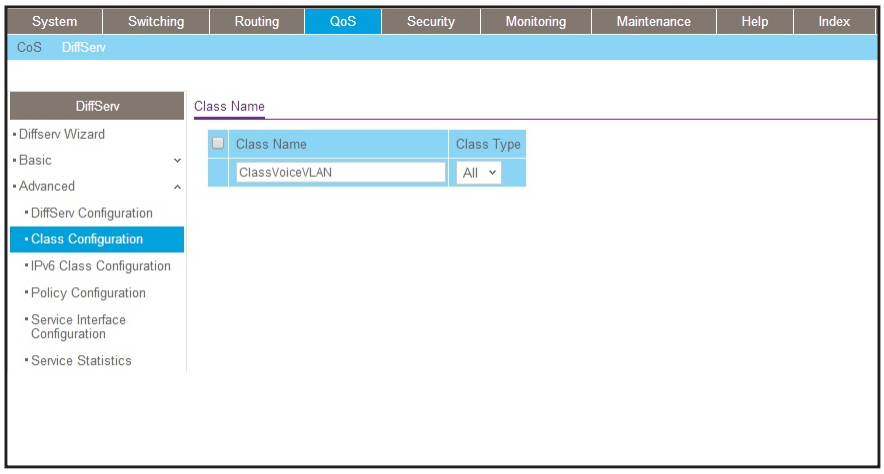
d. In the **Value** field, enter **10**.

e. Click the **Apply** button. Your settings are saved.

Note: The following steps are optional. These steps assign the packets with VLAN ID 10 to a high priority queue.

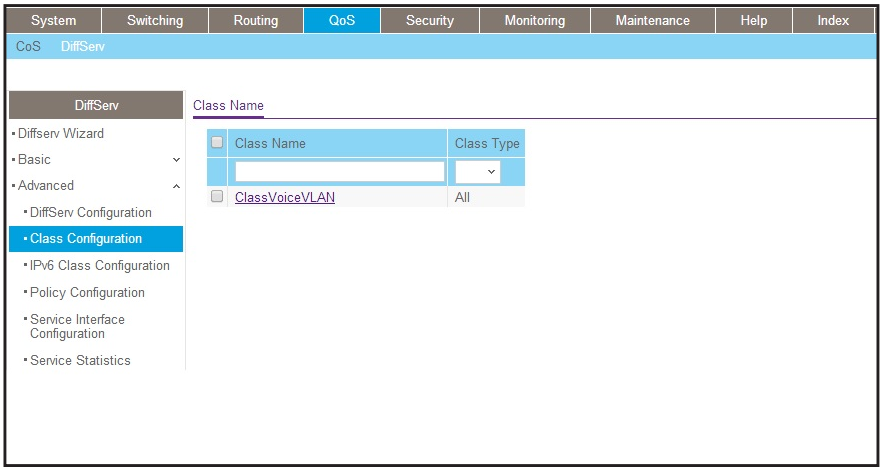
5. Create the DiffServ class ClassVoiceVLAN.
   a. Select **QoS > Advanced > DiffServ > Class Configuration**.

      A page similar to the following figure displays.



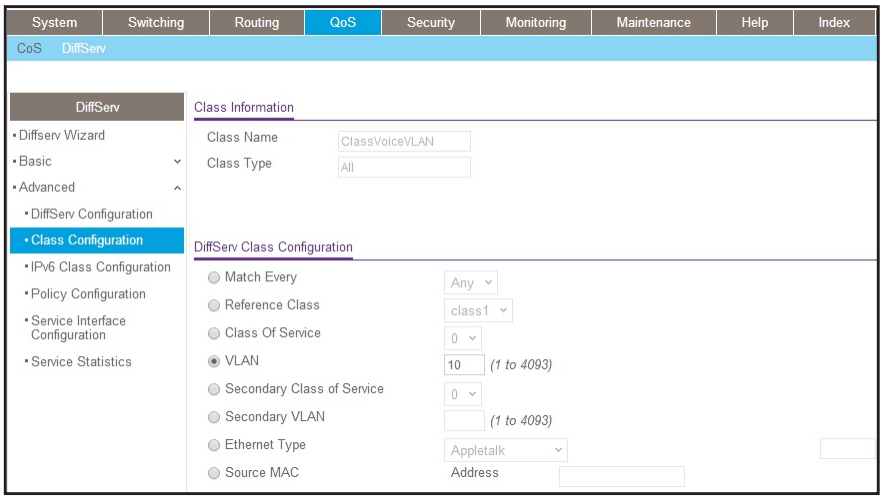
   b. In the **Class Name** field, enter **ClassVoiceVLAN**.
   c. In the **Class Type** menu, select **All**.
   d. Click the **Add** button. Your settings are saved.
6. Configure matching criteria for the class as **VLAN 10**.
   a. Select **QoS > DiffServ > Advanced > Class Configuration**.

      A page similar to the following figure displays.



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

A page similar to the following figure displays.

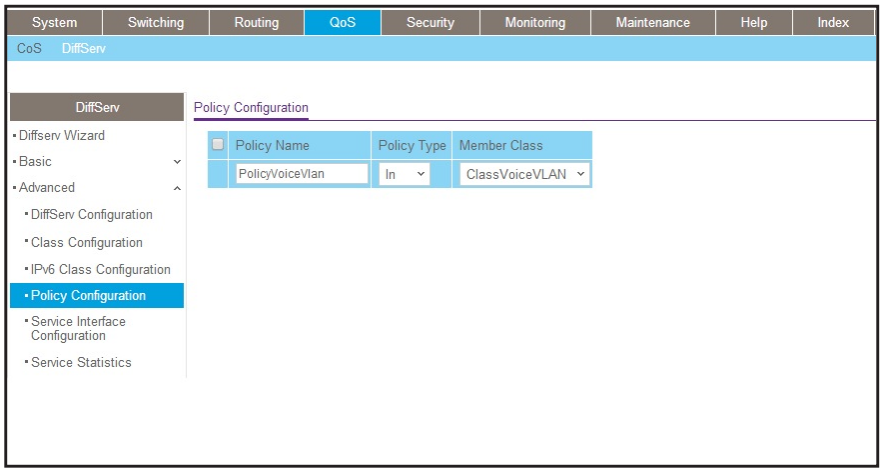


e. Click the **Apply** button. Your settings are saved.

7. Create the DiffServ policy PolicyVoiceVLAN.

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

A page similar to the following figure displays.



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

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

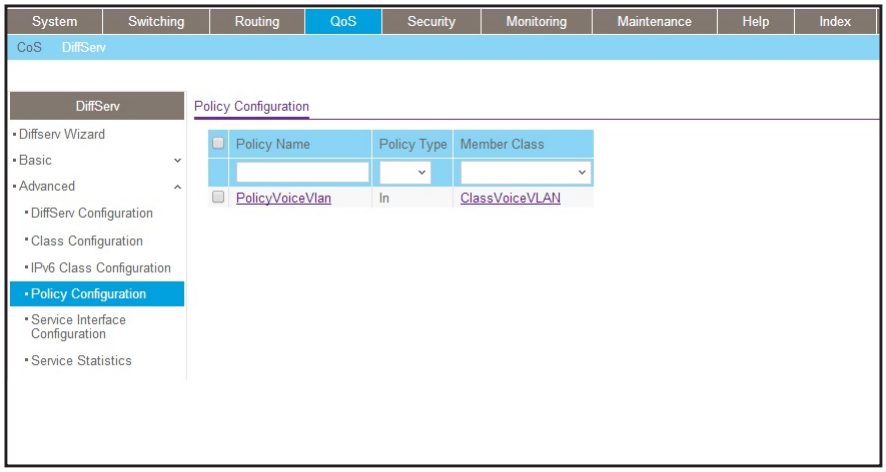
d. In the **Member Class** menu, select **ClassVoiceVLAN**.

e. Click the **Add** button. Your settings are saved.

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

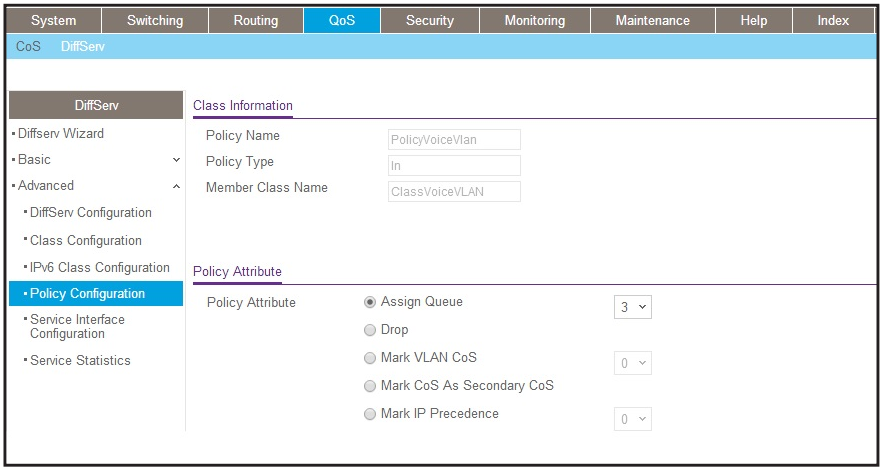
a. Select **QoS > DiffServ > Advanced > Policy Configuration**.

A page similar to the following figure displays.



b. Click **PolicyVoiceVLAN**.

A page similar to the following figure displays.



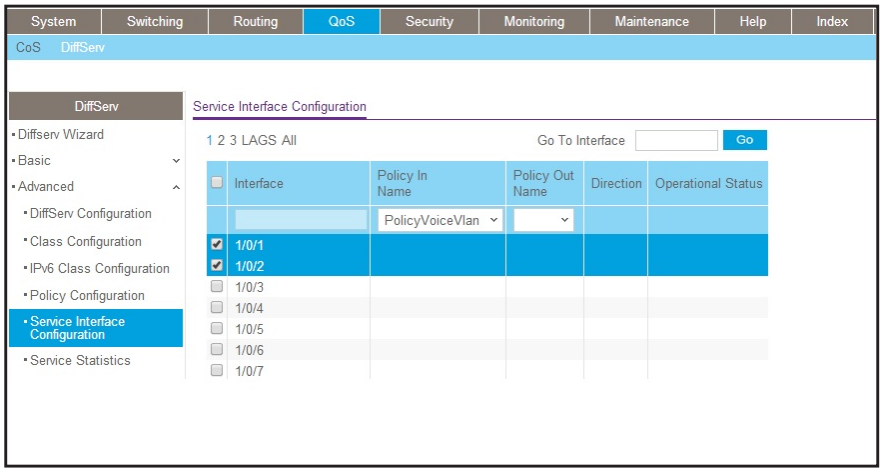
c. Select the **Assign Queue** radio button, and in the associated menu, select **3**.

d. Click the **Apply** button. Your settings are saved.

9. Assign the policy to interfaces 1/0/1 and 1/0/2.

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

A page similar to the following figure displays.



b. Select the Interface **1/0/1** check box and Interface **1/0/2** check box.

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

d. Click the **Apply** button. Your settings are saved.

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 6. GVRP configuration

CLI: Enable GVRP

To use the CLI to create VLANs on Switch A and enable GVRP on both switch A and Switch B:

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.

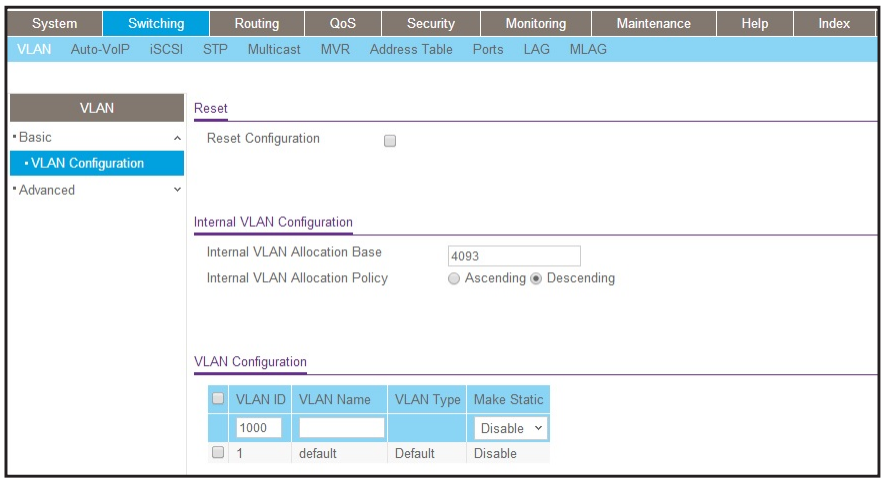
```
(Netgear Switch) #show vlan

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
```

Main UI: Configure GVRP on switch A

To use the main UI to create VLANs on Switch A and enable GVRP on switch A:

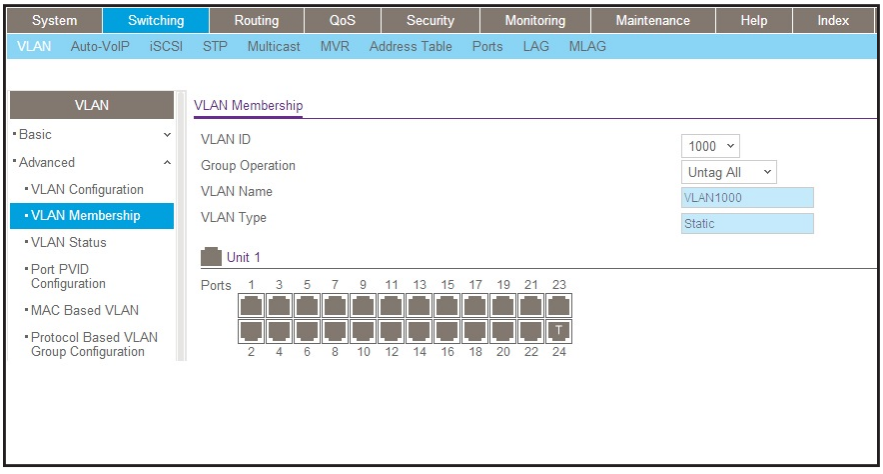
1. On Switch A, create VLANs 1000, 2000, and 3000:
   a. Select **Switching > VLAN > Advanced > VLAN Configuration**.

      A page similar to the following figure displays.



   b. In the **VLAN ID** field, enter **1000**.
   c. Click the **Add** button. Your settings are saved.
   d. Repeat Step b and Step c to create VLAN 2000 and then repeat these steps again to create VLAN 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 page similar to the following figure displays.



   b. From the **VLAN ID** menu, select **1000**.

c. Click the gray box under port **24** until a T displays, specifying that switch tags egress packets for port 24.

   If your switch is a member of a stack, be sure that you select the port in the correct unit.

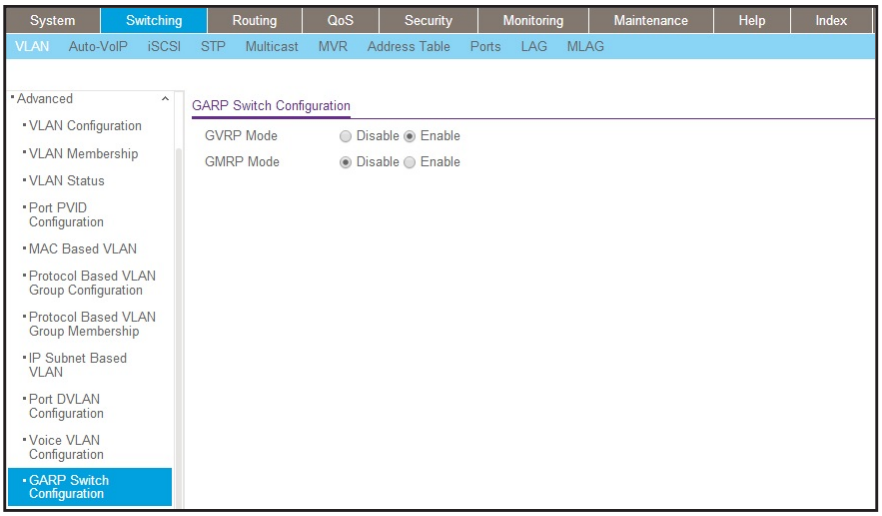
d. Click the **Apply** button. Your settings are saved.

e. Repeat Step b through Step d to add port 1/0/24 as a tagged port to VLAN 2000, and then repeat these steps again to do the same for VLAN 3000.

3. Enable GVRP globally:

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

      A page similar to the following figure displays.



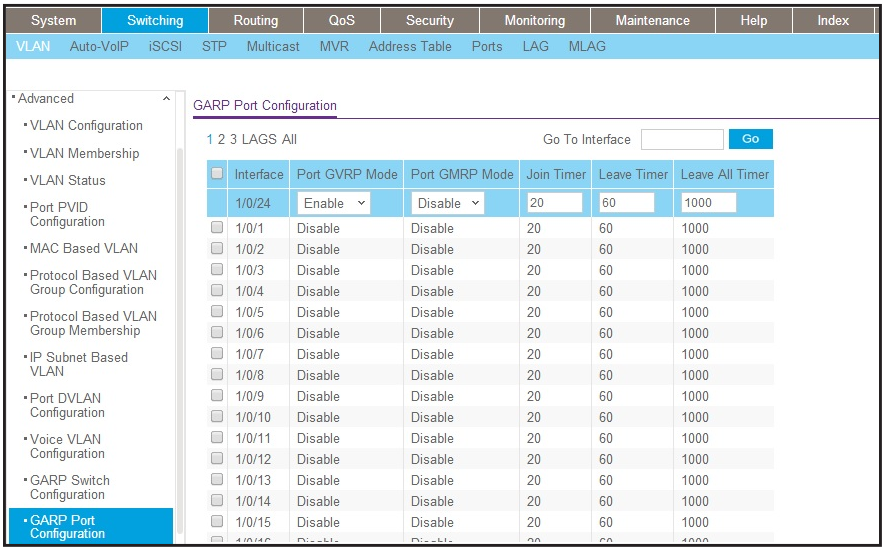
   b. Select the GVRP Mode **Enable** radio button.

   c. Click the **Apply** button. Your settings are saved.

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

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

      A page similar to the following figure displays.



b. Select the Interface **1/0/24** check box.

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

d. Click the **Apply** button. Your settings are saved.

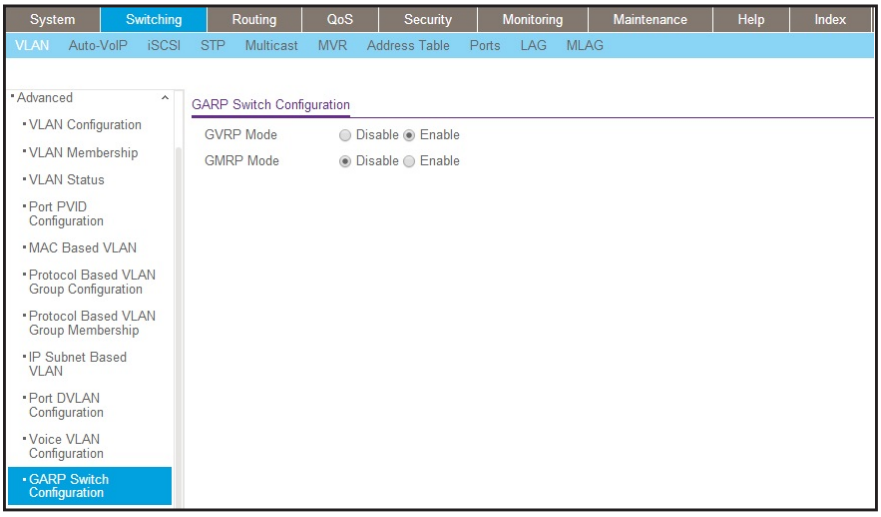
Main UI: Configure GVRP on Switch B

To use the main UI to enable GVRP on switch B:

1. Enable GVRP globally:

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

A page similar to the following figure displays.

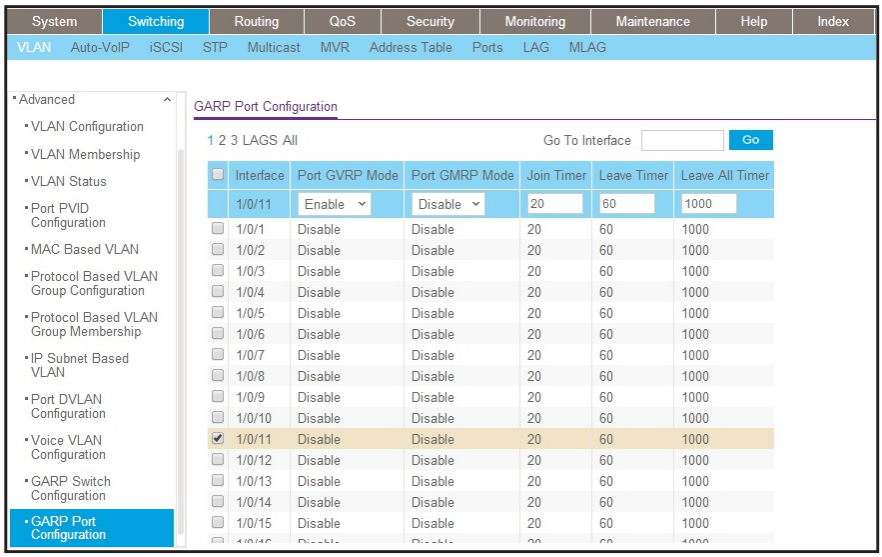


b. Select the GVRP Mode **Enable** radio button.

c. Click the **Apply** button. Your settings are saved.

2. Enable GVRP on port 1/0/11:
   a. Select **Switching > VLAN > Advanced > GARP Port Configuration**.

      A page similar to the following figure displays.



   b. Select the Interface **1/0/11** check box.
   c. In the **GVRP Mode** menu, select **Enable**.
   d. Click the **Apply** button. Your settings are saved.

Private VLANs

The Private VLAN 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 VLANs within a private VLAN:

- **Primary VLAN**. This VLAN 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**. This 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**. This VLAN is also a secondary VLAN. It carries traffic from isolated ports to promiscuous ports. For a private VLAN, only one isolated VLAN can be configured.

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

- **Promiscuous port**. This 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 port**. This port can communicate with other community ports and promiscuous ports.
- **Isolated port**. This port can communicate only with promiscuous ports.

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

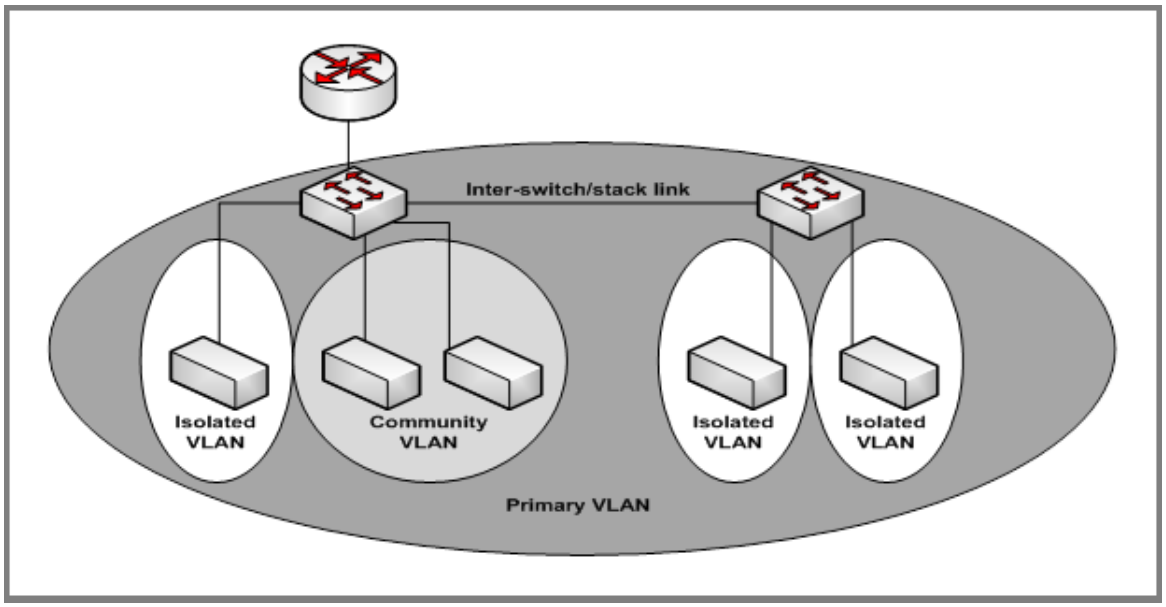


Figure 7. Private VLANs

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 link, and is configured to transmit VLANs 100, 101 and 102. Colored arrows represent possible packet flow paths in the private VLAN domain.

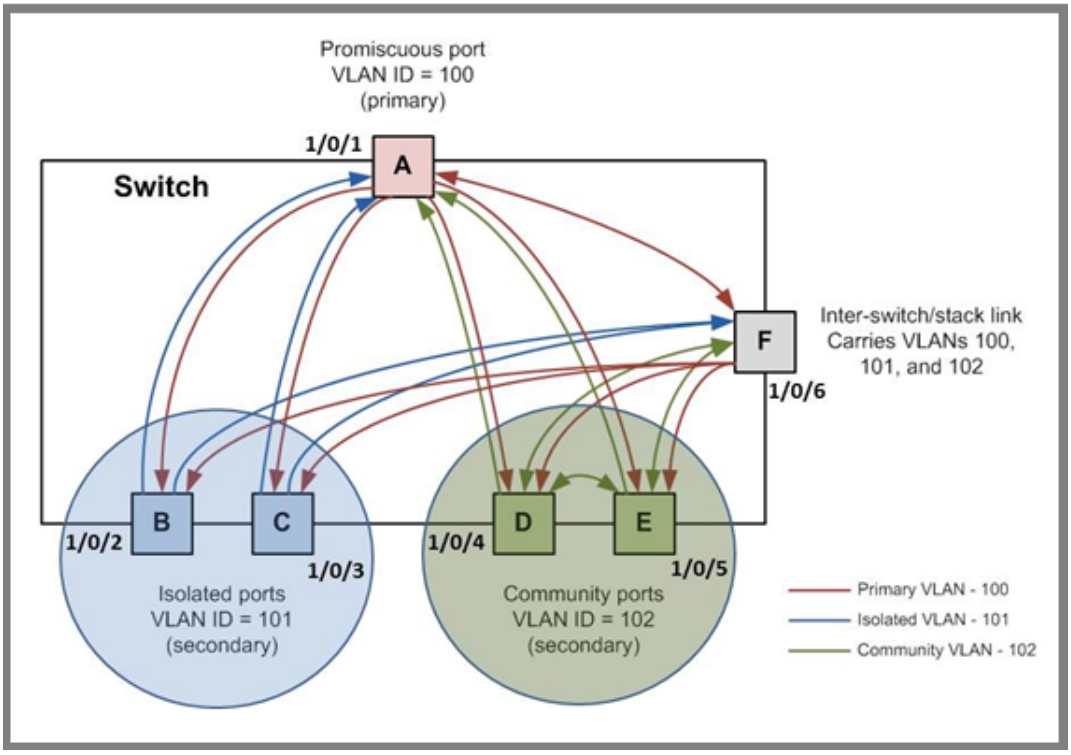


Figure 8. Packet flow within a Private VLAN domain

Assign private VLAN types (primary, isolated, community)

The example is shown as CLI commands and as a main UI procedure.

CLI: Assign private VLAN types (primary, isolated, community)

To use the CLI to assign private VLAN types:

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

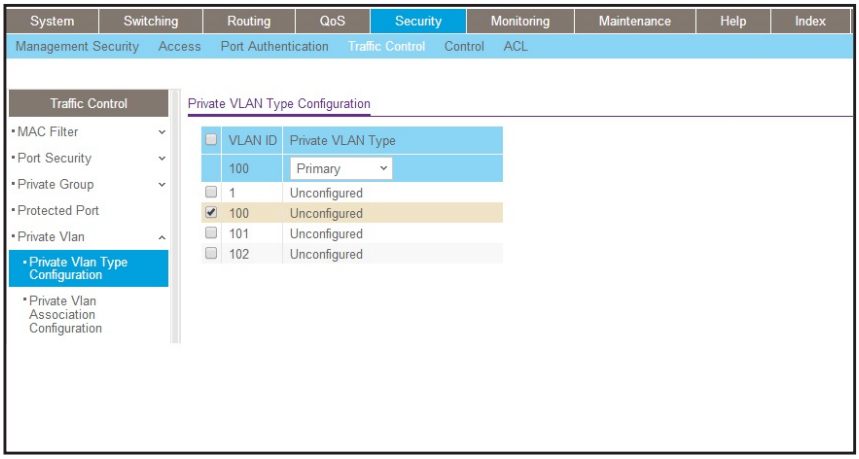
```
(Netgear Switch) #config
(Netgear Switch) (Config)#vlan 100
(Netgear Switch) (Config)(Vlan) #private-vlan primary
(Netgear Switch) (Config)(Vlan) #exit
(Netgear Switch) (Config)#vlan 101
(Netgear Switch) (Config)(Vlan) #private-vlan isolated
(Netgear Switch) (Config)(Vlan) #exit
(Netgear Switch)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

Main UI: Assign private VLAN types (primary, isolated, community)

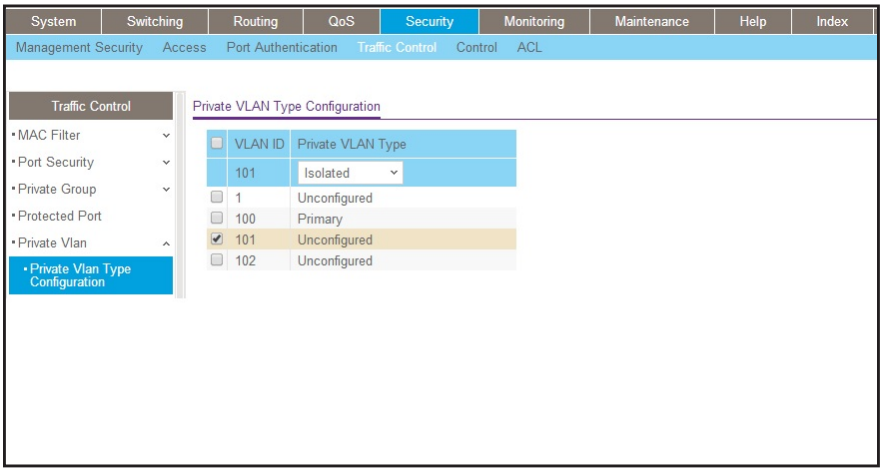
To use the main UI to assign private VLAN types:

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

      A page similar to the following figure displays.

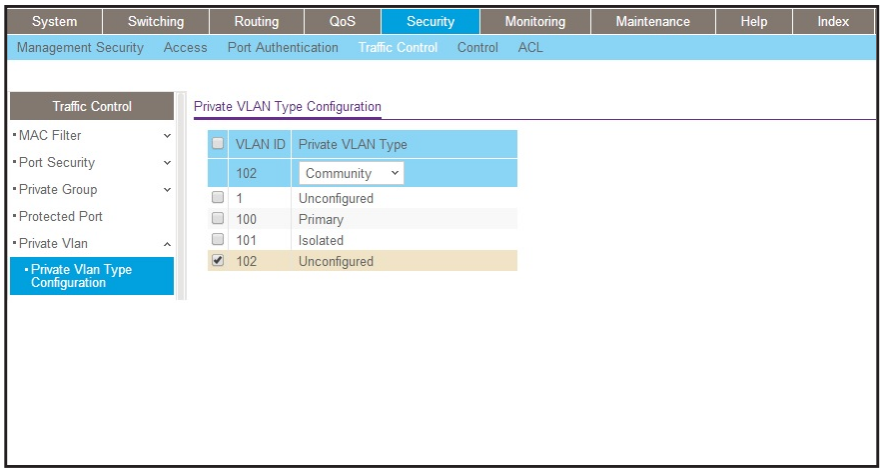


   b. Select the VLAN ID **100** check box.
   c. In the **Private VLAN Type** field, select **Primary** from the menu.
   d. Click **Apply** to save the settings
2. Assign VLAN 101 as an isolated VLAN.
   a. Remain on the same page.



   b. Select the VLAN ID **101** check box.
   c. In the **Private VLAN Type** menu, select **Isolated**.
   d. Click **Apply** to save the settings

3. Assign VLAN 102 to a community VLAN.
   a. Remain on the same page.



   b. Select the VLAN ID **102** check box.
   c. In the **Private VLAN Type** field, select **Community** from the menu.
   d. Click the **Apply** button. Your settings are saved.

Configure a private VLAN association

The example is shown as CLI commands and as a main UI procedure.

CLI: Configure a private VLAN association

To use the CLI to associate VLAN 101-102 (secondary VLAN) to VLAN 100 (primary VLAN):

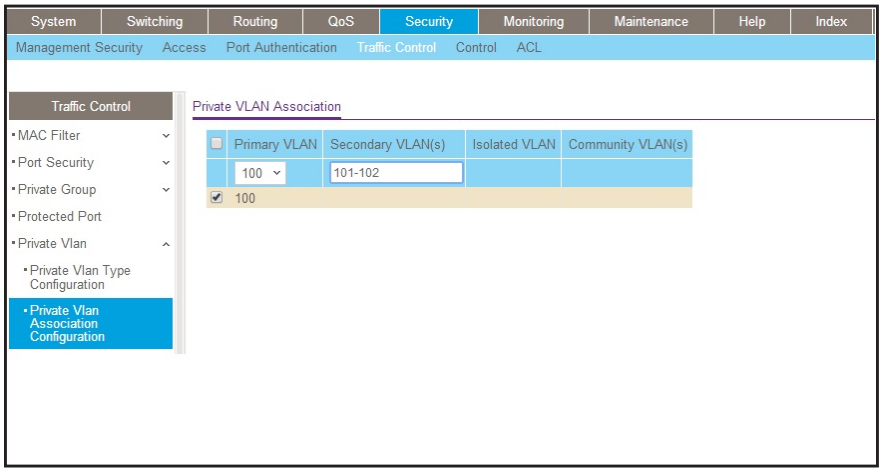
```
(Netgear Switch) #config
(Netgear Switch) (Config)#vlan 100
(Netgear Switch) (Config)(Vlan) #private-vlan association 101-102
(Netgear Switch) (Config)(Vlan) #end
```

Main UI: Configure a private VLAN association

To use the main UI to associate VLAN 101-102 (secondary VLAN) to VLAN 100 (primary VLAN):

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

   A page similar to the following figure displays.



2. Select the Primary VLAN **100** check box.
3. In the **Secondary VLAN(s)** field, type **101-102**.
4. Click the **Apply** button. Your settings are saved.

Configure the private VLAN port mode (promiscuous, host)

The example is shown as CLI commands and as a main UI procedure.

CLI: Configure the private VLAN port mode (promiscuous, host)

To use the CLI to configure the private-VLAN port mode:

Assign port 1/0/1 to promiscuous port mode and ports 1/0/2-1/0/5 to host port mode.

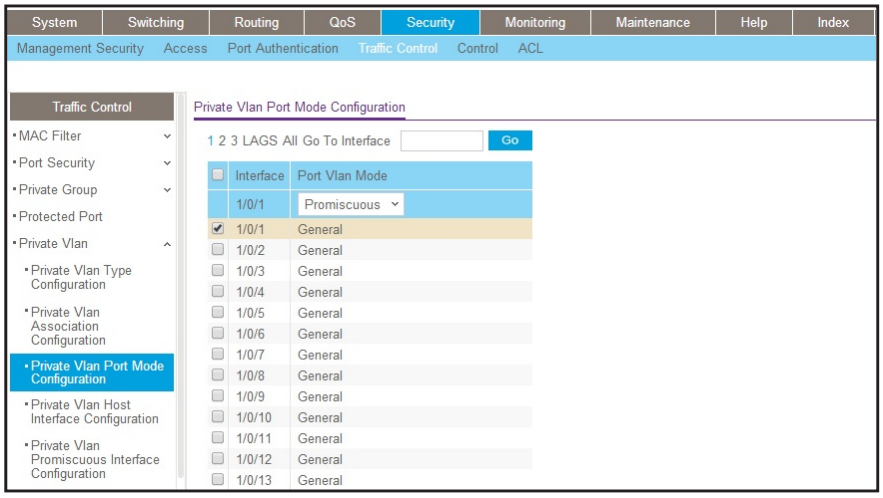
```
(Netgear Switch) #config
(Netgear Switch) (Config)#interface 1/0/1
(Netgear Switch) (Interface 1/0/1)#switchport mode private-vlan promiscuous
(Netgear Switch) (Interface 1/0/1)#exit
(Netgear Switch) (Config)#interface 1/0/2-1/0/5
(Netgear Switch) Interface 1/0/2-1/0/5)#switchport mode private-vlan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

Main UI: Configure the private VLAN port mode (promiscuous, host)

To use the main UI to configure the private-VLAN port mode:

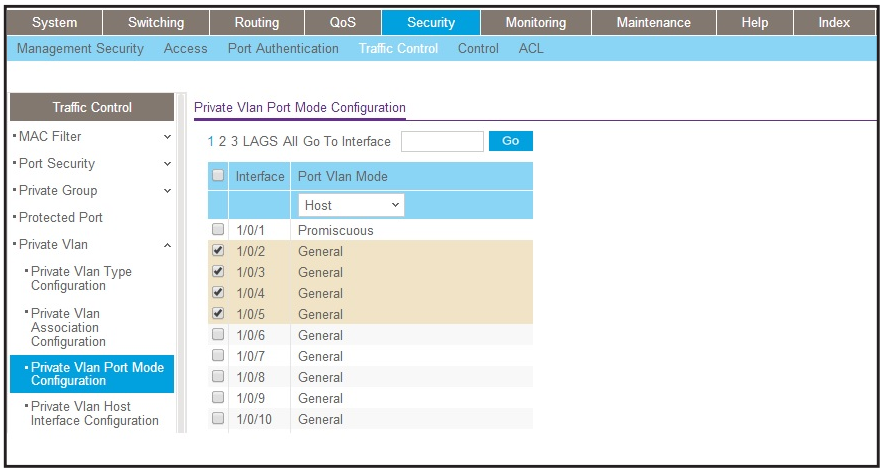
1. Configure port 1/0/1 to promiscuous port mode.
   a. Select **Security > Traffic Control > Private VLAN > Private VLAN Port Mode Configuration**.

      A page similar to the following figure displays.



   b. Select the Interface **1/0/1** check box.
   c. In the **VLAN Mode** field, select **Promiscuous** from the menu.
   d. Click the **Apply** button. Your settings are saved.
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 page similar to the following figure displays.



b. Select the Interface **1/0/2** through Interface **1/0/5** check boxes.
c. In the **VLAN Mode** field, select **Host** from the menu.
d. Click the **Apply** button. Your settings are saved.

Configure private VLAN host ports

The example is shown as CLI commands and as a main UI procedure.

CLI: Configure private VLAN host ports

To use the CLI to associate isolated ports 1/0/2-1/0/3 to a private-VLAN (primary=100, secondary=101) and community ports 1/0/4-1/0/5 to a private-VLAN (primary=100, secondary=102):

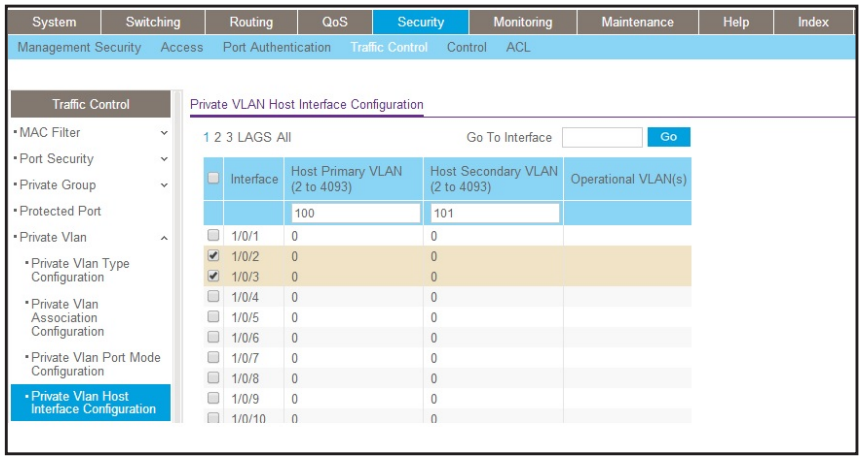
```
(Netgear Switch) #config
(Netgear Switch) (Config)#interface 1/0/2-1/0/3
(Netgear Switch) (Interface 1/0/2-1/0/3)#switchport private-vlan host-association
100 101
(Netgear Switch) (Interface 1/0/2-1/0/3)#exit
(Netgear Switch) (Config)#interface 1/0/4-1/0/5
(Netgear Switch) (Interface 1/0/4-1/0/5)#switchport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

Main UI: Configure private VLAN host ports

To use the main UI to associate isolated ports 1/0/2-1/0/3 to a private-VLAN (primary= 100, secondary=101) and community ports 1/0/4-1/0/5 to a private-VLAN (primary=100, secondary=102):

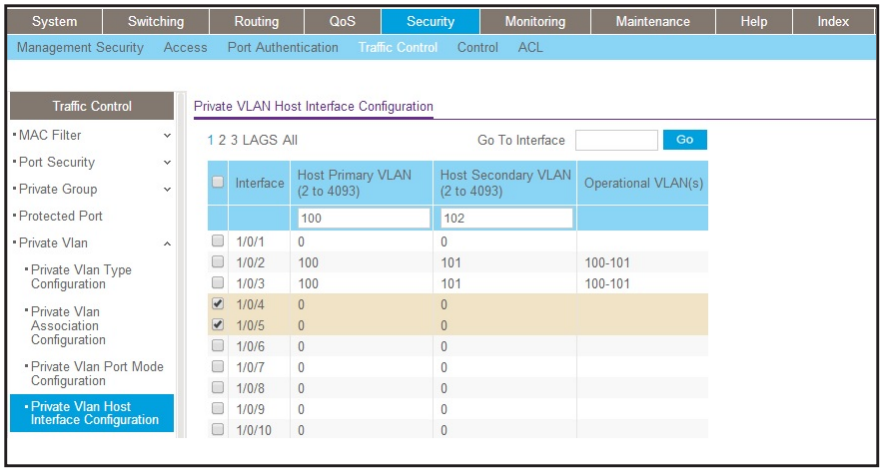
1. Associate isolated ports 1/0/2-1/0/3 with a private-VLAN (primary=100, secondary=101).
   a. Select **Security > Traffic Control > Private VLAN > Private VLAN Host Interface Configuration**.

   A page similar to the following figure displays.



b. Select the Interface **1/0/2** check box and Interface **1/0/3** check box.
c. In the **Host Primary VLAN** field, enter **100**.
d. In the **Host Secondary VLAN** field, enter **101**.
e. Click the **Apply** button. Your settings are saved.

2. Associate isolated ports 1/0/4-1/0/5 to a private-VLAN (primary=100, secondary=102).
   a. Remain on the same page.



   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 the **Apply** button. Your settings are saved.

Map a private VLAN promiscuous port

The example is shown as CLI commands and as a main UI procedure.

CLI: Map a private VLAN promiscuous port

To use the CLI to map private-VLAN promiscuous port 1/0/1 to a primary VLAN (100) and to select secondary VLANs (101-102):

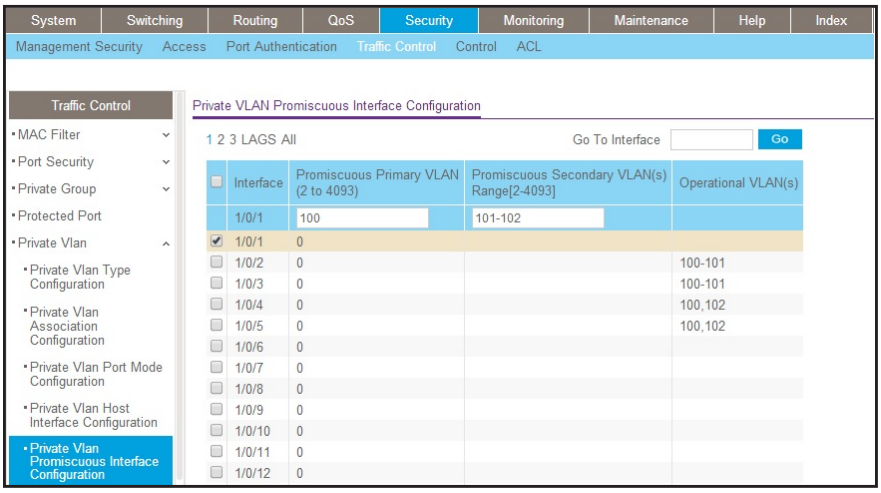
```
(Netgear Switch) #config
(Netgear Switch) (Config)#interface 1/0/1
(Netgear Switch) (Interface 1/0/1)#switchport private-vlan mapping 100 101-102
(Netgear Switch) (Interface 1/0/1)#end
```

Main UI: Map a private VLAN promiscuous port

To use the main UI to map private-VLAN promiscuous port 1/0/1 to a primary VLAN (100) and to select secondary VLANs (101-102):

1. Select **Security > Traffic Control > Private VLAN > Private VLAN Promiscuous Interface Configuration**.

   A page similar to the following figure displays.



2. Select the Interface **1/0/1** check box.
3. In the **Promiscuous Primary VLAN** field, enter **100**.
4. In the **Promiscuous Secondary VLAN** field, enter **101-102**.
5. 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 (for example, a desktop computer), 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:

- **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.
- **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.

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

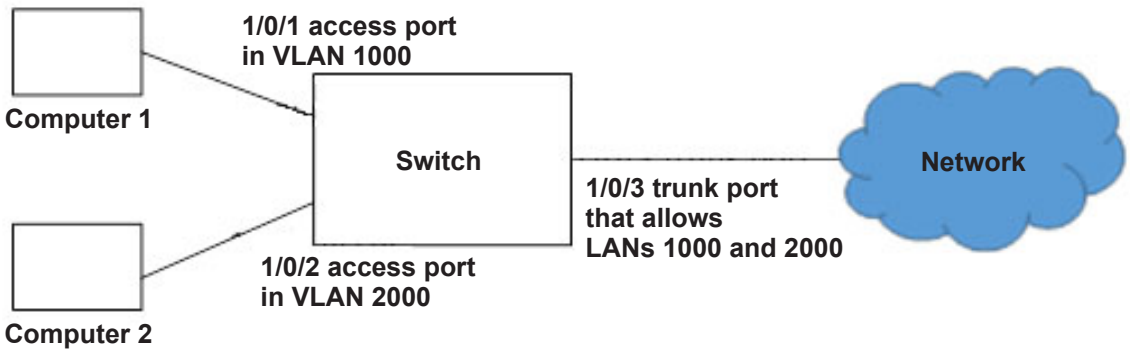


Figure 9. Access and trunk ports

CLI: Configure a VLAN trunk

To use the CLI to configure a trunk VLAN:

1. Create VLAN 1000 and VLAN 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.

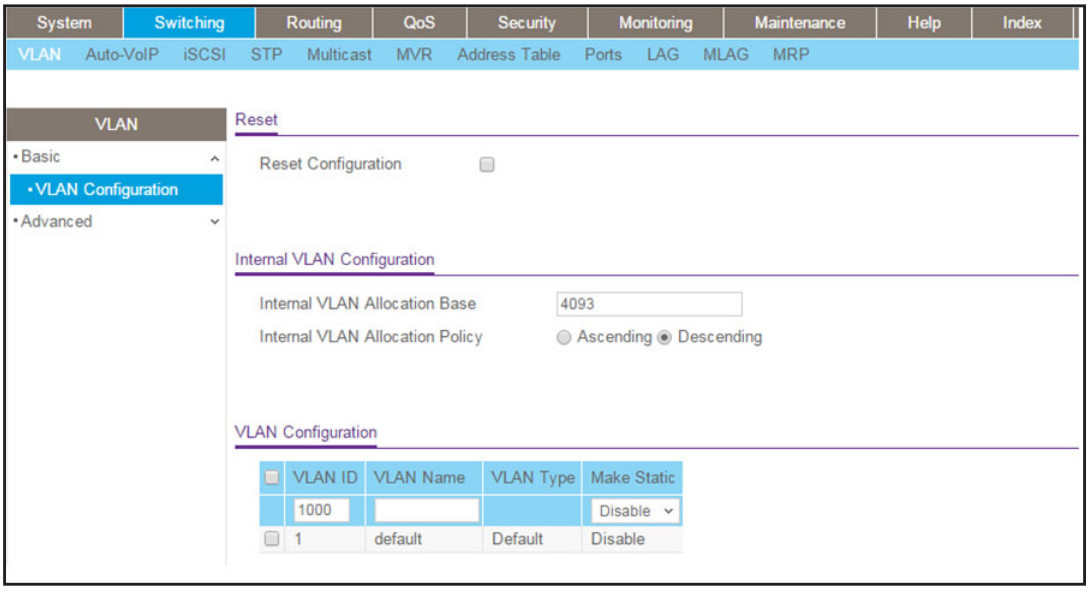
```
(Netgear Switch) (Interface 1/0/3)#switchport trunk native vlan 1000
```

Main UI: Configure a VLAN trunk

To use the main UI to configure a trunk VLAN:

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

      A page similar to the following figure displays.

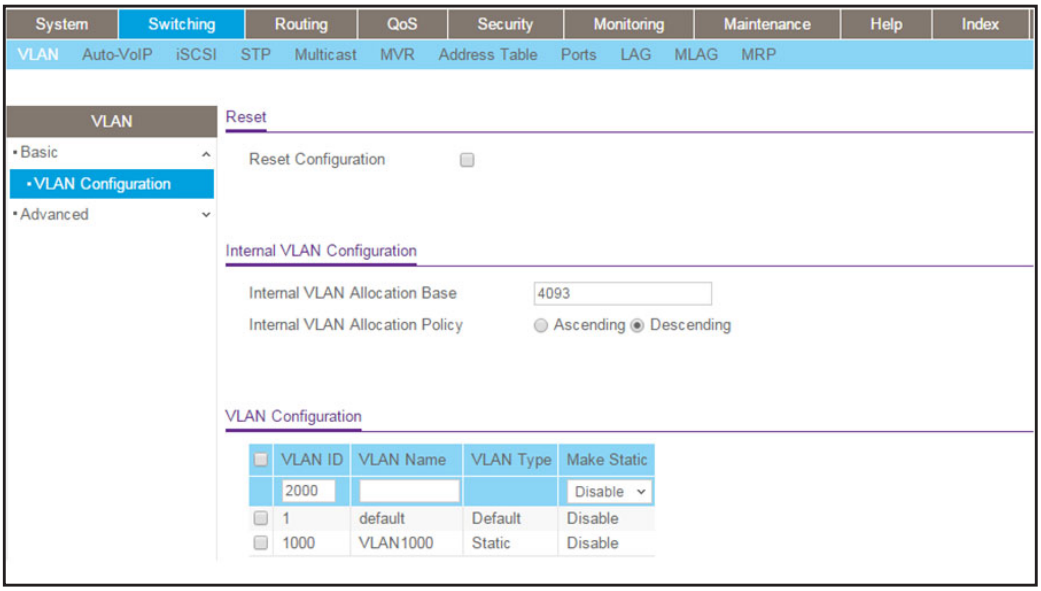


   b. In the **VLAN ID** field, enter **1000**.

c. Click the **Add** button. Your settings are saved.

2. Create VLAN 2000.

d. Remain on the same page.



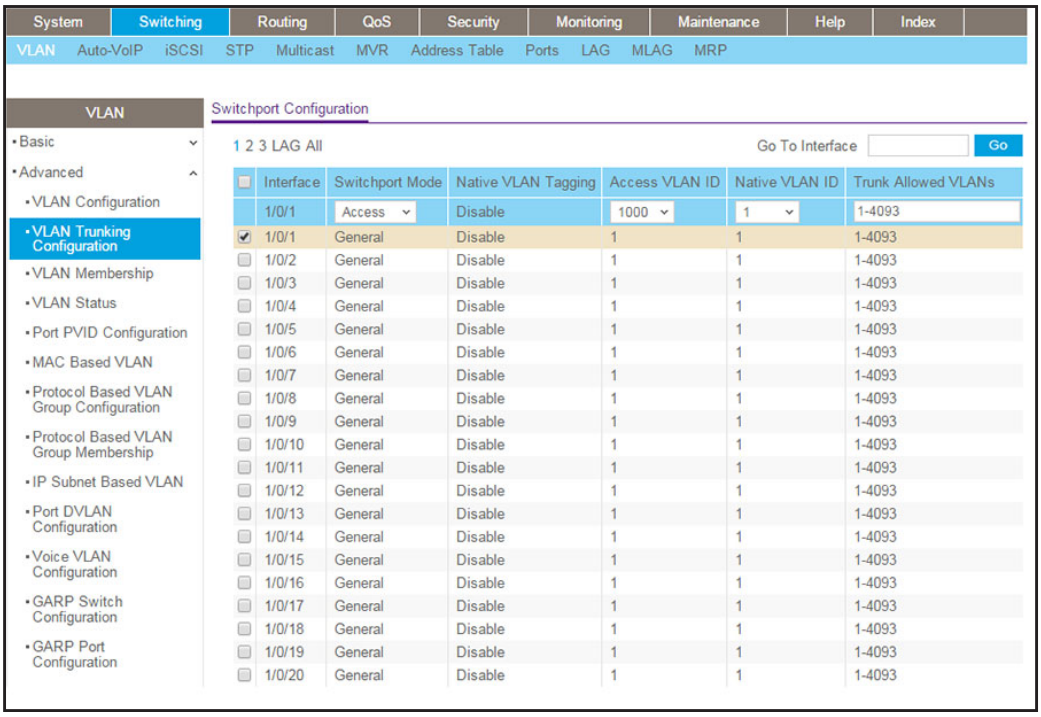
e. In the **VLAN ID** field, enter **2000**.

f. Click the **Add** button. Your settings are saved.

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

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

A page similar to the following figure displays.



b. Select the Interface **1/0/1** check box.

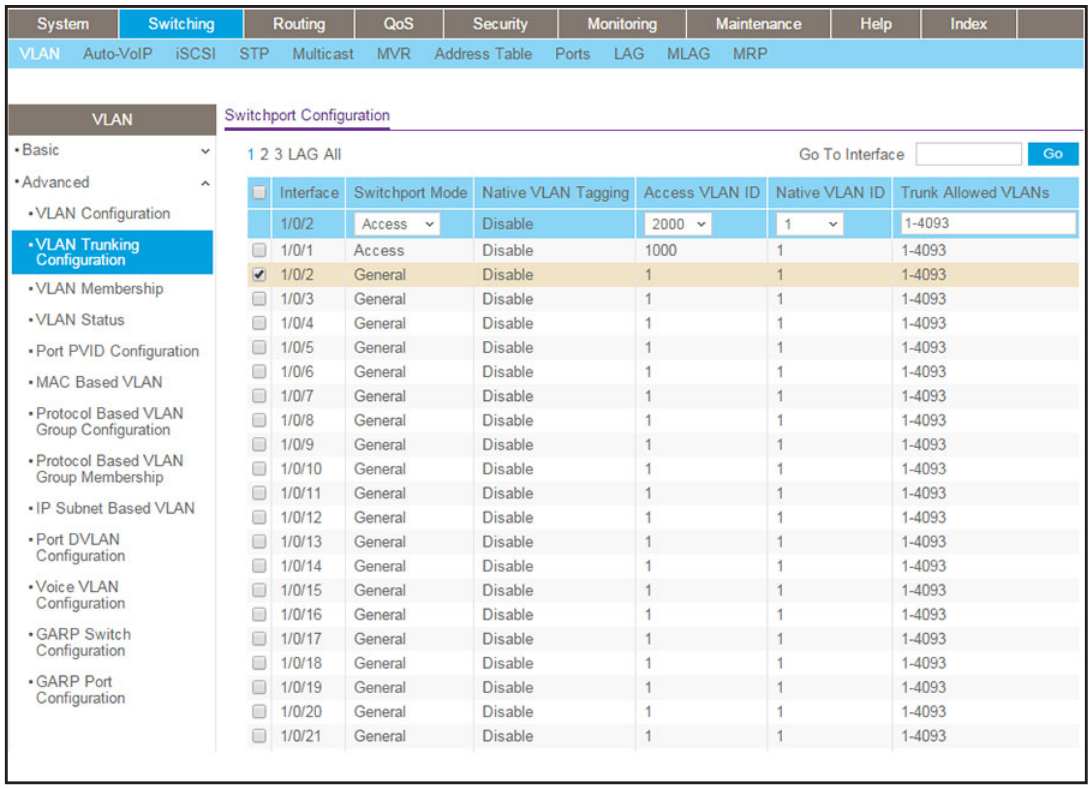
c. In the **Switch Port Mode** field, select **Access**.

d. In the **Access VLAN ID** field, select **1000**.

e. Click the **Apply** button. Your settings are saved.

4. Configure port 1/0/2 as an access port in VLAN 2000.

a. Remain on the same page.



b. Select the Interface **1/0/2** check box.

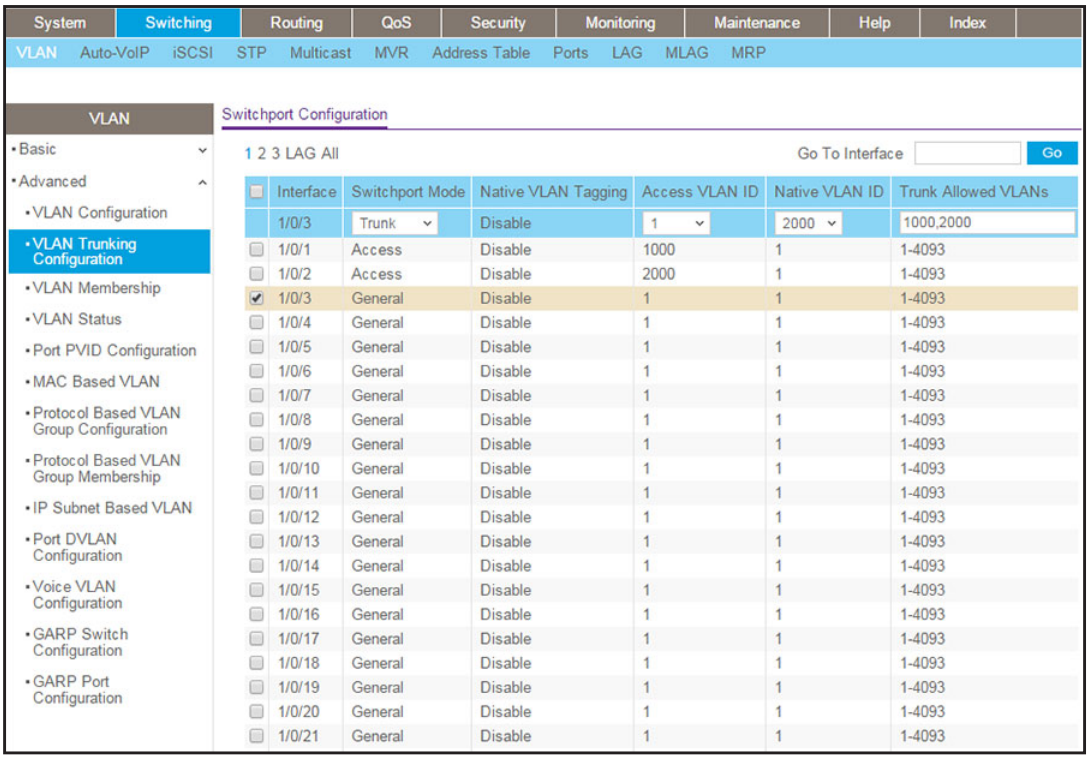
c. In the **Switch Port Mode** menu, select **Access**.

d. In the **Access VLAN ID** menu, select **2000**.

e. Click the **Apply** button. Your settings are saved.

5. Configure port 1/0/3 as a trunk port that allows VLANs 1000 and 2000.

a. Remain on the same page.



b. Select the Interface **1/0/3** check box.

c. In the **Switch Port Mode** menu, select **Trunk**.

d. In the **Native VLAN ID** menu, 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 the **Apply** button. Your settings are saved.

3

LAGs

Link Aggregation Groups

This feature is supported on the M4250 series switches

This feature is supported on the M4300 series switches

This feature is supported on the M4350 series switches

This chapter includes the following sections:

- Link aggregation concepts
- Add ports to LAGs
- Auto-LAG

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 link aggregation group (LAG) must operate in full-duplex mode and at the same speed. You can use a LAG to directly connect two switches if 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 were a single physical port. A Layer 2 LAG can carry one or more VLANs. You can configure more than one LAG for a switch.

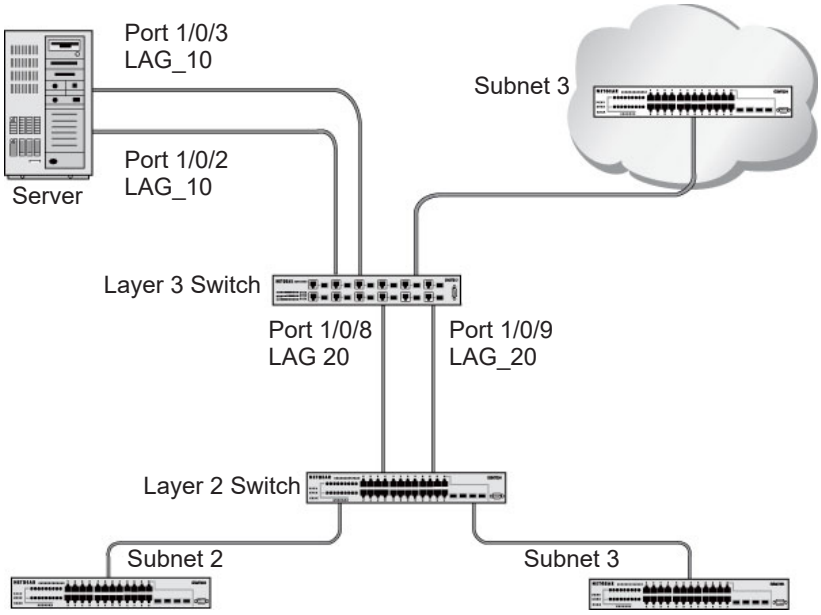


Figure 10. Example network with two LAGs

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.

Note: A LAG is also referred to as a port channel or an EtherChannel.

Add ports to LAGs

The example is shown as CLI commands and as a main UI procedure.

CLI: Add ports to LAG

To use the CLI to add ports to LAGs:

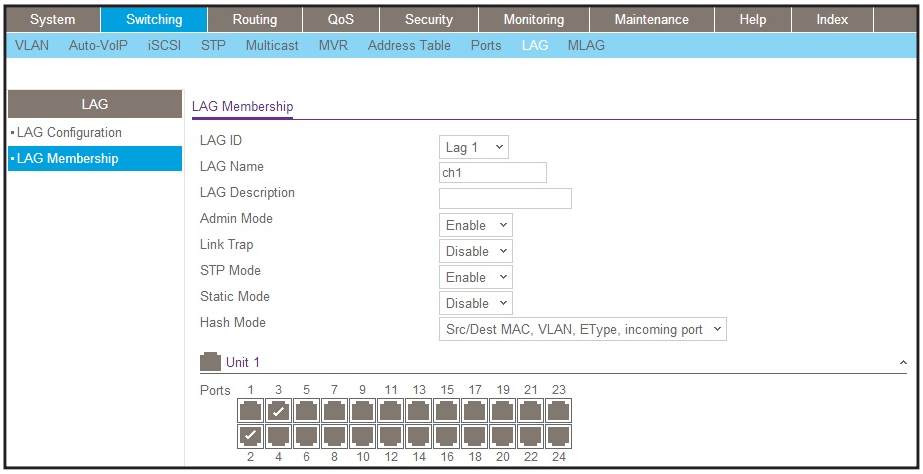
```
(Netgear Switch) #config
(Netgear Switch) (Config)#interface 0/2
(Netgear Switch) (Interface 0/2)#addport 1/1
(Netgear Switch) (Interface 0/2)#exit
(Netgear Switch) (Config)#interface 0/3
(Netgear Switch) (Interface 0/3)#addport 1/1
(Netgear Switch) (Interface 0/3)#exit
(Netgear Switch) (Config)#interface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

Main UI: Add ports to LAGs

To use the main UI to add ports to LAGs:

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

   A page similar to the following figure displays.



b. In the **LAG ID** menu, select **LAG 1**.

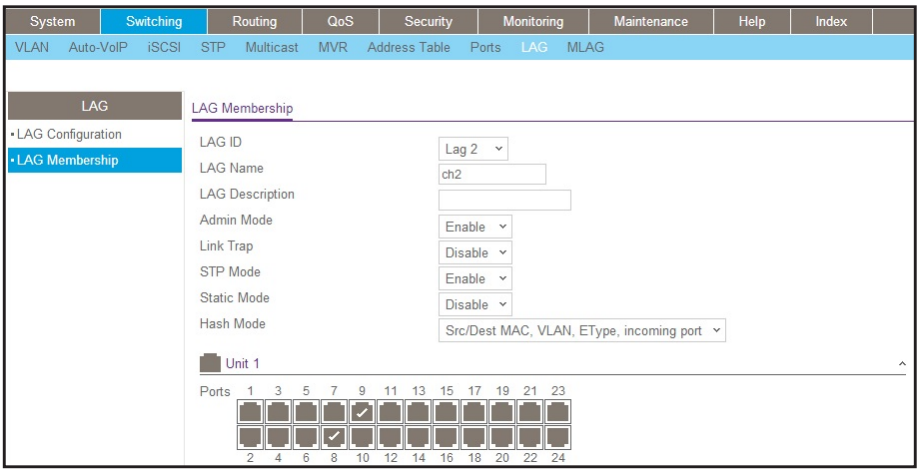
c. Click the gray boxes under ports **2** and **3**. A check mark displays in each box.

If your switch is a member of a stack, be sure that you select the ports in the correct unit.

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

2. Add ports to lag_20.

a. Remain on the same page.



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

c. Click the gray boxes under ports **8** and **9**. A check mark displays in each box.

If your switch is a member of a stack, be sure that you select the ports in the correct unit.

d. Click the **Apply** button. Your settings are saved.

Auto-LAG

An Auto-LAG is a LAG that forms automatically between two devices that support the Auto-LAG feature. An Auto-LAG is a dynamic Layer 2 LAG that is based on the Link Aggregation Control Protocol (LACP).

Note: A LAG is also referred to as a port channel or an EtherChannel.

The switch can detect the physical links with a partner device and automatically configure a LAG (that is, an Auto-LAG) on interconnected and capable ports at both ends. The switch can form one Auto-LAG only with each partner device.

The Auto-LAG feature functions together with the Auto-Trunk feature, which must also be supported and enabled on the partner device with which the LAG is formed. After an

Auto-LAG is formed, the switch automatically applies trunk mode (that is, an Auto-Trunk) to the LAG at both ends. In other words, after an Auto-LAG is formed, the mode for the ports that participate in an Auto-LAG changes from the default switch port mode to the trunk port mode. For more information about the Auto-Trunk feature, see Auto-Trunk on page 26.

For the switch to form an Auto-LAG with a partner device, the following are required:

- Both the Auto-LAG and Auto-Trunk features must be supported and globally enabled on the switch and the partner device. (On all M4250 and M4350 series switch models, the Auto-LAG and Auto-Trunk features are enabled by default; On all M4300 series switch models, the Auto-LAG and Auto-Trunk features are disabled by default.)
- At least two links must be established between the switch and the partner device, and these links must support the same speed and duplex mode.
- The links cannot be members of a manually configured static or dynamic LAG.
- LLDP must be enabled on the interconnected ports on the switch and the partner device. (On all M4250, M4300, and M4350 series switch models, LLDP is enabled by default on all ports.)
- The interconnected ports on the switch and the partner device must be in the default switch port mode, which is the General mode. If the ports are in the Access mode or already in the Trunk mode, an Auto-Trunk cannot be formed on the Auto-LAG.

An Auto-LAG can form with up to eight interfaces as members. Interfaces are automatically selected for the Auto-LAG based on whether they are up and available and on the following conditions:

- The interface is not already manually configured as a member of a LAG.
- The interface is not manually configured as a trunk port or an access port. That is, the interface must be a general interface.

Note: The switch can support multiple static and dynamic LAGs, but with each partner device, the switch can support a single Auto-LAG only.

CLI: Enable the Auto-LAG feature

By default, the Auto-LAG feature is enabled. If you disable it, you can enable it again.

To use the CLI to enable the Auto-LAG feature:

```
(Netgear Switch)#configure
(Netgear Switch)(Config)#port-channel auto
(Netgear Switch)(Config)#exit
(Netgear Switch)#
```

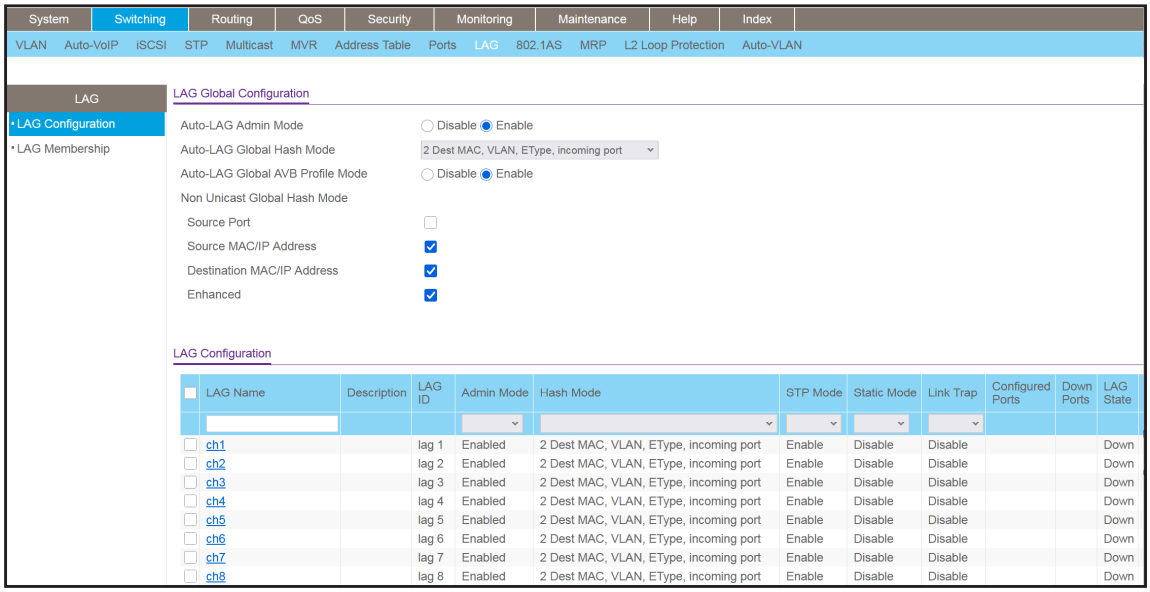
Main UI: Enable the Auto-LAG feature

By default, the Auto-LAG feature is enabled. If you disable it, you can enable it again.

To use the main UI to enable the Auto-LAG feature:

1. Select **Switching > LAG > LAG Configuration**.

   A page similar to the following figure displays.



2. Select the Auto-LAG Enable Mode **Enable** radio button.

   By default, the Auto-LAG feature is enabled. The default hash mode depends on the switch series. You can change the hash mode for the Auto-LAG feature.

3. To change the hash mode, from the **Auto-LAG Global Hash Mode** menu, select the hash mode.
4. Click the **Apply** button. Your settings are saved.

4

Port Routing

Port routing, default routes, and static routes

This feature is supported on the M4250 series switches

This feature is supported on the M4300 series switches

This feature is supported on the M4350 series switches

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

Historically, 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 globally (for the entire switch), and then for each port that must 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 must 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 you issue the routing configuration commands, the following functions will be active:

- IP forwarding, responsible for forwarding received IP packets.
- ARP mapping, responsible for maintaining the ARP table that is 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 that is used by all registered routing protocols.

You can then activate RIP or OSPF (supported on an M4350 switch only), which is 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.

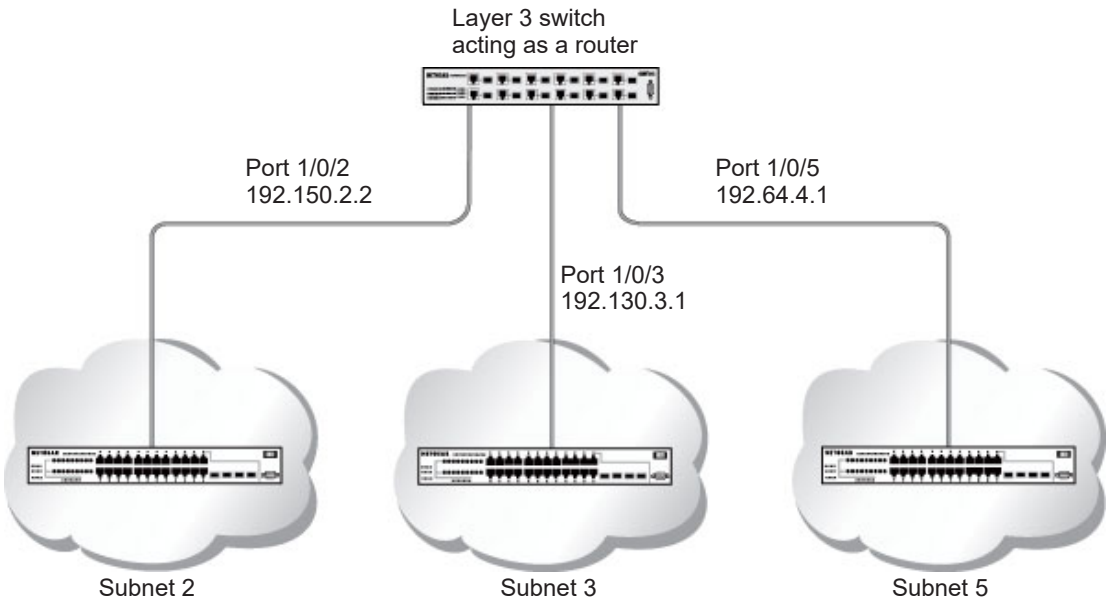


Figure 11. Layer 3 switch configured for port routing

Enable routing for the switch

The example is shown as CLI commands and as a main UI 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 11, Layer 3 switch configured for port routing on page 89.

To use the CLI to enable routing for the switch, which, by default, enables IP forwarding:

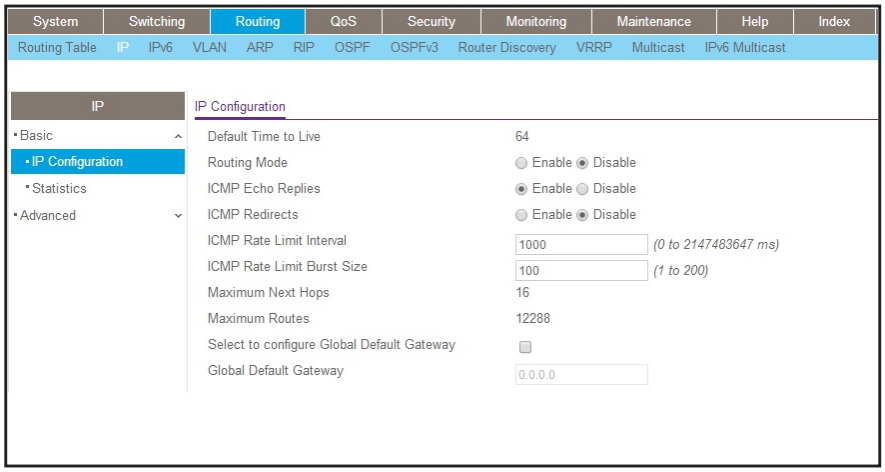
```
(Netgear Switch) #config
(Netgear Switch) (Config)#ip routing
(Netgear Switch) (Config)#exit
```

Main UI: Enable routing for the switch

To use the main UI to enable routing for the switch, which, by default, enables IP forwarding:

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

   A page similar to the following figure displays.



2. For Routing Mode, select the **Enable** radio button.
3. Click the **Apply** button. Your settings are saved.

Enable routing for ports on the switch

Use the following commands or the main UI 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 depends on the switch series:

- M4250 series switch: MTU from 1500 to 12227.
- M4300 series switch: MTU from 1500 to 9000.
- M4350 series switch: MTU from 1500 to 12266.

CLI: Enable routing for ports on the switch

To use the CLI to enable routing for ports on the switch:

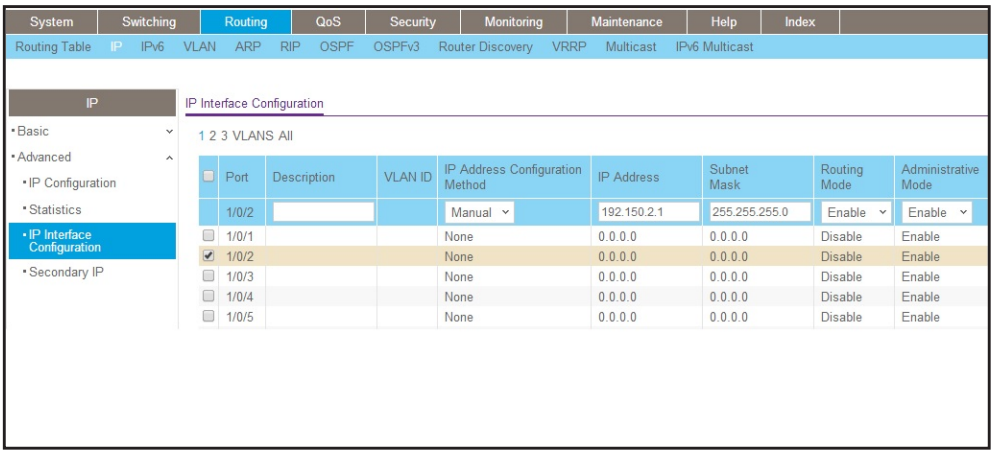
```
(Netgear Switch) #config
(Netgear Switch) (Config)#interface 1/0/2
(Netgear Switch) (Interface 1/0/2)#routing
(Netgear Switch) (Interface 1/0/2)#ip address 192.150.2.1 255.255.255.0
(Netgear Switch) (Interface 1/0/2)#exit

(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
```

Main UI: Enable routing for ports on the switch

To use the main UI to 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 page similar to the following figure displays.



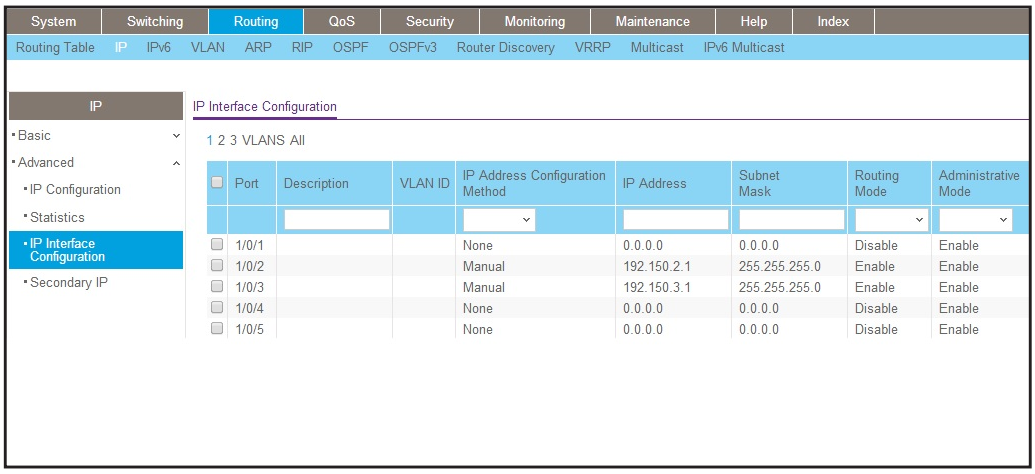
   b. Select the Port **1/0/2** check box.
   c. Under the IP Interface Configuration, configure the following settings:
      - In the **IP Address** field, enter **192.150.2.1**.

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

d. Click the **Apply** button. Your settings are saved.

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

a. Remain on the same page.



b. Select the Port **1/0/3** check box.

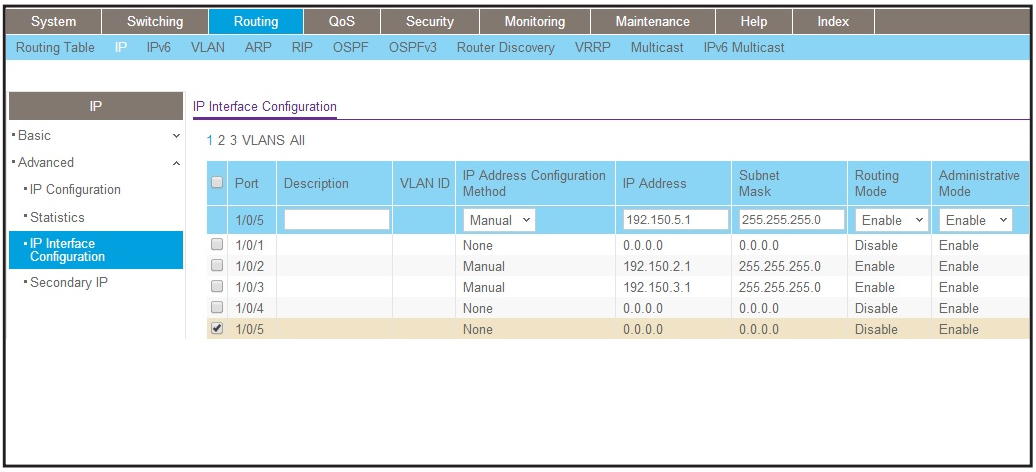
c. Configure the following settings:

- 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 the **Apply** button. Your settings are saved.

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

a. Remain on the same page.



b. Select the Port **1/0/5** check box.

c. Configure the following settings:
- 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 the **Apply** button. Your settings are saved.

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

To use the CLI to add a default route:

```
(Netgear Switch) (Config)#ip route default 10.10.10.2
```

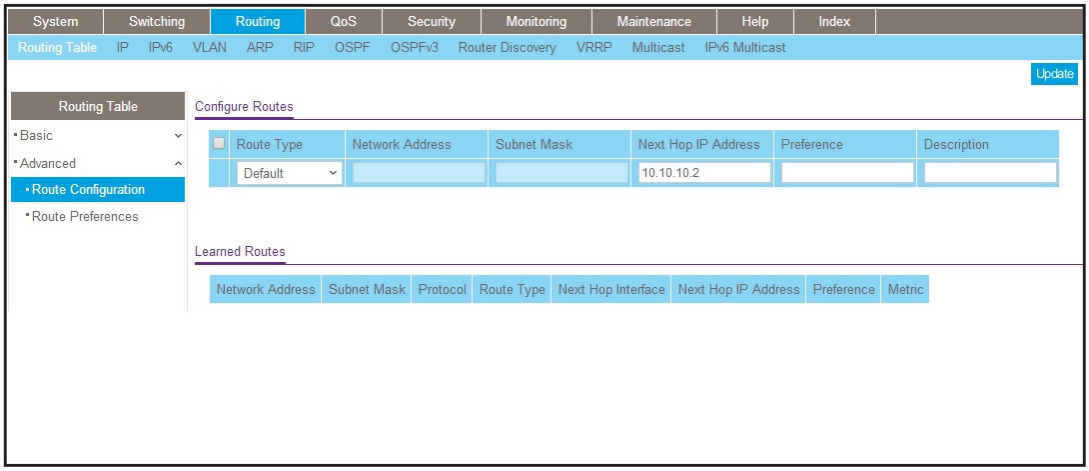
Note: Configure IP subnet 10.10.10.0 using either port routing (Enable routing for ports on the switch on page 90) or VLAN routing (see Set up VLAN routing for VLANs and the switch on page 103).

Main UI: Add a default route

To use the main UI to add a default route:

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

   A page similar to the following figure displays.



2. In the **Route Type** menu, select **Default**.
3. In the **Next Hop Address** field, enter one of the routing interface's IP addresses.

   Note the following:

   - The Network Address and Subnet Mask fields are masked.
   - The Preference field is optional. By default, a value of 1 (which is the highest) is assigned.
4. Click the **Add** button. Your settings are saved.

   The default route entry is created 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 from the default route. The following procedure shows how to add a static route to the switch routing table.

This example shows how to configure a static route to reach the 10.10.20.0/24 network. The next hop IP address is 192.168.1.1. For example, to reach the 10.10.20.123 address, the switch must send packets to IP address 192.168.1.1.

So that the route can be active in the routing table, an IP interface must be active on the switch that shares the same subnet address as the next hop IP address. That means that the

next hop router can be reached over that interface. In this example, interface 1/0/3 is the next hop interface.

CLI: Add a static route

To use the CLI to add a static route:

```
(Netgear Switch)#config
(Netgear Switch)(Config)#ip route 10.10.20.0 255.255.255.0 192.168.1.1
```

The following command assumes that the switch already has a routing interface with a network address of 10.10.20.0, and is configured so that all packets destined for network 10.10.20.123 take the path of the routing port.

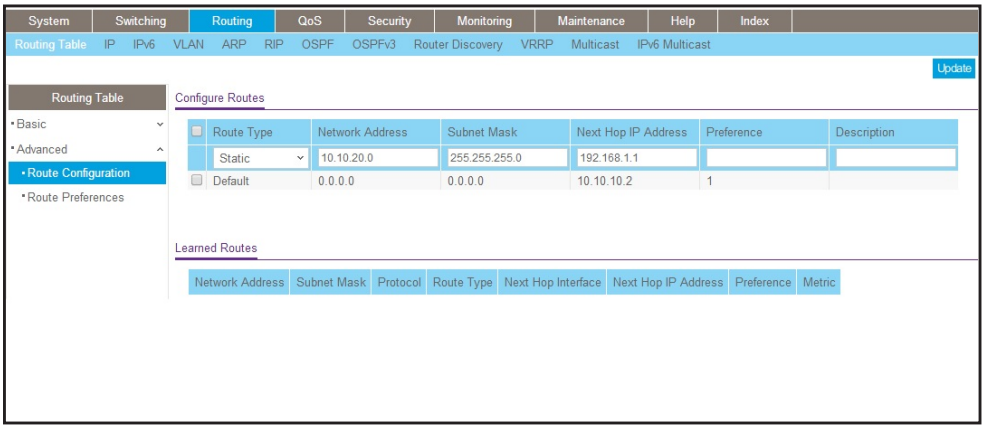
```
(Netgear Switch) #show ip route

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

Network     Subnet                    Next Hop    Next Hop
Address     Mask           Protocol   Intf        IP Address
----------  -------------  --------   ----------  -----------
10.10.20.0  255.255.255.0  Local      1/0/3       192.168.1.1
```

Main UI: Add a static route

To use the main UI to add a static route:

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

   A page similar to the following figure displays.



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

Note that this field must include a network IP address, not a host IP address. The last octet of the IP address must be 0 (zero).

4. In the **Subnet Mask** field, enter a value that matches the subnet range that you want to use.

   The Preference field is optional. By default, a value of 1 (which is the highest) is assigned.

5. Click the **Add** button. Your settings are saved.

   The static route entry is created in the routing table.

5

VLAN Routing

VLAN routing for a VLAN and for the switch

This feature is supported on the M4250 series switches

This feature is supported on the M4300 series switches

This feature is supported on the M4350 series switches

This chapter includes the following sections:

- VLAN routing concepts
- Create two VLANs in preparation for VLAN routing
- Set up VLAN routing for 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 in preparation for VLAN routing

This section provides an example of how to configure the switch to support VLAN routing.

In the CLI, the configuration of the VLAN router port is similar to that of a physical port. The main difference is that, after the VLAN is created, you must use the **`show ip vlan`** command in the CLI 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.

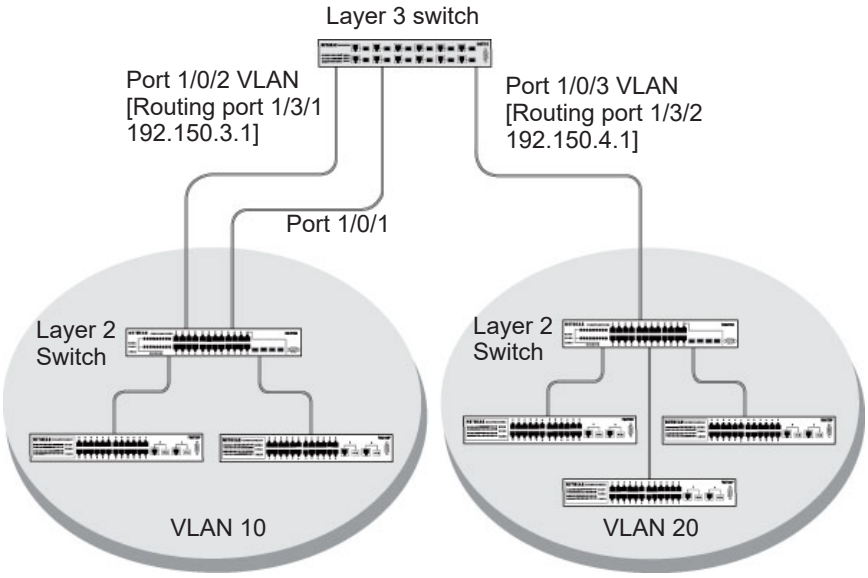


Figure 12. Layer 3 switch configured for port routing

The example is shown as CLI commands and as a main UI procedure.

CLI: Configure two VLANs

To use the CLI to configure two VLANs with egress frame tagging enabled:

1. Create VLAN 10 and VLAN 20.

```
(Netgear Switch) #vlan database
(Netgear Switch) (Vlan)#vlan 10
(Netgear Switch) (Vlan)#vlan 20
(Netgear Switch) (Vlan)#exit
```

2. Add interfaces to VLAN 10 and VLAN 20 and set the PVIDs.

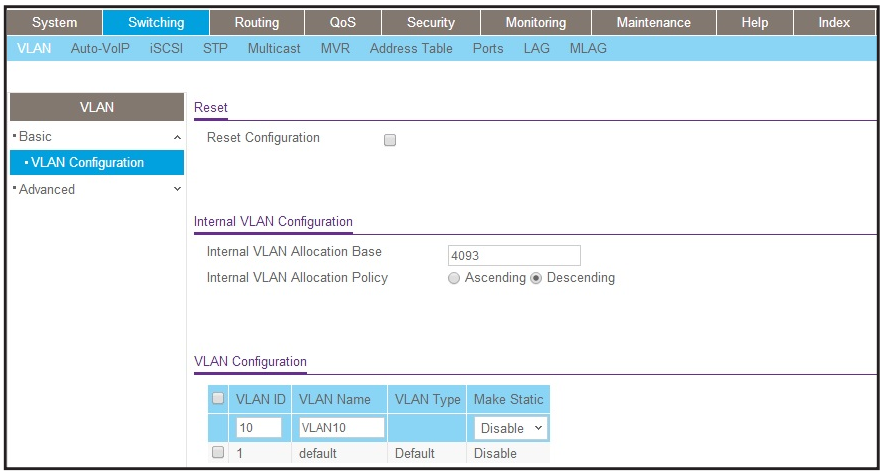
```
(Netgear Switch) #config
(Netgear Switch) (Config)#interface range 1/0/1-1/0/2
(Netgear Switch) (conf-if-range-1/0/1-1/0/2)#vlan participation include 10
(Netgear Switch) (conf-if-range-1/0/1-1/0/2)#vlan pvid 10
(Netgear Switch) (conf-if-range-1/0/1-1/0/2)#exit
(Netgear Switch) (Config)#interface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

Main UI: Configure two VLANs

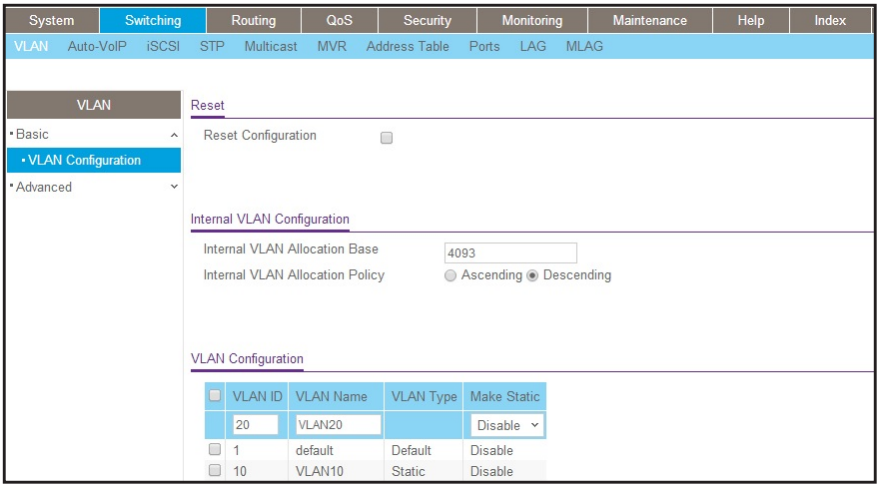
To use the main UI to configure two VLANs with egress frame tagging enabled:

1. Create VLAN 10 and VLAN 20.
   a. Select **Switching > VLAN > Advanced > VLAN Configuration**.

      A page similar to the following figure displays.



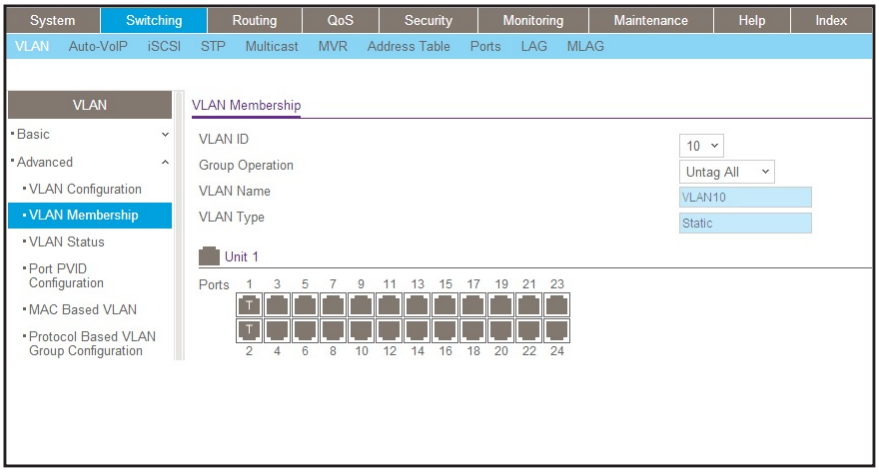
   b. In the **VLAN ID** field, enter **10**.
   c. In the **VLAN Name** field, enter **VLAN10**.
   d. In the **VLAN Type** menu, select **Static**.
   e. Click the **Add** button. Your settings are saved.
   f. Remain on the same page.



   g. In the **VLAN ID** field, enter **20**.
   h. In the **VLAN Name** field, enter **VLAN20**.
   i. In the **VLAN Type** menu, select **Static**.
   j. Click the **Add** button. Your settings are saved.

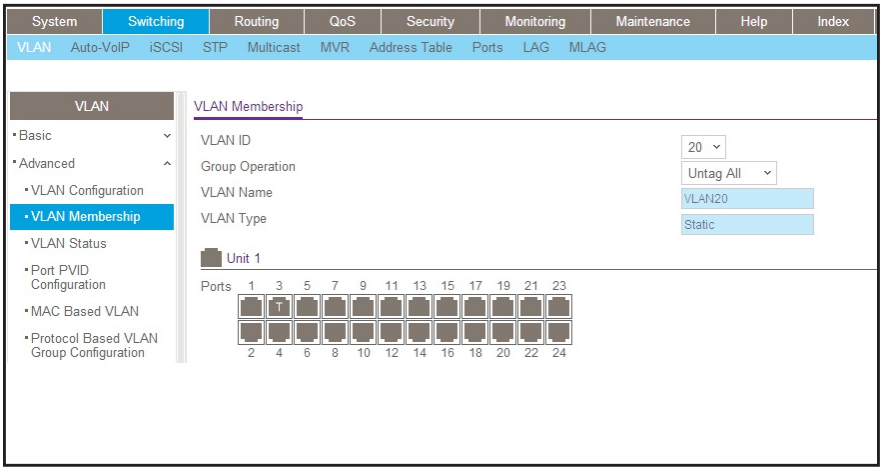
2. Add interfaces to VLAN 10 and VLAN 20.
   a. Select **Switching > VLAN > Advanced > VLAN Membership**.

      A page similar to the following figure displays.



   b. In the **VLAN ID** field, select **10**.
   c. Click the gray boxes under ports **1** and **2** until T displays, which specifies that the egress packets are tagged for the ports.

      If your switch is a member of a stack, be sure that you select the ports in the correct unit.
   d. Click the **Apply** button. Your settings are saved.
   e. Remain on the same page.

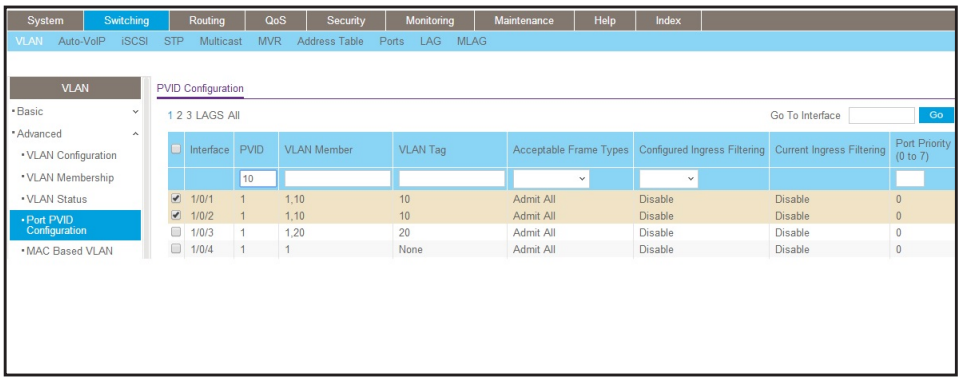


   f. In the **VLAN ID** menu, select **20**.
   g. Click the gray box under port **3**, until T displays, which specifies that the egress packets are tagged for the ports.

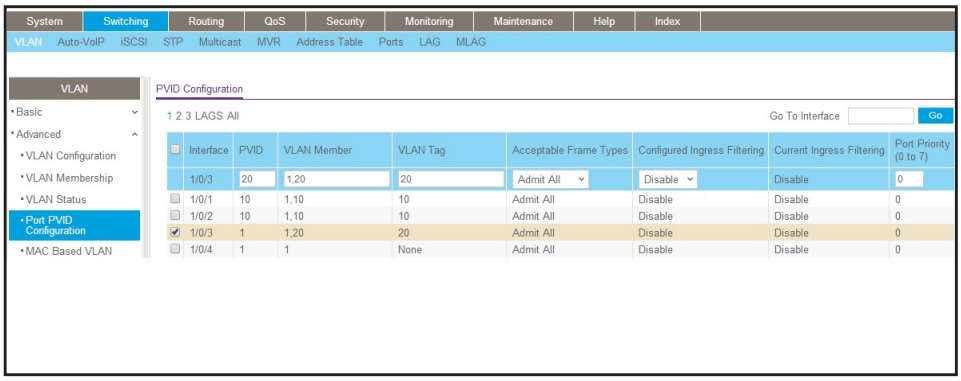
      If your switch is a member of a stack, be sure that you select the port in the correct unit.
   h. Click the **Apply** button. Your settings are saved.

3. Assign PVID 10 to interfaces 1/0/1 and 1/0/2 and PVID 20 to interface 1/0/3.
   a. Select **Switching > VLAN > Advanced > Port PVID Configuration**.

      A page similar to the following figure displays.



   b. Select the Interface **1/0/1** and **1/0/2** check boxes.
   c. In the **PVID** field, enter **10**.
   d. Click the **Apply** button. Your settings are saved.
   e. Remain on the same page.



   f. Select the Interface **1/0/3** check box.
   g. In the **PVID** field, enter **20**.
   h. Click the **Apply** button. Your settings are saved.

Set up VLAN routing for VLANs and the switch

The example is shown as CLI commands and as a main UI procedure.

CLI: Set up VLAN routing for the VLANs and the switch

To use the CLI to 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 database
(Netgear Switch) (Vlan)#vlan routing 10
(Netgear Switch) (Vlan)#vlan routing 20
(Netgear Switch) (Vlan)#exit
```

   This allows logical interface IDs to be used instead of the slot/port (M4250 series switch) or unit/slot/port (M4300 or M4350 series switch) designation in subsequent routing commands. Assume that VLAN 10 is assigned to ID 3/1, and VLAN 20 is assigned ID 3/2.

2. Enable routing globally for the switch.

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

3. Configure IP addresses and subnet masks for the virtual router ports.

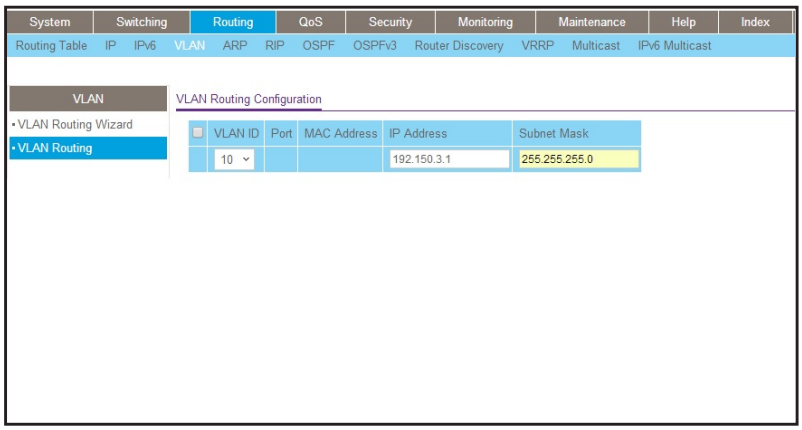
```
(Netgear Switch) (Config)#interface vlan 10
(Netgear Switch) (Interface-vlan 10)#ip address 192.150.3.1 255.255.255.0
(Netgear Switch) (Interface-vlan 10)#exit
(Netgear Switch) (Config)#interface vlan 20
(Netgear Switch) (Interface-vlan 20)#ip address 192.150.4.1 255.255.255.0
(Netgear Switch) (Interface-vlan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

Main UI: Set up VLAN routing for the VLANs and the switch

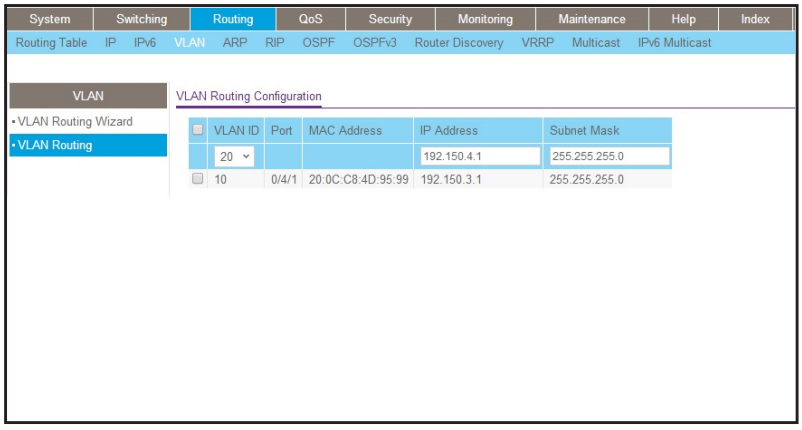
To use the main UI to set up VLAN routing for the VLANs and the switch:

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

   A page similar to the following figure displays.



2. Configure the following settings:
   - In the **VLAN ID** menu, select **10**.
   - In the **IP Address** field, enter **192.150.3.1**.
   - In the **Subnet Mask** field, enter **255.255.255.0**.
3. Click the **Add** button. Your settings are saved.
4. Remain on the sane page.



5. Configure the following settings:
   - Select **20** in the **VLAN ID** field.
   - In the **IP Address** field, enter **192.150.4.1**.
   - In the **Subnet Mask** field, enter **255.255.255.0**.
6. Click the **Add** button. Your settings are saved.

6

RIP

Routing Information Protocol

This feature is supported on the M4250 series switches

This feature is supported on the M4300 series switches

This feature is supported on the M4350 series switches

This chapter includes the following sections:

- Routing Information Protocol concepts
- Enable routing for the switch in preparation of RIP
- Enable routing for ports in preparation of RIP
- Enable RIP on the switch
- Enable RIP for ports
- 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 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.

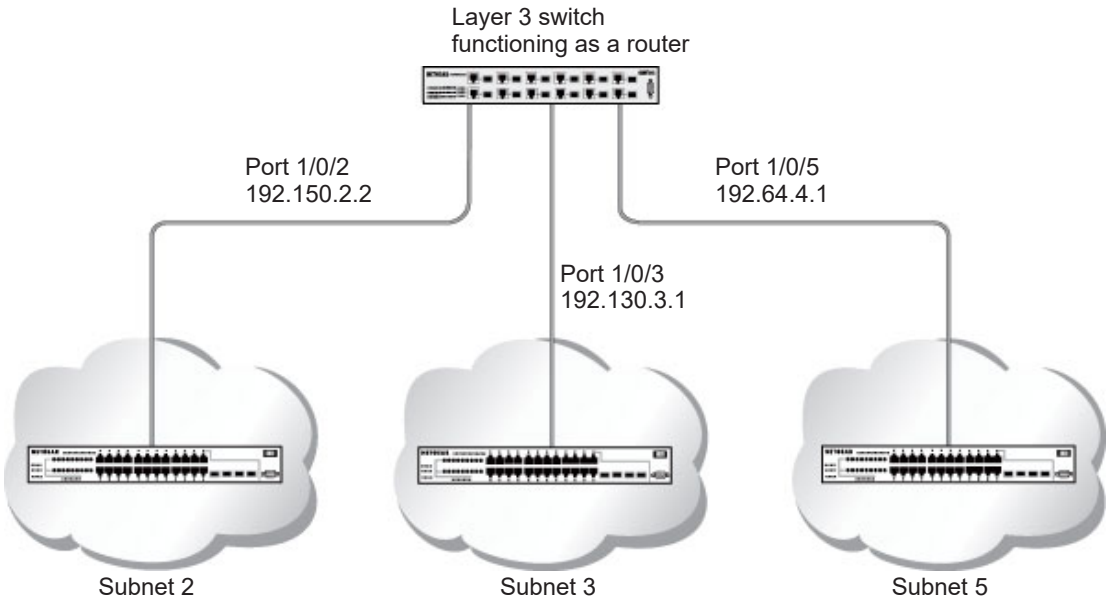


Figure 13. Network with RIP on ports 1/0/2 and 1/0/3

Enable routing for the switch in preparation of RIP

The example is shown as CLI commands and as a main UI procedure.

CLI: Enable routing for the switch

To use the CLI to enable routing for the switch:

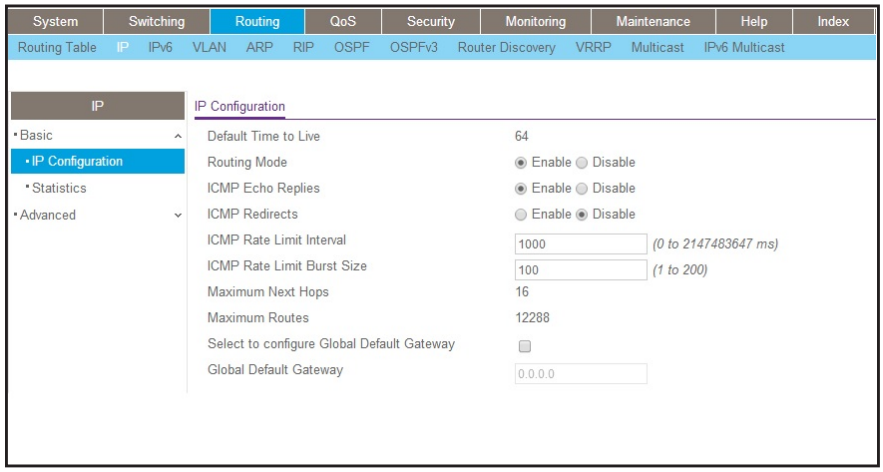
```
(Netgear Switch) #config
(Netgear Switch) (Config)#ip routing
(Netgear Switch) (Config)#exit
```

Main UI: Enable routing for the switch

To use the main UI CLI to enable routing for the switch:

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

   A page similar to the following figure displays.



2. Select the Routing Mode **Enable** radio button.
3. Click the **Apply** button. Your settings are saved.

Enable routing for ports in preparation of RIP

The example is shown as CLI commands and as a main UI procedure.

CLI: Enable routing and assign IP addresses to ports

To use the CLI to enable routing and assign IP addresses to ports 1/0/2 and 1/0/3:

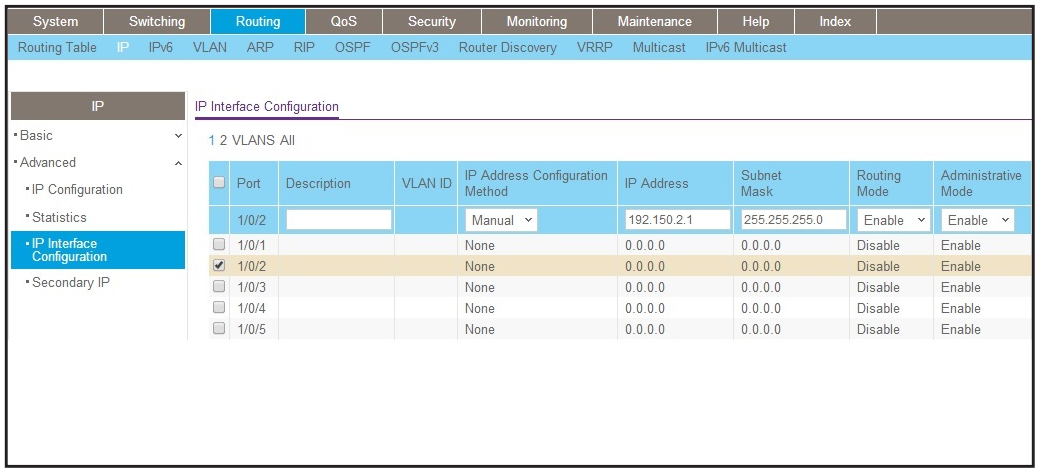
```
(Netgear Switch) #config
(Netgear Switch) (Config)#interface 1/0/2
(Netgear Switch) (Interface 1/0/2)#routing
(Netgear Switch) (Interface 1/0/2)#ip address 192.150.2.1 255.255.255.0
(Netgear Switch) (Interface 1/0/2)#exit
(Netgear Switch) (Config)#interface 1/0/3
(Netgear Switch) (Interface 1/0/3)#routing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

Main UI: Enable routing and assign IP addresses to ports

To use the main UI to enable routing and assign IP addresses to ports 1/0/2 and 1/0/3:

1. Assign IP address 192.150.2.1 with subnet mask 255.255.255.0 to interface 1/0/2.
   a. Select **Routing > Advanced > IP Interface Configuration**.

   A page similar to the following figure displays.



b. Select the Port **1/0/2** check box.

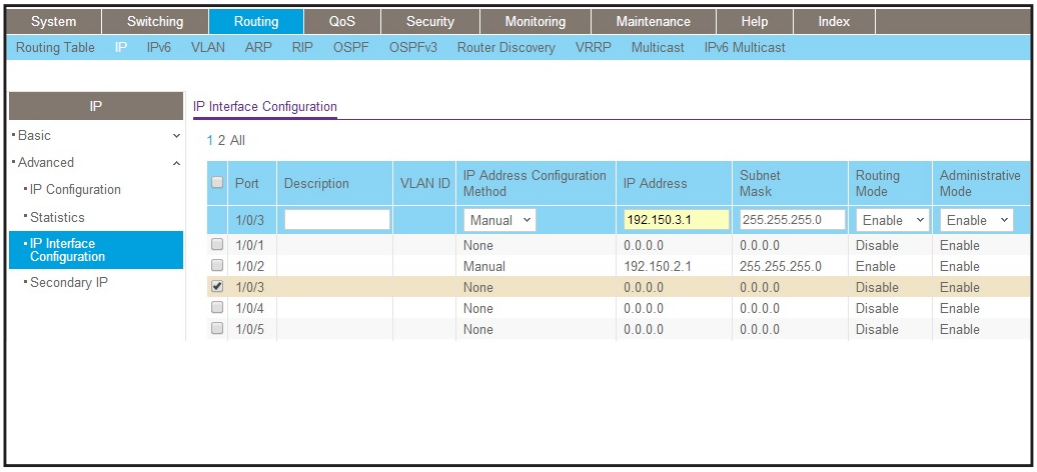
c. Configure the following settings:

- In the **IP Address Configuration Method** menu, 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** menu, select **Enable**.

d. Click the **Apply** button. Your settings are saved.

2. Assign IP address 192.150.3.1 with subnet mask 255.255.255.0 to interface 1/0/3.

a. Remain on the same page.



b. Select the Port **1/0/3** check box.

c. Configure the following settings:

- In the **IP Address Configuration Method** menu, 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** menu, select **Enable**.

d. Click the **Apply** button. Your settings are saved.

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

To use the CLI to enable RIP on the switch (the default route preference is 15):

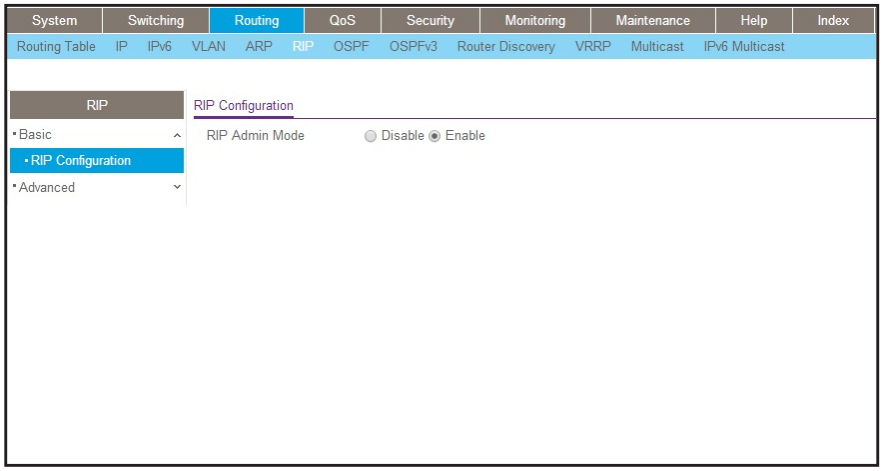
```
(Netgear Switch) #config
(Netgear Switch) (Config)#router rip
(Netgear Switch) (Config router)#enable
(Netgear Switch) (Config router)#exit
(Netgear Switch) (Config)#exit
```

Main UI: Enable RIP on the switch

To use the main UI to enable RIP on the switch (the default route preference is 15):

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

   A page similar to the following figure displays.



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

Enable RIP for ports

The example is shown as CLI commands and as a main UI procedure.

Note: In the example, authentication defaults to none, and no default route entry is created. The commands specify that both ports can receive both RIPv1 and RIPv2 frames, but can send only RIPv2-formatted frames.

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

To use the CLI to enable RIP for ports 1/0/2 and 1/0/3:

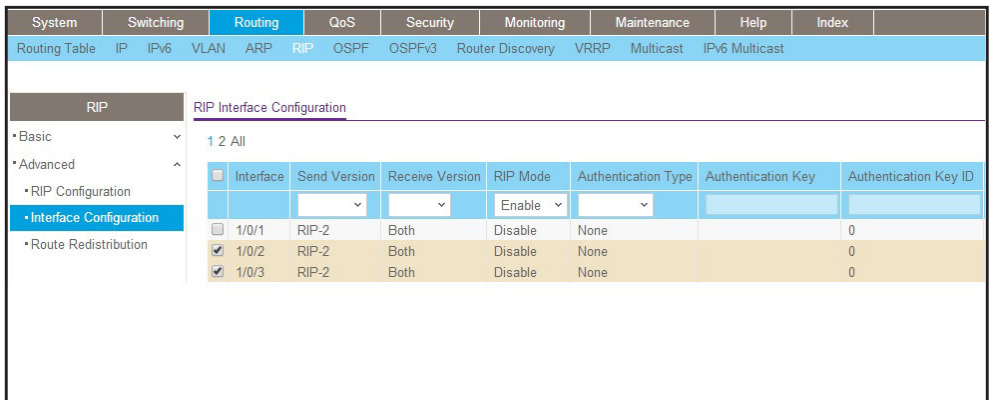
```
(Netgear Switch) #config
(Netgear Switch) (Config)#interface 1/0/2
(Netgear Switch) (Interface 1/0/2)#ip rip
(Netgear Switch) (Interface 1/0/2)#ip rip receive version both
(Netgear Switch) (Interface 1/0/2)#ip rip send version rip2
(Netgear Switch) (Interface 1/0/2)#exit
(Netgear Switch) (Config)#interface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

Main UI: Enable RIP for ports 1/0/2 and 1/0/3

To use the main UI to enable RIP for ports 1/0/2 and 1/0/3:

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

   A page similar to the following figure displays.



2. Select the Interface **1/0/2 and 1/0/3** check boxes.
3. In the **Send Version** menu, select **RIP-2**.
4. In the **Receive Version** menu, select **Both**.
5. In the **RIP Mode** menu, select **Enable**.
6. Click the **Apply** button. Your settings are saved.

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.

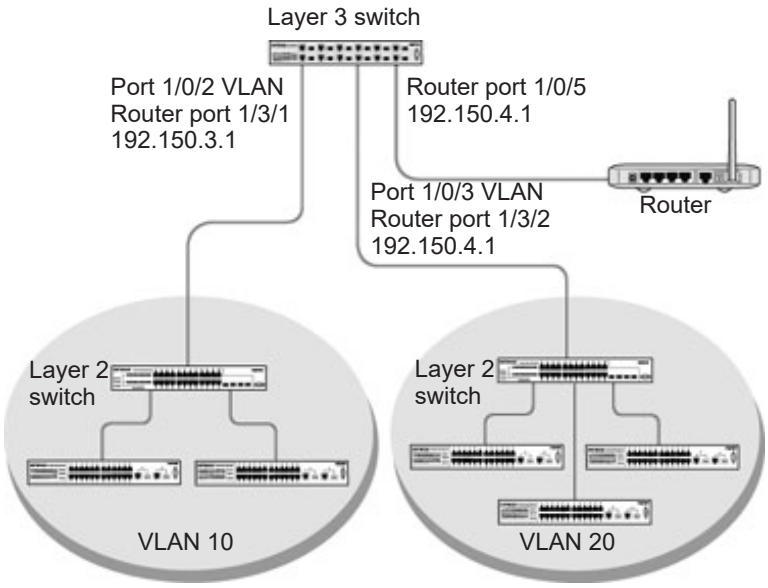


Figure 14. VLAN routing RIP configuration example

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

To use the CLI to configure VLAN routing with RIP support on the switch:

1. Configure routing VLAN 10 and routing VLAN 20 and add interfaces to the routing VLANs.

```
(Netgear Switch) #vlan database
(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) (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 non-virtual 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.

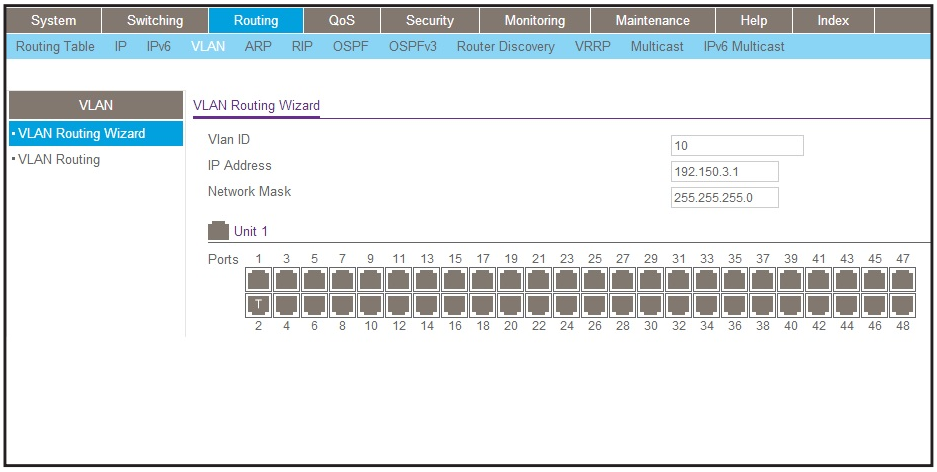
```
(Netgear Switch) (Config)#interface vlan 10
(Netgear Switch) (Interface vlan 10)#ip rip
(Netgear Switch) (Interface vlan 10)#exit
(Netgear Switch) (Config)#interface vlan 20
(Netgear Switch) (Interface vlan 20)#ip rip
(Netgear Switch) (Interface vlan 20)#exit
(Netgear Switch) (Config)#exit
```

Main UI: Configure VLAN Routing with RIP support

To use the main UI to configure VLAN routing with RIP support on the switch:

1. Configure routing VLAN 10 and include port 1/0/2 in the VLAN:
   a. Select **Routing > VLAN > VLAN Routing Wizard**.

      A page similar to the following figure displays.



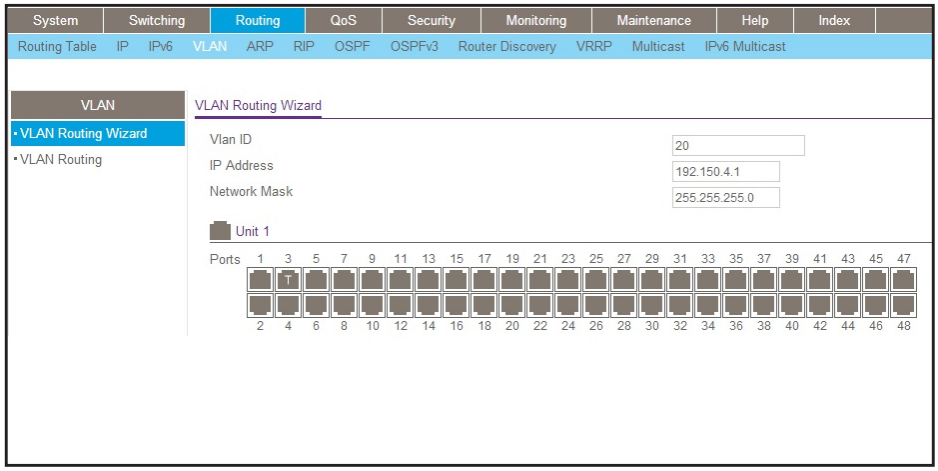
   b. Configure the following settings:
      - In the **VLAN ID** field, enter **10**.
      - In the **IP Address** field, enter **192.150.3.1**.
      - In the **Network Mask** field, enter **255.255.255.0**.

   c. Click the gray box under port **2**, until T displays, which specifies that the egress packets are tagged for the port.

      If your switch is a member of a stack, be sure that you select the port in the correct unit.

   d. Click the **Apply** button. Your settings are saved.

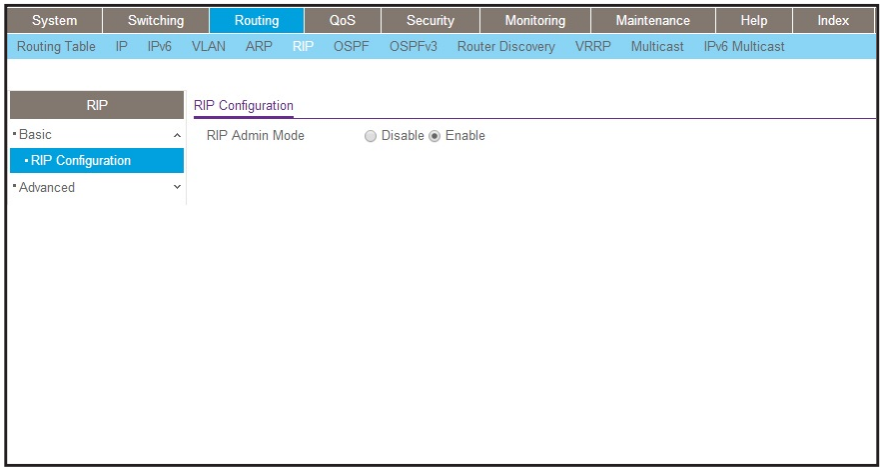
2. Configure routing VLAN 20 and include port 1/0/3 in the VLAN:
   a. Remain on the same page.



   b. Configure the following settings:
      - 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 the gray box under port **3**, until T displays, which specifies that the egress packets are tagged for the port.

      If your switch is a member of a stack, be sure that you select the port in the correct unit.
   d. Click the **Apply** button. Your settings are saved.
3. Enable RIP on the switch (you can skip this step because RIP is enabled by default).
   a. Select **Routing > RIP > Basic > RIP Configuration**.

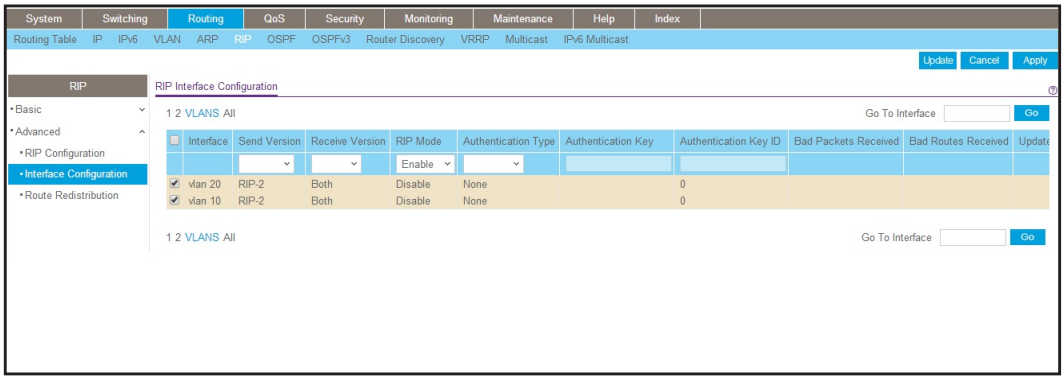
      A page similar to the following figure displays.



   b. Select the RIP Admin Mode **Enable** radio button.
   c. Click **Apply** to save the setting.

4. Enable RIP on VLANs 10 and 20.
   a. Select **Routing > RIP > Advanced > Interface Configuration**.

      A page similar to the following figure displays.



   b. Click **VLANS** at the top of table.
   c. Select the Interface **vlan 10** and **vlan 20** check boxes.
   d. In the RIP Mode menu, select **Enable**.
   e. Click the **Apply** button. Your settings are saved.

7

OSPF

Open Shortest Path First

This feature is supported on the M4300 series switches

This feature is supported on the M4350 series switches

This chapter includes the following sections:

- Open Shortest Path First concepts
- Inter-area router
- OSPF on a switch that functions as a border router
- Stub areas
- NSSA areas
- VLAN routing with OSPF
- OSPFv3

Note: The Open Shortest Path First (OSPF) feature is supported on the M4300 series and M4350 series switches only. The M4250 series switches do not support OSPF.

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 occurs.
  - Only the part of the table that changes is sent.
  - Updates are sent to a multicast address, 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**. This area is used when a source and destination address are in the same area.
- **Inter-area routing**. This area is used across an OSPF backbone when a source and destination address are not in the same area. An inter-area router communicates with border routers in each of the areas to which it provides connectivity.

A switch that operates as a router and runs OSPF determines the best route using the assigned cost and the type of the OSPF route. If more than one type of route exists, the order for selecting a route 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 that are 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.

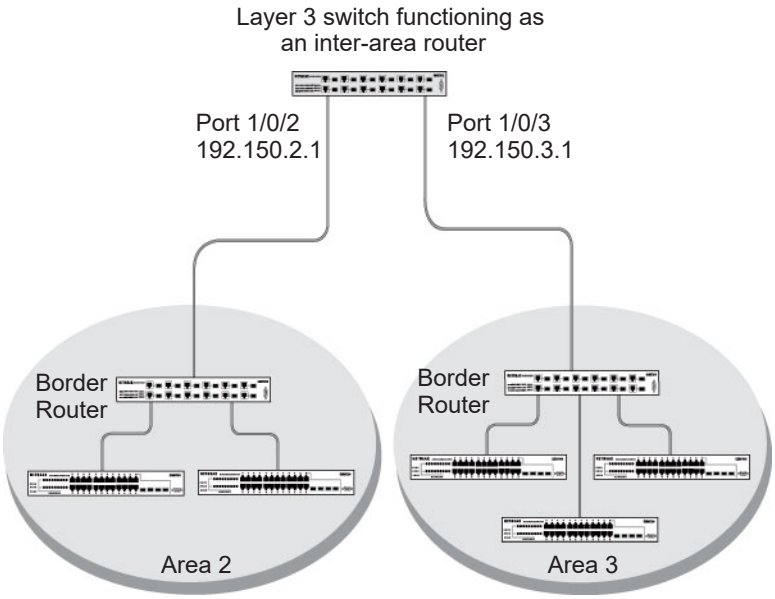


Figure 15. Network segment with an inter-area router connecting areas 0.0.0.2 and 0.0.0.3

CLI: Configure an inter-area router

To use the CLI to 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.

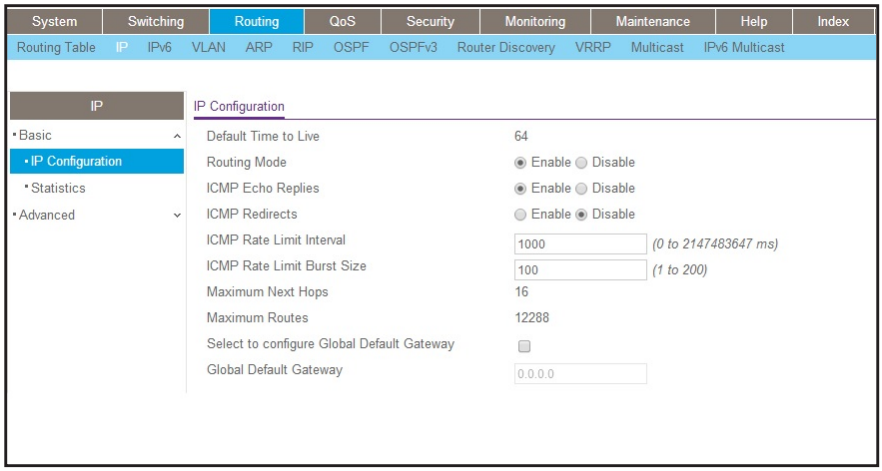
```
(Netgear Switch) #config
(Netgear Switch) (Config)#interface 1/0/2
(Netgear Switch) (Interface 1/0/2)#ip ospf
(Netgear Switch) (Interface 1/0/2)#ip ospf areaid 0.0.0.2
(Netgear Switch) (Interface 1/0/2)#ip ospf priority 128
(Netgear Switch) (Interface 1/0/2)#ip ospf cost 32
(Netgear Switch) (Interface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

Main UI: Configure an inter-area router

To use the main UI to configure an inter-area router:

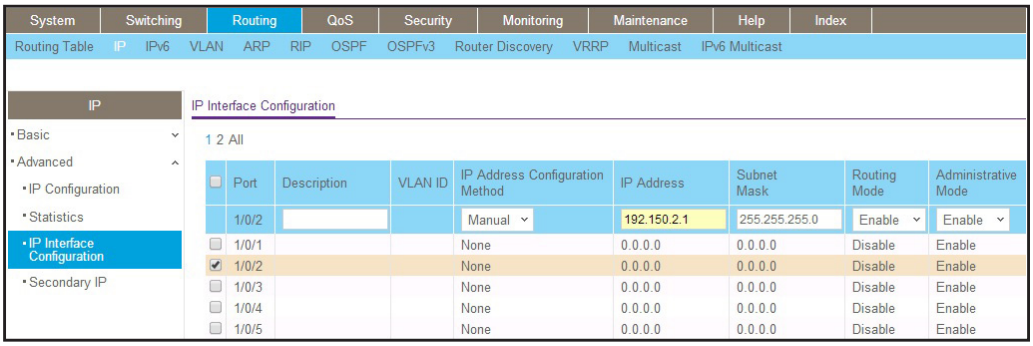
1. Enable IP routing on the switch.
   a. Select **Routing > IP > Basic > IP Configuration**.

      A page similar to the following figure displays.



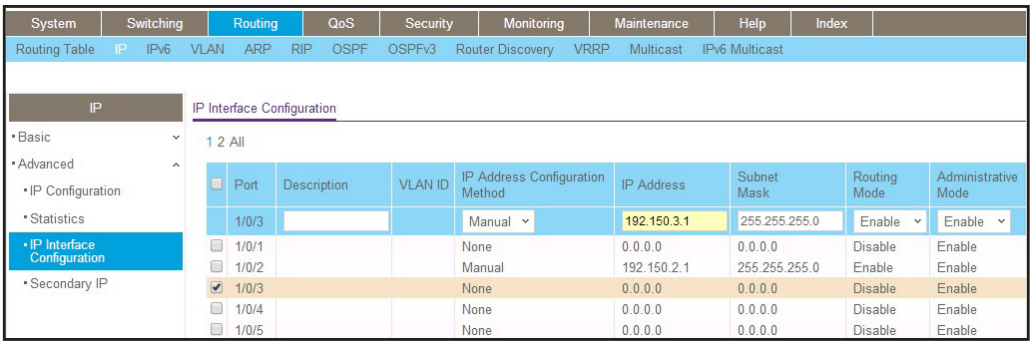
   b. Select the Routing Mode **Enable** radio button.
   c. Click the **Apply** button. Your settings are saved.
2. Assign IP address 192.150.2.1 to port 1/0/2.
   a. Select **Routing > IP > Advanced > IP Interface Configuration**.

      A page similar to the following figure displays.



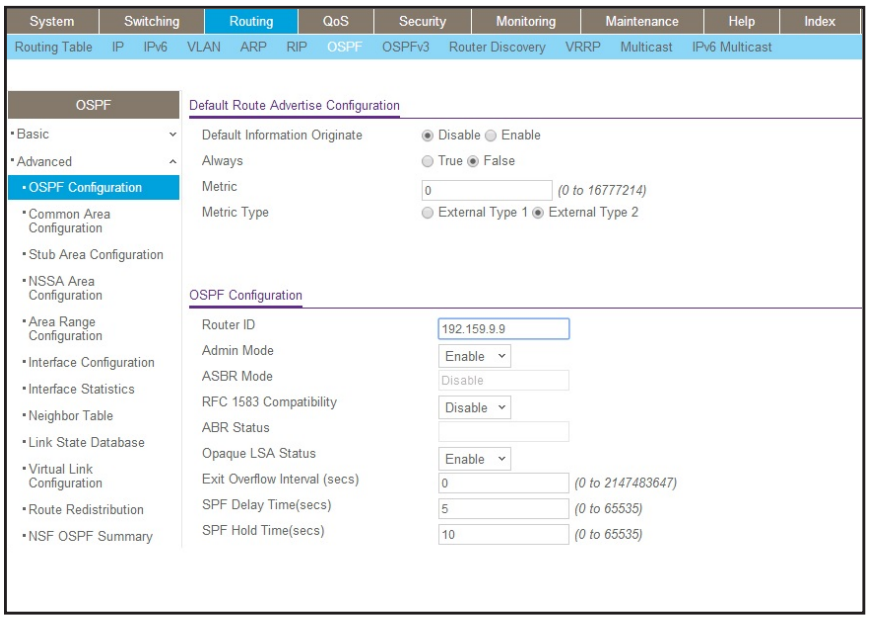
   b. Select the Port **1/0/2** check box.
   c. Configure the following settings:
      - In the **IP Address** field, enter **192.150.2.1**.
      - In the **Subnet Mask** field, enter **255.255.255.0**.
      - In the **Administrative Mode** menu, select **Enable**.
   d. Click the **Apply** button. Your settings are saved.

3. Assign IP address 192.150.3.1 to port 1/0/3:
   a. Remain on the same page.



   b. Select the Port **1/0/3** check box.
   c. Configure the following settings:
      - In the **IP Address** field, enter **192.150.3.1**.
      - In the **Subnet Mask** field, enter **255.255.255.0**.
      - In the **Administrative Mode** menu, select **Enable**.
   d. Click the **Apply** button. Your settings are saved.
4. Specify the router ID, and enable OSPF for the switch.
   a. Select **Routing > OSPF > Advanced > OSPF Configuration**.

      A page similar to the following figure displays.



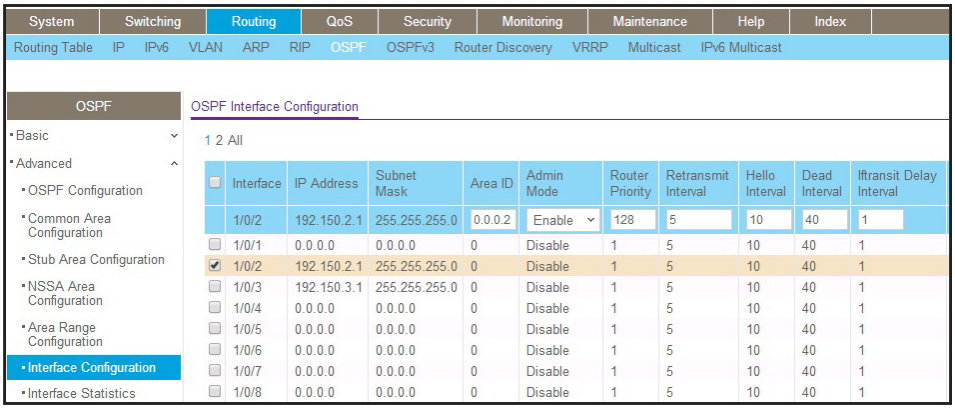
   b. Under OSPF Configuration, configure the following settings:
      - In the **Router ID** field, enter **192.150.9.9**.
      - In the **Admin Mode** menu, select **Enable**.
      - In the **RFC 1583 Compatibility** menu, select **Disable**.

c. Click the **Apply** button. Your settings are saved.

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

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

A page similar to the following figure displays.



b. Select the Interface **1/0/2** check box.

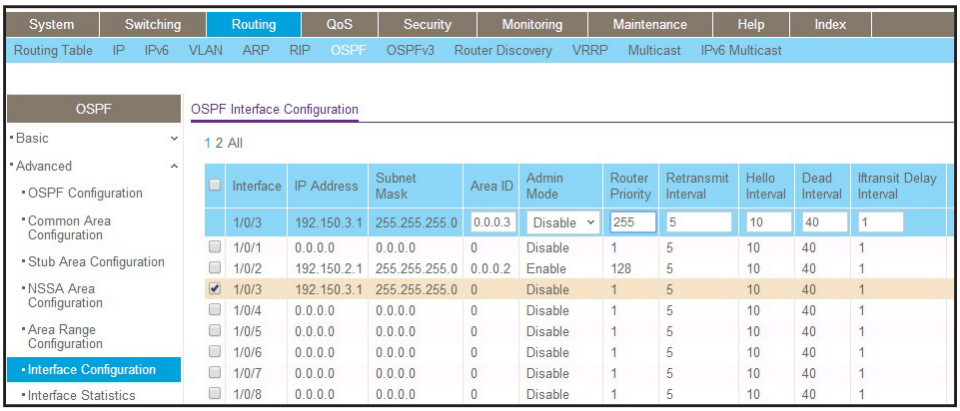
c. Configure the following settings:

- In the **Area ID** field, enter **0.0.0.2**.
- In the **Admin Mode** menu, select **Enable**.
- In the **Router Priority** field, enter **128**.
- In the **Metric Cost** field, enter **32**. (This field is not shown in the previous figure.)

d. Click the **Apply** button. Your settings are saved.

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

a. Remain on the same page.



b. Select the Interface **1/0/3** check box.

c. Configure the following settings:

- In the **Area ID** field, enter **0.0.0.3**.
- In the **Admin Mode** menu, select **Enable**.
- In the **Router Priority** field, enter **255**.

- In the **Metric Cost** field, enter **64**. (This field is not shown in the previous figure.)

d. Click the **Apply** button. Your settings are saved.

OSPF on a switch that functions as a border router

The example is shown as CLI commands and as a main UI procedure. For an OSPF sample network, see Figure 15 on page 120.

CLI: Configure OSPF on a switch that functions as a border router

To use the CLI to configure OSPF on a switch that functions as a border router:

1. Enable routing for the switch.

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

2. Enable routing and assign IP addresses to 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, enable OSPF for the switch, and 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.

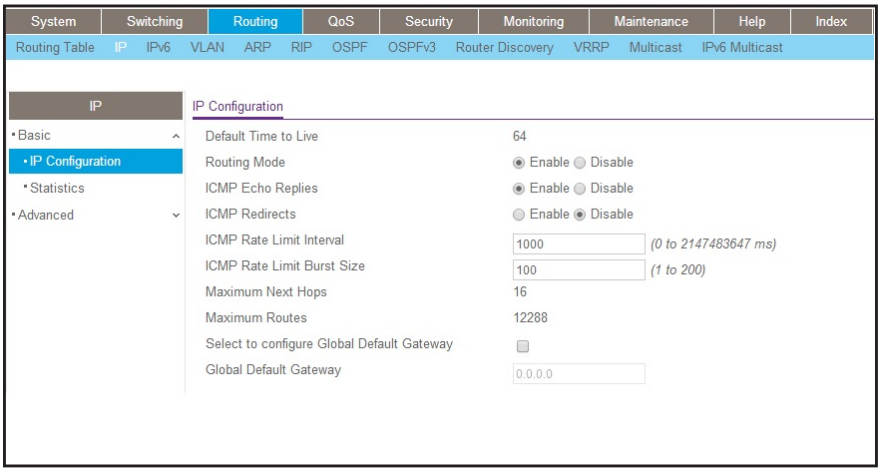
```
(Netgear Switch) #config
(Netgear Switch) (Config)#interface 1/0/2
(Netgear Switch) (Interface 1/0/2)#ip ospf
(Netgear Switch) (Interface 1/0/2)#ip ospf areaid 0.0.0.2
(Netgear Switch) (Interface 1/0/2)#ip ospf priority 128
(Netgear Switch) (Interface 1/0/2)#ip ospf cost 32
(Netgear Switch) (Interface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

Main UI: Configure OSPF on a switch that functions as a border router

To use the main UI to configure OSPF on a switch that functions as a border router:

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

      A page similar to the following figure displays.

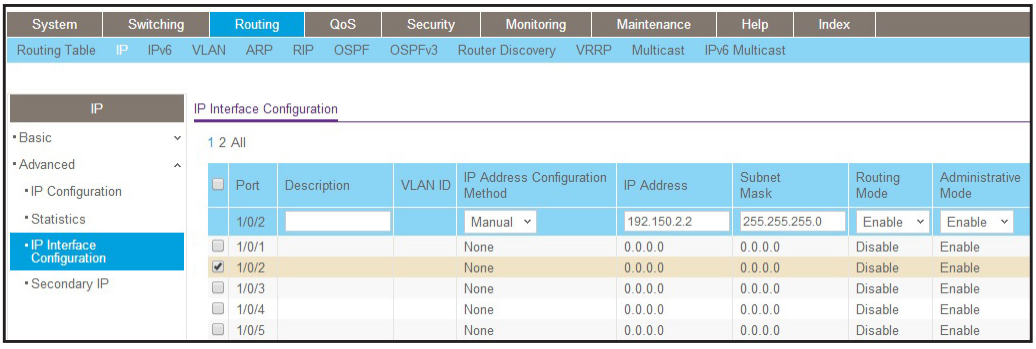


   b. Select the Routing Mode **Enable** radio button.

   c. Click the **Apply** button. Your settings are saved.

2. Assign IP address 192.150.2.2 to port 1/0/2.
   a. Select **Routing > IP > Advanced > IP Interface Configuration**.

      A page similar to the following figure displays.



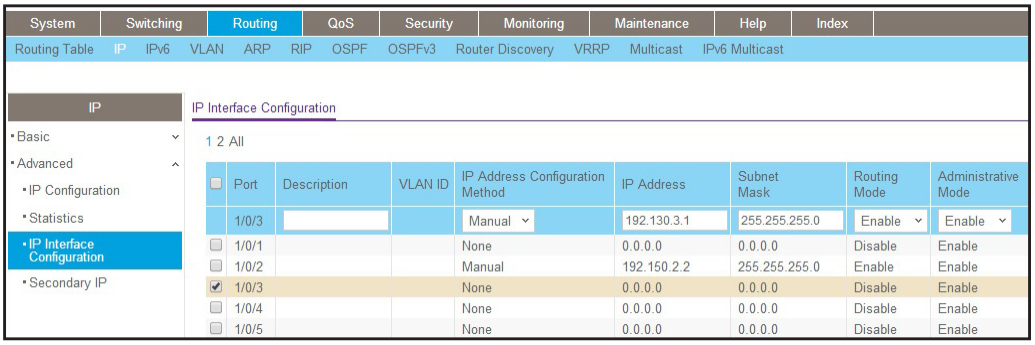
   b. Select the Port **1/0/2** check box.

   c. Configure the following settings:
      - In the **IP Address Configuration Method** menu, select **Manual**.
      - In the **IP Address** field, enter **192.150.2.2**.
      - In the **Subnet Mask** field, enter **255.255.255.0**.
      - In the **Admin Mode** menu, select **Enable**.

d. Click the **Apply** button. Your settings are saved.

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

a. Remain on the same page.



b. Select the Port **1/0/3** check box.

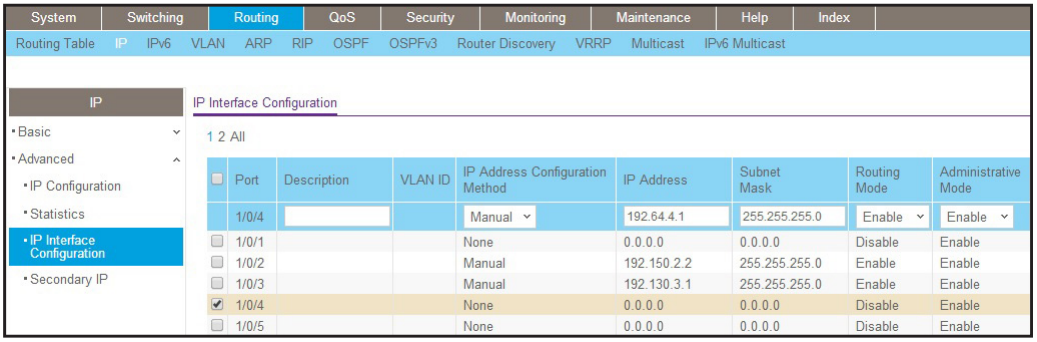
c. Configure the following settings:

- In the **IP Address Configuration Method** menu, select **Manual**.
- In the **IP Address** field, enter **192.130.3.1**.
- In the **Subnet Mask** field, enter **255.255.255.0**.
- In the **Administrative Mode** menu, select **Enable**.

d. Click the **Apply** button. Your settings are saved.

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

a. Remain on the same page.



b. Select the Port **1/0/4** check box.

c. Configure the following settings:

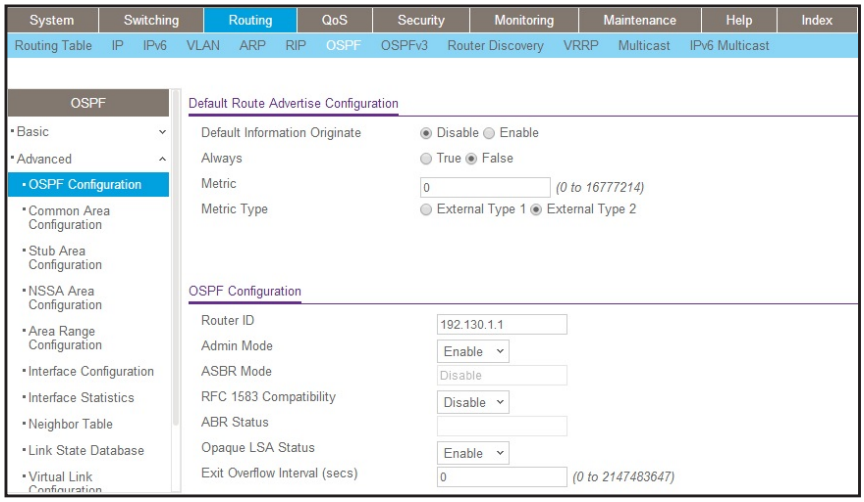
- In the **IP Address Configuration Method** menu, select **Manual**.
- In the **IP Address** field, enter **192.64.4.1**.
- In the **Subnet Mask** field, enter **255.255.255.0**.
- In the **Admin Mode** menu, select **Enable**.

d. Click the **Apply** button. Your settings are saved.

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

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

A page similar to the following figure displays.



b. Under OSPF Configuration, configure the following settings:

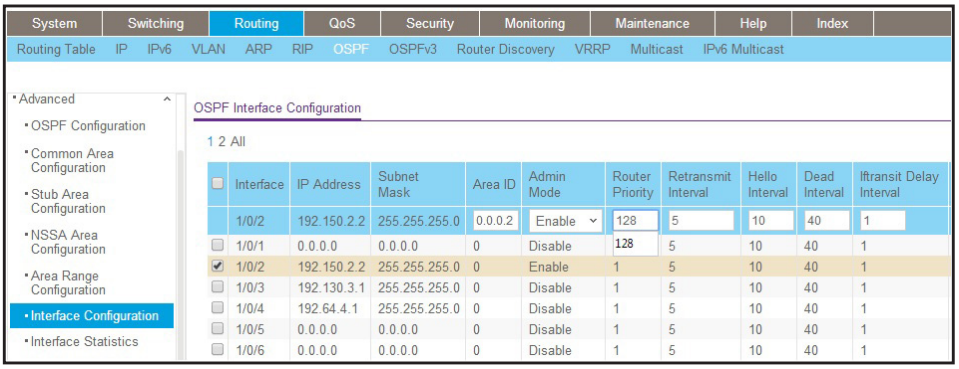
- In the **Router ID** field, enter **192.130.1.1**.
- In the **Admin Mode** menu, select **Enable**.
- In the **RFC 1583 Compatibility** menu, select **Disable**.

c. Click the **Apply** button. Your settings are saved.

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

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

A page similar to the following figure displays.



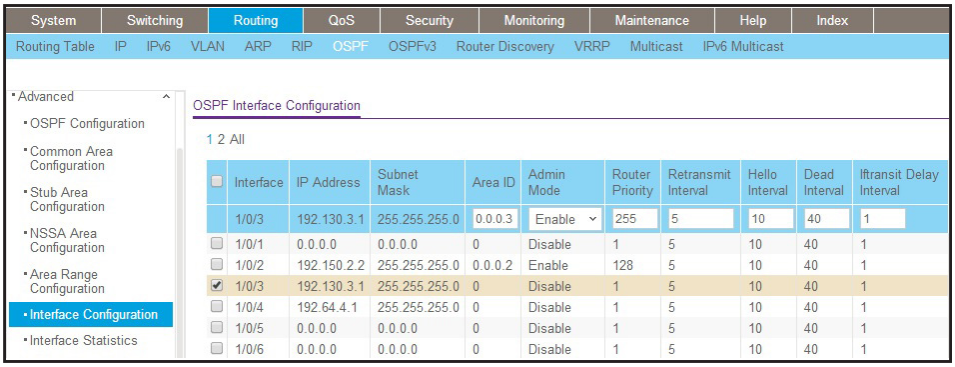
b. Select the Interface **1/0/2** check box.

c. Configure the following settings:

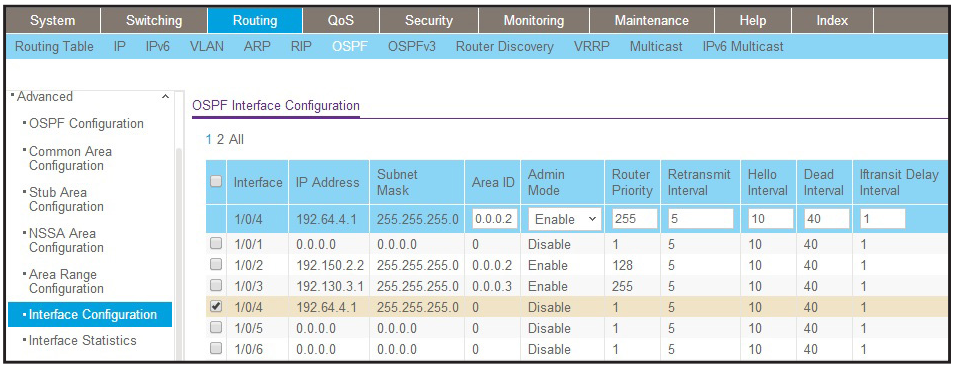
- In the **Area ID** field, enter **0.0.0.2**.
- In the **Admin Mode** menu, select **Enable**.
- In the **Router Priority** field, enter **128**.
- In the **Metric Cost** field, enter **32**. (This field is not shown in the previous figure.)

d. Click the **Apply** button. Your settings are saved.

7. Enable OSPF on port 1/0/3.
   a. Remain on the same page.



   b. Select the Interface **1/0/3** check box.
   c. Configure the following settings:
      - In the **Area ID** field, enter **0.0.0.3**.
      - In the **Admin Mode** menu, select **Enable**.
      - In the **Router Priority** field, enter **255**.
      - In the **Metric Cost** field, enter **64**. (This field is not shown in the previous figure.)
   d. Click the **Apply** button. Your settings are saved.
8. Enable OSPF on port 1/0/4.
   a. Remain on the same page.



   b. Select the Interface **1/0/4** check box.
   c. Configure the following settings:
      - In the **Area ID** field, enter **0.0.0.2**.
      - In the **Admin Mode** menu, select the **Enable**.
      - In the **Router Priority** field, enter **255**.
      - In the **Metric Cost** field, enter **64**. (This field is not shown in the previous figure.)
   d. Click the **Apply** button. Your settings are saved.

Stub areas

The purpose of an NSSA OSPF area is to allow the redistribution f external routes (from other routing protocols) into OSPF. This example shows how to inject external routes coming from RIP (running on port 1/0/11) into OSPF.

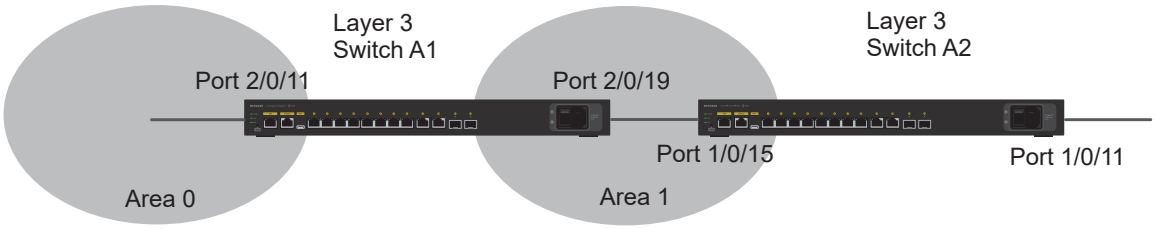


Figure 16. Area 1 is a stub area

The example is shown as CLI commands and as a main UI procedure.

CLI: Configure Area 1 as a stub area on Switch A1

To use the CLI to configure Area 1 as a stub area on Switch 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. Configure Switch A1 to inject 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 interface 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 interface 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
```

7. Display the OSPF neighbor interface configuration and the IP route configuration.

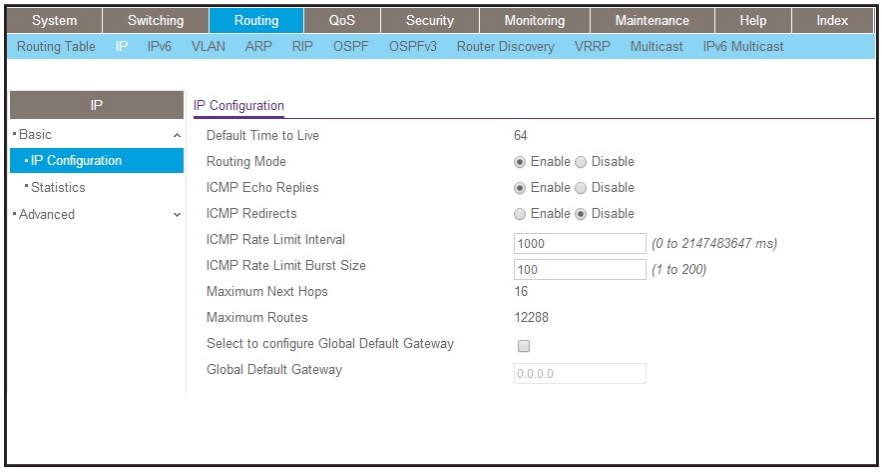
```
(Netgear Switch) #show ip ospf neighbor interface all
  Router ID        IP Address    Neighbor Interface    State
---------------   -----------   -------------------   ---------
4.4.4.4           192.168.10.2       2/0/11           Full
2.2.2.2           192.168.20.2       2/0/19           Full

(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
```

Main UI: Configure Area 1 as a stub area on Switch A1

To use the main UI to configure Area 1 as a stub area on Switch A1:

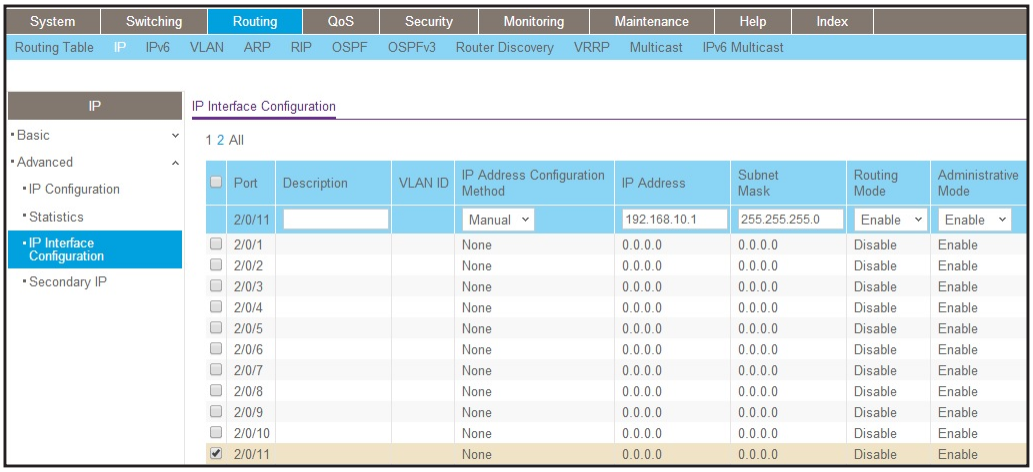
1. Enable IP routing on the switch.
   a. Select **Routing > IP > Basic > IP Configuration**.

      A page similar to the following figure displays.



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

      A page similar to the following figure displays.



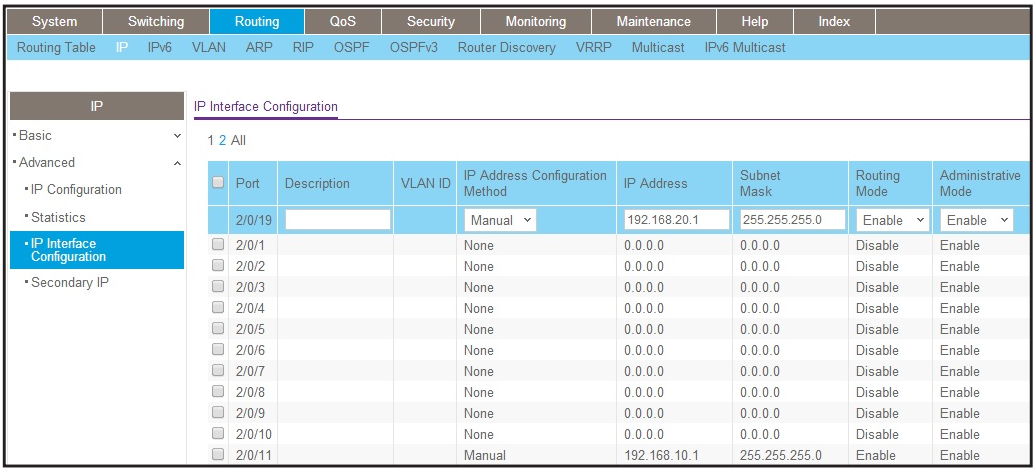
   b. Select the Port **2/0/11** check box.
   c. Configure the following settings:
      - In the **IP Address Configuration Method** menu, select **Manual**.
      - In the **IP Address** field, enter **192.168.10.1**.

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

d. Click the **Apply** button. Your settings are saved.

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

a. Remain on the same page.



b. Select the Port **2/0/19** check box.

c. Configure the following settings:

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

d. Click the **Apply** button. Your settings are saved.

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

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

A page similar to the following figure displays.

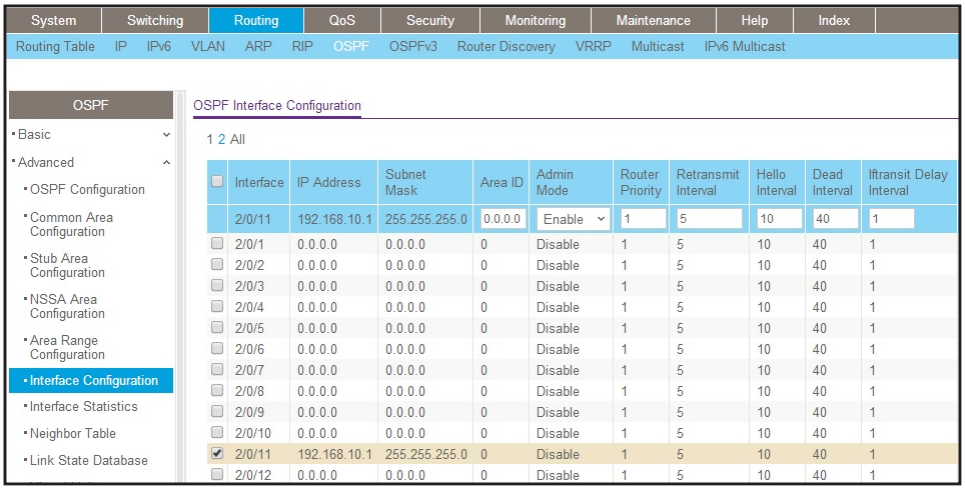
b. Under OSPF Configuration, in the **Router ID** field, enter **1.1.1.1**.

c. Click the **Apply** button. Your settings are saved.

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

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

A page similar to the following figure displays.



b. Select the Interface **2/0/11** check box.

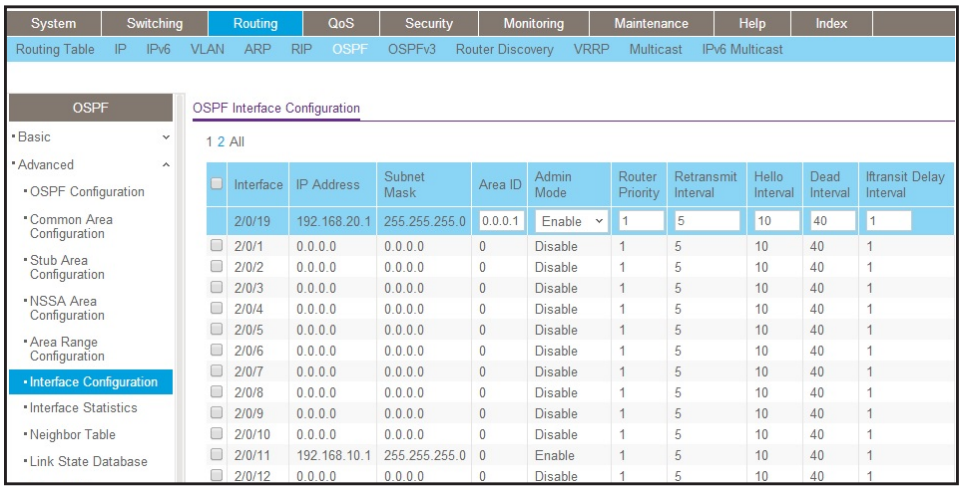
c. In the **Area ID** field, enter **0.0.0.0**.

d. In the **Admin Mode** menu, select **Enable**.

e. Click the **Apply** button. Your settings are saved.

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

a. Remain on the same page.



b. Select the Interface **2/0/19** check box.

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

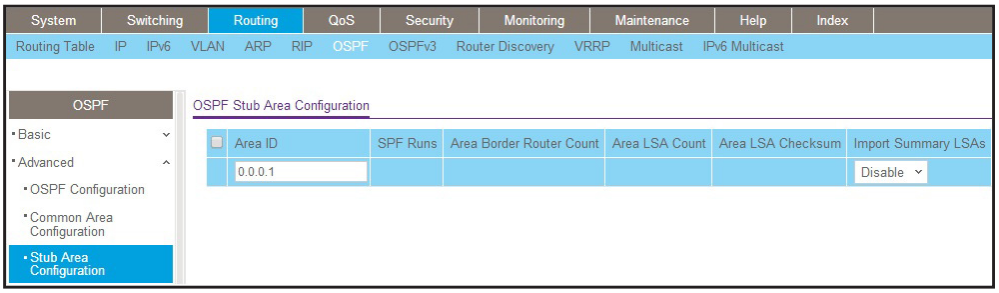
d. In the **Admin Mode** menu, select **Enable**.

e. Click the **Apply** button. Your settings are saved.

7. Configure area 0.0.0.1 as a stub area.

a. Remain on the same page.

A page similar to the following figure displays.



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

c. In the **Import Summary LSAs** menu, select **Disable**.

d. Click the **Add** button. Your settings are saved.

CLI: Configure Area 1 as a stub area on Switch A2

To use the CLI to configure Area 1 as a stub area on Switch 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 interface 1/0/15 and display the IP routes.

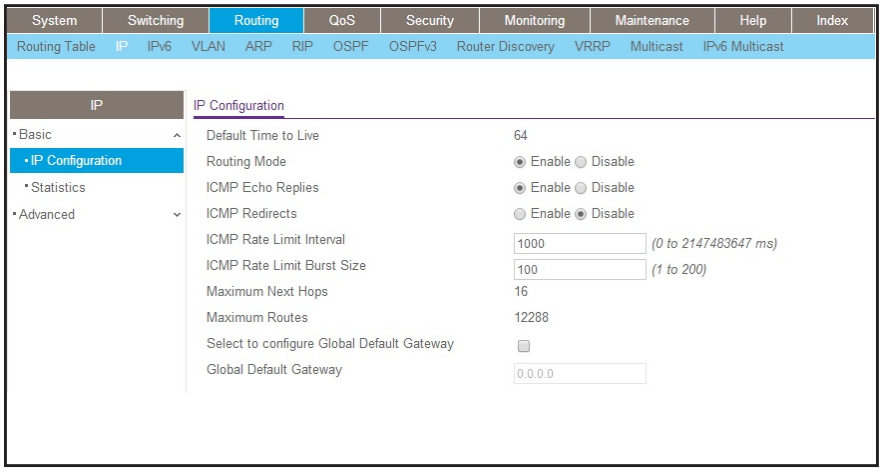
```
(Netgear Switch)  (Config-router)#exit
(Netgear Switch)  (Config)#interface 1/0/15
(Netgear Switch)  (Interface 1/0/15)#routing
(Netgear Switch)  (Interface 1/0/15)#ip address 192.168.20.2  255.255.255.0
(Netgear Switch)  (Interface 1/0/15)#ip ospf
(Netgear Switch)  (Interface 1/0/15)#ip ospf areaid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

Main UI: Configure Area 1 as a stub area on Switch A2

To use the CLI to configure Area 1 as a stub area on Switch A2:

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

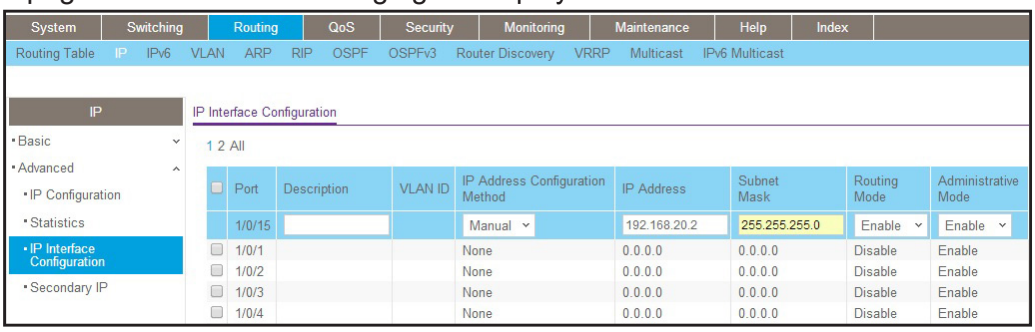
      A page similar to the following figure displays.



   b. Select the Routing Mode **Enable** radio button.
   c. Click the **Apply** button. Your settings are saved.

2. Assign IP address 192.168.20.2 to port 1/0/15.
   a. Select **Routing > IP > Advanced > IP Interface Configuration**.

      A page similar to the following figure displays.

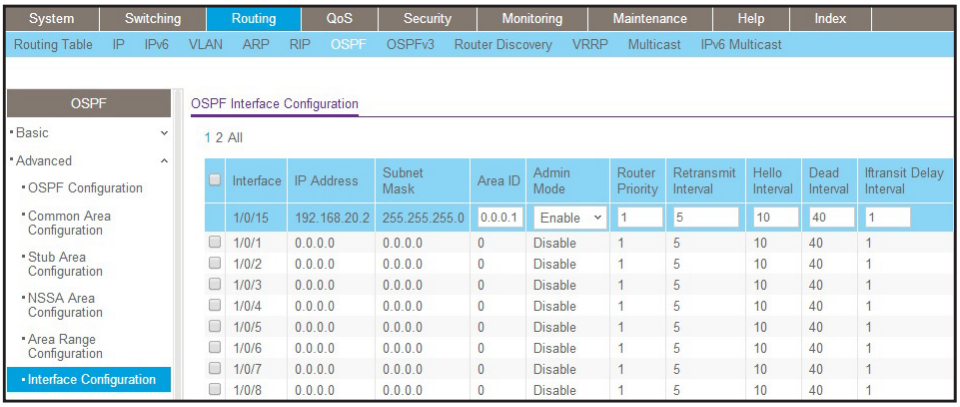


   b. Select the Port **1/0/15** check box.
   c. Configure the following settings:
      - In the **IP Address Configuration Method** menu, select **Manual**.
      - In the **IP Address** field, enter **192.168.20.2**.
      - In the **Subnet Mask** field, enter **255.255.255.0**.
      - In the **Admin Mode** field, select **Enable**.
   d. Click the **Apply** button. Your settings are saved.
3. Specify the router ID, and enable OSPF for the switch.
   a. Select **Routing > OSPF > Basic > OSPF Configuration**.

      A page similar to the following figure displays.

   b. In the **Router ID** field, enter **2.2.2.2**.
   c. Click the **Apply** button. Your settings are saved.
4. Enable OSPF on port 1/0/15.
   a. Select **Routing > OSPF > Advanced > Interface Configuration**.

A page similar to the following figure displays.



b. Select the Interface **1/0/15** check box.

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

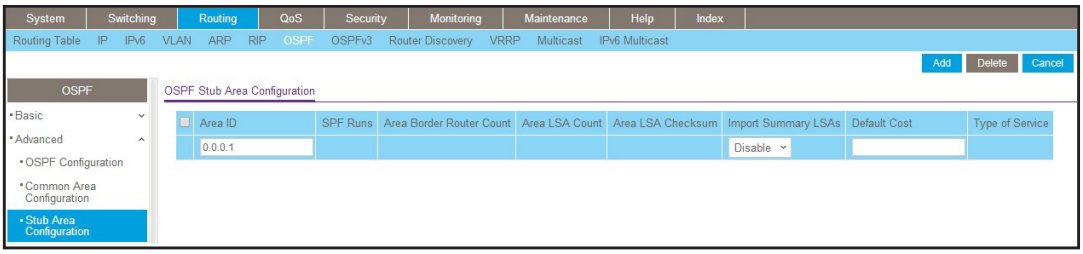
d. In the **Admin Mode** menu, select **Enable**.

e. Click the **Apply** button. Your settings are saved.

5. Configure area 0.0.0.1 as a stub area.

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

A page similar to the following figure displays.



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

c. Click the **Add** button. Your settings are saved.

NSSA areas

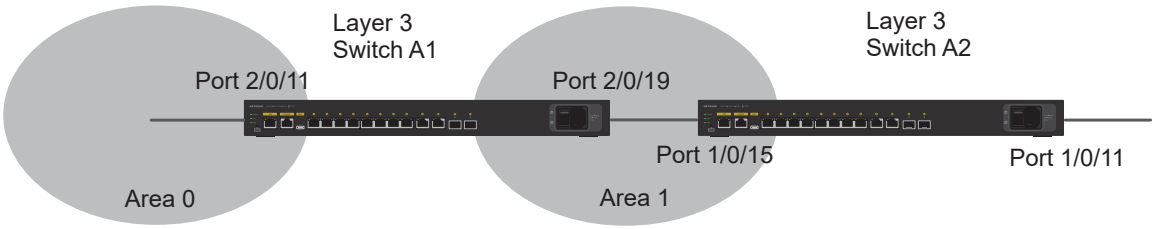


Figure 17. NSSA area

The example is shown as CLI commands and as a main UI procedure.

CLI: Configure Area 1 as an NSSA area on Switch A1

To use the CLI to configure Area 1 as an NSSA area on Switch A1:

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
```

5. Display the IP routes.

```
(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
```

Main UI: Configure Area 1 as an NSSA area on Switch A1

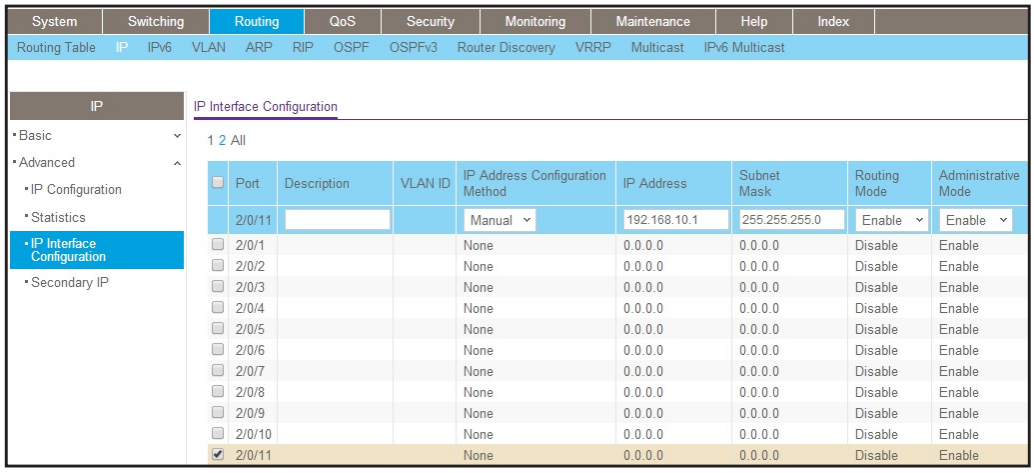
To use the main UI to configure Area 1 as an NSSA area on Switch A1:

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

      A page similar to the following figure displays.

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

      A page similar to the following figure displays.



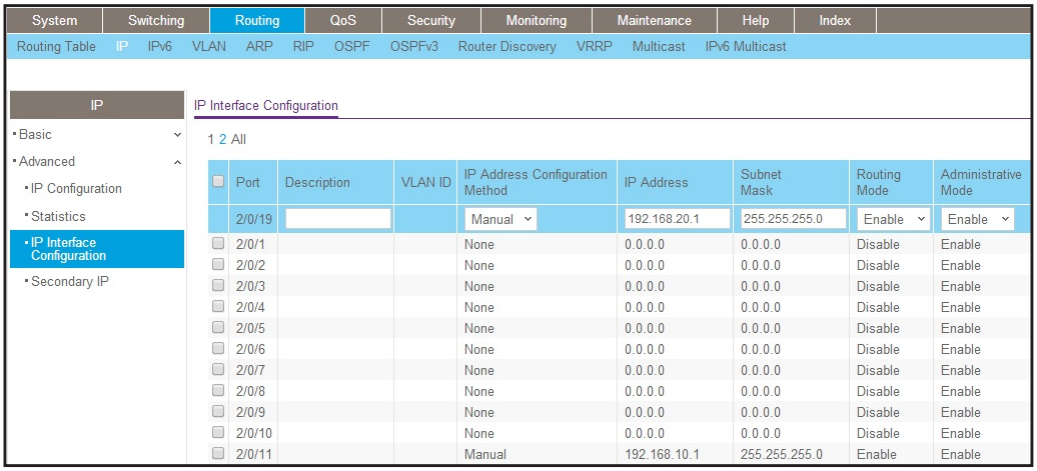
   b. Select the Port **2/0/11** check box.
   c. Configure the following settings:
      - In the **IP Address** field, enter **192.168.10.1**.
      - In the **Subnet Mask** field, enter **255.255.255.0**.

- In the **Admin Mode** menu, select **Enable**.

d. Click the **Apply** button. Your settings are saved.

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

a. Remain on the same page.



b. Select the Port **2/0/19** check box.

c. Configure the following settings:

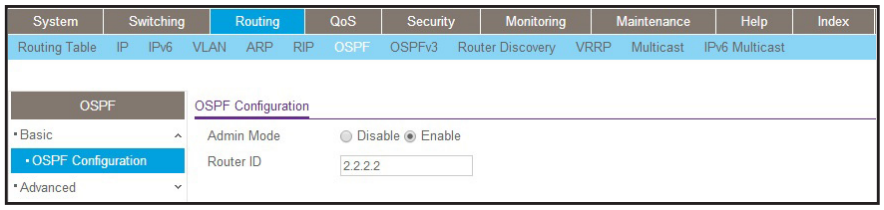
- In the **IP Address** field, enter **192.168.20.1**.
- In the **Subnet Mask** field, enter **255.255.255.0**.
- In the **Admin Mode** menu, select **Enable**.

d. Click the **Apply** button. Your settings are saved.

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

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

A page similar to the following figure displays.



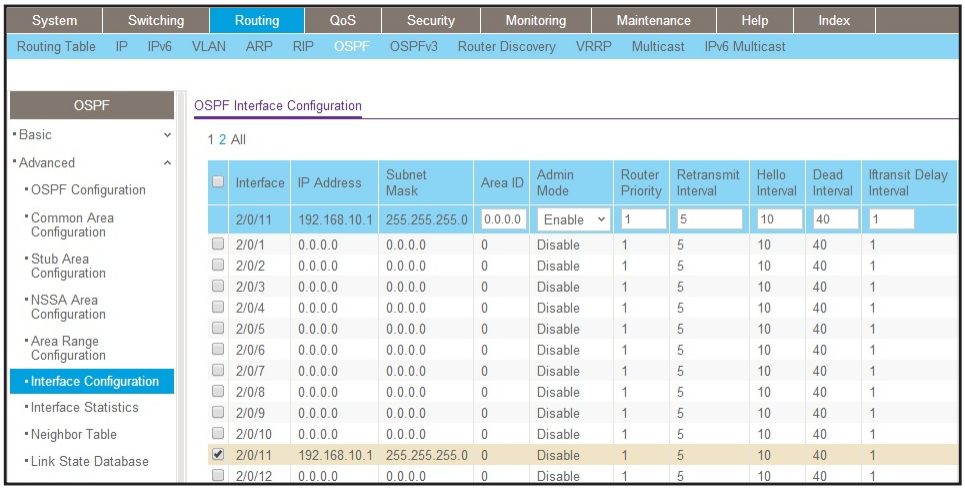
b. In the **Router ID** field, enter **2.2.2.2**.

c. Click the **Apply** button. Your settings are saved.

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

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

A page similar to the following figure displays.



b. Select the Interface **2/0/11** check box.

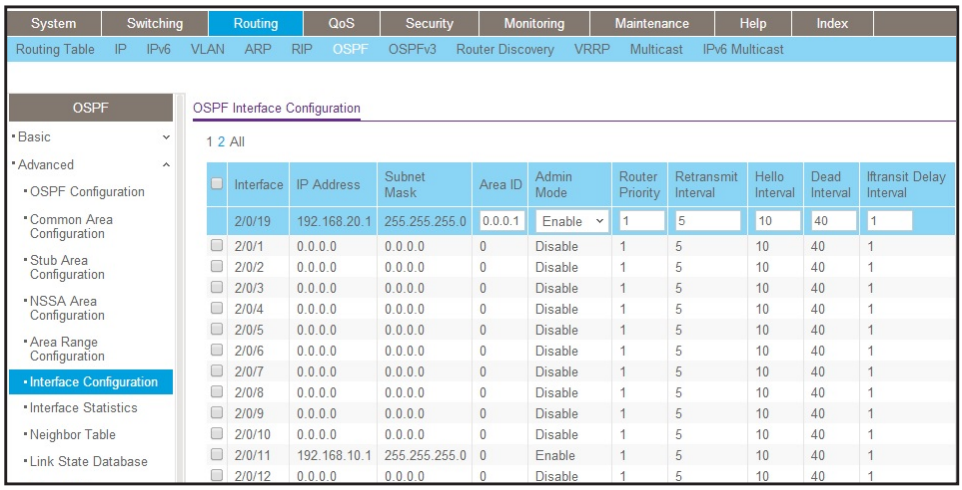
c. In the **Area ID** field, enter **0.0.0.0**.

d. In the **Admin Mode** menu, select **Enable**.

e. Click the **Apply** button. Your settings are saved.

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

a. Remain on the same page.



b. Select the Interface **2/0/19** check box.

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

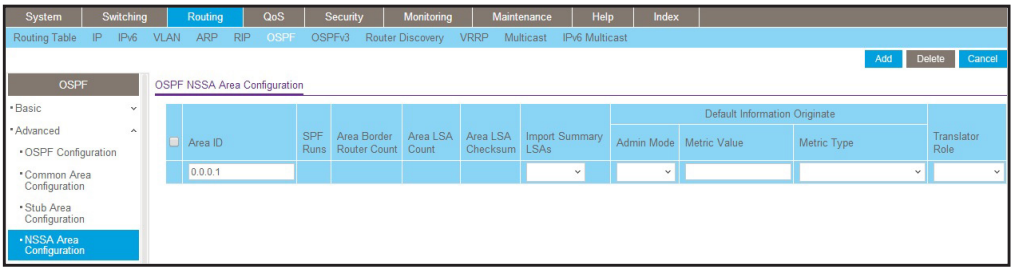
d. In the **Admin Mode** menu, select **Enable**.

e. Click the **Apply** button. Your settings are saved.

7. Configure area 0.0.0.1 as an NSSA area.

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

A page similar to the following figure displays.



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

c. In the **Import Summary LSA's** menu, select **Disable**.

d. Click the **Add** button. Your settings are saved.

CLI: Configure Area 1 as an NSSA area on Switch A2

To use the CLI to configure Area 1 as an NSSA area on Switch 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
(Netgear Switch) (Config-router)#exit
```

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

```
(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
```

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

```
(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
```

7. Display the IP routes.

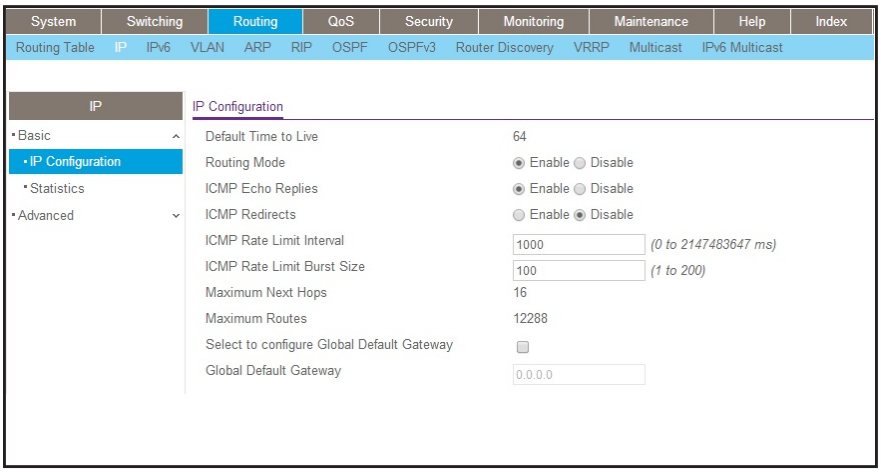
```
(Netgear Switch) #show ip route
Total Number of Routes..... 6
   Network          Subnet                    Next Hop     Next Hop
   Address           Mask         Protocol     Intf       IP Address
--------------- --------------- ------------  ---------  ---------------
0.0.0.0         0.0.0.0         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
```

Main UI: Configure Area 1 as an NSSA area on Switch A2

To use the CLI to configure Area 1 as an NSSA area on Switch A2:

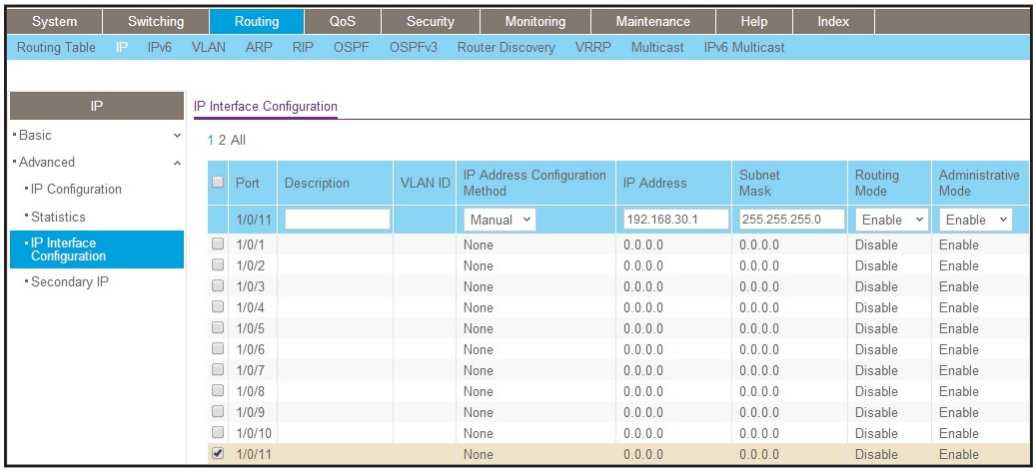
1. Enable IP routing on the switch.
   a. Select **Routing > IP > Basic > IP Configuration**.

      A page similar to the following figure displays.



   b. Select the Routing Mod **Enable** radio button.
   c. Click the **Apply** button. Your settings are saved.
2. Assign IP address 192.168.30.1 to port 1/0/11.
   a. Select **Routing > IP > Advanced > IP Interface Configuration**.

      A page similar to the following figure displays.



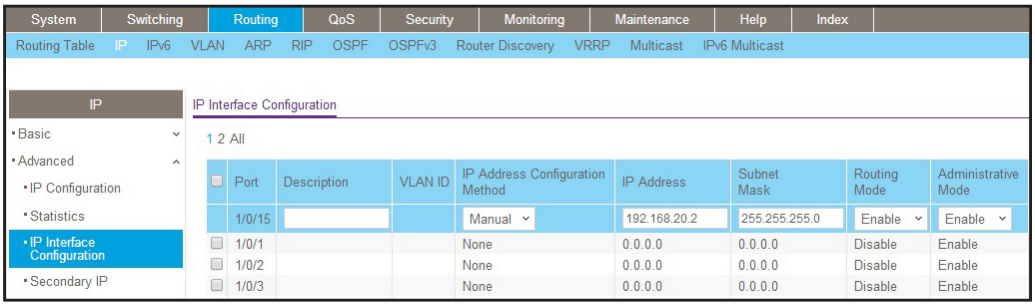
   b. Select the Port **1/0/11** check box.
   c. Configure the following settings:
      - In the **IP Address Configuration Method** menu, select **Manual**.
      - In the **IP Address** field, enter **192.168.30.1**.

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

d. Click the **Apply** button. Your settings are saved.

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

a. Remain on the same page.



b. Select the Port **1/0/15** check box.

c. Configure the following settings:

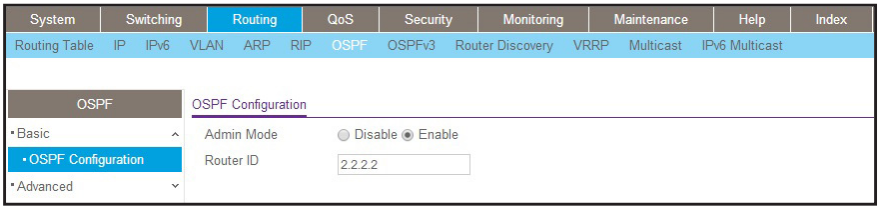
- In the **IP Address Configuration Method** menu, select **Manual**.
- In the **IP Address** field, enter **192.168.20.2**.
- In the **Subnet Mask** field, enter **255.255.255.0**.
- In the **Routing Mode** menu, select **Enable**.

d. Click the **Apply** button. Your settings are saved.

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

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

A page similar to the following figure displays.



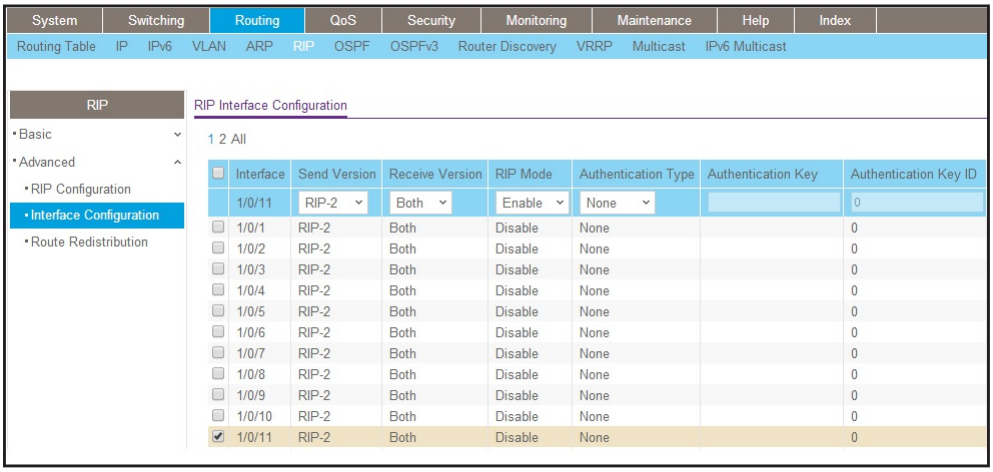
b. In the **Router ID** field, enter **2.2.2.2**.

c. Click the **Apply** button. Your settings are saved.

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

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

A page similar to the following figure displays.



b. Select the Interface **1/0/11** check box.

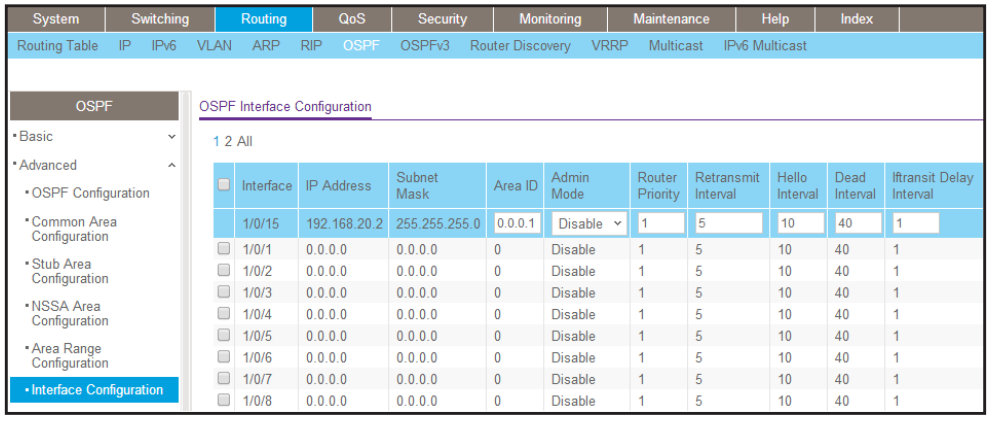
c. In the **Admin Mode** menu, select **Enable**.

d. Click the **Apply** button. Your settings are saved.

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

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

A page similar to the following figure displays.



b. Select the Interface **1/0/15** check box.

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

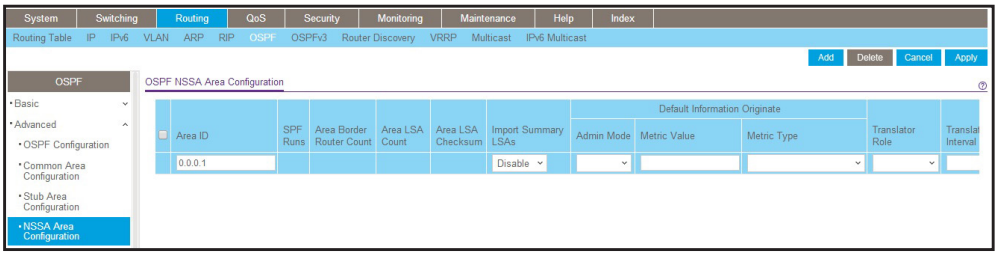
d. In the **Admin Mode** menu, select **Enable**.

e. Click the **Apply** button. Your settings are saved.

7. Configure area 0.0.0.1 as an NSSA area.

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

A page similar to the following figure displays.



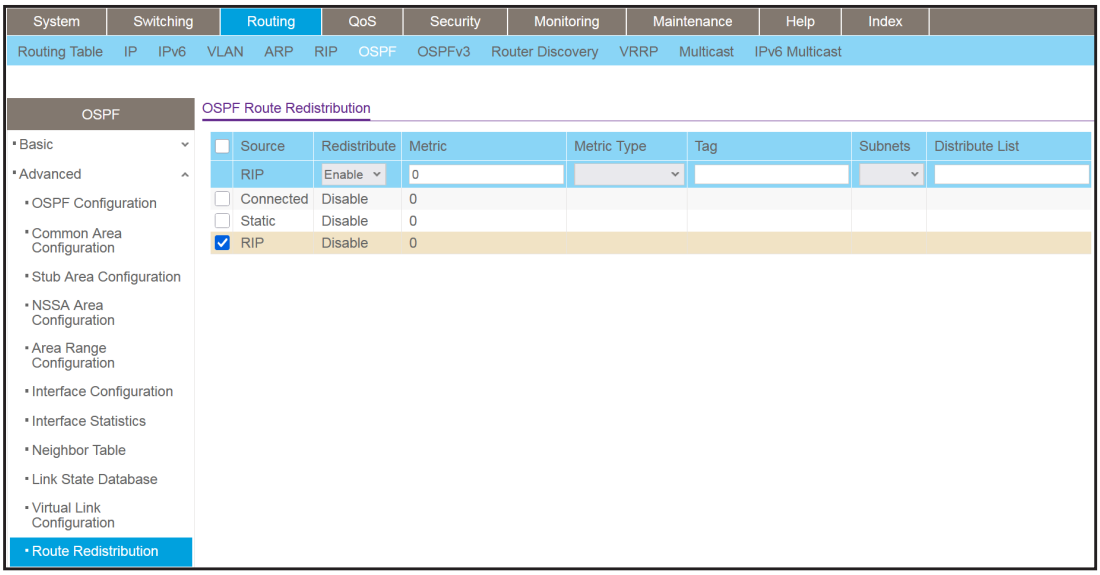
b. In the **Area ID** field, enter **0.0.0.1**.

c. Click the **Add** button. Your settings are saved.

8. Redistribute the RIP routes into the OSPF area.

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

A page similar to the following figure displays.



b. Select the Source **RIP** check box.

c. In the **Redistribute** menu, select **Enable**.

d. Click the **Apply** button. Your settings are saved.

VLAN routing with OSPF

This example adds support for OSPF to the configuration in the following base VLAN routing example.

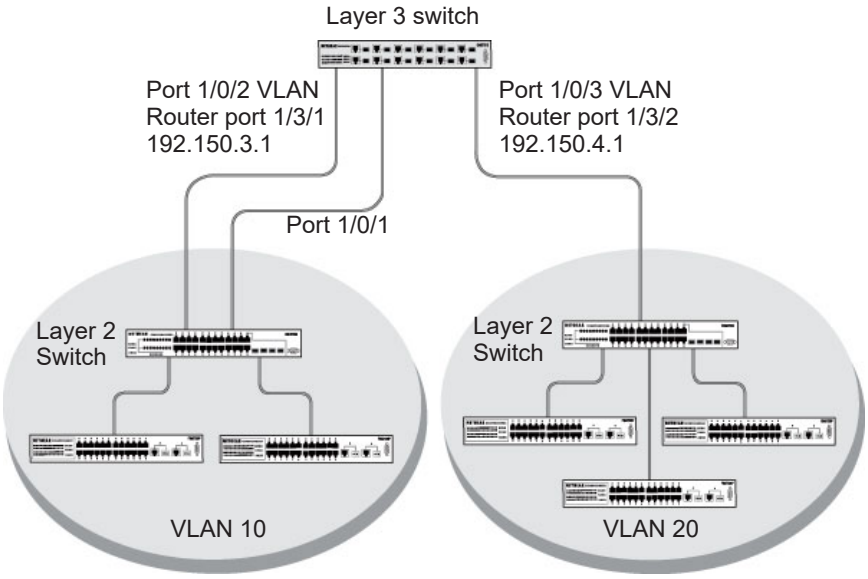


Figure 18. VLAN Routing OSPF

The example is shown as CLI commands and as a main UI procedure.

CLI: Configure VLAN routing with OSPF

To use the CLI to configure VLAN routing with OSPF:

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

```
(Netgear Switch) #vlan database
(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 VLANs 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 VLANs and physical router ports.

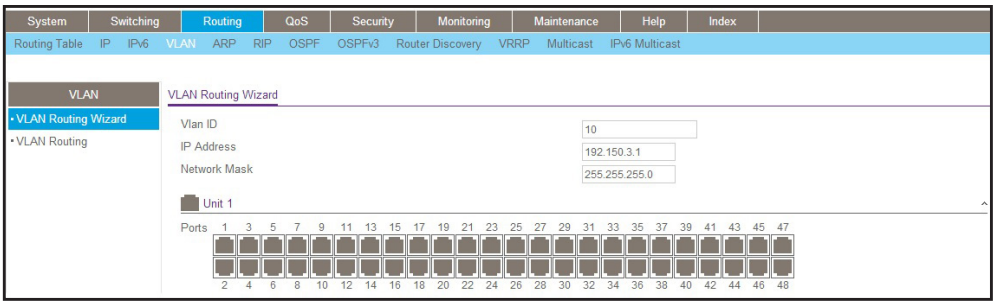
```
(Netgear Switch) (Config)#interface vlan 10
(Netgear Switch) (Interface vlan 10)#ip ospf priority 128
(Netgear Switch) (Interface vlan 10)#ip ospf cost 32
(Netgear Switch) (Interface vlan 10)#exit
(Netgear Switch) (Config)#interface vlan 20
(Netgear Switch) (Interface vlan 20)#ip ospf priority 255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

Main UI: Configure VLAN routing with OSPF

To use the main UI to configure VLAN routing with OSPF:

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

      A page similar to the following figure displays.



   b. Configure the following settings:
      - 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**.

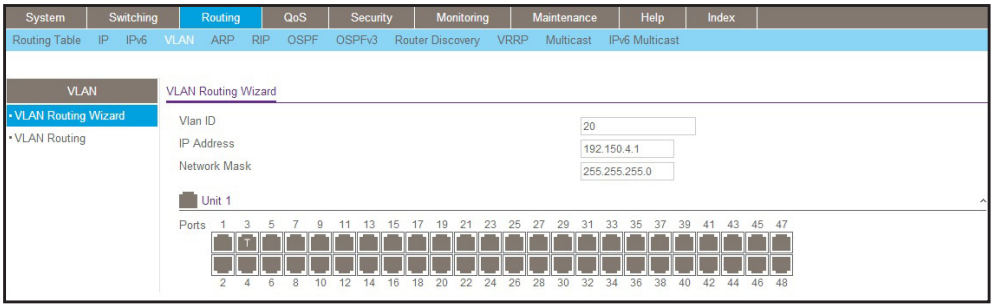
c. Click the gray box under port **2**, until T displays, which specifies that the egress packets are tagged for the port.

   If your switch is a member of a stack, be sure that you select the port in the correct unit.

d. Click the **Apply** button. Your settings are saved.

2. Configure a VLAN, and include port 1/0/3 in the VLAN.

a. Remain on the same page.



b. Configure the following settings:

- 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 the gray box under port **3**, until T displays, which specifies that the egress packets are tagged for the port.

   If your switch is a member of a stack, be sure that you select the port in the correct unit.

d. Click the **Apply** button. Your settings are saved.

3. Enable OSPF on the switch.

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

   A page similar to the following figure displays.

b. Select the Admin Mode **Enable** radio button.

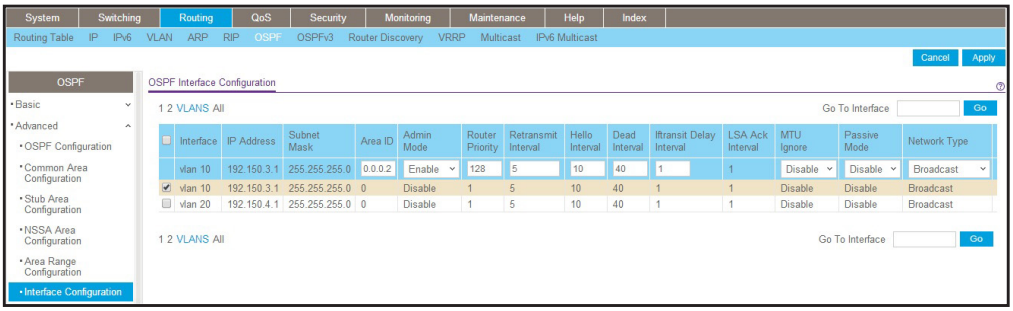
c. In the **Router ID** field, enter **192.150.9.9**.

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

4. Enable OSPF on VLAN 10.

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

A page similar to the following figure displays.



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

c. Select the Interface **vlan 10** check box.

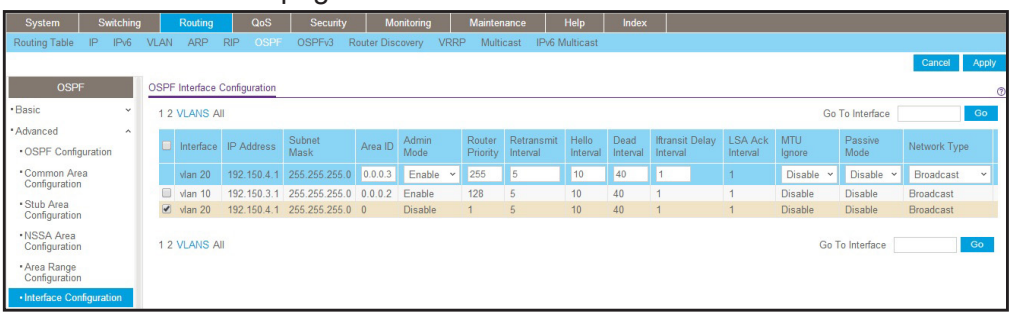
d. Configure the following settings:

- In the **Area ID** field, enter **0.0.0.2**.
- In the **Admin Mode** menu, select **Enable**.
- In the **Priority** field, enter **128**.
- In the **Metric Cost** field, enter **32**. (This field is not shown in the previous figure.)

e. Click the **Apply** button. Your settings are saved.

5. Enable OSPF on VLAN 20.

a. Remain on the same page.



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

c. Select the Interface **vlan 20** check box.

d. Configure the following settings:

- In the **Area ID** field, enter **0.0.0.3**.
- In the **Admin Mode** menu, select **Enable**.
- In the **Priority** field, enter **255**.
- In the **Metric Cost** field, enter **64**. (This field is not shown in the previous figure.)

e. Click the **Apply** button. Your settings are saved.

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.
- Addressing semantics are processed through leaf LSAs, which allow its use for both IPv4 and IPv6.
- Point-to-point links are supported 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.

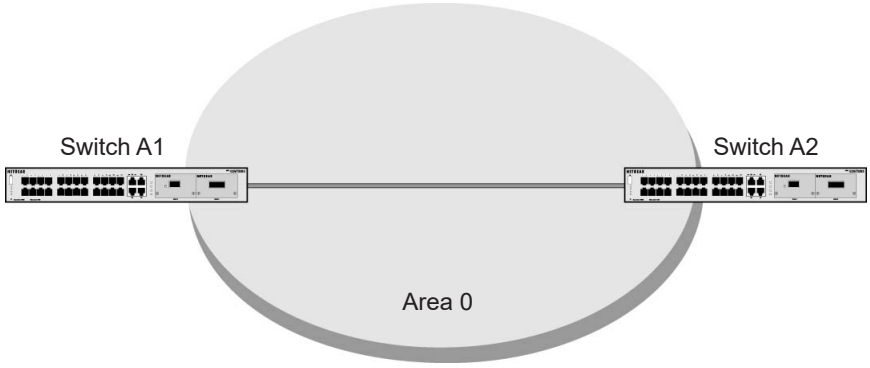


Figure 19. OSPFv3 Protocol for IPv6

The example is shown as CLI commands and as a main UI procedure.

CLI: Configure OSPFv3

To use the CLI to configure OSPFv3:

1. On Switch 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 interface 1/0/1, and assign the IP address 2000::1/64 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 interface 1/0/1, set the OSPF network mode to broadcast, and display the IPv6 OSPF neighbor.

```
(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 Switch 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::2/64 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, set the OSPF network mode to broadcast, and display the IPv6 OSPF neighbor.

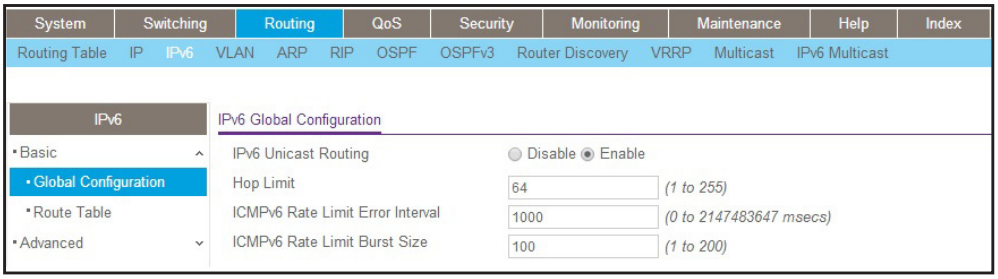
```
(Netgear Switch) (Interface 1/0/13)#ipv6 ospf
(Netgear Switch) (Interface 1/0/13)#ipv6 ospf network broadcast
(Netgear Switch) #show ipv6 ospf neighbor

Router ID Priority  IntfID   Interface    State      DeadTime
--------  --------  ------   ---------    ---------   ----
1.1.1.1      1        1      1/0/13       Full/ DR     34
```

Main UI: Configure OSPFv3

To use the main UI to configure OSPFv3:

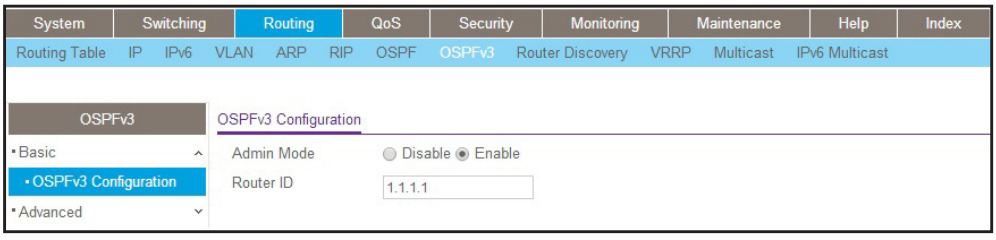
1. Enable IPv6 unicast routing on the switch.
   a. Select **Routing > IPv6 > Basic > IPv6 Global Configuration**.

   A page similar to the following figure displays.



   b. Select the IPv6 Unicast Routing **Enable** radio button.
   c. Click the **Apply** button. Your settings are saved.
2. Specify the router ID, and enable OSPFv3 for the switch.
   a. Select **Routing > OSPFv3 > Basic > OSPFv3 Configuration**.

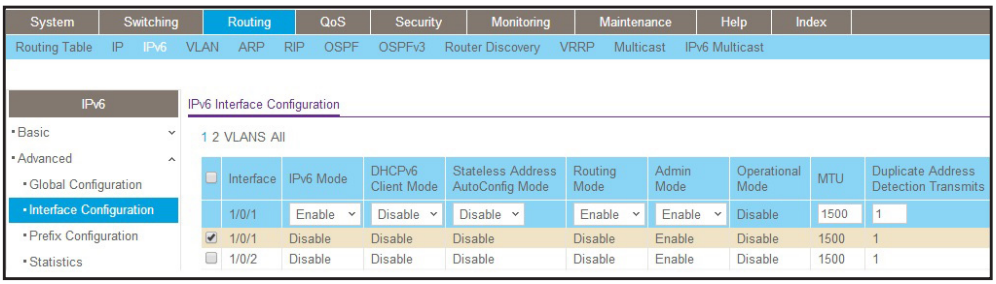
   A page similar to the following figure displays.



   b. In the **Router ID** field, enter **1.1.1.1**.
   c. Select the Admin Mode **Enable** radio button.
   d. Click the **Apply** button. Your settings are saved.

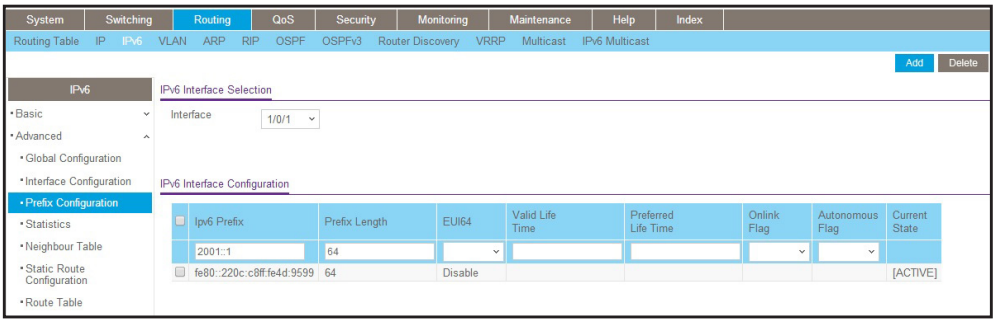
3. Enable IPv6 on port 1/0/1.
   a. Select **Routing > IPv6 > Advanced > IP Interface Configuration**.

      A page similar to the following figure displays.



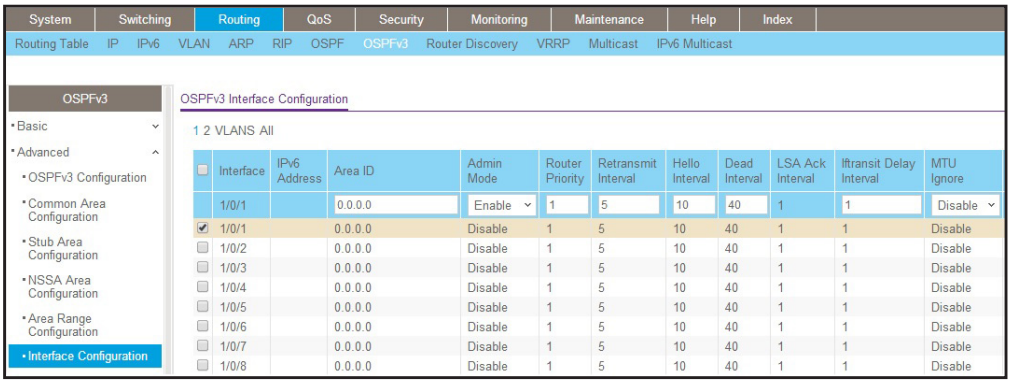
   b. Select the Interface **1/0/1** check box.
   c. In the **IPv6 Mode** menu, select **Enable**.
   d. In the **Routing Mode** menu, select **Enable**.
   e. Click the **Apply** button. Your settings are saved.
4. Assign the IP address 2001::1/64 to port 1/0/1.
   a. Select **Routing > IPv6 > Advanced > IP Interface Configuration**.

      A page similar to the following figure displays.



   b. Under IPv6 Prefix Selection, in the **Interface** menu, select **1/0/1**.
   c. Under IPv6 Interface Configuration, configure the following settings:
      - In the **IPv6 Prefix** field, enter **2001::1**.
      - In the **Prefix Length** field, enter **64**.
      - In the **EUI64** menu, select **Disable**.
      - In the **Onlink Flag** menu, select **Disable**.
      - In the **Autonomous Flag** menu, select **Disable**.
   d. Click the **Add** button. Your settings are saved.
5. Enable OSPFv3 on port 1/0/1.
   a. Select **Routing > OSPFv3 > Advanced > Interface Configuration**.

A page similar to the following figure displays.



b. Select the Interface **1/0/1** check box.

c. In the **OSPF Area ID** field, enter **0.0.0.0**.

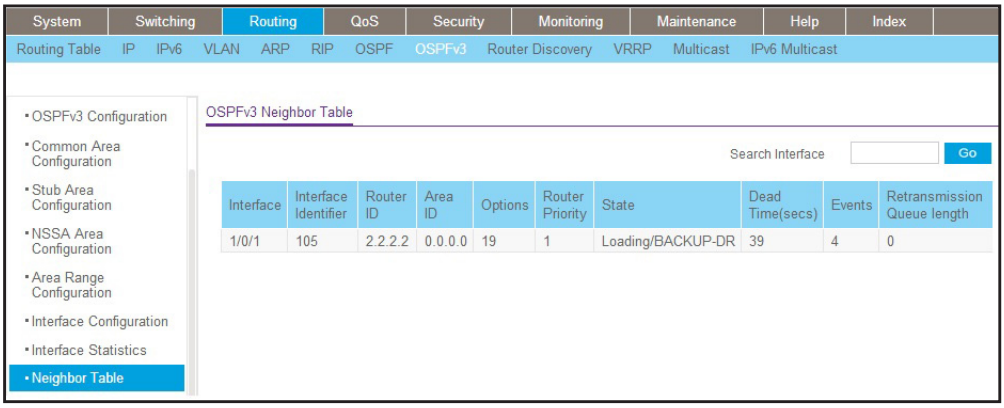
d. In the **Admin Mode** menu, select **Enable**.

e. Click the **Apply** button. Your settings are saved.

6. Display the OSPFv3 Neighbor Table.

a. Select **Routing > OSPFv3 > Advanced > Neighbor Table**.

A page similar to the following figure displays.



7. To use the main UI to configure OSPFv3 on Switch A2, repeat this process for Switch A2.

8

PBR

Policy-based routing

This feature is supported on the M4250 series switches

This feature is supported on the M4300 series switches

This feature is supported on the M4350 series switches

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 forward traffic based on the information in routing tables, which are populated by information provided by dynamic routing protocols or static routing, to forward packets to destination addresses. Policy-based routing (PBR) is a feature that enables you 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 you 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 you specify 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, 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 you 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 must 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.

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 must 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, you have 8 possible values for the IP precedence. If configured, this value is set in IPv4 header of packets.

PBR processing logic

If 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.

A route map with a permit statement uses the following processing 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 or MAC access list. An ACL that is used in the match term itself includes one or more permit or deny rules. The incoming packet is matched against the rules in the ACL, and a permit or deny decision is reached:
  - If the packet is permitted, policy-based routing executes the action specified in set terms of the route-map statement over an incoming packet.
  - If the packet is denied, 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 increased and the processing logic moves to the 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.

A route map with a deny statement uses the following processing 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 or 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 packet is permitted, policy-based routing terminates and the packet goes through standard destination-based routing logic.
- If the packet is denied, the counter for this match statement is not increased 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 actions:

Table 3. 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 the packets using the default routing table.
- **Set**. Route the packets according to the action in the set clause.
- **Route** (alone). Route the packets using the default routing table.

PBR configurations

PBR is configurable on the following types of routing interfaces:

- Physical ports
- VLAN interfaces

On VLAN interfaces, if 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 situation applies to ACLs specified in the match clause of PBR. That is, if a PBR route map is applied on a VLAN interface, a packet arriving with a corresponding VLAN ID on a port is matched against PBR rules corresponding to the match ACL clause and the corresponding set actions are taken. 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 pre-configuration of a route map on routing interfaces. If routing is not enabled on an interface, the route map can still be applied on that interface. When routing is not enabled on an interface, the route-map configuration is not pushed into the hardware. Rather, it is maintained only in the configuration. If routing is then enabled on that interface, the configuration is applied to the hardware.

PBR example

You 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 an organization, the bulk traffic associated with the organization activity must use a higher-bandwidth, high-cost link while the basic connectivity can continue over a lower bandwidth, low-cost link for interactive traffic. For such applications, policy-based routing is the right fit.

Consider a 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.

The example is shown as CLI commands only because you cannot configure PBR in the main UI.

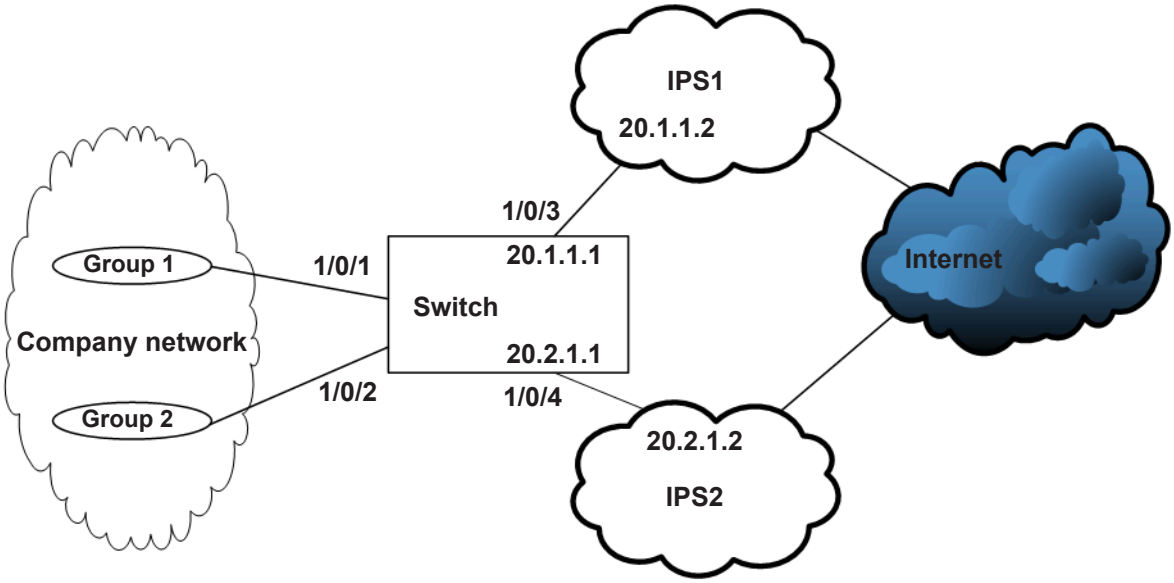


Figure 20. PBR topology

To use the CLI to set up ACLs and route maps for PBR to enable load-sharing for incoming traffic based on packet entities:

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 routing VLAN 30 and makes interfaces 1/0/1 and 1/0/2 members if 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
```

9

ARP

Proxy Address Resolution Protocol

This feature is supported on the M4250 series switches

This feature is supported on the M4300 series switches

This feature is supported on the M4350 series switches

This chapter includes the following sections:

- Proxy ARP concepts
- Configure Proxy ARP on a port

Proxy ARP concepts

Proxy ARP allows a switch that is has routing capacities enabled to answer ARP requests when the target IP address is not that of the switch itself but a destination that the switch can reach. If a host does not know the default gateway, proxy ARP can learn the first hop. Devices in one physical network appear to be part of another logical network. Without proxy ARP, a switch that is has routing capacities enabled responds to an ARP request only if the target IP address is an address configured on the interface where the ARP request arrives.

Configure Proxy ARP on a port

The example is shown as CLI commands and as a main UI procedure.

CLI: Configure Proxy ARP on a port

To display information about the IP configuration for a port and configure Proxy ARP on the port:

1. Display information about the IP configuration for a port.

```
(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
```

2. Configure the Proxy ARP on the port.

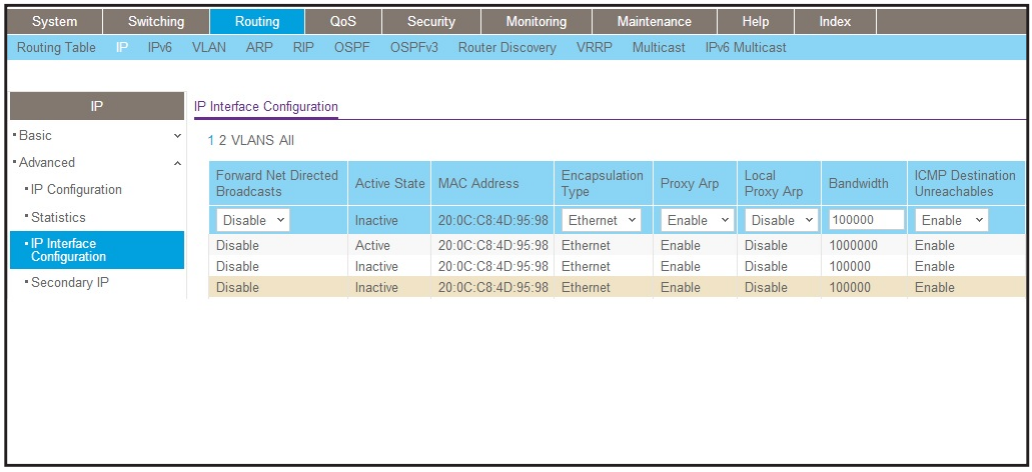
```
(Netgear Switch) (Interface 0/24)#ip proxy-arp ?

<cr>                        Press Enter to execute the command.

(Netgear Switch) (Interface 0/24)#ip proxy-arp
```

Main UI: Configure Proxy ARP on a port

To configure Proxy ARP on a port:

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

   A page similar to the following figure displays.



2. Select the Port **1/0/3** check box.
3. In the **Proxy Arp** menu, select **Enable**.
4. Click the **Apply** button. Your settings are saved.

10

VRRP

Virtual Router Redundancy Protocol

This feature is supported on the M4350 series switches

This feature is supported on the M4300 series switches

This chapter includes the following sections:

- Virtual Router Redundancy Protocol concepts
- Configure VRRP on a primary router
- Configure VRRP on a secondary router

Note: The Virtual Router Redundancy Protocol (VRRP) feature is supported on the M4300 series and M4350 series switches only. The M4250 series switches do not support VRRP.

Virtual Router Redundancy Protocol concepts

When an end station is statically configured with the address of a switch that has routing capabilities enabled and that processes the end station's routed traffic, a single point of failure is introduced into the network. If the switch goes down, the end station is unable to communicate. Virtual Router Redundancy Protocol (VRRP) can provide a backup mechanism in a configuration with static routing addresses.

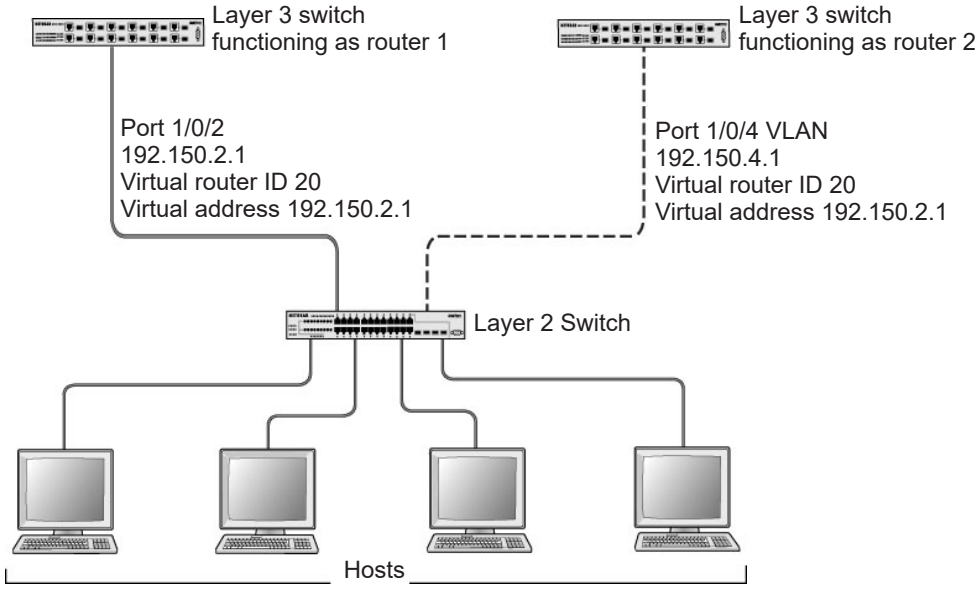


Figure 21. VRRP configuration

VRRP eliminates the single point of failure associated with static default routes by enabling a switch that is functioning as secondary router to take over from a switch that is functioning as a primary router without affecting the end stations using the route. The end stations use a virtual IP address that is recognized by the secondary router if the primary router fails.

Participating routers use an election protocol to determine which router is the primary router. A 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.

Configure VRRP on a primary router

This example shows how to configure the switch to support VRRP. Router 1 is the default primary router for the virtual route, and Router 2 is the secondary router.

The example is shown as CLI commands and as a main UI procedure.

CLI: Configure VRRP on a primary router

To use the CLI to configure VRRP on a primary router:

1. Enable routing for the switch. IP forwarding is then enabled by default.

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

2. Configure the IP addresses and subnet masks for the port that must participate in VRRP.

```
(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 a virtual router ID to the port that must participate in VRRP.

```
(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 must recognize. The virtual IP address on port 1/0/2 is the same as the port's actual IP address. Therefore, when the port is active, this switch is always the primary VRRP router. 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.

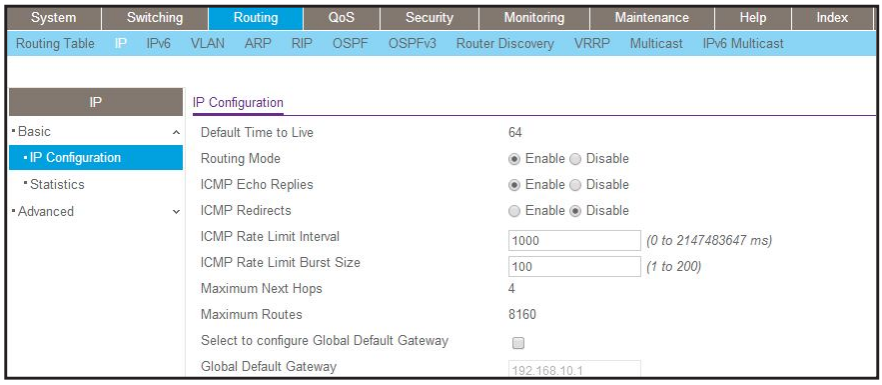
```
(Netgear Switch) (Interface 1/0/2)#ip vrrp 20 mode
(Netgear Switch) (Interface 1/0/2)#exit
(Netgear Switch) (Config)#exit
```

Main UI: Configure VRRP on a primary router

To use the main UI to configure VRRP on a primary router:

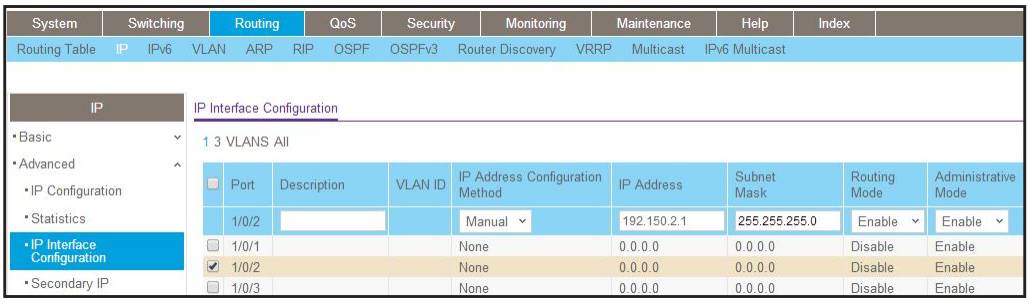
1. Enable IP routing on the switch.
   a. Select **Routing > IP > Basic > IP Configuration**.

      A page similar to the following figure displays.



   b. Select the Routing Mode **Enable** radio button.
   c. Click the **Apply** button. Your settings are saved.
2. Assign the IP address 192.150.2.1 to port 1/0/2:
   a. Select **Routing > IP > Advanced > IP Interface Configuration**.

      A page similar to the following figure displays.



   b. Select the Port **1/0/2** check box.
   c. Configure the following settings:
      - In the **IP Address** field, enter **192.150.2.1**.
      - In the **Subnet Mask** field, enter **255.255.0.0**.
      - In the **Routing Mode** menu, select **Enable**.

d. Click the **Apply** button. Your settings are saved.

3. Enable VRRP on port 1/0/2.

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

A page similar to the following figure displays.

b. Under Global Configuration, select the Admin Mode **Enable** radio button.

c. Under Table Configuration, configure the following settings:

- In the **VRID (1 to 255)** field, enter **20**.
- In the **Interface** menu, select **1/0/2**.
- In the **Primary IP Address** field, enter **192.150.2.1**.
- In the **Mode** menu, select **Active**.

d. Click the **Apply** button. Your settings are saved.

Configure VRRP on a secondary router

The example is shown as CLI commands and as a main UI procedure.

CLI: Configure VRRP on a secondary router

To use the CLI to configure VRRP on a secondary router:

1. Enable routing for the switch. IP forwarding is then enabled by default.

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

2. Configure the IP addresses and subnet masks for the port that must participate in VRRP.

```
(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 a virtual router ID to port that must participate in VRRP.

```
(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 must recognize. The virtual IP address on port 1/0/4 is the same as the actual IP address of port 1/0/2 on the primary router. Therefore, when the primary router (with port 1/0/2) is active, this router (with port 1/0/4) is always the secondary VRRP router.

```
(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.

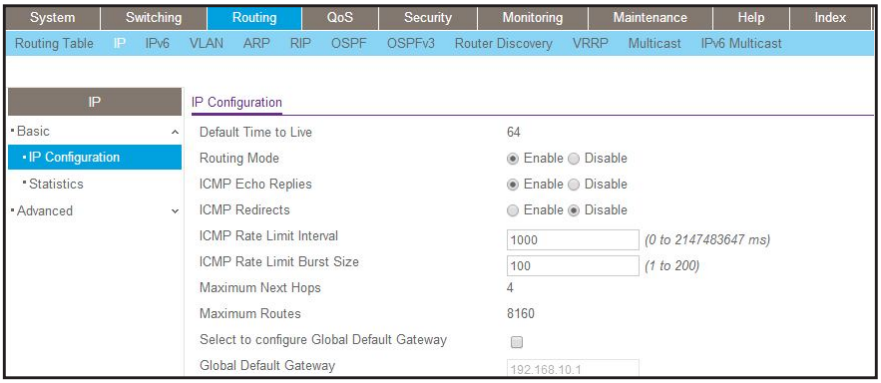
```
(Netgear Switch) (Interface 1/0/4)#ip vrrp 20 mode
(Netgear Switch) (Interface 1/0/4)#exit
(Netgear Switch) (Config)#exit
```

Main UI: Configure VRRP on a secondary router

To use the main UI to configure VRRP on a secondary router:

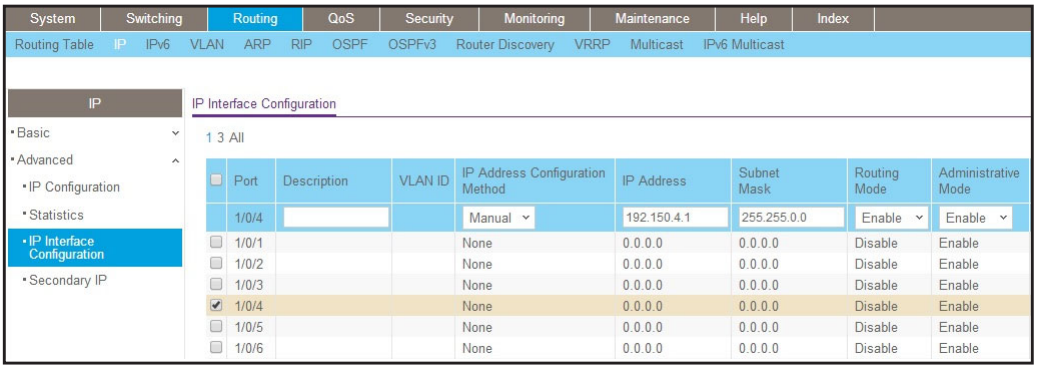
1. Enable IP routing on the switch.
   a. Select **Routing > IP > IP Configuration**.

      A page similar to the following figure displays.



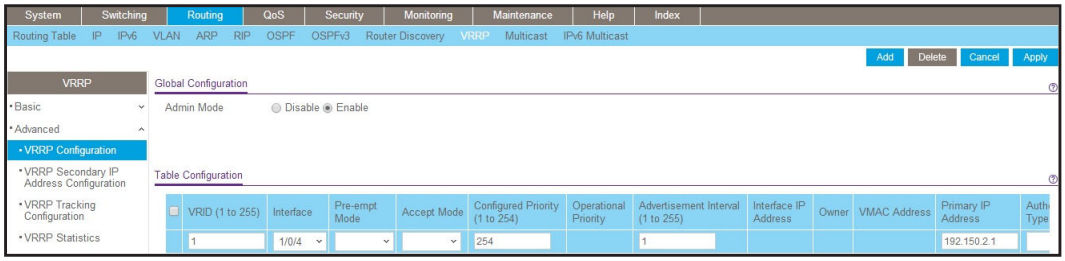
   b. Select the Routing Mode **Enable** radio button.
   c. Click the **Apply** button. Your settings are saved.
2. Assign IP address 192.150.4.1 to port 1/0/4.
   a. Select **Routing > IP > Advanced > IP Interface Configuration**.

      A page similar to the following figure displays.



   b. Select the Port **1/0/4** check box.
   c. Configure the following settings:
      - In the **IP Address** field, enter **192.150.4.1**.
      - In the **Subnet Mask** field, enter **255.255.0.0**.
      - In the **Administrative Mode** menu, select **Enable**.
   d. Click the **Apply** button. Your settings are saved.
3. Enable VRRP on port 1/0/4.
   a. Select **Routing > VRRP > Advanced > VRRP Configuration**.

A page similar to the following figure displays.



b. Under Global Configuration, select the Admin Mode **Enable** radio button.

c. Under Table Configuration, configure the following settings:

- In the **VRID (1 to 255)** field, enter **20**.
- In the **Interface** menu, select **1/0/4**.
- In the **Configured Priority (1 to 255)**, enter **254**.
- In the **Primary IP Address** field, enter **192.150.2.1**.
- In the **Status** menu, select **Active**.

d. Click the **Add** button. Your settings are saved.

11

ACLs

Access Control Lists

This feature is supported on the M4250 series switches

This feature is supported on the M4300 series switches

This feature is supported on the M4350 series switches

This chapter includes the following sections:

- Access Control List concepts
- MAC ACLs
- Set up an IP ACL with two rules
- Configure one-way access using a TCP flag in an ACL
- Use ACLs to isolate VLANs on a Layer 3 switch
- Set up a MAC ACL with two rules
- Configure ACL mirroring
- Configure ACL redirection for a traffic stream
- Add ACL remarks
- Manage ACL rule sequences
- Configure a management ACL
- Configure an IPv6 ACL

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, but the switch supports ACLs too. 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 field must be used to permit or deny access to the network, and can 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.
- The switch does not support MAC ACLs and IP ACLs on the same interface.
- The switch supports ACLs 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).

The following applies to MAC ACLs:

- 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 field must 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 describes how to set up an IP ACL with two rules: one applicable to TCP traffic and another one applicable to UDP traffic. The content of the two rules is the same. TCP and UDP packets are accepted by the switch only if the source and destination stations have IP addresses within the defined sets.

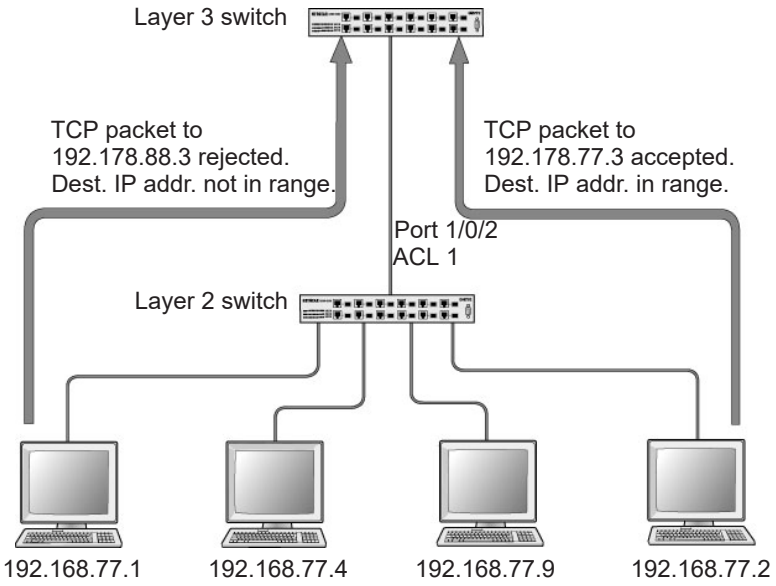


Figure 22. IP ACL with rules for TCP traffic and UDP traffic

The example is shown as CLI commands and as a main UI procedure.

CLI: Set up an IP ACL with two rules

To use the CLI to set up an IP ACL with two rules:

1. Create ACL 101 and define the first rule in which the ACL permits 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.:

```
(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, after which only traffic matching the criteria is accepted.

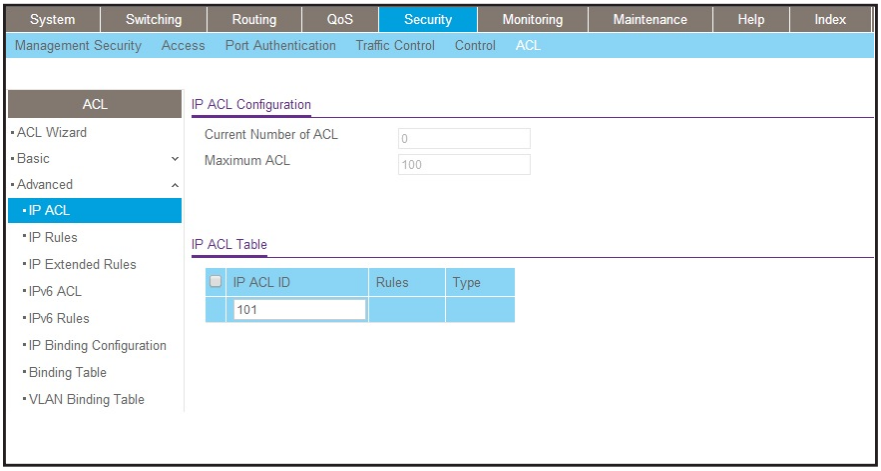
```
(Netgear Switch) (Config)#interface 1/0/2
(Netgear Switch) (Interface 1/0/2)#ip access-group 101 in
(Netgear Switch) (Interface 1/0/2)#exit
(Netgear Switch) (Config)#exit
```

Main UI: Set up an IP ACL with two rules

To use the main UI to set up an IP ACL with two rules:

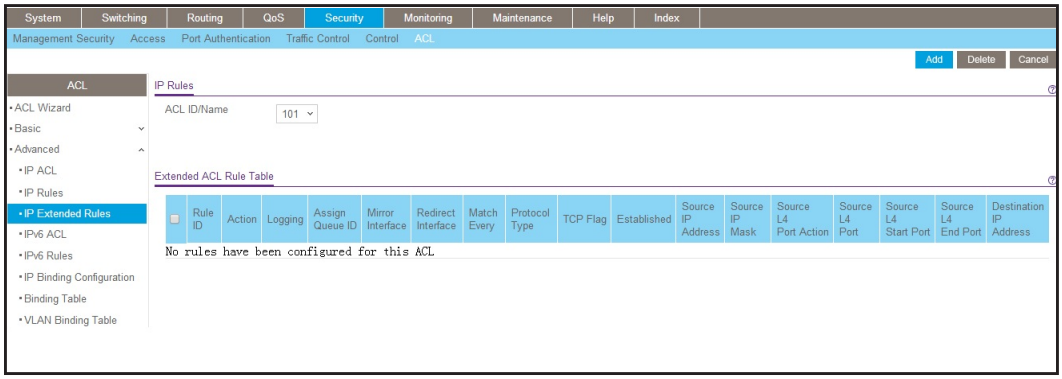
1. Create IP ACL 101 on the switch.
   a. Select **Security > ACL > Advanced > IP ACL**.

      A page similar to the following figure displays.



   b. In the **IP ACL ID** field, enter **101**.
   c. Click the **Add** button. Your settings are saved.
2. Create a first ACL rule and add it to ACL 101.
   a. Select **Security > ACL > Advanced > IP Extended Rules**.

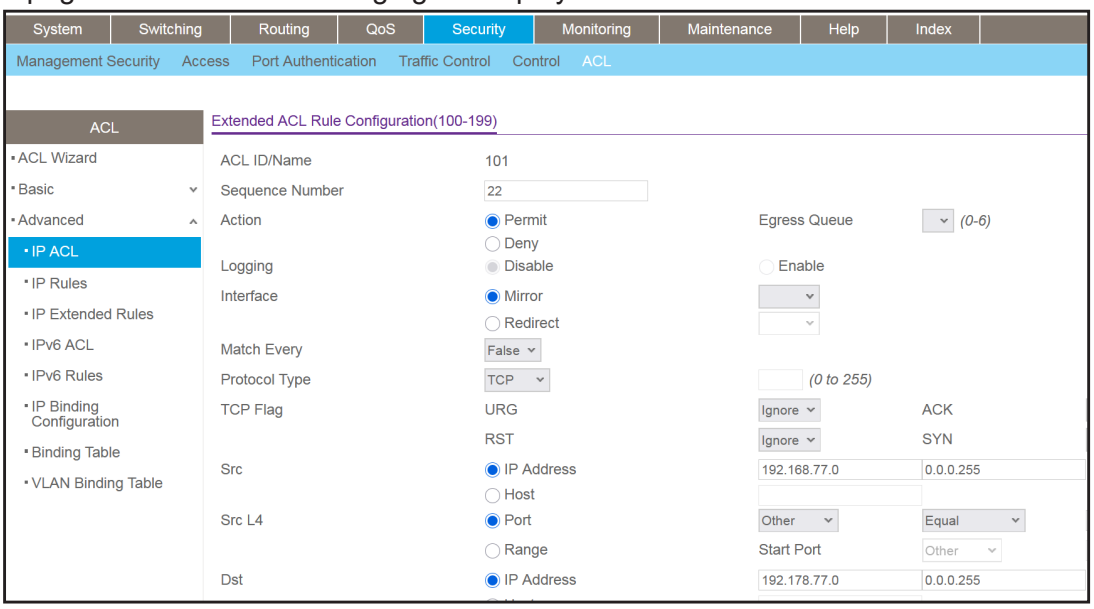
      A page similar to the following figure displays.



b. In **ACL ID/Name** menu, select **101**.

c. Click **Add** to open a page that lets you add a rule.

A page similar to the following figure displays.



a. Configure the following settings:

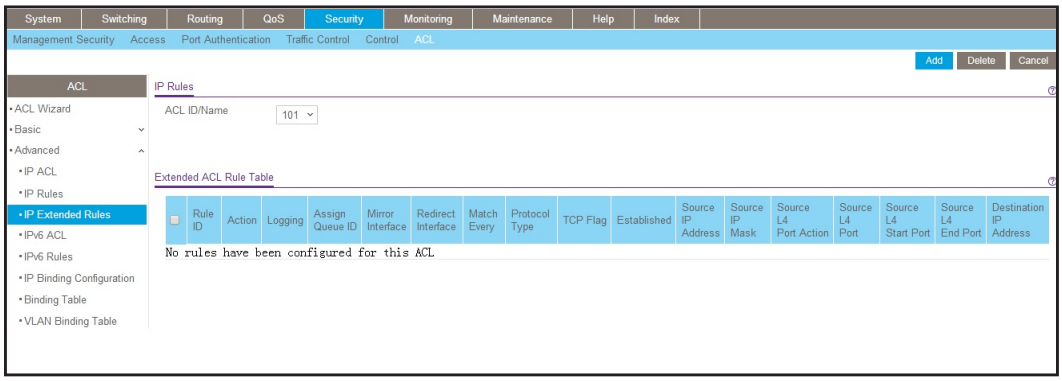
- In the **Sequence Number** field, enter **22**.
- Select the **Action Permit** radio button.
- In the **Match Every** menu, select **False**.
- In the **Protocol Type** menu, select **TCP**.
- In the **Src IP Address** field, enter **192.168.77.0**.
- In the source subnet mask field to the right, enter **0.0.0.255**.
- In the **Dst IP Address** field, enter **192.178.77.0**.
- In the destination subnet mask field to the right, enter **0.0.0.255**.

b. Click the **Apply** button. Your settings are saved.

3. Define a second ACL rule and add it to ACL 101.

a. Select **Security > ACL > Advanced > IP Extended Rules**.

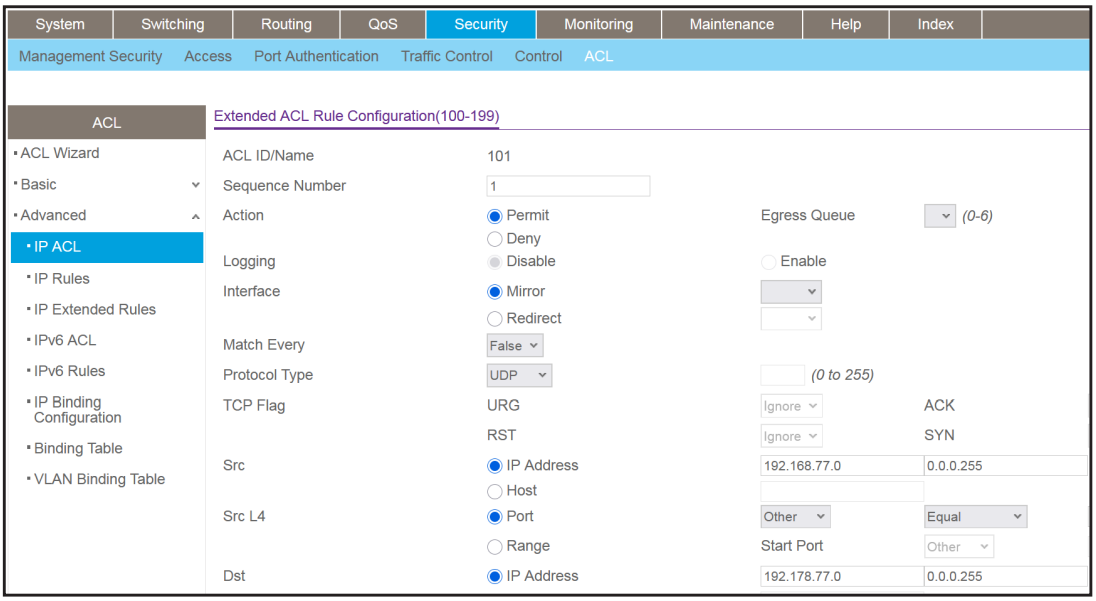
A page similar to the following figure displays.



b. In **ACL ID/Name** menu, select **101**.

c. Click **Add** to open a page that lets you add a rule.

A page similar to the following figure displays.



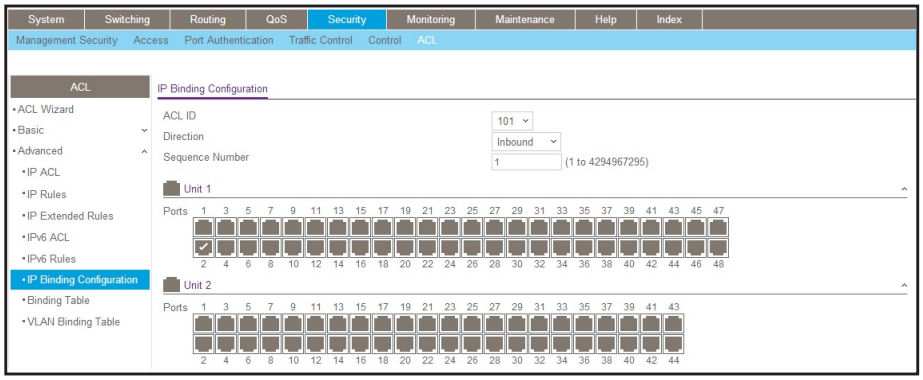
d. Configure the following settings:

- In the **Sequence Number** field, enter **1**.
- Select the **Action Permit** radio button.
- In the **Match Every** menu, select **False**.
- In the **Protocol Type** menu, select **UDP**.
- In the **Src IP Address** field, enter **192.168.77.0**.
- In the source subnet mask field to the right, enter **0.0.0.255**.
- In the **Dst IP Address** field, enter **192.178.77.0**.
- In the destination subnet mask field to the right, enter **0.0.0.255**.

e. Click the **Apply** button. Your settings are saved.

4. Apply ACL 101 to port 2.
   a. Select **Security > ACL > Advanced > IP Binding Configuration**.

      A page similar to the following figure displays.



   b. Under IP Binding Configuration, configure the following settings:
      - In the **ACL ID** menu, select **101**.
      - In the **Sequence Number** field, enter **1**.

   c. Click the gray box under port **2**. A check mark displays in the box.

      If your switch is a member of a stack, be sure that you select the ports in the correct unit.

   d. Click the **Apply** button. Your settings are saved.

Configure 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. Desktop 1 can access FTP server 1 and FTP server 2, but Desktop 2 can access only FTP server 2.

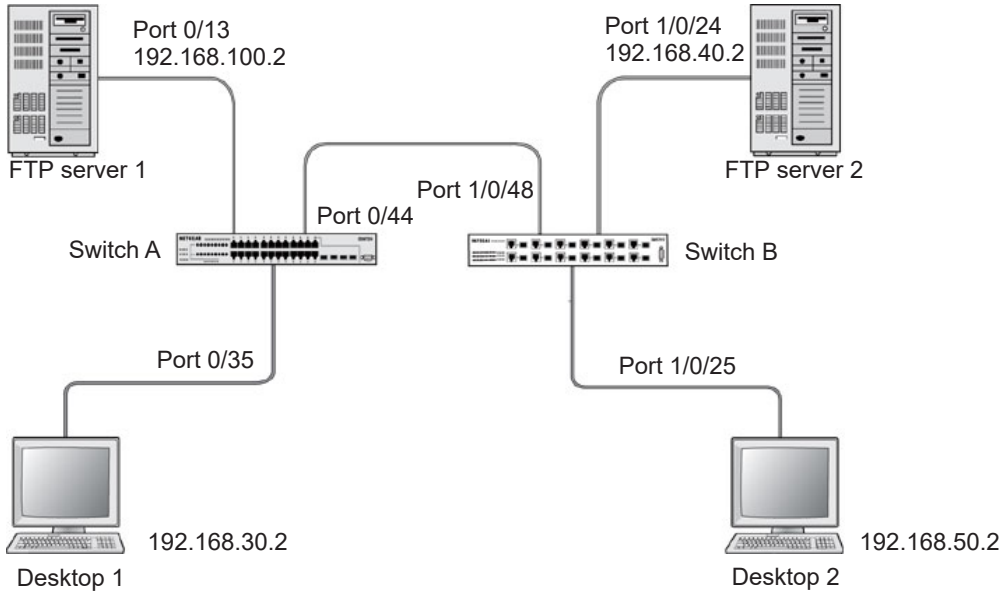


Figure 23. One-Way Web access using a TCP flag in an ACL

The example is shown as CLI commands and as a main UI procedure.

CLI: Configure one-way access using a TCP flag in an ACL

This is a two-step process:

- CLI Step 1: Configure VLANs, IP addresses, static routes, and ACLs on Switch A
- CLI Step 2: Configure VLANs, IP addresses, and static routes on Switch B

CLI Step 1: Configure VLANs, IP addresses, static routes, and ACLs on Switch A

ALso see Figure 23, One-Way Web access using a TCP flag in an ACL.

To use the CLI to configure VLANs, IP addresses, static routes, and ACLs on Switch A:

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 with a sequence of 1 for ACL 101 and a sequence of 2 for ACL 102.

```
(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
```

CLI Step 2: Configure VLANs, IP addresses, and static routes on Switch B

Also see Figure 23, One-Way Web access using a TCP flag in an ACL.

To use the CLI to configure VLANs, IP addresses, and static routes on Switch B:

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
(Netgear Switch) (Config)#exit
```

2. Create VLAN 50 with port 1/0/25 and assign IP address 192.168.50.1/24.

```
(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
```

Main UI: Configure one-way access using a TCP flag in an ACL

This is a two-part process:

- Main UI Step 1: Configure VLANs, IP addresses, static routes, and ACLs on Switch A
- Main UI Step 2: Configure VLANs, IP addresses, and static routes on Switch B

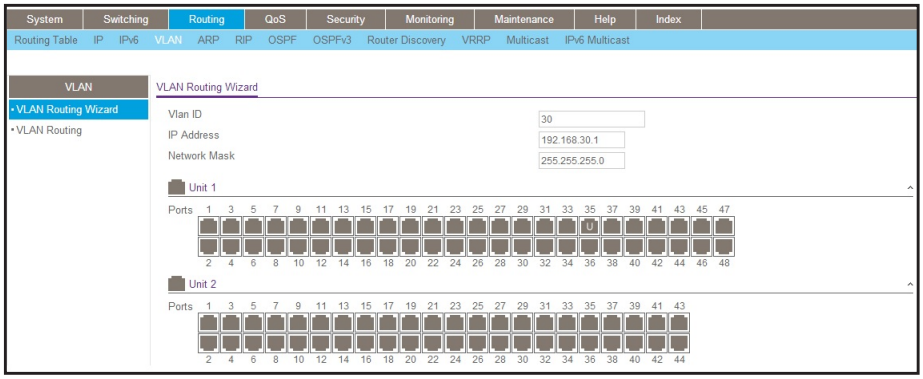
Main UI Step 1: Configure VLANs, IP addresses, static routes, and ACLs on Switch A

Also see Figure 23, One-Way Web access using a TCP flag in an ACL.

To use the main UI to configure VLANs, IP addresses, static routes, and ACLs on Switch B:

1. Create VLAN 30 with IP address 192.168.30.1/24.
   a. Select **Routing > VLAN > VLAN Routing Wizard**.

      A page similar to the following figure displays.



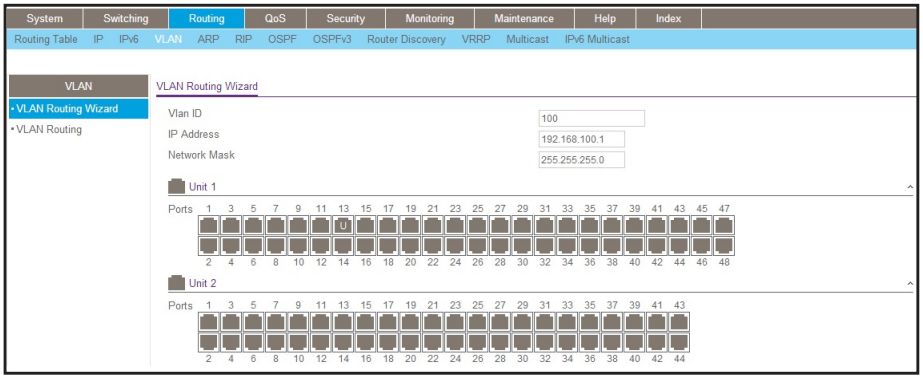
   b. In the VLAN Routing Wizard, configure the following settings:
      - In the **VLAN ID** field, enter **30**.
      - In the **IP Address** field, enter **192.168.30.1**.
      - In the **Network Mask** field, enter **255.255.255.0**.

   c. Click the gray box under port **35** until U displays, specifying that the egress packets are untagged for the port.

      If your switch is a member of a stack, be sure that you select the ports in the correct unit.

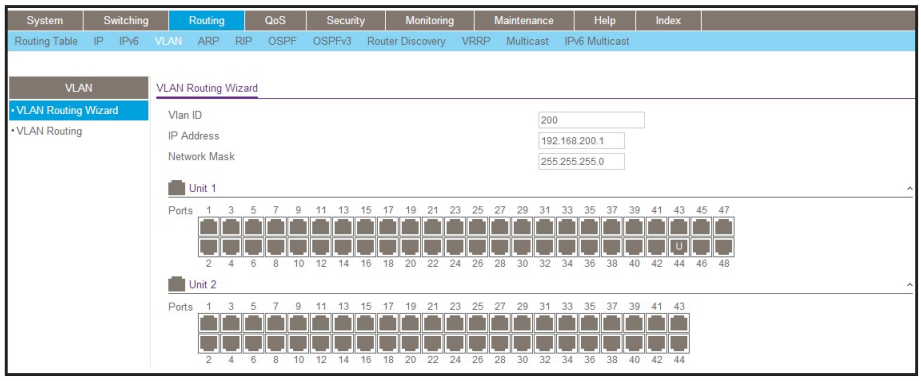
   d. Click the **Apply** button. Your settings are saved.

2. Create VLAN 100 with IP address 192.168.100.1/24.
   a. Remain on the same page.



   b. Configure the following settings:
      - 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 the gray box under port **13** until U displays, specifying that the egress packets are untagged for the port.

      If your switch is a member of a stack, be sure that you select the ports in the correct unit.
   d. Click the **Apply** button. Your settings are saved.
3. Create VLAN 200 with IP address 192.168.200.1/24.
   a. Remain on the same page.



   b. Configure the following settings:
      - 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 the gray box under port **44** until U displays, specifying that the egress packets are untagged for the port.

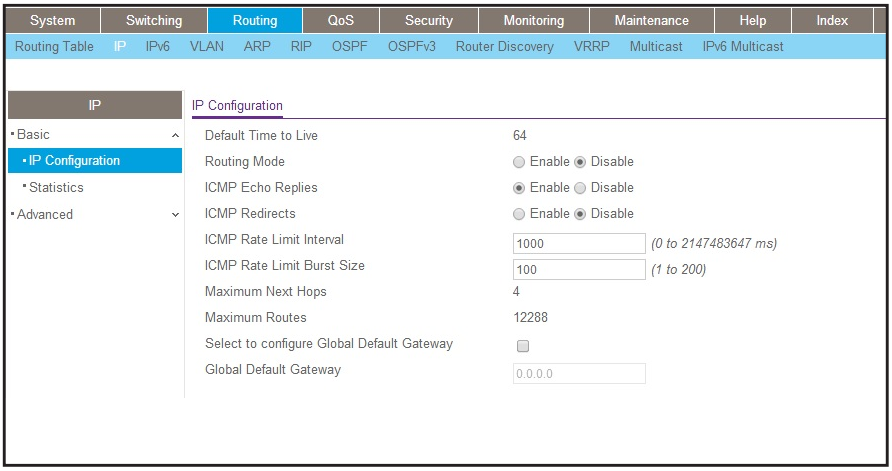
      If your switch is a member of a stack, be sure that you select the ports in the correct unit.

d. Click the **Apply** button. Your settings are saved.

4. Enable IP routing.

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

A page similar to the following figure displays.



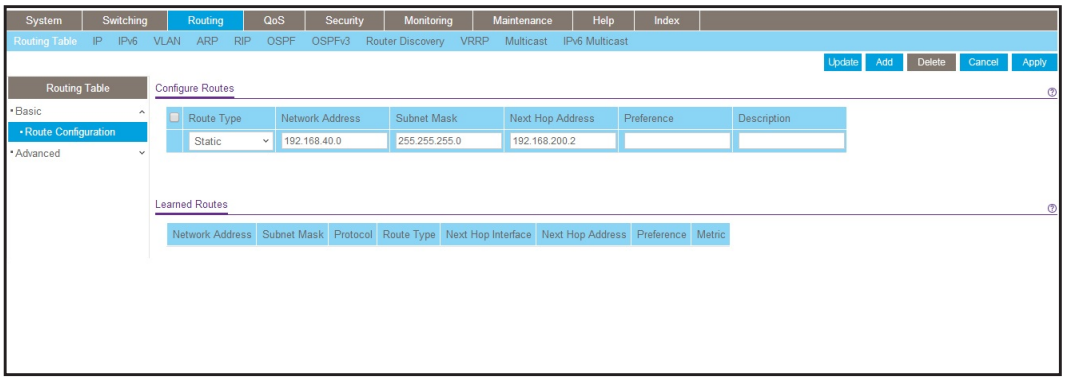
b. Select the Routing Mode **Enable** radio button.

c. Click the **Apply** button. Your settings are saved.

5. Add a static route with IP address 192.268.40.0/24:

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

A page similar to the following figure displays.

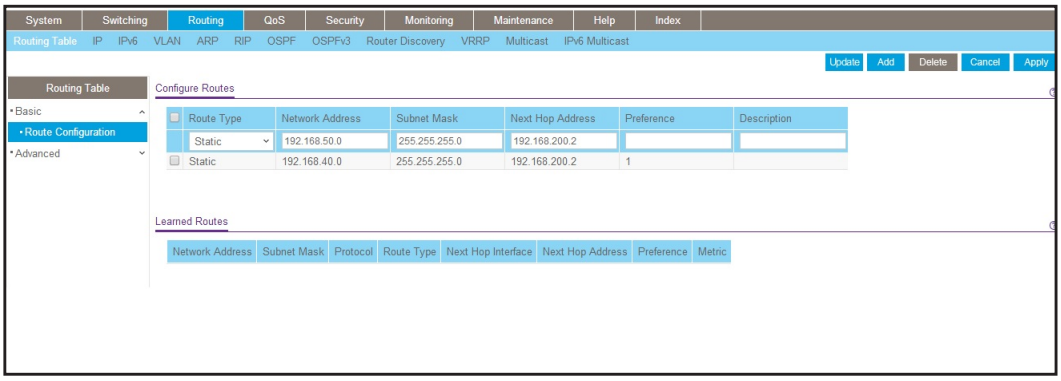


b. Under Configure Routes, configure the following settings:

- In the **Route Type** menu, 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**.

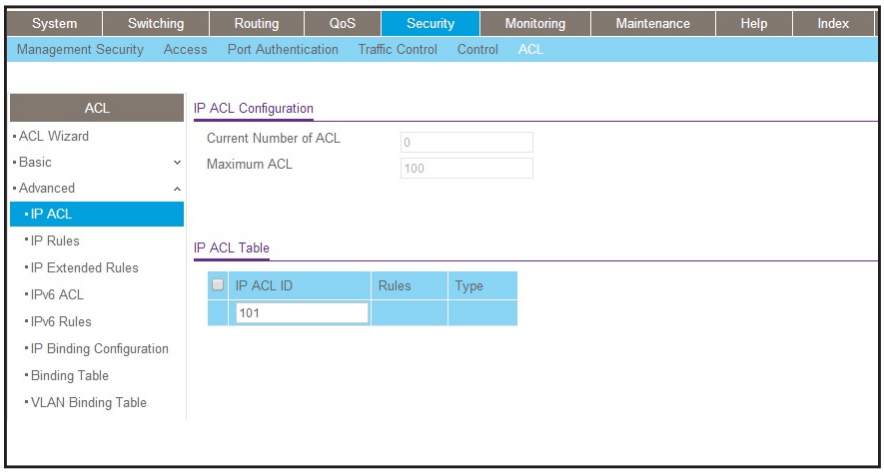
c. Click the **Add** button. Your settings are saved.

6. Create a static route with IP address 192.168.50.0/24:
   a. Remain on the same page.



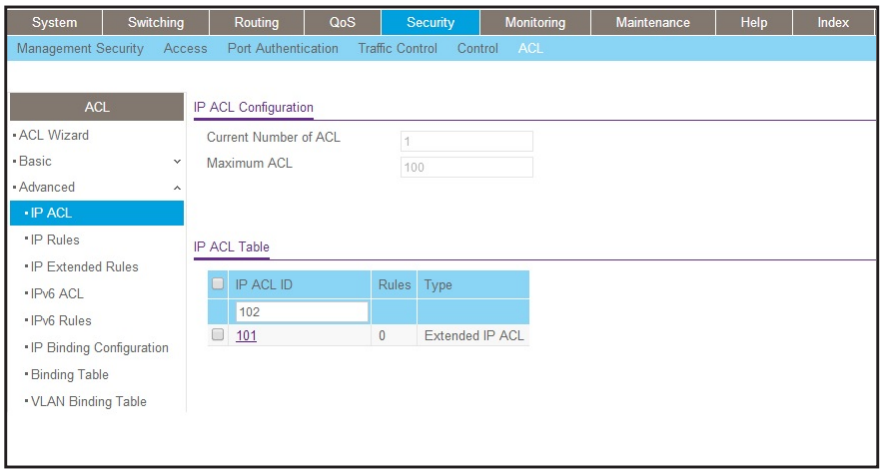
   b. Under Configure Routes, configure the following settings:
      - In the **Route Type** menu, select **Static**.
      - In the **Network Address** field, enter **192.168.50.0**.
      - In the **Subnet Mask** field, enter **255.255.255.0**.
      - In the **Next Hop IP Address** field, enter **192.168.200.2**.
   c. Click the **Add** button. Your settings are saved.
7. Create an ACL with ID 101.
   a. Select **Security > ACL > Advanced > IP ACL**.

      A page similar to the following figure displays.



   b. In the IP ACL Table, in the **IP ACL ID** field, enter **101**.
   c. Click the **Add** button. Your settings are saved.
8. Create an ACL with ID 102.
   a. Select **Security > ACL > Advanced > IP ACL**.

A page similar to the following figure displays.



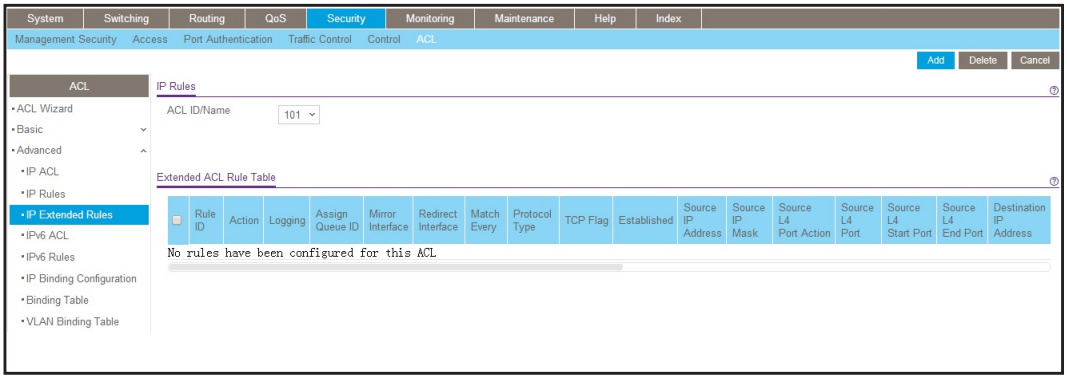
b. In the IP ACL Table, in the **IP ACL ID** field, enter **102**.

c. Click the **Add** button. Your settings are saved.

9. Add and configure an IP extended rule that is associated with ACL 101.

a. Select **Security > ACL > Advanced > IP Extended Rules**.

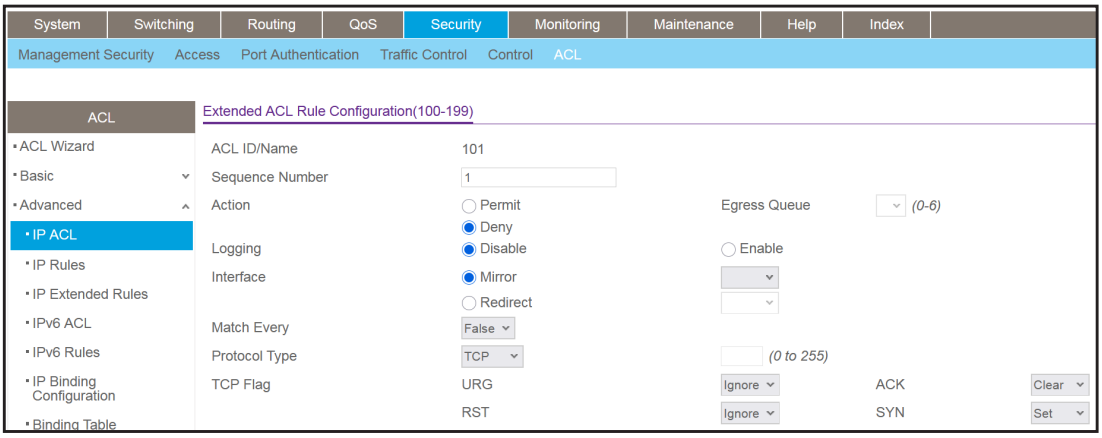
A page similar to the following figure displays.



b. In the **ACL ID/Name** menu, select **101**.

c. Click the **Add** button.

A page similar to the following figure displays.



d. Configure the following settings:

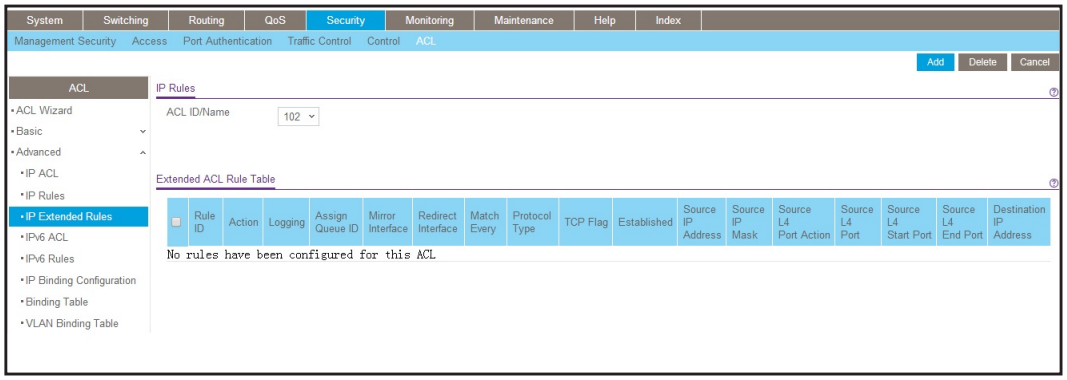
- In the **Sequence Number** field, enter **1**.
- Select the **Action Deny** radio button.
- In the **Match Every** menu, select **False**.
- In the **Protocol Type** menu, select **TCP**.
- For TCP Flag, in the **ACK** menu, select **Clear**, and in the **SYN** menu, select **Set**.

e. Click the **Apply** button. Your settings are saved.

10. Add and configure an IP extended rule that is associated with ACL 102.

a. Select **Security > ACL > Advanced > IP Extended Rules**.

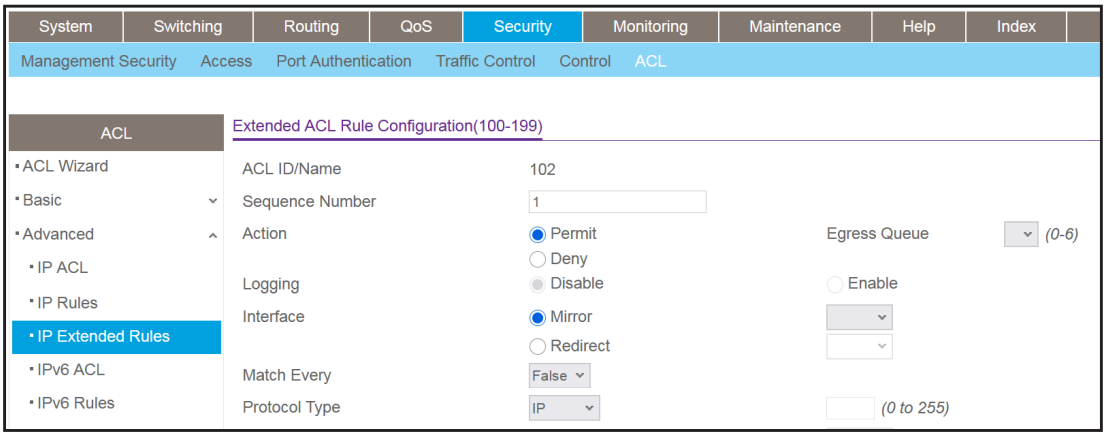
A page similar to the following figure displays.



b. In the **ACL ID/Name** menu, select **102**.

c. Click the **Add** button.

A page similar to the following figure displays.



d. Under Extended ACL Rule Configuration (100-199), enter the following information and make the following selections:

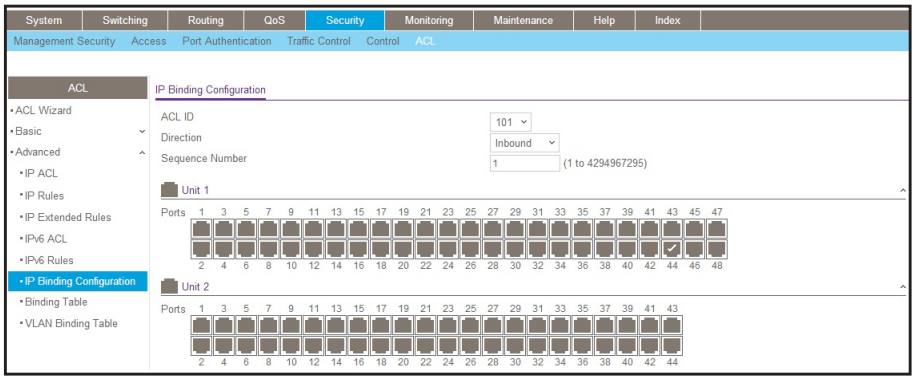
- In the **Sequence Number** field, enter **1**.
- Select the **Action Permit** radio button.
- In the **Match Every** menu, select **False**.
- In the **Protocol Type** menu, select **IP**.

e. Click the **Apply** button. Your settings are saved.

11. Apply ACL 101 to port 44.

a. Select **Security > ACL > Advanced > IP Binding Configuration**.

A page similar to the following figure displays.



b. Under Binding Configuration, specify the following:

- In the **ACL ID** menu, select **101**.
- In the **Sequence Number** field, enter **1**.

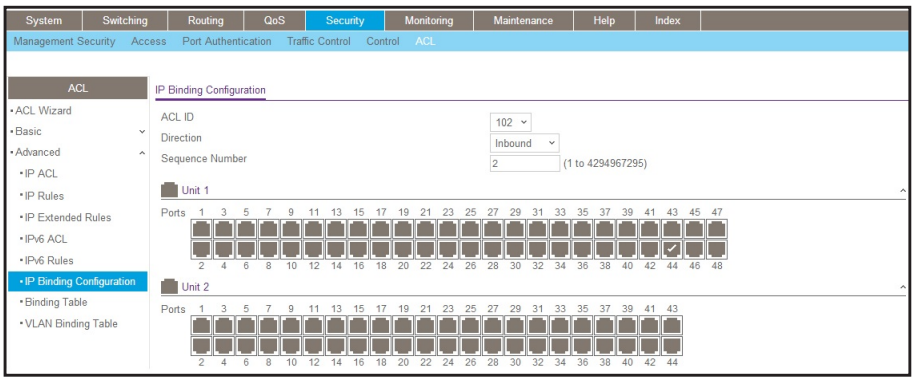
c. Click the gray box under port **44**. A check mark displays in the box.

If your switch is a member of a stack, be sure that you select the port in the correct unit.

d. Click the **Apply** button. Your settings are saved.

12. Apply ACL 102 to port 44.

a. Remain on the same page.



b. Under Binding Configuration, configure the following settings:

- In the **ACL ID** menu, select **102**.
- In the **Sequence Number** field, enter **2**.

c. Click the gray box under port **44**. A check mark displays in the box.

If your switch is a member of a stack, be sure that you select the port in the correct unit.

d. Click the **Apply** button. Your settings are saved.

Main UI Step 2: Configure VLANs, IP addresses, and static routes on Switch B

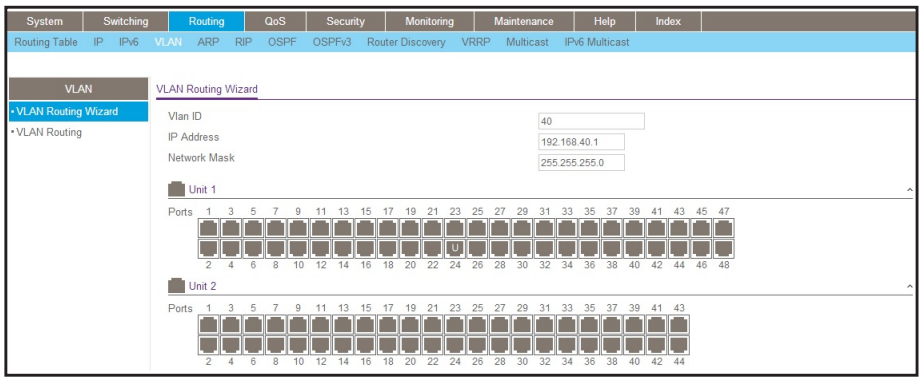
Also see Figure 23, One-Way Web access using a TCP flag in an ACL.

To use the CLI to configure VLANs, IP addresses, and static routes on Switch B:

1. Create VLAN 40 with IP address 192.168.40.1/24.

a. Select **Routing > VLAN > VLAN Routing Wizard**.

A page similar to the following figure displays.



b. Configure the following settings:

- 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**.

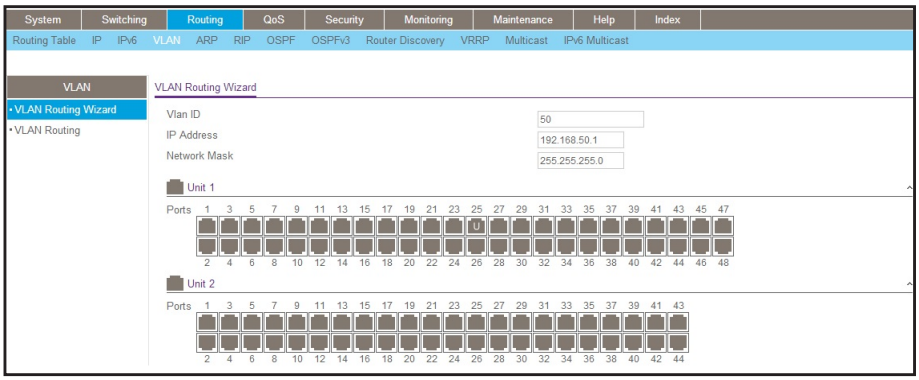
c. Click the gray box under port **24** until U displays, specifying that the egress packets are untagged for the port.

If your switch is a member of a stack, be sure that you select the ports in the correct unit.

d. Click the **Apply** button. Your settings are saved.

2. Create VLAN 50 with IP address 192.168.50.1/24:

a. Remain on the same page.



b. Configure the following settings:

- 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**.

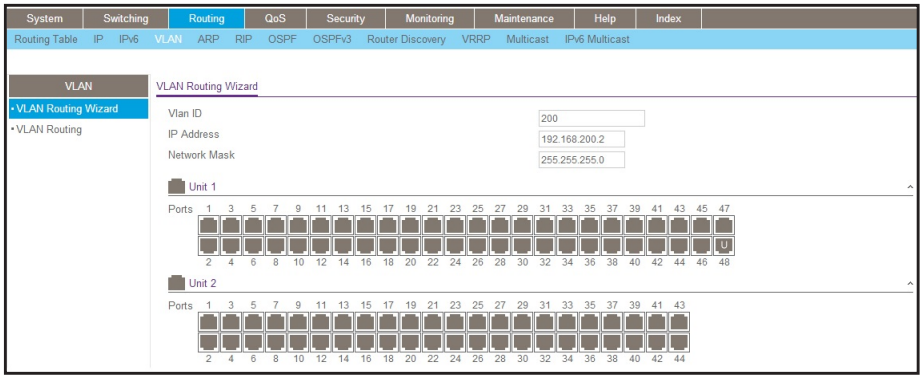
c. Click the gray box under port **25** until U displays, specifying that the egress packets are untagged for the port.

If your switch is a member of a stack, be sure that you select the ports in the correct unit.

d. Click the **Apply** button. Your settings are saved.

3. Create VLAN 200 with IP address 192.168.200.2/24.

a. Remain on the same page.



b. Configure the following settings:
   - 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 the gray box under port **48** until U displays, specifying that the egress packets are untagged for the port.

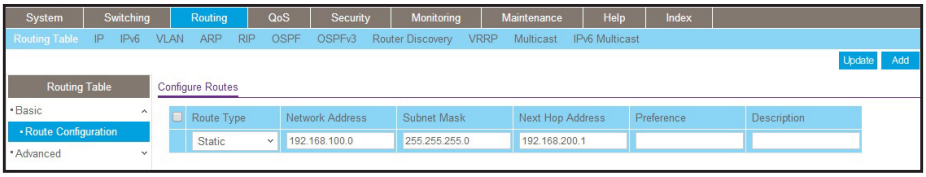
   If your switch is a member of a stack, be sure that you select the ports in the correct unit.

d. Click the **Apply** button. Your settings are saved.

4. Create a static route with IP address 192.168.100.0/24:

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

   A page similar to the following figure displays.

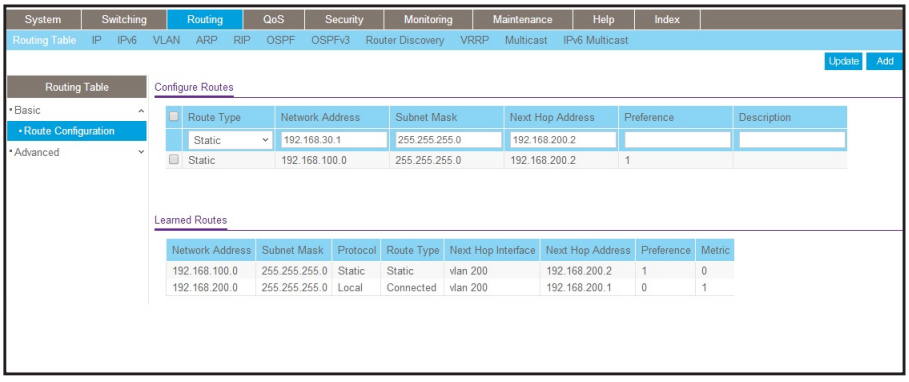


b. Under Configure Routes, configure the following settings:
   - In the **Route Type** menu, select **Static**.
   - In the **Network Address** field, enter **192.168.100.0**.
   - In the **Subnet Mask** field, enter **255.255.255.0**.
   - In the **Next Hop IP Address** field, enter **192.168.200.1**.

c. Click the **Add** button. Your settings are saved.

5. Create a static route with IP address 192.168.30.0/24:

a. Remain on the same page.



b. Under Configure Routes, configure the following settings:
   - 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 the **Add** button. Your settings are saved.

Use ACLs to isolate VLANs on a Layer 3 switch

This example shows how to isolate VLANs on a Layer 3 switch by using ACLs. In this example, Desktop 1 is in VLAN 24, Desktop 2 is in VLAN 48, and the server is in VLAN 38. Desktop 1 and Desktop 2 are isolated by an ACL but can both access the server.

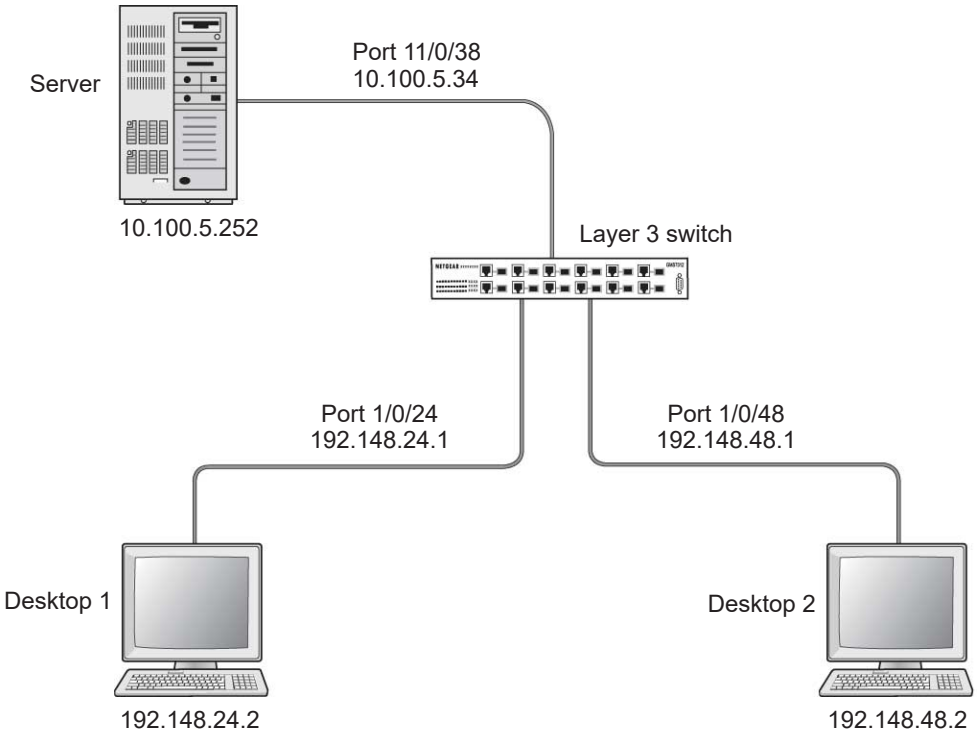


Figure 24. Using ACLs to isolate VLANs on a Layer 3 switch

The example is shown as CLI commands and as a main UI procedure.

CLI: Configure ACLs that isolate VLANs

To use the CLI to configure ACLs that isolate VLANs:

1. Create VLAN 24, add port 1/0/24 to the VLAN, and assign IP address 192.168.24.1 to it.

```
(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 the VLAN, 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 the VLAN, 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. On interface 1/0/24, 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. On interface 1/0/48, deny all traffic with the destination IP address 192.168.24.0/24, and permit all other traffic.

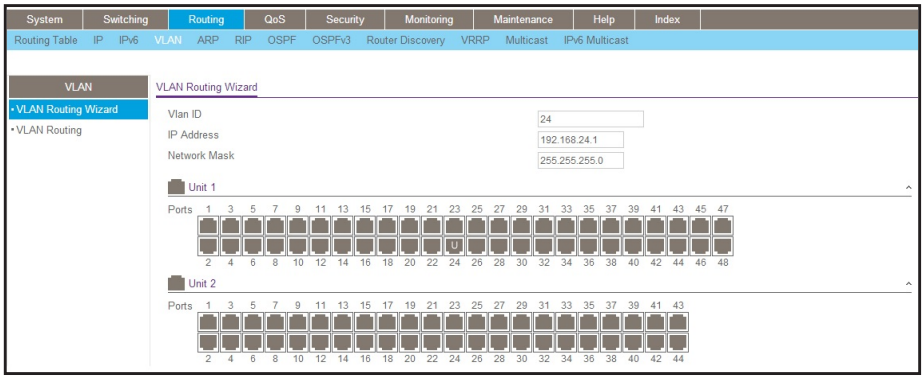
```
(Netgear Switch) (Config)#interface 1/0/48
(Netgear Switch) (Interface 1/0/48)#ip access-group 101 in 1
(Netgear Switch) (Interface 1/0/48)#ip access-group 103 in 2
(Netgear Switch) (Interface 1/0/48)#exit
```

Main UI: Configure ACLs that isolate VLANs

To use the main UI to configure ACLs that isolate VLANs:

1. Create VLAN 24 with IP address 192.168.24.1.
   a. Select **Routing > VLAN > VLAN Routing Wizard**.

      A page similar to the following figure displays.



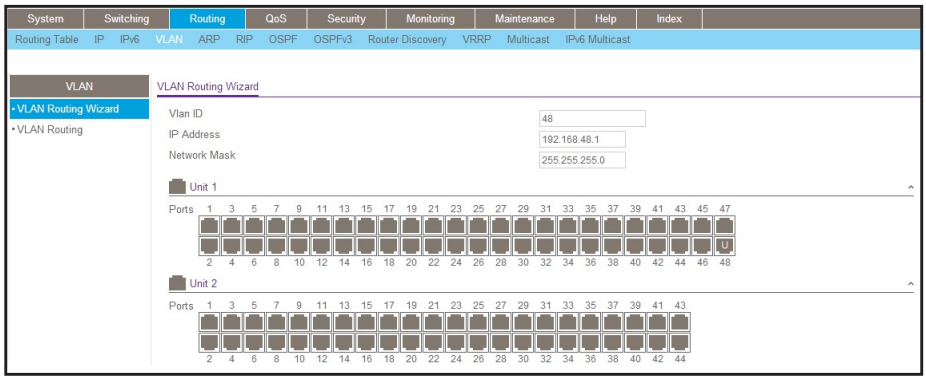
   b. Configure the following settings:
      - In the **VLAN ID** field, enter **24**.
      - In the **IP Address** field, enter **192.168.24.1**.
      - In the **Network Mask** field, enter **255.255.255.0**.

   c. Click the gray box under port **24** until U displays, specifying that the egress packets are untagged for the port.

      If your switch is a member of a stack, be sure that you select the ports in the correct unit.

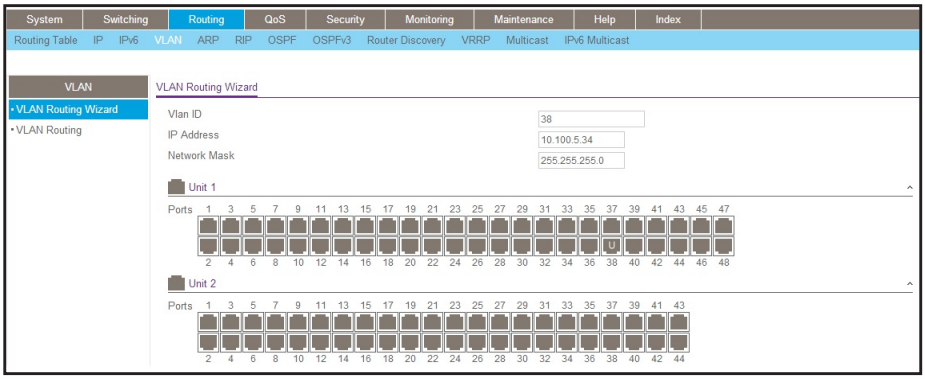
   d. Click the **Apply** button. Your settings are saved.

2. Create VLAN 48 with IP address 192.168.48.1.
   a. Remain on the same page.



   b. Configure the following settings:
      - 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 the gray box under port **48** until U displays, specifying that the egress packets are untagged for the port.

      If your switch is a member of a stack, be sure that you select the ports in the correct unit.
   d. Click the **Apply** button. Your settings are saved.
3. Create VLAN 38 with IP address 10.100.5.34.
   a. Remain on the same page.



   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 the gray box under port **38** until U displays, specifying that the egress packets are untagged for the port.

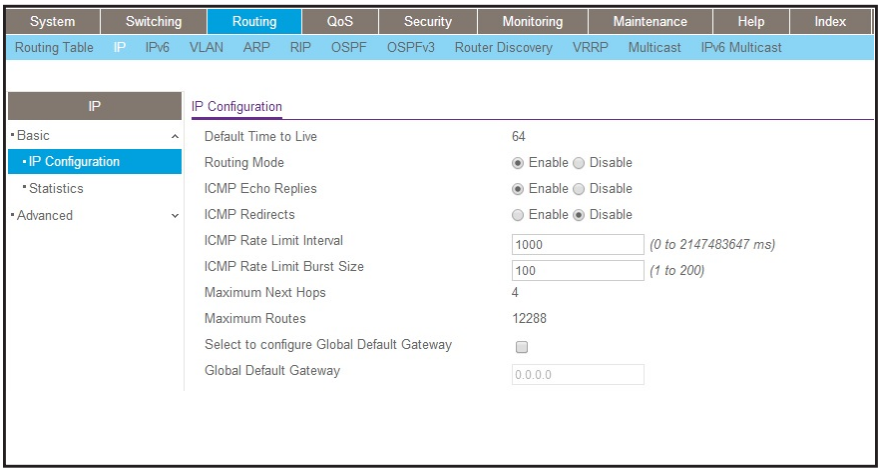
If your switch is a member of a stack, be sure that you select the ports in the correct unit.

d. Click the **Apply** button. Your settings are saved.

4. Enable IP routing:

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

A page similar to the following figure displays.



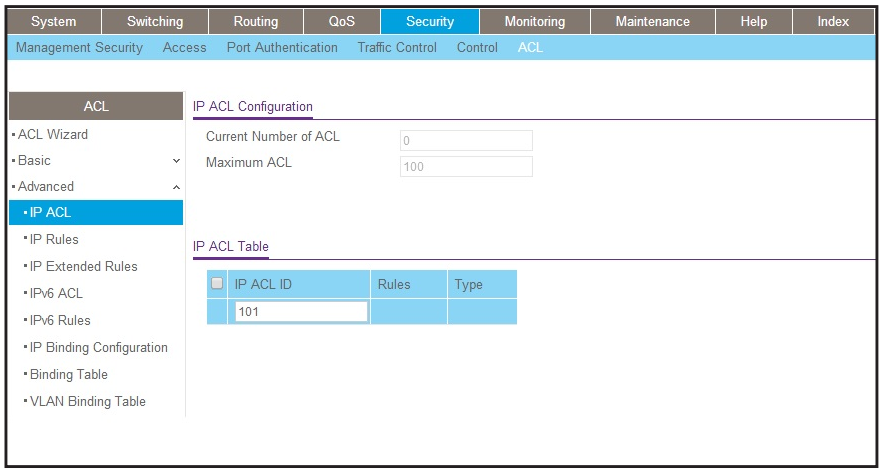
b. Select the Routing Mode **Enable** radio button.

c. Click the **Apply** button. Your settings are saved.

5. Create an ACL with ID 101.

a. Select **Security > ACL > Advanced > IP ACL**.

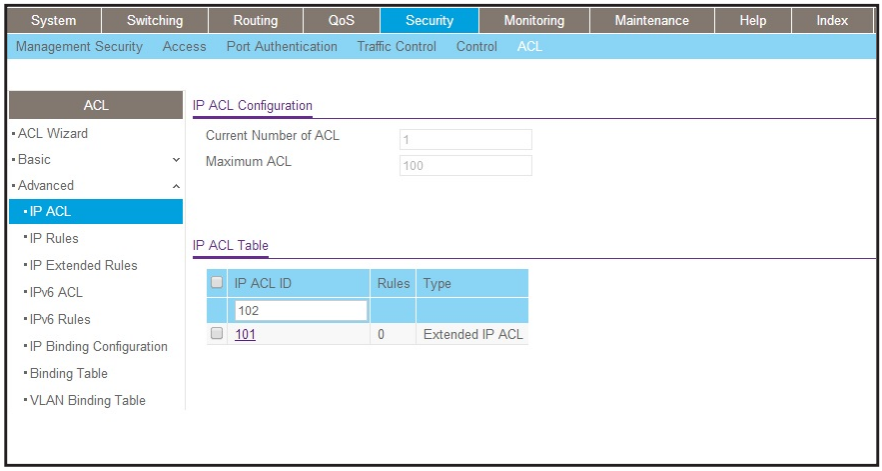
A page similar to the following figure displays.



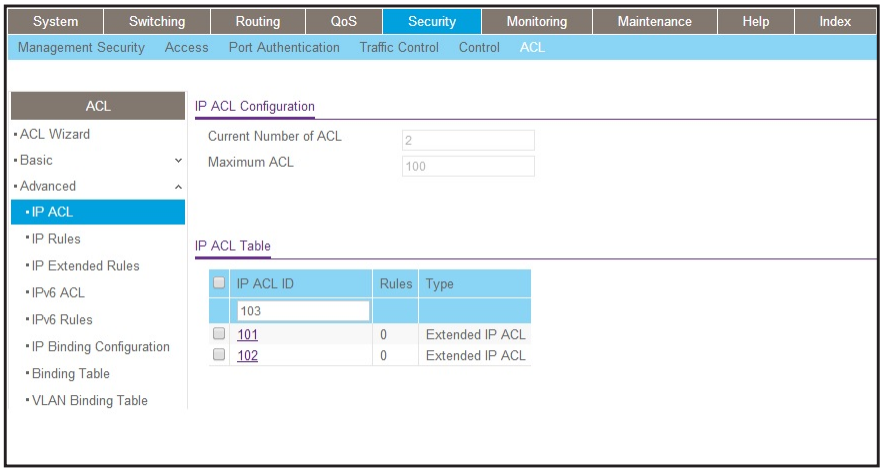
b. In the IP ACL Table, in the **IP ACL ID** field, enter **101**.

c. Click the **Add** button. Your settings are saved.

6. Create an ACL with ID 102.
   a. Remain on the same page.

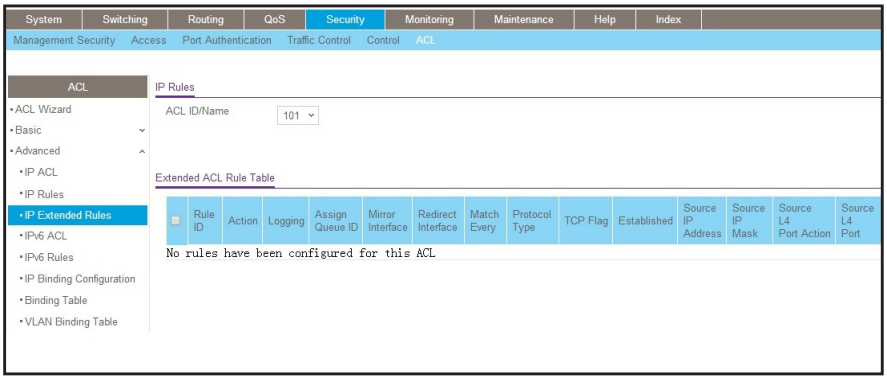


   b. In the IP ACL Table, in the **IP ACL ID** field, enter **102**.
   c. Click the **Add** button. Your settings are saved.
7. Create an ACL with ID 103.
   a. Remain on the same page.



   b. In the **IP ACL ID** field of the IP ACL Table, enter **103**.
   c. Click the **Add** button. Your settings are saved.
8. Add and configure an IP extended rule that is associated with ACL 101:
   a. Select **Security > ACL > Advanced > IP Extended Rules**.

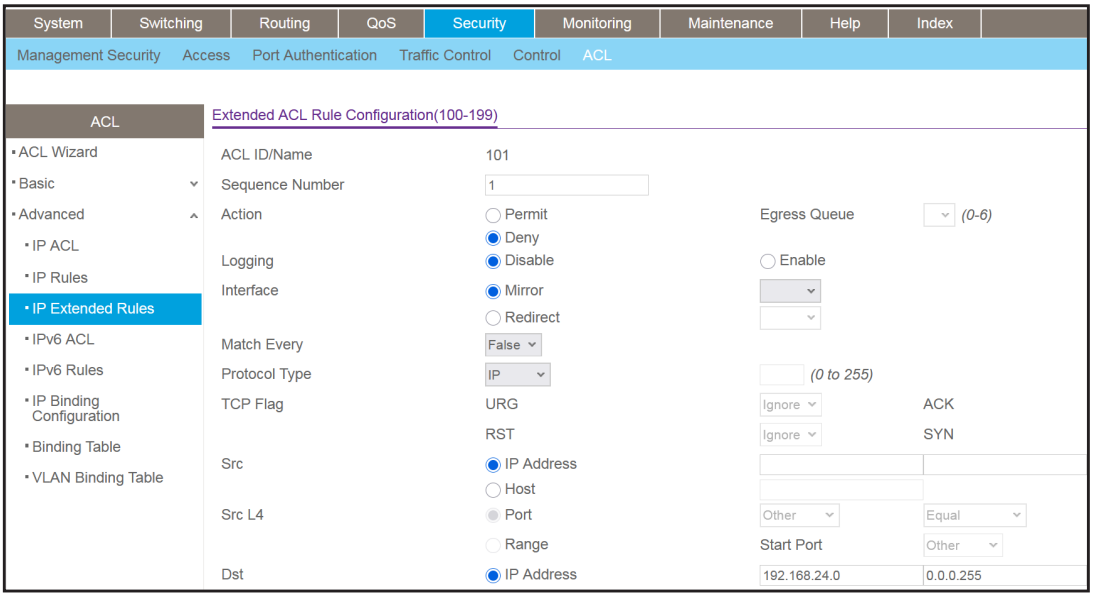
A page similar to the following figure displays.



b. In the **ACL ID/Name** menu, select **101**.

c. Click the **Add** button.

A page similar to the following figure displays.



d. Under Extended ACL Rule Configuration (100-199), configure the following settings:

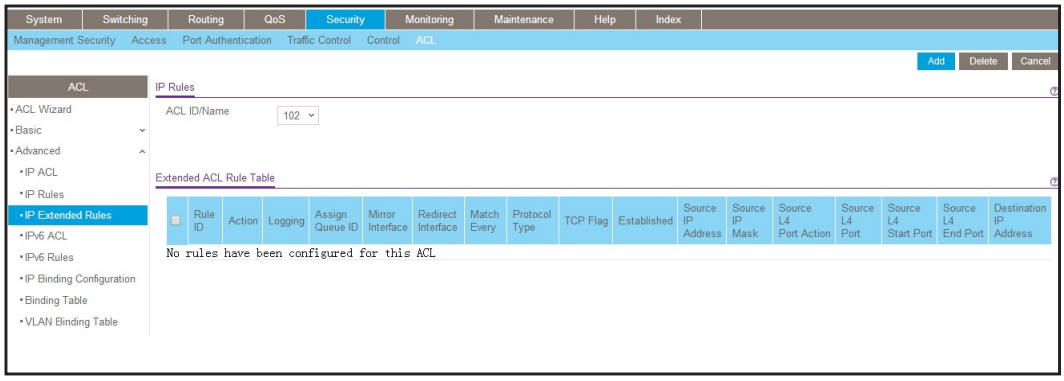
- In the **Sequence Number** field, enter **1**.
- Select the **Action Deny** radio button.
- In the **Match Every** menu, select **False**.
- In the **Protocol Type** menu, select **IP**.
- In the **Dst IP Address** field, enter **192.168.24.0**.
- In the destination subnet mask field to the right, enter **0.0.0.255**.

e. Click the **Apply** button. Your settings are saved.

9. Add and configure an IP extended rule that is associated with ACL 102.

a. Select **Security > ACL > Advanced > IP Extended Rules**.

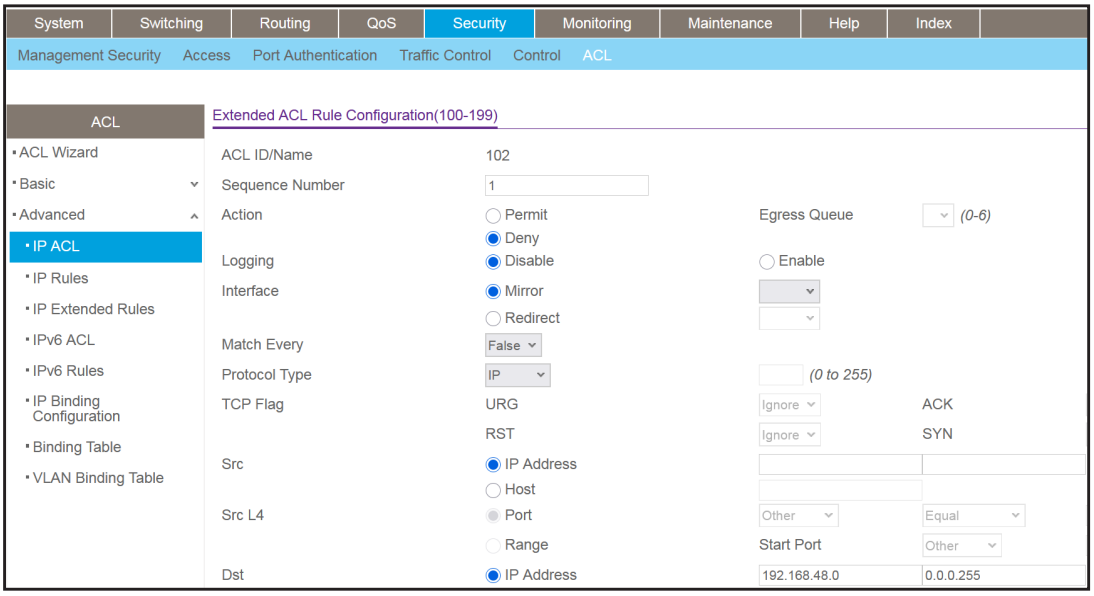
A page similar to the following figure displays.



b. In the **ACL ID/Name** menu, select **102**.

c. Click the **Add** button.

A page similar to the following figure displays.



d. Under Extended ACL Rule Configuration (100-199), enter the following information and make the following selections:

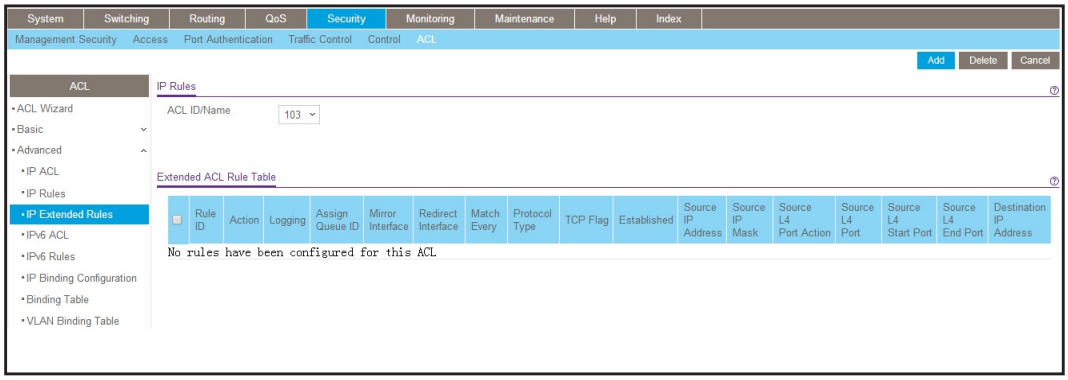
- In the **Sequence Number** field, enter **1**.
- Select the **Action Deny** radio button.
- In the **Match Every** menu, select **False**.
- In the **Dst IP Address** field, enter **192.168.48.0**.
- In the destination subnet mask field to the right, enter **0.0.0.255**.

e. Click the **Apply** button. Your settings are saved.

10. Add and configure an IP extended rule that is associated with ACL 103:

a. Select **Security > ACL > Advanced > IP Extended Rules**.

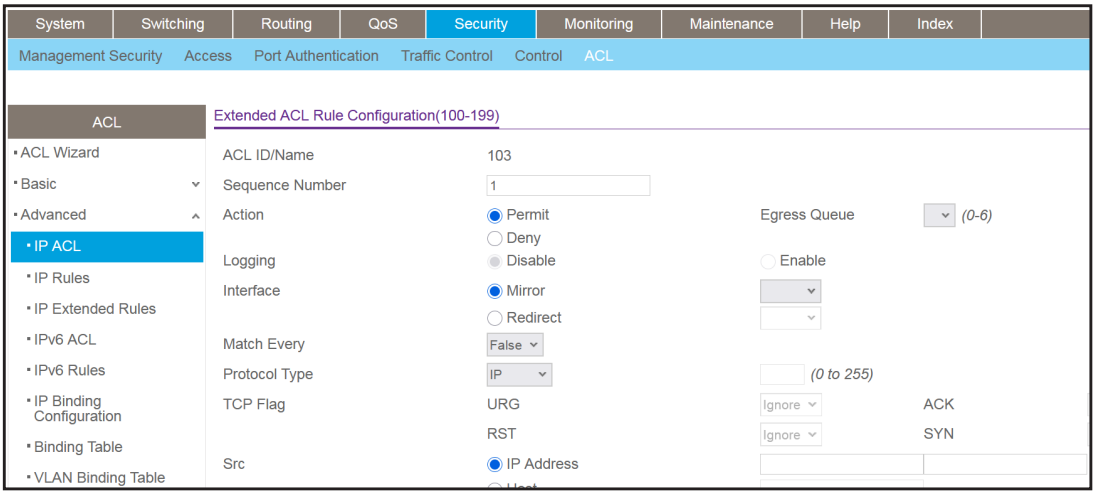
A page similar to the following figure displays.



b. In the **ACL ID/Name** menu, select **103**.

c. Click the **Add** button.

A page similar to the following figure displays.



d. Under Extended ACL Rule Configuration (100-199), enter the following information and make the following selections:

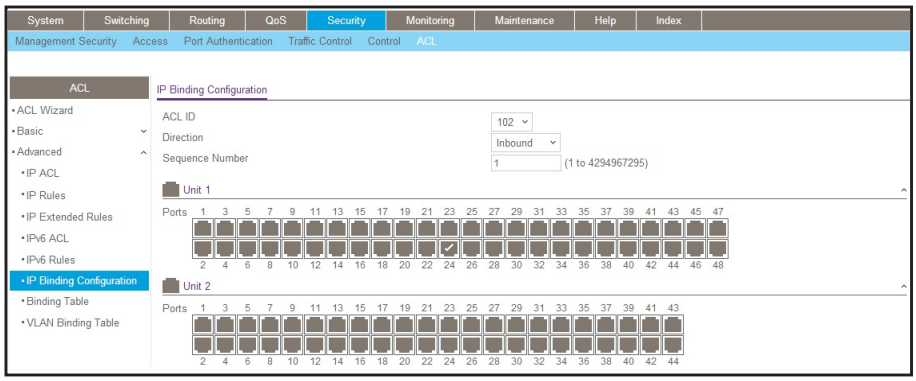
- In the **Sequence Number** field, enter **1**.
- Select the **Action Permit** radio button.
- In the **Match Every** menu, select **False**.
- In the **Protocol Type** menu, select **IP**.

e. Click the **Apply** button. Your settings are saved.

11. Apply ACL 102 to port 24:

a. Select **Security > ACL > Advanced > IP Binding Configuration**.

A page similar to the following figure displays.



b. Under Binding Configuration, configure the following settings:

- In the **ACL ID** menu, select **102**.
- In the **Sequence Number** field, enter **1**.

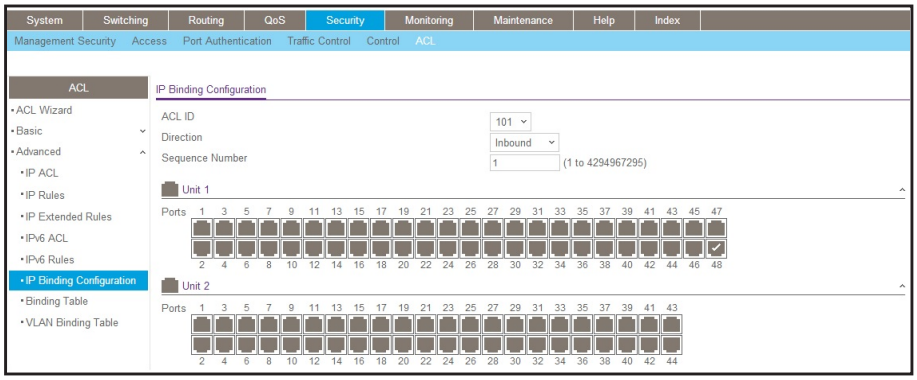
c. Click the gray box under port **24**. A check mark displays in the box.

If your switch is a member of a stack, be sure that you select the port in the correct unit.

d. Click the **Apply** button. Your settings are saved.

12. Apply ACL 101 to port 48:

a. Remain on the same page.



b. Under Binding Configuration, configure the following settings:

- In the **ACL ID** menu, select **101**.
- In the **Sequence Number** field, enter **1**.

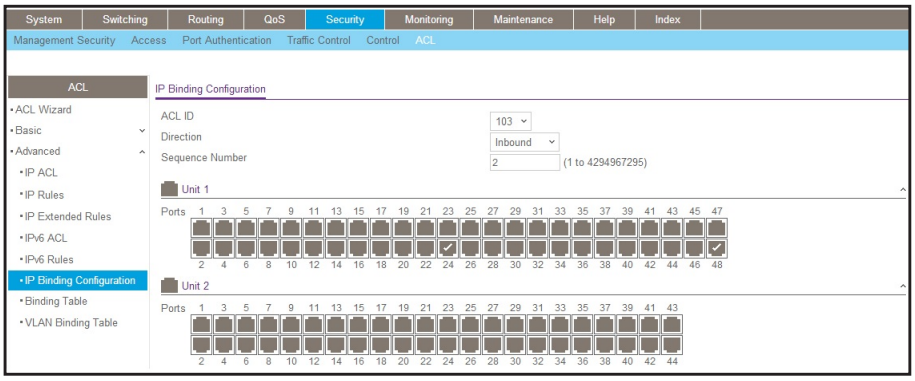
c. Click the gray box under port **48**. A check mark displays in the box.

If your switch is a member of a stack, be sure that you select the port in the correct unit.

d. Click the **Apply** button. Your settings are saved.

13. Apply ACL 103 to port 24 and port 48.

a. Remain on the same page.



b. Under Binding Configuration, configure the following settings:

- In the **ACL ID** menu, select **103**.
- In the **Sequence Number** field, enter **2**.

c. Click the gray boxes under ports **24** and **48**. A check mark displays in each box.

If your switch is a member of a stack, be sure that you select the ports in the correct unit.

d. Click the **Apply** button. Your settings are saved.

Set up a MAC ACL with two rules

The example is shown as CLI commands and as a main UI procedure.

CLI: Set up a MAC ACL with two rules

To use the CLI to 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 for 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.

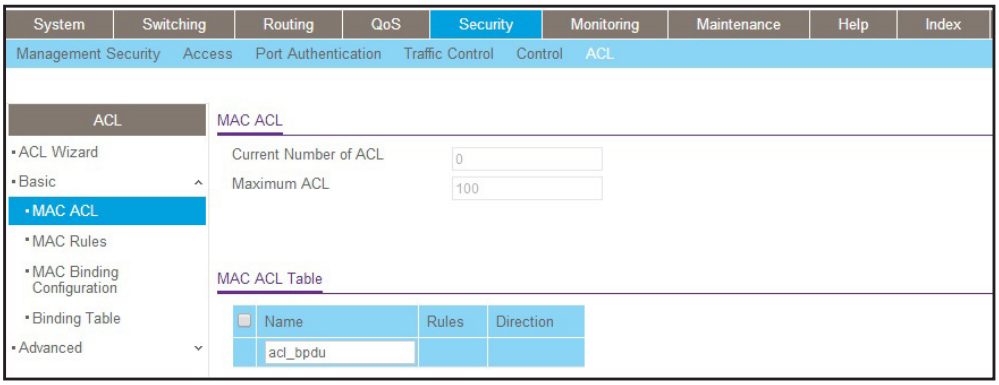
```
(Netgear Switch) (Config)#interface 1/0/2
(Netgear Switch) (Interface 1/0/2)#mac access-group acl_bpdu in
```

Main UI: Set up a MAC ACL with two rules

To use the main UI to set up a MAC ACL with two rules:

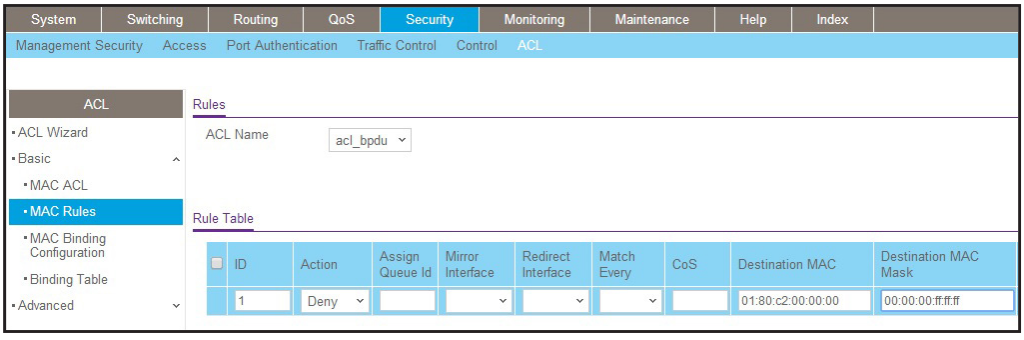
1. Create MAC ACL 101 on the switch.
   a. Select **Security > ACL > Basic > MAC ACL**.

      A page similar to the following figure displays.



   b. In the **Name** field, enter **acl_bpdu**.
   c. Click the **Add** button. Your settings are saved.
2. Create a new rule that is associated with the ACL acl_bpdu.
   a. Select **Security > ACL > Basic > MAC ACL > MAC Rules**.

      A page similar to the following figure displays.



b. In the **ACL Name** menu, select **acl_bpdu**.

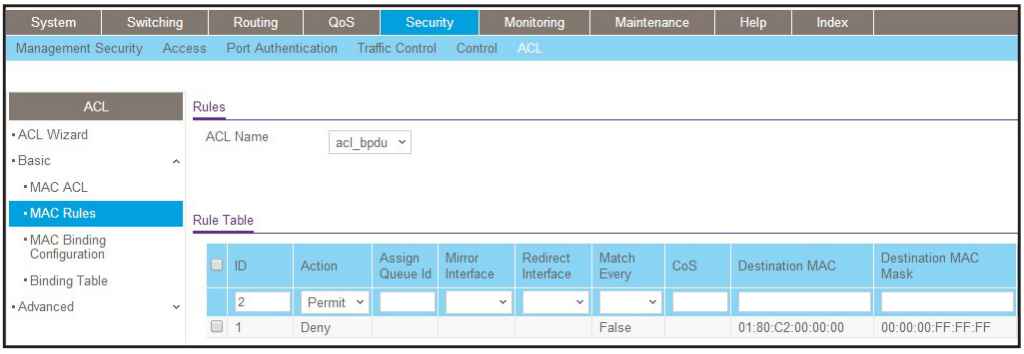
c. Enter the following information in the Rule Table.

- In the **Sequence Number** field, enter **1**.
- In the **Action** menu, select **Deny**.
- 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. Your settings are saved.

3. Create another rule that is associated with the ACL acl_bpdu.

a. Remain on the same page.



b. In the **ACL Name** menu, select **acl_bpdu**.

c. Enter the following information in the Rule Table.

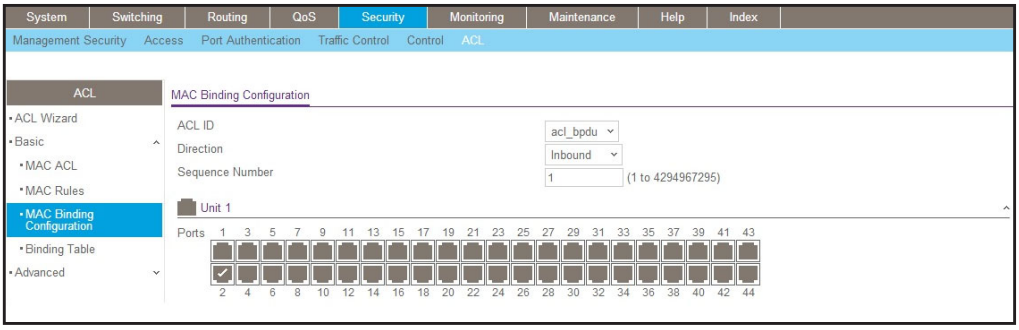
- In the **Sequence Number** field, enter **2**.
- In the **Action** menu, select **Permit**.

d. Click the **Add** button. Your settings are saved.

4. Apply the ACL acl_bpdu to port 2.

a. Select **Security > ACL > Basic > MAC ACL > MAC Binding Configuration**.

A page similar to the following figure displays.



b. Enter the following information in the MAC Binding Configuration.

- In the **ACL ID** menu, select **acl_bpdu**.
- In the **Sequence Number** field, enter **1**.

c. Click the gray box under port **2**. A check mark displays in the box.

If your switch is a member of a stack, be sure that you select the port in the correct unit.

d. Click the **Apply** button. Your settings are saved.

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.

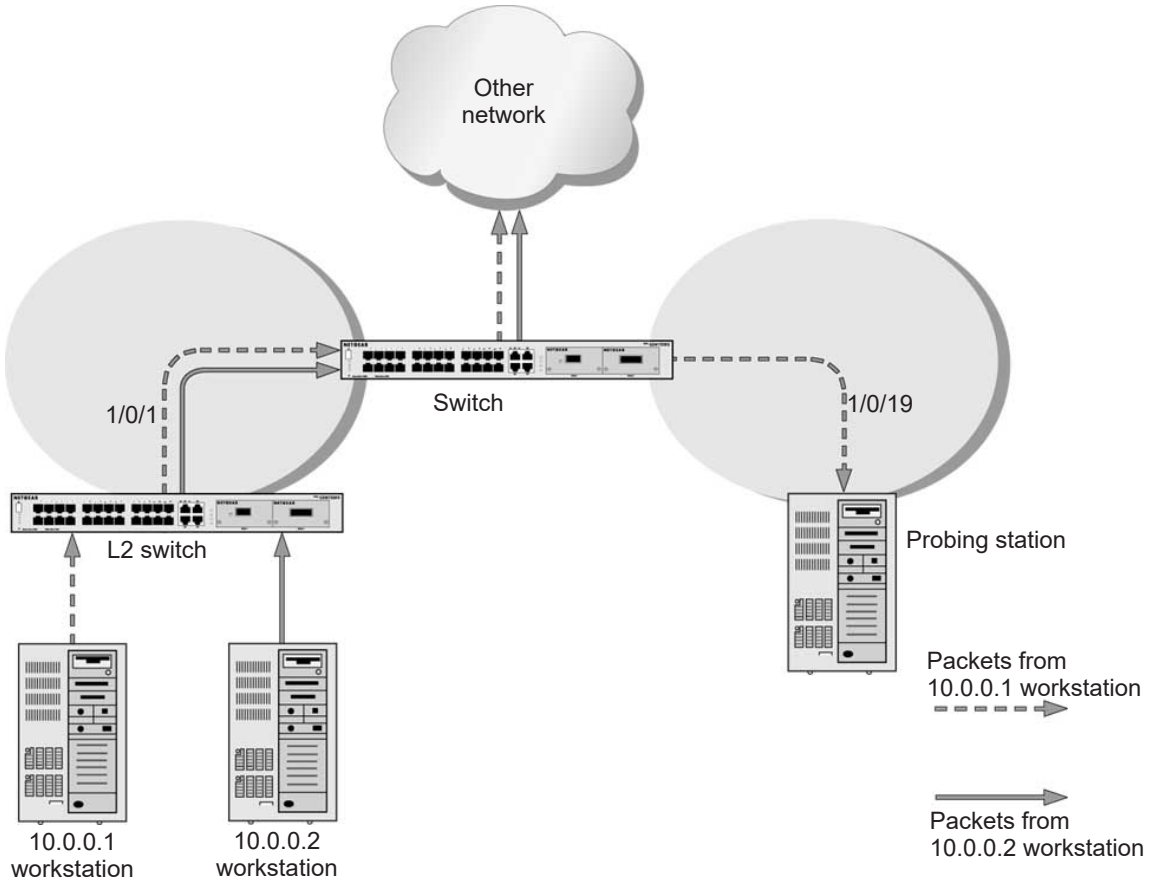


Figure 25. ACL mirroring

The example is shown as CLI commands and as a main UI procedure.

CLI: Configure ACL mirroring

To use the CLI to 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 to interface 1/0/1.

```
(Netgear Switch) (Interface 1/0/1)#ip access-group monitorHost in 1
```

4. Display the configuration.

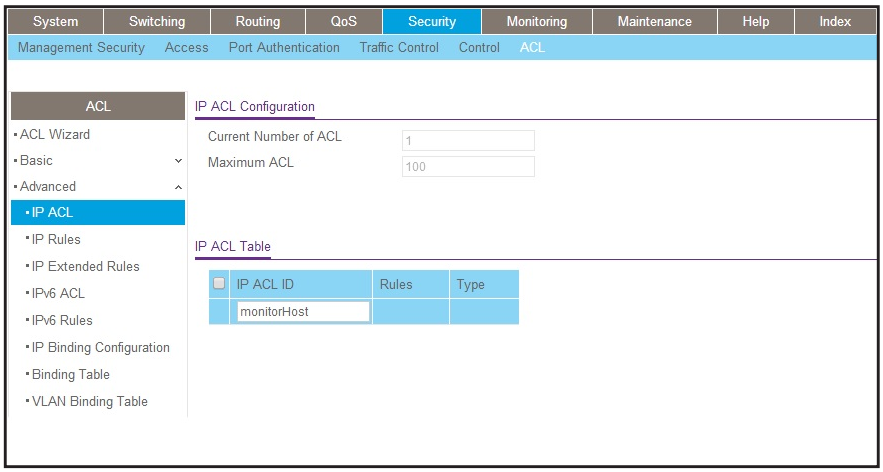
```
(Netgear Switch) # show ip access-lists
Current number of ACLs: 1  Maximum number of ACLs: 100

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
```

Main UI: Configure ACL mirroring

To use the main UI to configure ACL mirroring:

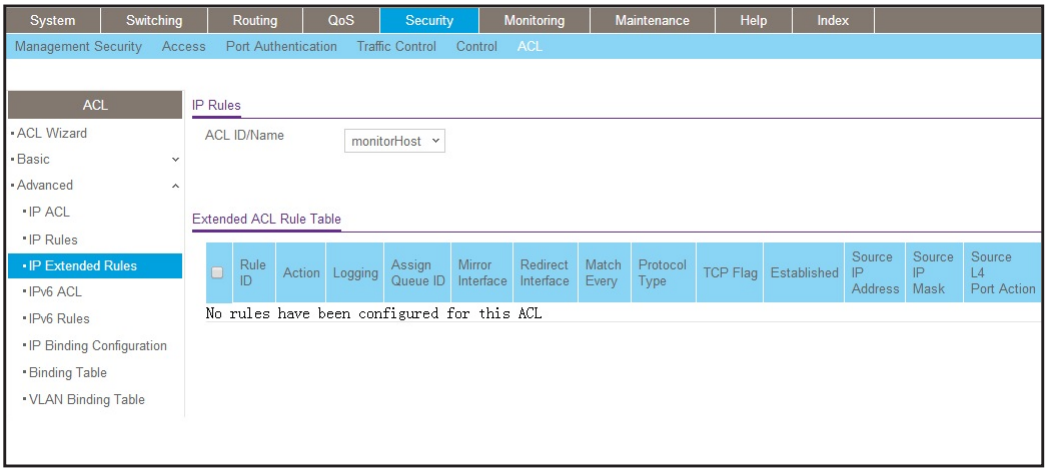
1. Create an IP access control list with the name monitorHost on the switch.
   a. Select **Security > ACL > Advanced > IP ACL**.

      A page similar to the following figure displays.



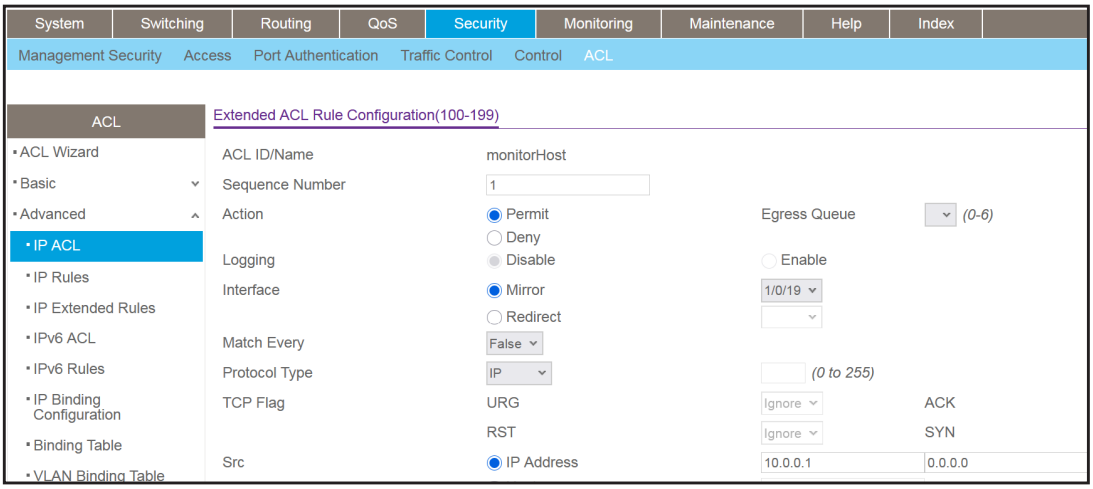
   b. In the **IP ACL ID** field, enter **monitorHost**.
   c. Click the **Add** button. Your settings are saved.
2. Create a rule to match host 10.0.0.1 in the ACL monitorHost.
   a. Select **Security > ACL > Advanced > IP Extended Rules**.

      A page similar to the following figure displays.



   b. In the **ACL ID/Name** menu, select **monitorHost**.
   c. Click the **Add** button.

A page similar to the following figure displays.



d. In the **Sequence Number** field, enter **1**.

e. Select the **Action Permit** radio button.

f. Select the **Interface Mirror** radio button, and in the associated menu, select **1/0/19**.

g. In the **Match Every** menu, select **False**.

h. In the **Protocol Type** menu, select **IP**.

i. In the **Src IP Address** field, enter **10.0.0.1**.

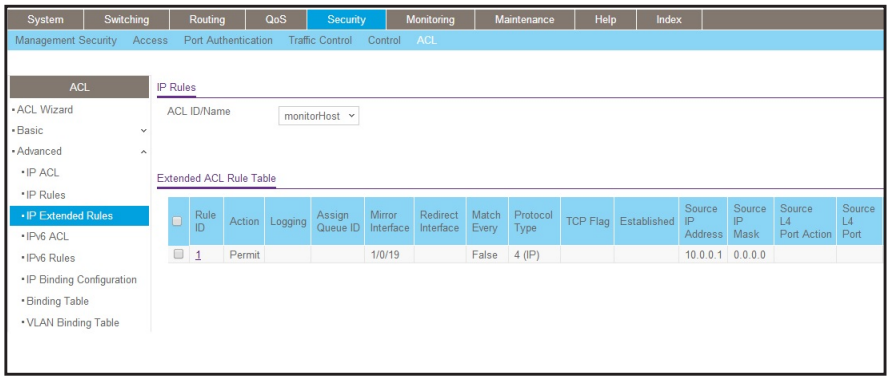
j. In the source subnet mask field to the right, enter **0.0.0.0**.

k. Click the **Apply** button. Your settings are saved.

3. Create a rule to match all other traffic.

a. Select **Security > ACL > Advanced > IP Extended Rules**.

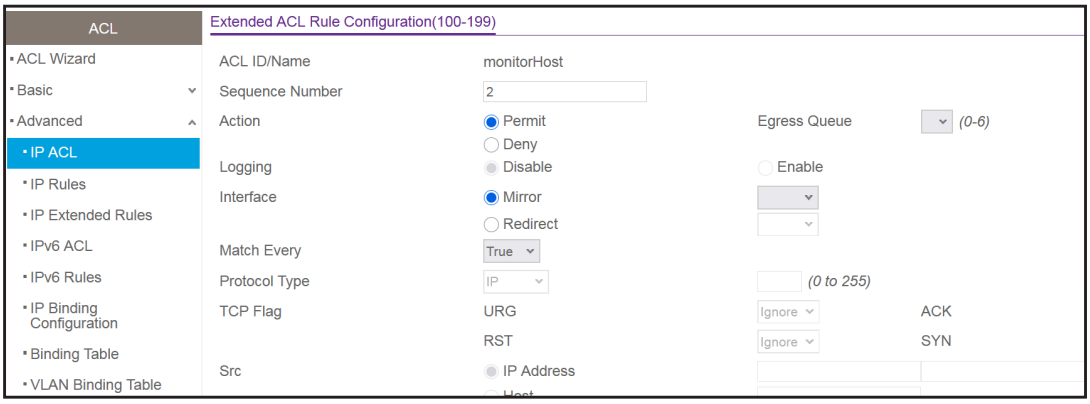
A page similar to the following figure displays.



b. In the **ACL ID/Name** menu, select **monitorHost**.

c. Click the **Add** button.

A page similar to the following figure displays.



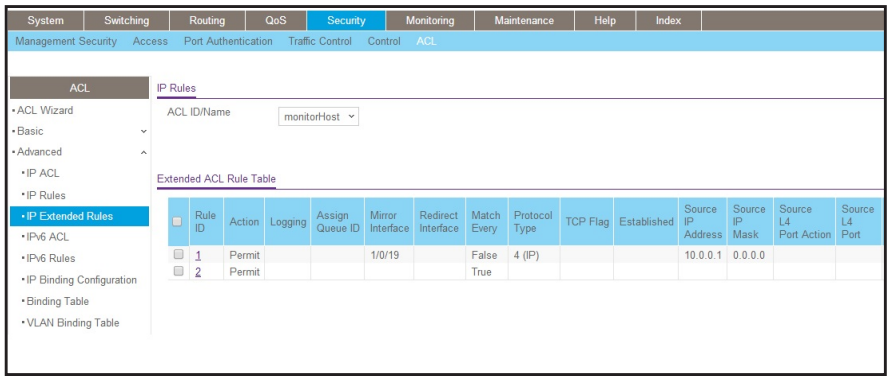
d. In the **Sequence Number** field, enter **2**.

e. Select the **Action Permit** radio button.

f. In the **Match Every** menu, select **True**.

g. Click the **Apply** button. Your settings are saved.

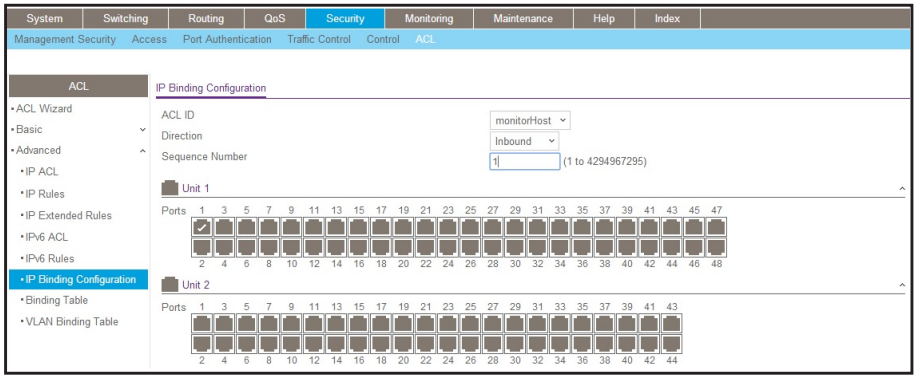
A page similar to the following figure displays.



4. Bind the ACL to interface 1/0/1.

a. Select **Security > ACL > Advanced > IP Binding Configuration**.

A page similar to the following figure displays.



b. In the **ACL ID** menu, select **monitorHost**.

c. In the **Sequence Number** field, enter **1**.

d. Click the gray box under port **1**. A check mark displays in the box.

If your switch is a member of a stack, be sure that you select the port in the correct unit.

e. Click the **Apply** button. Your settings are saved.

Configure ACL redirection for a traffic stream

This feature redirects a specified traffic stream to a specified interface.

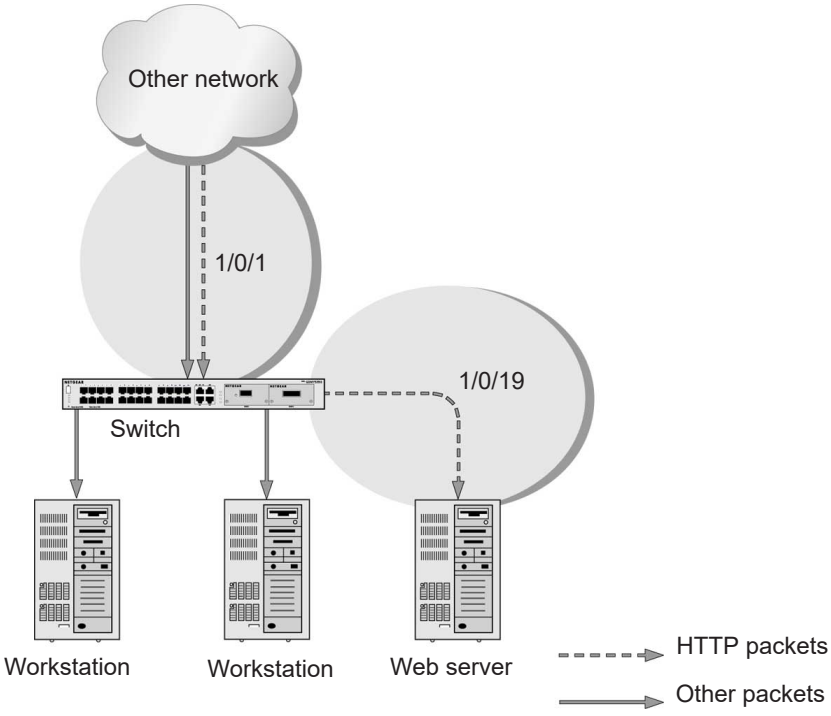


Figure 26. ACL Redirect

The example is shown as CLI commands and as a main UI procedure.

CLI: Configure an ACL that redirects a traffic stream

To use the CLI to redirect an HTTP traffic stream that is received on one interface (1/0/1) to another interface (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 to interface 1/0/1.

```
(Netgear Switch) (Interface 1/0/1)#ip access-group redirectHTTP in 1
```

4. Display the configuration.

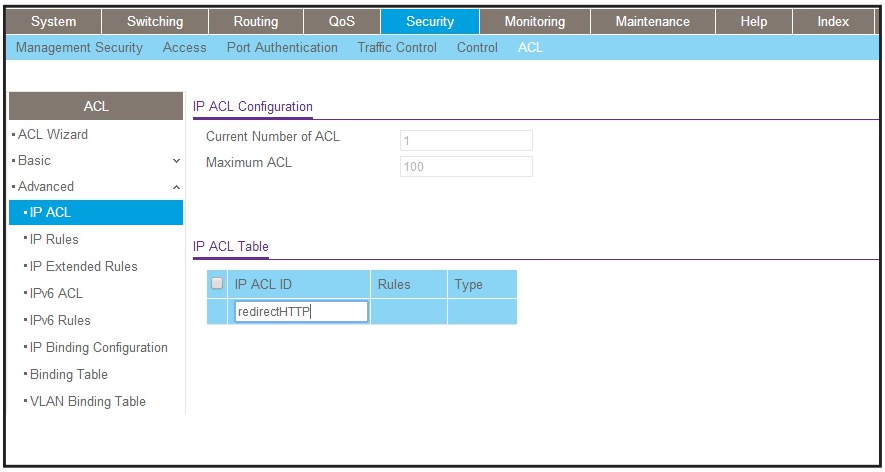
```
(Netgear Switch) # show ip access-lists
Current number of ACLs: 1  Maximum number of ACLs: 100

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
```

Main UI: Configure an ACL that redirects a traffic stream

To use the main UI to redirect an HTTP traffic stream that is received on one interface (1/0/1) to another interface (1/0/19):

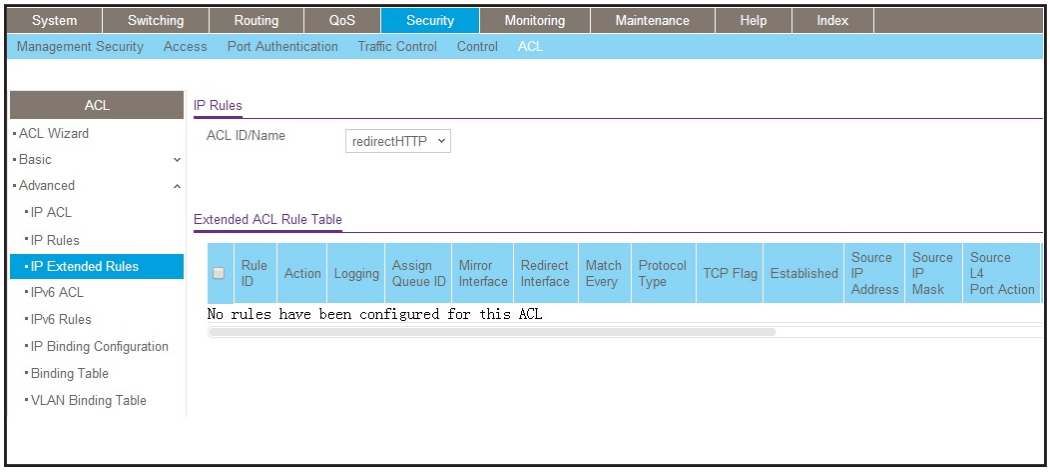
1. Create an IP access control list with the name redirectHTTP.
   a. Select **Security > ACL > Advanced > IP ACL**.

      A page similar to the following figure displays.



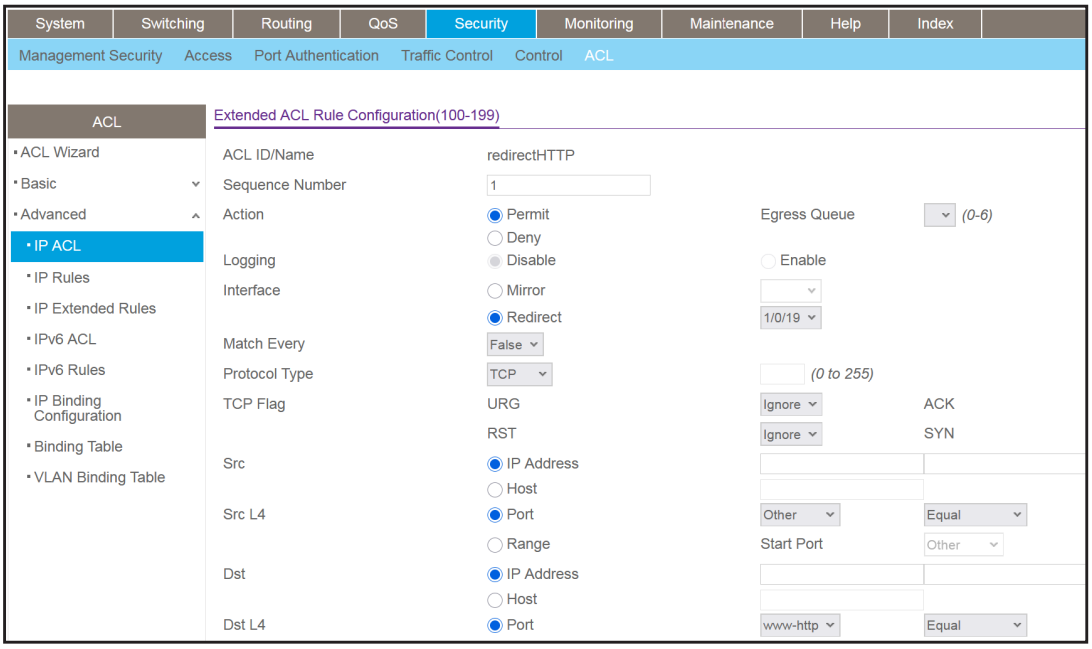
   b. In the **IP ACL** field, enter **redirectHTTP**.
   c. Click the **Add** button. Your settings are saved.
2. Create a rule to redirect HTTP traffic.
   a. Select **Security > ACL > Advanced > IP Extended Rules**.

      A page similar to the following figure displays.



   b. In the **ACL ID/Name** menu, select **redirectHTTP**.
   c. Click the **Add** button.

A page similar to the following figure displays.



d. In the **Sequence Number** field, enter **1**.

e. Select the **Action Permit** radio button.

f. Select the **Interface Redirect** radio button, and in the associated menu, select **1/0/19**.

g. In the **Match Every** menu, select **False**.

h. In the **Protocol Type** menu, select **TCP**.

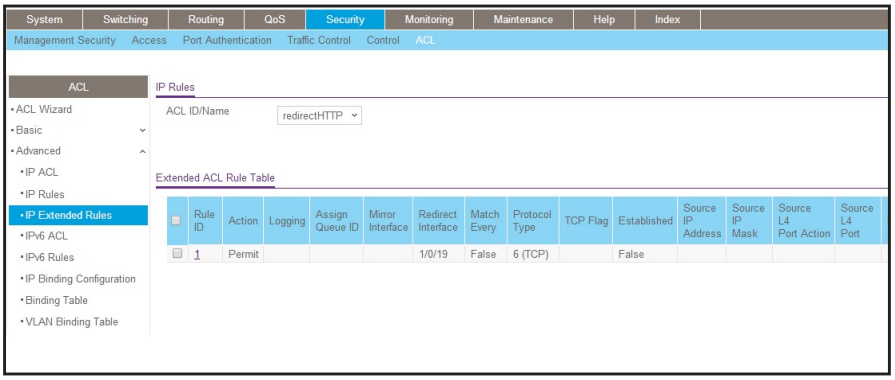
i. Select the **Dst L4 Port** radio button, and in the associated menu, select **www-http**.

j. Click the **Apply** button. Your settings are saved.

3. Create a rule to match all other traffic.

a. Select **Security > ACL > Advanced > IP Extended Rules**.

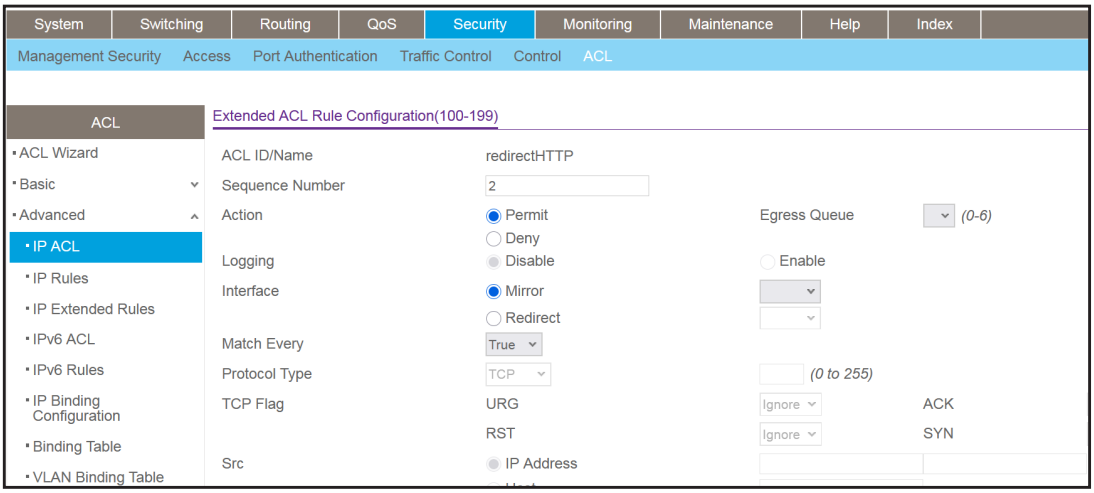
A page similar to the following figure displays.



b. In the **ACL ID/Name** menu, select **redirectHTTP**.

c. Click the **Add** button.

A page similar to the following figure displays.



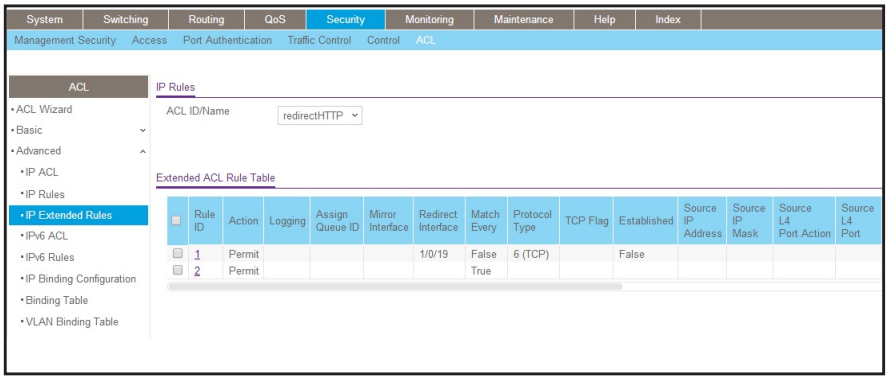
d. In the **Sequence Number** field, enter **2**.

e. Select the **Action Permit** radio button.

f. In the **Match Every** menu, select **True**.

g. Click the **Apply** button. Your settings are saved.

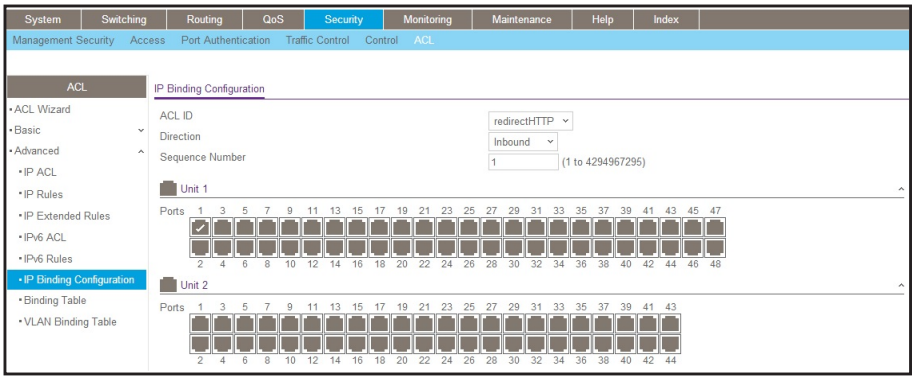
A page similar to the following figure displays.



4. Bind the ACL to interface 1/0/1.

a. Select **Security > ACL > Advanced > IP Binding Configuration**.

A page similar to the following figure displays.



b. In the **Sequence Number** field, enter **1**.

c. Click the gray box under port **1**. A check mark displays in the box.

If your switch is a member of a stack, be sure that you select the port in the correct unit.

d. Click the **Apply** button. Your settings are saved.

Add ACL remarks

In the CLI, 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.

The main UI does not provide the option to add remarks.

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.

To use the CLI to add remarks to ACL rules:

1. Create an ACL.

```
(Netgear Switch) (Config)#ip access-list acl_voice
```

2. Add remarks before you add rules.

```
(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. Display the configuration.

```
(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
```

Manage ACL rule sequences

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 space 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 assigns 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. However, the order of the ACL rules is maintained after the switch comes back up.

The following examples show how you can use thew CLI to 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.

CLI: Add an IP ACL with rules without specifying sequence numbers

The following example shows how you can insert an ACL rule and let the switch automatically assign a sequence number.

Note: Only the CLI lets you add rules without specifying sequence numbers. When you add a rule in the main UI, you must specify a sequence number.

To use the CLI to add an IP ACL with three rules without specifying sequence numbers for the rules:

1. Create an IP ACL named voice_acl and add three rules without specifying sequence numbers.

```
(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
(Netgear Switch) (Config)#exit
```

2. Verify that the sequence numbers of the rules are automatically assigned by the switch.

The sequence number for the first rule is 10, for the second rule 20, for the third rule 30, 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
```

CLI: Change sequence numbers and increments numbers for ACL rules

The following example shows how to change the start sequence number and the sequence increment number (that is, the number by which the sequence increases) for ACL rules, and then insert an ACL rule at a particular position.

Note: Only the CLI lets you change the start sequence number and the sequence increment number for ACL rules, and then insert an ACL rule at a particular position. These options are not available in the main UI. That is, you cannot change the sequence numbers of existing rules in the main UI.

To use the CLI to change sequence numbers for rules in an ACL and insert a new rule:

1. If you must add more than 10 ACL rules, change the start sequence number and sequence increment number before you add ACL rules.

```
(Netgear Switch) (Config)#ip access-list resequence voice_acl 1000 100(Netgear Switch)
(Netgear Switch) (Config)#exit
```

2. Verify that the sequence numbers are assigned by the switch in the way that you configured it.

In the following example, the start sequence number of the rules is 1000 and the sequence increment number is 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
```

3. Insert a new ACL rule at a specific position.

In this example, a new ACL rule with sequence number 900 is inserted 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
```

4. Verify the order of the rules.

```
(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 in the CLI.

Note: Only the CLI lets you add and ACL to the CPU port. The main UI does not provide this option.

CLI: Add an ACL to the CPU port, permitting any host to access the switch through Telnet or HTTP

To use the CLI to add an ACL to the CPU port, permitting any host to access the managed VLAN IP address of 169.254.100.100 through a Telnet or HTTP connection:

1. Create an ACL that permits 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)#
```

2. Add the ACL to the CPU port.

```
(Netgear Switch) (Config)#ip access-group acl_for_cpu control-plane
```

CLI: Add an ACL to the CPU port, permitting a specific host to access the switch through SSH only

To use the CLI to add an ACL to the CPU port, permitting a specific host to access the switch over an SSH connection only.

1. Create an ACL that permits a specific host to 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)#
```

2. Add the ACL to the CPU port.

```
(Netgear Switch) (Config)#ip access-group acl_for_cpu control-plane
```

Configure an IPv6 ACL

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

The order of the rules is important: When a packet matches multiple rules, the first rule takes precedence. Also, after you define an ACL for a port, all traffic that is not specifically permitted by the ACL is denied access.

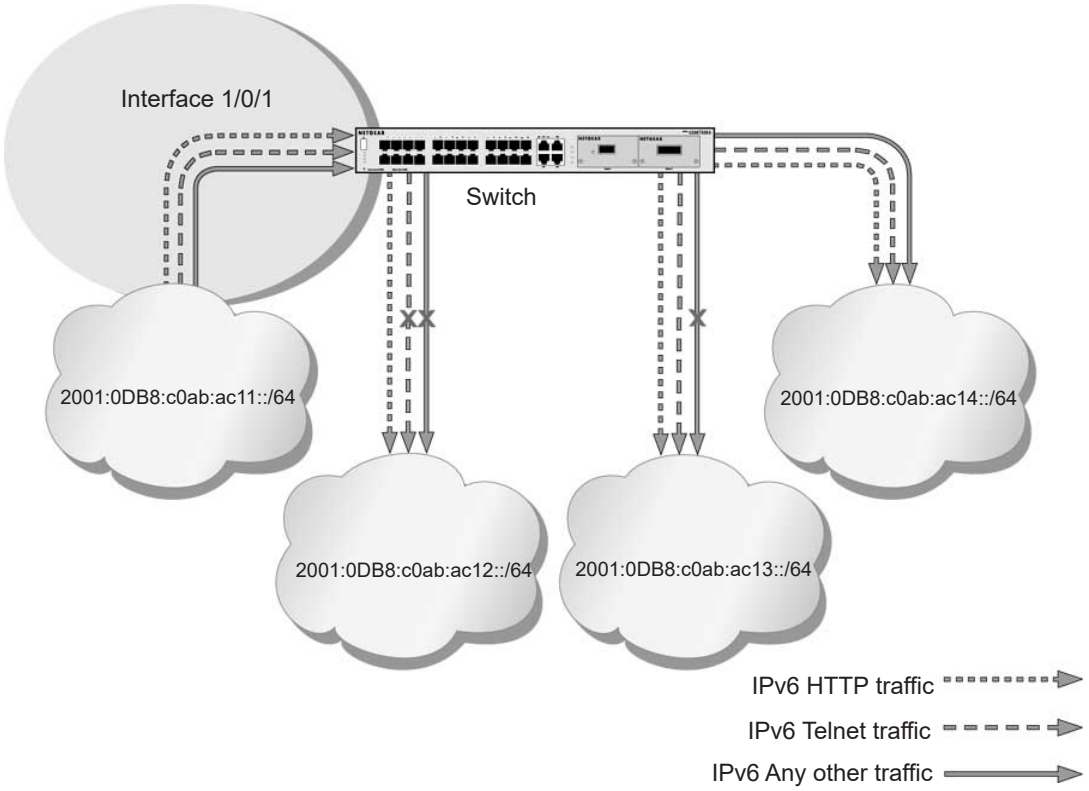


Figure 27. IPv6 ACLs

The script in this section shows you how to set up an IPv6 ACL with the following three rules:

- **Rule 1**. Permits all 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.

The example is shown as CLI commands and as a main UI procedure.

CLI: Configure an IPv6 ACL

To use the CLI to configure an IPv6 ACL with three rules:

1. Create the access control list with the name ipv6-acl.

```
(Netgear Switch) (Config)# ipv6 access-list ipv6-acl
```

2. Define three rules to do the following:
   - 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 is 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. Display the configuration.

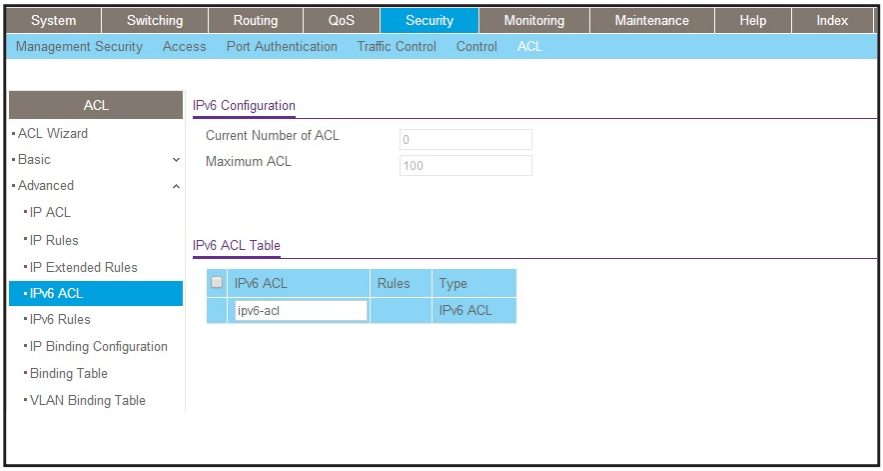
```
(Netgear Switch) #show ipv6 access-lists
Current number of all ACLs: 1  Maximum number of all ACLs: 100

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)
```

Main UI: Configure an IPv6 ACL

To use the main UI to configure an IPv6 ACL with three rules:

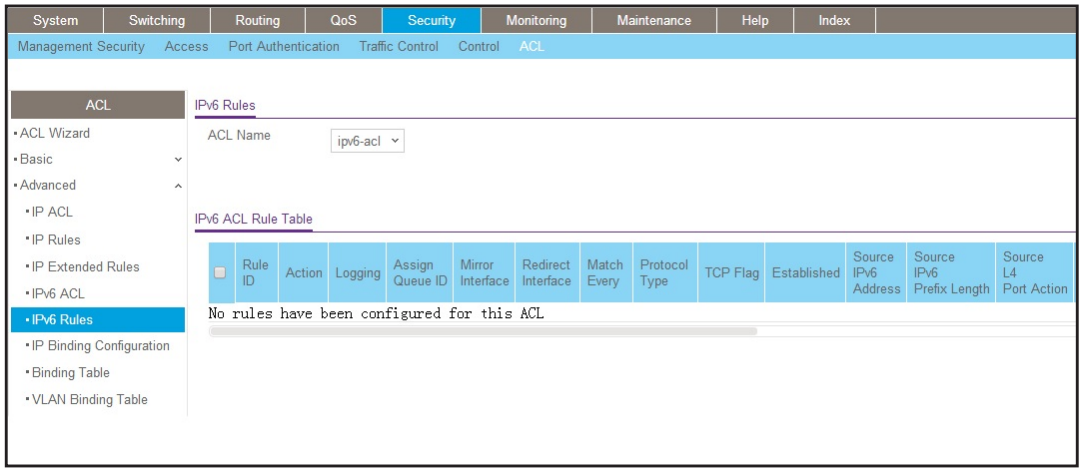
1. Create the access control list with the name ipv6-acl.
   a. Select **Security > ACL > Advanced > IPv6 ACL**.

      A page similar to the following figure displays.



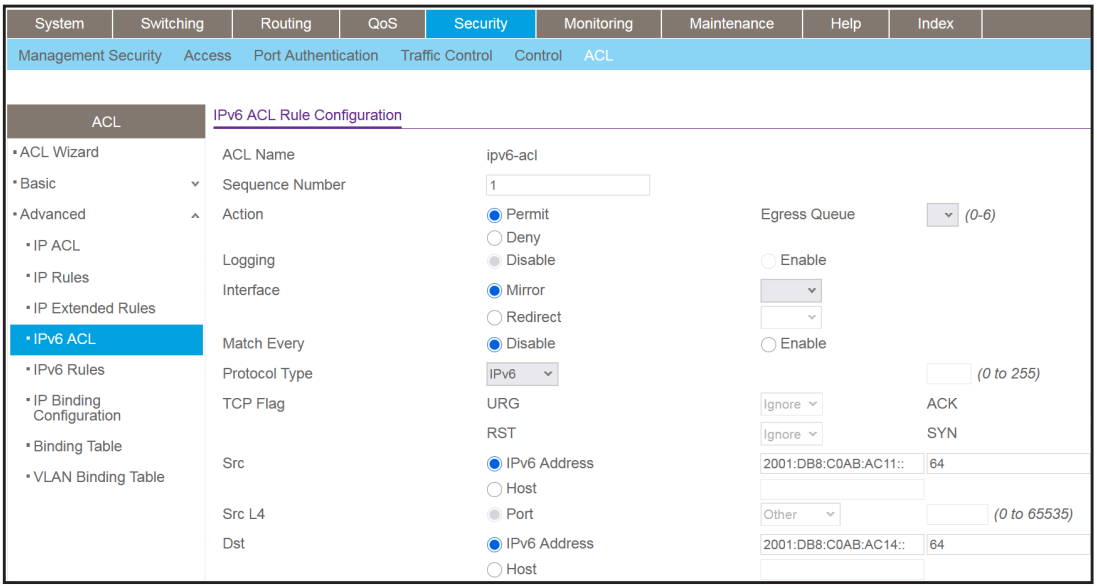
   b. In the IPv6 ACL Table, in the **IPv6 ACL** field, enter **ipv6-acl**.
   c. Click the **Add** button. Your settings are saved.
2. Define the first rule (1 of 3).
   a. Select **Security > ACL > Advanced > IPv6 Rules**.

      A page similar to the following figure displays.



   b. In the **ACL Name** menu, select **ipv6-acl**.
   c. Click the **Add** button.

A page similar to the following figure displays.



d. In the **Sequence Number** field, enter **1**.

e. Select the **Action Permit** radio button.

f. Select the **Match Every Disable** radio button.

g. In the **Protocol Type** menu, select **IPv6**.

h. In the **Src IPv6 Address** field, enter **2001:DB8:C0AB:AC11::**.

i. In the source prefix length field to the right, enter **64**.

j. In the **Dst IPv6 Address** field, enter **2001:DB8:C0AB:AC14::**.

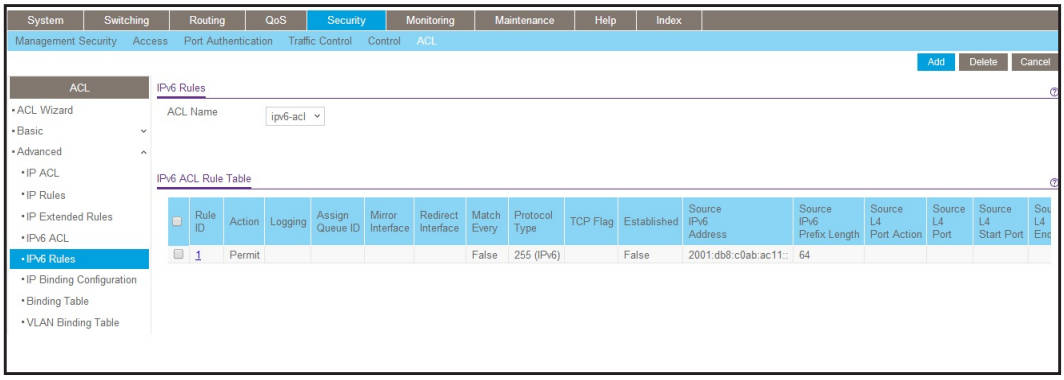
k. In the destination prefix length field to the right, enter **64**.

l. Click the **Apply** button. Your settings are saved.

3. Add Rule 2.

a. Select **Security > ACL > Advanced > IPv6 Rules**.

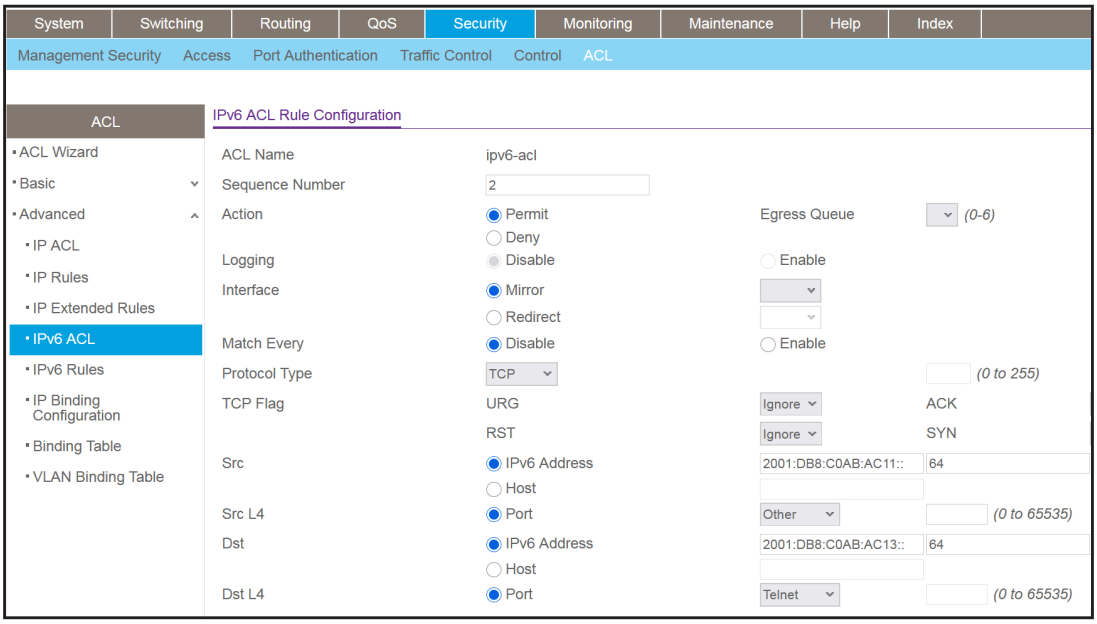
A page similar to the following figure displays.



b. In the **ACL Name** menu, select **ipv6-acl**.

c. Click the **Add** button.

A page similar to the following figure displays.



d. In the **Sequence Number** field, enter **2**.

e. Select the **Action Permit** radio button.

f. Select the **Match Every Disable** radio button.

g. In the **Protocol Type** menu, select **TCP**.

h. In the **Src IPv6 Address** field, enter **2001:DB8:C0AB:AC11::**.

i. In the source prefix length field to the right, enter **64**.

j. In the **Dst IPv6 Address** field, enter **2001:DB8:C0AB:AC13::**.

k. In the destination prefix length field to the right, enter **64**.

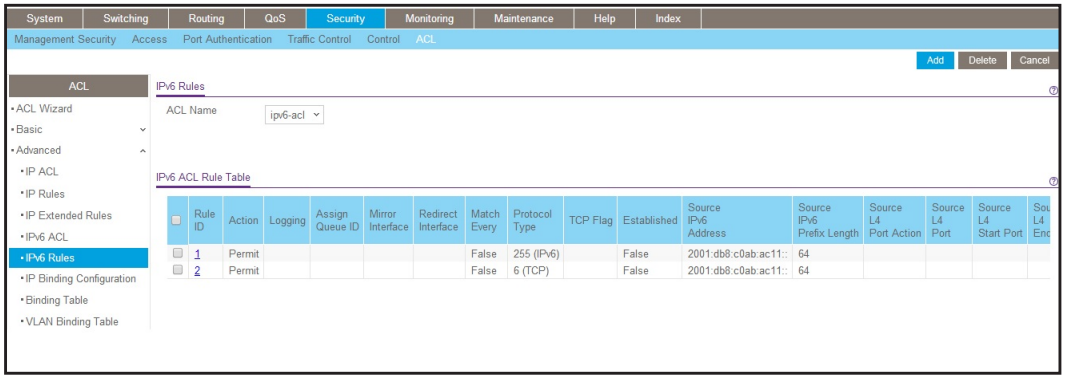
l. Select the **Dst L4 Port** radio button, and in the associated menu, select **Telnet**.

m. Click the **Apply** button. Your settings are saved.

4. Add Rule 3.

a. Select **Security > ACL > Advanced > IPv6 Rules**.

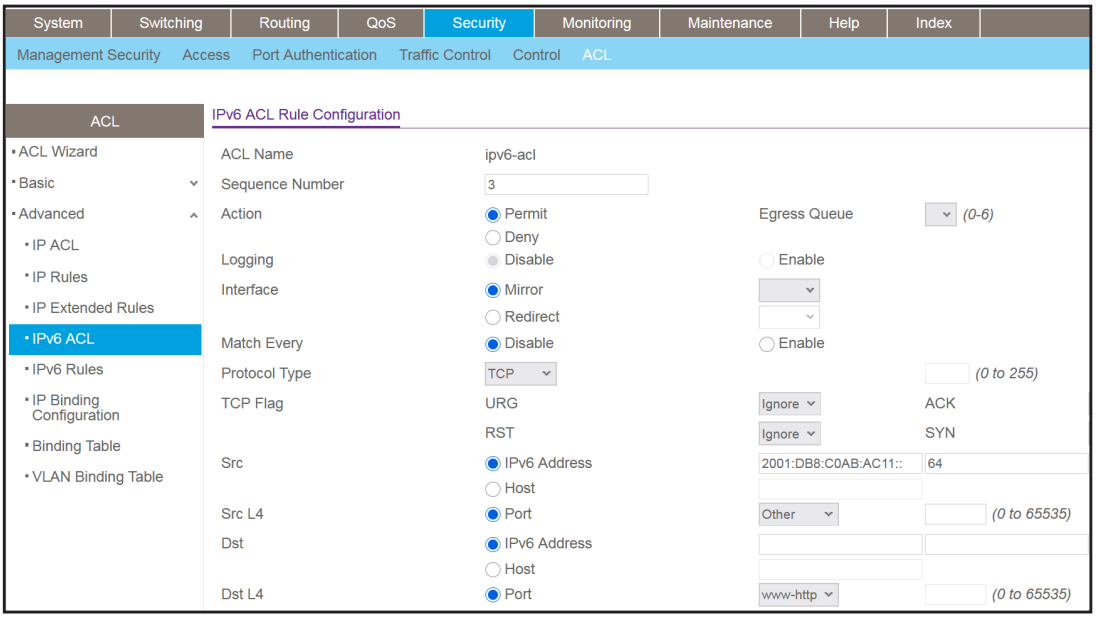
A page similar to the following figure displays.



b. In the **ACL Name** menu, select **ipv6-acl**.

c. Click the **Add** button.

A page similar to the following figure displays.



d. In the **Sequence Number** field, enter **3**.

e. Select the **Action Permit** radio button.

f. Select the **Match Every Disable** radio button.

g. In the **Protocol Type** menu, select **TCP**.

h. In the **Src IPv6 Address** field, enter **2001:DB8:C0AB:AC11::**.

i. In the source prefix length field to the right, enter **64**.

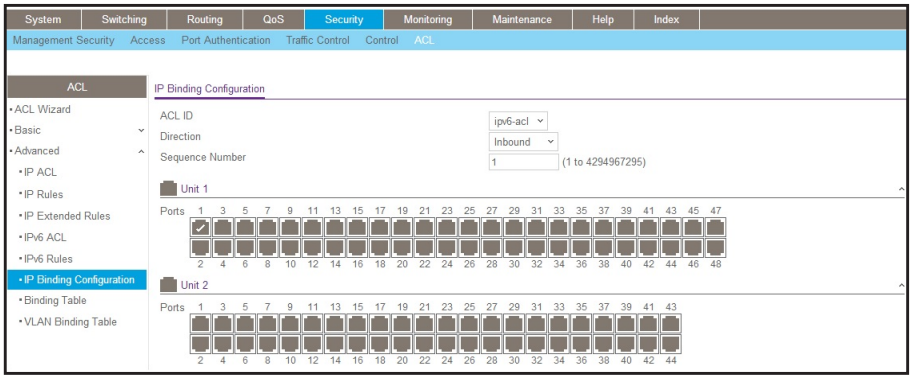
j. Select the **Dst L4 Port** radio button, and in the associated menu, select **www-http**.

k. Click the **Apply** button. Your settings are saved.

5. Apply the rules to inbound traffic on port 1/0/1.

a. Select **Security > ACL > Advanced > IP Binding Configuration**.

A page similar to the following figure displays.



b. In the **ACL ID** menu, select **ipv6-acl**.

c. In the **Sequence Number** menu, select **1**.

d. Click the gray box under port **1**. A check mark displays in the box.

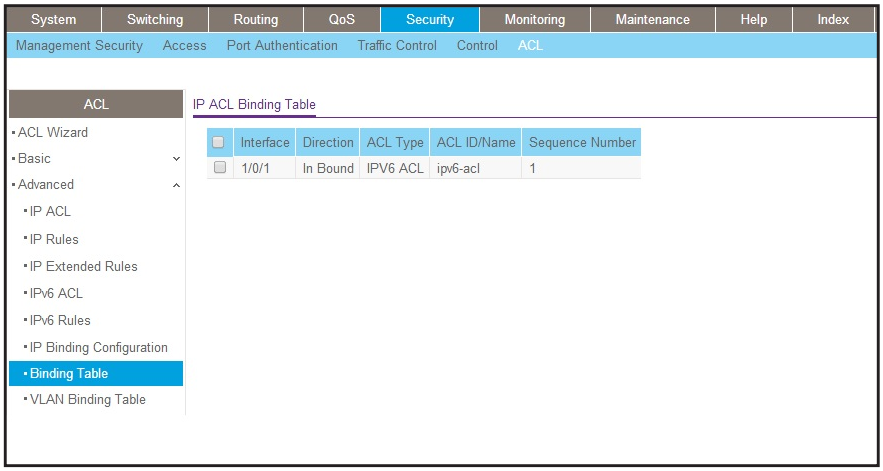
If your switch is a member of a stack, be sure that you select the port in the correct unit.

e. Click the **Apply** button. Your settings are saved.

6. Display the binding table.

a. Select **Security > ACL > Advanced > Binding Table**.

A page similar to the following figure displays.



12

CoS Queuing

Class of Service queuing

This feature is supported on the M4250 series switches

This feature is supported on the M4300 series switches

This feature is supported on the M4350 series switches

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 the trust mode for a class of service
- Set the trust mode for a class of service
- Configure CoS queue minimum bandwidth and strict priority scheduler mode
- Set the 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 switch 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 configure 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 switch trusts certain priority designations for incoming packets. Trust applies only to packets that have that trust information.
- One of the following trust settings is supported on a port, and these settings are mutually exclusive, that is, you can configure only one of these settings on an individual port:
  - 802.1p user priority, which is the default trust mods.
  - IP precedence
  - IP DiffServ Code Point (DSCP)

The switch can assign a service level based on the 802.1p priority field of the Layer 2 header. You configure this by mapping the 802.1p priorities to one of three traffic class queues:

- **Queue 2**. Minimum of 50 percent of available bandwidth
- **Queue 1**. Minimum of 33 percent of available bandwidth
- **Queue 0**. Minimum of 17 percent of available bandwidth (this is the lowest priority)

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.
- In a configuration in which packets are classified by an ACL or a DiffServ policy, all ingress packets from untrusted ports are directed to specific CoS queues on the appropriate egress port. This specific CoS queue is determined by either the default priority of the port or a DiffServ or ACL-assigned queue attribute.
- An untrusted port is used when trusted port mapping cannot be honored, for example, 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, which combined let you create service characteristics for different types of traffic:

- Port egress queue configuration:
  - Scheduler type is strict or weighted
  - Minimum guaranteed bandwidth
  - Maximum allowed bandwidth per-queue shaping
  - Queue management type is tail-drop or 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 is tail-drop or WRED
- Only if per-queue configuration is not supported:
  - WRED decay exponent
  - Traffic shaping for an entire interface

Note: The M4250 series switches support queue IDs 0 through 7. The M4300 series and M4350 switches support queue IDs 0 through 6 because one queue ID is reserved for stacking.

Show the trust mode for a class of service

The example is shown as CLI commands and as a main UI procedure.

CLI: Show the trust mode for a class of service

To use the CLI to show CoS trust mode:

```
(Netgear Switch) #show classofservice trust
Class of Service Trust Mode: Dot1P
```

Main UI: Show the trust mode for a class of service

To use the main UI to show CoS trust mode:

Select **QoS > CoS > Basic > CoS Configuration**.

A page similar to the following figure displays.

Set the trust mode for a class of service

The example is shown as CLI commands and as a main UI procedure.

CLI: Set the trust mode for a class of service

To use the CLI to set the trust mode for a class of service:

```
(Netgear Switch)# config
(Netgear Switch) (Config)#classofservice trust dot1p
```

Main UI: Set the trust mode for a class of service

To use the main UI to set the trust mode for a class of service:

1. Select **QoS > CoS > Basic > CoS Configuration**.

   A page similar to the following figure displays.

2. Select the **Global** radio button.
3. In the **Global Trust Mode** menu, select **trust dot1p**.
4. Click the **Apply** button. Your settings are saved.

Configure CoS queue minimum bandwidth and strict priority scheduler mode

The example is shown as CLI commands and as a main UI procedure.

CLI: Configure CoS queue minimum bandwidth and strict priority scheduler mode

To use the CLI to configure CoS queue minimum bandwidth and strict priority scheduler mode:

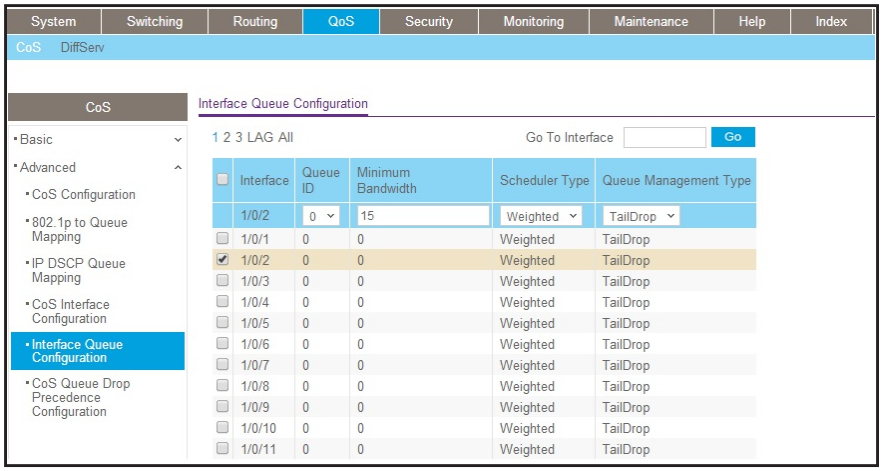
```
(Netgear Switch) #config
(Netgear Switch) (Config)#cos-queue min-bandwidth 15 25 10 5 5 20 10 10
(Netgear Switch) (Config)#cos-queue strict 1
```

Main UI: Configure CoS queue minimum bandwidth and strict priority scheduler mode

To use the main UI to configure CoS queue minimum 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 page similar to the following figure displays.



b. Select the Interface **1/0/2** check box.

c. In the **Queue ID** menu, select **0**.

d. Configure the following settings:

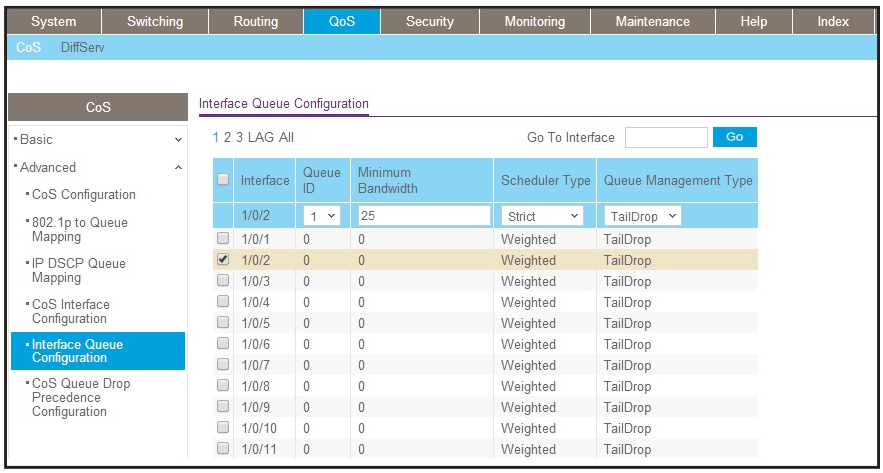
- In the **Minimum Bandwidth** field, enter **15**.
- In the **Scheduler Type** menu, select **Weighted**.
- In the **Queue Management Type** menu, select **TailDrop**.

e. Click the **Apply** button. Your settings are saved.

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 page similar to the following figure displays.



b. Select the Interface **1/0/2** check box.

c. In the **Queue ID** menu, select **1**.

d. Configure the following settings:
   - In the **Minimum Bandwidth** field, enter **25**.
   - In the **Scheduler Type** menu, select **Strict**.
   - In the **Queue Management Type** menu, select **TailDrop**.

e. Click the **Apply** button. Your settings are saved.

Set the CoS trust mode for an interface

The example is shown as CLI commands and as a main UI procedure.

CLI: Set the CoS trust mode for an interface

Use the CLI to set the CoS trust mode for an interface:

```
(Netgear Switch) #config
(Netgear Switch) (Config)#interface 1/0/3
(Netgear Switch) (Interface 1/0/3)#classofservice trust dot1p
```

Main UI: Set the CoS trust mode for an interface

Use the main UI to set the CoS trust mode for an interface:

1. Select **QoS > CoS > Advanced > CoS Configuration**.

   A page similar to the following figure displays.

2. Select the **Interface** radio button.
3. In the **Interface** menu, select **1/0/3**.
4. In the **Interface Trust Mode** menu, select **trust dot1p**.
5. Click the **Apply** button. Your settings are saved.

Configure traffic shaping

Traffic shaping controls the amount of traffic transmitted through a network. This has the effect of smoothing temporary traffic bursts over time.

CLI: Configure traffic shaping

In the CLI, you can use the **`traffic-shape`** command to enable traffic shaping by specifying the maximum transmission bandwidth limit for all interfaces (in Global Config mode) or for a single interface (in Interface Config mode).

The value of the *bw* argument is a percentage that ranges from 0 to 100 in increments of 5. The default bandwidth value is 0, meaning that no upper limit is enforced, which allows the interface to transmit up to its maximum line rate.

The value of the *bw* argument is independent of any per-queue maximum bandwidth values in effect for the interface and must be considered a second-level transmission rate control mechanism that regulates the output of the entire interface, regardless of which queues originate the outbound traffic.

Use the CLI to configure traffic shaping for the switch globally and then change the value for an individual interface:

1. Configure traffic shaping with 90 percent bandwidth globally on the switch.

```
(Netgear Switch) #config
(Netgear Switch) (Config)#traffic-shape 90
```

2. For interface 0/3, change traffic shaping to 70 percent bandwidth.

```
(Netgear Switch) #config
(Netgear Switch) (Config)#interface 0/3
(Netgear Switch) (Interface 0/3)#traffic-shape 70
```

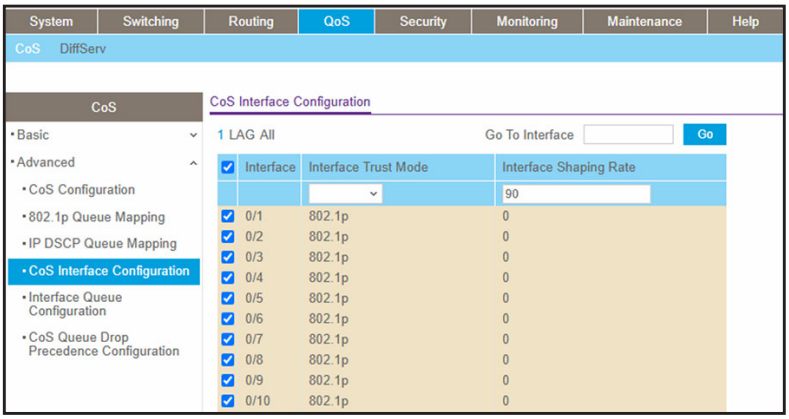
Main UI: Configure traffic shaping

Using the main UI, you configure traffic shaping for individual interfaces but you cannot configure traffic shaping globally for the switch, as you can do in the CLI.

To use the main UI to configure traffic shaping for all interfaces and the change traffic shaping for an individual interface:

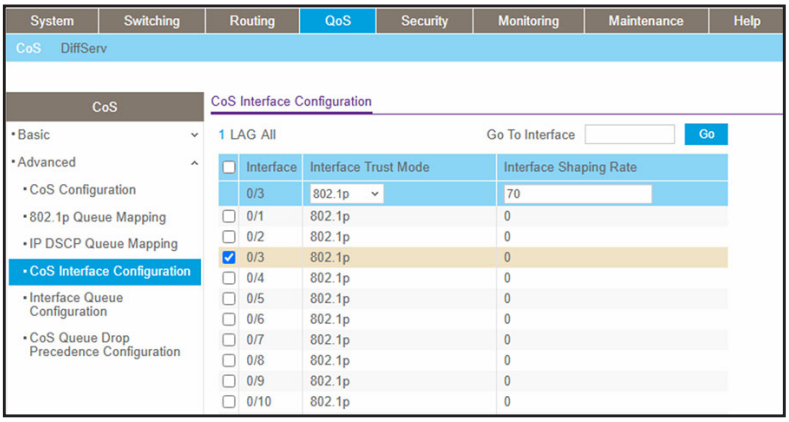
1. Configure traffic shaping with 90 percent bandwidth for all interfaces on the switch.
   a. Select **QoS > CoS > Advanced > CoS Interface Configuration**.

      A page similar to the following figure displays.



   b. Select the check box the table header so that all interfaces are selected.
   c. In the **Interface Trust Mode** menu, make sure that **802.1p** is selected (this is the default setting).
   d. In the **Interface Shaping Rate** field, enter **90**.
   e. Click the **Apply** button. Your settings are saved.
2. For interface 0/3, change traffic shaping to 70 percent bandwidth.
   a. Select **QoS > CoS > Advanced > CoS Interface Configuration**.

      A page similar to the following figure displays.



   b. Select the Interface **0/3** check box.
   c. In the **Interface Shaping Rate** field, enter **70**.
   d. Click the **Apply** button. Your settings are saved.

13

DiffServ

Differentiated Services

This feature is supported on the M4250 series switches

This feature is supported on the M4300 series switches

This feature is supported on the M4350 series switches

This chapter includes the following sections:

- Differentiated services concepts
- Configure DiffServ to allocate bandwidth
- Configure DiffServ for VoIP
- Configure Auto VoIP
- DiffServ for IPv6
- Color conform policy
- Weighted random early detection

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 describes how to configure the switch to identify which traffic class a packet belongs to, and how the traffic must be handled to provide the quality of service that is required. DiffServ lets you to control which traffic is accepted and which 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 value 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 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. Two types of classes are supported:
  - All: The All class type option specifies that each match criteria within a class must be true for a packet to match that class.
  - Any: The Any class type option specifies that at least one match criteria must be true for a packet to match that class.
- **Policy**. A 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 switch supports a traffic conditions policy. This type of policy is associated with an inbound traffic class and specifies the actions to be taken on packets that meet the class rules:
  - Marking the packet with a DSCP value, IP precedence, or CoS
  - Policing the packet by dropping or re-marking the packet that exceed the class's assigned data rate
  - Counting the traffic within the class
- **Service**. Assigns a policy to an interface for inbound traffic.

Configure DiffServ to allocate bandwidth

This example shows how you can provide equal access to the Internet (or another 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.

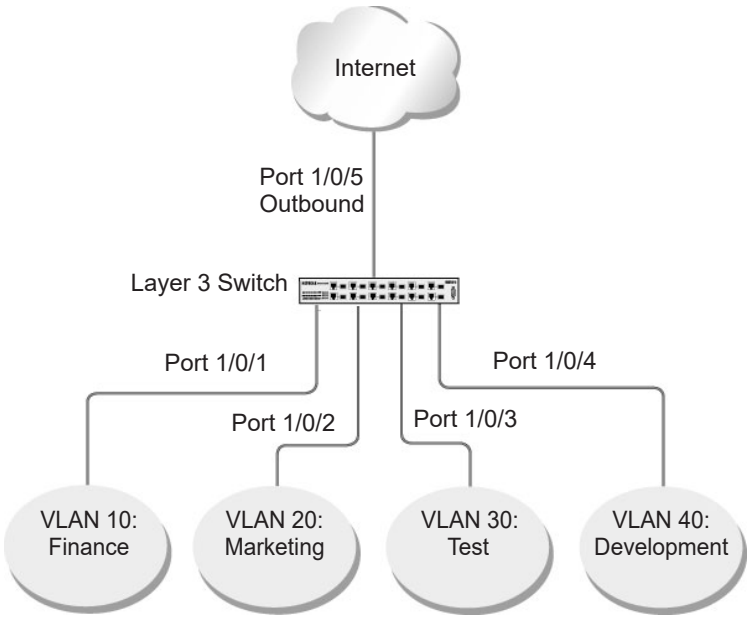


Figure 28. Class B subnet with differentiated services

The example is shown as CLI commands and as a main UI procedure.

CLI: Configure DiffServ to allocate bandwidth

To use the CLI to configure DiffServ to allocate bandwidth:

1. Enable DiffServ on 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 place each department's traffic on a different egress queue. This is how the DiffServ inbound policy connects to the CoS queue settings.

```
(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 must be used for the departmental traffic through the assign-queue attribute. The switch forwards this traffic to interface 1/0/5 based on a normal destination address lookup for Internet traffic.

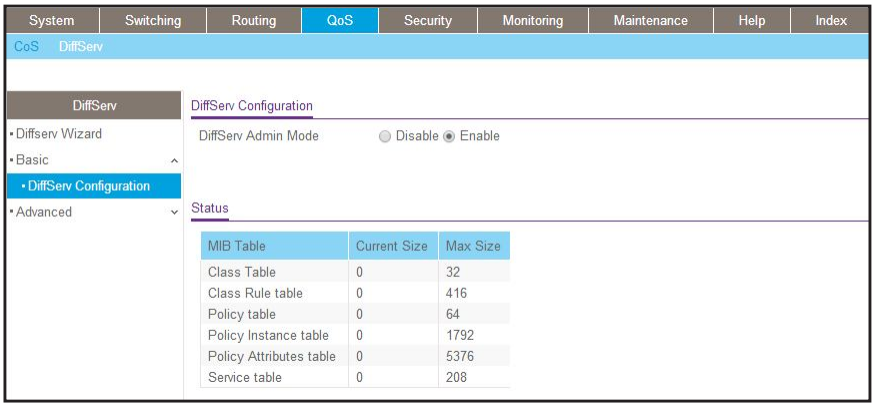
```
(Netgear Switch) (Config)#interface 1/0/5
(Netgear Switch) (Interface 1/0/5)#cos-queue min-bandwidth 0 25 25 25 25 0 0 0
(Netgear Switch) (Interface 1/0/5)#exit
(Netgear Switch) (Config)#exit
```

Main UI: Configure DiffServ to allocate bandwidth

To use the main UI to configure DiffServ to allocate bandwidth:

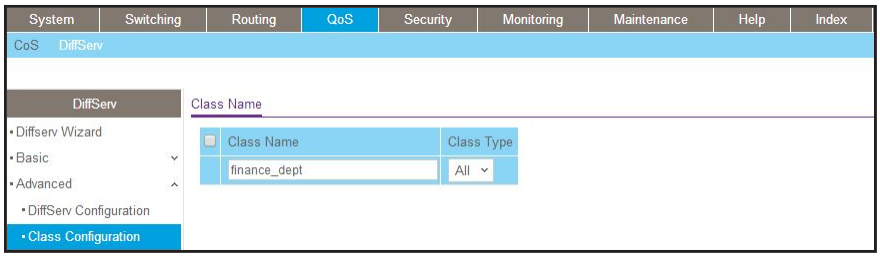
1. Enable Diffserv on the switch.
   a. Select **QoS > DiffServ > Basic > DiffServ Configuration**.

      A page similar to the following figure displays.



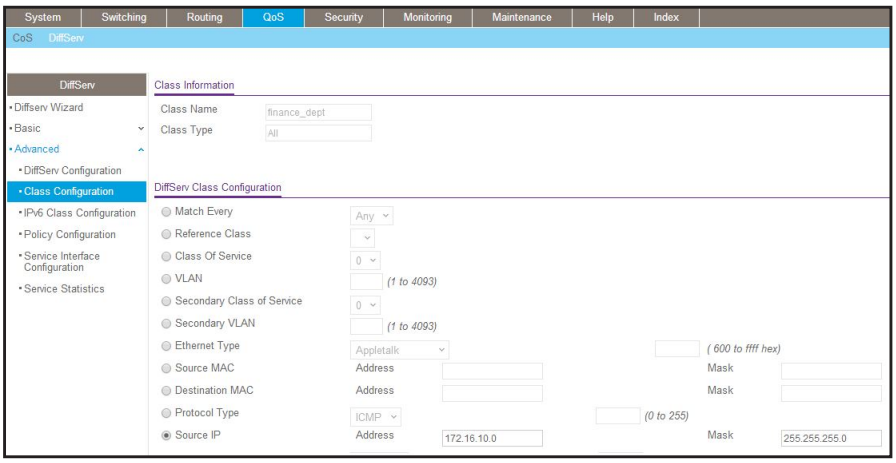
   b. Select the Diffserv Admin Mode **Enable** radio button.
   c. Click the **Apply** button. Your settings are saved.
2. Create the class finance_dept.
   a. Select **QoS > DiffServ > Advanced > Class Configuration**.

      A page similar to the following figure displays.



   b. Configure the following settings:
      - In the **Class Name** field, enter **finance_dept**.
      - In the **Class Type** menu, select **All**.
   c. Click the **Add** button. Your settings are saved.
   d. Click the **finance_dept** link to configure this class.

A page similar to the following figure displays.



e. Under Diffserv Class Configuration, configure the following settings:

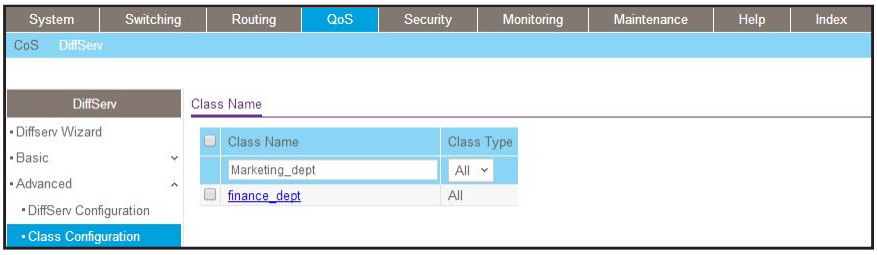
- In the **Source IP Address** field, enter **172.16.10.0**.
- In the **Source IP Mask** field, enter **255.255.255.0**.

f. Click the **Apply** button. Your settings are saved.

3. Create the class Marketing_dept:

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

A page similar to the following figure displays.



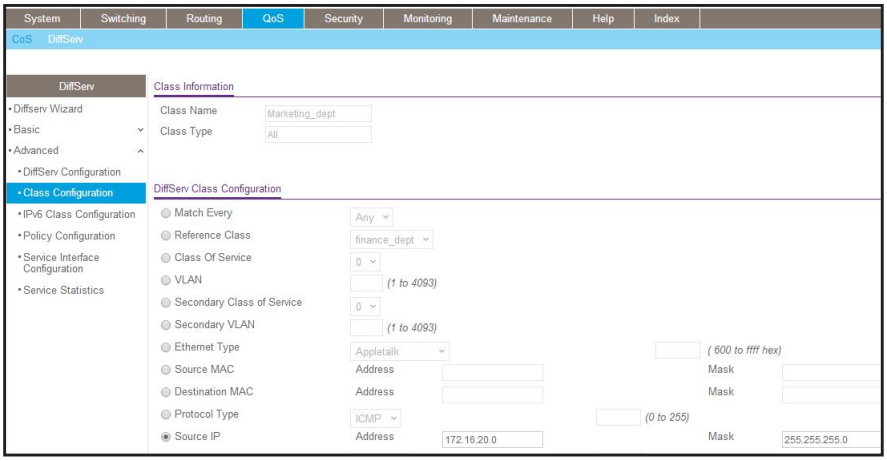
b. Configure the following settings:

- In the **Class Name** field, enter **Marketing_dept**.
- In the **Class Type** menu, select **All**.

c. Click the **Add** button. Your settings are saved.

d. Click the **Marketing_dept** link to configure this class.

A page similar to the following figure displays.



e. Under Diffserv Class Configuration, configure the following settings:

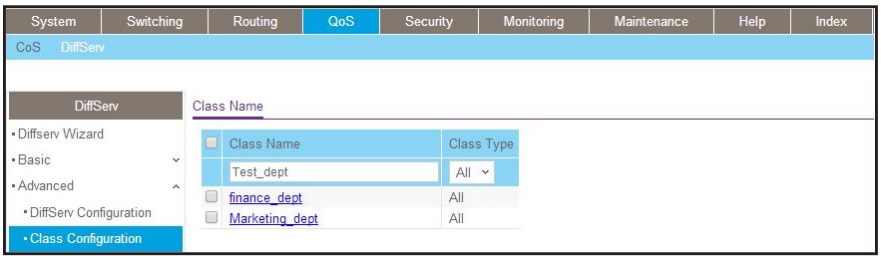
- In the **Source IP Address** field, enter **172.16.20.0**.
- In the **Source IP Mask** field, enter **255.255.255.0**.

f. Click the **Apply** button. Your settings are saved.

4. Create the class Test_dept:

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

A page similar to the following figure displays.



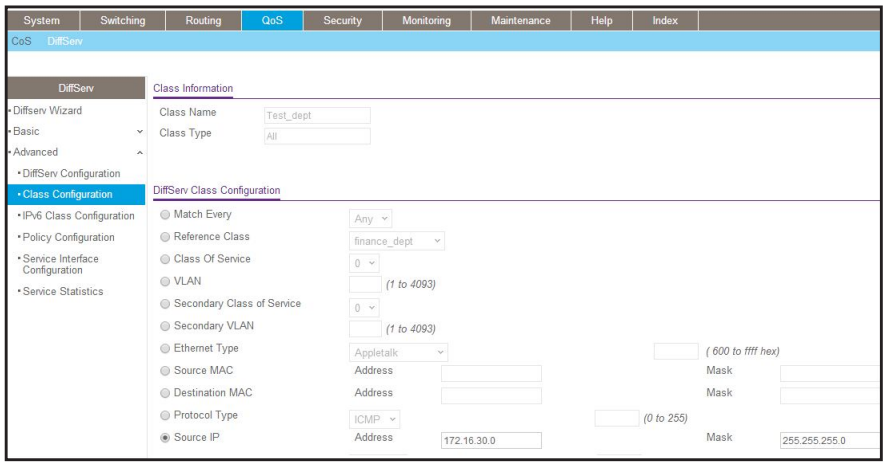
b. Configure the following settings:

- In the **Class Name** field, enter **Test_dept**.
- In the **Class Type** menu, select **All**.

c. Click the **Add** button. Your settings are saved.

d. Click the **Test_dept** link to configure this class.

A page similar to the following figure displays.



e. Under Diffserv Class Configuration, configure the following settings:

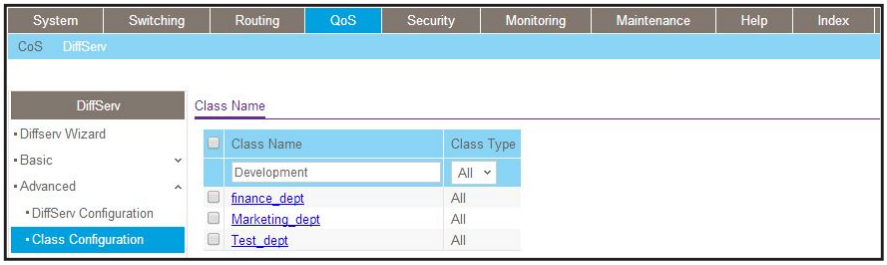
- In the **Source IP Address** field, enter **172.16.30.0**.
- In the **Source IP Mask** field, enter **255.255.255.0**.

f. Click the **Apply** button. Your settings are saved.

5. Create class Development.

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

A page similar to the following figure displays.



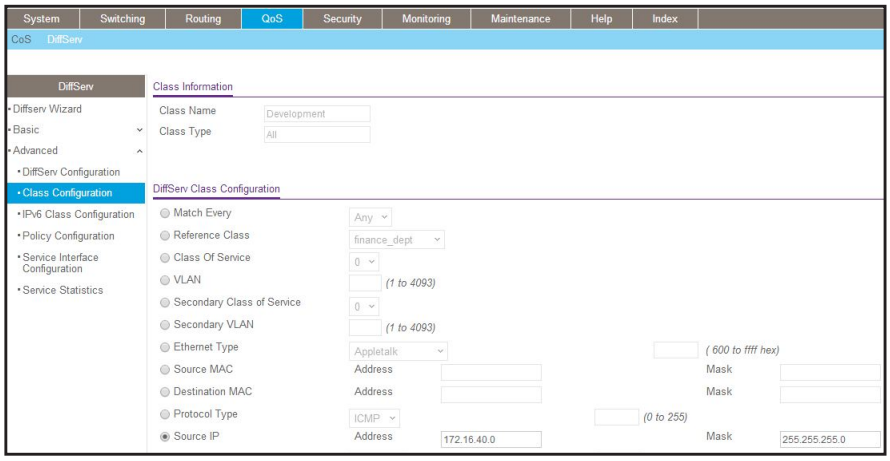
b. Configure the following settings:

- In the **Class Name** field, enter **Development**.
- In the **Class Type** menu, select **All**.

c. Click the **Add** to create a new class development_dept.

d. Click the **Development** link to configure this class.

A page similar to the following figure displays.



e. Under Diffserv Class Configuration, configure the following settings:

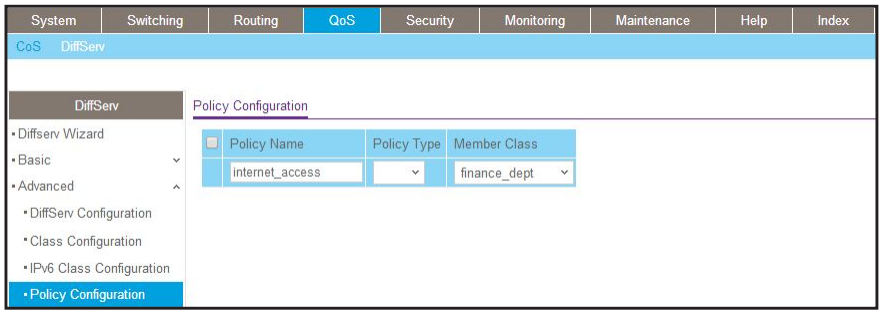
- In the **Source IP Address** field, enter **172.16.40.0**.
- In the **Source IP Mask** field, enter **255.255.255.0**.

f. Click the **Apply** button. Your settings are saved.

6. Create a policy named internet_access and add the class finance_dept to it.

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

A page similar to the following figure displays.



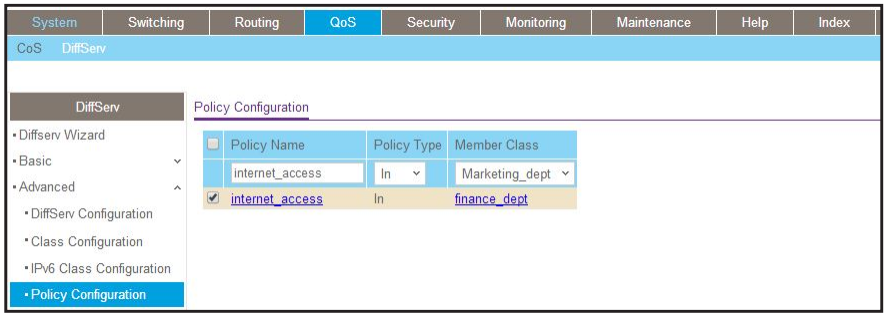
b. Configure the following settings:

- In the **Policy Name** field, enter **internet_access**.
- In the **Policy Type** menu, select **In**.
- In the **Member Class** menu, select the **finance_dept**.

c. Click the **Add** button. Your settings are saved.

7. Add the class Marketing_dept to the policy internet_access.

a. Remain on the same page.



b. Select the Policy Name **internet_access** check box.

c. In the **Member Class** menu, select **Marketing_dept**.

d. Click the **Apply** button. Your settings are saved.

8. Add the class Test_dept to the policy internet_access.

a. Remain on the same page.

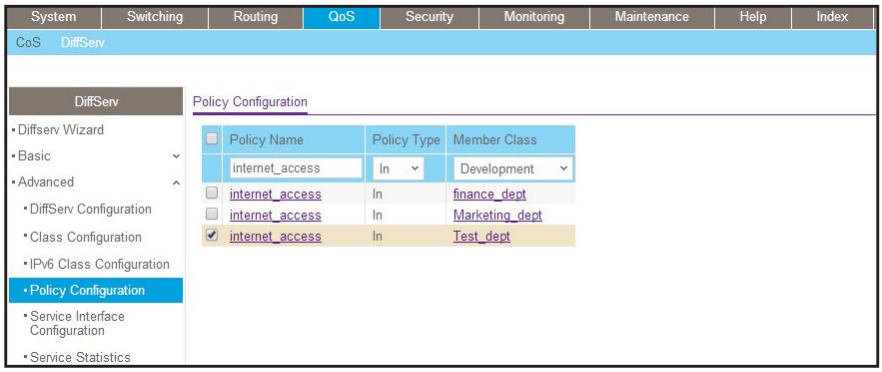
b. Select the Policy Name **internet_access** check box.

c. In the **Member Class** menu, select **Test_dept**.

d. Click the **Apply** button. Your settings are saved.

9. Add the class development_dept to the policy internet_access.

a. Remain on the same page.



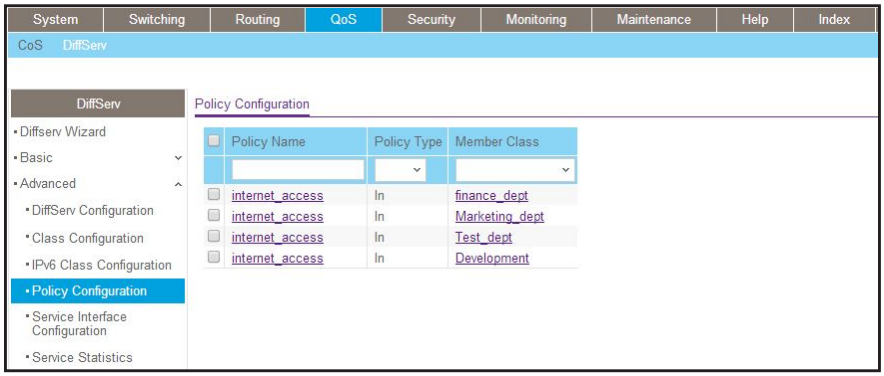
b. Select the Policy Name **internet_access** check box.

c. In the **Member Class** menu, select **Development**.

d. Click the **Apply** button. Your settings are saved.

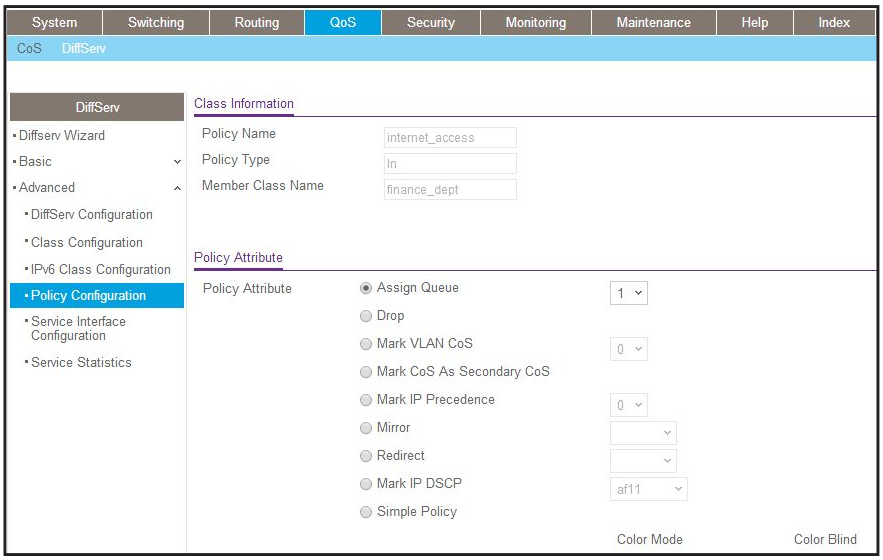
10. Assign queue 1 to the class finance_dept.

a. Remain on the same page.



b. Click the **internet_access** link for the member class finance_dept.

A page similar to the following figure displays.



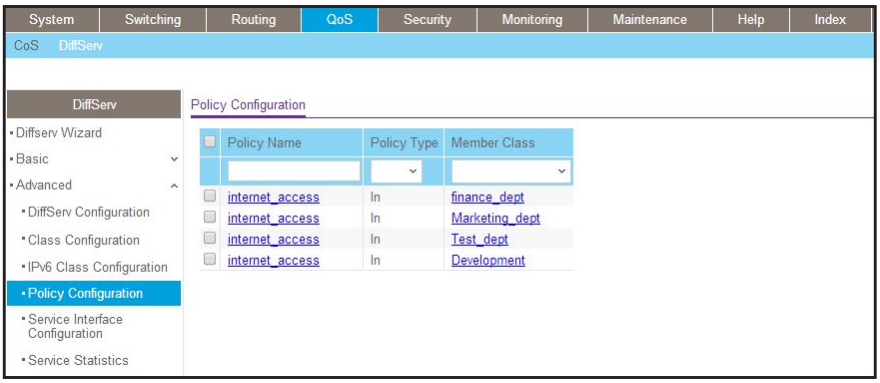
c. Select the **Assign Queue** radio button, and in the associated menu, select **1**.

d. Click the **Apply** button. Your settings are saved.

11. Assign queue 2 to the class Marketing_dept.

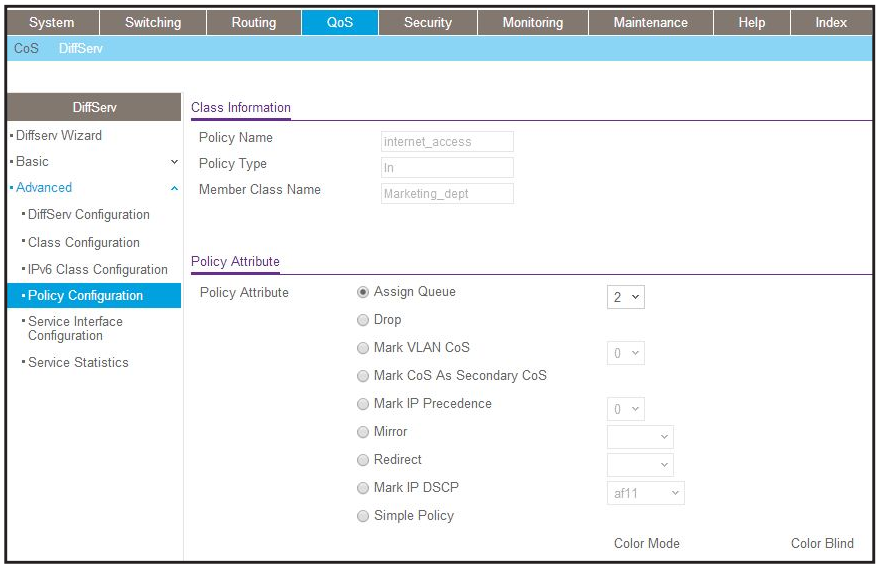
a. Select **QoS > DiffServ > Advanced > Policy Configuration**.

A page similar to the following figure displays.



b. Click the **internet_access** link for the member class Marketing_dept.

A page similar to the following figure displays.



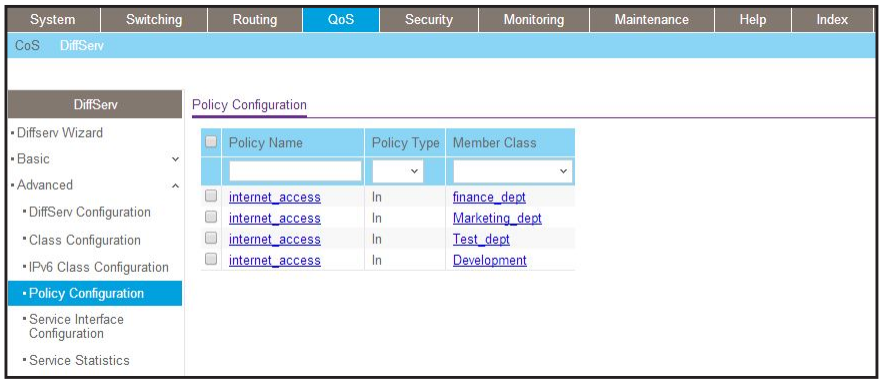
c. Select the **Assign Queue** radio button, and in the associated menu, select **2**.

d. Click the **Apply** button. Your settings are saved.

12. Assign queue 3 to the class Test_dept.

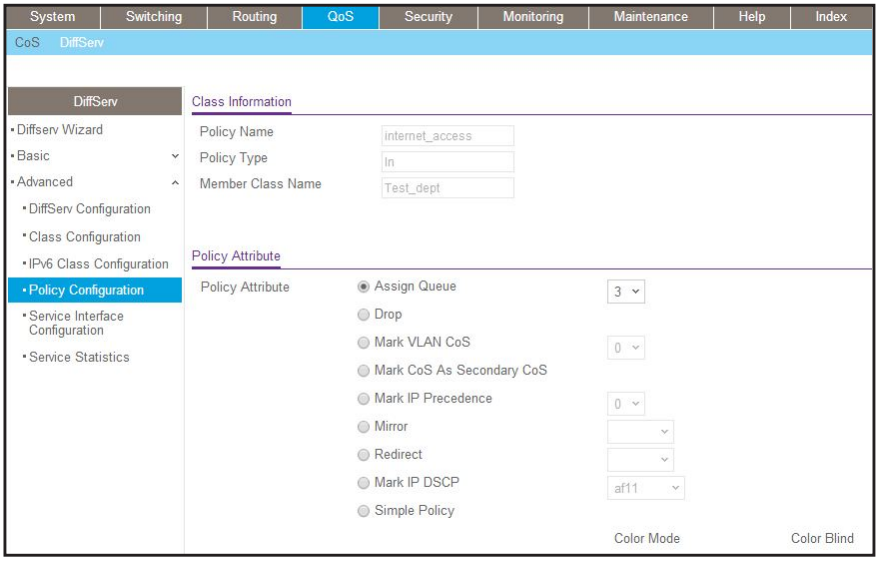
a. Select **QoS > DiffServ > Advanced > Policy Configuration**.

A page similar to the following figure displays.



b. Click the **internet_access** link for the member class Test_dept.

A page similar to the following figure displays.



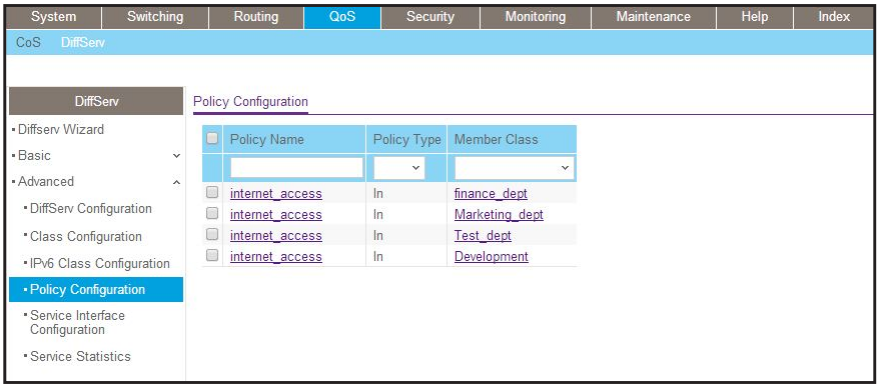
c. Select the **Assign Queue** radio button, and in the associated menu, select **3**.

d. Click the **Apply** button. Your settings are saved.

13. Assign queue 4 to the class Development.

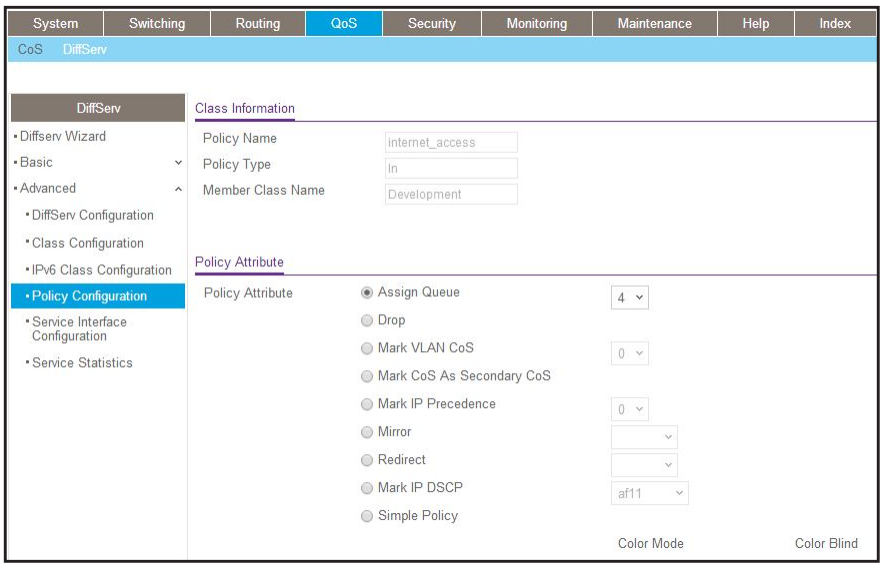
a. Select **QoS > DiffServ > Advanced > Policy Configuration**.

A page similar to the following figure displays.



b. Click the **internet_access** link for the member class Development.

A page similar to the following figure displays.



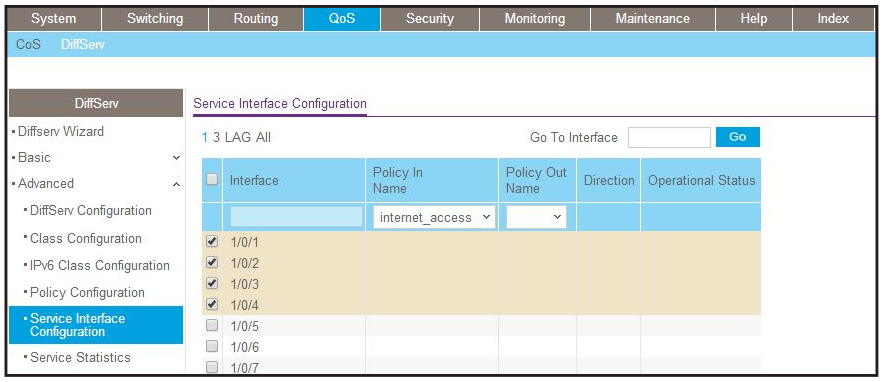
c. Select the **Assign Queue** radio button, and in the associated menu, select **4**.

d. Click the **Apply** button. Your settings are saved.

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 page similar to the following figure displays.



b. Select the check boxes for interfaces **1/0/1**, **1/0/2**, **1/0/3**, and **1/0/4**.

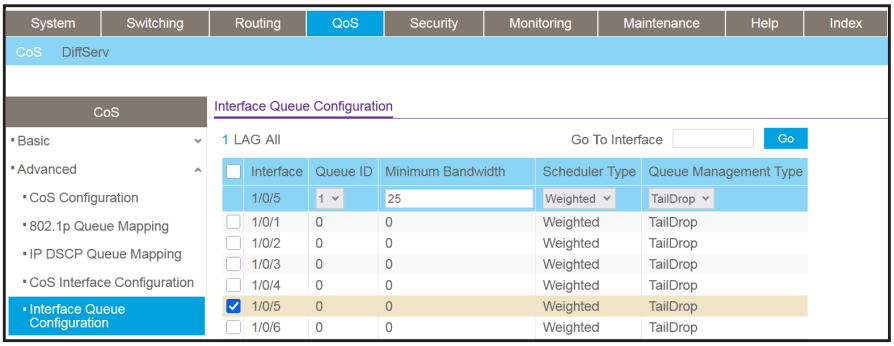
c. In the **Policy In Name** menu, select **internet_access**.

d. Click the **Apply** button. Your settings are saved.

15. Set the CoS queue 1 configuration for interface 1/0/5.

a. Select **QoS > CoS > Advanced > Interface Queue Configuration**.

A page similar to the following figure displays.



b. Select the Interface **1/0/5** check box.

c. In the **Queue ID** menu, select **1**.

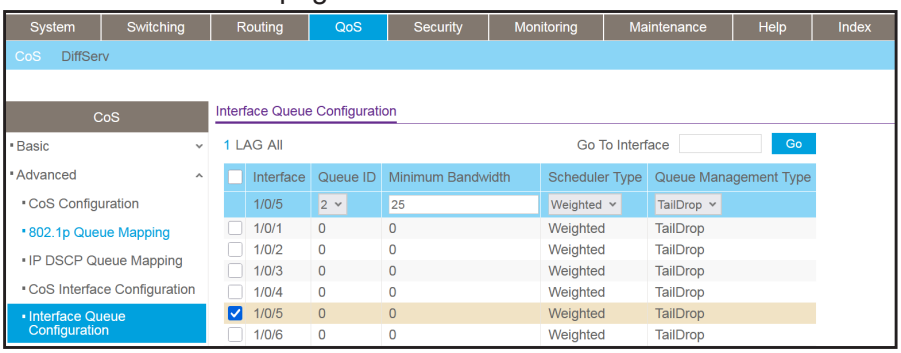
d. In the **Minimum Bandwidth** field, enter **25**.

e. In the **Scheduler Type** menu, select **Weighted**.

f. In the **Queue Management Type** menu, select **TailDrop**.

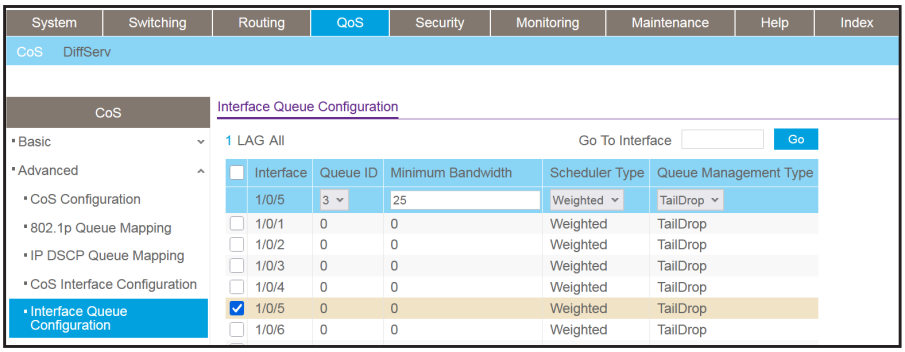
g. Click the **Apply** button. Your settings are saved.

16. Set the CoS queue 2 configuration for interface 1/0/5.
    a. Remain on the same page.



    b. Select the Interface **1/0/5** check box.
    c. In the **Queue ID** menu, select **2**.
    d. In the **Minimum Bandwidth** field, enter **25**.
    e. In the **Scheduler Type** menu, select **Weighted**.
    f. In the **Queue Management Type** menu, select **TailDrop**.
    g. Click the **Apply** button. Your settings are saved.

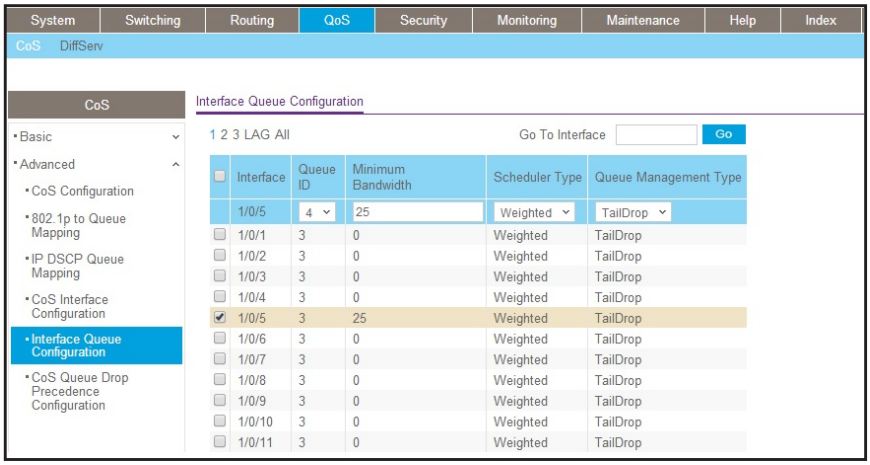
17. Set the CoS queue 3 configuration for interface 1/0/5.
    a. Remain on the same page.



    b. Select the Interface **1/0/5** check box.
    c. In the **Queue ID** menu, select **3**.
    d. In the **Minimum Bandwidth** field, enter **25**.
    e. In the **Scheduler Type** menu, select **Weighted**.
    f. In the **Queue Management Type** menu, select **TailDrop**.
    g. Click the **Apply** button. Your settings are saved.

18. Set the CoS queue 4 configuration for interface 1/0/5.
    a. Select **QoS > CoS > Advanced > Interface Queue Configuration**.

A page similar to the following figure displays.



b. Select the Interface **1/0/5** check box.

c. In the **Queue ID** menu, select **4**.

d. In the **Minimum Bandwidth** field, enter **25**.

e. In the **Scheduler Type** menu, select **Weighted**.

f. In the **Queue Management Type** menu, select **TailDrop**.

g. Click the **Apply** button. Your settings are saved.

Configure 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.

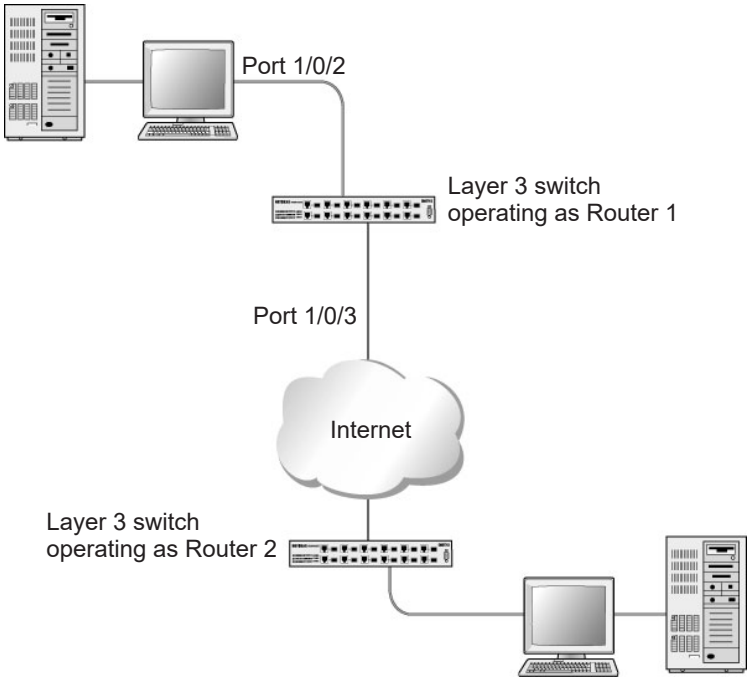


Figure 29. Diffserv for VoIP in Router 1

The example is shown as CLI commands and as a main UI procedure.

CLI: Configure DiffServ for VoIP

Use the CLI to configure DiffServ for VoIP:

1. Set queue 5 on all ports to use strict priority mode. This queue is used for all VoIP packets. Then, enable 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 DSCP value 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.

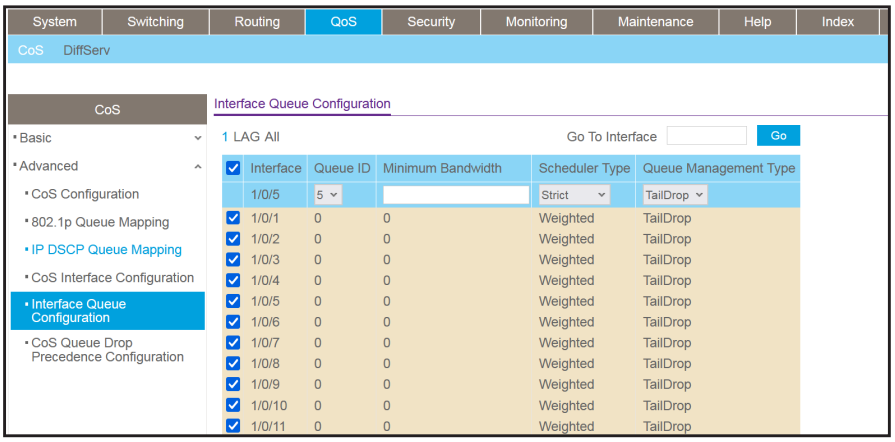
```
(Netgear Switch) (Config)#interface 1/0/2
(Netgear Switch) (Interface 1/0/2)#service-policy in pol_voip
(Netgear Switch) (Interface 1/0/2)#exit
(Netgear Switch) (Config)#exit
```

Main UI: Diffserv for VoIP

Use the main UI to configure DiffServ for VoIP:

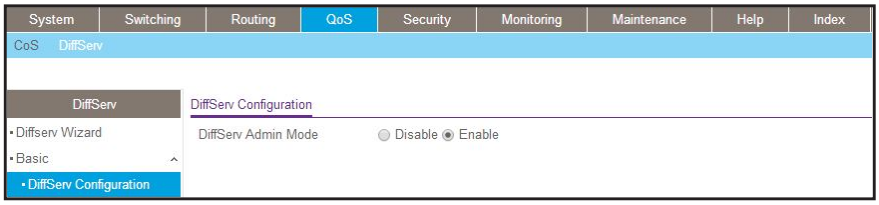
1. Set queue 5 on all interfaces to use strict mode.
   a. Select **QoS > CoS > Advanced > Interface Queue Configuration**.

      A page similar to the following figure displays.



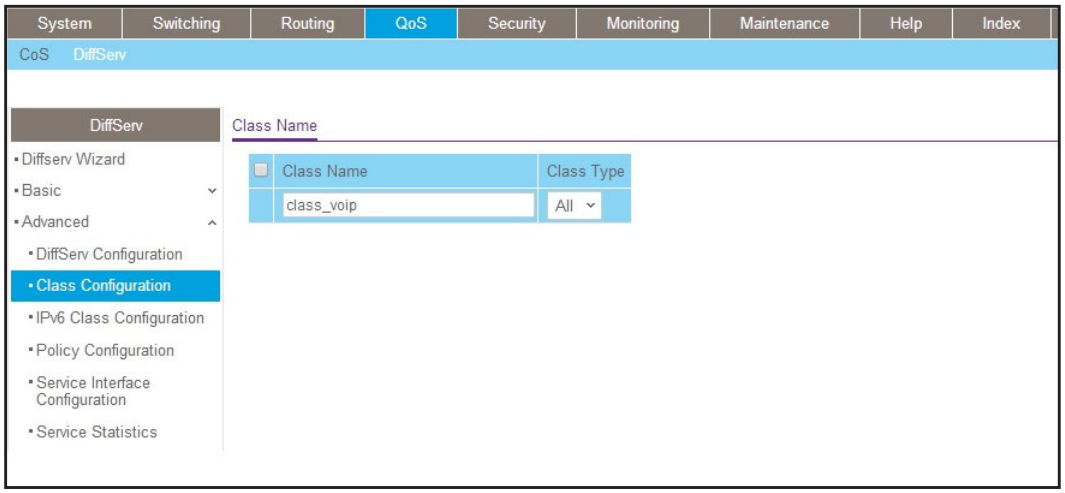
   b. Under Interface Queue Configuration, select all the interfaces.
   c. In the **Queue ID** menu, select **5**.
   d. In the **Scheduler Type** menu, select **Strict**.
   e. In the **Queue Management Type** menu, select **TailDrop**.
   f. Click the **Apply** button. Your settings are saved.
2. Enable DiffServ.
   a. Select **QoS > DiffServ > Basic > DiffServ Configuration**.

      A page similar to the following figure displays.



   b. Select the Diffserv Admin Mode **Enable** radio button.
   c. Click the **Apply** button. Your settings are saved.
3. Create a class class_voip.
   a. Select **QoS > DiffServ > Advanced > DiffServ Configuration**.

A page similar to the following figure displays.



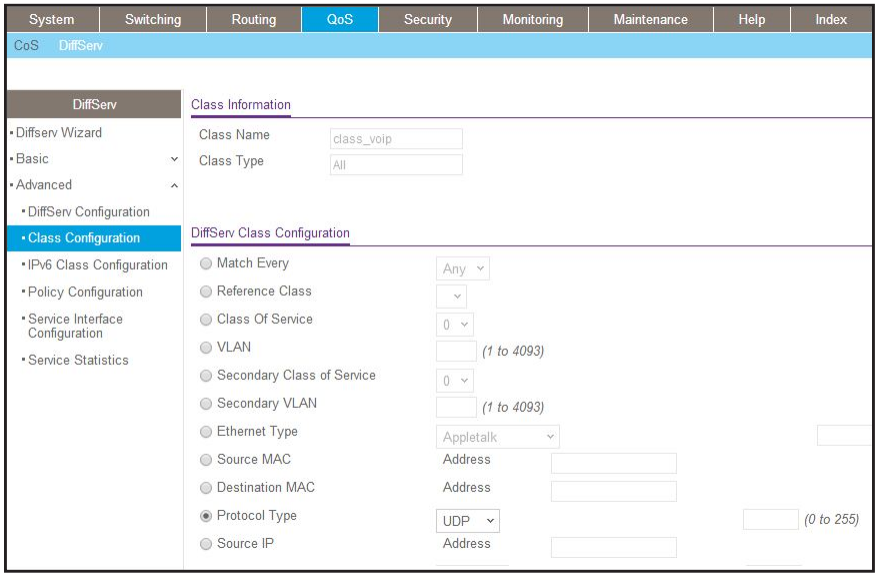
b. In the **Class Name** field, enter **class_voip**.

c. In the **Class Type** menu, select **All**.

d. Click the **Add** button. Your settings are saved.

e. Click the **class_voip** link.

A page similar to the following figure displays.



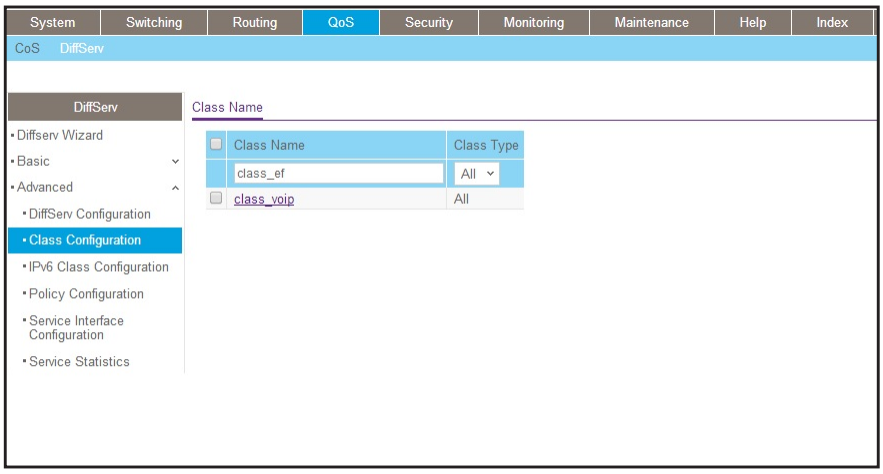
f. Select the **Protocol Type** radio button, and in the associated menu, select **UDP**.

g. Click **Apply** to create a new class.

4. Create a class class_ef:

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

A page similar to the following figure displays.



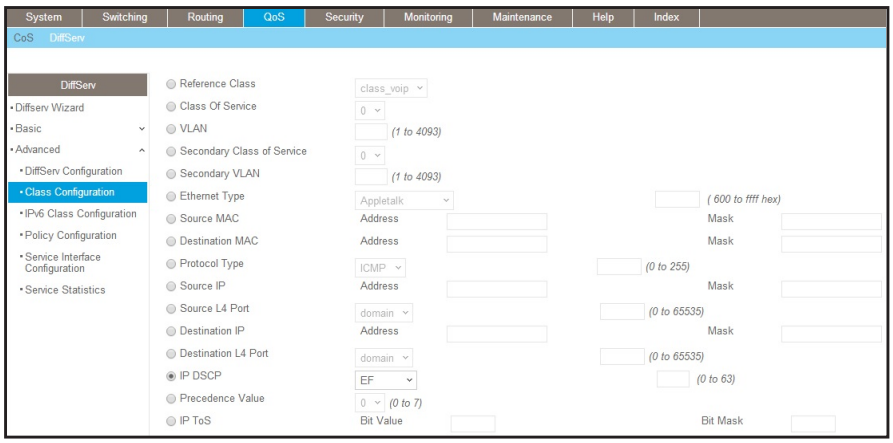
b. In the **Class Name** field, enter **class_ef**.

c. In the **Class Type** menu, select **All**.

d. Click the **Add** button. Your settings are saved.

e. Click the **class_ef** link.

A page similar to the following figure displays.



f. Select the **IP DSCP** radio button, and in the associated menu, select **ef**.

g. Click **Apply** to create a new class.

5. Create a policy pol_voip and add the class_voip to this policy.

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

A page similar to the following figure displays.

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

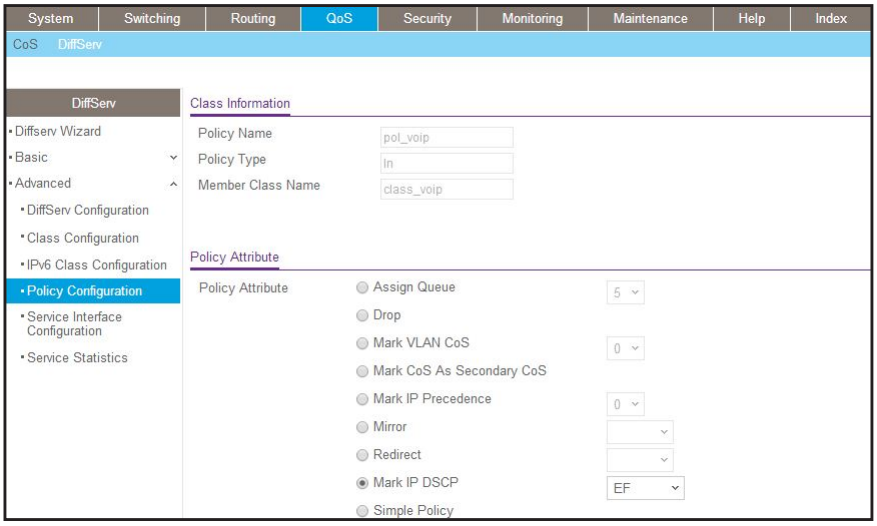
c. In the **Policy Type** menu, select **In**.

d. In the **Member Class** menu, select **class_voip**.

e. Click the **Add** button. Your settings are saved.

f. Click the **pol_voip** link for the member class class_voip.

A page similar to the following figure displays.



g. Select the **Assign Queue** radio button, and in the associated menu, select **5**.

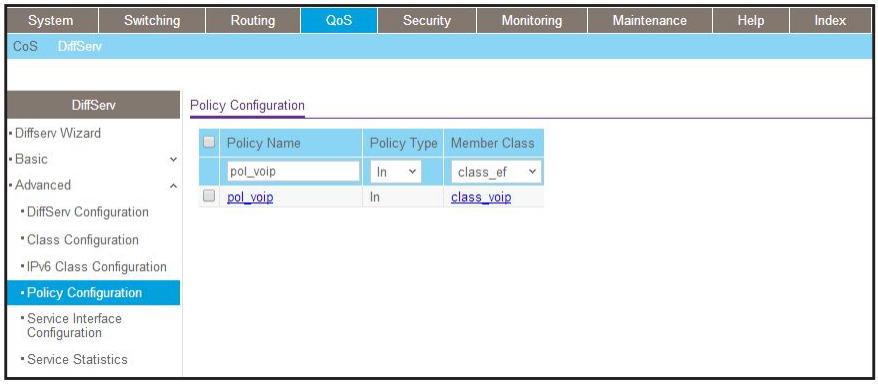
h. For Policy Attribute, select the **Mark IP DSCP** radio button, and in the associated menu, select **ef**.

i. Click the **Apply** button. Your settings are saved.

6. Add the class class_ef to the policy pol_voip.

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

A page similar to the following figure displays.



b. In the **Policy Name** field, select the **pol_voip** check box.

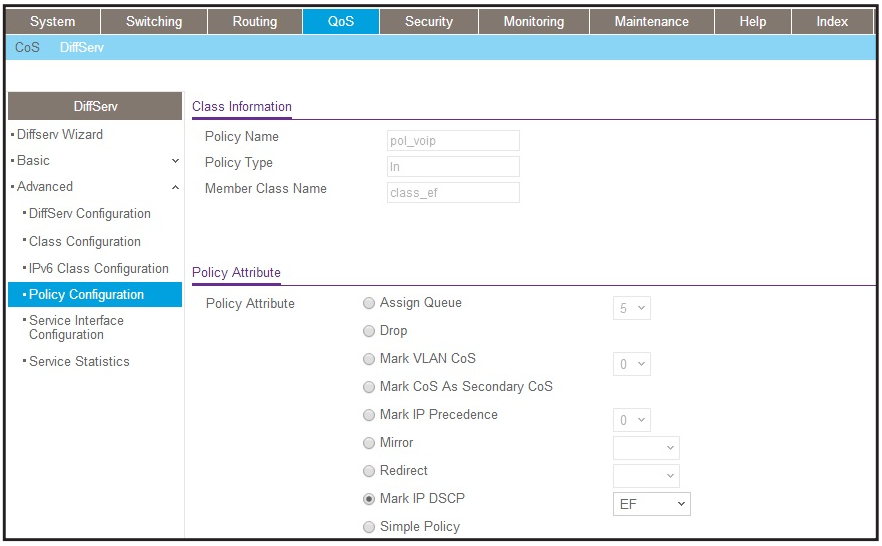
c. IM the **Policy Type** menu, select **In**.

d. In the **Member Class** menu, select **class_ef**.

e. Click the **Apply** button. Your settings are saved.

f. Click the **pol_voip** link for the member class class_ef.

A page similar to the following figure displays.



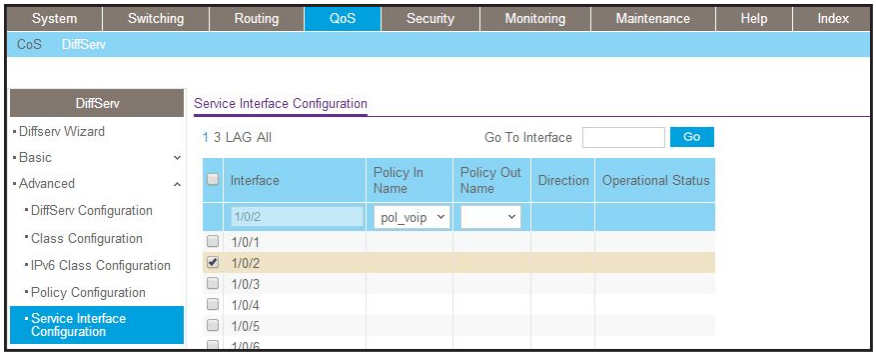
g. Select the **Assign Queue** radio button, and in the associated menu, select **5**.

h. Click the **Apply** button. Your settings are saved.

7. Attach the defined policy to interface 1/0/2 in the inbound direction.

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

A page similar to the following figure displays.



b. Select the Interface **1/0/2** check box.

c. In the **Policy In Name** menu, select **pol_voip**.

d. Click the **Apply** button. Your settings are saved.

Configure Auto VoIP

The Auto VoIP feature can help you to set up Voice over IP (VoIP) for IP phones on a switch. 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 (see Voice VLANs on page 47).

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.

Note: If you enable port mirroring on a port that is configured for Auto VoIP, the port remains nonoperational.

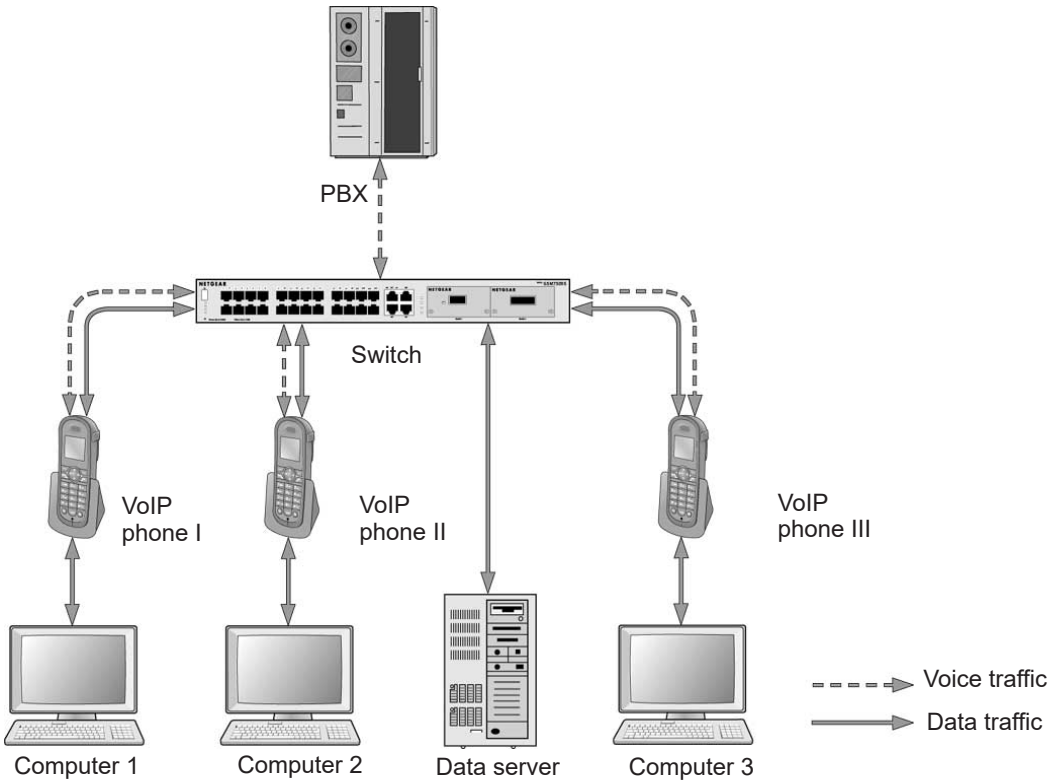


Figure 30. OUI-based Auto VoIP topology

Example 1: Enable protocol-based Auto VoIP

This example is provided as CLI commands and as a main UI procedure.

CLI: Enable protocol-based Auto VoIP

To use the CLI to set up protocol-based Auto VoIP on a port:

1. Enable protocol-based Auto VoIP on port 2/0/1 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.

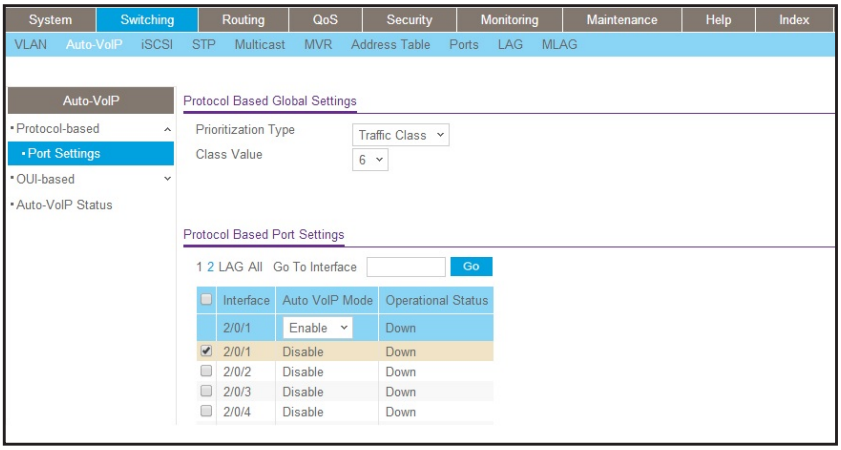
```
(Netgear Switch) #show auto-voip protocol-based interface 2/0/1
VoIP VLAN Id................................ 2
Prioritization Type......................... traffic-class
Class Value................................. 6
Interface  Auto VoIP Mode Operational Status
---------  -------------- -----------------
2/0/1      Enabled        Up
```

Main UI: Enable protocol-based Auto VoIP

To use the main UI to set up protocol-based Auto VoIP on a port:

1. Enable protocol-based Auto VoIP on port 2/0/1 of the switch:
   a. Select **Switching > Auto-VoIP > Protocol-based > Port Settings**.

      A page similar to the following figure displays.



   b. Select the Interface **2/0/1** check box.
   c. In the **Auto VoIP Mode** menu, select **Enable**.
   d. Click the **Apply** button. Your settings are saved.

Example 2: Change the queue of protocol-based Auto VoIP

This example is provided as CLI commands and as a main UI 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

To use the CLI 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.

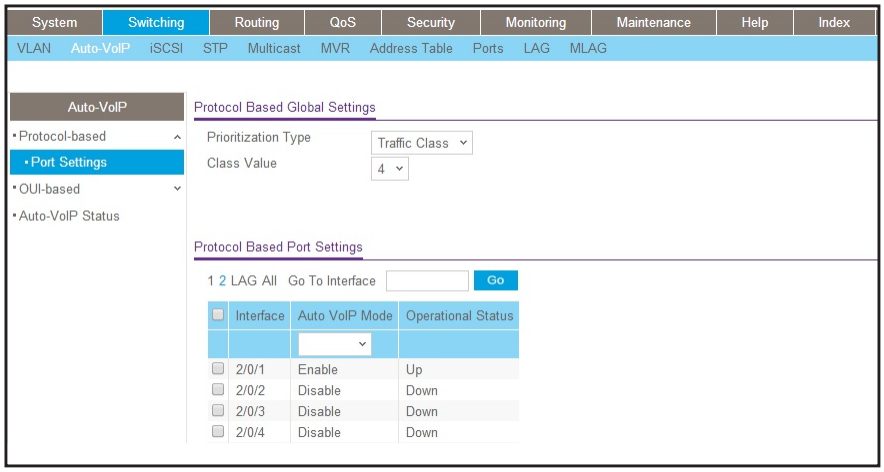
```
(Netgear Switch) #show auto-voip protocol-based interface 2/0/1
VoIP VLAN Id..................................... 2
Prioritization Type.............................. traffic-class
Class Value...................................... 4
Interface  Auto VoIP Mode Operational Status
---------  -------------- -----------------
2/0/1      Enabled        Up
```

Main UI: Change the queue of protocol-based Auto VoIP

To use the main UI to assign the protocol-based Auto VoIP to egress queue 4:

1. Change the queue of protocol-based Auto VoIP.
   a. Select **Switching > Auto-VoIP > Protocol-based > Port Settings**.

      A page similar to the following figure displays.



   b. In the **Prioritization Type** menu, select **Traffic Class**.
   c. In the **Class Value** menu, select **4**.
   d. Click the **Apply** button. Your settings are saved.

Example 3: Create an Auto VoIP VLAN

This example is provided as CLI commands and as a main UI procedure.

CLI: Create an Auto VoIP VLAN

To use the CLI to create an Auto VoIP VLAN:

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.

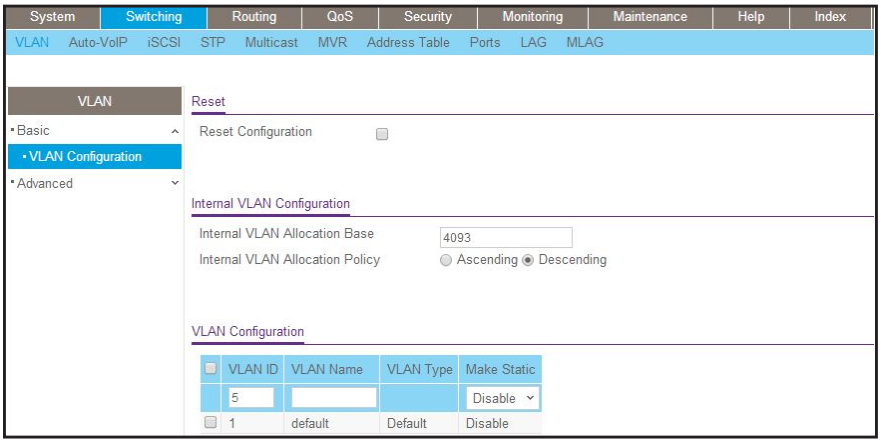
```
(Netgear Switch) #show auto-voip oui-based interface 2/0/1

VoIP VLAN Id..................................... 5
Priority......................................... 7
Interface  Auto VoIP Mode Operational Status
---------  -------------- ------------------
2/0/1      Disabled       Down
```

Main UI: Change the Auto VoIP VLAN

To use the main UI to create an Auto VoIP VLAN:

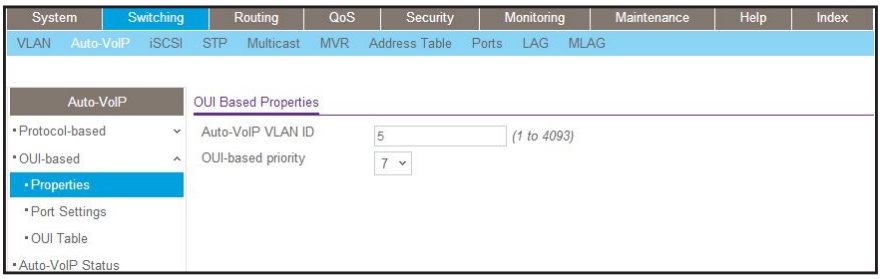
1. Create a VLAN 5:
   a. Select **Switching > VLAN > Basic > VLAN Configuration**.

      A page similar to the following figure displays.



   b. In the **VLAN ID** field, enter **5**.
   c. Click the **Add** button. Your settings are saved.
2. Assign the VoIP traffic to VLAN 5.
   a. Select **Switching > Auto-VoIP > OUI-based > Properties**.

      A page similar to the following figure displays.



   b. In the **Auto VoIP VLAN ID** menu, select **5**.
   c. Click the **Apply** button. Your settings are saved.

DiffServ for IPv6

This feature extends the QoS ACL and DiffServ functionality by providing support for IPv6 packet classification.

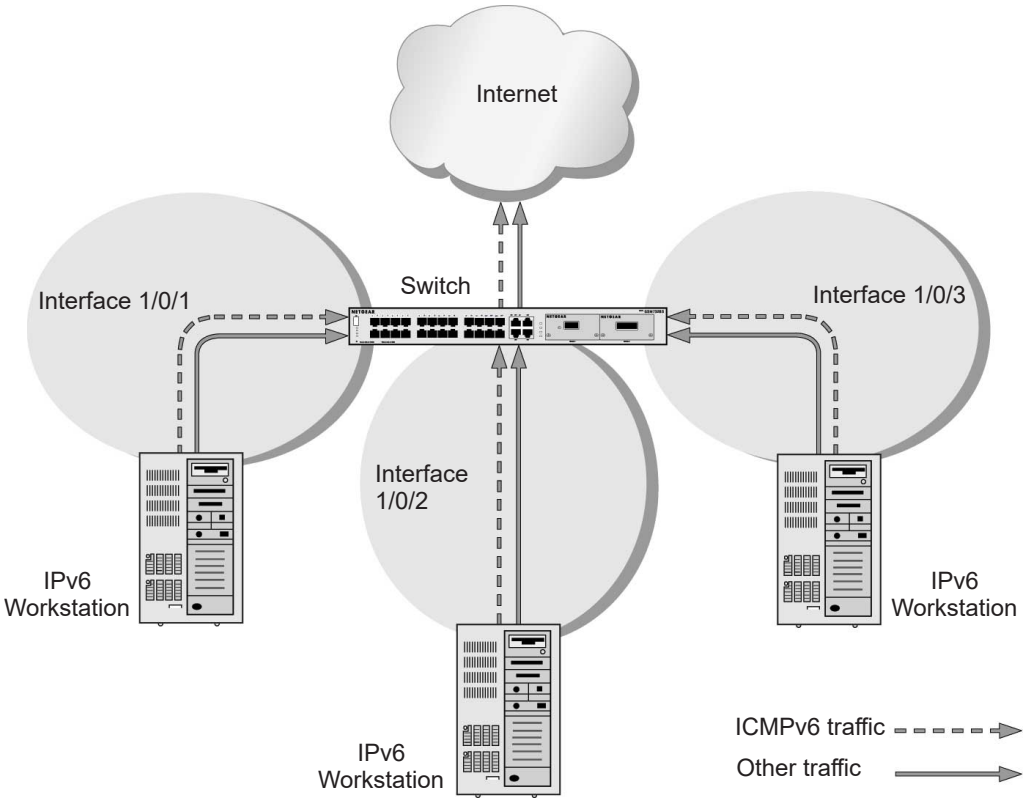


Figure 31. DiffServ for IPv6

The example is shown as CLI commands and as a main UI procedure.

CLI: Configure DiffServ for IPv6

To use the CLI 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:

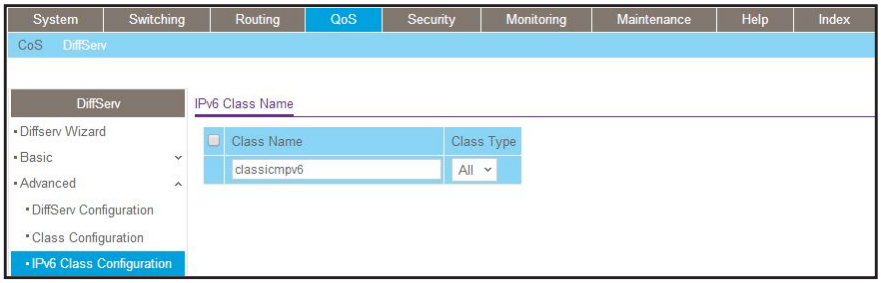
```
(Netgear Switch) (Config)# interface 1/0/1
(Netgear Switch) (Interface 1/0/1)# service-policy in policyicmpv6
(Netgear Switch) (Interface 1/0/1)# exit

(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
```

Main UI: Configure DiffServ for IPv6

To use the main UI to prioritize ICMPv6 traffic over other IPv6 traffic:

1. Create the IPv6 class classicmpv6.
   a. Select **QoS > DiffServ > Advanced > IPv6 Class Configuration**.

      A page similar to the following figure displays.

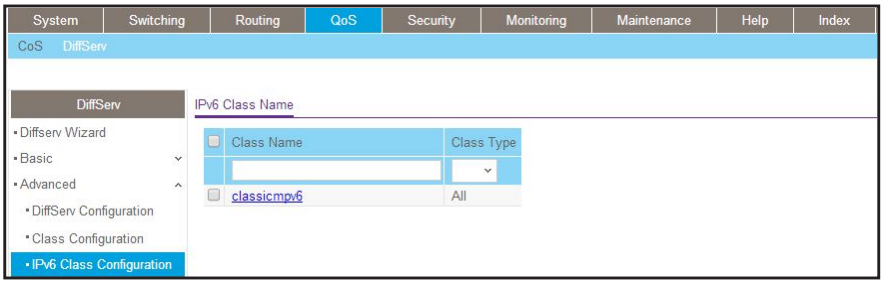


   b. In the **Class Name** field, enter **classicmpv6**.
   c. In the **Class Type** menu, select **All**.

      A page similar to the following figure displays.

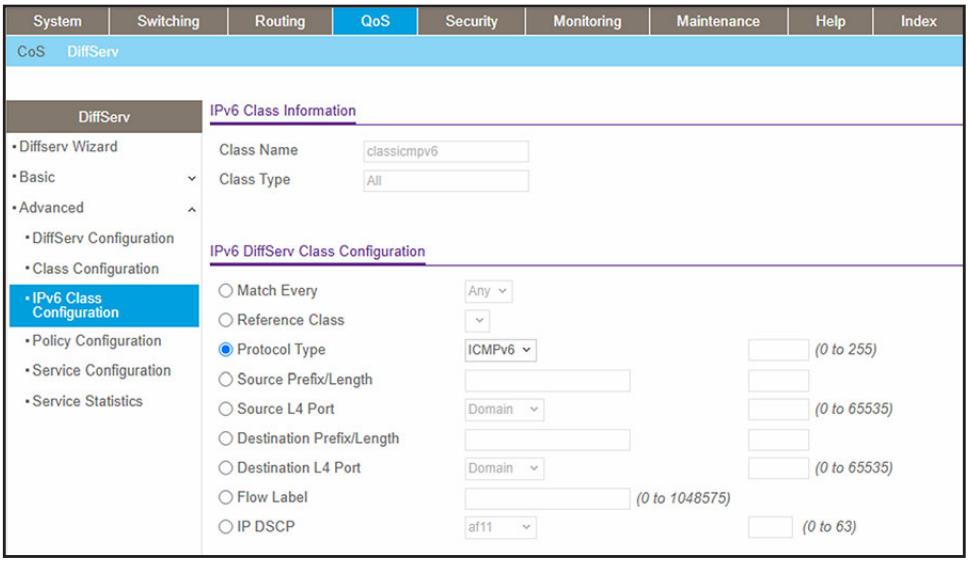
   d. Click the **Add** button. Your settings are saved.
2. Define matching criteria as protocol ICMPv6.
   a. Select **QoS > DiffServ > Advanced > IPv6 Class Configuration**.

      A page similar to the following figure displays.



   b. Click the Class Name **classicmpv6** link.

A page similar to the following figure displays.



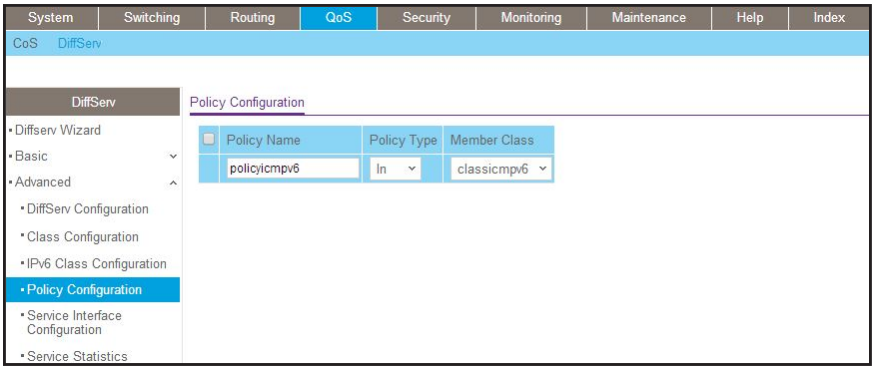
c. Select the **Protocol Type** radio button, and from the associated menu, select **ICMPv6**.

d. Click the **Apply** button. Your settings are saved.

3. Create the policy policyicmpv6, and associate the previously created class classicmpv6.

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

A page similar to the following figure displays.



b. In the **Policy Name** field, enter **policyicmpv6**.

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

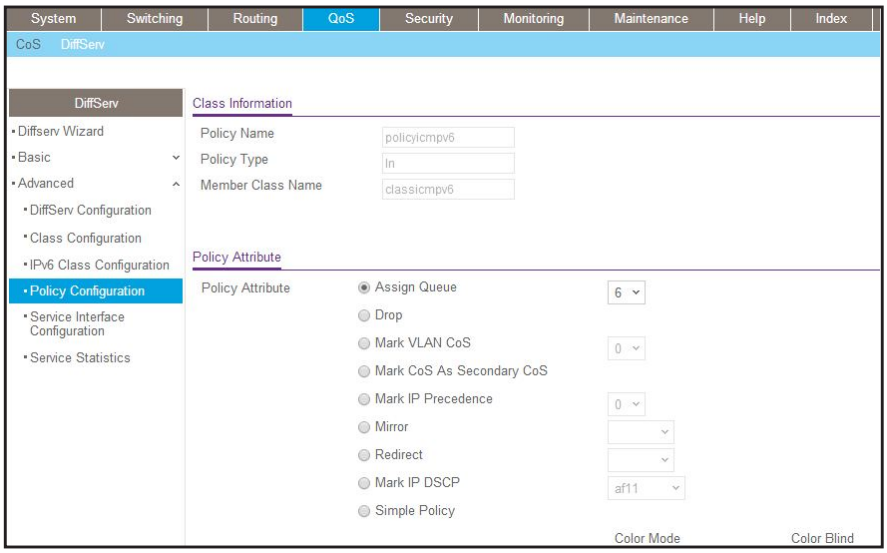
d. In the **Member Class** menu, select **classicmpv6**.

e. Click the **Add** button. Your settings are saved.

4. Set the attribute as assignment to queue 6.

a. Click the Policy Name **policyicmpv6**.

A page similar to the following figure displays.



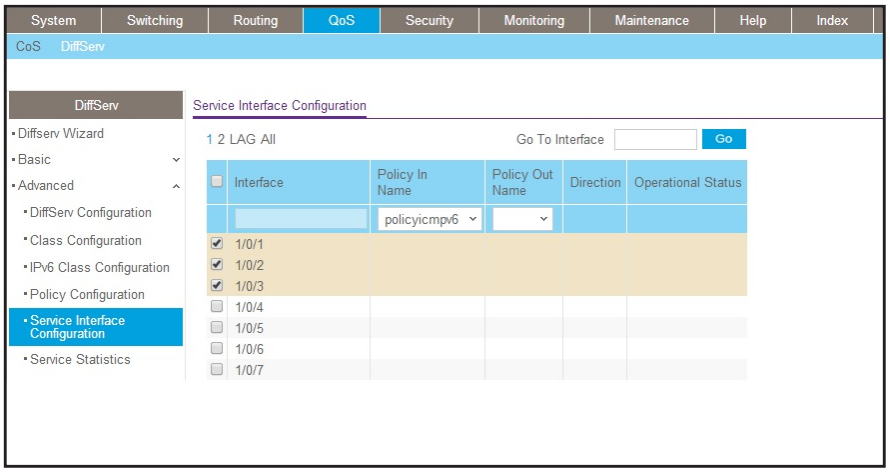
b. In the **Assign Queue** menu, select **6**.

c. Click the **Apply** button. Your settings are saved.

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 page similar to the following figure displays.



b. In the **Policy In Name** menu, select **policyicmpv6**.

c. Select the Interface **1/0/1**, **1/0/2**, and **1/0/3** check boxes.

d. Click the **Apply** button. Your settings are saved.

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 main UI procedure.

CLI: Configure a color conform policy

To use the CLI to configure a color conform policy:

1. Create 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 at a rate of 1000 kbps with an allowed burst size of 64 KB. Furthermore, the packets with IP precedence value of 7 must be colored green. That

means these packets must 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 the policy to port 1/0/13.

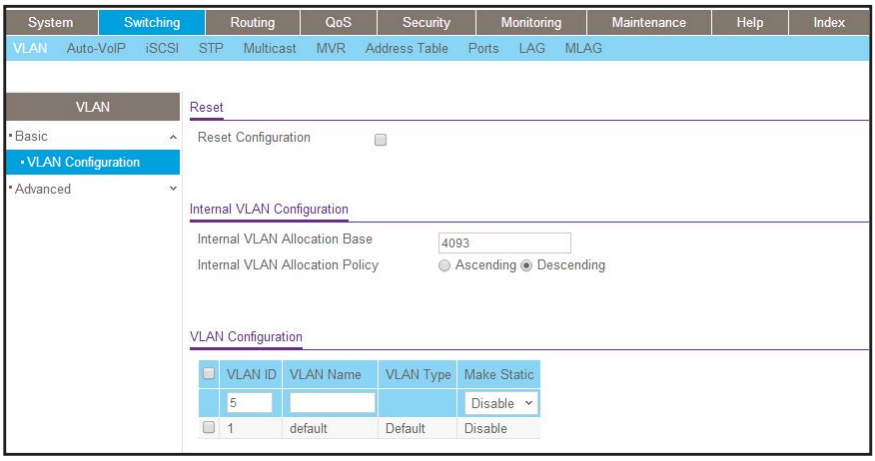
```
(Netgear Switch) (Config)#interface 1/0/13
(Netgear Switch) (Interface 1/0/13)#service-policy in policy_vlan
(Netgear Switch) (Interface 1/0/13)#exit
(Netgear Switch) (Config)#exit
```

Main UI: Configure a color conform policy

To use the main UI to configure a color conform policy:

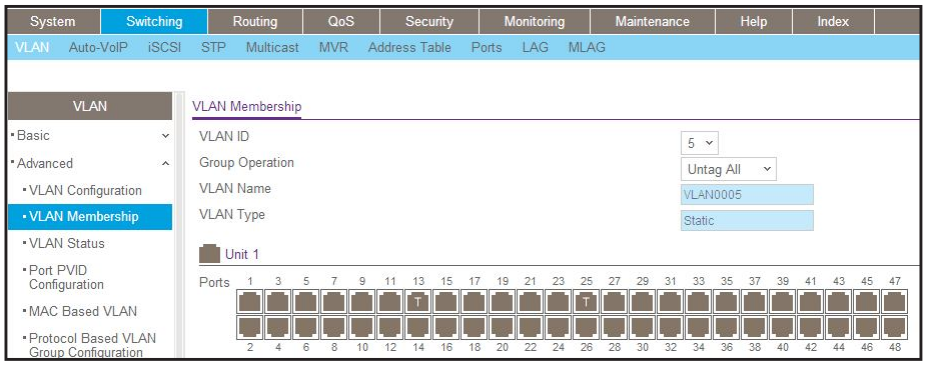
1. Create a VLAN.
   a. Select **Switching > VLAN > Basic > VLAN Configuration**.

      A page similar to the following figure displays.



   b. In the **VLAN ID** field, enter **5**.
   c. Click the **Add** button. Your settings are saved.
2. Add ports 1/0/13 and 1/0/25 to VLAN 5.
   a. Select **Switching > VLAN > Advanced > VLAN Membership**.

A page similar to the following figure displays.



b. In the **VLAN ID** menu, select **5**.

c. Click the gray boxes under ports **13** and **25** until T displays, which specifies that the egress packets are tagged for the ports.

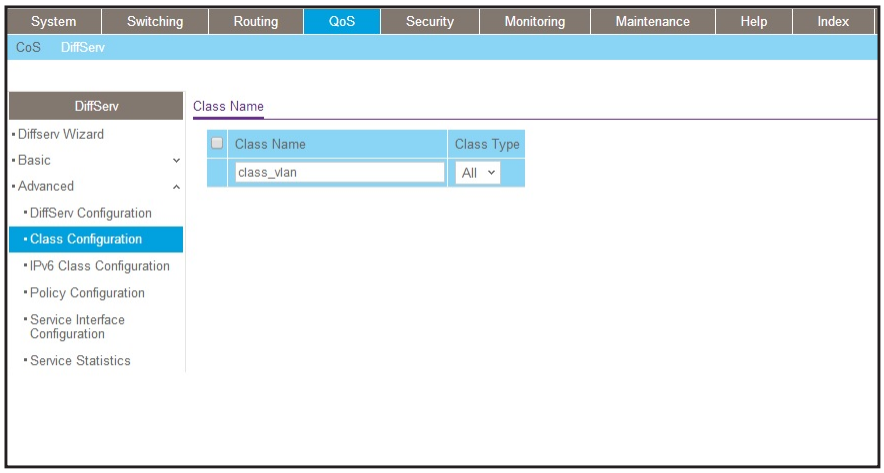
If your switch is a member of a stack, be sure that you select the ports in the correct unit.

d. Click the **Apply** button. Your settings are saved.

3. Create a class class_vlan:

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

A page similar to the following figure displays.

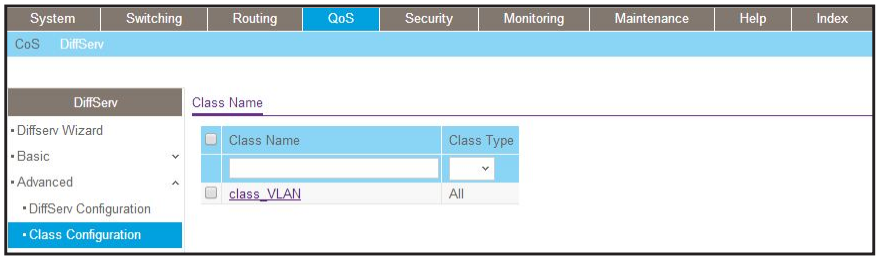


b. Configure the following settings:

- In the **Class Name** field, enter **class_vlan**.
- In the **Class Type** menu, select **All**.

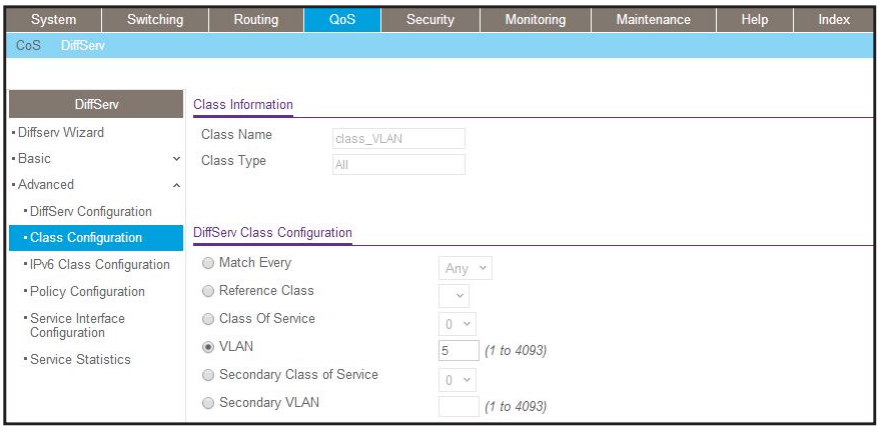
c. Click the **Add** button. Your settings are saved.

A page similar to the following figure displays.



d. Click the Class Name **class_vlan** link to configure this class.

A page similar to the following figure displays.



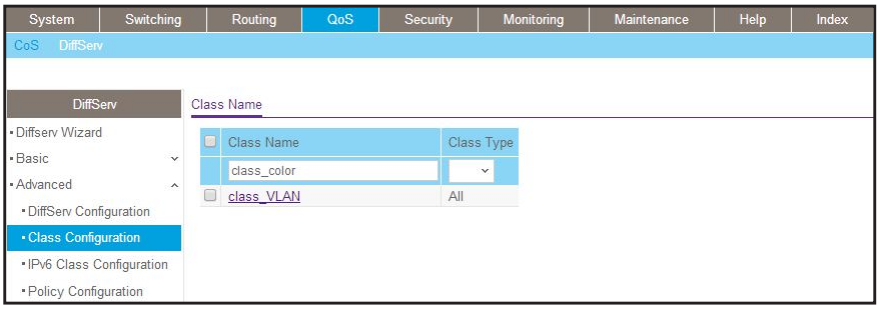
e. Under Diffserv Class Configuration, select the in the **VLAN** radio button, and in the associated field, enter **5**.

f. Click the **Apply** button. Your settings are saved.

4. Create a class class_color.

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

A page similar to the following figure displays.

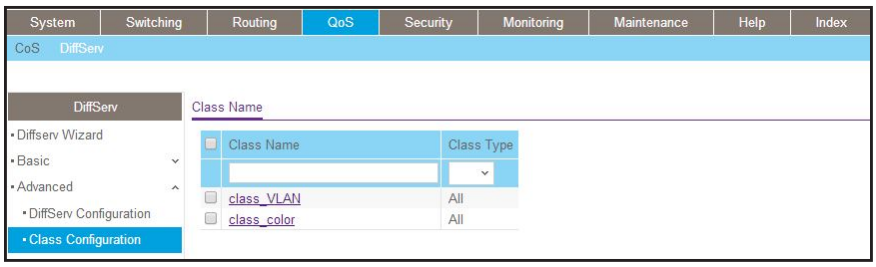


b. Configure the following settings:

- In the **Class Name** field, enter **class_color**.
- In the **Class Type** menu, select **All**.

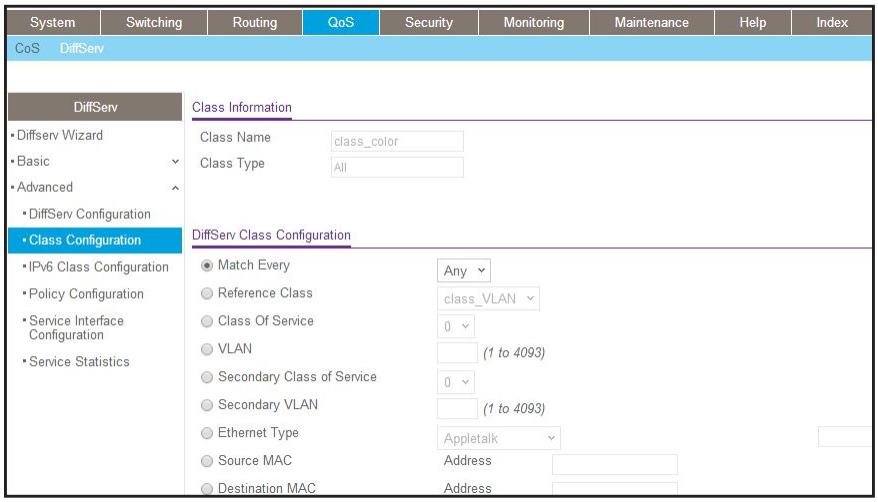
c. Click the **Add** button. Your settings are saved.

A page similar to the following figure displays.



d. Click the Class Name **class_color** link to configure this class.

A page similar to the following figure displays.



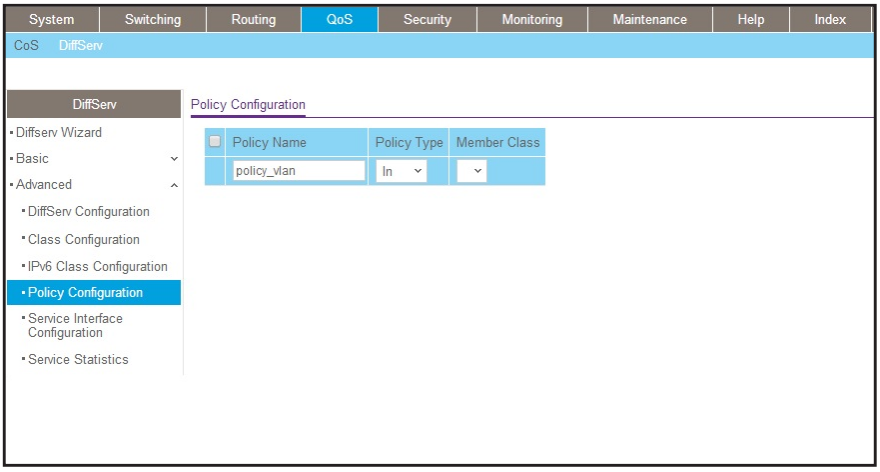
e. Under Diffserv Class Configuration, select the **Precedence Value** radio button, and in the associated field, select **7**.

f. Click the **Apply** button. Your settings are saved.

5. Create a policy policy_vlan.

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

A page similar to the following figure displays.



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

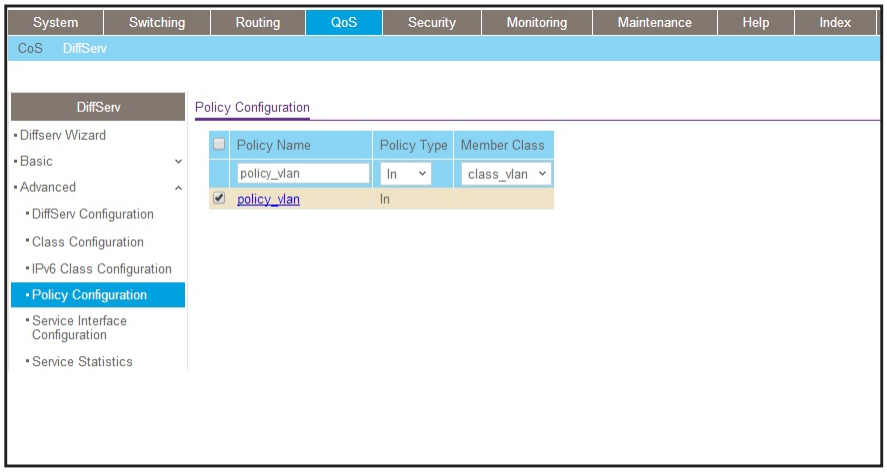
c. In the **Policy Type** menu, select **In**.

d. Click the **Add** button. Your settings are saved.

6. Associate policy_vlan with class_vlan.

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

A page similar to the following figure displays.



b. Select the **policy_vlan** check box.

c. In the **Member Class** field, enter **class_vlan**.

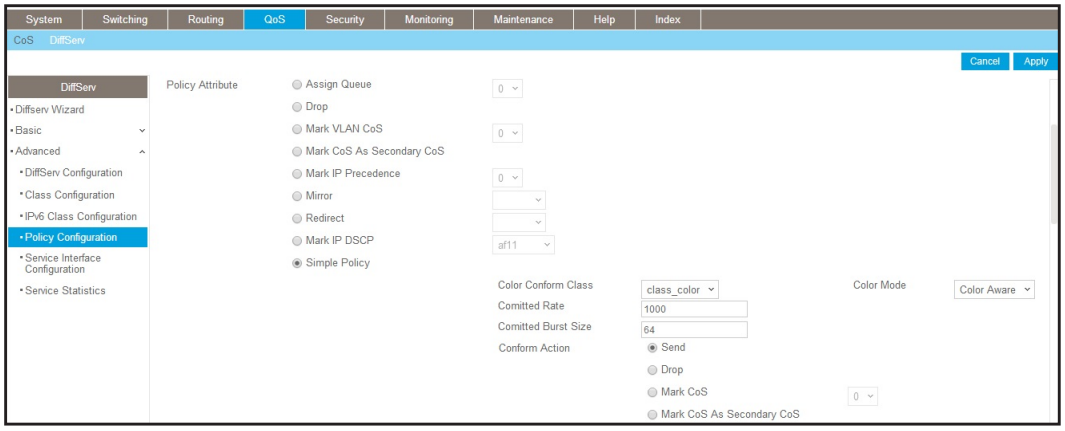
d. Click the **Apply** button. Your settings are saved.

7. Configure the policy policy_vlan.

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

b. Click **policy_vlan**.

A page similar to the following figure displays.



c. Select the **Simple Policy** radio button.

d. In the **Color Conform Class** menu, select **class_color**.

e. In the **Color Mode** menu, select **Color Aware**.

f. In the **Committed Rate** menu, select **kbps**, and in the associated field, enter **1000**.

g. In the **Committed Burst Size** field, enter **64**.

h. For Conform Action, select the **Send** radio button.

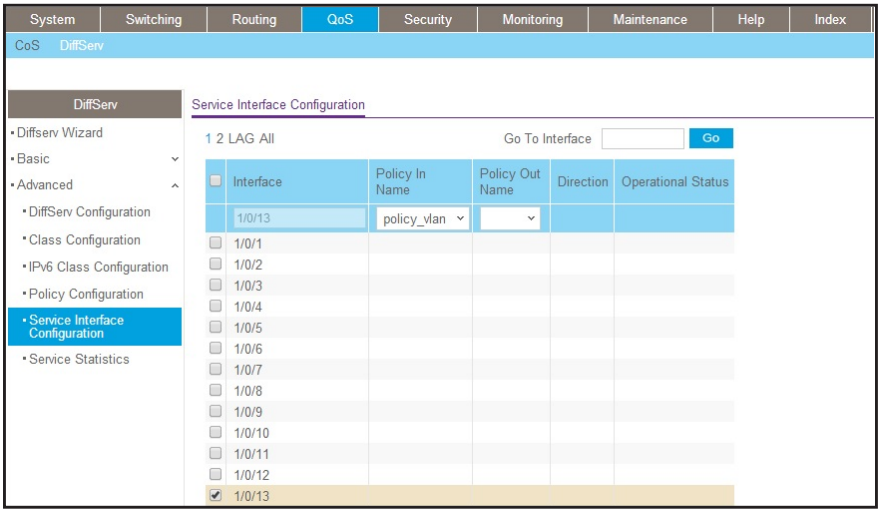
i. For Violate Action, select the **Drop** radio button.

j. Click the **Apply** button. Your settings are saved.

8. Apply policy_vlan to interface 1/0/13.

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

A page similar to the following figure displays.



b. Select the Interface **1/0/13** check box.

c. In the **Policy In Name** menu, select **policy_vlan**.

d. Click the **Apply** button. Your settings are saved.

Weighted random early detection

Weighted random early detection (WRED) 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 congestion occurs, 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.

In the following example, switch interface 1/0/25 is connected to a client with IP address 192.0.2.55, packets are assigned to queue 3, and WRED is configured on queue 3.

Figure 32. WRED configuration

To configure WRED:

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 192.0.2.55 255.255.255.255
(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 to port 1/0/25.

```
(Netgear Switch) (Config)#interface 1/0/25
(Netgear Switch) (Interface 1/0/25)#service-policy in p1
```

4. Assign packets with dot1p priority 3 to 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 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
```

14

IGMP Snooping and Querier

Internet Group Management Protocol features

This feature is supported on the M4250 series switches

This feature is supported on the M4300 series switches

This feature is supported on the M4350 series switches

This chapter includes the following sections:

- Internet Group Management Protocol concepts
- Enable IGMP snooping
- Display the IGMP snooping configuration
- Display the IGMP snooping group information
- Multicast router interface
- Multicast router VLAN
- IGMP Querier concepts
- Enable the IGMP querier
- Display the 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.

Enable IGMP snooping

The example is shown as CLI commands and as a main UI procedure.

CLI: Enable IGMP snooping

To use the CLI to globally enable IGMP snooping and enable IGMP snooping on a VLAN:

1. Globally enable IGMP snooping.

```
(Netgear Switch) #config
(Netgear Switch) (Config)#set igmp
(Netgear Switch) (Config)#exit
```

2. Enable IGMP snooping on a VLAN (in this example, on VLAN 300).

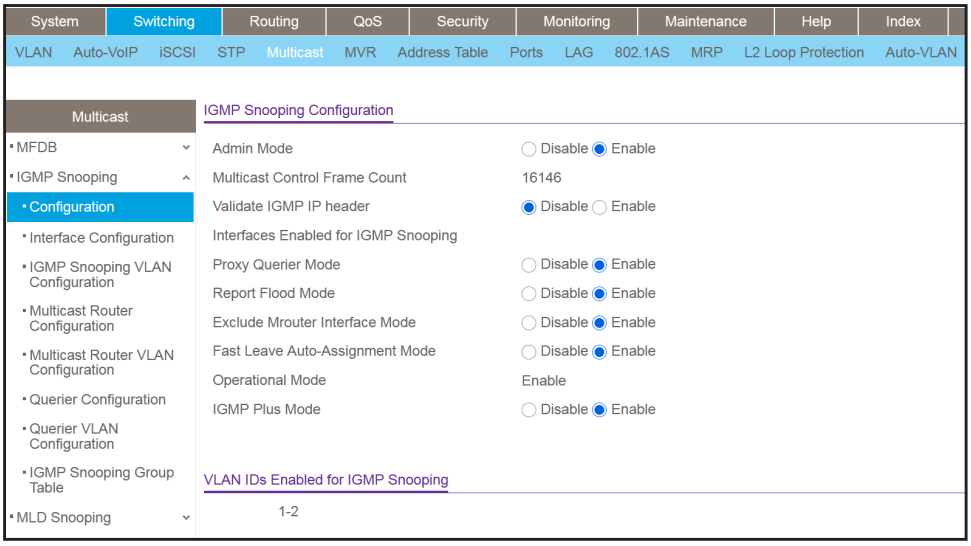
```
(Netgear Switch) #vlan database
(Netgear Switch) (Vlan)#set igmp 300
(Netgear Switch) (Vlan)#exit
```

Main UI: Enable IGMP snooping

To use the main UI to globally enable IGMP snooping and enable IGMP snooping on a VLAN:

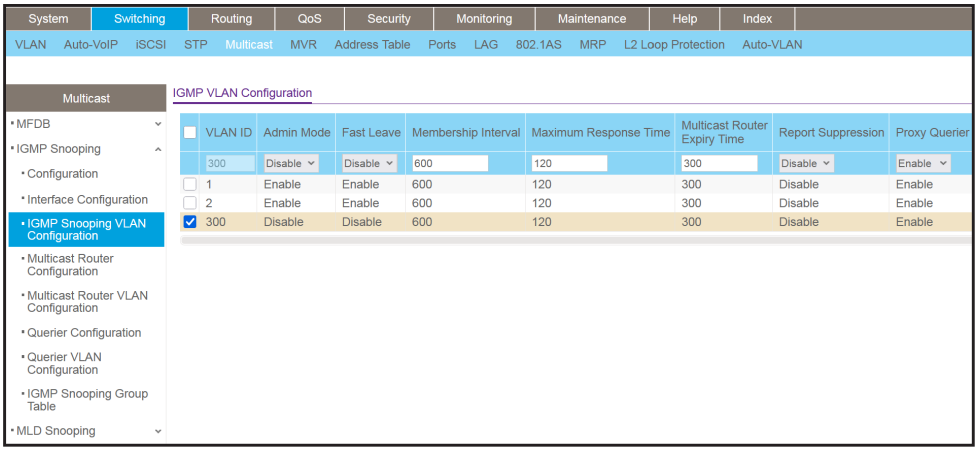
1. Globally enable IGMP snooping.
   a. Select **Switching > Multicast > IGMP Snooping > Configuration**.

      A page similar to the following figure displays.



   b. Select the Admin Mode **Enable** radio button.
   c. Click the **Apply** button. Your settings are saved.
2. Enable IGMP snooping on a VLAN (in this example, on VLAN 300).
   a. Select **Switching > Multicast > IGMP Snooping VLAN Configuration**.

      A page similar to the following figure displays.



   b. Select the VLAND ID **300** check box.
   c. In the **Admin Mode** menu, select **Enable**.

d. Click the **Apply** button. Your settings are saved.

Display the IGMP snooping configuration

The example is shown as CLI commands and as a main UI procedure.

CLI: Display the IGMP snooping configuration

To use the CLI to display the IGMP snooping configuration:

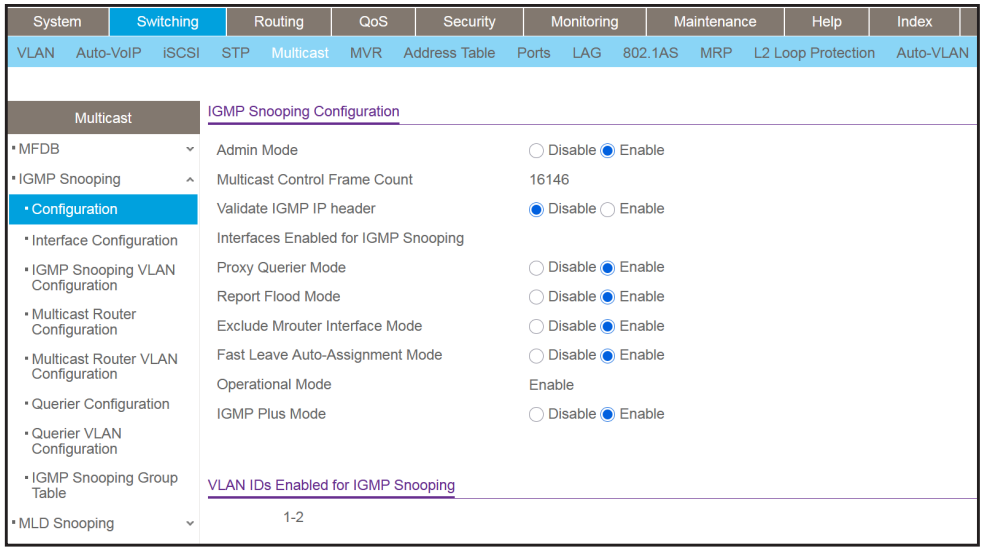
```
(Netgear Switch) #show igmpsnooping
Admin Mode..................................... Disable
Multicast Control Frame Count.................. 0
Interfaces Enabled for IGMP Snooping........... None
VLANs enabled for IGMP snooping................ None
```

Main UI: Display the IGMP snooping configuration

To use the main UI to display the IGMP snooping configuration:

Select **Switching > Multicast > IGMP Snooping Configuration**.

A page similar to the following figure displays.



Display the IGMP snooping group information

CLI: Display the IGMP snooping group table

You can use the **`show mac-address-table igmpsnooping`** command to display the MAC address table for IGMPv1 and IGMPv2 snooping. You can also use the **`show igmpsnooping ssm entries`** command to display the SSM entries for IGMPv3 snooping.

A better choice is the **`show igmpsnooping group`** command because it provides all multicast groups with their associated IP and MAC addresses.

To use the CLI to display the IGMP snooping group table:

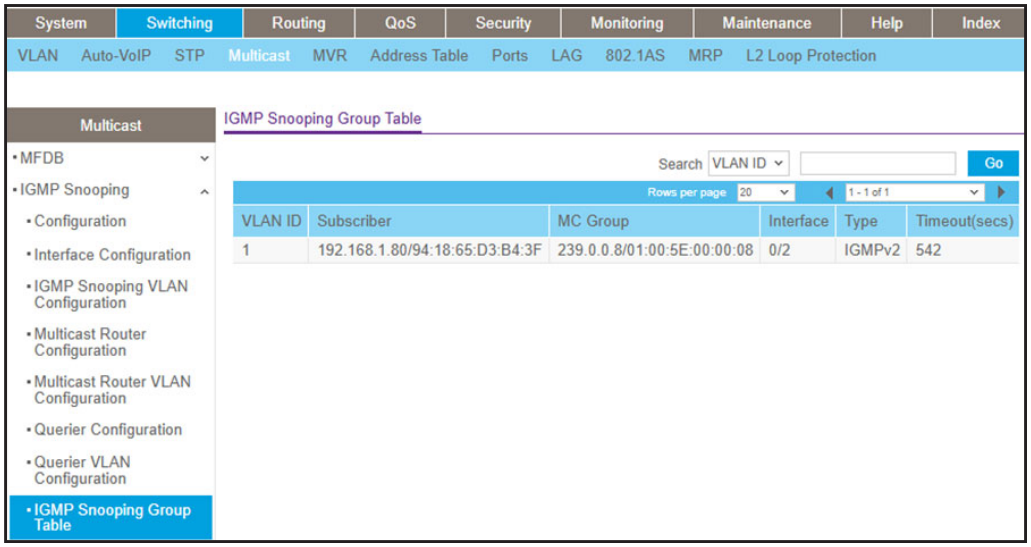
```
(Netgear Switch) #show igmpsnooping group

VLAN ID Subscriber                      MC Group                     Interface Type    Timeout(Sec)
------- ------------------------------- ---------------------------- --------- ------ ------------
1       192.168.1.80/94:18:65:D3:B4:3F  239.0.0.8/01:00:5E:00:00:08  0/2       IGMPv2  536
```

Main UI: Display the IGMP snooping group table

To use the main UI to display the IGMP snooping group table:

Select **Switching > Multicast > IGMP Snooping > IGMP Snooping Group Table**.

A page similar to the following figure displays.



Multicast router interface

This example configures a router interface that is attached to a multicast router. All IGMP packets that are snooped by the switch are forwarded to the multicast router that is reachable from this interface.

The example is shown as CLI commands and as a main UI procedure.

CLI: Configure a multicast router interface

To use the CLI to configure a router interface that is attached to a multicast router:

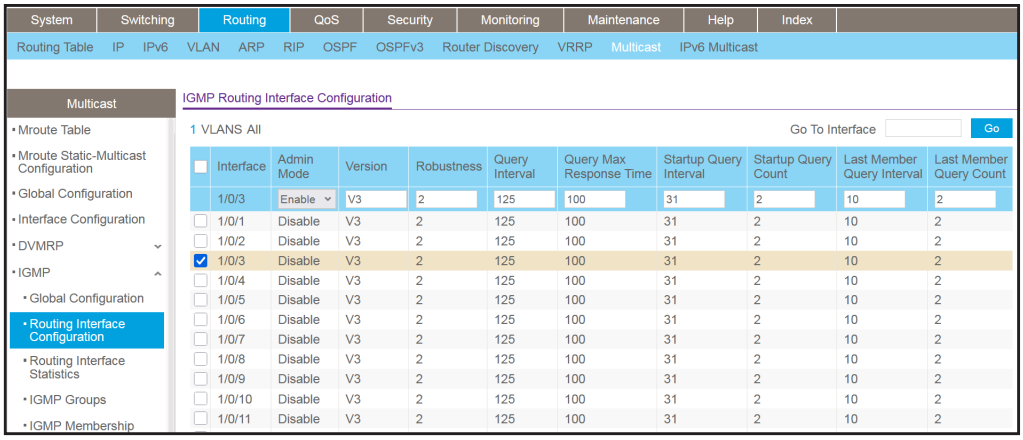
```
(Netgear Switch) interface 1/0/3
(Netgear Switch)(Interface 1/0/3)# set igmp mrouter interface
```

Main UI: Configure a multicast router interface

To use the main UI to configure a router interface that is attached to a multicast router:

1. Select **Routing > Multicast > IGMP > Routing Interface Configuration**.

   A page similar to the following figure displays.



2. Select the Interface **1/0/3** check box.
3. In the **Admin Mode** menu, select **Enable**.
4. Click the **Apply** button. Your settings are saved.

Multicast router VLAN

This example configures a router interface to forward only the snooped IGMP packets from a specific VLAN ID to a multicast router that is attached to the router interface.

The example is shown as CLI commands and as a main UI procedure.

CLI: Configure a multicast router VLAN

To use the CLI to configure a router interface to forward only the snooped IGMP packets from a specific VLAN ID:

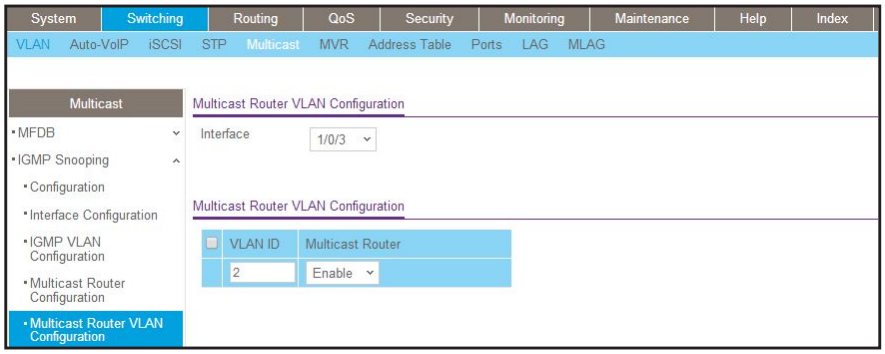
```
(Netgear Switch) interface 1/0/3
(Netgear Switch)(Interface 1/0/3)# set igmp mrouter 2
```

Main UI: Configure a multicast router VLAN

To use the main UI to configure a router interface to forward only the snooped IGMP packets from a specific VLAN ID:

1. Select **Switching > Multicast > IGMP Snooping > Multicast Router VLAN Configuration**.

   A page similar to the following figure displays.



2. Select the Interface **1/0/3** check box.
3. Configure the following settings:
   - In the **VLAN ID** field, enter **2**.
   - In the **Multicast Router** menu, select **Enable**.
4. Click the **Apply** button. Your settings are saved.

IGMP Querier concepts

If you use the switch 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. You can enable IGMP snooping 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 clients to respond. Because the switch supports the IGMP querier feature, such an external device is not required.

Because the IGMP querier functions with IGMP snooping, you must enable IGMP snooping.

The following figure shows a network application for video streaming service using the IGMP querier feature.

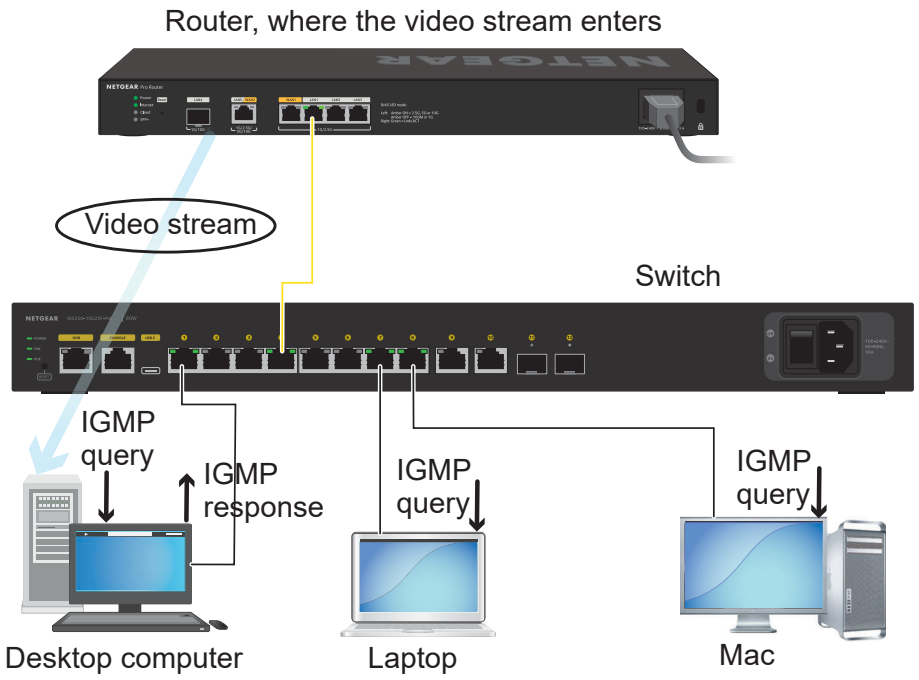


Figure 33. IGMP Querier

Enable the IGMP querier

This example configures the switch to generate an IGMP querier packet for a VLAN 1, which is then transmitted to every port on the VLAN. The source IP address in querier packets is 10.10.10.1.

The example is shown as CLI commands and as a main UI procedure.

CLI: Enable the IGMP querier

To use the CLI to enable the IGMP querier:

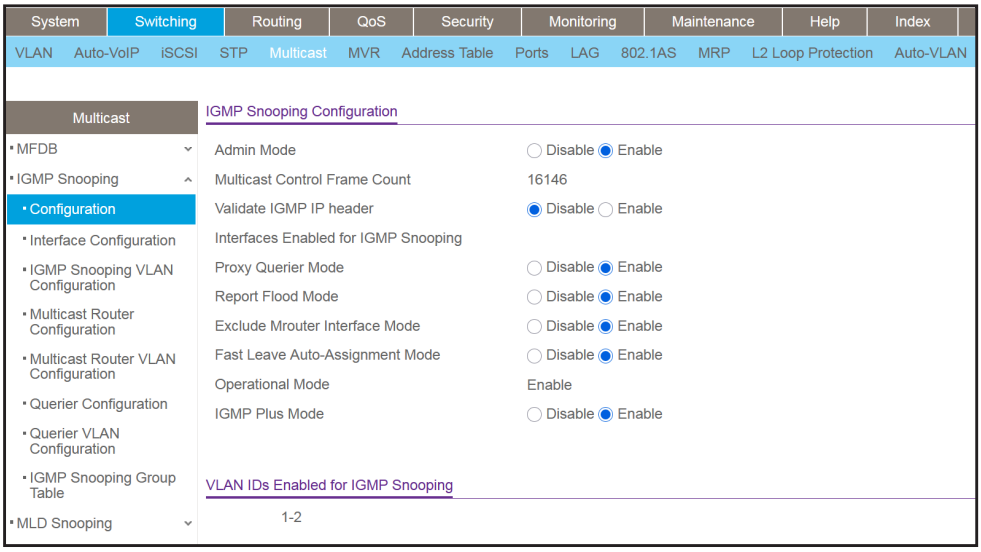
```
(Netgear switch) #vlan database
(Netgear switch) (vlan)#set igmp 1
(Netgear switch) (vlan)#set igmp querier 1
(Netgear switch) (vlan)#exit
(Netgear switch) #config
(Netgear switch) (config)#set igmp querier
(Netgear switch) (config)#set igmp querier address 10.10.10.1
(Netgear switch) (config)#exit
```

Main UI: Enable the IGMP Querier

To use the main UI to enable the IGMP querier:

1. Enable IGMP snooping.
   a. Select **Switching > Multicast > IGMP Snooping > Configuration**.

   A page similar to the following figure displays.

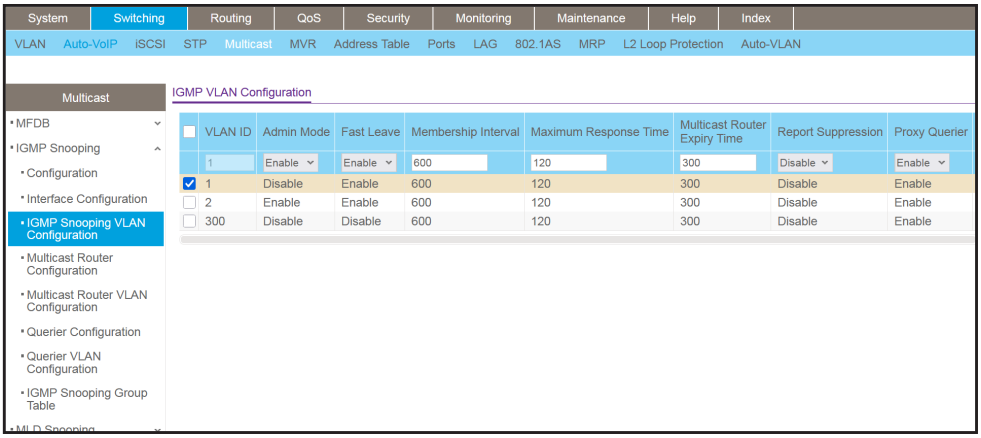


b. Select the Admin Mode **Enable** radio button.

2. Enable IGMP snooping on VLAN 1.

a. Select **Switching > Multicast > IGMP Snooping > IGMP Snooping VLAN Configuration**.

A page similar to the following figure displays.



b. Configure the following settings:

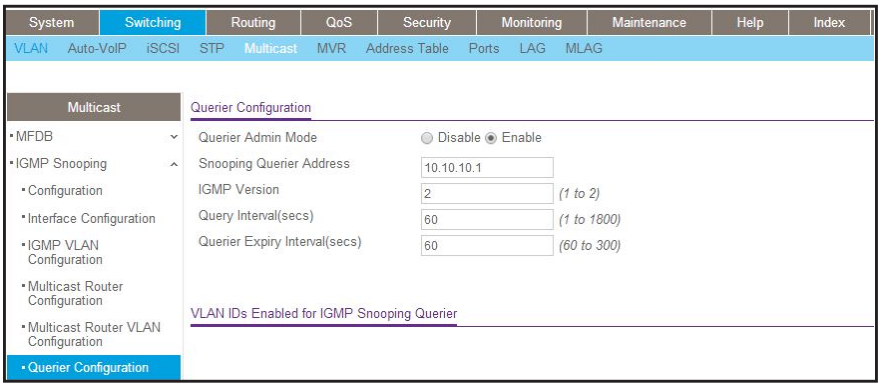
- In the **VLAN ID** field, enter **1**.
- In the **Admin Mode** menu, select **Enable**.

c. Click the **Apply** button. Your settings are saved.

3. Enable the IGMP snooping querier globally.

a. Select **Switching > Multicast > IGMP Snooping > Querier Configuration**.

A page similar to the following figure displays.



b. Configure the following settings:

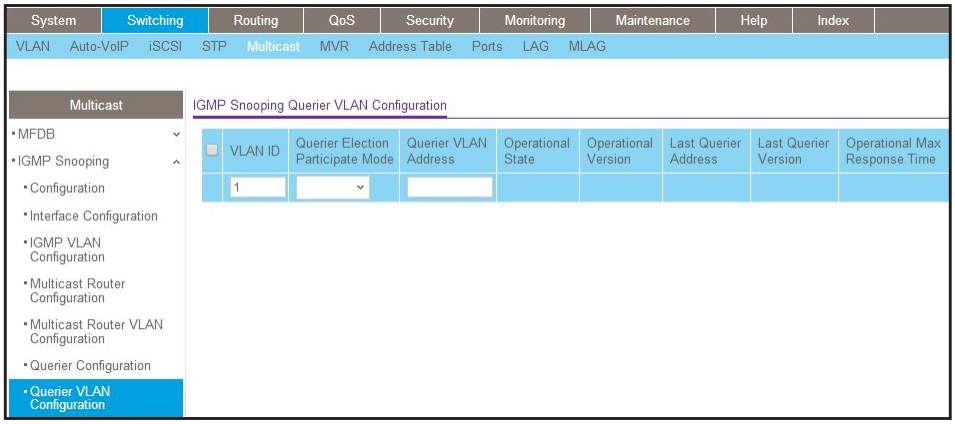
- Select the Querier Admin Mode **Enable** radio button.
- In the **Snooping Querier Address** field, enter **10.10.10.1**.

c. Click the **Apply** button. Your settings are saved.

4. Enable the IGMP snooping querier on VLAN 1.

a. Select **Switching > Multicast > IGMP Snooping > Querier VLAN Configuration**.

A page similar to the following figure displays.



b. In the **VLAN ID** field, enter **1**.

5. Click the **Add** button. Your settings are saved.

Display the IGMP querier status

The example is shown as CLI commands and as a main UI procedure.

CLI: Display the IGMP querier status

To use the CLI to display IGMP querier status:

```
(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
```

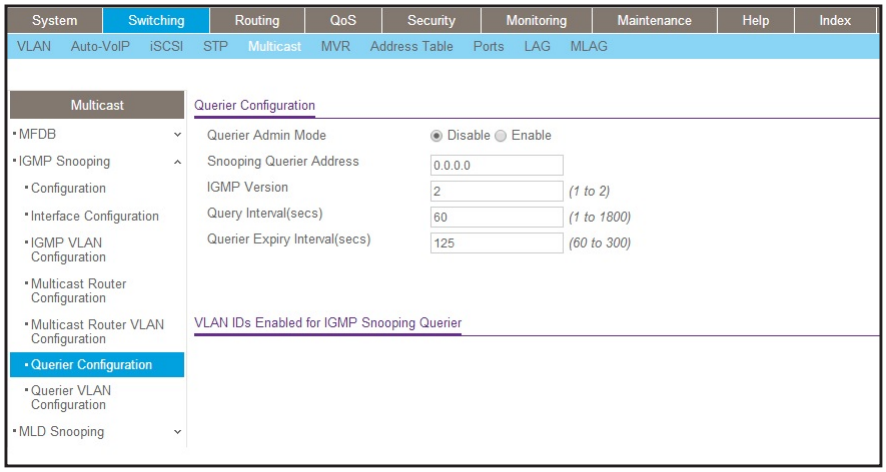
The command shows that the IGMP admin mode is Active. The mode is controlled by the **`set igmp`** command. If the mode is inactive, no query packet is sent.

Main UI: Display IGMP querier status

To use the main UI to display IGMP querier status:

Select **Switching > Multicast > IGMP Snooping > Querier Configuration**.

A page similar to the following figure displays.



15

MVR

Multicast VLAN registration

This feature is supported on the M4250 series switches

This feature is supported on the M4300 series switches

This feature is supported on the M4350 series switches

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 distributes multicast traffic to all ports, even if receivers are connected to only a few ports. The IGMP snooping protocol resolves this issue so that multicast traffic is distributed only to the receivers that request it.

Multicast VLAN registration (MVR) resolves the same issue if receivers are located in different VLANs. After you manually configure a VLAN, called the multicast VLAN, MVR allows multicast traffic to be forwarded over a Layer 2 network in conjunction with IGMP snooping.

MVR, like the IGMP snooping protocol, lets a Layer 2 switch snoop on the IGMP control protocol. Both protocols operate independently of each other. You can enable both protocols on the switch interfaces at the same time. In such a case, MVR listens to the join and report messages only for groups that are statically configured. All other groups are managed by IGMP snooping.

MVR functions with source ports and receiver ports:

- **Source port**: The port to which the multicast traffic flows using the multicast VLAN.
- **Receiver port**: The port to which a listening host is connected. The port 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 that is 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 prevent duplication of multicast streams for clients in different VLANs. You must configure the multicast VLAN manually for all source ports in the network. The following figure shows a diagram of a network that is configured for MVR. (SP is the source port and RP is a receiver port.)

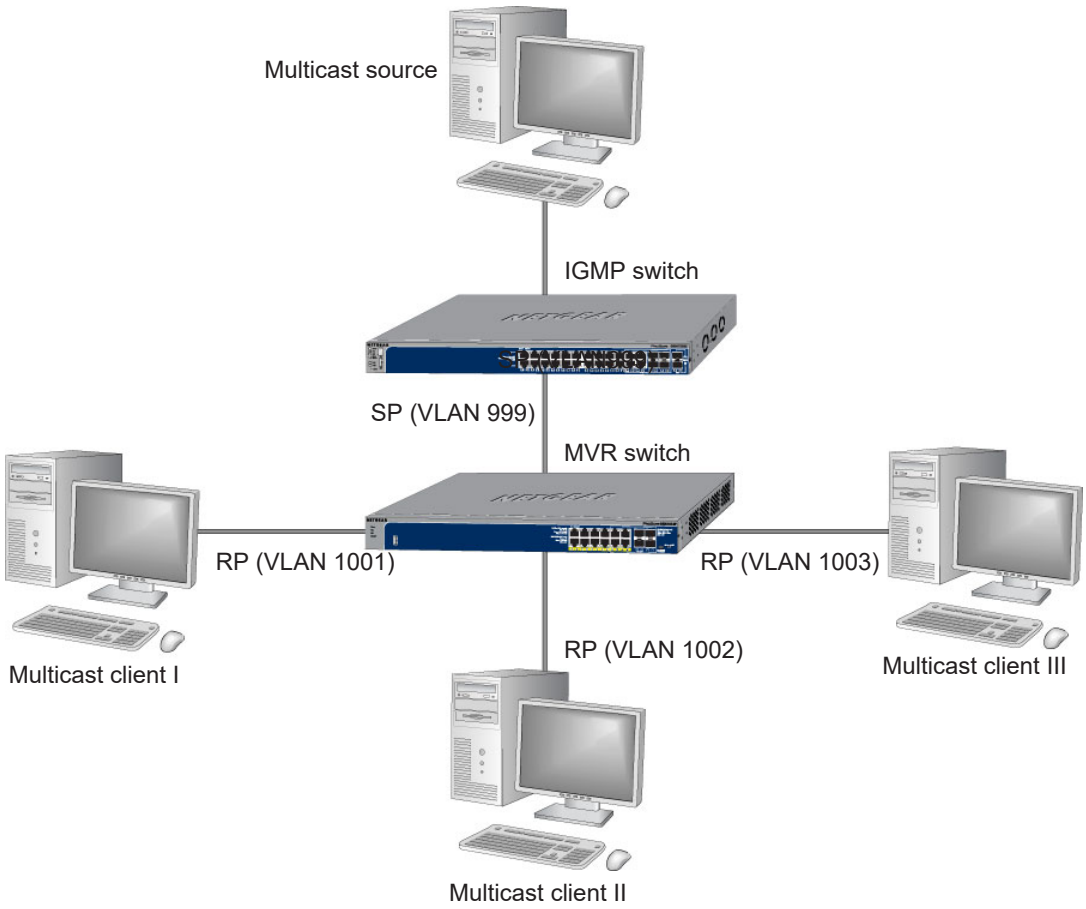


Figure 34. Network configured for MVR

Configure MVR in compatible mode

In compatible mode, the MVR switch does not learn multicast groups; You must configure the groups because MVR does not forward IGMP reports from the hosts (RP ports) to the IGMP router (SP port). To operate in this mode, you must statically configure the IGMP router (or switch functioning as an IGMP router) to transmit all required multicast streams to the MVR switch.

The example is shown as CLI commands and as a main UI procedure.

CLI: Configure MVR in compatible mode

To use the CLI to configure MVR in compatible mode:

1. Create multicast VLAN (MVLAN) 999, VLAN 1 with ID 1001, VLAN 2 with ID 1002, and VLAN 3 with ID 1003.

```
(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 compatible mode.

```
(Netgear Switch) (Config)#mvr mode compatible
```

Note: The MVR default setting is compatible. If you did not yet configure MVR, you can omit this step.

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 receiver ports.

Note: A receiver port can participate in one VLAN only.

```
(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
```

6. Display the MVR status.

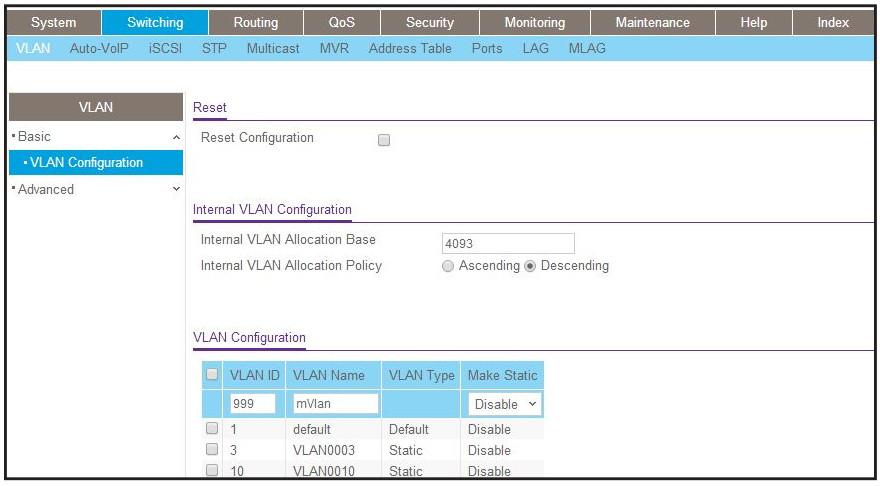
```
(Netgear Switch) #show mvr
MVR Running...................... TRUE
MVR multicast VLAN............... 999
MVR Max Multicast Groups.......... 256
MVR Current multicast groups...... 1
MVR Global query response time.... 5 (tenths of sec)
MVR Mode......................... compatible

(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
```

Main UI: Configure MVR in compatible mode

To use the main UI to configure MVR in compatible mode:

1. Create multicast VLAN (MVLAN) 999, VLAN 1 with ID 1001, VLAN 2 with ID 1002, and VLAN 3 with ID 1003.
   a. Select **Switching > VLAN > Basic > VLAN Configuration**.

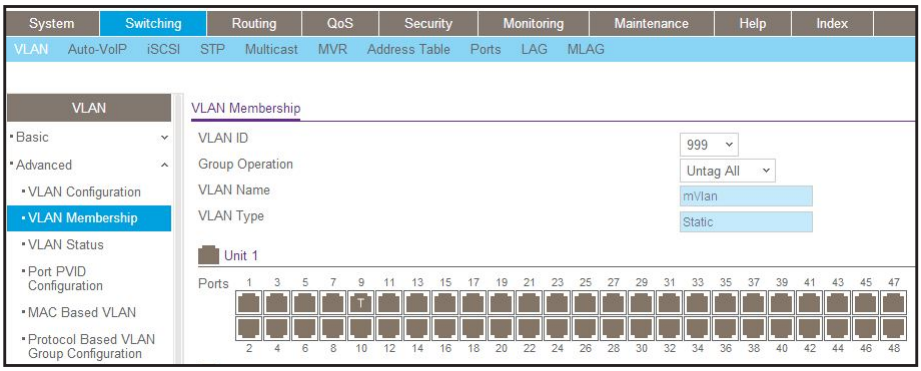
      A page similar to the following figure displays.



   b. In the VLAN ID field, enter **999**, and in the VLAN Name field, enter **mVlan**.
   c. Click the **Add** button. Your settings are saved.
   d. Repeat the previous two steps to create VLAN 1 with ID 1001, VLAN 2 with ID 1002, and VLAN 3 with ID 1003.

2. Add port 9 to MVLAN 999 with tagged mode.
   a. Select **Switching > VLAN > Advanced > VLAN Membership**.

      A page similar to the following figure displays.

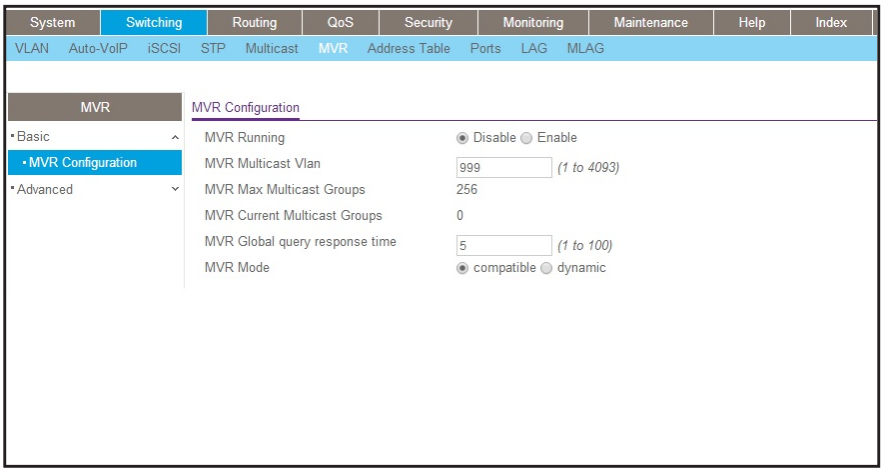


   b. In the **VLAN ID** menu, select **999**.
   c. Click the gray box under port **9** until T displays. The T specifies that the egress packets are tagged for the port.

      If your switch is a member of a stack, be sure that you select the port in the correct unit.

   d. Click the **Apply** button. Your settings are saved.
   e. Repeat the previous three steps to add port 0/1 as a tagged port to VLAN 1 with ID 1001, port 0/5 as a tagged port to VLAN 2 with ID 1002, and port 0/7 as a tagged port to VLAN 3 with ID 1003.
3. Enable MVR and multicast VLAN.
   a. Select **Switching > MVR > Basic > MVR Configuration**.

      A page similar to the following figure displays.



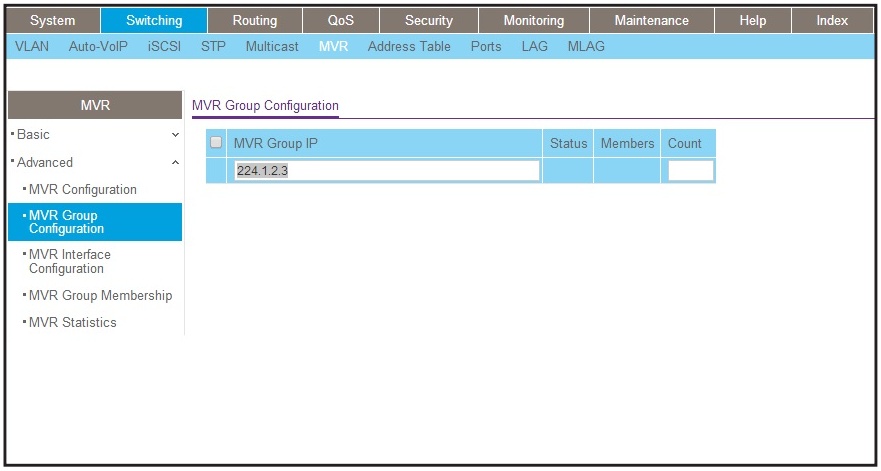
   b. Select the MVR Running **Enable** radio button.
   c. In the **MVR Multicast VLAN** field, enter **999**.
   d. Select the MVR Mode **compatible** radio button.

e. Click the **Apply** button. Your settings are saved.

4. Add multicast group 224.1.2.3 to MVR.

a. Select **Switching > MVR > Basic > MVR Group Configuration**.

A page similar to the following figure displays.



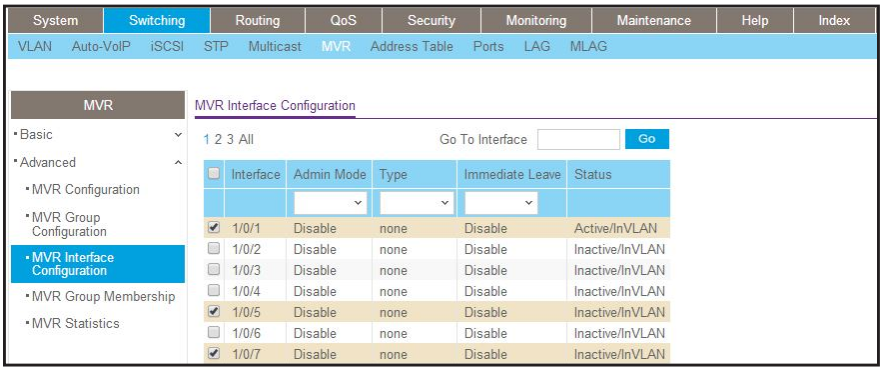
b. In the **MVR Group IP** field, enter **224.1.2.3**.

c. Click the **Add** button. Your settings are saved.

5. Configure interfaces 0/1, 0/5, and 0/7 as receiver ports.

a. Select **Switching > MVR > Basic > MVR Interface Configuration**.

A page similar to the following figure displays.



b. Select the Interface **0/1**, **0/5** and **0/7** check boxes.

c. Configure the following settings:

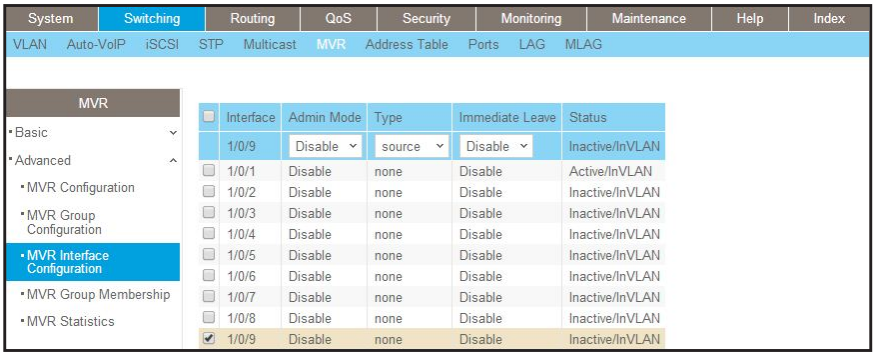
- In the **Admin Mode** menu, select **Enable**.
- In the **Type** menu, select **receiver**.

d. Click the **Apply** button. Your settings are saved.

6. Configure interface 0/9 as the source port.

a. Select **Switching > MVR > Basic > MVR Interface Configuration**.

A page similar to the following figure displays.



b. Select the Interface **0/9** check box.

c. Configure the following settings:

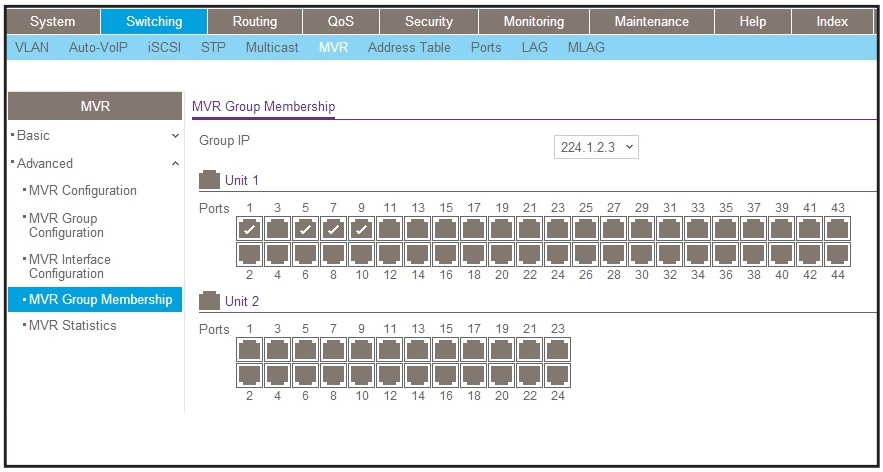
- In the **Admin Mode** menu, select **Enable**.
- In the **Type** menu, select **source**.

d. Click the **Apply** button. Your settings are saved.

7. Configure MVR Group Membership.

a. Select **Switching > MVR > Advanced > MVR Membership**.

A page similar to the following figure displays.



b. In the **Group IP** menu, select **224.1.2.3**.

c. Click the gray box under ports **1**, **5**, and **7**. A check mark displays in the box.

If your switch is a member of a stack, be sure that you select the ports in the correct unit.

Note: Port 9 is already in MVR group 224.1.2.3 because it is configured as the source port.

d. Click the **Apply** button. Your settings are saved.

Configure MVR in dynamic mode

In dynamic mode, the MVR switch learns existing multicast groups by snooping the IGMP queries from a router (or switch functioning as a router) on source ports and forwarding the IGMP reports from the hosts to the IGMP router on the multicast VLAN (with the translation of the VLAN ID).

The example is shown as CLI commands and as a main UI procedure.

CLI: Configure MVR in dynamic mode

To use the CLI to configure MVR in dynamic mode:

1. Create multicast VLAN (MVLAN) 999, VLAN 1 with ID 1001, VLAN 2 with ID 1002, and VLAN 3 with ID 1003.

```
(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 receiver ports.

Note: A receiver port can participate in one VLAN only.

```
(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. 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......................... dynamic

(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
```

After port 0/1 receives an IGMP report for multicast group 224.1.2.3, the port is added to the MVR group 224.1.2.3.

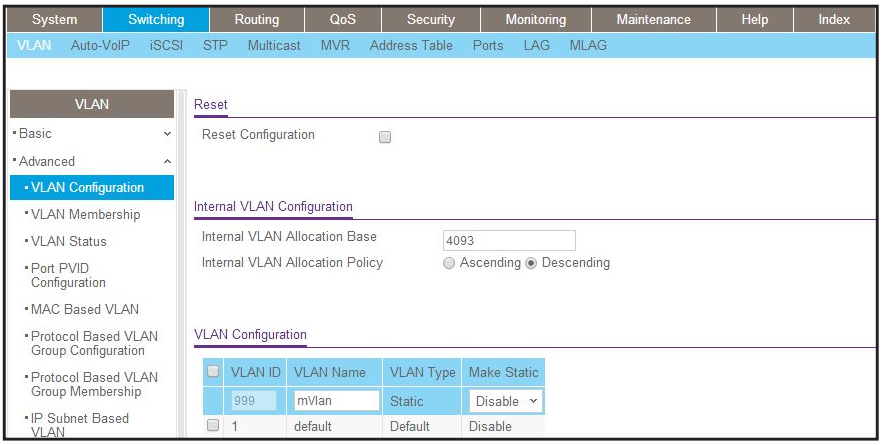
```
(Netgear Switch) #show mvr members

MVR Group IP         Status               Members
---------------     ---------------     ----------------------------------
224.1.2.3           ACTIVE              0/1(d)
```

Main UI: Configure MVR in dynamic mode

To use the main UI to configure MVR in dynamic mode:

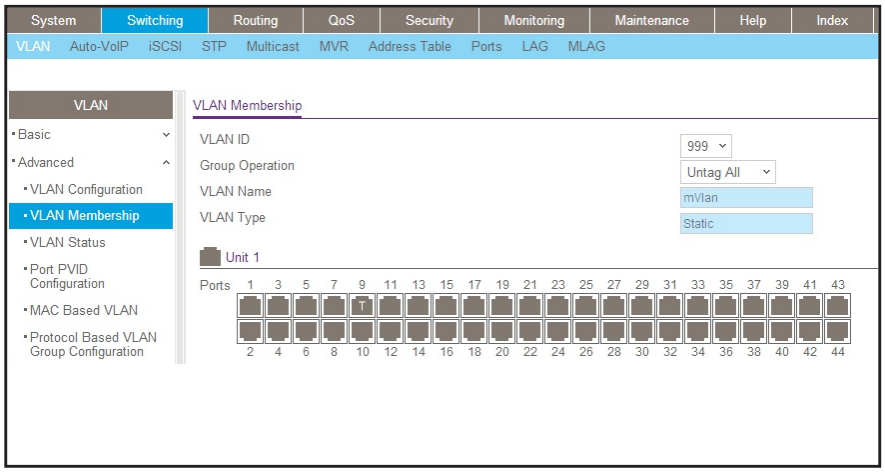
1. Create multicast VLAN (MVLAN) 999, VLAN 1 with ID 1001, VLAN 2 with ID 1002, and VLAN 3 with ID 1003.
   a. Select **Switching > VLAN > Basic > VLAN Configuration**.

      A page similar to the following figure displays.



   b. In the VLAN ID field, enter **999**, and in the VLAN Name field, enter **mVlan**.
   c. Click the **Add** button. Your settings are saved.
   d. Repeat the previous two steps to create VLAN 1 with ID 1001, VLAN 2 with ID 1002, and VLAN 3 with ID 1003.
2. Add port 9 to MVLAN 999 with tagged mode.
   a. Select **Switching > VLAN > Advanced > VLAN Membership**.

      A page similar to the following figure displays.



   b. In the **VLAN ID** menu, select **999**.

c. Click the gray box under port **9** until T displays. The T specifies that the egress packets are tagged for the port.

   If your switch is a member of a stack, be sure that you select the port in the correct unit.

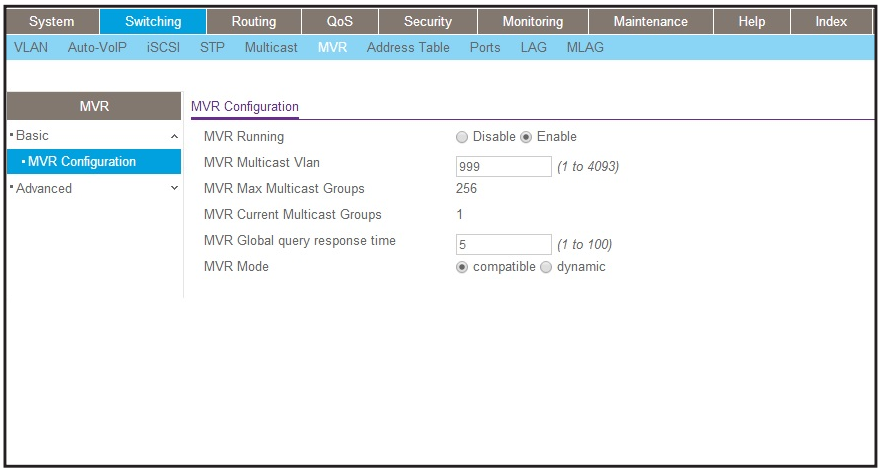
d. Click the **Apply** button. Your settings are saved.

e. Repeat the previous three steps to add port 0/1 as a tagged port to VLAN 1 with ID 1001, port 0/5 as a tagged port to VLAN 2 with ID 1002, and port 0/7 as a tagged port to VLAN 3 with ID 1003.

3. Enable MVR and multicast VLAN.

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

      A page similar to the following figure displays.



   b. Select the **Enable** radio button.

   c. In the **MVR Multicast VLAN** field, enter **999**.

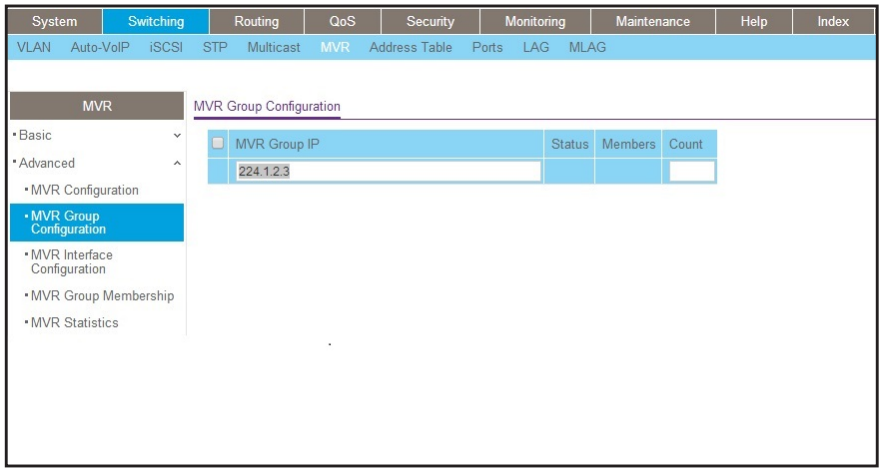
   d. Select the MVR mode **dynamic** radio button.

   e. Click the **Apply** button. Your settings are saved.

4. Add multicast group 224.1.2.3 to the MVR.

   a. Select **Switching > MVR > Basic > MVR Group Configuration**.

A page similar to the following figure displays.



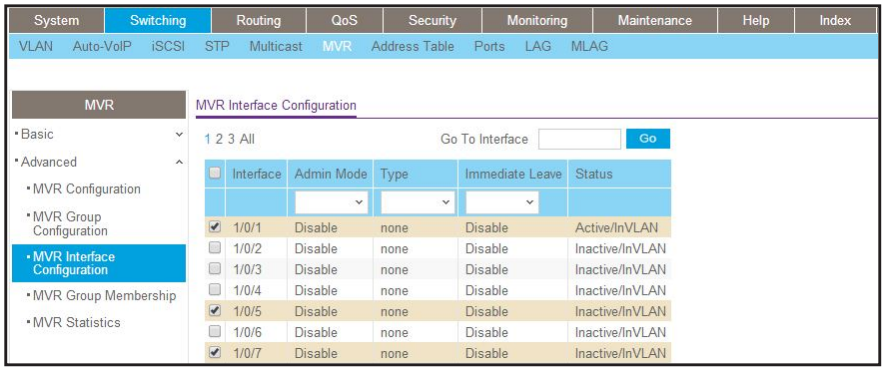
b. In the **MVR Group IP** field, enter **224.1.2.3**.

c. Click the **Add** button. Your settings are saved.

5. Configure interfaces 0/1, 0/5, and 0/7 as receiver ports.

a. Select **Switching > MVR > Basic > MVR Interface Configuration**.

A page similar to the following figure displays.



b. Select the Interface **0/1**, **0/5** and **0/7** check boxes.

c. Configure the following settings:

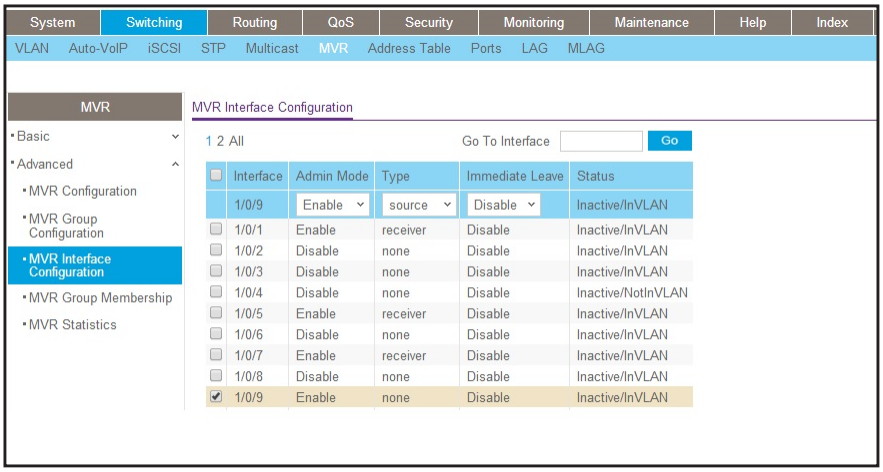
- In the **Admin Mode** menu, select **Enable**.
- In the **Type** menu, select **receiver**.

d. Click the **Apply** button. Your settings are saved.

6. Configure interface 0/9 as the source port.

a. Select **Switching > MVR > Basic > MVR Interface Configuration**.

A page similar to the following figure displays.



b. Select the Interface **0/9** check box.

c. Configure the following settings:

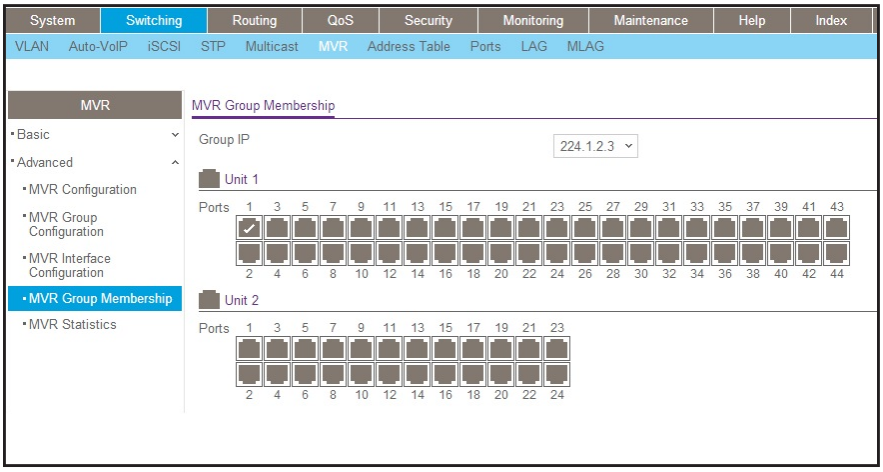
- In the **Admin Mode** menu, select **Enable**.
- In the **Type** menu, select **source**.

d. Click the **Apply** button. Your settings are saved.

Because this is dynamic MVR, you do not need to configure MVR group membership.

After port 1 receives an IGMP report for multicast group 224.1.2.3, the port is added to MVR group 224.1.2.3, as is then displayed on the **Switching > MVR > Advanced > MVR Group Membership** page.

A page similar to the following figure displays.



16

MAB

MAC Authentication Bypass

This feature is supported on the M4250 series switches

This feature is supported on the M4300 series switches

This feature is supported on the M4350 series switches

This chapter includes the following sections:

- MAC Authentication Bypass concepts
- MAB and authentication servers
- Configure MAC authentication bypass on a switch

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.

For MAB, you must preconfigure the known and allowable MAC addresses and corresponding access rights on the authentication server.

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 format (that is, a nondotted decimal MAC format) as the user name and the password that is associated with EAP-MD5, PAP, or CHAP, depending on the MAB authentication type that you configured.
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 transmit 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.

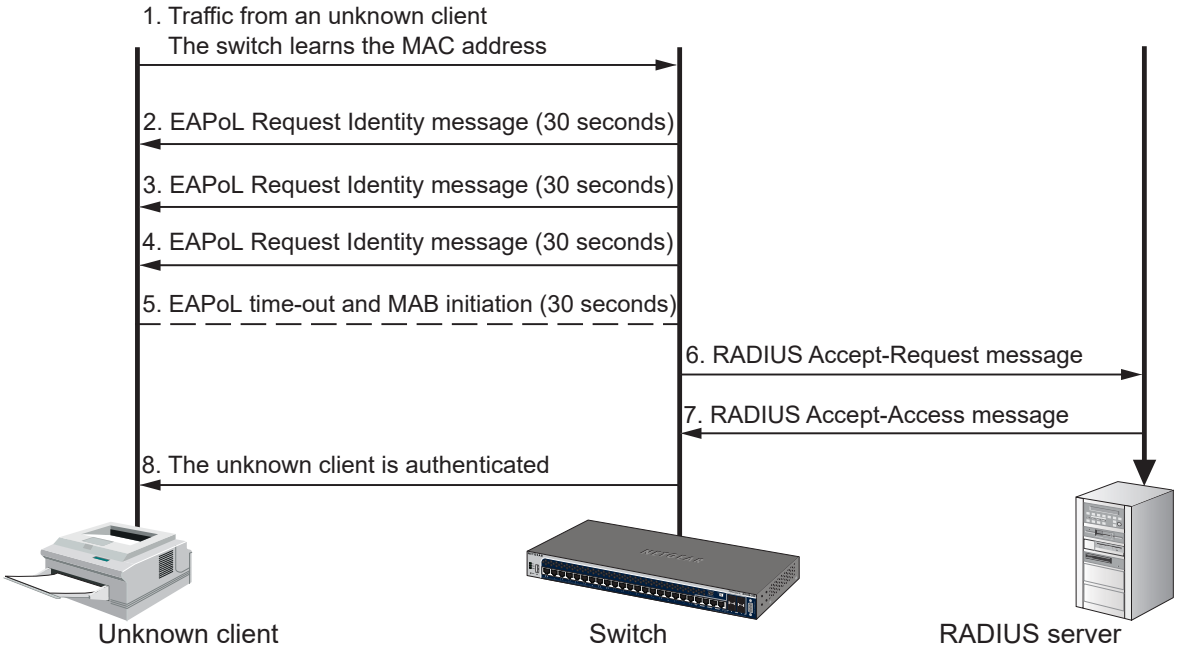


Figure 35. MAB operation

MAB and authentication servers

An authentication server can authenticate and then accept or reject a client that wants to access the network. When you use MAB for access to your network, the network must be able to reach an authentication server application such as a network policy server (NPS), RADIUS server (as in the previous figure), TACACs server, or active directory server.

Multiple third-party authentication server applications are available, including the following:

- **Microsoft**:
  - https://learn.microsoft.com/en-us/windows-server/networking/technologies/nps/nps-top
  - https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/get-started/virtual-dc/active-directory-domain-services-overview
- **FreeRADIUS**: https://www.freeradius.org/
- **Secure W2**: https://www.securew2.com/products/cloud-radius
- **Electron**: https://www.electronjs.org/
- **Xperience Technologies**: https://xperiencetech.com/
- **Cisco**: https://www.cisco.com/site/us/en/products/security/identity-services-engine/index.html
- **ManageEngine**: https://www.manageengine.com/

Configure MAC authentication bypass on a switch

The following figure shows a switch that has MAB configured on port 0/1. The IP phone that is connected to this port can access the network after being authenticated successfully by the network policy server or RADIUS server.

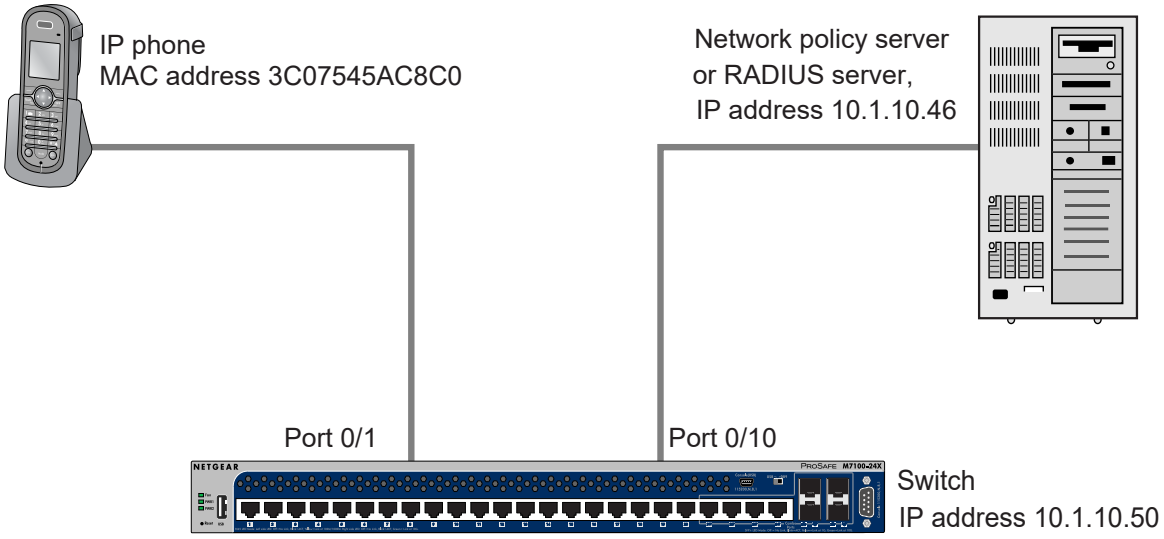


Figure 36. MAB topology with a switch, IP phone, and server

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 main UI procedure.

CLI: Configure the switch to perform MAB with a RADIUS server

To use the CLI to configure the switch to perform MAB with a RADIUS server:

1. Enable authentication on the switch.

```
(Netgear Switch) #config
(Netgear Switch) (Config)#authentication enable
```

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 RADIUS 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 RADIUS server (port 0/10 in this example).

```
(Netgear Switch) (Config)#interface 0/10
(Netgear Switch) (Interface 0/10)#authentication port-control force-authorized
(Netgear Switch) (Interface 0/10)#exit
```

5. Configure MAB on the port that connects to the IP phone (port 0/1 in this example).

```
((Netgear Switch) #configure
(Netgear Switch) (Config)#interface 0/1
(Netgear Switch) (Interface 0/1)#mab
(Netgear Switch) (Interface 0/1)#mab auth-type chap
(Netgear Switch) (Interface 0/1)#exit
```

6. To reduce the MAB authentication time, decrease the time of guest VLAN period.

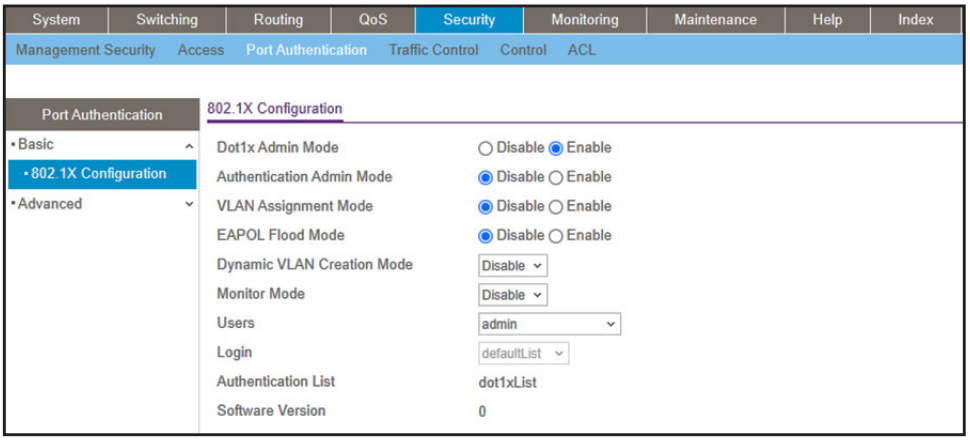
```
(Netgear Switch) #config
(Netgear Switch) (Config)#interface 0/1
(Netgear Switch) (Interface 0/1)#dot1x max-reauth-req 1
(Netgear Switch) (Interface 0/1)#dot1x timeout tx-period 10
```

Main UI: Configure the switch to perform MAB with a RADIUS server

To use the main UI to configure the switch to perform MAB with a RADIUS server:

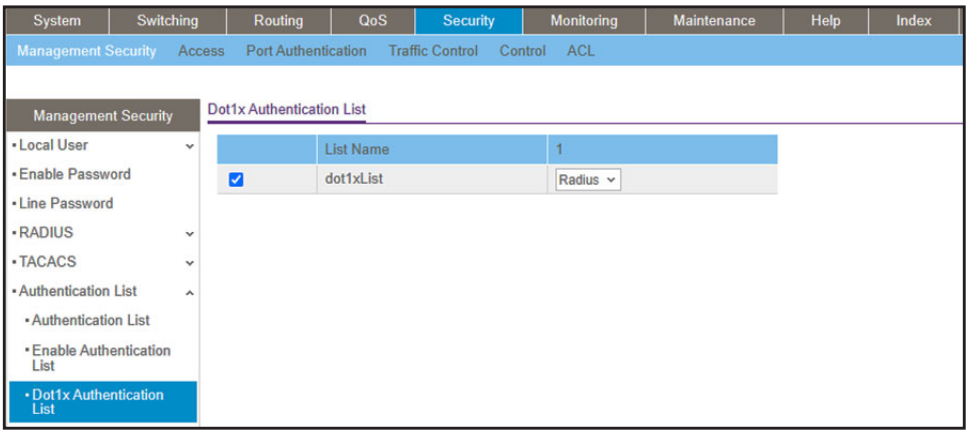
1. Enable authentication on the switch:
   a. Select **Security > Port Authentication > Basic > 802.1X Configuration**.

      A page similar to the following figure displays.



   b. Select the Dot1x Admin Mode **Enable** radio button.
   c. Select the Authentication Admin Mode **Enable** radio button
   d. Click the **Apply** button. Your settings are saved.
2. Configure RADIUS to authenticate 802.1X users:
   a. Select **Security > Management Security > Authentication List > Dot1x Authentication List**.

      A page similar to the following figure displays.



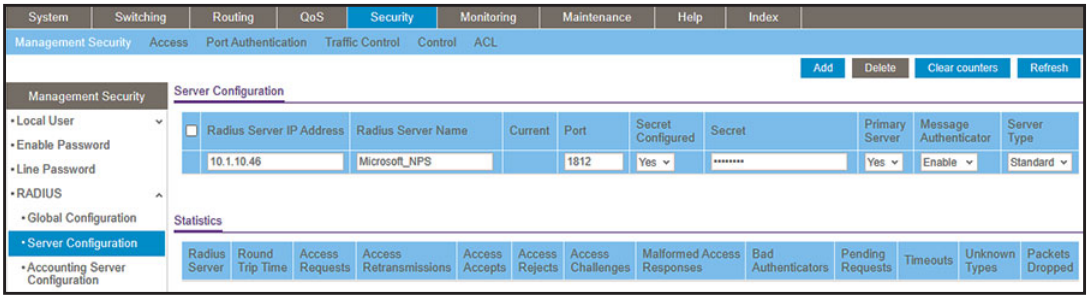
   b. Select the **dot1xList** check box.
   c. In the **1** menu, select **Radius**.
   d. Click the **Apply** button. Your settings are saved.

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 page similar to the following figure displays.



   b. Configure the following settings:

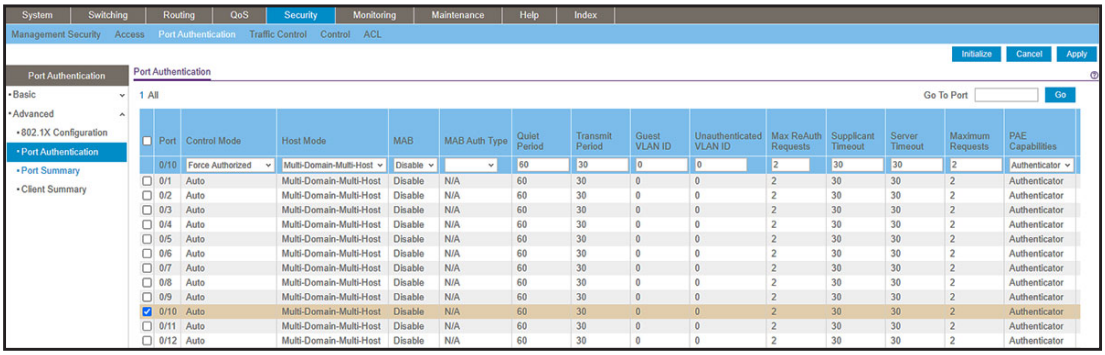
      - In the **RADIUS Server IP Address** field, enter **10.1.10.46**.
      - In the **RADIUS Server Name** field, enter **Microsoft-NPS.**
      - In the **Port** field, enter **1812.**
      - In the **Secret Configured** menu, select **Yes**.
      - In the **Secret** field, enter the secret key.
      - In the **Primary Server** menu, select **Yes**.
      - In the **Message Authenticator** menu, select **Enable**.
      - In the **Server Type** menu, select **Standard**.

   c. Click the **Add** button. Your settings are saved.

4. Configure the port that connects to the Microsoft network policy server (in this example, port 0/10) to be force-authorized:

   a. Select **Security > Port Authentication > Advanced > Port Authentication**.

      A page similar to the following figure displays.



   b. Select the Port **0/10** check box.

   c. Configure the following settings:

      - In the **Control Mode** menu, select **Force Authorized**.

- In the **MAB** menu, select **Disable**.

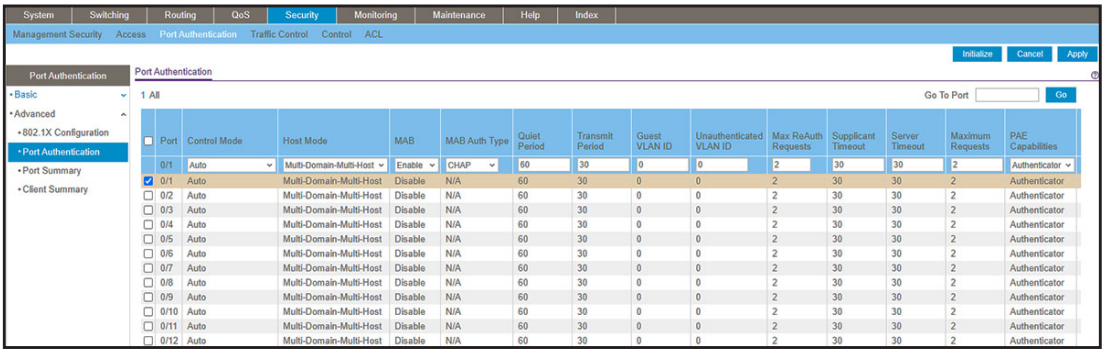
  Leave all other settings on the page at their default value.

d. Click the **Apply** button. Your settings are saved.

5. Configure the port that connects to the IP phone (in this example, port 0/1) for MAB:

a. Select **Security > Port Authentication > Advanced > Port Authentication**.

A page similar to the following figure displays.



b. Select the Port **0/1** check box.

c. Configure the following settings:

- In the **MAB** menu, select **Enable**.
- In the **MAB Auth Type** menu, select **CHAP**.

  Leave all other settings on the page at their default value.

d. Click the **Apply** button. Your settings are saved.

17

Security Management

Port security features

This feature is supported on the M4250 series switches

This feature is supported on the M4300 series switches

This feature is supported on the M4350 series switches

This chapter includes the following sections:

- Port security concepts
- Set dynamic and static MAC address limits on a port
- Convert dynamically learned MAC addresses to static addresses
- Create a static MAC address
- Protected ports
- 802.1x port security
- Create a guest VLAN
- Assign VLANs using RADIUS
- Dynamic ARP inspection
- Static mapping for dynamic ARP inspection
- DHCP snooping
- Find a rogue DHCP server
- Enter a static binding into the binding database
- Maximum rate of DHCP messages
- IP Source Guard
- Command authorization for the CLI
- Privileged Exec Command mode authorization for the CLI
- Accounting
- Use the authentication manager to set up an authentication method list
- RADIUS change of authorization
- IPv6 Stateless RA Guard
- Change SSH and Telnet login authentication to RADIUS

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 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, which you can use 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 data sheets. 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 time out if another packet with that address is not detected within the time-out time. You can set the time-out value. Dynamically locked MAC addresses can still be learned by another port.
- **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. Static MAC addresses do not time-out.

Set dynamic and static MAC address limits on a port

The example is shown as CLI commands and as a main UI procedure.

CLI: Set the dynamic and static MAC address limits on a port

To use the CLI to set the dynamic and static MAC address limits on port 1/0/1:

1. Enable port-security globally.

```
(Netgear Switch) Config
(Netgear Switch) (Config)#
(Netgear Switch) (Config)#port-security
```

2. Enable port-security on port 1/0/1, set the dynamic limit to ten addresses, and set the static limit to three addresses.

```
(Netgear Switch) (Config)#interface 1/0/1
(Netgear Switch) (Interface 1/0/1)#
(Netgear Switch) (Interface 1/0/1)#port-security
(Netgear Switch) (Interface 1/0/1)#port-security max-dynamic 10
(Netgear Switch) (Interface 1/0/1)#port-security max-static 3
(Netgear Switch) (Interface 1/0/1)#exit
(Netgear Switch) (Config)#exit
```

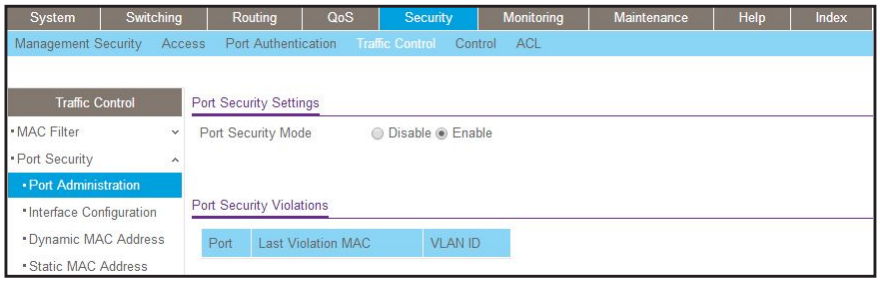
3. Display the port security configuration for port 1/0/1.

```
(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
```

Main UI: Set the dynamic and static MAC address limits on a port

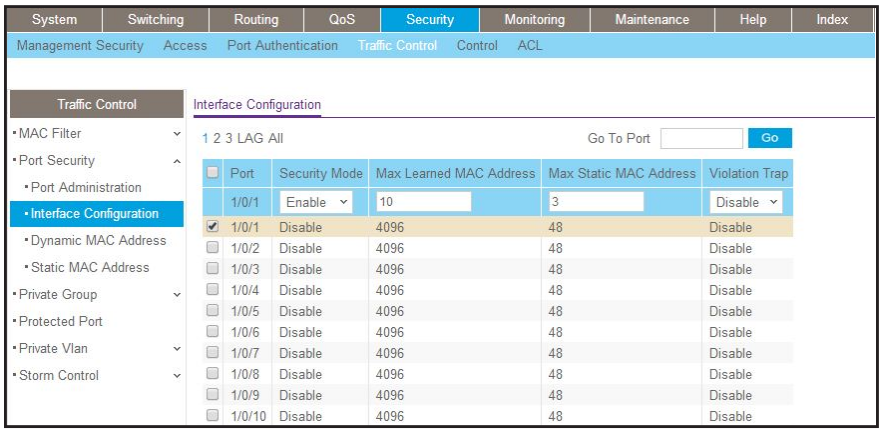
To use the main UI to set the dynamic and static MAC address limits on port 1/0/1:

1. Select **Security > Traffic Control > Port Security > Port Administration**.
   a. A page similar to the following figure displays.



   b. Select the Port Security Mode **Enable** radio button.
   c. Click the **Apply** button. Your settings are saved.
2. Set the dynamic and static MAC address limits on port 1/0/1:
   a. Select **Security > Traffic Control > Port Security >Interface Configuration**.

      A page similar to the following figure displays.



   b. Select the Port **1/0/1** check box.
   c. Configure the following settings:
      - In the **Security Mode** menu, select **Enable**.
      - In the **Max Learned MAC Address** field, enter **10**.
      - In the **Max Static MAC Address** field, enter **3**.
   d. Click the **Apply** button. Your settings are saved.

Convert dynamically learned MAC addresses to static addresses

The example is shown as CLI commands and as a main UI procedure.

CLI: Convert dynamically learned MAC addresses to static addresses

To use the CLI to convert dynamically learned MAC addresses on port 1/0/1 to static addresses and display them:

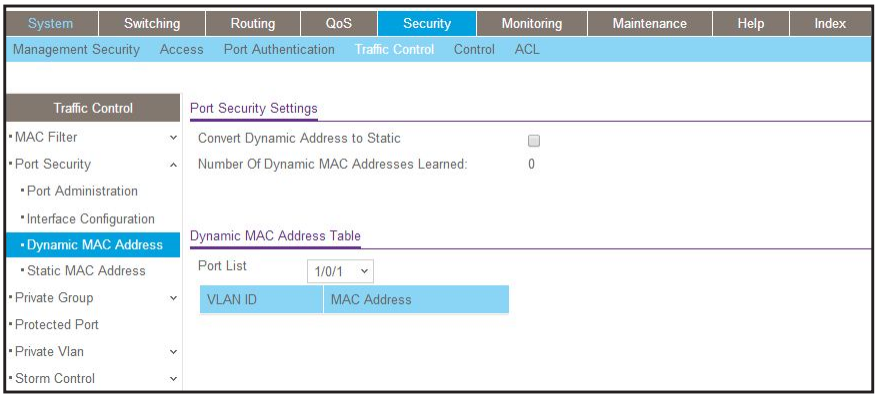
```
(Netgear Switch)(Interface 1/0/1)#port-security mac-address move
(Netgear Switch)(Interface 1/0/1)#exit
(Netgear Switch)(Config)#exit
(Netgear Switch)#show port-security static 1/0/1
 Number of static MAC addresses configured: 3
 Statically configured MAC Address VLAN ID
 ------------------------------------------
 00:0E:45:30:15:F3  1
 00:13:46:EC:2F:62  1
 00:14:6C:E8:81:23  1
```

Main UI: Convert dynamically learned MAC addresses to static addresses

To use the main UI to convert dynamically learned MAC addresses on port 1/0/1 to static addresses:

1. Select **Security > Traffic Control > Port Security > Dynamic MAC Address**.

   A page similar to the following figure displays.



2. Under Dynamic MAC Address Table, in the **Port List** menu, select **1/0/1**.
3. Select the **Convert Dynamic Address to Static** check box.
4. Click the **Apply** button. Your settings are saved.

Create a static MAC address

The example is shown as CLI commands and as a main UI procedure.

CLI: Create a static MAC address

To use the CLI to create a static MAC address:

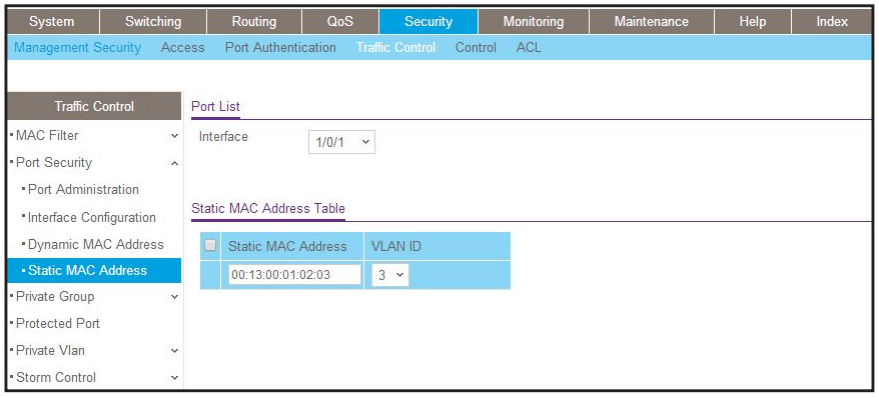
```
(Netgear Switch) (Interface 1/0/1)#port-security mac-address 00:13:00:01:02:03
```

Main UI: Create a static MAC address

To use the main UI to create a static MAC address:

1. Select **Security > Traffic Control > Port Security > Static MAC address**.

   A page similar to the following figure displays.



2. In the **Interface** menu, select **1/0/1**.
3. Under Static MAC Address Table, configure the following settings:
   - In the **Static MAC Address** field, enter **00:13:00:01:02:03.**
   - In the **VLAN** menu, select **3**.
4. Click the **Add** button. Your settings are saved.

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 do the following:

- Prevent traffic from being forwarded between protected ports.
- Allow traffic to be forwarded between a protected port and a non-protected port.

In following figure, Desktop 1 and Desktop 2 can access the Internet, but Desktop cannot see the traffic that is generated by Desktop, that is, no traffic is forwarded between Desktop and Desktop.

The example is shown as CLI commands and as a main UI procedure.

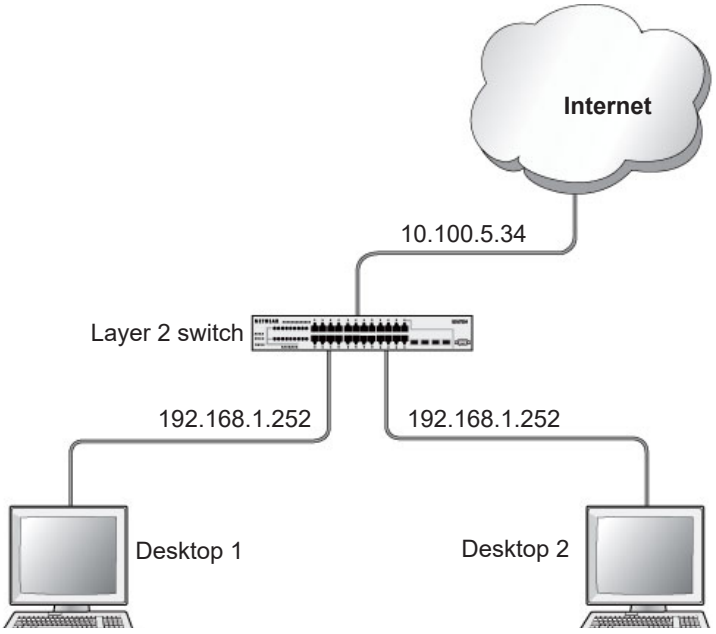


Figure 37. Protected ports

CLI: Configure protected ports to isolate ports on the switch

To use the CLI to configure protected ports to isolate ports on the switch:

1. Create VLAN 192 and add port 1/0/23 (Desktop) 1 and port 1/0/24 (Desktop 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 a routing VLAN 202 that is 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 1/0/16
(Netgear Switch) (Interface 1/0/16)#vlan pvid 202
(Netgear Switch) (Interface 1/0/16)#vlan participation include 202
(Netgear Switch) (Interface 1/0/16)#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 allocate IP addresses to the desktops.

```
(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 ports 1/0/23 and 1/0/24 as protected ports.

```
(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
```

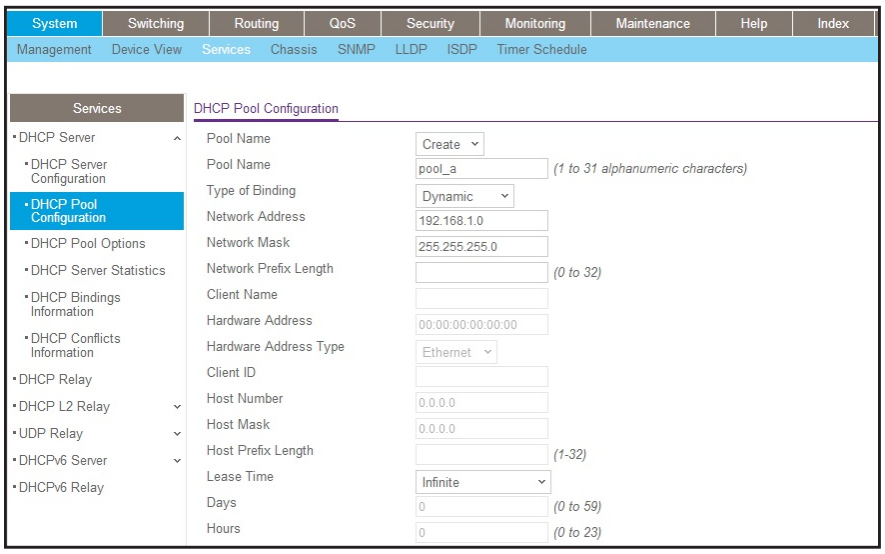
Main UI: Configure protected ports to isolate ports on the switch

Note: This example assumes that the DHCP service is enabled. For information about how to enable the DHCP service, see the main UI procedure in Configure a DHCP server in dynamic mode on page 500.

To use the main UI to configure protected ports to isolate ports on the switch:

1. Create a DHCP pool.
   a. Select **System > Services > DHCP Server > DHCP Pool Configuration**.

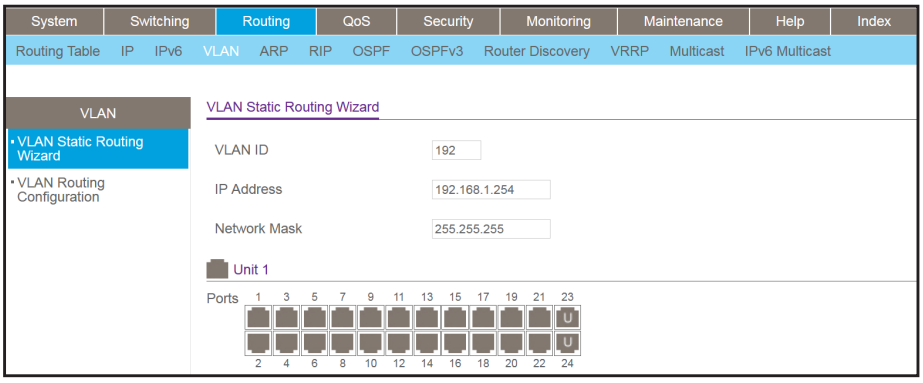
      A page similar to the following figure displays.



   b. Configure the following settings.
      - In the **Pool Name** menu, select **Create**.
      - In the **Pool Name** field, enter **pool-a**.
      - In the **Type of Binding** menu, 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 the **Add** button. Your settings are saved.
2. Configure a routing VLAN and make ports 1/0/23 and 1/0/24 members of the VLAN.
   a. Select **Routing > VLAN > VLAN Static Routing Wizard**.

A page similar to the following figure displays.



b. Configure the following settings.

- 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 the gray boxes under ports **23** and **24** until U displays, which specifies that the egress packets are untagged for the ports.

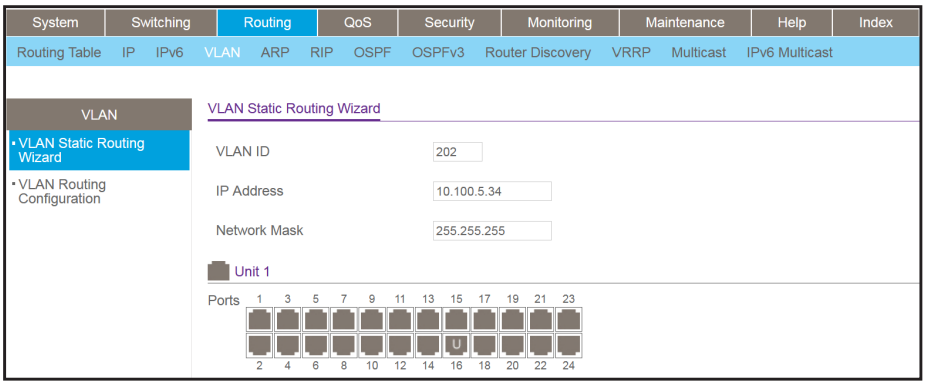
If your switch is a member of a stack, be sure that you select the ports in the correct unit.

d. Click the **Apply** button. Your settings are saved.

3. Configure a VLAN and make port 1/0/16 member of the VLAN.

a. Select **Routing > VLAN > VLAN Static Routing Wizard**.

A page similar to the following figure displays.



b. Configure the following settings:

- 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 the gray box under port **16** until U displays, which specifies that the egress packets are untagged for the port.

If your switch is a member of a stack, be sure that you select the port in the correct unit.

d. Click the **Apply** button. Your settings are saved.

4. Enable IP routing.

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

A page similar to the following figure displays.

b. Configure the following settings:

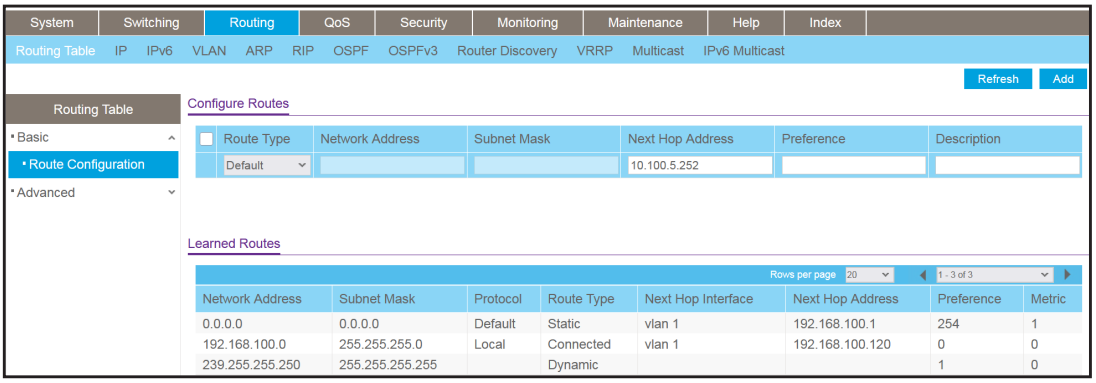
- Select the Routing Mode **Enable** radio button.

c. Click the **Apply** button. Your settings are saved.

5. Configure the default route for VLAN 202.

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

A page similar to the following figure displays.



b. Under Configure Routes, configure the following settings:

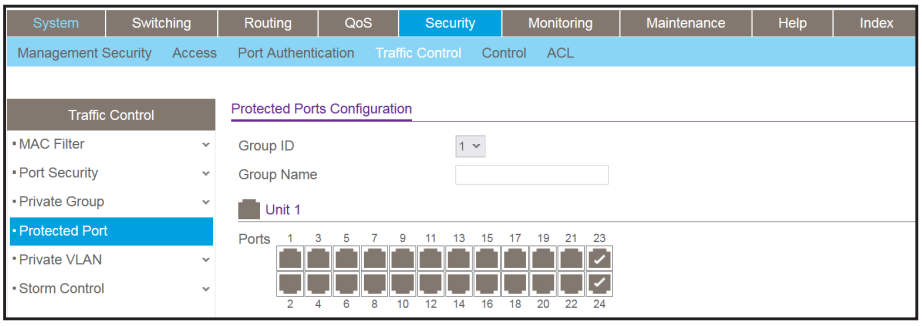
- In the **Route Type** menu, select **Default**.
- In the **Next Hop Address** field, enter **10.100.5.252**.

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

6. Configure port 23 and port 24 as protected ports.

a. Select **Security > Traffic Control > Protected Port**.

A page similar to the following figure displays.



b. Click the gray boxes under ports **23** and **24**. A check mark displays in the boxes.

If your switch is a member of a stack, be sure that you select the ports in the correct unit.

c. Click the **Apply** button. Your settings are saved.

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. You can configure 802.1x port security on a per-port basis.

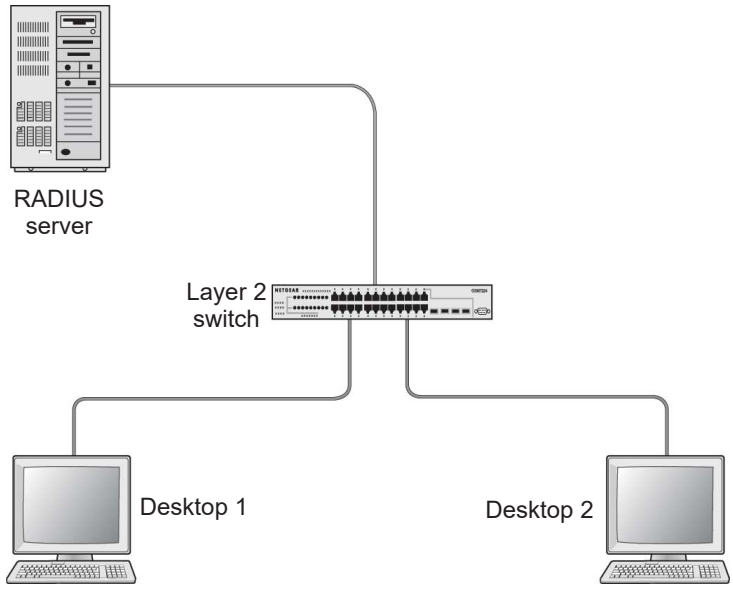


Figure 38. Using 802.1x port security

The following example shows how to authenticate the dot1x users through a RADIUS server. The management IP address is 10.100.5.33 with subnet mask 255.255.255.0.

The example is shown as CLI commands and as a main UI procedure.

CLI: Authenticate dot1x users through a RADIUS server

To use the CLI to authenticate dot1x users through a RADIUS server:

1. Assign an IP address to port 1/0/19, configure the port for forced authorization, 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 for use between the RADIUS clients 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 clients.

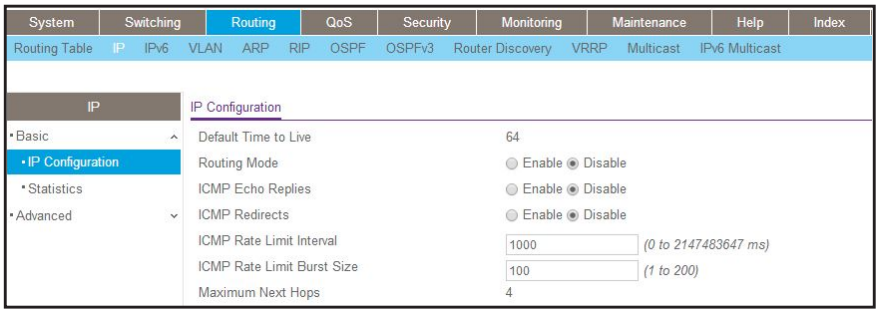
```
(Netgear Switch) (Config)#radius server key acct 10.100.5.17
Enter secret (16 characters max):123456
Re-enter secret:123456
```

Main UI: Authenticate dot1x users through a RADIUS server

To use the main UI to authenticate dot1x users through a RADIUS server:

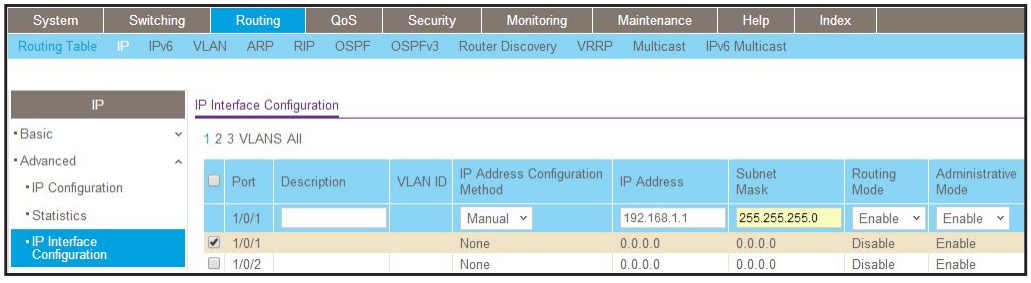
1. Enable routing for the switch.
   a. Select **Routing > IP > Basic > IP Configuration**.

      A page similar to the following figure displays.



   b. Select the Routing Mode **Enable** radio button.
   c. Click the **Apply** button. Your settings are saved.
2. Assign IP address 192.168.1.1 with subnet mask 255.255.255.0 to port 1/0/1.
   a. Select **Routing > IP > Advanced > IP Interface Configuration**.

      A page similar to the following figure displays.



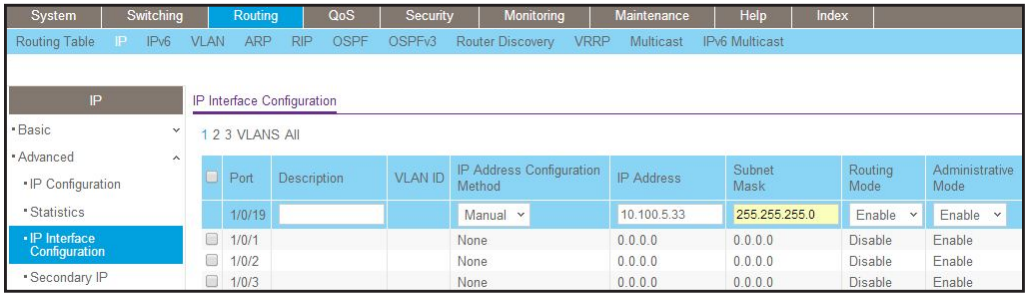
   b. Select the Port **1/0/1** check box.
   c. Configure the following settings:
      - In the **IP Address** field, enter **192.168.1.1**.
      - In the **Subnet Mask** field, enter **255.255.255.0**.
      - In the **Routing Mode** menu, select **Enable**.

d. Click the **Apply** button. Your settings are saved.

3. Assign IP address 10.100.5.33 with subnet mask 255.255.255.0 to port 1/0/19:

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

A page similar to the following figure displays.



b. Select the Port **1/0/19** check box.

c. Configure the following settings:

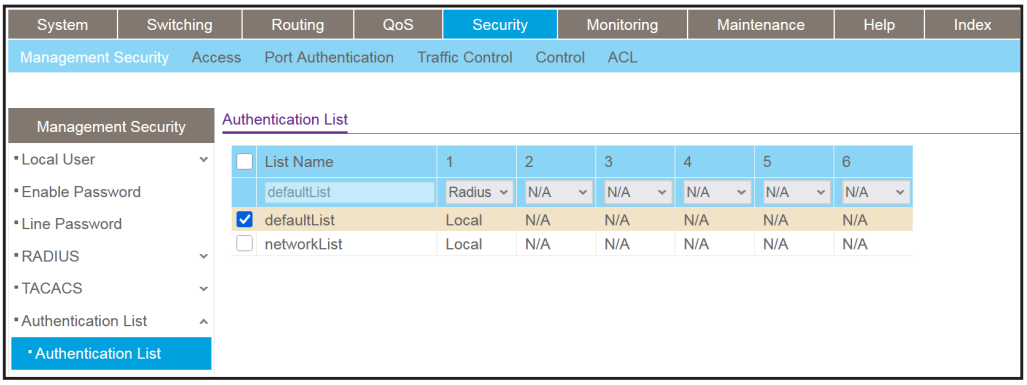
- In the **IP Address** field, enter **10.100.5.33**.
- In the **Subnet Mask** field, enter **255.255.255.0**.
- In the **Routing Mode** menu, select **Enable**.

d. Click the **Apply** button. Your settings are saved.

4. Configure the authentication list.

a. Select **Security > Management Security > Authentication List > Authentication List**.

A page similar to the following figure displays.



b. Select the **defaultList** check box.

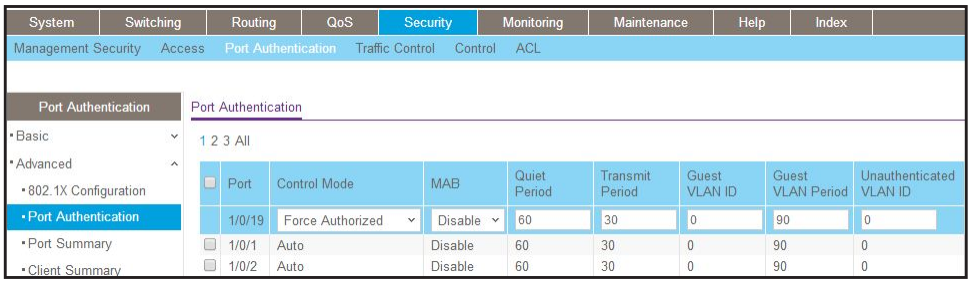
c. In the **1** menu, select **Radius**.

d. Click the **Apply** button. Your settings are saved.

5. Set port 1/0/19 to forced authorization. (In this example, the RADIUS server is connected to this port.)

a. Select **Security > Port Authentication > Advanced > Port Authentication**.

A page similar to the following figure displays.



b. Select the Port **1/0/19** check box.

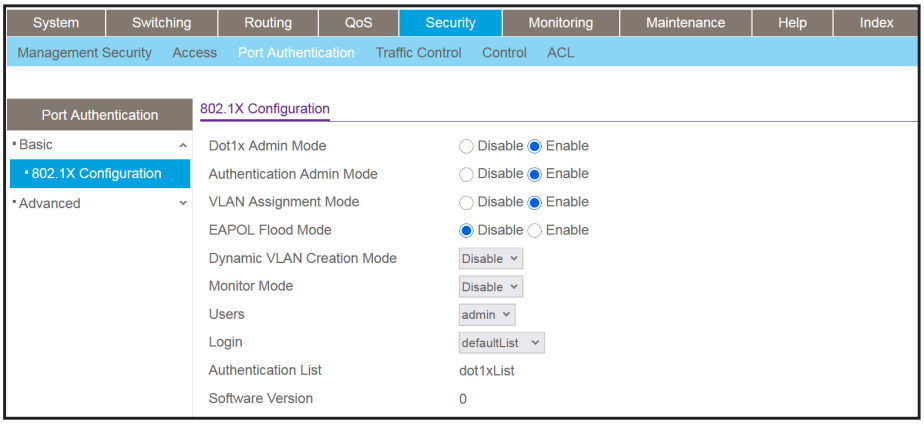
c. In the **Control Mode** menu, select **Force Authorized**.

d. Click the **Apply** button. Your settings are saved.

6. Enable dot1x on the switch.

a. Select **Security > Port Authentication > 8021X Configuration**.

A page similar to the following figure displays.



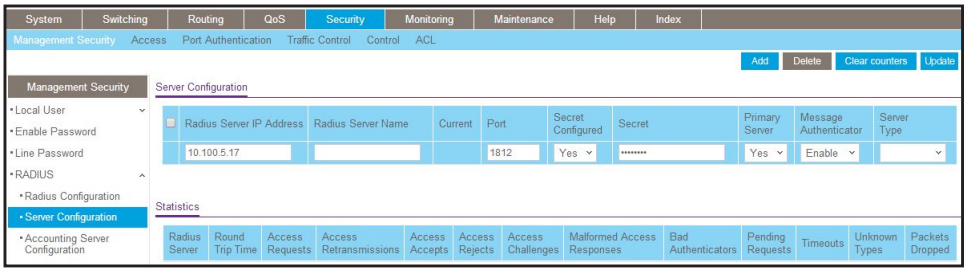
b. Select the Dot1x Admin Mode **Enable** radio button.

c. Click the **Apply** button. Your settings are saved.

7. Configure the RADIUS authentication server.

a. Select **Security > Management Security > RADIUS > Server Configuration**.

A page similar to the following figure displays.



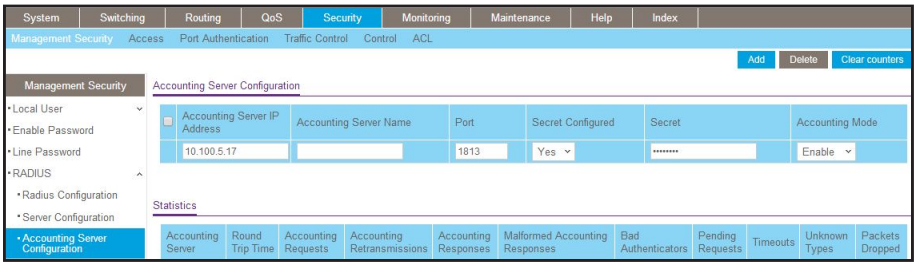
b. In the **RADIUS Server IP Address** field, enter **10.100.5.17**.

c. In the **Secret Configured** menu, select **Yes**.

d. In the **Secret** field, enter **123456**.
e. In the **Primary Server** menu, select **Yes**.
f. In the **Message Authenticator** menu, select **Enable**.
g. Click the **Add** button. Your settings are saved.

8. Configure a RADIUS accounting server.
   a. Select **Security > Management Security > RADIUS > Accounting Server Configuration**.

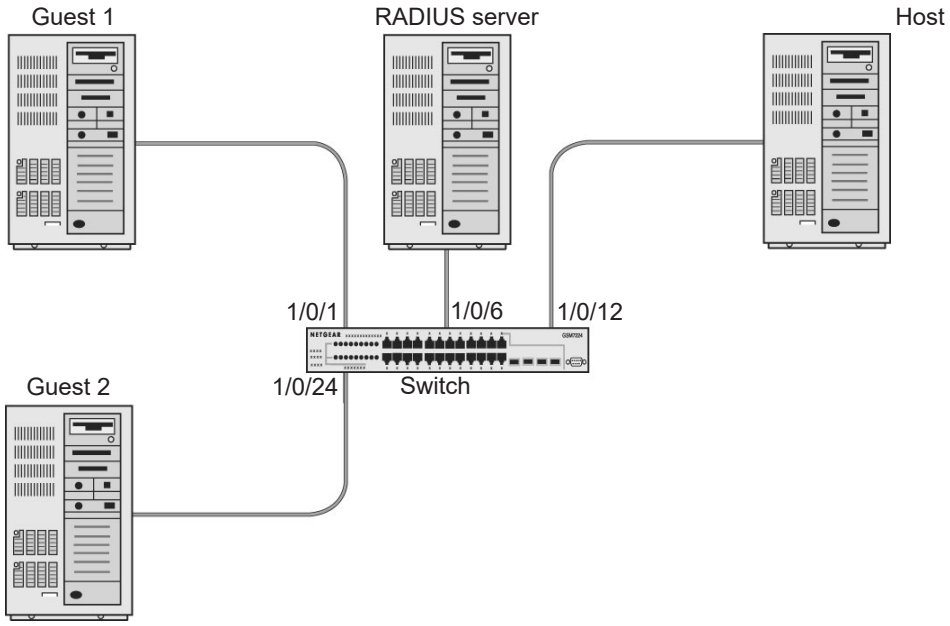
      A page similar to the following figure displays.



   b. In the **Accounting Server IP Address** field, enter **10.100.5.17**.
   c. In the **Accounting Mode** menu, select **Enable**.
   d. Click the **Add** button. Your settings are saved.

Create a guest VLAN

A 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 clients such as visitors and contractors to have network access to reach an external network with no ability to surf the internal LAN.



If an unauthorized switch port has 802.1X enabled and a connected client is 802.1x aware, the client responds to 802.1X requests from the switch.

If a connected client does not support 802.1X, 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 you configure a guest VLAN for the port, the port is placed in the guest VLAN, and the port is moved to the authorized state, allowing access to the client when the guest VLAN period expires.

For a port in MAC-based mode, if you configure a guest VLAN for the port and traffic from an unauthenticated client is detected on the port, the guest VLAN timer is started for the 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 the following 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, a guest VLAN is enabled. If guests connect to the port, they are assigned to guest VLAN 2000, preventing guests from accessing the internal VLAN but allowing them to access each other in the guest VLAN.

The example is shown as CLI commands and as a main UI procedure.

CLI: Create a guest VLAN

To use the CLI to create a guest VLAN:

1. Create VLAN 2000 and add interfaces 1/0/1 and 1/0/24 as members of VLAN 2000.

```
(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. Enable dot1 and RADIUS on the switch.

```
(Netgear Switch) (Config)#aaa authentication dot1x default radius
(Netgear Switch) (Config)#dot1x system-auth-control
(Netgear Switch) (Config)#authentication enable
(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
(Netgear Switch) (Config)#interface 1/0/1
(Netgear Switch) (Interface 1/0/1)#authentication port-control force-authorized
(Netgear Switch) (Interface 1/0/1)#exit
(Netgear Switch) (Config)#interface 1/0/24
(Netgear Switch) (Interface 1/0/24)#authentication port-control force-authorized
(Netgear Switch) (Interface 1/0/24)#exit
```

3. Enable the guest VLAN on interfaces 1/0/1 and 1/0/24.

```
(Netgear Switch) (Config)#interface 1/0/1
(Netgear Switch) (Interface 1/0/1)#authentication event no-response action
authorize vlan 2000
(Netgear Switch) (Interface 1/0/1)#exit
(Netgear Switch) (Config)#interface 1/0/2
(Netgear Switch) (Interface 1/0/24)#authentication event no-response action
authorize vlan 2000
(Netgear Switch) (Interface 1/0/24)#exit
```

4. Verify the configuration.

The output of the **show authentication interface 1/0/1** command is similar to the following example.

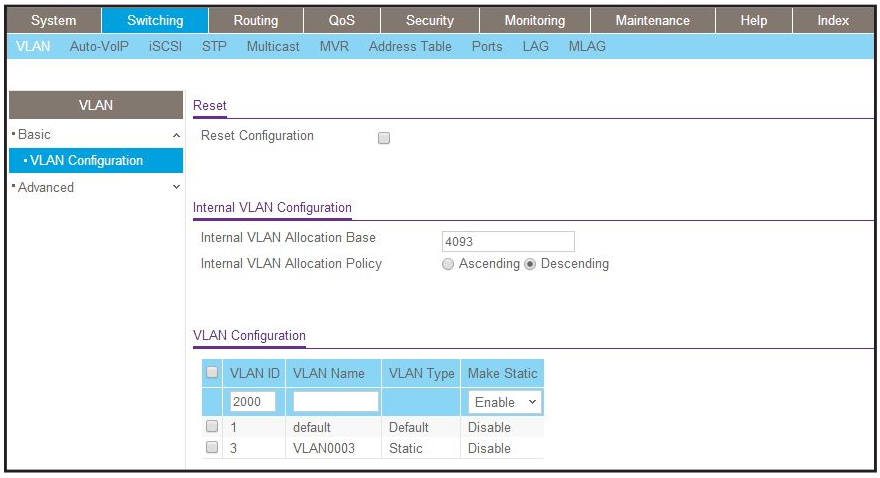
```
(Netgear Switch)#show authentication interface 1/0/1

Authentication Manager Status.................. Disabled

Interface...................................... 1/0/1
Port Control Mode.............................. auto
Host Mode...................................... multi-domain-multi-host
Open Authentication............................ Disabled
Authentication Restart timer................... 30
Configured method order........................ dot1x mab captive-portal
Enabled method order........................... undefined undefined undefined
Configured method priority..................... dot1x mab captive-portal
Enabled method priority........................ undefined undefined undefined
Reauthentication Enabled....................... FALSE
Reauthentication Session timeout from server .. TRUE
Maximum Users.................................. 48
Guest VLAN ID.................................. 2000
Authentication retry attempts.................. 3
Unauthenticated VLAN ID........................ 0
Critical Vlan Id............................... 0
Authentication Violation Mode.................. Restrict
Authentication Server Dead action.............. None
Authentication Server Dead action for Voice.... None
Authentication Server Alive action.............. None
Allowed protocols on unauthorized port......... None
```

Main UI: Create a guest VLAN

To use the main UI to create a guest VLAN:

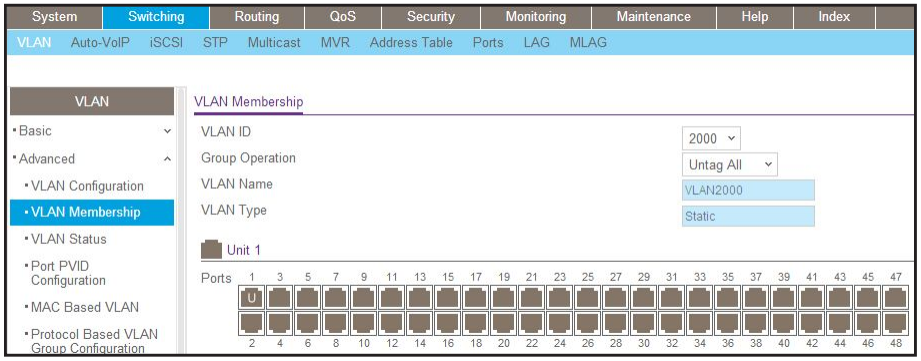
1. Create VLAN 2000.
   a. Select **Switching > VLAN > Basic > VLAN Configuration**.

      A page similar to the following figure displays.



   b. In the **VLAN ID** field, enter **2000**.
   c. In the **Make Static** field, select **Enable**.
   d. Click the **Add** button. Your settings are saved.
2. Add ports to VLAN 2000.
   a. Select **Switching > VLAN > Advanced > VLAN Membership**.

      A page similar to the following figure displays.



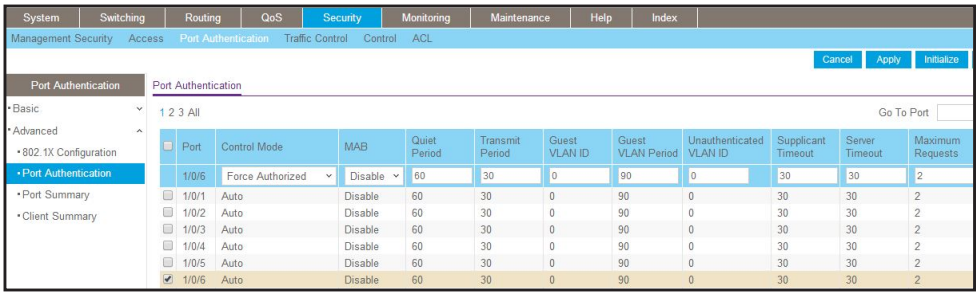
   b. In the **VLAN ID** menu, select **2000**.
   c. Click the gray boxes under ports **1** and **24** until U displays, which specifies that the egress packets are untagged for the ports.

      If your switch is a member of a stack, be sure that you select the ports in the correct unit.

   d. Click the **Apply** button. Your settings are saved.

3. Configure ports 1/0/1 and 1/0/24 for forced authorization.
   a. Select **Security > Port Authentication > Advanced > Port Authentication**.

      A page similar to the following figure displays.

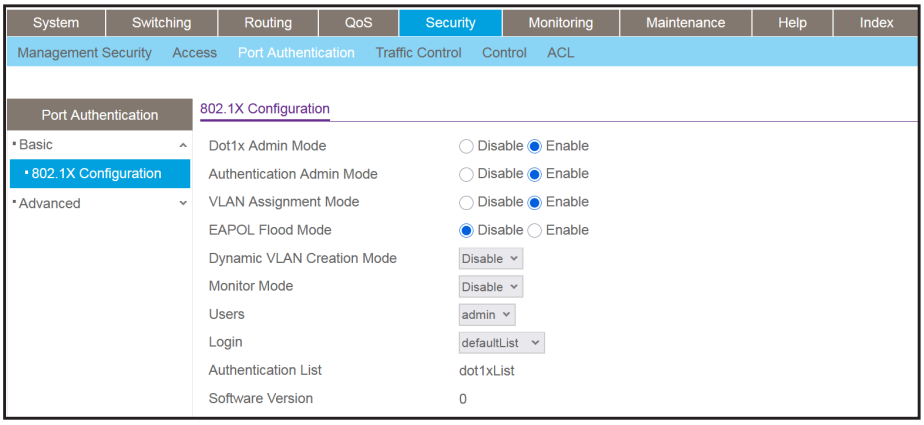


   b. Select the Interface **1/0/1** and **1/0/24** check boxes.
   c. In the **Control Mode** menu, select **Force Authorized**.
   d. Click the **Apply** button. Your settings are saved.
4. Enable dot1x on the switch.

   Note: Make sure that interfaces 1/0/1 and 1/0/24 are configured as force authorized before you perform this step. Otherwise, you cannot access the switch through the main UI.

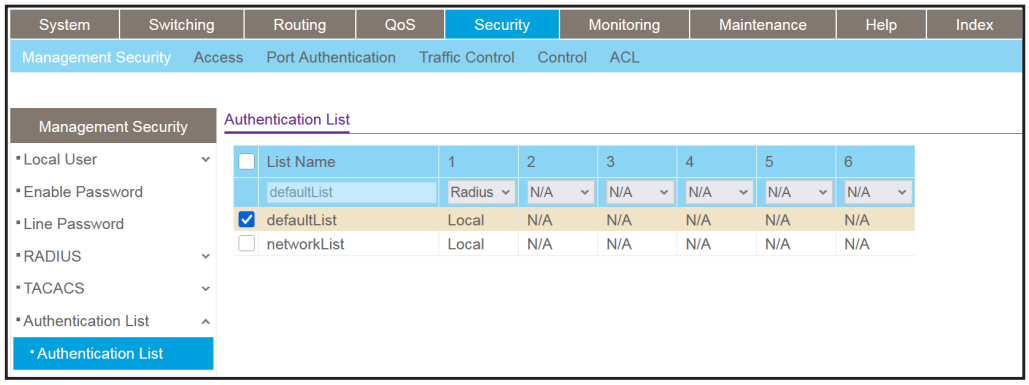
   a. Select **Security > Port Authentication > Basic > 802.1x Configuration**.

      A page similar to the following figure displays.



   b. Select the Dot1x Admin Mode **Enable** radio button.
   c. Select the Authentication Admin Mode **Enable** radio button.
   d. Click the **Apply** button. Your settings are saved.
5. Configure the authentication list.
   a. Select **Security > Management Security > Authentication List > Authentication List**.

A page similar to the following figure displays.



b. Select the **defaultList** check box.

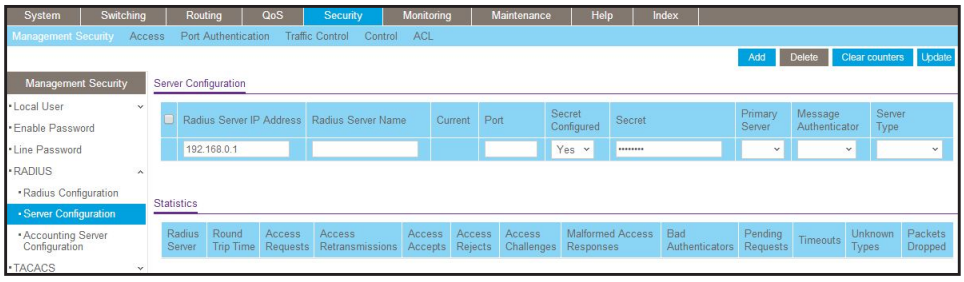
c. In the **1** menu, select **Radius**.

d. Click the **Apply** button. Your settings are saved.

6. Configure the RADIUS authentication server.

a. Select **Security > Management Security > RADIUS > Server Configuration**.

A page similar to the following figure displays.



b. In the **Radius Server IP Address** field, enter **192.168.0.1**.

c. In the **Secret Configured** menu, select **Yes**.

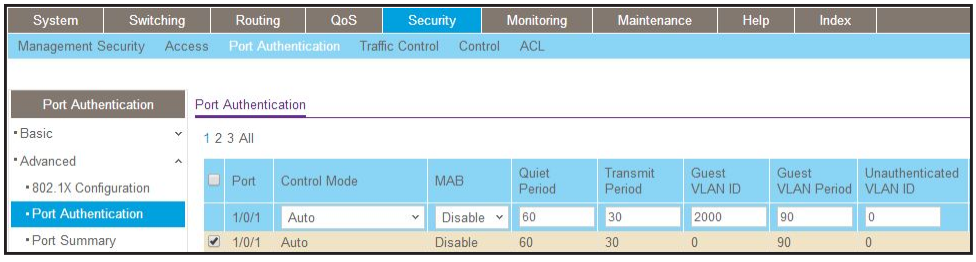
d. In the **Secret** field, enter **12345**.

e. Click the **Add** button. Your settings are saved.

7. Configure the guest VLAN.

a. Select **Security > Port Authentication > Advanced > Port Authentication**.

A page similar to the following figure displays.



b. Select the Port **1/0/1** and **1/0/24** check boxes.

c. In the **Guest VLAN ID** field, enter **2000**.

d. Click the **Apply** button. Your settings are saved.

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 you to configure static VLANs. 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.

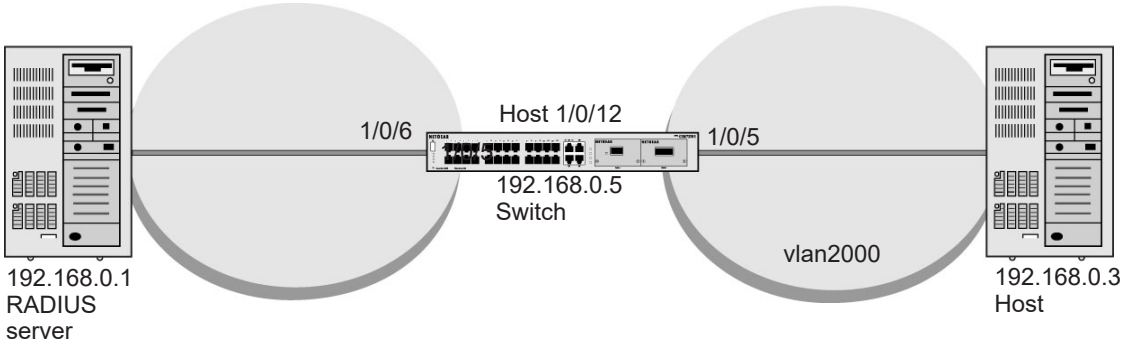


Figure 39. VLAN assignment using RADIUS

In the previous figure, the switch placed the host in the VLAN (vlan2000) based on the user details of the clients. The configuration on the RADIUS server for a user logged in as admin is as follows:

- Tunnel-Type = VLAN (13)
- Tunnel-Medium-Type = 802
- Tunnel-Private-Group-ID = 2000

CLI: Assign VLANS using RADIUS

To use the CLI to configure the switch to let a RADIUS server assign VLANs:

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 RADIUS as the authenticator.

```
(Netgear Switch) (Config)#aaa authentication dot1x default radius
```

4. Enable the switch to accept a VLAN assignment from the RADIUS server.

```
(Netgear Switch) (Config)#authorization network radius
```

5. Specify the RADIUS server IP address.

```
(Netgear Switch) (Config)#radius server host auth 192.168.0.1
```

6. Specify 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 interface 1/0/6 to be authorized for a connection to the RADIUS server.

```
(Netgear Switch) (Config)#authentication enable
(Netgear Switch) (Config)#interface 1/0/6
(Netgear Switch) (Interface 1/0/6)#authentication port-control force-authorized
(Netgear Switch) (Interface 1/0/6)#authentication host-mode multi-host
(Netgear Switch) (Interface 1/0/6)#exit
```

8. Enter the **`show authentication interface`** command for interface 1/0/6 to display the dot1x details.

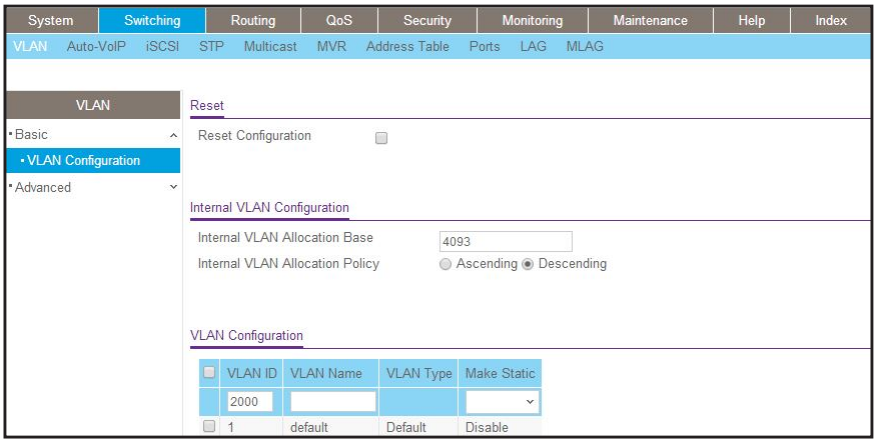
```
(Netgear Switch)#show authentication interface 1/0/6

Authentication Manager Status.................. Disabled

Interface..................................... 1/0/6
Port Control Mode............................. auto
Host Mode..................................... multi-domain-multi-host
Open Authentication........................... Disabled
Authentication Restart timer.................. 30
Configured method order....................... dot1x mab captive-portal
Enabled method order.......................... dot1x mab undefined
Configured method priority.................... dot1x mab captive-portal
Enabled method priority....................... dot1x mab undefined
Reauthentication Enabled...................... FALSE
Reauthentication Session timeout from server .. TRUE
Maximum Users................................. 48
Guest VLAN ID................................. 2000
Authentication retry attempts................. 3
Unauthenticated VLAN ID....................... 0
Critical Vlan Id.............................. 0
Authentication Violation Mode................. Restrict
Authentication Server Dead action.............. None
Authentication Server Dead action for Voice.... None
Authentication Server Alive action............. None
Allowed protocols on unauthorized port......... None
```

Main UI: Assign VLANS using RADIUS

To use the main UI to configure the switch to let a RADIUS server assign VLANs:

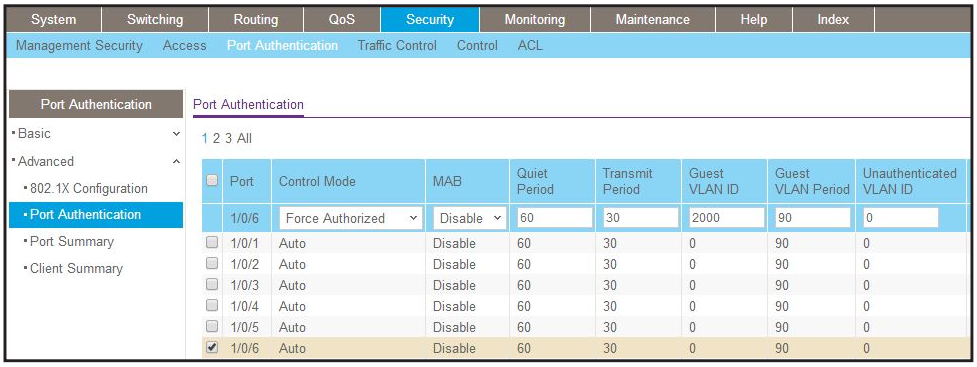
1. Create VLAN 2000.
   a. Select **Switching > VLAN > Basic > VLAN Configuration**.

      A page similar to the following figure displays.



   b. In the **VLAN ID** field, enter **2000**.
   c. In the **Make Static** menu, select **Static**.
   d. Click the **Add** button. Your settings are saved.
2. Configure ports 1/0/6 and 1/0/12 for forced authorization.
   a. Select **Security > Port Authentication > Advanced > Port Authentication**.

      A page similar to the following figure displays.



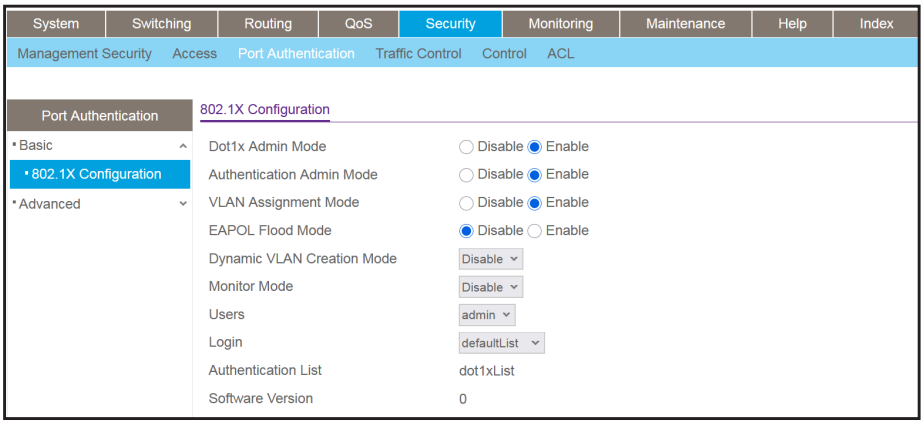
   b. Select the Port **1/0/6** and **1/0/12** check boxes.
   c. In the **Control Mode** menu, select **Force Authorized**.
   d. Click the **Apply** button. Your settings are saved.

3. Enable dot1x on the switch.

   Note: Make sure that ports 1/0/6 and 1/0/12 are configured as force authorized before you do this step. Otherwise, you cannot access the switch through the main UI.

   a. Select **Security > Port Authentication > Basic > 802.1x Configuration**.

      A page similar to the following figure displays.



   b. Select the Dot1x Admin Mode **Enable** radio button.

   c. Select the Authentication Admin Mode **Enable** radio button.

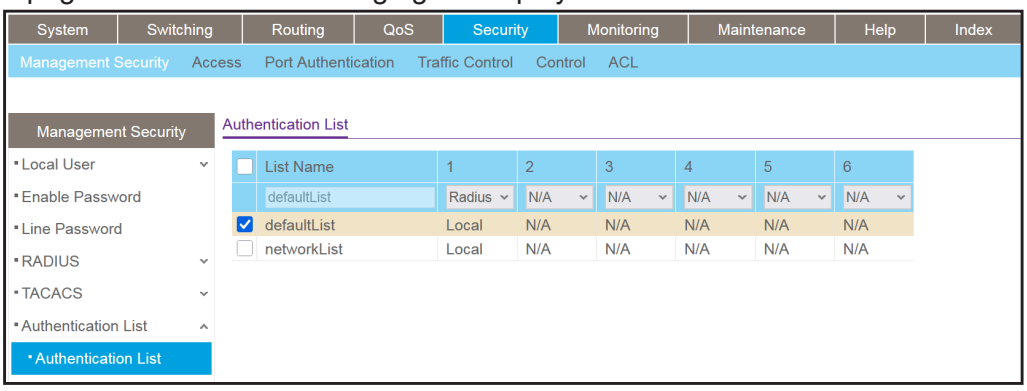
   d. Select the VLAN Assignment Mode **Enable** radio button.

   e. Click the **Apply** button. Your settings are saved.

4. Configure the authentication list.

   a. Select **Security > Management Security > Authentication List > Authentication List**.

      A page similar to the following figure displays.



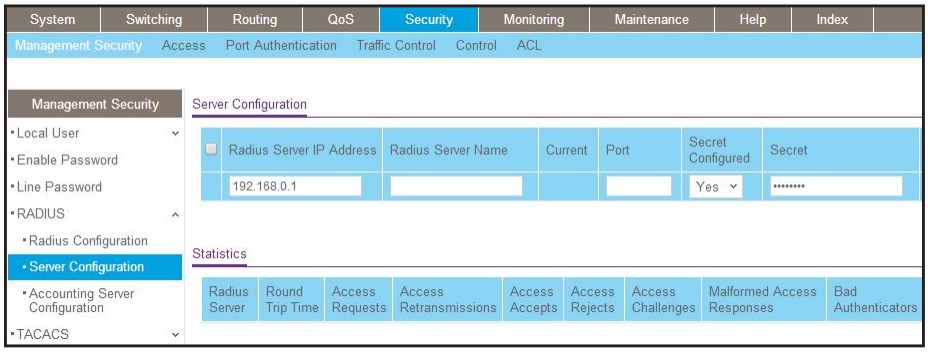
   b. Select the **defaultList** check box.

   c. In the **1** menu, select **Radius**.

   d. Click the **Add** button. Your settings are saved.

5. Configure the RADIUS authentication server.
   a. Select **Security > Management Security > RADIUS > Server Configuration**.

      A page similar to the following figure displays.



   b. In the **Radius Server IP Address** field, enter **192.168.0.1**.
   c. In the **Secret Configured** menu, select **Yes**.
   d. In the **Secret** field, enter **12345**.
   e. Click the **Add** button. Your settings are saved.

Dynamic ARP inspection

Dynamic ARP inspection (DAI) is a security feature that rejects invalid and malicious Address Resolution Protocol (ARP) packets. The feature prevents a class of man-in-the-middle attacks, where an unfriendly device intercepts traffic for other devices by poisoning the ARP caches of its unsuspecting neighbors. The attacker 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 combinations of MAC addresses, IP addresses, and VLAN interfaces.

When DAI is enabled, the switch drops an ARP packet if the sender MAC address and sender IP address do not match an entry in the DHCP snooping bindings database. However, you can prevent the ARP packet drop by configuring static mappings. Static mappings are useful when hosts configure static IP addresses, DHCP snooping cannot be enabled, or other switches in the network do not support dynamic ARP inspection. A static mapping associates an IP address to a MAC address on a VLAN.

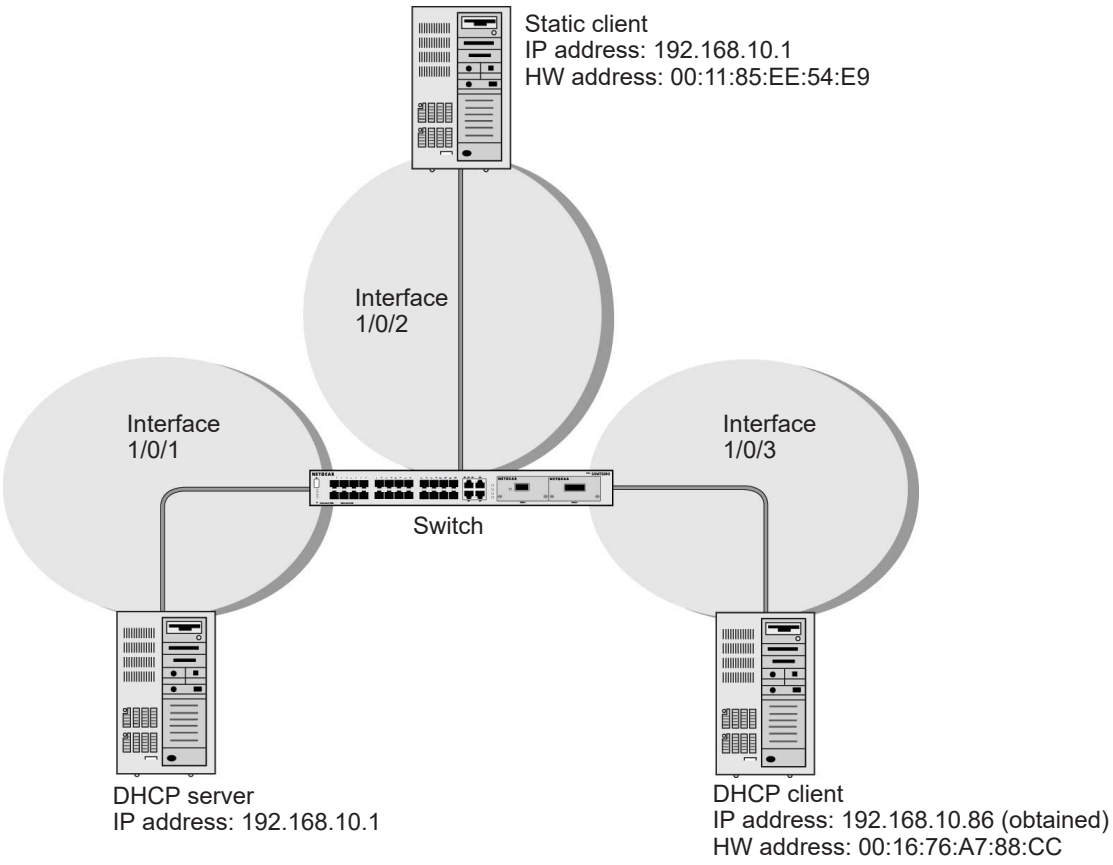


Figure 40. Dynamic ARP inspection

The example is shown as CLI commands and as a main UI procedure.

CLI: Configure Dynamic ARP inspection

To use the CLI to 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
```

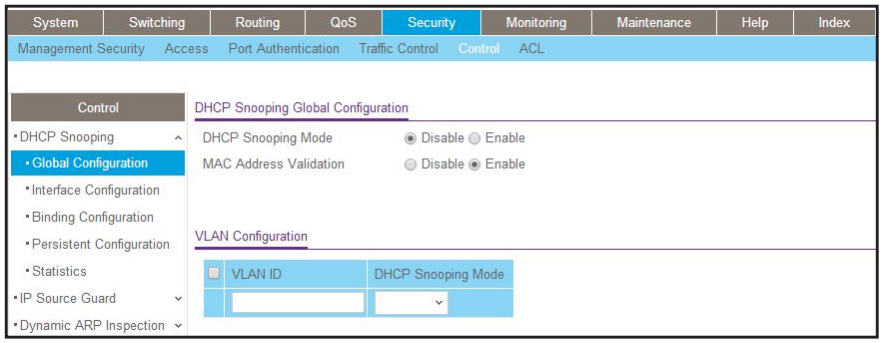
Now, ARP packets from the DHCP client go through because a DHCP snooping entry exists. However, ARP packets from the static client are dropped. For information about how to prevent ARP packets from static clients to be dropped, see Static mapping for dynamic ARP inspection on page 366.

Main UI: Configure Dynamic ARP inspection

To use the main UI to configure Dynamic ARP Inspection:

1. Enable DHCP snooping globally and then enable DHCP snooping for a VLAN.
   a. Select **Security > Control > DHCP Snooping > Global Configuration**.

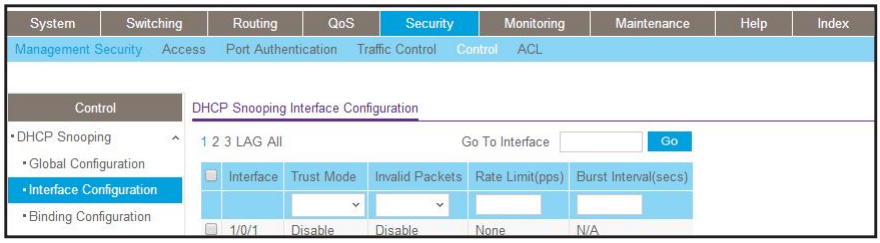
      A page similar to the following figure displays.



   b. Select the DHCP Snooping Mode **Enable** radio button.
   c. Click the **Apply** button. Your settings are saved.
   d. In the **VLAN ID** field, enter **1**.
   e. In the **DHCP Snooping Mode** menu, select **Enable**.
   f. Click the **Apply** button. Your settings are saved.

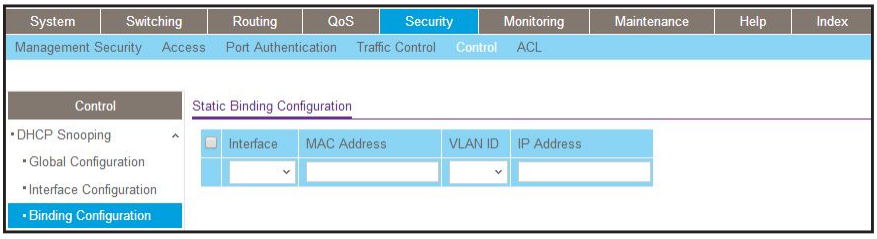
2. Configure interface 1/0/1 as trusted, which is the interface through which the DHCP server is reached.
   a. Select **Security > Control > DHCP Snooping > Interface Configuration**.

      A page similar to the following figure displays.



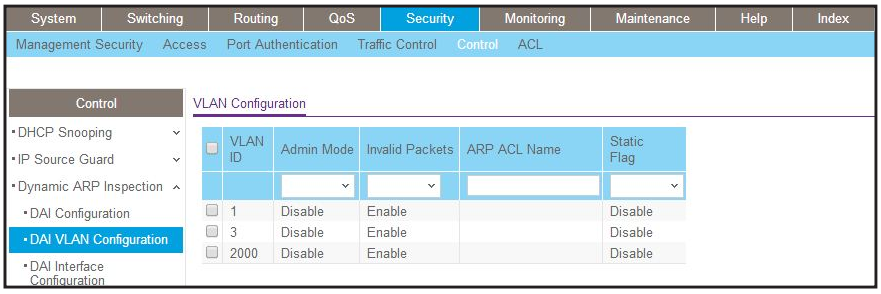
   b. Select the Interface **1/0/1** check box.
   c. In the **Trust Mode** menu, select **Enable**.
   d. Click the **Apply** button. Your settings are saved.
3. Display the DHCP Snooping Binding table.
   a. Select **Security > Control > DHCP Snooping > Binding Configuration**.

A page similar to the following figure displays.



4. Enable ARP Inspection on VLAN 1.
   a. Select **Security > Control > Dynamic ARP Inspection > DAI VLAN Configuration**.

      A page similar to the following figure displays.



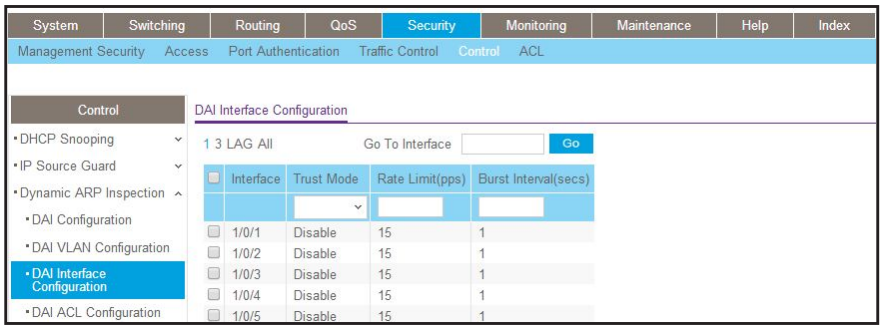
   b. Select the VLAN ID **1** check box.
   c. In the **Admin Mode** menu, select **Enable**.
   d. Click the **Apply** button. Your settings are saved.

      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 device with which you are accessing the main UI has a DHCP snooping entry or that you can access the switch through the trusted port for ARP. Otherwise, you might get locked out of main UI.

5. Configure port 1/0/1 as trusted.
   a. Select **Security > Control > Dynamic ARP Inspection > DAI Interface Configuration**.

A page similar to the following figure displays.



b. Select the Interface **1/0/1** check box.

c. In the **Trust Mode** menu, select **Enable**.

d. Click the **Apply** button. Your settings are saved.

Now ARP packets from the DHCP client go through. However, an ARP packet from a static client is dropped because it does not have a DHCP snooping entry. You can prevent this from occurring by configuring static mapping (see Static mapping for dynamic ARP inspection on page 366).

Static mapping for dynamic ARP inspection

The example is shown as CLI commands and as a main UI procedure.

CLI: Configure static mapping for dynamic ARP inspection

To use the CLI to configure static mapping for Dynamic ARP Inspection:

1. Create an ARP ACL.

```
(Netgear Switch) (Config)# arp access-list ArpFilter
```

2. Configure the ARP ACL 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
(Netgear Switch) (Config-arp-access-list)# exit
(Netgear Switch) (Config)#
```

3. Configure VLAN 1 to use the ARP ACL.

```
(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.

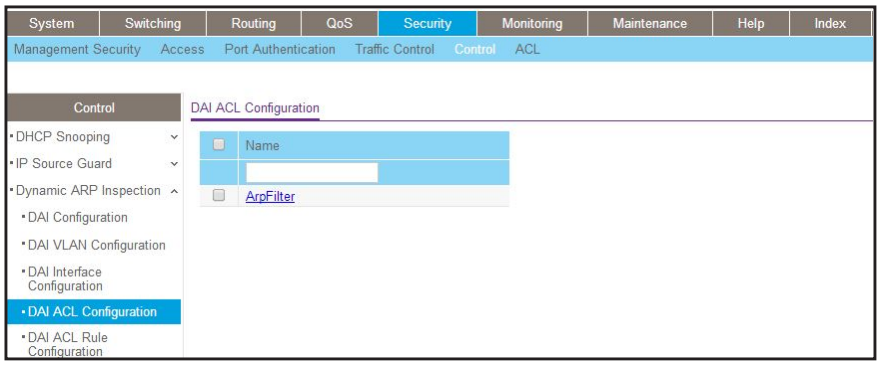
Note: This command can include the optional static keyword. If you use the **`static`** keyword, packets that do not match a permit statement are dropped without consulting the DHCP snooping bindings table. In the example that is described in this section, ARP packets from the DHCP client are dropped since it does not have a matching rule, though it has a DHCP snooping entry.

Main UI: Configure static mapping for dynamic ARP inspection

To use the main UI to configure static mapping for Dynamic ARP Inspection:

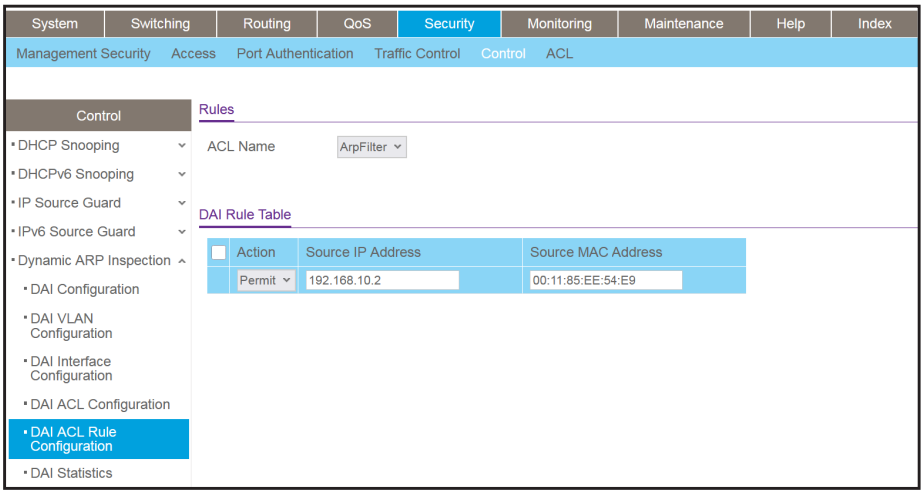
1. Create an ARP ACL.
   a. Select **Security > Control > Dynamic ARP Inspection > DAI ACL Configuration**.

      A page similar to the following figure displays.



   b. In the **Name** field, enter **ArpFilter**.
   c. Click the **Add** button. Your settings are saved.
2. Configure a rule to allow the static client.
   a. Select **Security > Control > Dynamic ARP Inspection > DAI ACL Rule Configuration**.

A page similar to the following figure displays.



b. In the **ACL Name** menu, select **ArpFilter**.

c. In the **Action** menu, select **Permit**.

d. In the **Source IP Address** field, enter **192.168.10.2**.

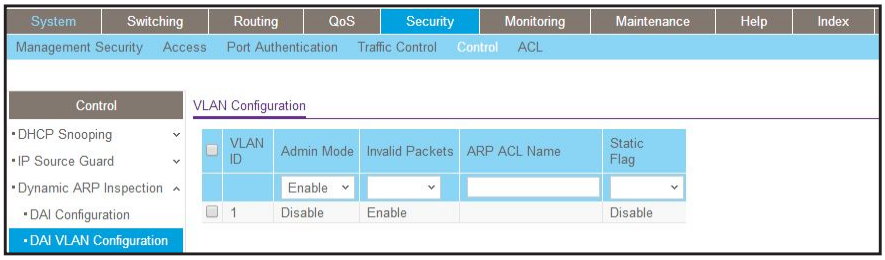
e. In the **Source MAC Address** field, enter **00:11:85:EE:54:E9**.

f. Click the **Add** button. Your settings are saved.

3. Configure VLAN 1 to use the ARP ACL.

a. Select **Security > Control > Dynamic ARP Inspection > DAI VLAN Configuration**.

A page similar to the following figure displays.



b. Select the VLAN ID **1** check box.

c. In the **ARP ACL Name** field, enter **ArpFilter**.

d. Click the **Apply** button. Your settings are saved.

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 addresses, IP addresses, VLAN IDs, and ports that are considered authorized. You can enable DHCP snooping globally and on specific VLANs, and then configure ports within the VLAN to be trusted or untrusted. DHCP servers must be reached through trusted ports.

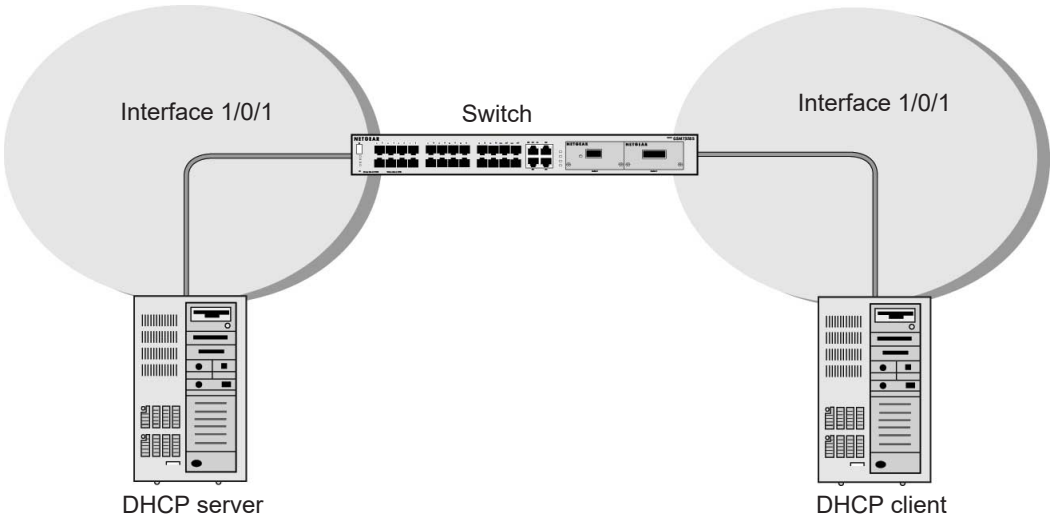


Figure 41. DHCP Snooping

The example is shown as CLI commands and as a main UI procedure.

CLI: Configure DHCP snooping

To use the CLI to 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. Display the DHCP Snooping Binding table.

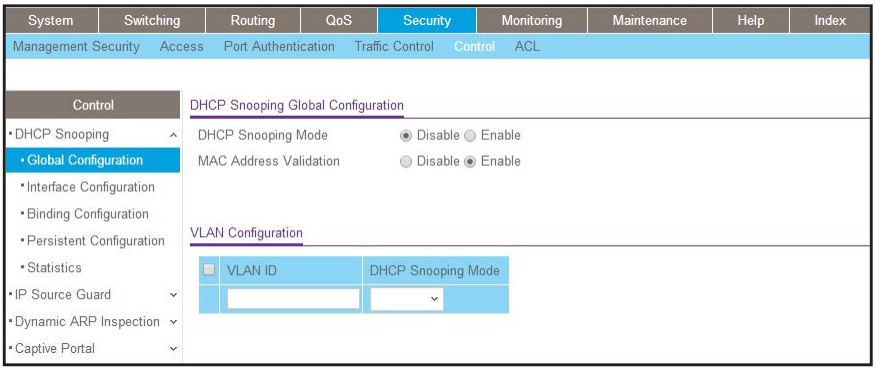
```
(Netgear Switch) #show ip dhcp snooping binding

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
```

Main UI: Configure DHCP snooping

To use the main UI to configure DHCP Snooping:

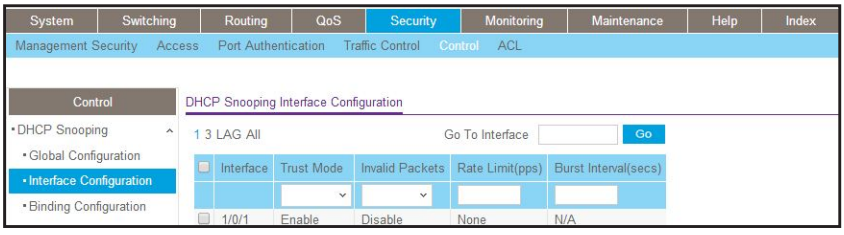
1. Enable DHCP Snooping globally and enable DHCP Snooping on VLAN 1.
   a. Select **Security > Control > DHCP Snooping > Global Configuration**.

      A page similar to the following figure displays.



   b. Select the DHCP Snooping Mode **Enable** radio button.
   c. Click the **Apply** button. Your settings are saved.
   d. In the **VLAN ID** field, enter **1**.
   e. In the **DHCP Snooping Mode** menu, select **Enable**.
   f. Click the **Apply** button. Your settings are saved.
2. Configure the port through which DHCP server is reached as trusted.
   a. Select **Security > Control > DHCP Snooping > Interface Configuration**.

      A page similar to the following figure displays.



b. Select the Interface **1/0/1** check box.

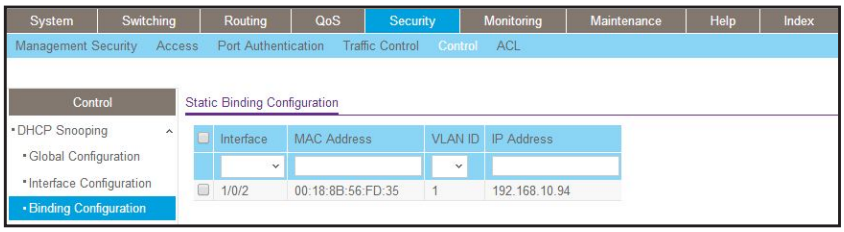
c. In the **Trust Mode** menu, select **Enable**.

d. Click the **Apply** button. Your settings are saved.

3. Display the DHCP snooping binding configuration.

   Select **Security > Control > DHCP Snooping > Binding Configuration**.

   A page similar to the following figure displays.



Find a rogue DHCP server

If you enable DHCP snooping, you can find a rogue DHCP server in the network.

The example is shown as CLI commands and as a main UI procedure.

CLI: Find a rogue DHCP server

To use the CLI to find a rogue DHCP sever:

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
.....................................................................................
1/0/25                 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.
```

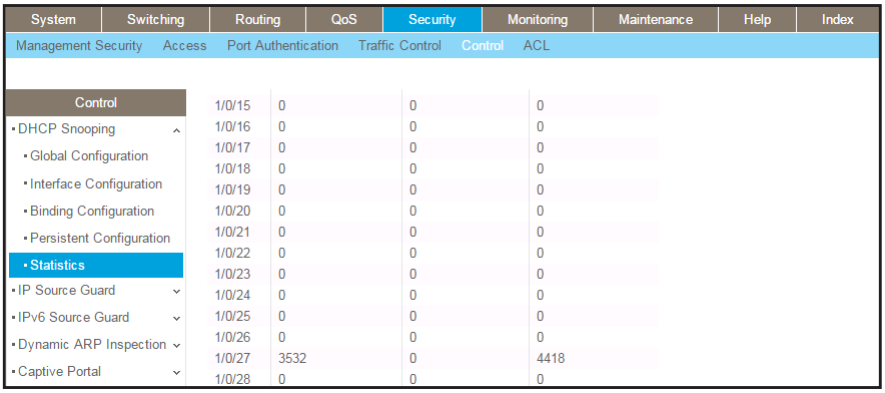
In the previous example, the IP address of the rogue DHCP server is 10.100.5.253 and the MAC address is 00:26:F2:F6:B3:6C.

Main UI: Find a rogue DHCP server

To use the main UI to find a rogue DHCP server:

1. Check the statistics on the untrusted ports:
   a. Select **Security > Control > DHCP Snooping > Statistics**.

      A page similar to the following figure displays.

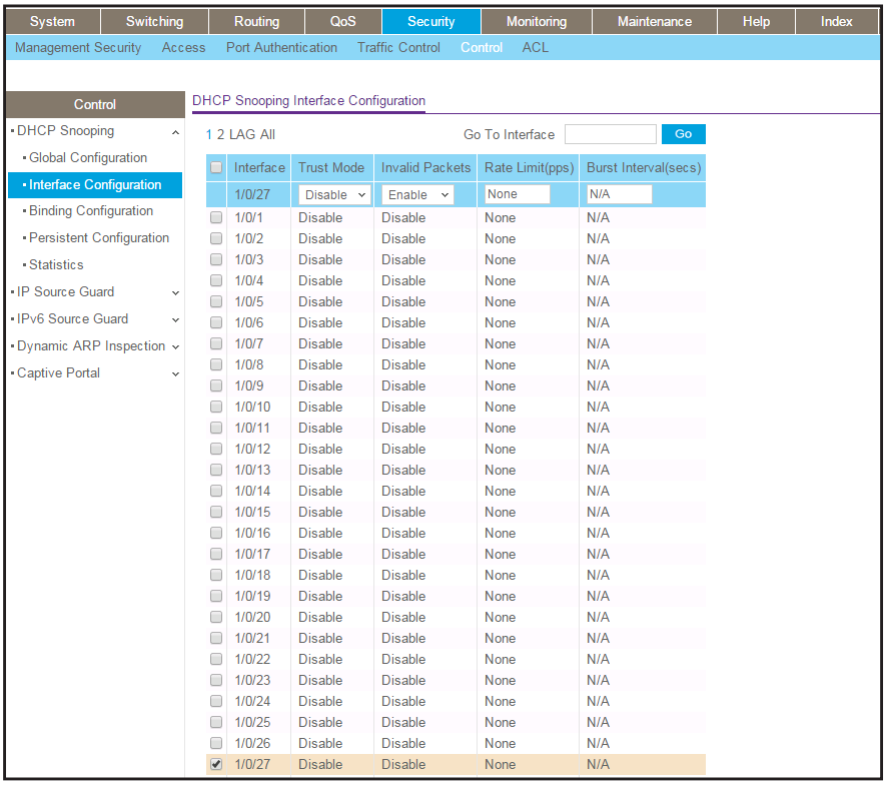


   b. Determine if messages in the DHCP Server Msgs Rec'd column increase for any port.

      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 page similar to the following figure displays.



b. Select the Interface **1/0/27** check box.

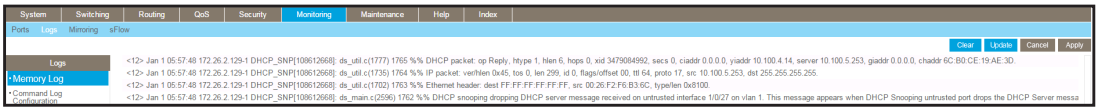
c. In the **Invalid Packets** menu, select **Enable**.

d. Click the **Apply** button. Your settings are saved.

3. Determine the IP address and MAC address of the rogue DHCP server:

a. Select **Monitoring > Logs > Memory log**.

A page similar to the following figure displays.



b. Search for “DHCP packet; op Reply”.

Enter a static binding into the binding database

You can enter a static binding into the binding database. In the following example, MAC address 00:11:11:11:11:11 is bound to IP address 192.168.10.1 on VLAN 1 on interface 1/0/2.

The example is shown as CLI commands and as a main UI procedure.

CLI: Enter a static binding into the binding database

To use the CLI to enter a 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.

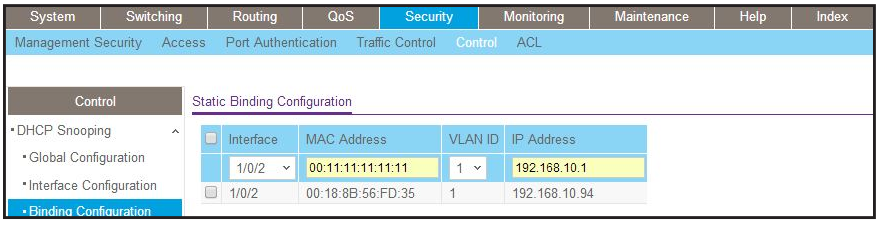
```
(Netgear Switch) #show ip dhcp snooping binding
Total number of bindings:  2

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
```

Main UI: Enter a static binding into the binding database

To use the main UI to enter a static binding into the binding database:

1. Select **Security > Control > DHCP Snooping > Binding Configuration**.

   A page similar to the following figure displays.



2. Configure the following settings:
   a. Select the Interface **1/0/2** check box.
   b. In the **MAC Address** field, enter **00:11:11:11:11:11**.
   c. In the VLAN ID menu, select **1**.
   d. In the **IP Address** field, enter **192.168.10.1**.
3. Click the **Add** button. Your settings are saved.

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 that are received on untrusted interfaces. DHCP snooping monitors the receive rate on each interface separately. If the receive rate exceeds the configured limit, DHCP snooping shuts down the interface. You then must manually enter the **no shutdown** command on the interface to bring the interface back up.

In the following example, on interface 1/0/2, the maximum rate of incoming DHCP messages is 5 pps and the maximum burst interval is 1 second.

The example is shown as CLI commands and as a main UI procedure.

CLI: Configure the maximum rate of DHCP messages

To use the CLI to configure the maximum rate of incoming DHCP messages:

1. Configure the maximum rate of DHCP messages.

```
(Netgear Switch) (Interface 1/0/2)# ip dhcp snooping limit rate 5
```

2. Display the configured rate.

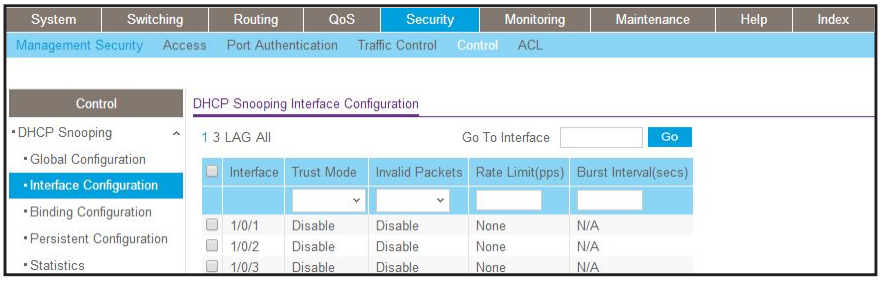
```
(Netgear Switch) #show ip dhcp snooping interfaces 1/0/2

Interface     Trust State     Rate Limit      Burst Interval
                                 (pps)           (seconds)
----------   -------------   -------------   ---------------

1/0/2              No               5                1
```

Main UI: Configure the maximum rate of DHCP messages

To use the main UI to configure the maximum rate of incoming DHCP messages:

1. Select **Security > Control > DHCP Snooping > Interface Configuration**.

   A page similar to the following figure displays.



2. Configure the following settings:
   a. Select the Interface **1/0/2** check box.
   b. In the **Rate Limit (pps)** field, enter **5**.
   c. In the **Burst Interval (secs)** field, enter **1**.
3. Click the **Apply** button. Your settings are saved.

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. You can configure IP Source Guard to enforce the source IP address only or both the source IP address and the source MAC address.

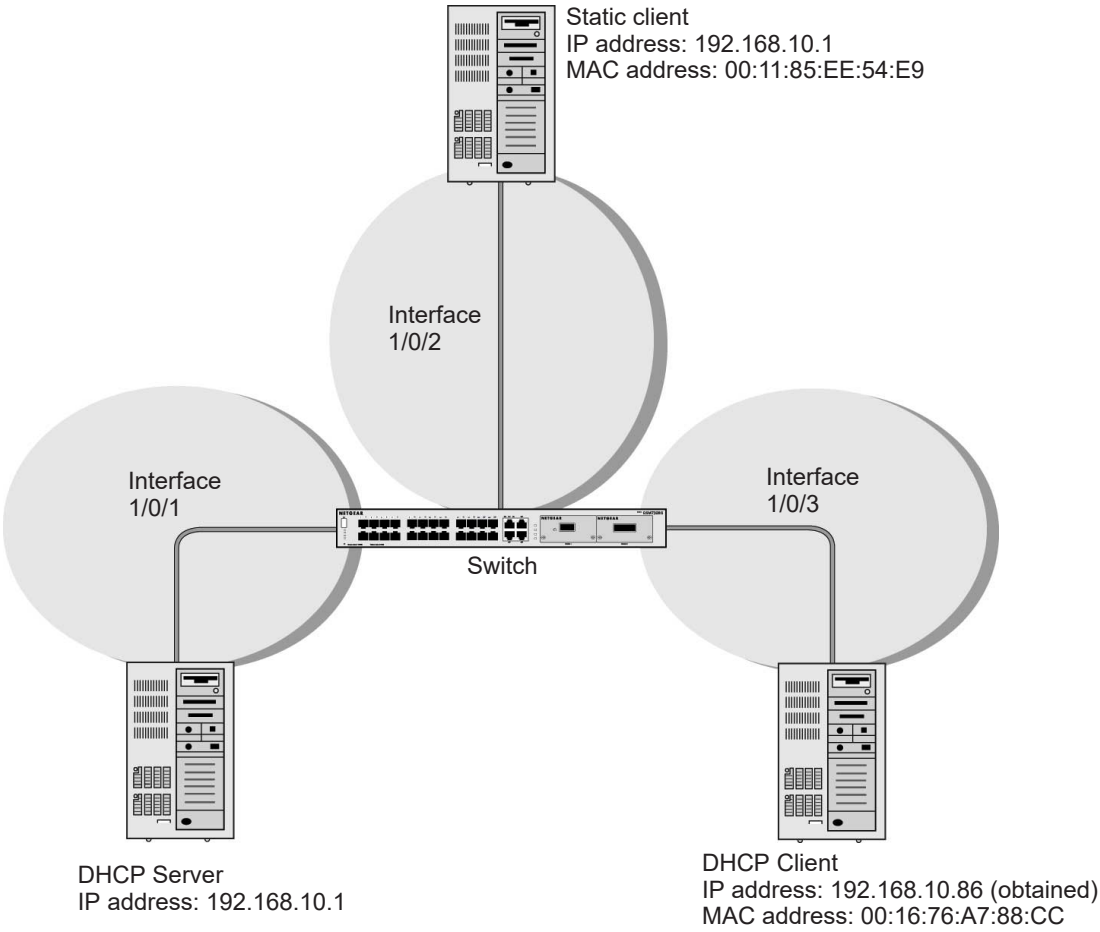


Figure 42. IP Source Guard

The example is shown as CLI commands and as a main UI procedure.

CLI: Configure IP Source Guard

To use the CLI to configure IP Source Guard:

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 interface 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. Display 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 on interface 1/0/2.

```
(Netgear Switch) (Interface 1/0/2)#ip verify source [port-security]
```

Without the port security option in Interface Config mode, the switch verifies the source IP address only. With the port-security option in Interface Config mode, the switch verifies both the source IP address and the source MAC address.

However, you can also globally enable port-security in Global Config mode, as shown in the following example.

```
(Netgear Switch) (Config) # port-security
```

6. Configure an IP Source Guard static binding.

(This example binds MAC address 00:05:05:05:05:05 to IP address 192.168.10.80 on VLAN 1 on interface 1/0/2.)

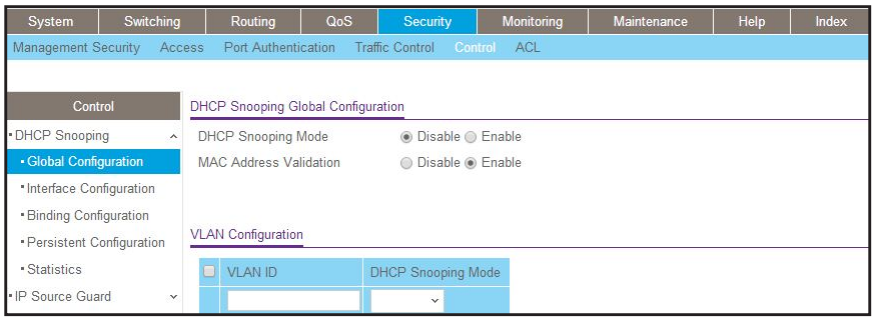
```
(Netgear Switch) (Config) #ip verify binding 00:05:05:05:05:05 vlan 1 192.168.10.80
interface 1/0/2
```

Main UI: Configure IP Source Guard

To use the main UI to configure IP Source Guard:

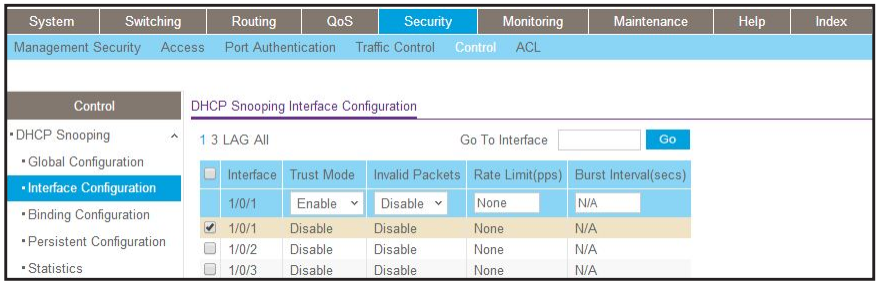
1. Enable DHCP snooping globally and enable DHCP snooping on a VLAN.
   a. Select **Security > Control > DHCP Snooping > Global Configuration**.

      A page similar to the following figure displays.



   b. Select the DHCP Snooping Mode **Enable** radio button.
   c. Click the **Apply** button. Your settings are saved.
   d. In the VLAN Configuration table, configure the following settings:
   e. In the **VLAN ID** menu, select **1**.
   f. In the **DHCP Snooping Mode** menu, select **Enable**.
   g. Click the **Apply** button. Your settings are saved.
2. Configure the interface through which the DHCP server is reached as trusted.
   a. Select **Security > Control > DHCP Snooping > Interface Configuration**.

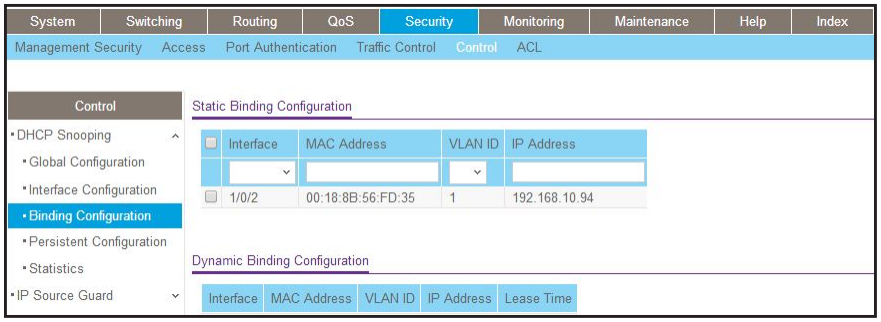
      A page similar to the following figure displays.



   b. Select Interface **1/0/1** check box.
   c. In the **Trust Mode** menu, select **Enable**.
   d. Click the **Apply** button. Your settings are saved.
3. Display the DHCP Snooping Binding table.

   Select **Security > Control > DHCP Snooping > Binding Configuration**.

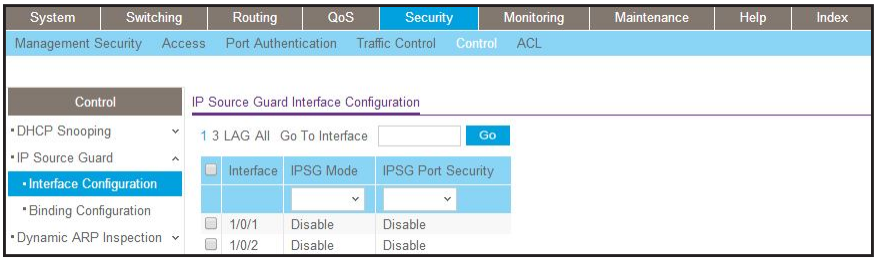
A page similar to the following figure displays.



4. Enable IP Source Guard on interface 1/0/2.

   Select **Security > Control > IP Source Guard > Interface Configuration**.

   A page similar to the following figure displays.



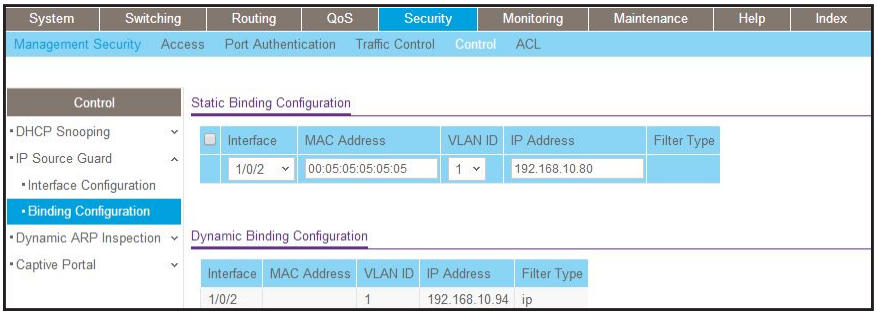
   e. Select the Interface **1/0/2** check box.
   f. In the **IPSG Mode** menu, select **Enable**.
   g. Click the **Apply** button. Your settings are saved.

5. Configure an IP Source Guard static binding.

   (This example binds MAC address 00:05:05:05:05:05 to IP address 192.168.10.80 on VLAN 1 on interface 1/0/2.)

   a. Select **Security > Control > IP Source Guard > Binding Configuration**.

      A page similar to the following figure displays.



   b. Select the Interface **1/0/2** check box.
   c. In the **MAC Address** field, enter the MAC address **00:05:05:05:05:05**.
   d. In the **VLAN ID** menu, enter **1**.
   e. In the **IP Address** field, enter **192.168.10.80**.

f. Click the **Add** button. Your settings are saved.

Command authorization for the CLI

Authorization determines if a user is authorized to perform certain activities such as entering specific EXEC commands in the CLI.

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 off 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

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

To use the CLI to configure command authorization by a RADIUS server for a Telnet user and deny the user to access specific command:

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 for the CLI

Authorization determines if a user is authorized to perform certain activities such entering privileged EXEC commands in the CLI.

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

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

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
```

CLI: Configure Telnet EXEC accounting by a RADIUS server

Note: 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 in the CLI lets you configure an authentication method menu, 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.

Dot1x MAB authentication method lists

This section describes the dot1x authentication order and priority.

Dot1x MAB authentication method list with MAB dot1x priority

Note: 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 344.

In the following figure, 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.

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 menu, 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.

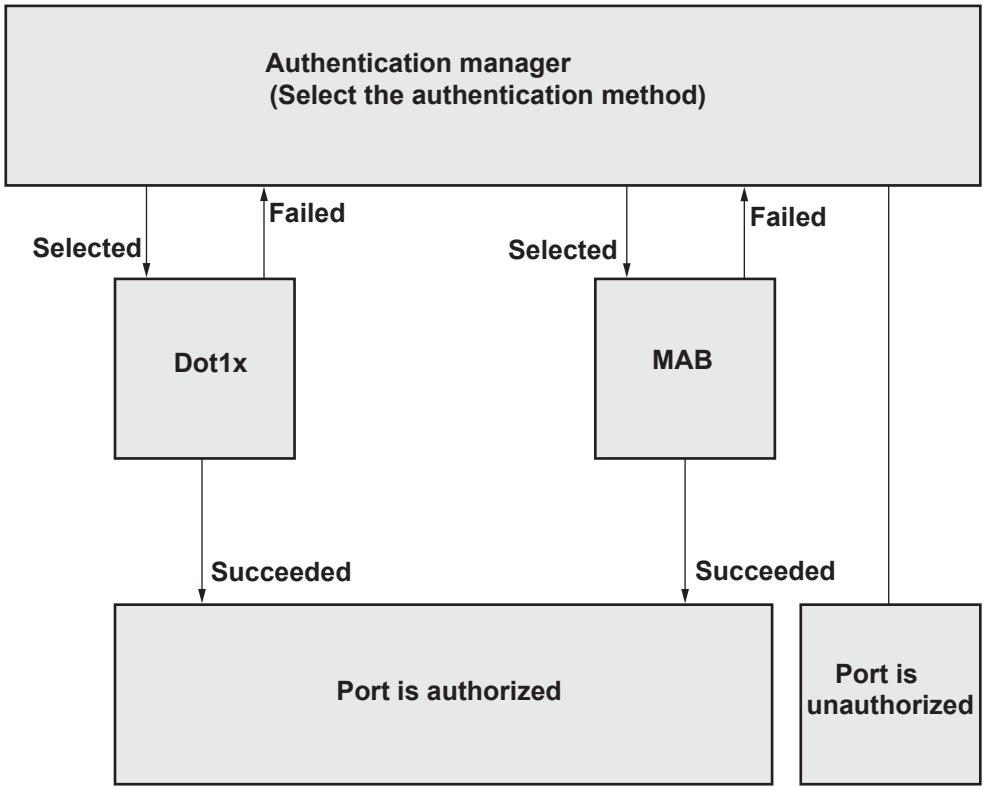


Figure 43. Dot1x, MAB, and captive portal authentication method list with default priority

Dot1x, MAB, and captive portal authentication method list with default priority

Note: For information about configuring the captive portal authentication method, see Chapter 38, Captive Portals.

In this following figure, 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 menu, 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 menu, 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.

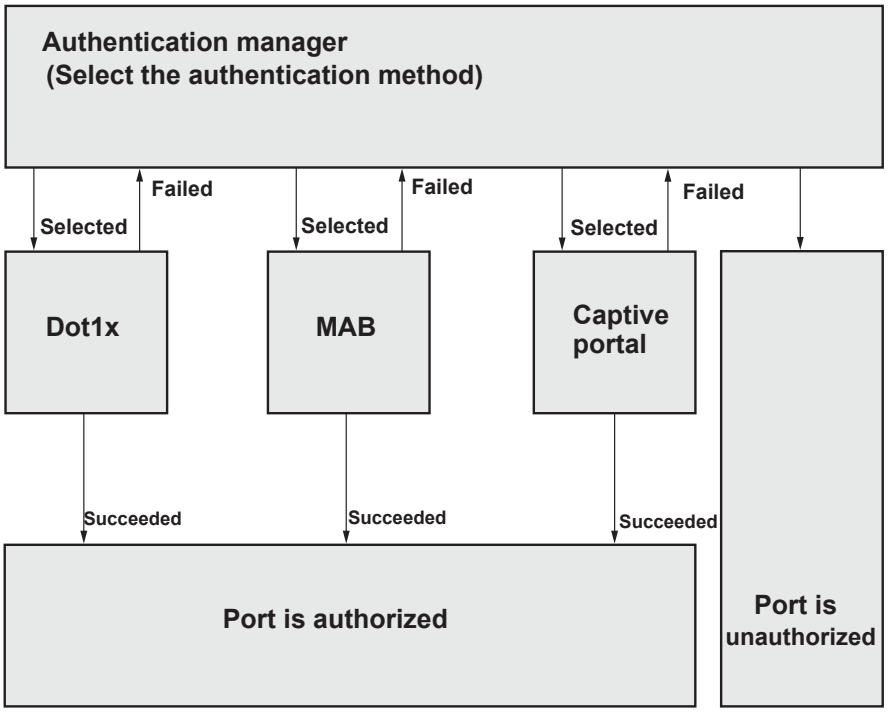


Figure 44. Dot1x, MAB, and captive portal authentication method list with default priority

RADIUS change of authorization

Note: You can configure the RADIUS change of authorization feature in the CLI only.

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.

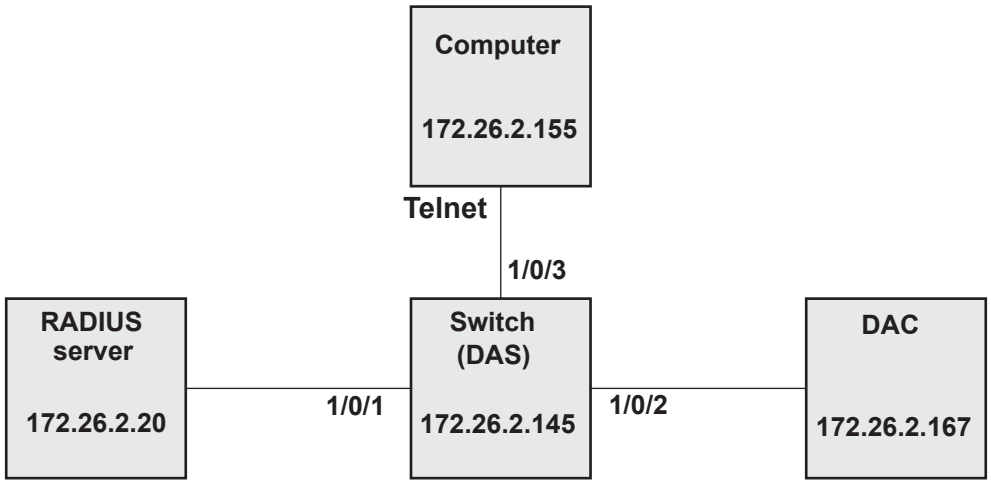


Figure 45. Configuration with a RADIUS server, DAS, and DAC

To use the CLI to configure RADIUS authentication with change of authorization:

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
```

As an option, to use Linux to configure a Dynamic Authorization Client (DAC):

1. On the 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"
```

2. Authenticate a Telnet user with RADIUS server credentials.

   If the authentication is successful, the session displays in the output of the **`show login sessions`** CLI command on the switch.

3. 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 the stateless mode only.

Note: You can configure the IPv6 Stateless RA Guard feature in the CLI only.

CLI: Configure IPv6 RA Guard

To use the CLI 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
```

Change SSH and Telnet login authentication to RADIUS

This example shows how to change SSH and Telnet login authentication to RADIUS.

By default, SSH and Telnet login are authenticated through the local authentication method. This section describes how to configure RADIUS as the authentication method. You can also configure additional authentication methods for SSH and Telnet.

The example is shown as CLI commands and as a main UI procedure.

CLI: Change the SSH and Telnet login authentication to RADIUS

To use the CLI to change the SSH and Telnet login authentication to RADIUS:

1. Change the authentication list networkList to RADIUS as the login authentication.

```
(Netgear Switch) (Config)#aaa authentication login networkList radius
```

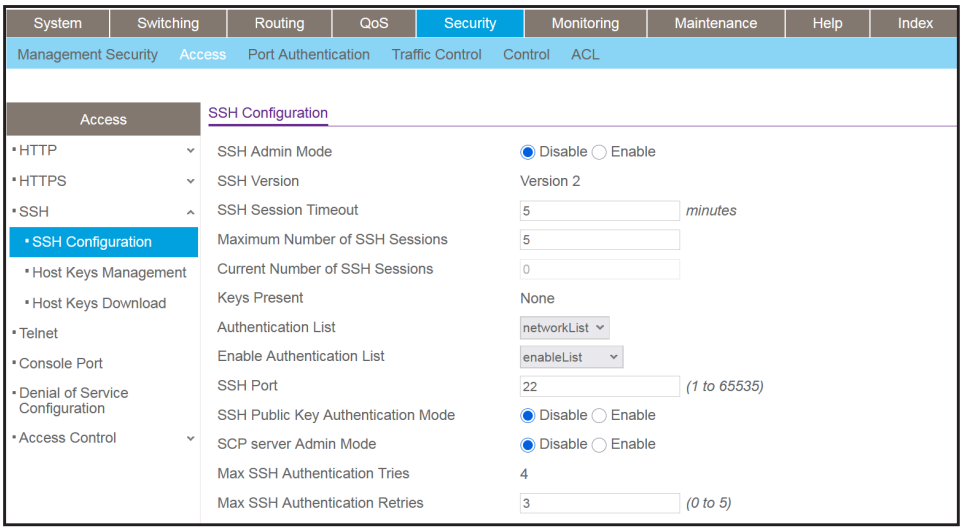
2. Verify that the networkList login authentication changed from local authentication to RADIUS.

```
(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
```

Main UI: Change the SSH and Telnet login authentication to RADIUS

To use the main UI to change the SSH and Telnet login authentication to RADIUS:

1. Set the authentication list for SSH to networkList.
   a. Select **Security > Access > SSH > SSH Configuration**.
      A page similar to the following figure displays.



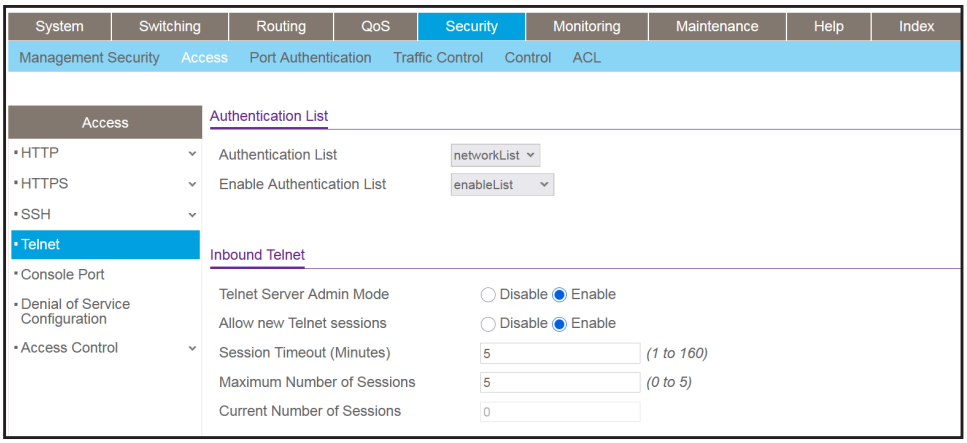
b. In the **Authentication List** menu, select **networkList**.

c. Click the **Apply** button. Your settings are saved.

2. Set the authentication list for Telnet to networkList.

a. Select **Security > Access > Telnet > Telnet Configuration**.

A page similar to the following figure displays.



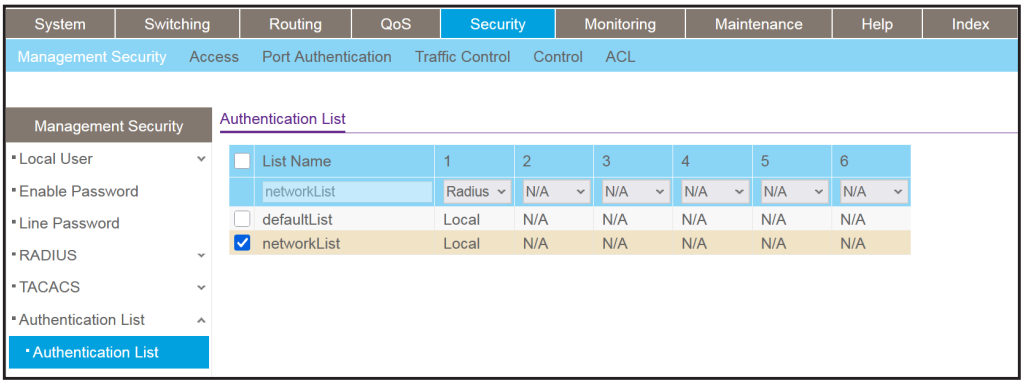
b. Under Authentication List, in the **Authentication List** menu, select **networkList**.

c. Click the **Apply** button. Your settings are saved.

3. Change the networkList authentication method to RADIUS.

a. Select **Security > Management Security > Authentication list > Authentication List.**

A page similar to the following figure displays.



b. Select the List Name **networkList** check box.

c. In the **1** menu, select **Radius**.

d. Click the **Apply** button. Your settings are saved.

18

NTP

Network Time Protocol

This feature is supported on the M4250 series switches

This feature is supported on the M4350 series switches

This chapter includes the following sections:

- Network Time Protocol concepts
- Show commands for NTP in the CLI
- Configure NTP
- Set the time zone
- Configure a NETGEAR NTP server using its DNS address

Note: The Network Time Protocol (NTP) feature is supported on the M4250 series and M4350 series switches only. The M4300 series switches do not support NTP; they support Simple Network Time Protocol (SNTP).

Network Time Protocol concepts

Network Time Protocol (SNTP) offers the following benefits:

- Polls a known time server that is identified by its DNS or IP address and then synchronizes the time for a network resource such as a switch.
- Can use a key for authentication with the SHA2 algorithm.
- Provides synchronized network timestamps.
- Can be used in a unicast or broadcast mode.
- Supports an NTP client implemented over UDP, which listens on port 123.

Show commands for NTP in the CLI

The following are examples of CLI commands used to display information about NTP.

show ntp

```
(Netgear Switch) #show sntp?

<cr>                     Press enter to execute the command.
associations             Displays the NTP associations.
authentication-keys      Displays the NTP authentication keys informations.
information              Displays the NTP software information.
packets                  Displays the NTP packet statistics.
servers                  Displays the NTP servers informations.
status                   Displays the NTP status.
```

show ntp authentication-keys

```
(Netgear Switch) #show ntp authentication-keys
Key Id ..................................... 1
Key Value .................................. 66f7e003db45a5f4688fd3a7ee7112df
Message Authentication Algorithm ............ sha2
Trusted .................................... Yes

Key Id ..................................... 2
Key Value .................................. 66f7e003db45a5f4688fd3a7ee7112df
Message Authentication Algorithm ............ sha2
Trusted .................................... No
```

show ntp information

```
(Netgear Switch) #show ntp information

Ntp Software Name ............................ ntpd
Ntp Software Version ......................... ntpd 4.2.8p17@1.4004-o
Ntp System Type .............................. Linux/4.14.174-ldk_6.x-4d296fa3
```

show ntp packets

```
(Netgear Switch) #show ntp packets

Ntp In packets ............................... 336
Ntp Out packets .............................. 324
Ntp old version packets ...................... 0
Ntp protocol error packets ................... 0
```

show ntp servers

```
(Netgear Switch) #show ntp servers

Address ...................................... time-a.netgear.com
Version ...................................... 4
Key Id ....................................... 0
Minimum Poll Interval ........................ 6
Maximum Poll Interval ........................ 10
Prefer ....................................... No
Burst ........................................ Yes
Iburst ....................................... Yes

Address ...................................... time-c.netgear.com
Version ...................................... 4
Key Id ....................................... 0
Minimum Poll Interval ........................ 6
Maximum Poll Interval ........................ 10
Prefer ....................................... No
Burst ........................................ Yes
Iburst ....................................... Yes
```

show ntp status

```
(Netgear Switch) #show ntp status

associd=0 status=0615 leap_none, sync_ntp, 1 event, clock_sync,
system peer:        ec2-52-20-169-152.compute-1.amazonaws.com:123
system peer mode:   client
leap indicator:     00
stratum:            6
log2 precision:     -22
root delay:         90.024
root dispersion:    42.735
reference ID:       0x3414a998
reference time:     eb512bd1.a9b0b7cb  Sat, Feb  8 2025  1:03:13.662
system jitter:      0.332047
clock jitter:       1.385
clock wander:       0.083
broadcast delay:    3.000
symm. auth. delay:  0.00
```

Configure NTP

NETGEAR switches do not have a built-in real-time clock. However, you can configure an NTP server to get the time from a public NTP server over the Internet. The following steps configure NTP on the switch:

The example is shown as CLI commands and as a main UI procedure.

CLI: Configure an NTP server and an NTP source interface

To use the CLI to configure an NTP Server and an NTP source interface:

1. Configure the NTP server IP address.

   The IP address can be either a public NTP server or a company NTP server. You can search the Internet to locate a public server. The servers available could be listed in domain-name format instead of address format. In that case, use the `ping` command on a computer to find the server's IP address. The following example configures the NTP server IP address to 203.0.113.19.

```
(Netgear Switch) (Config)#ntp server 203.0.113.13
```

2. Configure the NTP source interface through which the switch can reach the NTP server.

```
(Netgear Switch) (Config)#ntp broadcast client
```

3. After the switch connects to the NTP server (by default, the global NTP mode is enabled), you can display the NTP server status, which includes the reference time. This time is then used in all logging messages.

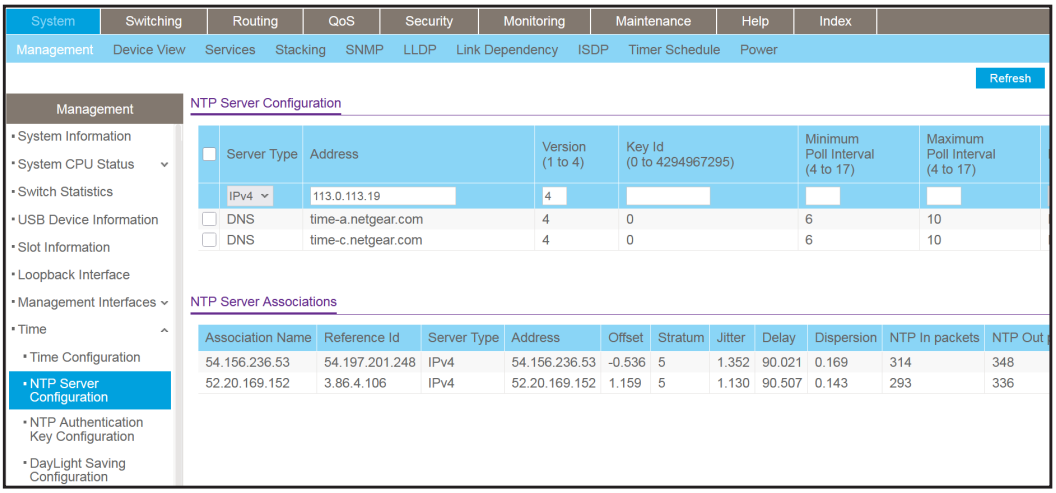
```
(Netgear Switch) #show sntp status
associd=0 status=0615 leap_none, sync_ntp, 1 event, clock_sync,
system peer:        ec2-52-20-169-152.compute-1.amazonaws.com:123
system peer mode:   client
leap indicator:     00
stratum:            6
log2 precision:     -22
root delay:         88.788
root dispersion:    4.622
reference ID:       0x3414a998
reference time:     eb514857.a9da1e9f  Sat, Feb  8 2025  3:04:55.663
system jitter:      0.849967
clock jitter:       1.173
clock wander:       0.074
broadcast delay:    3.000
symm. auth. delay:  0.000
```

Main UI: Configure an NTP server and an NTP source interface

To use the main UI to configure an NTP Server and an NTP source interface:

1. Configure the SNTP server.
   a. Select **System > Management > Time > SNTP Server Configuration**.

A page similar to the following figure displays.



b. Configure the following settings:

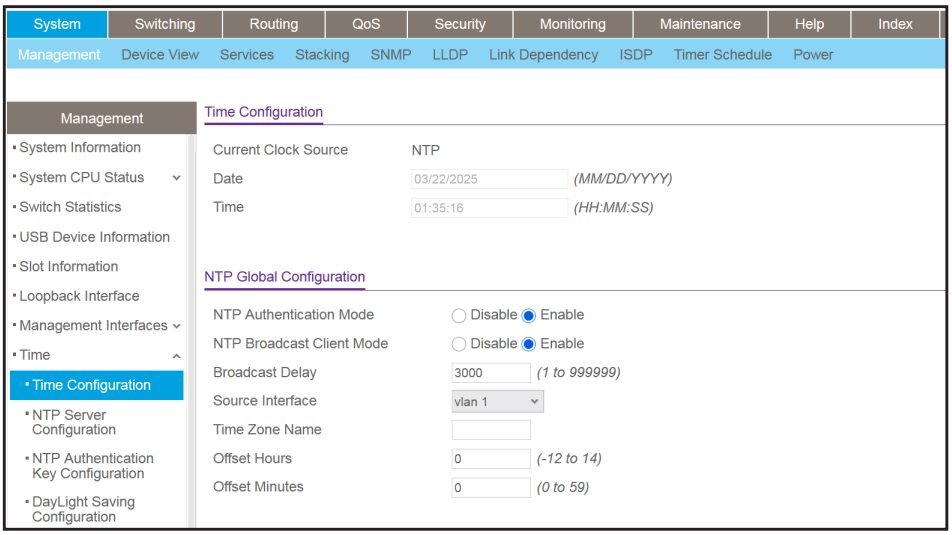
- In the **Server Type** field, select **IPv4**.
- In the **Address** field, enter **113.0.113.19**.
- In the **Version** field, enter **4**.

c. Click the **Add** button. Your settings are saved.

2. Configure the NTP source interface.

a. Select **System > Management > Time > Time Configuration**.

A page similar to the following figure displays.



b. Under NTP Global Configuration, in the **Source Interface** menu, select **vlan 1**.

c. Click the **Apply** button. Your settings are saved.

Set the time zone

The 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 UTC.

The example is shown as CLI commands and as a main UI procedure.

CLI: Set the time zone

To use the CLI to set the time to PST:

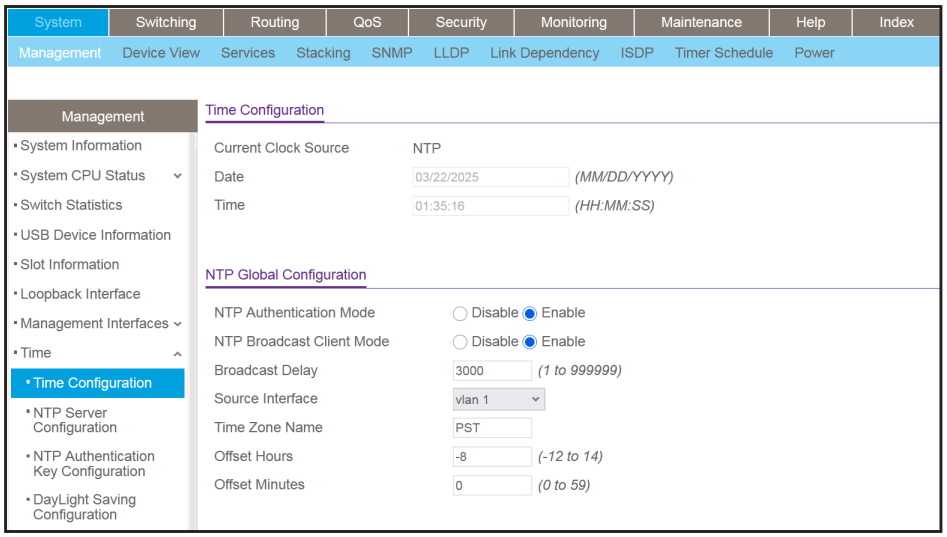
```
(Netgear switch)(config)#clock timezone -8 zone PST
```

Main UI: Set the time zone

To use the main UI to set the time to PST:

1. Select **System > Management > Time > Time Configuration**.

   A page similar to the following figure displays.



2. Under NTP Global Configuration, configure the following settings:
   a. In the **Time Zone Name** field, enter **PST**.
   b. In the **Offset Hours** field, enter **-8**.
3. Click the **Apply** button. Your settings are saved.

Configure a NETGEAR NTP server using its DNS address

NETGEAR provides NTP servers that are accessible by NETGEAR devices. Because NETGEAR might change the IP addresses assigned to its time servers, we recommend that you configure an NTP server to be accessed by its DNS name. The public NETGEAR time servers that are available include time-a.netgear.com, time-b.netgear.comare, and time-c.netgear.com.

The example is shown as CLI commands and as a main UI procedure.

CLI: Configure a NETGEAR NTP server using its DNS address

To use the CLI to configure a NETGEAR NTP server using its DNS address:

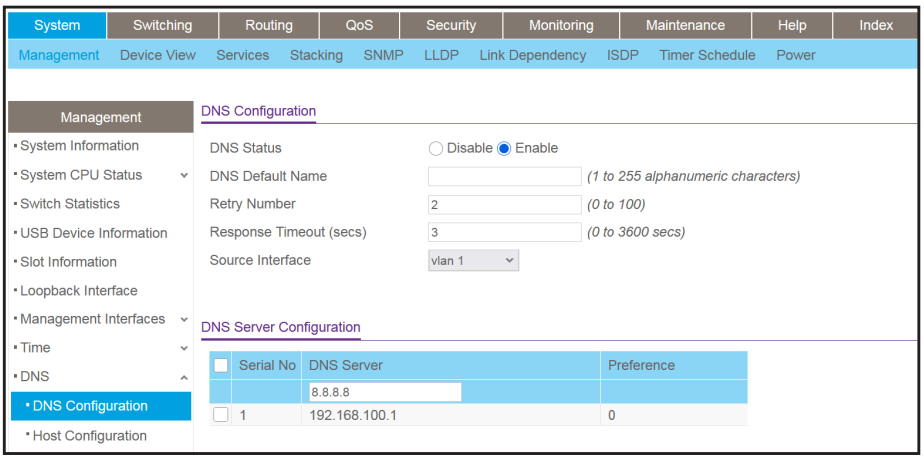
```
(Netgear switch)  (config)#ip domain lookup
(Netgear switch)  (config)#ip name-server 8.8.8.8
(Netgear switch)  (config)#ntp server time-a.netgear.com
```

Main UI: Configure a NETGEAR NTP server using its DNS address

To use the main UI to configure a NETGEAR NTP server using its DNS address:

1. Configure the DNS server.
   a. Select **System > Management > DNS > DNS Configuration**.

   A page similar to the following figure displays.



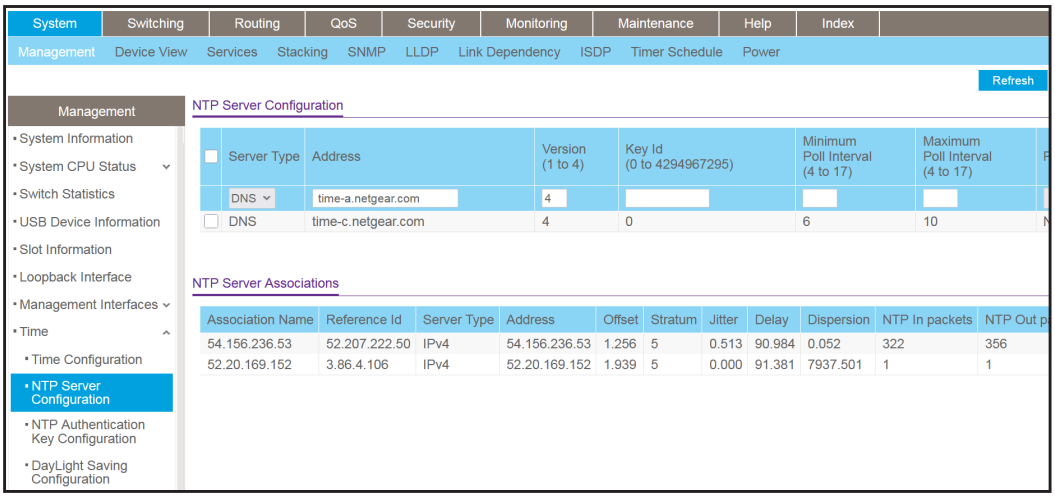
b. Configure the following settings:
   - Under DNS Configuration, select the DNS Status **Enable** radio button.
   - Under DSN Server Configuration, in the **DNS Server** field, enter **8.8.8.8**.

c. Click the **Add** button. Your settings are saved.

2. Configure the SNTP server.

a. Select **System > Management > Time > NTP Server Configuration**.

A page similar to the following figure displays.



b. Configure the following settings:
   - In the **Server Type** menu, select **DNS**.
   - In the **Address** field, enter **time-a.netgear.com**.
   - In the **Version** field, enter **4**.

c. Click the **Add** button. Your settings are saved.

19

SNTP

Simple Network Time Protocol

This feature is supported on the M4300 series switches

This chapter includes the following sections:

- Simple Network Time Protocol concepts
- Show commands for SNTP in the CLI
- Configure SNTP and set the time zone
- Configure a NETGEAR SNTP server using its DNS address

Note: The Simple Network Time Protocol (SNTP) feature is supported on the M4300 series switches only. The M4250 series and M4350 series switches do not support SNTP; they support Network Time Protocol (NTP).

Simple Network Time Protocol concepts

Simple Network Time Protocol (SNTP) offers the following benefits:

- Synchronizes network resources and functions as an adaptation of NTP.
- Provides a synchronized network timestamp.
- Can be used in broadcast or unicast mode.
- Supports an SNTP client implemented over UDP, which listens on port 123.

Show commands for SNTP in the CLI

The following are examples of the commands used to display information about SNTP.

show sntp

```
(Netgear Switch) #show sntp?

<cr>                    Press enter to execute the command.
client                  Display SNTP Client Information.
server                  Display SNTP Server Information.
source-interface        Display SNTP Client Source Interface 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 Host Address:               54.156.236.53
Server Type:                       IPv4
Server Stratum:                    5
Server Reference Id:               NTP Bits: 0x04ba0671
Server Mode:                       Server
Server Maximum Entries:            4
Server Current Entries:            2

SNTP Servers
------------

Host Address: time-a.netgear.com
Address Type: DNS
Priority: 1
Version: 4
Port: 123
Last Update Time: Jan 23 23:51:20 2025 (UTC+0:00)
Last Attempt Time: Jan 24 00:01:28 2025 (UTC+0:00)
Last Update Status: Request Timed Out
Total Unicast Requests: 12614
Failed Unicast Requests: 70
```

show sntp source-interface

```
(Netgear Switch) #show sntp source-interface

SNTP Client Source Interface:.....................vlan1
SNTP Client Source IPv4 Address:.................172.22.10.168          [Up]
```

Configure SNTP and set the time zone

NETGEAR switches do not have a built-in real-time clock. However, you can configure SNTP to get the time from a public NTP server over the Internet. The following steps configure NTP on the switch:

The example is shown as CLI commands and as a main UI procedure.

CLI: Configure SNTP and set the time zone

To use the CLI to configure SNTP and set the time zone:

1. Configure the SNTP server IP address.

   The IP address can be either from a public NTP server or your own server. You can search the Internet to locate a public server. The servers available could be listed in domain-name format instead of IP address format. In that case, use the `ping` command on a computer 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
```

3. Set the time zone.

   The SNTP 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 UTC.

```
(Netgear switch)(config)#clock timezone PST -8
```

4. After the switch connects to the server, you can display the SNTP server status, which includes the reference time. This time is then used in all logging messages.

The time is used in all logging messages.

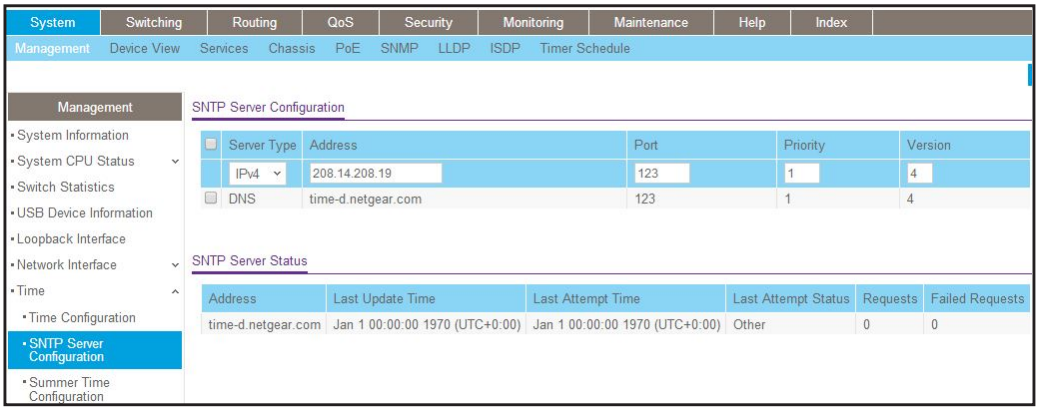
```
(Netgear Switch) #show sntp server
Server IP Address:                  208.14.208.19
Server Type:                        ipv4
Server Stratum:                     4
Server Reference Id:                NTP Srv: 208.14.208.3
Server Mode:                        Server
Server Maximum Entries:             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 2025
Last Attempt Time: Mar 26 03:36:09 2025
Last Update Status: Success
Total Unicast Requests: 2
Failed Unicast Requests: 0
```

Main UI: Configure SNTP and set the time zone

To use the main UI to configure SNTP and set the time zone:

1. Configure the SNTP server.
   a. Select **System > Management >Time > SNTP Server Configuration**.\

      A page similar to the following figure displays.



   b. Configure the following settings:
      - In the **Server Type** menu, select **IPv4**.

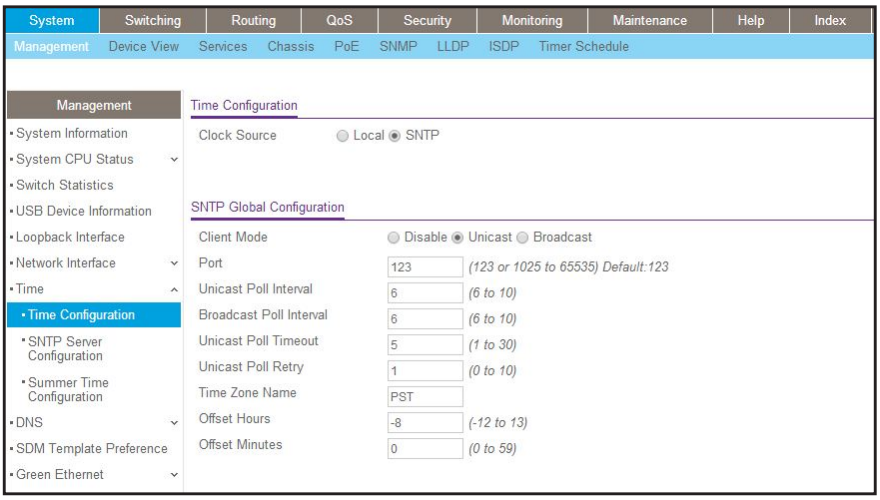
- In the **Address** field, enter **208.14.208.19**.
- In the **Port** field, enter **123**.
- In the **Priority** field, enter **1**.
- In the **Version** field, enter **4**.

c. Click the **Add** button. Your settings are saved.

2. Configure SNTP globally.

a. Select **System > Management > Time > Time Configuration**.

A page similar to the following figure displays.



b. Under SNTP Global Configuration, configure the following settings:

- Select the Client Mode **Unicast** radio button.
- In the **Time Zone Name** field, enter **PST**.
- In the **Offset Hours** field, enter **-8**.

c. Click the **Apply** button. Your settings are saved.

Configure a NETGEAR SNTP server using its DNS address

NETGEAR provides NTP servers that are accessible by NETGEAR devices. Because NETGEAR might change the IP addresses assigned to its time servers, we recommend that you configure an NTP server to be accessed by its DNS name. The public NETGEAR time servers that are available include time-a.netgear.com, time-b.netgear.comare, and time-c.netgear.com.

The example is shown as CLI commands and as a main UI procedure.

CLI: Configure a NETGEAR SNTP server using its DNS address

To use the CLI to configure a NETGEAR SNTP server using its DNS address:

Enable a DNS name server and access a time server with the following commands:

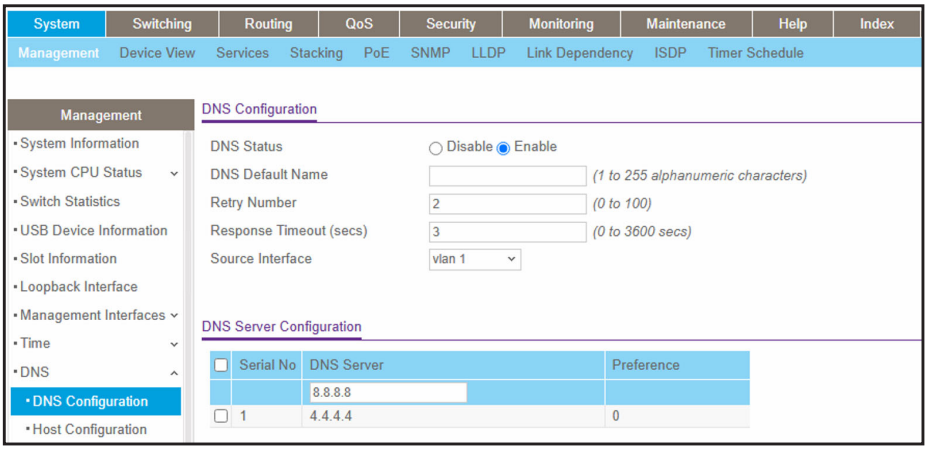
```
(Netgear switch) (config)#ip domain lookup
(Netgear switch) (config)#ip name server 8.8.8.8
(Netgear switch) (config)#sntp server time-f.netgear.com
```

Main UI: Configure a NETGEAR SNTP server using its DNS address

To use the main UI to configure a NETGEAR SNTP server using its DNS address:

3. Configure the DNS server.
   a. Select **System > Management > DNS > DNS Configuration**.

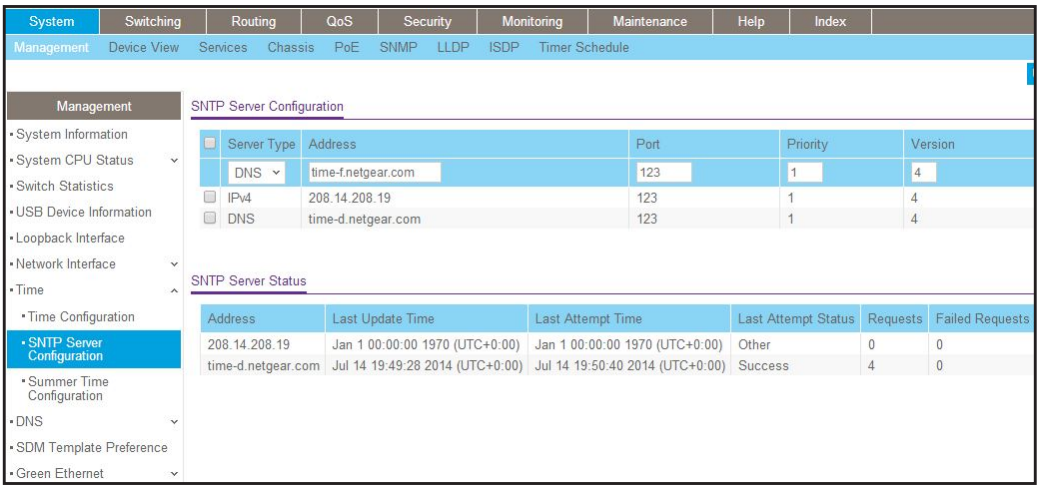
      A page similar to the following figure displays.



   b. Configure the following settings:
      - Select the DNS Status **Enable** radio button
      - In the **DNS Server** field, enter **8.8.8.8**.

   c. Click the **Add** button. Your settings are saved.
4. Configure the SNTP server.
   a. Select **System > Management > Time > SNTP Server Configuration**.

A page similar to the following figure displays.



b. Configure the following settings:

- In the **Server Type** menu, 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 the **Add** button. Your settings are saved.

20

Tools

Tools to manage, monitor, and personalize the switch and network

This feature is supported on the M4250 series switches

This feature is supported on the M4300 series switches

This feature is supported on the M4350 series switches

This chapter includes the following sections:

- Trace a route
- Configuration scripting (CLI only)
- Pre-login banner (CLI only)
- Port mirroring
- Remote SPAN
- Dual Image feature
- Outbound Telnet
- Error disablement and automatic error recovery (CLI only)
- Loop protection
- Nondisruptive Configuration Management feature (CLI only)
- Full memory dump

Trace a route

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 feature displays all L3 devices.
- You can use the traceroute feature to detect issues in the network.
- Traceroute tracks up to 20 hops.
- The default UPD port is 33343, unless you specify otherwise.

The following example uses the traceroute feature to determine how many hops there are to a destination. The 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.

The example is shown as CLI commands and as a main UI procedure.

CLI: Trace a route

To use the CLI to trace a route:

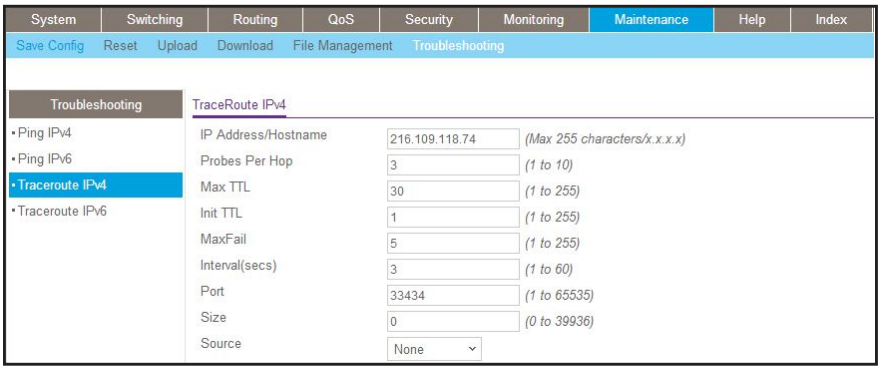
```
(Netgear Switch) #traceroute 216.109.118.74
tracing route over a maximum of 20 hops
 1  10.254.24.1         40 ms       9 ms      10 ms
 2  10.254.253.1        30 ms      49 ms      21 ms
 3  63.237.23.33        29 ms      10 ms      10 ms
 4  63.144.4.1          39 ms      63 ms      67 ms
 5  63.144.1.141        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
```

Main UI: Trace a route

To use the main UI to trace a route:

1. Select **Maintenance > Troubleshooting > Traceroute IPv4**

   A page similar to the following figure displays.



2. In the **IP Address/Hostname** field, enter **216.109.118.74**.
3. Click the **Apply** button.

   The switch sends three traceroute packets to each hop and the results are displayed in the Result pane.

Configuration scripting (CLI only)

Configuration scripting let's you do the following:

- Generate text-formatted files.
- Provides scripts that can be uploaded and downloaded to the switch.
- 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.
- The 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.

Pre-login banner (CLI only)

A pre-login banner lets you create message screens that display when a user logs in to the CLI. This feature is for the CLI only.

Consider the following:

- By default, no banner file exists.
- You can upload or download or banner.
- The banner file size cannot be larger than 2 K.

Create a Pre-login banner and upload it to the switch

To use Notepad to create a pro-login banner and use the CLI to upload it to the switch:

1. On your computer, use Notepad to create a banner.txt file that contains the banner that must be displayed.

```
Login Banner - Unauthorized access is punishable by law.
```

2. Transfer the file from the computer to the switch by 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

Port mirroring lets you monitor network traffic with an external network analyzer. You can use port mirroring as a diagnostic tool, debugging tool, or a means of fending off attacks.

Port mirroring does the following:

- Forwards a copy of each incoming and outgoing packet on the source port (or ports) to a specific port, which is called the destination port or probe port. A source port is also referred to as a mirrored port.
- Assigns the probe port to which the packets must be copied. A single probe port only is supported.
- Allows inbound packets, outbound packets, or both to be switched to their destination and to be copied to the probe port.

The example is shown as CLI commands and as a main UI procedure.

CLI: Specify a source port and a destination port

To use the CLI to specify a source port and a destination port:

1. Enable monitor session 1.

```
(Netgear Switch)#config
(Netgear Switch)(Config)#monitor session 1 mode
```

2. Set the source interface.

```
(Netgear Switch)(Config)#monitor session 1 source interface 1/0/2
```

3. Set the destination interface.

```
(Netgear Switch)(Config)#monitor session 1 destination interface 1/0/3
```

4. Display the port mirroring configuration. The source port is the mirrored ports; The destination port is the probe port.

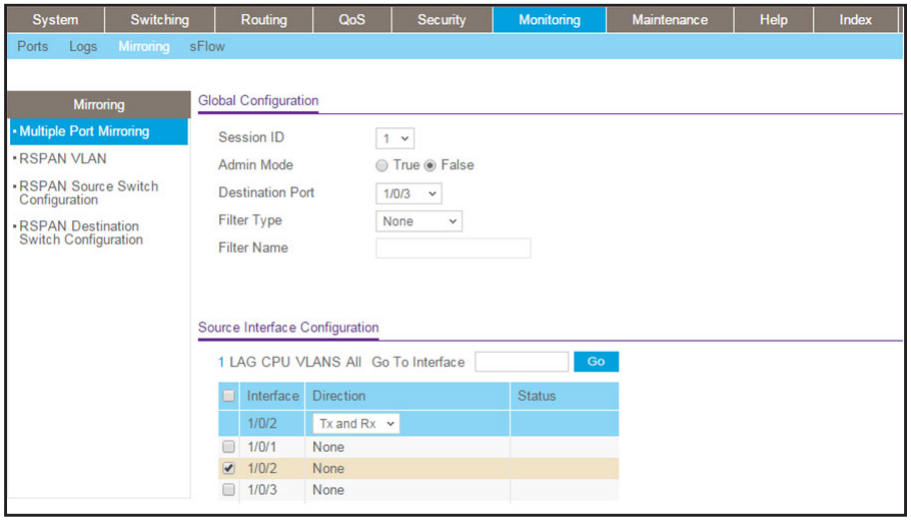
```
(Netgear Switch)(Config)#exit
(Netgear Switch)#show monitor session 1
Session ID     Admin Mode          Probe Port       Mirrored Port
-------------  ---------------     -------------    ----------------
      1        Enable              1/0/3             1/0/2
```

Main UI: Specify a source port and a destination port

To use the main UI to specify a source port and a destination port:

1. Select **Monitoring > Mirroring > Multiple Port Mirroring**.

   A page similar to the following figure displays.



2. Select the Admin Mode **True** radio button.
3. From the **Destination Port** menu, select **1/0/3**.
4. Select the Interface **1/0/2** check box.
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.

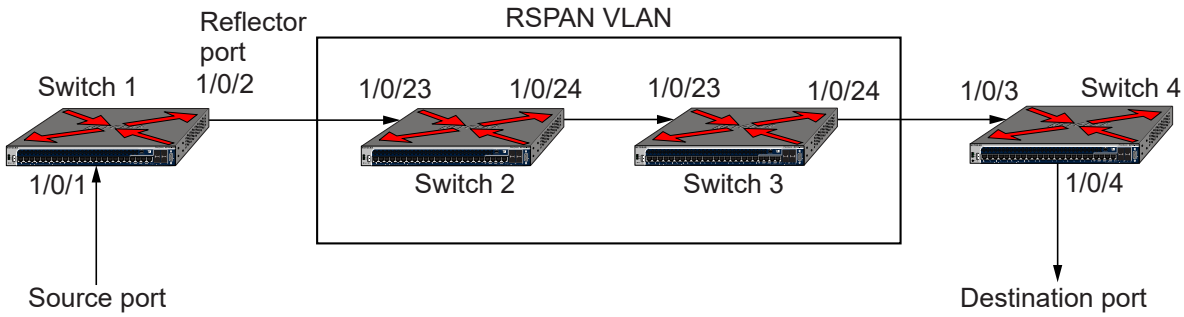


Figure 46. Example of an RSPAN topology

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 source, intermediate, and destination switches

You must configure RSPAN on source Switch 1, set the RSPAN-associated VLANs on intermediate Switches 2 and Switch 3, and configure RSPAN on destination Switch 4.

CLI: Configure the source switch (Switch 1)

On the source switch (Switch 1), to use the CLI to configure the RSPAN settings:

1. Configure the RSPAN VLAN (the destination for the mirrored traffic).

```
(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
```

2. Enable monitor session 1.

```
(Netgear Switch)#config
(Netgear Switch)(Config)#monitor session 1 mode
```

3. Configure the source interface (the port for which the traffic must be mirrored).

```
(Netgear Switch) (Config)#monitor session 1 source interface 1/0/1
```

4. Configure the reflector port, which is the port that is connected, through the intermediate switches, to the destination switch.

```
(Netgear Switch) (Config)#monitor session 1 destination remote vlan 5 reflector-port
1/0/2
```

5. Display the RSPAN configuration on the source switch. Both egress (Tx) and ingress (Rx) traffic is mirrored.

```
(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
```

CLI: Configure the intermediate switches (Switch 2 and Switch 3)

On the intermediate switches (Switch 2 and Switch 3), to use the CLI to 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. The traffic is just passing through.

1. Configure the VLAN.

```
(Netgear Switch) #vlan database
(Netgear Switch) (Vlan)#vlan 5
(Netgear Switch) (Vlan)#exit
(Netgear Switch) #config
```

2. Configure the interfaces that must be members of the VLAN.

```
(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
```

CL:I: Configure the destination switch (Switch 4)

On the destination switch (Switch 4), to use the CLI to configure the RSPAN settings:

1. Configure the RSPAN VLAN (the source of the mirrored traffic).

```
(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
```

2. Configure the source interface (the port that is connected, through the intermediate switches, to the source switch).

```
(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
```

3. Enable monitor session 1.

```
(Netgear Switch)#config
(Netgear Switch)(Config)#monitor session 1 mode
```

4. Set the VLAN as the source for RSPAN.

```
(Netgear Switch) (Config)#monitor session 1 source remote vlan 5
```

5. Set the destination interface.

```
(Netgear Switch) (Config)#monitor session 1 destination interface 1/0/4
```

6. Display the RSPAN configuration on the destination switch.

```
(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
```

Main UI: Enable RSPAN on source, intermediate, and destination switches

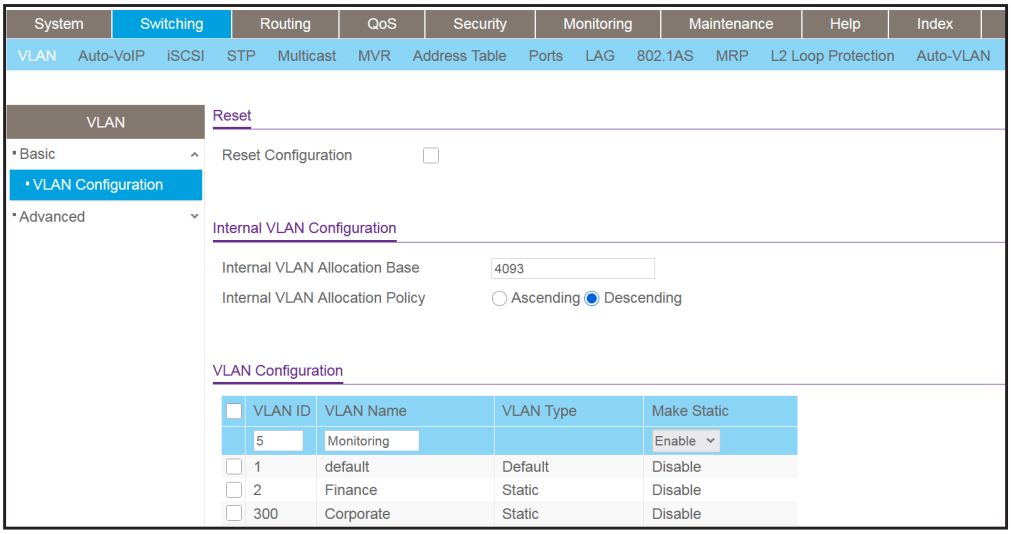
You must configure RSPAN on source Switch 1, set the RSPAN-associated VLANs on intermediate Switches 2 and Switch 3, and configure RSPAN on destination Switch 4.

Main UI: Configure the source switch (Switch 1)

On the source switch (Switch 1), to use the main UI to configure the RSPAN settings:

1. Add the VLAN that you plan to use for the RSPAN.
   a. Select **Switching > VLAN > Basic > VLAN Configuration**.

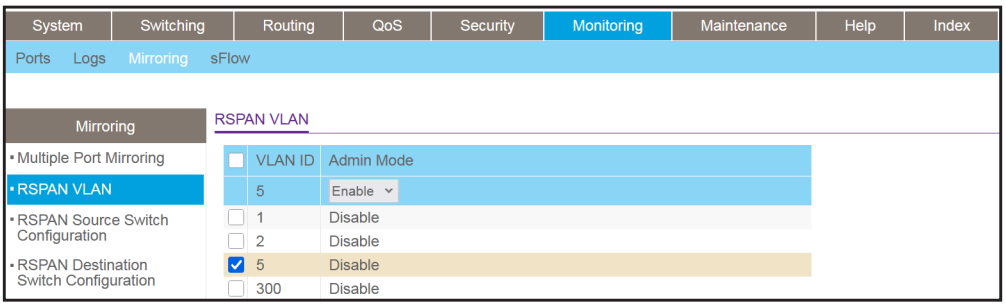
      A page similar to the following figure displays.



   b. In the **VLAN ID** field, enter **5**.
   c. Click the **Add** button. Your settings are saved.

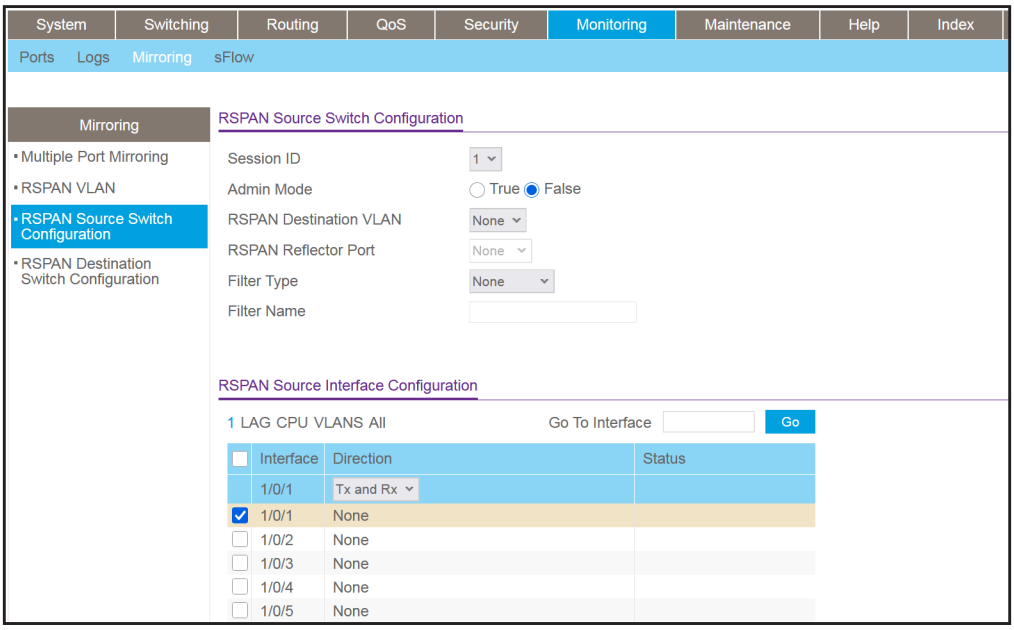
2. Configure the VLAN as an RSPAN VLAN.
   a. Select **Monitoring > Mirroring > RSPAN VLAN**.

      A page similar to the following figure displays.



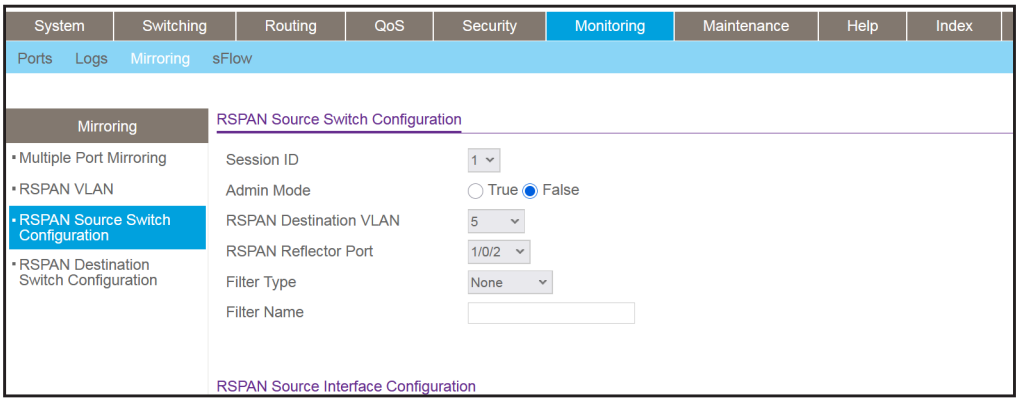
   b. Select the VLAN ID **5** check box.
   c. In the **Admin Mode** menu, select **Enable**.
   d. Click the **Apply** button. Your settings are saved.
3. Configure the source interface (the port for which the traffic must be mirrored).
   a. Select **Monitoring > Mirroring > RSPAN Source Switch Configuration**.

      A page similar to the following figure displays.



   b. Select the Interface **1/0/1** check box.
   c. In the **Direction** menu, select **Tx and Rx**.
   d. Click the **Apply** button. Your settings are saved.
4. Configure the destination RSPAN VLAN (the destination for the mirrored traffic) and the reflector port, which is the port that is connected, through the intermediate switches, to the destination switch.

e. Remain on the same page.



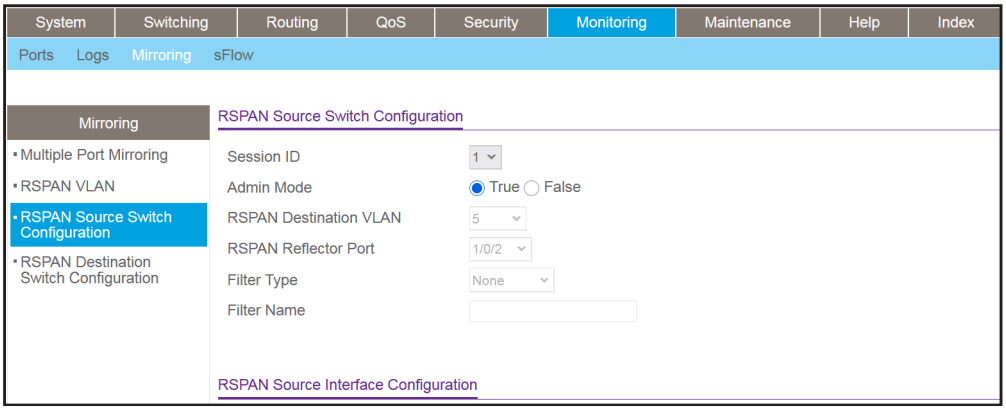
f. In the **RSPAN Destination VLAN** menu, select **5**.

g. In the **RSPAN Reflector Port** menu, select, **1/0/2**.

h. Click the **Apply** button. Your settings are saved.

5. Enable monitor session 1.

a. Remain on the same page.



b. In the **Session ID** menu, select **1**.

c. Select the Admin Mode **True** radio button.

d. Click the **Apply** button. Your settings are saved.

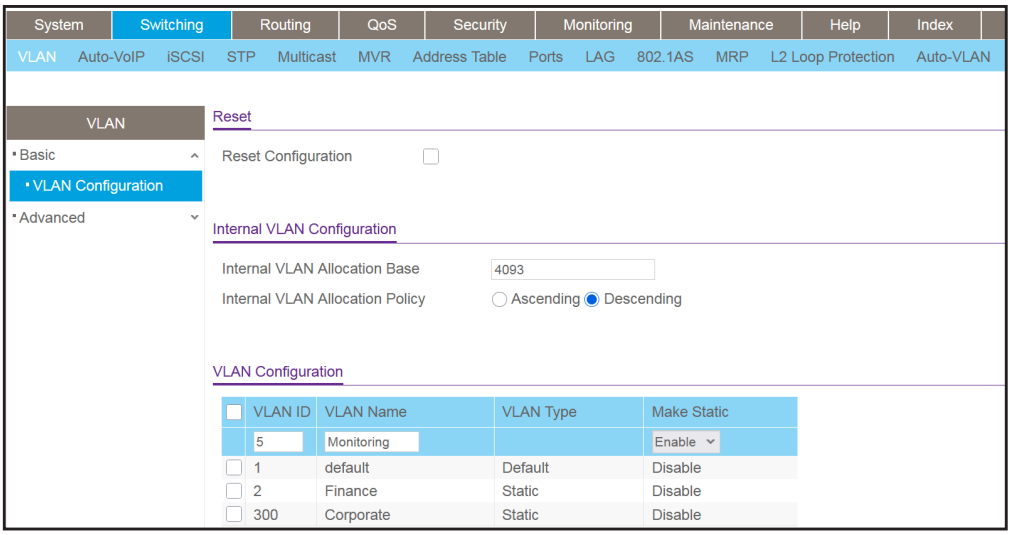
Main UI: Configure the intermediate switches (Switch 2 and Switch 3)

On the intermediate switches (Switch 2 and Switch 3), to use the main UI to 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. The traffic is just passing through.

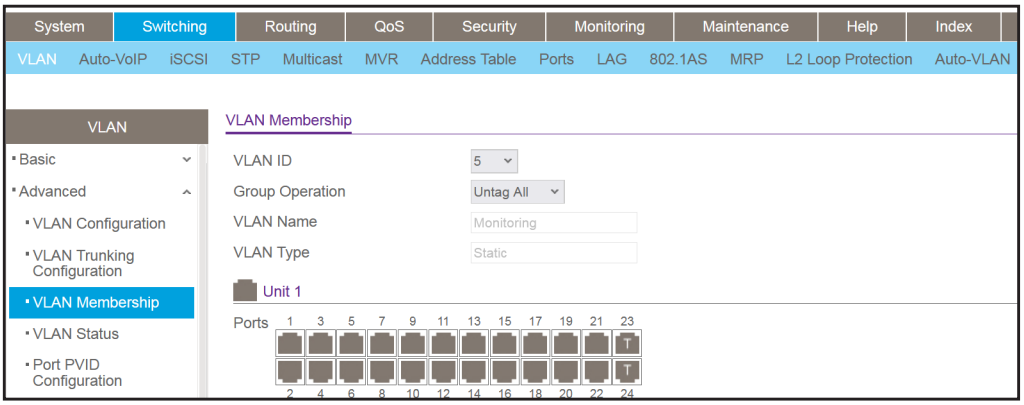
1. Add a VLAN.
   a. Select **Switching > VLAN > Basic > VLAN Configuration**.

      A page similar to the following figure displays.



   b. In the **VLAN ID** field, enter **5**.
   c. Click the **Add** button. Your settings are saved.
2. Configure the interfaces that must be members of the VLAN.
   a. Select **Switching > VLAN > Basic > VLAN Membership**.

      A page similar to the following figure displays.



b. In the **VLAN ID** menu, select **5**.

c. Click the gray boxes under ports **23** and **24** until T displays, which specifies that the egress packets are tagged for the ports.

If your switch is a member of a stack, be sure that you select the ports in the correct unit.

d. Click the **Apply** button. Your settings are saved.

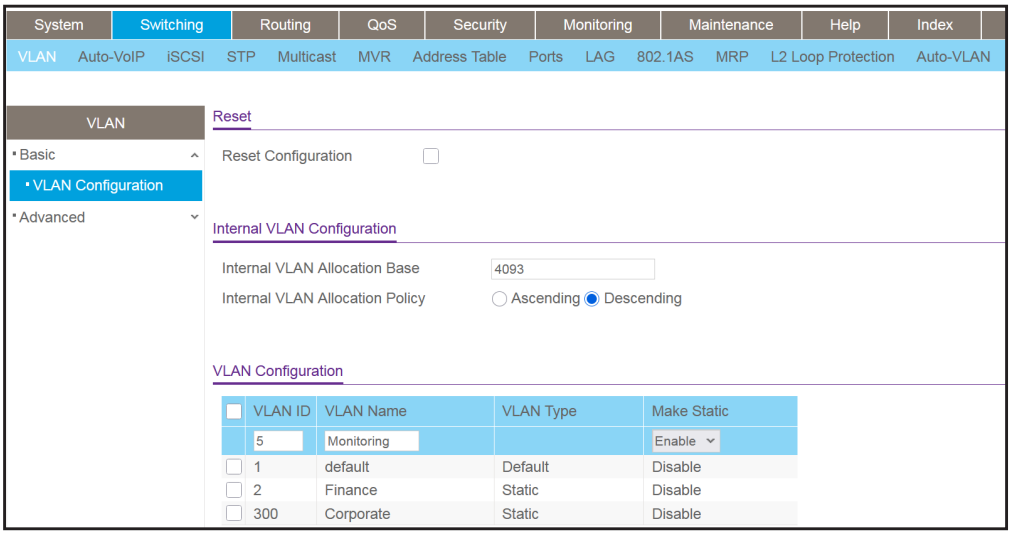
Main UI: Configure the destination switch (Switch 4)

On the destination switch (Switch 4), to use the main UI CLI to configure the RSPAN settings:

1. Add the VLAN that you are already using for the RSPAN on Switch 1.

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

A page similar to the following figure displays.



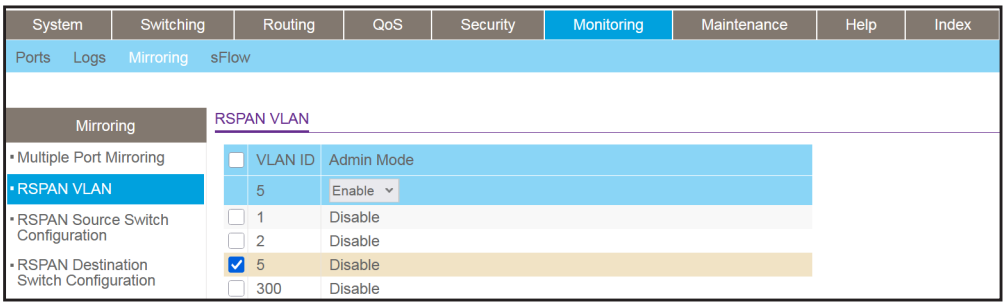
b. In the **VLAN ID** field, enter **5**.

c. Click the **Add** button. Your settings are saved.

2. Configure the VLAN as an RSPAN VLAN.

d. Select **Monitoring > Mirroring > RSPAN VLAN**.

A page similar to the following figure displays.



e. Select the VLAN ID **5** check box.

f. In the **Admin Mode** menu, select **Enable**.

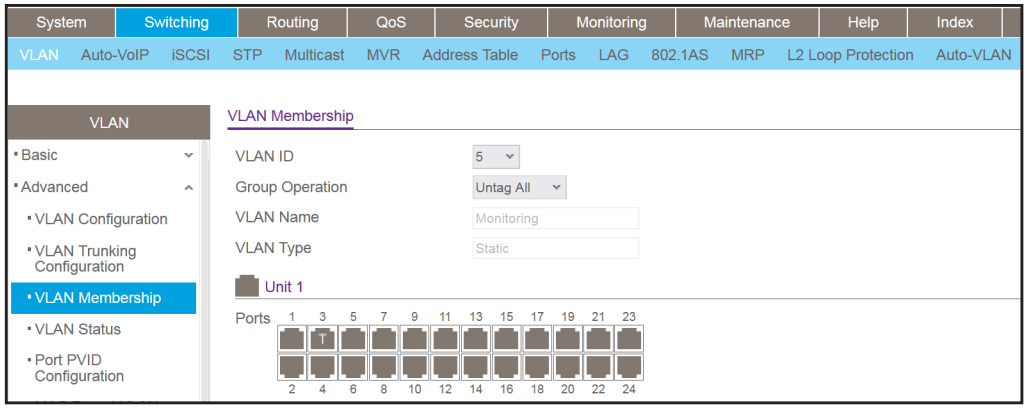
g. Click the **Apply** button. Your settings are saved.

3. Configure the source interface as a member of the VLAN.

   The source interface is the port that is connected, through the intermediate switches, to the source switch.

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

      A page similar to the following figure displays.



   b. In the **VLAN ID** menu, select **5**.

   c. Click the gray box under port **3** until T displays, which specifies that the egress packets are tagged for the port.

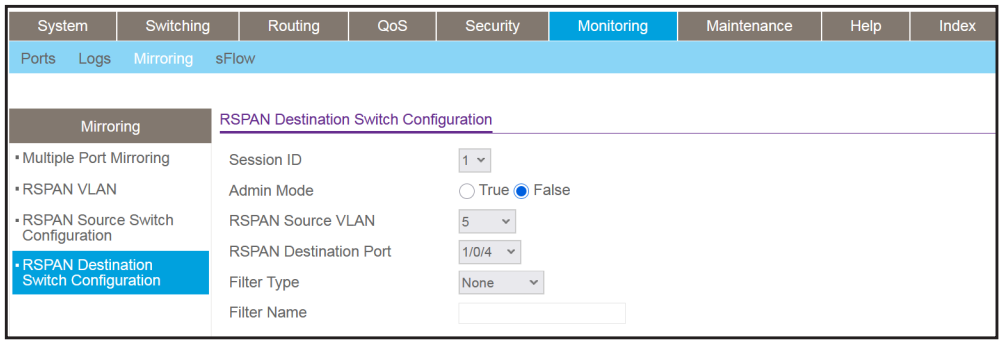
      If your switch is a member of a stack, be sure that you select the port in the correct unit.

   d. Click the **Apply** button. Your settings are saved.

4. Configure the destination RSPAN VLAN (the destination for the mirrored traffic) and the destination port.

   a. Select **Monitoring > Mirroring > RSPAN Destination Switch Configuration**.

      A page similar to the following figure displays.



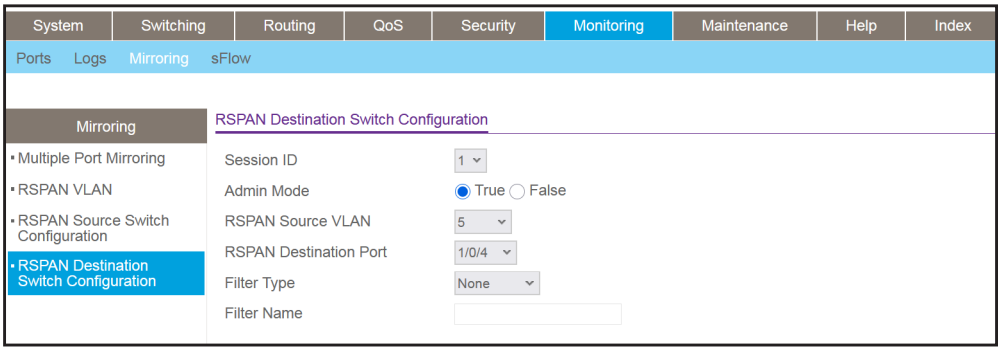
   b. In the **RSPAN Source VLAN** menu, select **5**.

   c. In the **RSPAN Destination Port** menu, select, **1/0/4**.

d. Click the **Apply** button. Your settings are saved.

5. Enable monitor session 1.

a. Remain on the same page.



b. In the **Session ID** menu, select **1**.

c. Select the Admin Mode **True** radio button.

d. Click the **Apply** button. Your settings are saved.

Dual Image feature

Many switches contain a single image only 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 configure one of these images as an active image that must be loaded in subsequent reboots and the other image as a backup image. This feature reduces down time for a switch, 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, main UI, and SNMP interfaces. Each of the images can be associated with a text description. The switch provides commands to associate and retrieve the text description for an image.

The switch also provides a command to activate the backup image so that it is loaded in subsequent reboots. This activation command configures the current active image as the backup image for subsequent reboots.

Note: On three successive errors executing the **`active-image`** command, the switch automatically executes the **`backup-image`** command. If errors also occur executing the **`backup-image`** command, the bootloader invokes the boot menu.

CLI: Download a backup image and make it active

To use the CLI to download a backup image from a TFTP server and make the image the active image:

1. Download a backup image from a TFTP server and display the image configuration.

```
(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
File transfer operation completed successfully.
(Netgear Switch) #
(Netgear Switch) #show bootvar
Image Descriptions
 image1 : default image
 image2 :
```

2. Make the downloaded image (image 2) the active image and display the image configuration.

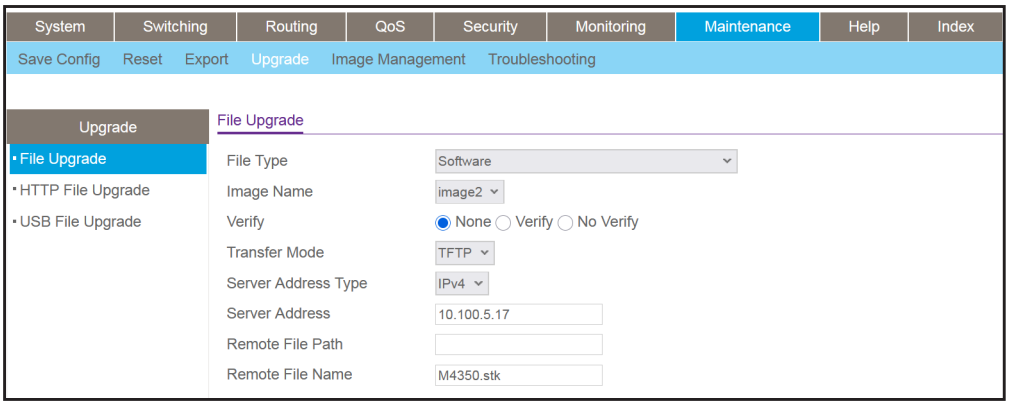
```
 Images currently available on Flash
--------------------------------------------------------------------
unit    image1        image2      current-active        next-active
--------------------------------------------------------------------
1       5.11.2.51     8.0.0.2         image1              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.
```

Main UI: Download a backup image and make it active

To use the main UI to download a backup image from a TFTP server and make the image the active image:

1. Download a backup image using a TFTP server.
   a. Select **Maintenance > Upgrade > File Upgrade**.

      A page similar to the following figure displays.



   b. In the **File Type** menu, select **Software**.
   c. In the **Image Name** menu, select **image2**.
   d. In the **Transfer Mode** menu, select **TFTP**.

e. In the **Server Address Type** menu, select the type of address of the TFTP server (in this example, **IPv4**).

f. In the **Server Address** field, enter the IP address of the TFTP server (in this example, **10.100.5.17**).

g. In the **Remote File Name**, enter the name of the image file (in this example, **M4350.stk**).

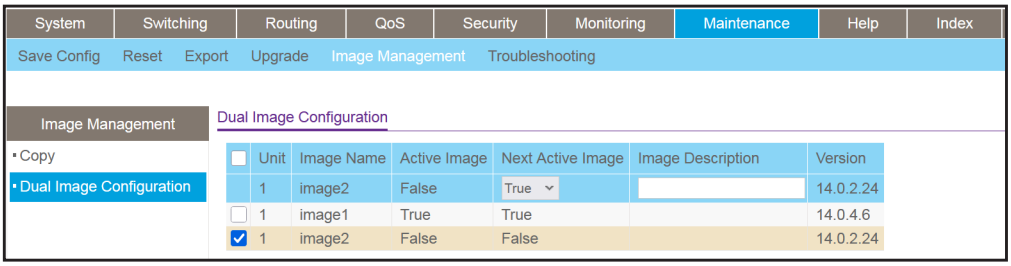
h. Click the **Apply** button. Your settings are saved.

2. Activate image2.

Note: The next time that the switch reboots, image 2 will be the active image.

a. Select **Maintenance > Image Management > Dual Image Configuration**.

A page similar to the following figure displays.



b. Select the Unit **image2** check box.

c. In the **Next Active Image** menu, select **True**.

d. Click the **Apply** button. Your settings are saved.

Outbound Telnet

Outbound Telnet establishes an outbound Telnet connection between the switch and a remote host. Note the following about outbound Telnet:

- After an outbound Telnet connection is initiated, each side of the connection is assumed to originate and terminate at a network virtual terminal (NVT).
- The server and user hosts do not maintain information about the characteristics of each other's terminals and terminal handling conventions.

Configure outbound Telnet

The example is shown as CLI commands and as a main UI procedure.

CLI: Configure outbound Telnet

To use the CLI to configure outbound Telnet:

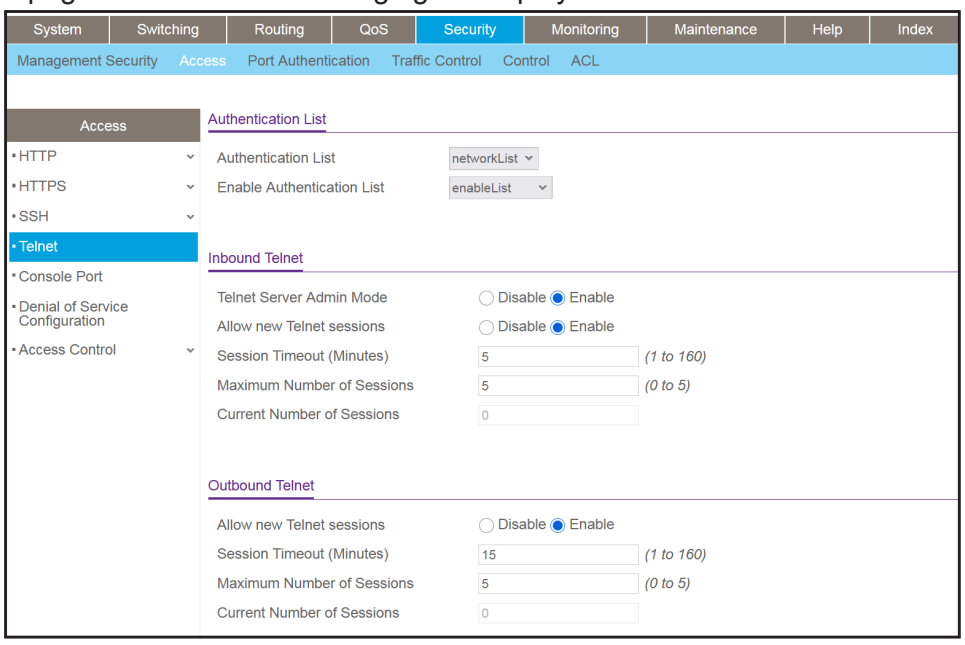
```
(Netgear Switch)#config
(Netgear Switch)(Config)#line console
(Netgear Switch)(Config-line)#transport output telnet
(Netgear Switch)(Config-line)#exit
(Netgear Switch)(Config)#
```

Main UI: Configure outbound Telnet

To use the main UI to configure outbound Telnet:

1. Select **Security > Access > Telnet**.

   A page similar to the following figure displays.



2. Under Outbound Telnet, select the Allow new Telnet sessions **Enable** radio button.
3. Click the **Apply** button. Your settings are saved.

Configure the outbound Telnet session limit and session time-out

The maximum number of simultaneously supported outbound Telnet sessions is five. The Telnet session limit can be from 1 to 160 minutes.

The example is shown as CLI commands and as a main UI procedure.

CLI: Configure the outbound Telnet session limit and session time-out

To use the CLI to configure the outbound Telnet session limit and session time-out:

1. Set the session limit.

```
(Netgear Switch) #telnetcon maxsessions 5
```

2. Set the session time-out period.

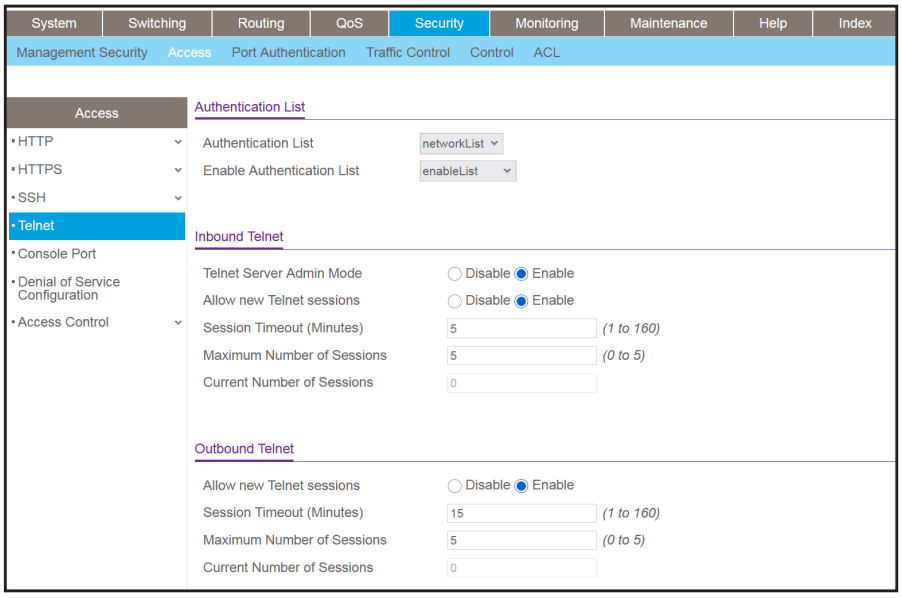
```
(Netgear Switch)#telnetcon timeout 15
```

Main UI: Configure the outbound Telnet session limit and session time-out

To use the main UI to configure the outbound Telnet session limit and session time-out:

1. Select **Security > Access > Telnet**.

   A page similar to the following figure displays.



2. Configure the following settings:
   - 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 (CLI only)

The switch supports interface error disablement, also referred to as Diagnostic Disable (D-Disable), and error autorecovery of a 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.

To use the CLI to 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 example is shown as CLI commands and as a main UI procedure.

CLI: Enable loop protection

To use the CLI to globally enable loop protection and 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.

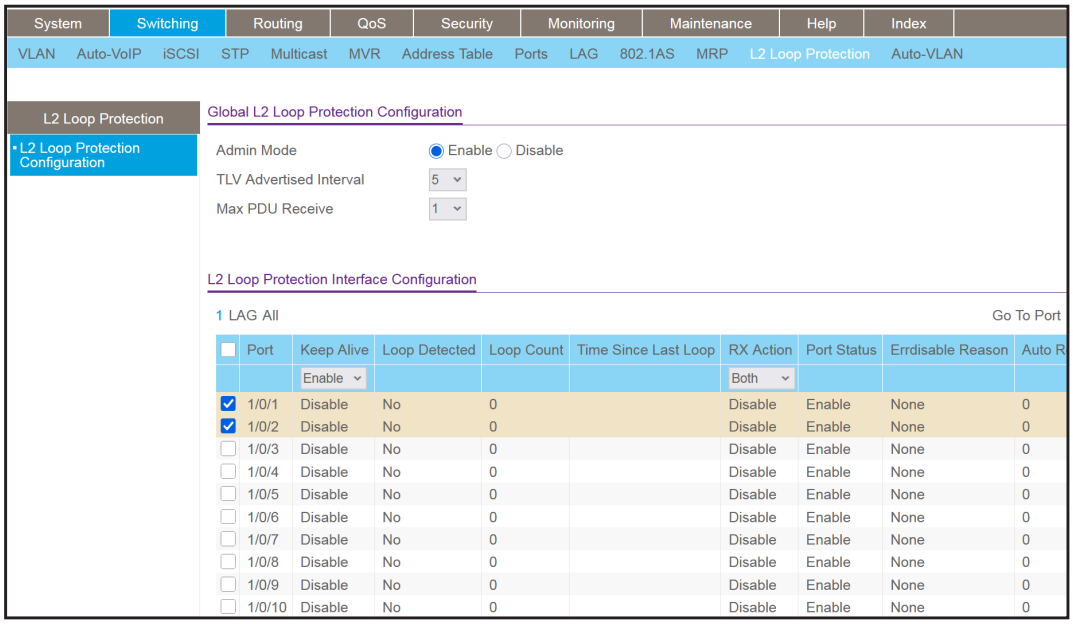
```
(Netgear Switch) (Config)#interface 1/0/1,1/0/2
(Netgear Switch) (Interface 1/0/1-1/0/2)#keepalive
(Netgear Switch) (Interface 1/0/1-1/0/2)#keepalive action both
```

Main UI: Enable loop protection

To use the main UI to globally enable loop protection and enable loop protection on ports 1/0/1 and 1/0/2:

1. Select **Switching > L2 Loop Protection > L2 Loop Protection Configuration**.

   A page similar to the following figure displays.



2. Under Global L2 Loop Protection Configuration, select the Admin Mode **Enable** radio button.
3. Under L2 Loop Protection Interface Configuration, configure the following settings:
   - Select the Interface **1/0/1 and 1/0/2** check boxes.
   - In the **Keep Alive** menu, select **Enable**.
   - In the **RX Action** menu, select **Both**.
4. Click the **Apply** button. Your settings are saved.

Nondisruptive Configuration Management feature (CLI only)

If you are managing a large network with hundreds 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.

To use the CLI to 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 lets you retrieve the state of a crashed switch and load it into a debugger to recreate the crashed state. This capability is useful after a crash occurs on a switch.

You can select NFS, TFTP, or USB to dump the memory to. 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 drive connected to the USB slot of the switch (model-dependent).

The file name for a full memory dump 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.

The example is shown as CLI commands and as a main UI procedure.

CLI: Perform a full memory dump

To use the CLI to perform a full memory dump using TFTP:

1. Configure TFTP as the method to transfer the full memory dump.

```
(Netgear Switch) (Config) #exception protocol tftp
```

2. Configure the IP address for the TFTP server.

```
(Netgear Switch) (Config) #exception dump tftp-server 172.26.2.100
```

3. Change the name of the full memory dump file.

```
(Netgear Switch) (Config) #exception core-file switchdump
```

4. (Optional) Enable the switch-chip-register to dump the register value in the chipset.

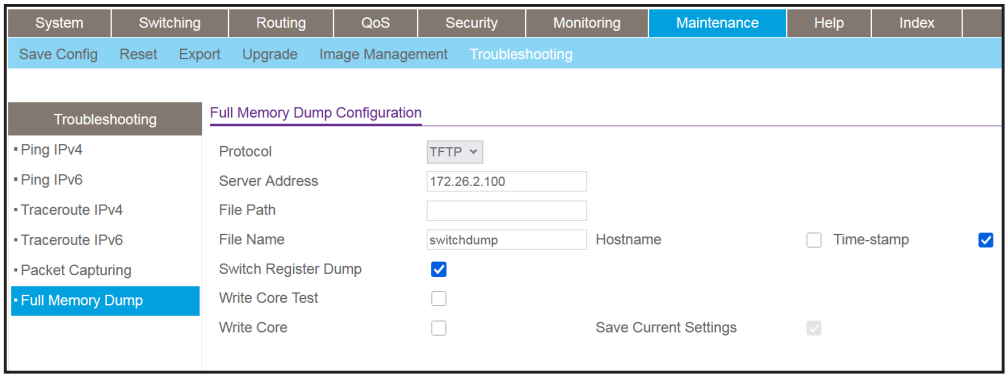
```
(Netgear Switch) (Config) #exception switch-chip-register enable
```

Main UI: Perform a full memory dump

To use the main UI to perform a full memory dump using TFTP:

1. Select **Maintenance > Troubleshooting > Full Memory Dump**.

   A page similar to the following figure displays.



2. Configure the following settings:
   - In the **Protocol** menu, select **TFTP**.
   - In the **Server Address** field, enter **172.26.2.100**.
   - In the **File Name** field, enter **switchdump**.
   - Select the **Switch Register Dump** check box.

     This enables the switch-chip-register to dump the register value in the chipset.
3. Click the **Apply** button. Your settings are saved. The full memory dump file is saved to the TFTP server.

21

Syslog

System logging

This feature is supported on the M4250 series switches

This feature is supported on the M4300 series switches

This feature is supported on the M4350 series switches

This chapter includes the following sections:

- Syslog concepts
- Syslog message logging
- Trap logs
- Logging
- Email alerting (CLI only)

Syslog concepts

The syslog feature lets you store system messages and errors. The featured provides a method of collecting message logs from many switches.

You can store the messages a local file on the switch or to a remote server that supports syslog.

The following illustration describes how to interpret log files.

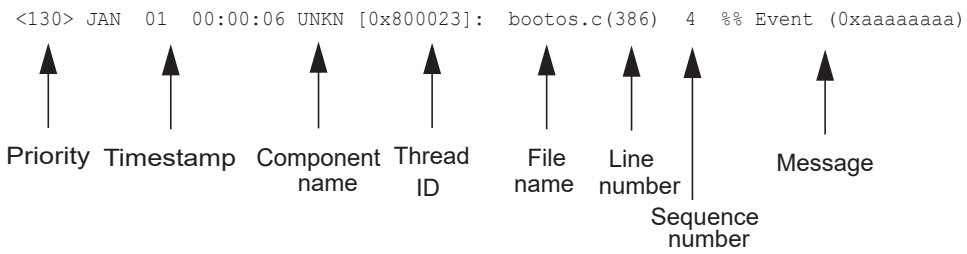


Figure 47. Log Files

Syslog message logging

You can configure the switch to log messages in its message log, also referred to as buffered log.

The priority of a log message is the number that is stated in angle brackets before each logging message, for example, <14>. This priority 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.

The example is shown as CLI commands and as a main UI procedure.

CLI: Configure the syslog settings and display the syslog messages

To use the CLI to configure the syslog settings and display the syslog messages:

1. Configure a syslog server.

```
(Netgear Switch) (Config)#logging host 192.168.100.120 ipv4 514 debug
```

2. Enable logging to the syslog server.

```
(Netgear Switch) (Config)#logging syslog
```

3. Display logging details.

```
(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
```

4. Display the buffered log messages.

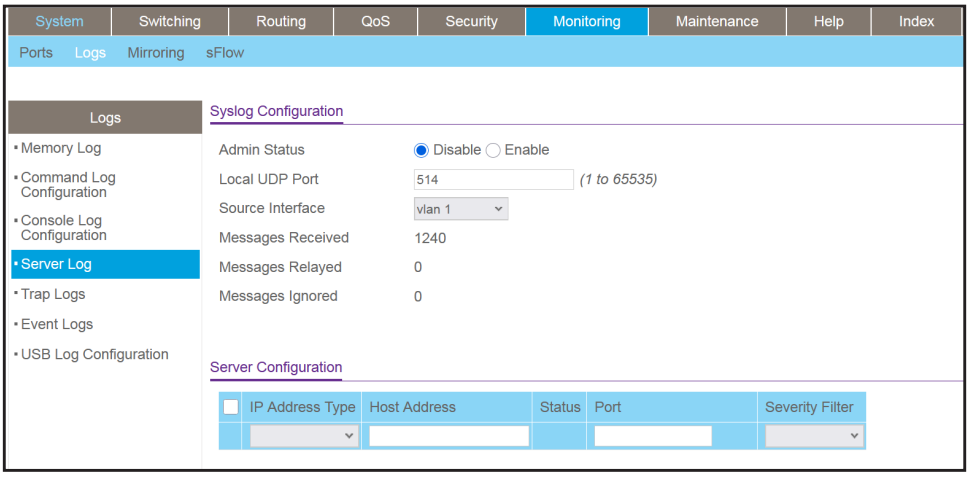
```
(Netgear Switch) #show logging buffered

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
```

Main UI: Configure the syslog settings and display the syslog messages

To use the main UI to configure the syslog settings and display the syslog messages:

1. Enable the syslog.
   a. From the main menu, select **Monitoring > Logs > Server Log**.

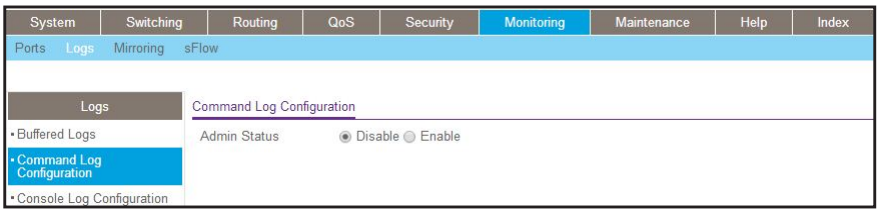
      A page similar to the following figure displays.



   b. Select the Admin Status **Enable** radio button.
   c. Click the **Apply** button. Your settings are saved.

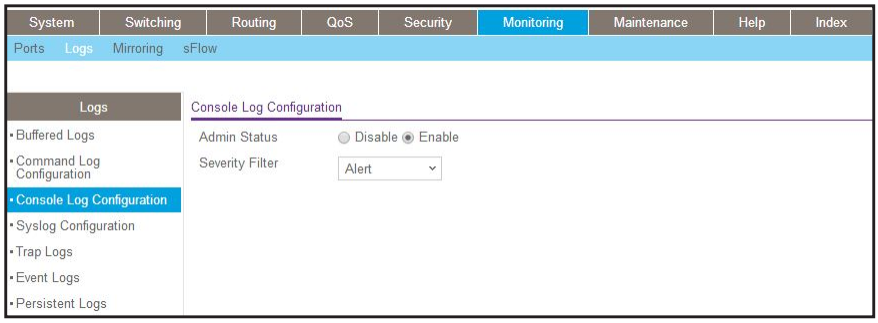
2. Make sure that the command log is disabled.
   a. Select **Monitoring > Logs > Command Log Configuration**.

      A page similar to the following figure displays.



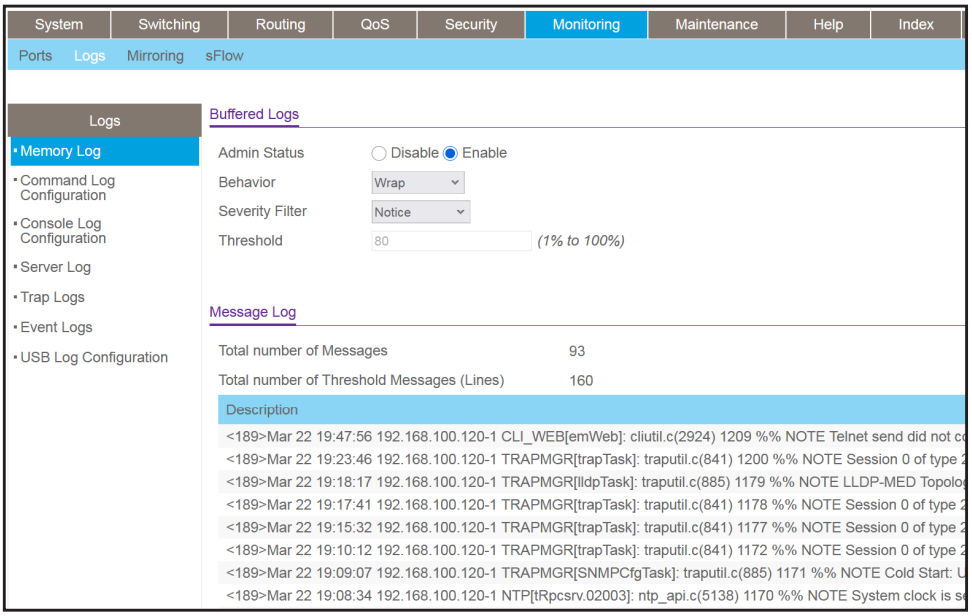
   b. Select the Admin Status **Disable** radio button.
   c. Click the **Apply** button. Your settings are saved.
3. Make sure that the console log is disabled.
   a. **Select Monitoring > Logs > Console Log Configuration**.

      A page similar to the following figure displays.



   b. Select the Admin Status **Disable** radio button.
   c. Click the **Apply** button. Your settings are saved.
4. Configure the memory log.
   a. Select **Monitoring > Logs > Memory Log**.

A page similar to the following figure displays.



b. Select the Admin Status **Enable** radio button.

c. Click the **Apply** button. Your settings are saved.

The Message Log section display the messages.

Trap logs

You can display the trap logs.

The example is shown as CLI commands and as a main UI procedure.

CLI: Display the trap logs

To use the CLI to display the trap logs:

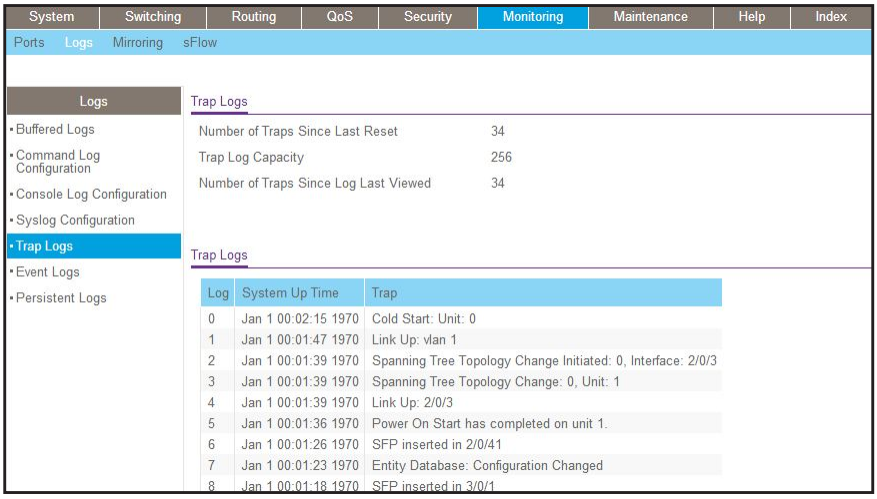
```
(Netgear Switch)                      #show logging traplogs
Number of Traps Since Last Reset..... 6
Trap Log Capacity.....................256
Number of Traps Since Log Last Viewed..... 6

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
```

Main UI: Display the trap logs

To use the main UI to display the trap logs:

Select **Monitoring > Logs > Trap Logs**.

A page similar to the following figure displays.



Logging

You can set the logging severity level to one of the following:

- emergency, 0
- alert, 1
- critical, 2
- error, 3
- warning, 4
- notice, 5
- info, 6
- debug, 7

The example is shown as CLI commands and as a main UI procedure.

CLI: Configure logging for a port and display the syslog server

To use the CLI to configure logging for a port and display the syslog server:

1. Set the host (server) IP address, set the port to 4, and the logging severity level to 1.

```
(Netgear Switch) (Config)#logging host 192.168.21.253 4 1
```

2. Display the syslog server configuration.

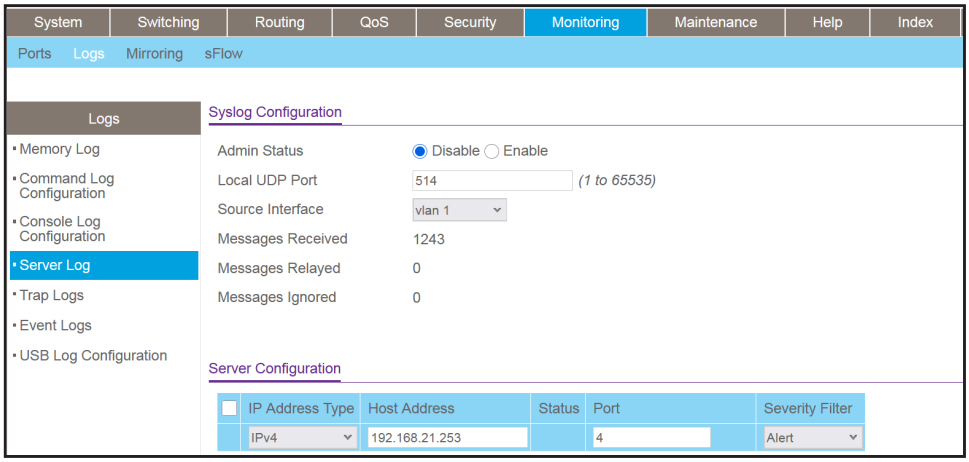
```
(Netgear Switch) #show logging hosts

Index  IP Address         Severity    Port  Status
-----  -----------------  ----------  ----  -------------
1      192.168.21.253     alert       4     Active
```

Main UI: Configure logging for a port and display the syslog server

To use the main UI to configure logging for a port and display the syslog server:

1. Select **Monitoring > Logs > Server Log**.

   A page similar to the following figure displays.



2. Under Server Configuration, configure the following settings:
   - In the **IP Address Type** field, enter **IPv4**.
   - In the **IP Address Type** field, enter your host address **192.168.21.253**.
   - In the **Port** field, enter **4**.
   - In the **Severity Filter** menu, select **Alert**.
3. Click the **Add** button. Your settings are saved. The configured syslog server displays in the table.

Email alerting (CLI only)

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 so that you can receive the log at an email address.

This feature is enabled globally, allowing selected log messages to be sent to an SMTP server. Log messages are divided into three groups by severity level:
urgent, nonurgent, and never.

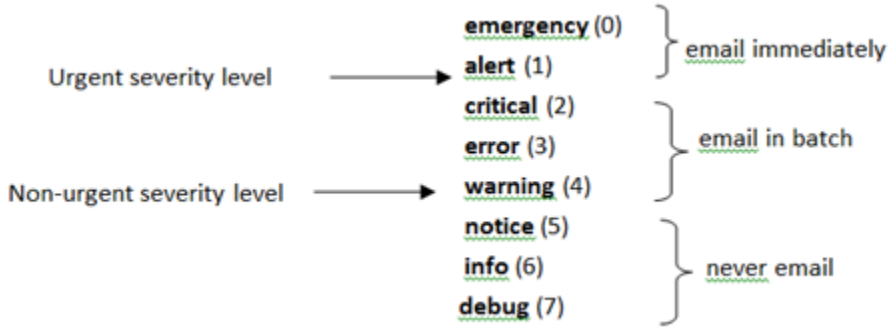


Figure 48. Log message severity levels

You 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 lets you specify the severity level at which SNMP traps are logged so that you can place traps in the urgent group, the non-urgent group, or the never group for emailing. By default, traps are not emailed. For traps to be emailed, you can either increase the severity at which traps are logged, or lower the severity level of log messages that are emailed.

You 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.

To use the CLI to send log messages to admin@company.com using account aaaa@company.com, and increase the severity level of trap messages to 3:

1. Configure an SMTP server, for example, smtp.netgear.com. (You must have an account on the 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 email address and the to-addr is the destination email address.

```
(Netgear Switch) (Config)#logging email
(Netgear Switch) (Config)#logging email from-addr aaaa@company.com
(Netgear Switch) (Config)#logging email message-type urgent to-addr
admin@company.com
(Netgear Switch) (Config)#logging email message-type non-urgent to-addr
admin@company.com
```

3. Increase the severity of traps to 3 (error). By default, it is 6 (informational).

```
(Netgear Switch) (Config)#logging traps 3
```

22

Switch Stacks

Manage switch stacks

This feature is supported on the M4300 series switches

This feature is supported on the M4350 series switches

This chapter describes the concepts and configuration examples of managing NETGEAR stackable managed switches.

This chapter includes the following sections:

- Switch stack management and connectivity
- Stack management switch and stack members
- Stack switches using 10G Ethernet ports
- Switch firmware and firmware mismatch
- Add, remove, or replace a stack member
- Switch stack configuration files
- Preconfigure a switch
- Renumber stack members
- Make a different unit the stack management switch

Note: Stacking is supported on the M4300 series and M4350 series switches only. The M4250 series switches do not support stacking.

Note: On model M4300-96X in which an APM402XL port card is installed, the APM402XL port card supports stacking over 40G ports only (that is, over port 1 and port 5 only). When you expands the ports, you cannot use the 10G ports for stacking.

Note: On the M4350 series switches, a stacking link works only on the highest speed supported by a stack port. For example, a 25G port that is also capable of operating at 10G speed operates only at 25G speed in stack mode. When you set up a stacking link between two switches, you must ensure that both ports operate at the same speed. For example, set up a stacking link between two ports that each support a maximum speed of 25G, or between two ports that each support a maximum speed of 10G.

Switch stack management and connectivity

You manage the switch stack through the stack management switch. You cannot manage stack members on an individual basis. To access the stack management switch, use either a serial connection to the management switch's console port or a Telnet connection to the IP address of the stack.

You can use these methods to manage switch stacks:

- Main UI
- CLI (over a serial connection).
- A network management application through SNMP

Stack management switch 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 management switch. The stack management switch and the other switches in the stack are stack members. Stack members use stacking technology to function 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.

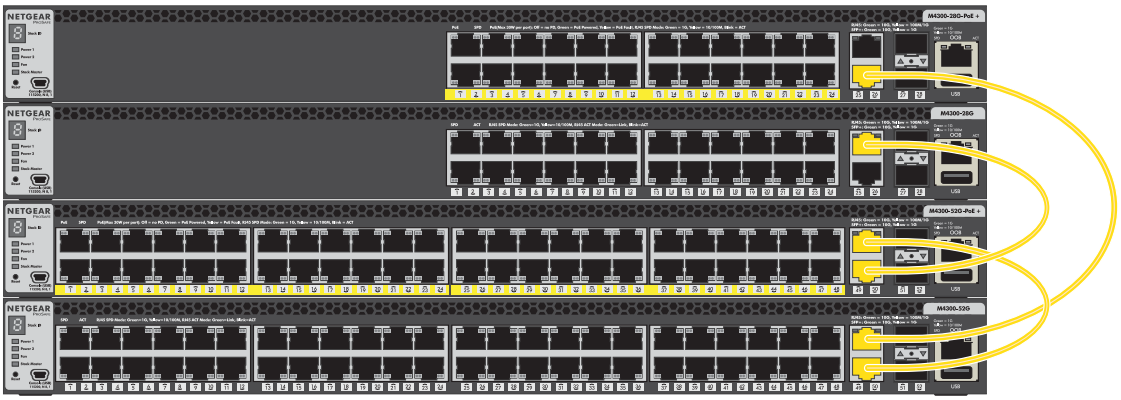


Figure 49. Stacked switches

Stack management switch

The stack management switch is the single point of stack-wide management. From the stack management switch, 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 management switch. Every stack member is uniquely identified by its own stack member number.

The stack management switch 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 management switches. If the stack management switch becomes unavailable, the remaining stack members participate in electing a new stack management switch. A set of factors determine which switch is elected the stack management switch.

The stack management switch is elected or re-elected based on one of these factors and in the order listed:

1. The switch that is currently the stack management switch
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 management switch. This ensures that the switch is re-elected as stack management switch if a re-election occurs.

---

3. The switch with the higher MAC address

A stack management switch retains its role unless one of these events occurs:

- The stack management switch is removed from the switch stack.
- The stack management switch is reset or powered off.
- The stack management switch fails.
- The switch stack membership is increased by adding powered-on standalone switches or switch stacks.

If a different stack management switch is elected, the new stack management switch 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 management switch is elected. If a new stack management switch is elected and the previous stack management switch becomes available, the previous stack management switch does not resume its role as stack management switch.

Stack members

A switch stack can include up to eight stack members connected through their stack ports. A switch stack always includes one stack management switch.

You could consider a standalone switch a switch stack with one stack member that also operates as the stack management switch. You can connect one standalone switch to another to create a switch stack containing two stack members, with one of them being the stack management switch. 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 management switch 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 480.

Stack member priority values

You can change a stack member priority. This is useful if you want to change the management switch of the stack. To change the stack member priority, issue the **`switch unit priority value`** command in the global config mode.

Install a switch stack

For more details see the hardware installation guide for your switch.

To install a switch stack:

1. Install the switches in a rack.
2. Install all stacking cables, including the redundant stack link.

   We highly recommend that you install a redundant link between the switches.
3. Identify the switch to be the stack management switch and power it up.
4. Monitor the console port.

   Allow the stack management 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 stack management 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 479.
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 management switch of a separate stack.
7. Monitor the stack management 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 480.
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.

Stack switches using 10G Ethernet ports

This example shows how to stack two switches at close range.

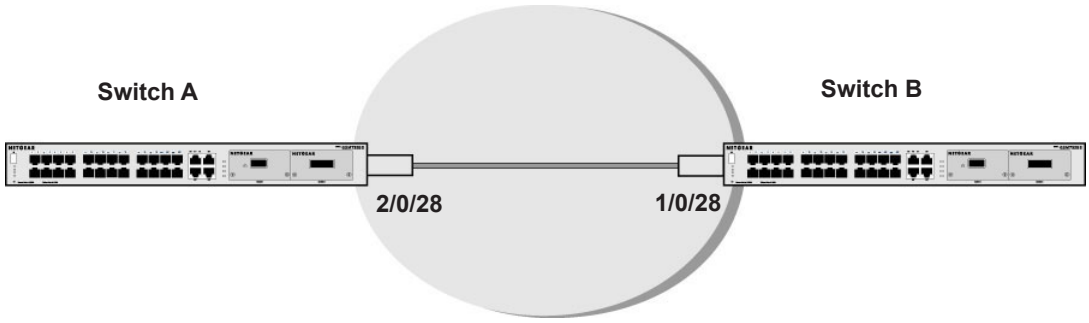


Figure 50. Connect switches through their 10G Ethernet ports

To set up a stack between two switches:

1. Using a Cat6e Ethernet cable, connect a 10G Ethernet port on one switch to a 10G Ethernet port on the other switch.
2. Configure Switch A and Switch B as described in the following sections:
   a. CLI: Configure 10G Ethernet ports as stack ports on page 469 or Main UI: Configure 10G Ethernet ports as stack ports on page 471
   b. Main UI: Copy the firmware of the stack management switch to a stack member on page 475

CLI: Configure 10G Ethernet ports as stack ports

To use the CLI to configure 10G Ethernet ports as stack ports:

1. On Switch A, display the stack port configuration, configure a 10G Ethernet port as a 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, display the stack port configuration again.

```
(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             Stack      Stack      Link Down    10
```

3. On Switch B, display the stack port configuration, configure a 10G Ethernet port as a 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, display the stack port configuration again.

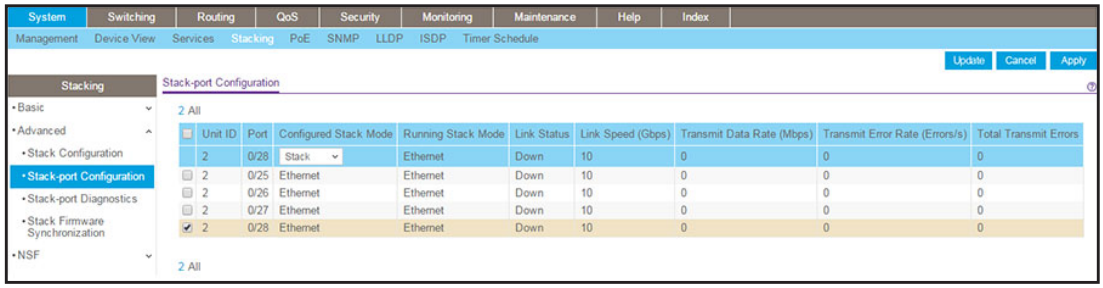
```
(Netgear Switch) #show stack-port

                     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            Stack      Stack      Link Down    10
```

Main UI: Configure 10G Ethernet ports as stack ports

To use the main UI to configure 10G Ethernet ports as stack ports:

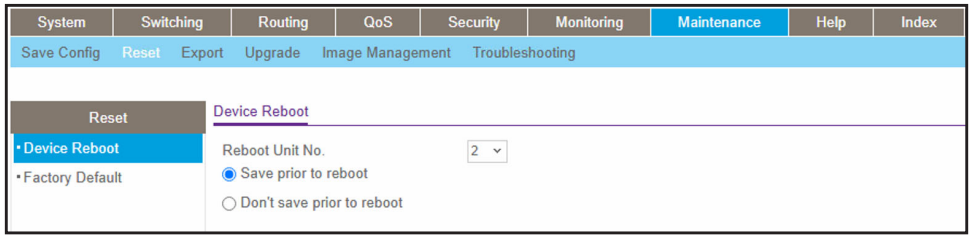
1. On Switch A, configure an Ethernet port as a stack port.
   a. Select **System > Stacking > Advanced > Stack Port Configuration**.

      A page similar to the following figure displays.



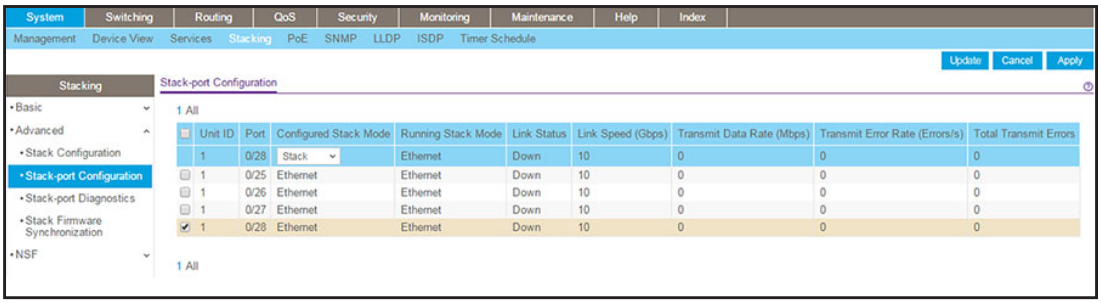
   b. Select the Port **2/0/28** check box.
   c. In the **Configured Stack Mode** menu, select **Stack**.
   d. Click the **Apply** button. Your settings are saved.
2. Reboot the switch.
   a. Select **Maintenance > Reset > Device Reboot**.

      A page similar to the following figure displays.



   b. In the **Reboot Unit No.** menu, select **2**.
   c. Select the **Save prior to reboot** radio button.
   d. Click the **Apply** button. Your settings are saved, and the switch reboots.
3. On Switch B, configure an Ethernet port as a stack port.
   a. Select **System > Stacking > Advanced > Stack Port Configuration**.

      A page similar to the following figure displays.



b. Select the Port **1/0/28** check box.

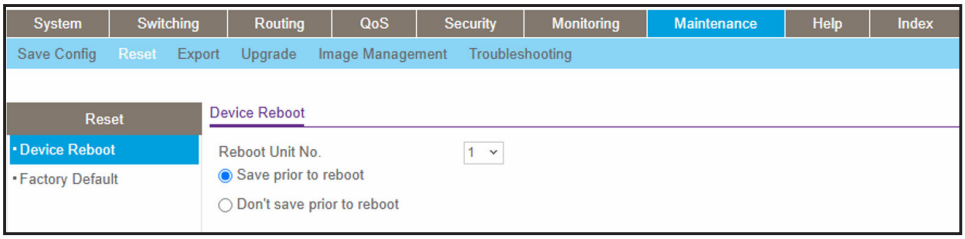
c. In the **Configured Stack Mode** menu, select **Stack**.

d. Click the **Apply** button. Your settings are saved.

4. Reboot the switch.

a. Select **Maintenance > Reset > Device Reboot**.

A page similar to the following figure displays.



b. In the **Reboot Unit No.** menu, select **1**.

c. Select the **Save prior to reboot** radio button.

d. Click the **Apply** button. Your settings are saved, and the switch reboots.

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 management switch, 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 stack management switch, 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 stack management 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 stack management 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 stack management 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 stack management 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 management switch.
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 stack management switch.

   This saved configuration is automatically propagated to all members of the stack.

Manually copy the firmware of the stack management switch to a stack member

This example is provided as CLI commands and a main UI procedure.

CLI: Copy the firmware of the stack management switch to a stack member

To use the CLI to copy the firmware of the stack management switch to a stack member with member number 2:

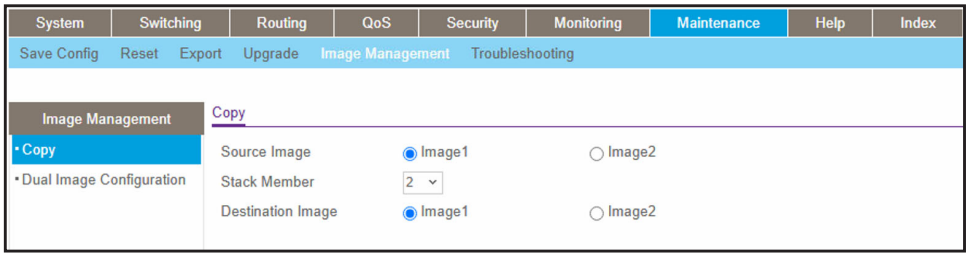
```
(Netgear Switch) #copy image1 unit 2 image1
```

Main UI: Copy the firmware of the stack management switch to a stack member

To use the main UI to copy the firmware of the stack management switch to a stack member with member number 2:

1. Select **Maintenance > Image Management > Copy**.

   A page similar to the following figure displays.



2. Select the radio button for a source image.
3. In the **Stack Member** menu, select **2**.
4. Select the radio button for a destination image.
5. Click the **Apply** button. Your settings are saved.

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. If you installed a redundant link between the switches (as we recommend), 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 management switch, and you cannot specify which switch becomes the new stack management switch. All stack members assume the configuration that is based on the new stack management switch. 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. Make a connection to the console port on the stack management switch so that you can verify that the new switch joins the stack by issuing the **`show switch`** command. The new switch joins as a member (not as a stack management switch; the existing stack management switch 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 473.).

Remove a switch from a stack

To remove a switch from a stack:

1. If you installed a redundant link between the switches (as we recommend), 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. If you installed a redundant link between the switches (as we recommend), 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 issuing 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.

Make a connection to the console port on the stack management switch so that you can verify that the new switch joins the stack by issuing the **show switch** command. The new switch joins as a member (not as a stack management switch; the existing stack management switch 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 473).

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 management switch becomes unavailable, the stack member that assumes the role of stack management switch 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 4. Stack management switch scenarios

Scenario	Action	Result
Stack management switch election specifically determined by the existing stack management switch. **Note:** We does not recommend this scenario.	Connect two powered-on switch stacks through the stack ports.	Only one of the two stack management switches can becomes the new stack management switch. No other stack member can become the stack management switch.
Stack management switch 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 management switch.
Stack management switch 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 management switch.

Table 4. Stack management switch 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 management switch is retained. The new switch is added to the switch stack.
Stack management switch failure.	Remove (or power off) the stack management switch.	One of the remaining stack members becomes the new stack management switch. 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 display 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 5. 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

Note: When you issue a CLI command such as **`move management`** or **`renumber`**, we recommend 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, we recommend 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>`** CLI 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 prevent this situation, we recommend that you power down all switches except the stack management switch, and then add them back one at a time (see Add switches to an operating stack on page 475).

This example is provided as CLI commands and a main UI procedure.

CLI: Renumber stack members

To use the CLI to renumber stack members:

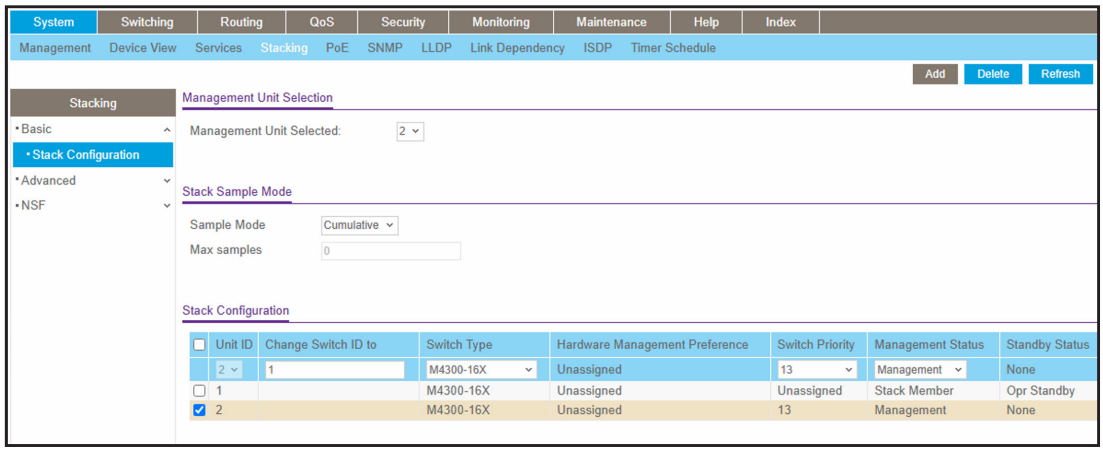
```
(Netgear Switch) (Config)#switch 3 renumber 2
All the switches in the stack will be reset to perform Manager unit renumbering and
the configuration of Manager switch interfaces will be cleared.
Are you sure you want to renumber? (y/n) y
```

Main UI: renumber stack members

To use the main UI to renumber stack members:

1. Renumber the stacking member's ID from 2 to 1.
   a. Select **System > Stacking > Basic > Stack Configuration**.

      A page similar to the following figure displays.



   b. In the Stack Configuration section, select the **1** check box.
   c. In the **Change Switch ID to** field, enter **1**.
   d. Click the **Apply** button. Your settings are saved.

Make a different unit the stack management switch

In the following example, the stack management switch is unit 2 and you are changing the management switch to unit 1.

This example is provided as CLI commands and a main UI procedure.

CLI: Make a different unit the stack management switch

To use the CLI to make a different unit the stack management switch:

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 stack management switch.
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 management switch to a different unit number, issue the following CLI command:

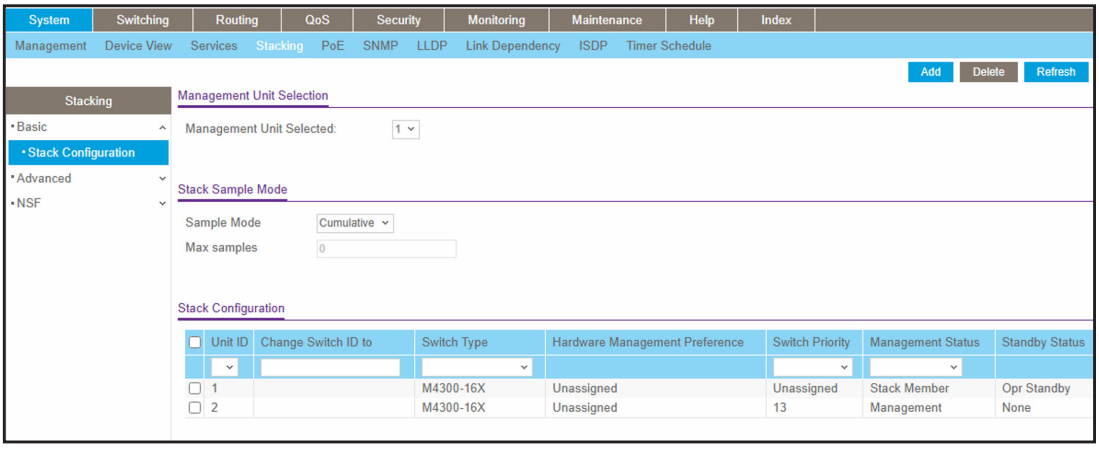
```
(Netgear Switch) (Config)#stack
(Netgear Switch) (Config-stack)#movemanagement 2 1
```

Main UI: Make a different unit the stack management switch

To use the main UI to make a different unit the stack management switch

1. Select **System > Management > Basic > Stack Configuration**.

   A page similar to the following figure displays.



2. In the **Management Unit Selected** menu, select **1**. A warning window displays.
3. Click the **OK** button.
4. Click the **Apply** button. Your settings are saved.

Note: If the stack management switch receives its IP address from a DHCP server and you move the stack management switch to a different unit, its IP address might change and you could lose the connection to the switch.

23

SNMP and sFlow

Simple Network Management Protocol and sampled Flow

This feature is supported on the M4250 series switches

This feature is supported on the M4300 series switches

This feature is supported on the M4350 series switches

This chapter includes the following sections:

- Add a new SNMP community
- Enable an SNMP trap
- SNMPv3 users
- sFlow
- Time-based sampling of counters with sFlow

Add a new SNMP community

The example is shown as CLI commands and as a main UI procedure.

CLI: Add a new SNMP community

To use the CLI to add a new SNMP community:

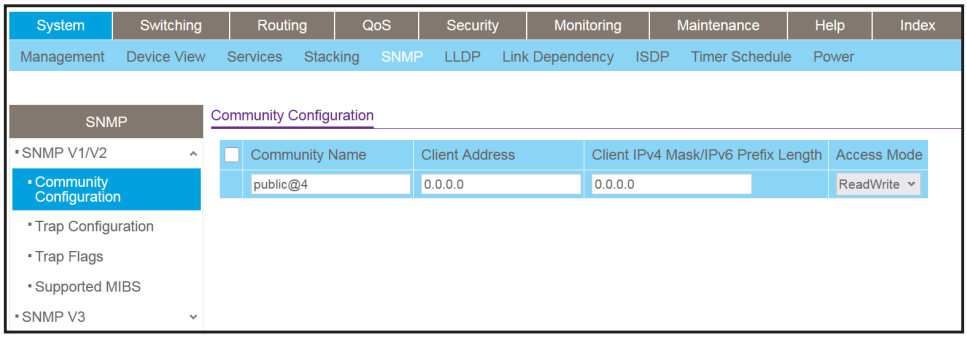
```
(Netgear switch) #config
(Netgear switch) (Config)#snmp-server community rw public@4
```

Main UI: Add a new SNMP community

To use the main UI to add a new SNMP community:

1. Select **System > SNMP > SNMP V1/V2 > Community Configuration**.

   A page similar to the following figure displays.



2. Configure the following settings:
   a. In the **Community Name** field, enter **public@4**.
   b. In the **Client Address** field, enter **0.0.0.0**.
   c. In the **Client IP Mask** field, enter **0.0.0.0**.
   d. In the **Access Mode** menu, select **Read/Write**.
3. Click the **Add** button. Your settings are saved.

Enable an SNMP trap

The example is shown as CLI commands and as a main UI procedure.

CLI: Enable an SNMP trap

To use the CLI to send an SNMP trap to the SNMP server:

1. Enable the switch to send a trap to an SNMP server with IP address 10.100.5.17.

```
(Netgear switch) #config
(Netgear switch) (Config)# snmptrap public 10.100.5.17
```

2. Enable the switch to send the link status to the SNMP server.

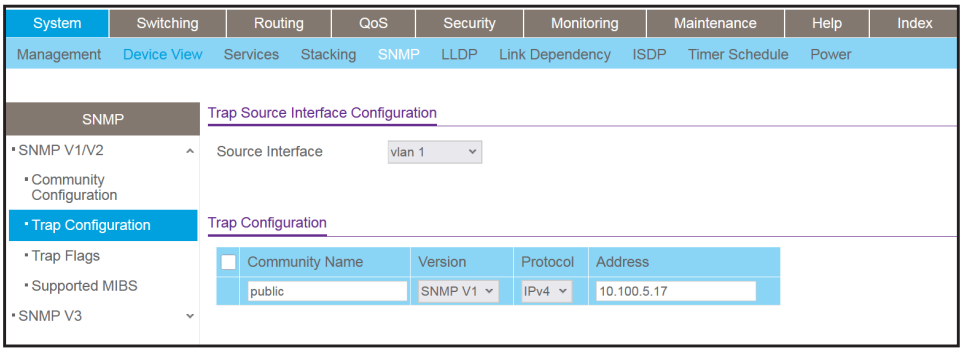
```
(Netgear switch) (Config)#snmp-server traps linkmode
```

Main UI: Enable an SNMP trap

To use the main UI to send an SNMP trap to the SNMP server:

1. Enable a trap for the SNMP server with UIP address 10.100.5.17.
   a. Select **System > SNMP > SNMP V1/V2 > Trap Configuration**.

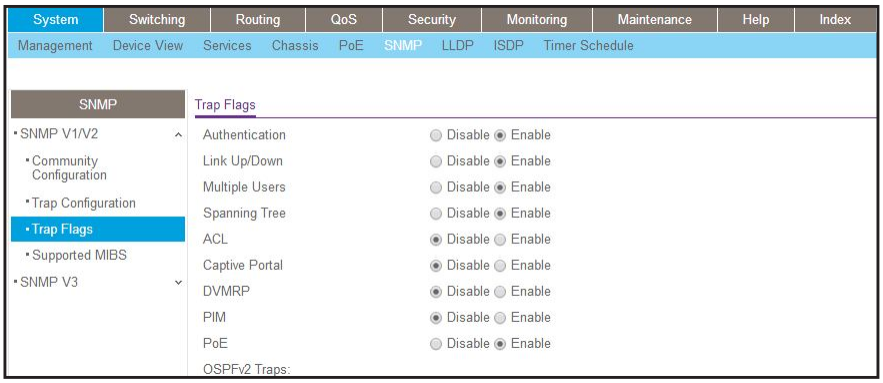
      A page similar to the following figure displays.



   b. In the **Community Name** field, enter **public**.
   c. In the **Version** menu, select **SNMPv1**.
   d. In the **Protocol** menu, select **IPv4**.
   e. In the **Address** field, enter **10.100.5.17**.
   f. Click the **Add** button. Your settings are saved.

2. Set the Link Up/Down flag.
   a. Select **System > SNMP > SNMP V1/V2 > Trap Flags**.

      A page similar to the following figure displays.



   b. Select the Link Up/Down **Enable** radio button.
   c. Click the **Apply** button. Your settings are saved.

SNMPv3 users

The example is shown as CLI commands and as a main UI procedure.

CLI: Add an SNMPv3 user

To use the CLI to configure the admin user as an SNMPv3 user with SHA512 key authentication and AES128 key encryption:

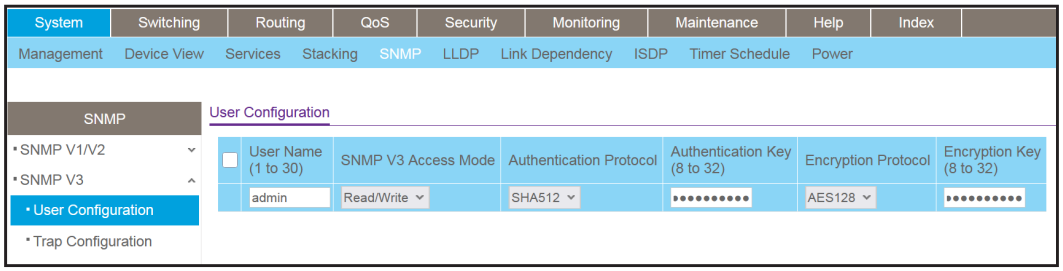
```
(Netgear Switch)(Config)#
(Netgear Switch)(Config)#snmp-server user admin testgroup auth-sha512-key
1234567890 priv-aes-key 1234567890
```

Main UI: Add an SNMPv3 user

To use the main UI to configure the admin user as an SNMPv3 user with SHA512 authentication and AES128 encryption:

1. Select **System > SNMP > SNMPv3 > User Configuration**.

   A page similar to the following figure displays.



2. Configure the following settings:
   a. In the **User Name** field, enter **admin**.
   b. In the **SNMP V3 Access Mode** menu, select **Read/Write**.
   c. In the **Authentication Protocol** menu, select **SHA512**, which is the only option.
   d. In the **Authentication Key** field, enter **1234567890** as the authentication password (key).
   e. In the **Encryption Protocol** menu, select **AES128**, which is the only option.
   f. In the **Encryption Key** field, enter **1234567890** as the encryption password (key).
3. Click the **Apply** button. Your settings are saved.

sFlow

Sampled flow (sFlow) is the standard for monitoring high-speed switched and routed networks. sFlow technology is built into network equipment and gives visibility into network activity, enabling 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.

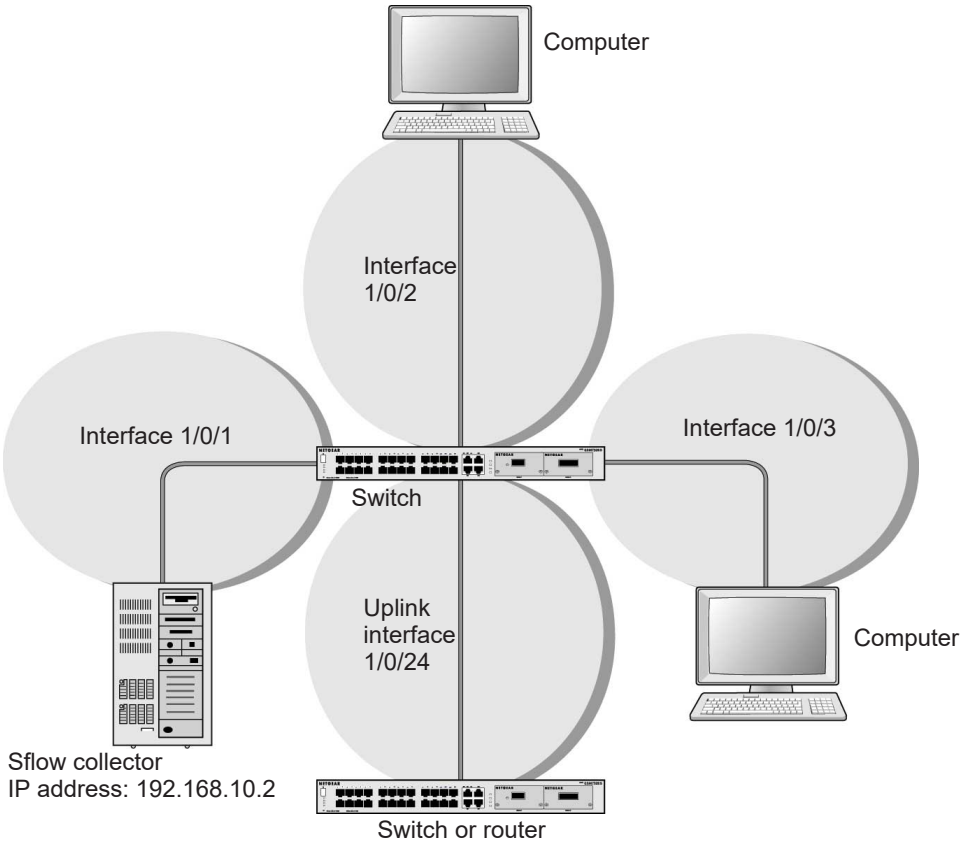


Figure 51. sFlow in a network

CLI: Configure statistical packet-based sampling of packet flows with sFlow

To use the CLI to configure statistical packet-based sampling of packet flows with sFlow:

1. Configure the IP address of the sFlow receiver (sFlow collector).

   In this example, sFlow samples are 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 time-out value.

   In this example, sFlow samples are sent to the receiver for the duration of 31536000 seconds (approximately 1 year).

```
(Netgear Switch) (Config)# sflow receiver 1 owner NetMonitor timeout 31536000
```

3. Display the sFlow configuration.

   In this example, the default maximum datagram size is 1400. You can modify the size 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 must repeat the commands in this step for all the ports that must 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. Display the sampling port configuration.

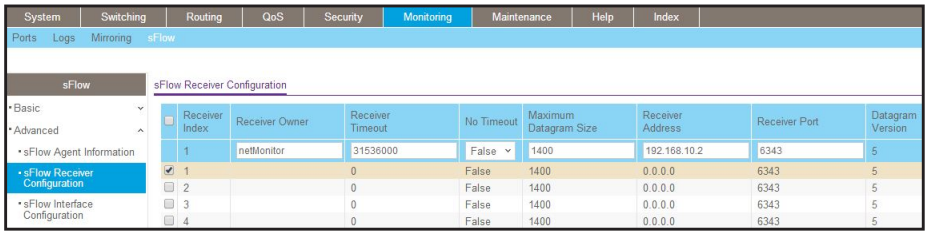
```
(Netgear Switch)) #show sflow samplers
Sampler            Receiver                Packet         Max Header
Data Source        Index                 Sampling Rate       Size
-----------       ---------------     -----------------  ------------------
1/0/1                    1               1024                 64
```

Main UI: Configure statistical packet-based sampling with sFlow

To use the main UI to configure statistical packet-based sampling of packet flows with sFlow:

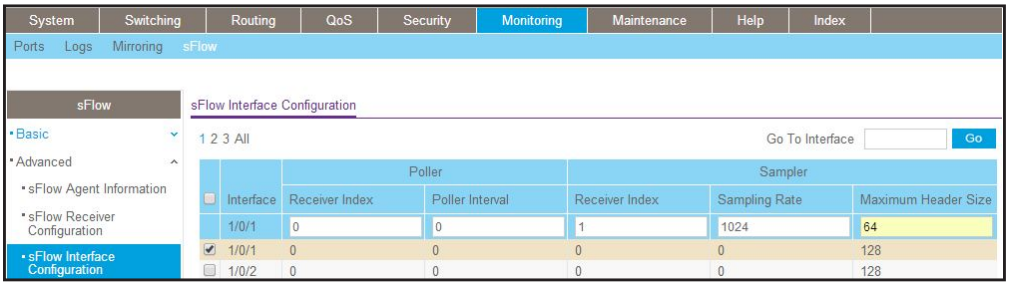
1. Configure the IP address of the sFlow receiver.
   a. Select **Monitoring > sFlow > Advanced > sFlow Receiver Configuration**.

   A page similar to the following figure displays.



   b. Select the Receiver Index **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**.
   f. Click the **Apply** button. Your settings are saved.
2. Configure the sampling ports sFlow receiver index, sampling rate, and sampling maximum header size.
   a. Select **Monitoring > sFlow > Advanced > sFlow Interface Configuration**.

   A page similar to the following figure 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 the **Apply** button. Your settings are saved.

Time-based sampling of counters with sFlow

The example is shown as CLI commands and as a main UI procedure.

CLI: Configure time-based sampling of counters with sFlow

To use the CLI to configure sampling port sFlow receiver index and polling interval:

1. Configure the sampling port sFlow receiver index, and polling interval. You must repeat the commands in this step for all the ports that must 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. Display the polling port configuration.

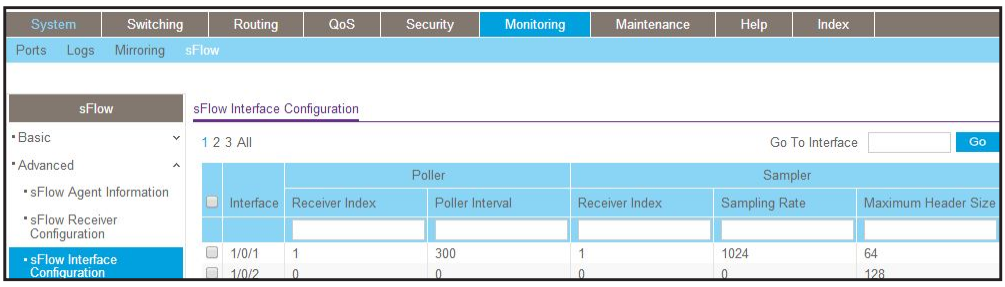
```
(Netgear Switch) #show sflow pollers
Poller             Receiver            Poller
Data Source        Index               Interval
-----------        ---------           ---------
1/0/1              1                   300
```

Main UI: Configure time-based sampling of counters with sFlow

To use the main UI to configure sampling port sFlow receiver index and polling interval:

1. Select **Monitoring > sFlow > Advanced > sFlow Interface Configuration**.

   A page similar to the following figure displays.



2. Select the Interface **1/0/1** check box.
3. In the **Poller Interval** field, enter **300**.
4. In the **Receiver Index** field, enter **1**.
5. Click the **Apply** button. Your settings are saved.

24

DNS

Domain Name System

This feature is supported on the M4250 series switches

This feature is supported on the M4300 series switches

This feature is supported on the M4350 series switches

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, which allows a static host name entry to be used to resolve the IP address. The following sections provide 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 main UI procedure.

CLI: Specify two DNS servers and ping a DNS name

To use the CLI to configure two DNS servers, enable domain lookup, and ping a DNS name:

1. Configure two DNS servers and enable domain lookup.

```
(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
```

2. Ping a DNS name.

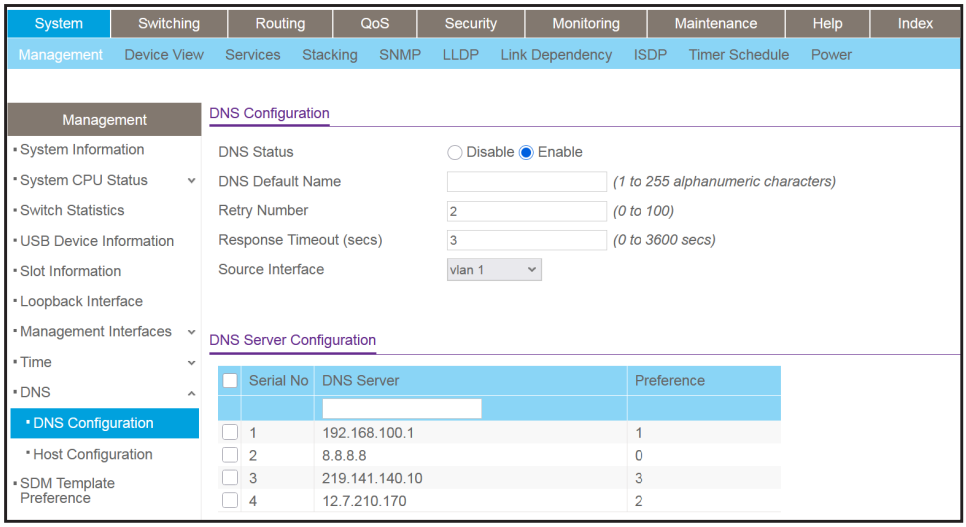
```
(Netgear Switch)#ping www.netgear.com

Send count=3, Receive count=3 from 206.82.202.46
```

Main UI: Specify two DNS servers and ping a DNS name

To use the main UI to configure two DNS servers and ping a DNS name:

1. Select **System > Management > DNS > DNS Configuration**.

   A page similar to the following figure displays.

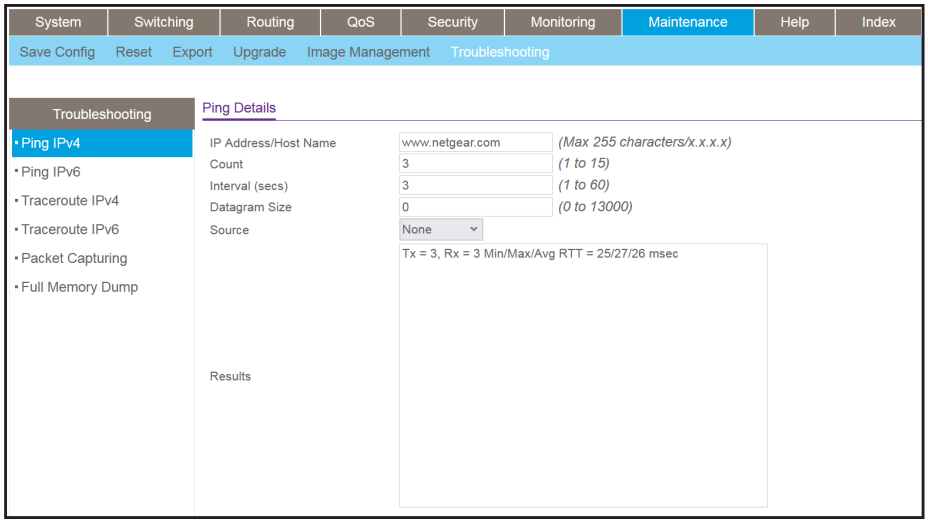


2. Configure the following settings:
   a. In the **DNS Server** field, enter **12.7.210.170**.
   b. Click the **Add** button. Your settings are saved.
   c. In the **DNS Server** field, enter **219.141.140.10**.
   d. Click the **Add** button. Your settings are saved.

   Both DNS servers now display in the DNS Server Configuration table.

3. Select **Maintenance > Troubleshooting > Ping IPv4**.

   The Ping Details page displays.



4. In the **IP Address/Host Name** field, enter **www.netgear.com**.
5. Click the **Apply** button. The ping results display in the Results field.

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 main UI procedure.

CLI: Manually add a host name and an IP address and ping a DNS name

To use the CLI to add a host name and an IP address and ping an IP address:

1. 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
```

2. Ping a DNS name.

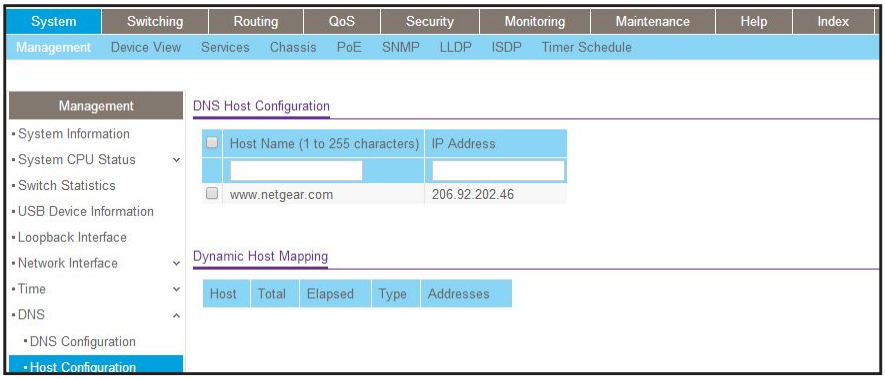
```
(Netgear Switch) (Config)#ping www.netgear.com

Send count=3, Receive count=3 from 206.82.202.46
```

Main UI: Manually add a host name and an IP address and ping a DNS name

To use the main UI to add a host name and an IP address and ping an IP address:

1. Select **System > Management > DNS > Host Configuration**.

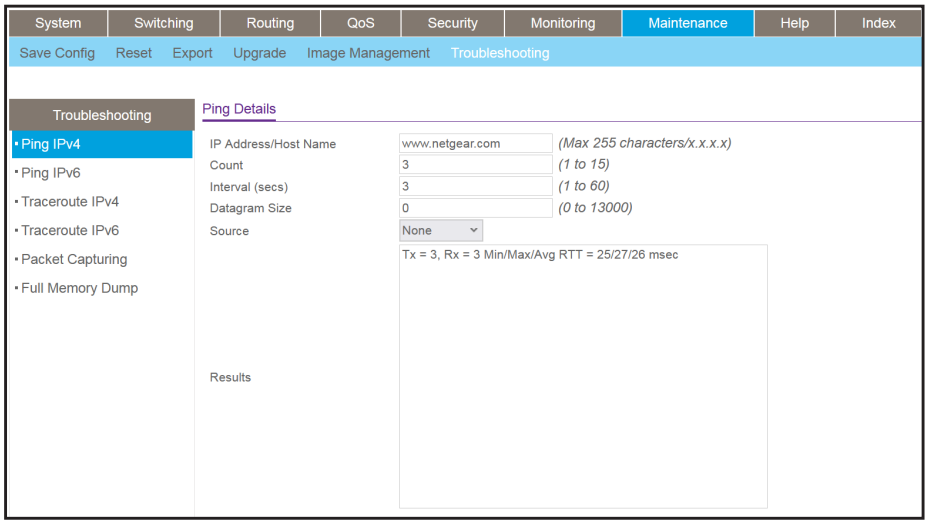
   A page similar to the following figure displays.



2. Configure the following settings:
   - In the **Host Name** field, enter **www.netgear.com**.
   - In the **IP Address** field, enter **206.82.202.46**.
3. Click the **Add** button. Your settings are saved.

   The host name and IP address display in the DNS Host Configuration table.
4. Select **Maintenance > Troubleshooting > Ping IPv4**.

   The Ping Details page displays.



5. In the **IP Address/Host Name** field, enter **www.netgear.com**.
6. Click the **Apply** button. The ping results display in the Results field.

25

DHCP Server

Dynamic Host Configuration Protocol Server

This feature is supported on the M4250 series switches

This feature is supported on the M4300 series switches

This feature is supported on the M4350 series switches

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 and the client's IP or IP VLAN interface over which the DHCP server can be reached must belong to the same subnet.

A DHCP server allows the switch to dynamically assign an IP address to a DHCP client that is connected to the switch. A DHCP server also enables the IP address to be assigned based on a 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 main UI procedure.

CLI: Configure a DHCP server in dynamic mode

To use the CLI to configure a routing VLAN and a DHCP server in dynamic mode:

1. **Configure a routing VLAN.**

```
(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
```

2. **Configure a DHCP server in dynamic mode.**

```
(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
```

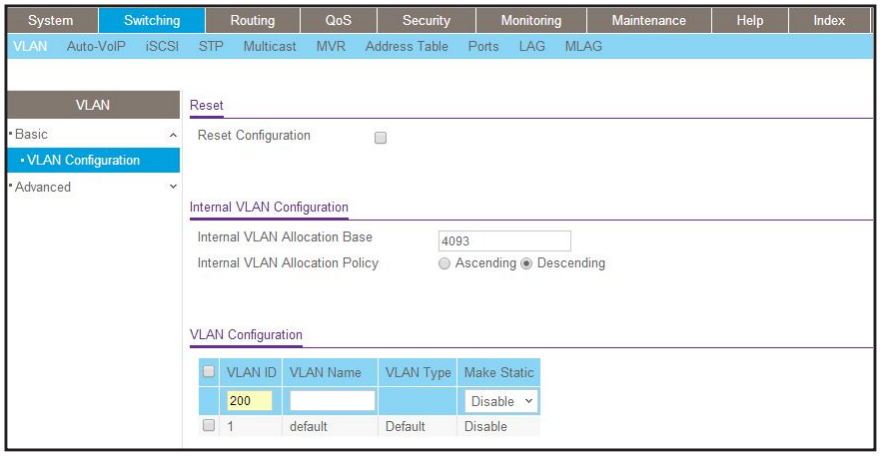
Note: If no DHCP L3 relay exists between the client device and the DHCP server, an active route must exist for which the subnet is the same as the subnet for the DHCP dynamic pool.

Main UI: Configure a DHCP server in dynamic mode

To use the main UI to configure a routing VLAN and a DHCP server in dynamic mode:

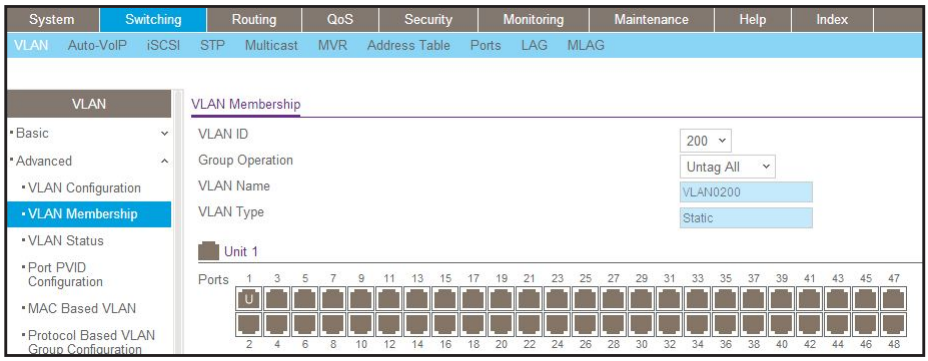
1. Create VLAN 200.
   a. Select **Switching > VLAN > Basic > VLAN Configuration**.

      A page similar to the following figure displays.



   b. Under VLAN Configuration, in the **VLAN ID** field, enter **200**.
   c. Click the **Add** button. Your settings are saved.
2. Add port 1/0/1 to VLAN 200.
   a. Select **Switching > VLAN > Advanced > VLAN Membership**.

A page similar to the following figure displays.



b. In the **VLAN ID** menu, select **200**.

c. Click the gray box under port **1** until U displays, which specifies that the egress packets are untagged for the port.

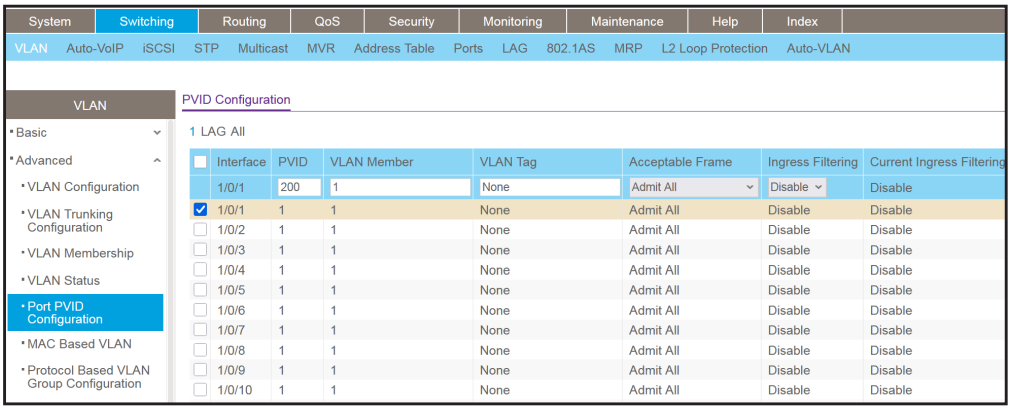
If your switch is a member of a stack, be sure that you select the port in the correct unit.

d. Click the **Apply** button. Your settings are saved.

3. Assign a PVID to VLAN 200.

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

A page similar to the following figure displays.



b. Select the Interface **1/0/1** check box.

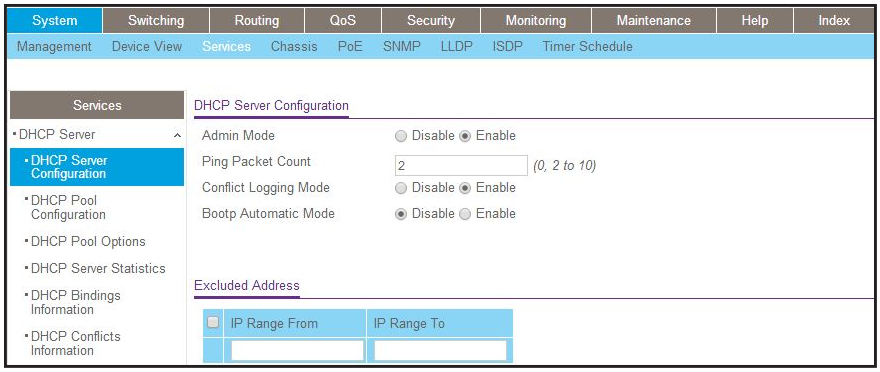
c. In the **PVID** field, enter **200**.

d. Click the **Apply** button. Your settings are saved.

4. Create a new DHCP pool.

a. Select **System > Services > DHCP Server > DHCP Server Configuration**.

A page similar to the following figure displays.



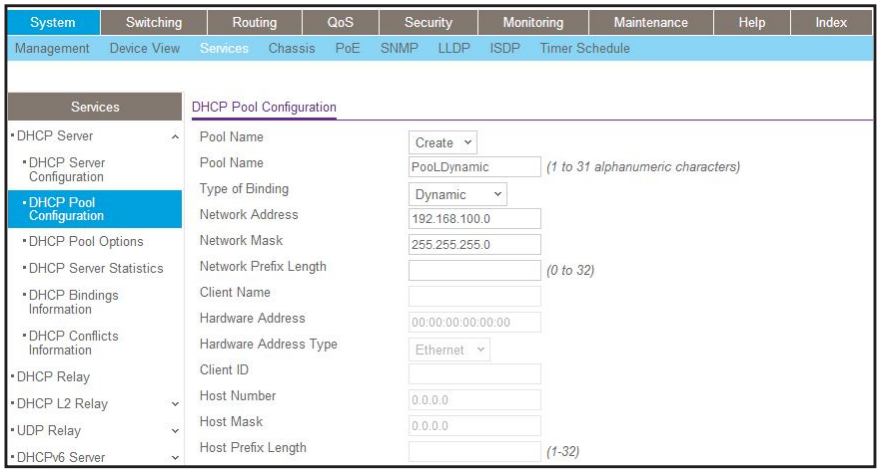
b. Select the Admin Mode **Enable** radio button.

c. Click the **Apply** button. Your settings are saved

5. Configure a DHCP pool.

a. Select **System > Services > DHCP Server > DHCP Pool Configuration**.

A page similar to the following figure displays.



b. Configure the following settings:

- In the **Pool Name** menu, select **Create**.
- In the **Pool Name** field, enter **PooLDynamic**.
- In the **Type of Binding** menu, select **Dynamic**.
- In the **Network Address** field, enter **192.168.100.0**.
- In the **Network Mask** field, enter **255.255.255.0**.

  You can also enter **24** in the **Network Prefix Length** field. However, do not specify information in both the Network Mask field and the Network Prefix Length field.

- In the **Days** field, enter **1**.

c. Click the **Add** button. Your settings are saved.

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 main UI procedure.

CLI: Configure a DHCP server that assigns a fixed IP address

To use the CLI to 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-dhcp-pool)#client-name dhcpclient
(Netgear Switch) (Config-dhcp-pool)#hardware-address 00:01:02:03:04:05
(Netgear Switch) (Config-dhcp-pool)#host 192.168.200.1 255.255.255.0
(Netgear Switch) (Config-dhcp-pool)#client-identifier 01:00:01:02:03:04:05
```

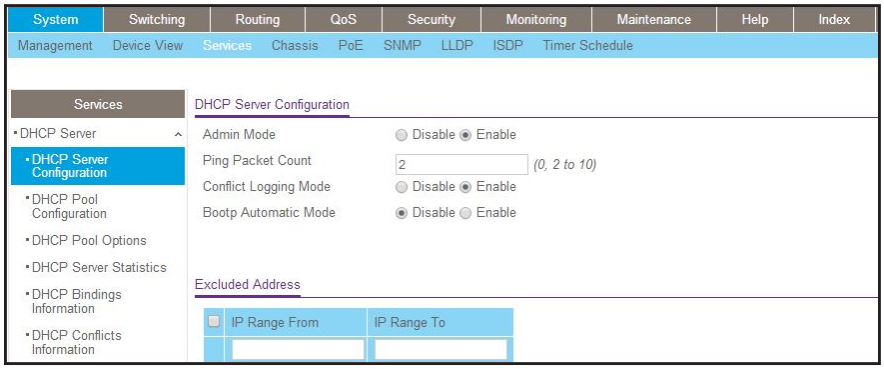
Note: The unique identifier is a concatenation of the media type and MAC addresses. For example, the Microsoft client identifier for Ethernet address c8:19:24:88:f1:77 is 01:c8:19:24:88:f1:77, where 01 represents the Ethernet media type. For more information, see the “Address Resolution Protocol Parameters” section of RFC 1700.

Main UI: Configure a DHCP server that assigns a fixed IP address

To use the main UI to configure a DHCP server that assigns a fixed IP address:

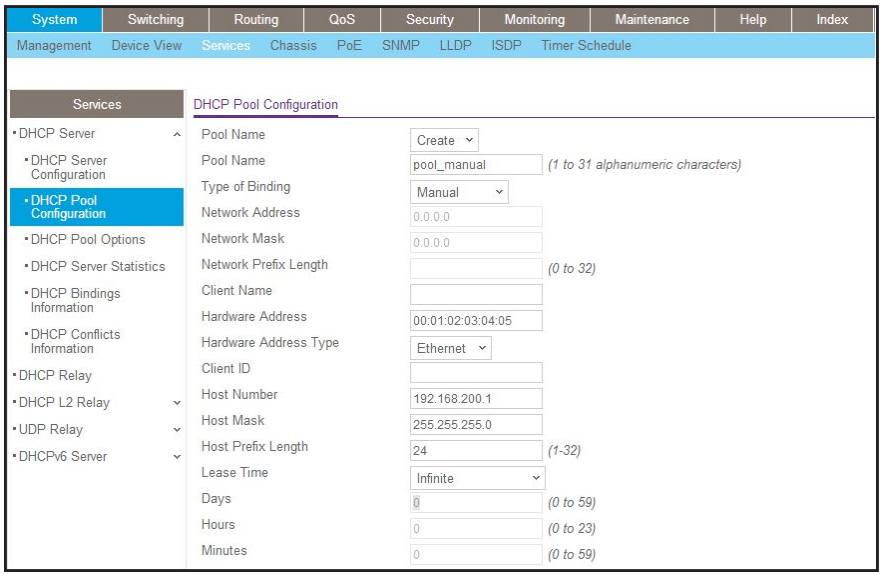
1. Select **System > Services > DHCP Server > DHCP Server Configuration**.

   A page similar to the following figure displays.



2. Select the Admin Mode **Enable** radio button.
3. Click the **Apply** button. Your settings are saved.
4. Select **System > Services > DHCP Server > DHCP Pool Configuration**.

   A page similar to the following figure displays.



5. Configure the following settings:
   - In the **Pool Name** menu, select **Create**.
   - In the **Pool Name** field, enter **pool_manual**.
   - In the **Type of Binding** menu, 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** menu, select **Ethernet**.
- In the **Host Number** field, enter **192.168.200.1**.
- In the **Network Mask** field, enter **255.255.255.0**.

  You can also enter **24** in the **Network Prefix Length** field. However, do not specify information in both the Network Mask field and the Network Prefix Length field.

- In the **Lease Time** menu, select **Infinite**.

6. Click the **Add** button. Your settings are saved.

26

DHCPv6 Server

Dynamic Host Configuration Protocol version 6 Server

This feature is supported on the M4250 series switches

This feature is supported on the M4300 series switches

This feature is supported on the M4350 series switches

This chapter includes the following sections:

- DHCPv6 concepts
- Configure DHCPv6 prefix delegation
- Configure a stateless DHCPv6 server
- Configure a stateful DHCPv6 server
- Set up a configuration with a DHCPv6 server and DHCPv6 relay

DHCPv6 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 the 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 example, a customer premise equipment (CPE) router requests prefix from a provider edge (PE) router. The PE router uses 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. Then, the CPE router assigns the 2001:1:1::/96 IPv6 address to one user's network and the 2001:1:2::/96 IPv6 address to another user's network.

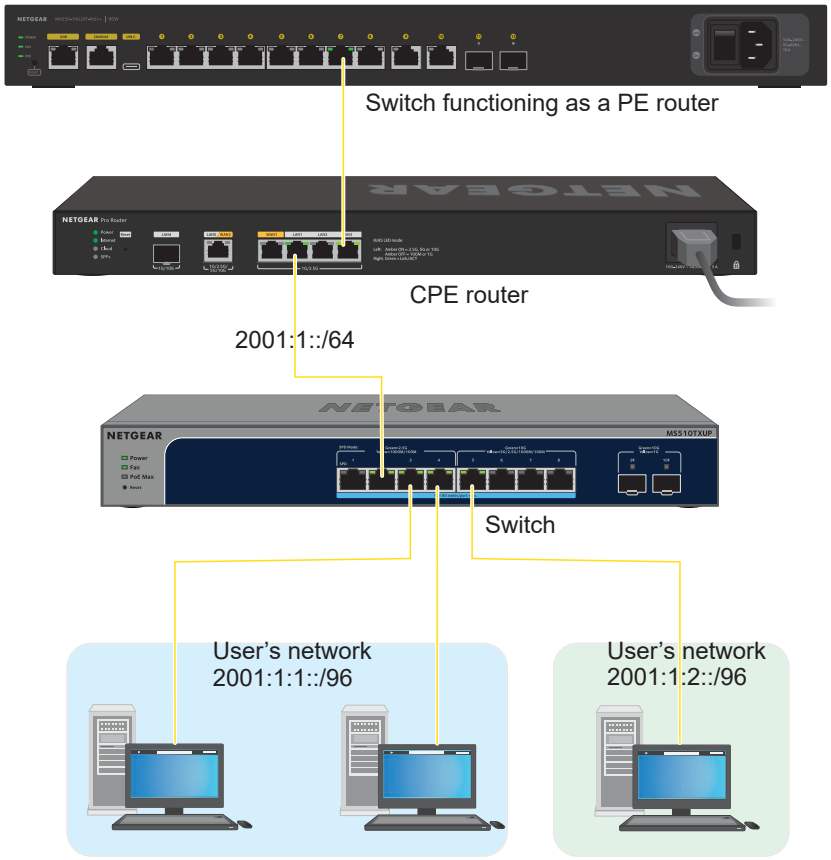


Figure 52. DHCPv6 stateful IPv6 address assignment

Configure DHCPv6 prefix delegation

The example is shown as CLI commands and as a main UI procedure.

CLI: Configure DHCPv6 prefix delegation

To use the CLI to configure DHCPv6 delegation and display the DHCPv6 binding:

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. Display the DHCPv6 binding.

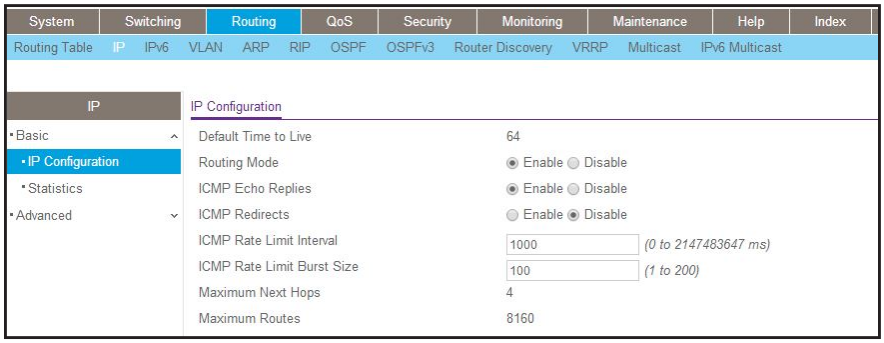
```
(NETGEAR SWITCH) #show ipv6 dhcp binding
Client Address................................ FE80::200:FF:FE4D:AAD0
Client Interface.............................. 1/0/9
Client DUID.....................................
00:01:00:01:15:40:14:4f:00:00:00:4d:aa:d0
Identity Association ID....................... 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
```

Main UI: Configure DHCPv6 prefix delegation

To use the main UI to configure DHCPv6 delegation and display the DHCPv6 binding:

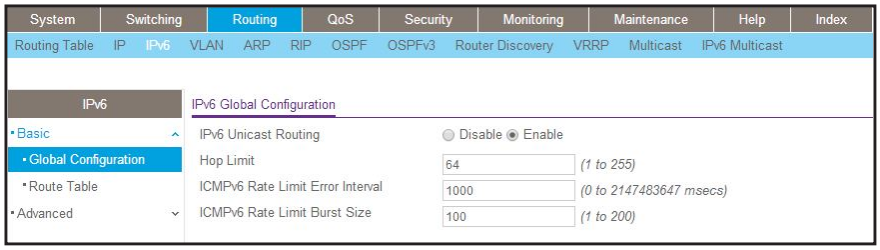
1. Enable IP routing globally.
   a. Select **Routing > IP > Basic > IP Configuration**.

      A page similar to the following figure displays.



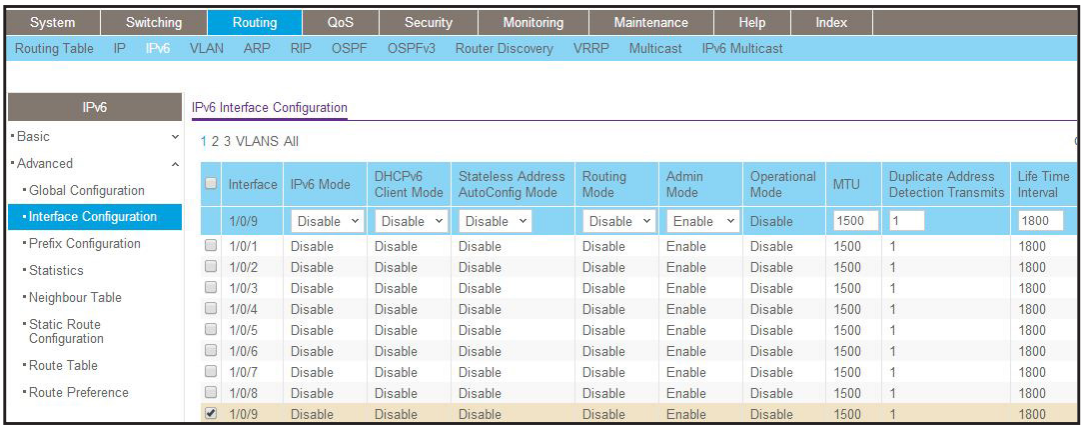
   b. Select the Routing Mode **Enable** radio button.
   c. Click the **Apply** button. Your settings are saved.
2. Enable IPv6 unicast globally.
   a. Select **Routing > IPv6 > Basic > Global Configuration**.

      A page similar to the following figure displays.



   b. Select the IPv6 Unicast Routing **Enable** radio button.
   c. Click the **Apply** button. Your settings are saved.
3. Enable IPv6 address on interface 1/0/9.
   a. Select **Routing > IPv6 > Advanced > Interface Configuration**.

A page similar to the following figure displays.



b. Select the Interface **1/0/9** check box.

c. Configure the following settings:

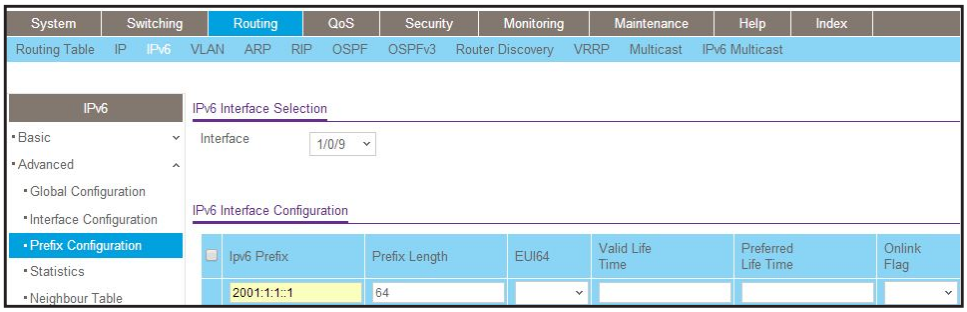
- In the **IPv6 Mode** menu, select **Enable**.
- In the **Routing Mode** menu, select **Enable**.

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

4. Configure the prefix on interface 1/0/9.

a. Select **Routing > IPv6 > Advanced > Prefix Configuration**.

A page similar to the following figure displays.



b. In the **Interface** menu, select **1/0/9**.

c. In the **IPv6 Prefix** field, enter **2001:1::1**.

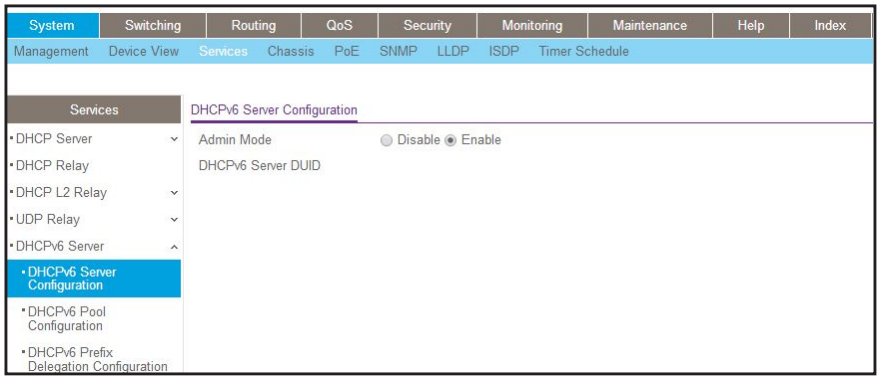
d. In the **Prefix Length** field, enter **64**.

e. Click the **Add** button. Your settings are saved.

5. Enable the DHCPv6 server configuration.

a. Select **System > Services > DHCPv6 Server > DHCPv6 Server Configuration**.

A page similar to the following figure displays.



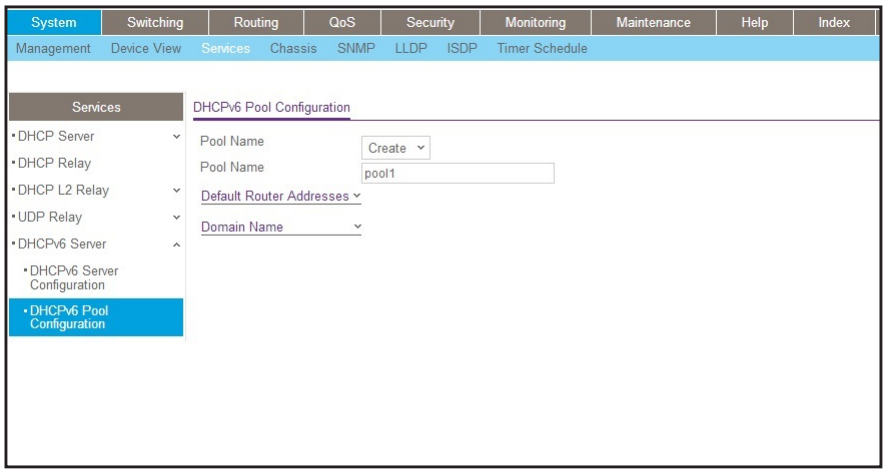
b. Select the Admin Mode **Enable** radio button.

c. Click the **Apply** button. Your settings are saved.

6. Create a DHCPv6 pool.

a. Select **System > Services > DHCPv6 Server > DHCPv6 Pool Configuration**.

A page similar to the following figure displays.



b. In the **Pool Name** menu, select **Create**.

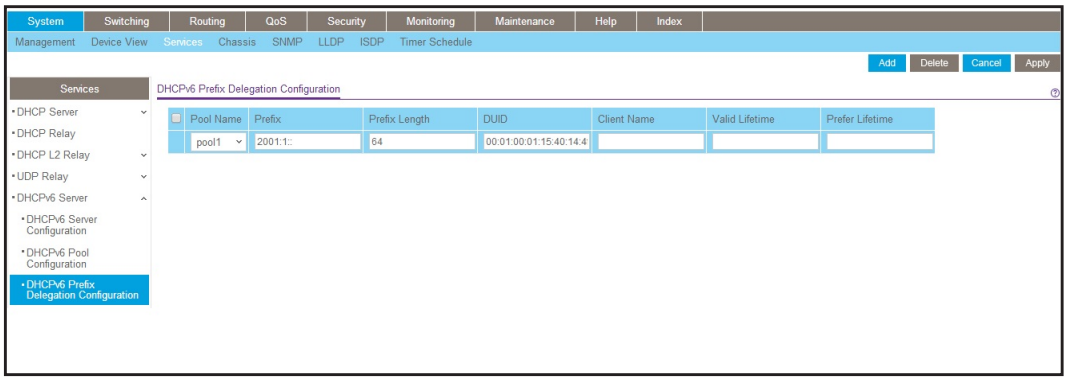
c. In the **Pool Name** field, enter **pool1**.

d. Click the **Apply** button. Your settings are saved.

7. Configure the prefix in the DHCPv6 pool.

a. Select **System > Services > DHCPv6 Server > DHCPv6 Prefix Delegation Configuration**.

A page similar to the following figure displays.



b. In the **Pool Name** menu, select **pool1**.

c. In the **Prefix** field, enter **2001:1::**.

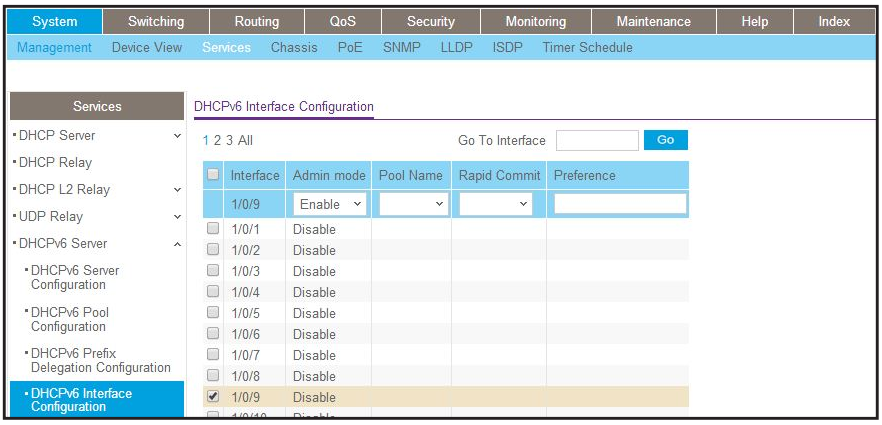
d. In the **Prefix Length** field, enter **64**.

e. Click the **Apply** button. Your settings are saved.

8. Configure DHCPv6 on interface 1/0/9.

a. Select **System > Services > DHCPv6 Server > DHCPv6 Interface Configuration**.

A page similar to the following figure displays.



b. Select the Interface **1/0/9** check box.

c. In the **Admin mode** menu, select **Enable**.

d. In the **Pool Name** menu, select **pool1**.

e. Click the **Apply** button. Your settings are saved.

9. Display the DHCPv6 binding information.

a. Select **System > Services > DHCPv6 Server > DHCPv6 Binding Information**.

The DHCPv6 Binding Information page displays.

Configure a stateless DHCPv6 server

This example shows 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. In the CLI, 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.

The example is shown as CLI commands and as a main UI procedure.

CLI: Configure a stateless DHCPv6 server

To use the CLI to 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 example, you must configure the **ipv6 nd other-config-flag** command on the interface, otherwise the host cannot update the DNS server.

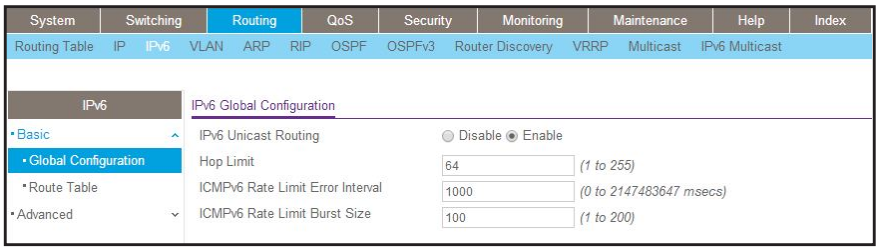
```
(Netgear Switch) (Config)#interface 2/0/21
(Netgear Switch) (Interface 2/0/21)#routing
(Netgear Switch) (Interface 2/0/21)#ipv6 address 2003:1000::1/64
(Netgear Switch) (Interface 2/0/21)#ipv6 enable
(Netgear Switch) (Interface 2/0/21)#ipv6 nd other-config-flag
(Netgear Switch) (Interface 2/0/21)#ipv6 dhcp server ipv6_server
(Netgear Switch) (Interface 2/0/21)#exit
```

Main UI: Configure a stateless DHCPv6 server

To use the main UI to configure a stateless DHCPv6 server:

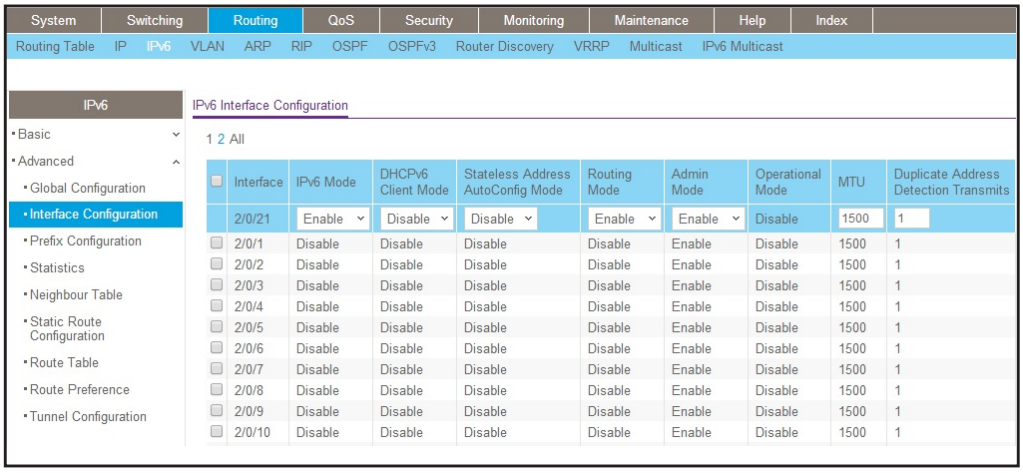
1. Enable IPv6 routing.
   a. Select **Routing > IPv6 > Basic > Global Configuration**.

      A page similar to the following figure displays.



   b. Select the IPv6 Unicast Routing **Enable** radio button.
   c. Click the **Apply** button. Your settings are saved.
2. Enable IPv6 routing on interface 2/0/21.
   a. Select **Routing > IPv6 > Advanced > Interface Configuration**.

      A page similar to the following figure displays.

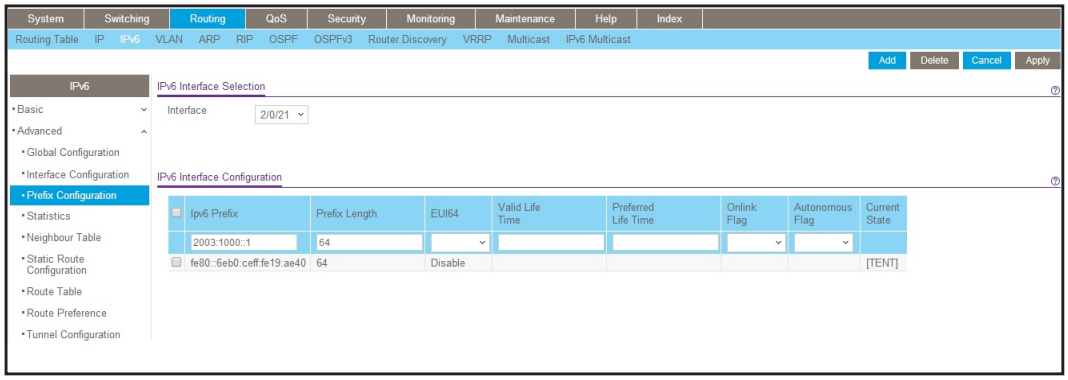


   b. Select the Interface **2/0/21** check box.
   c. In the **IPv6 Mode** menu, select **Enable**.
   d. In the **Routing Mode** menu, select **Enable**.
   e. In the **Adv Other Config Flag** menu, select **Enable**.

      This menu is not shown in the previous figure. To show the menu, scroll to the right on the page.

   f. Click the **Apply** button. Your settings are saved.
3. Configure an IPv6 address on interface 2/0/21.
   a. Select **Routing > IPv6 > Advanced > Prefix Configuration**.

A page similar to the following figure displays.



b. In the **Interface** menu, select **1/0/21**.

c. In the **IPv6 Prefix** field, enter **2003:1000::1**.

d. In the **Prefix Length** field, enter **64**.

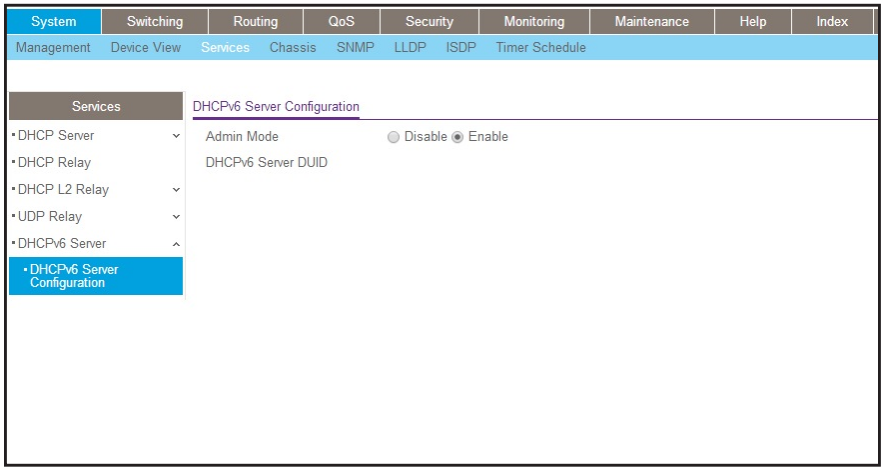
e. In the **EUI64** menu, select **Disable**.

f. Click the **Add** button. Your settings are saved.

4. Enable the DHCPv6 service.

a. Select **System > Services > DHCPv6 Server > DHCPv6 Server Configuration**.

A page similar to the following figure displays.



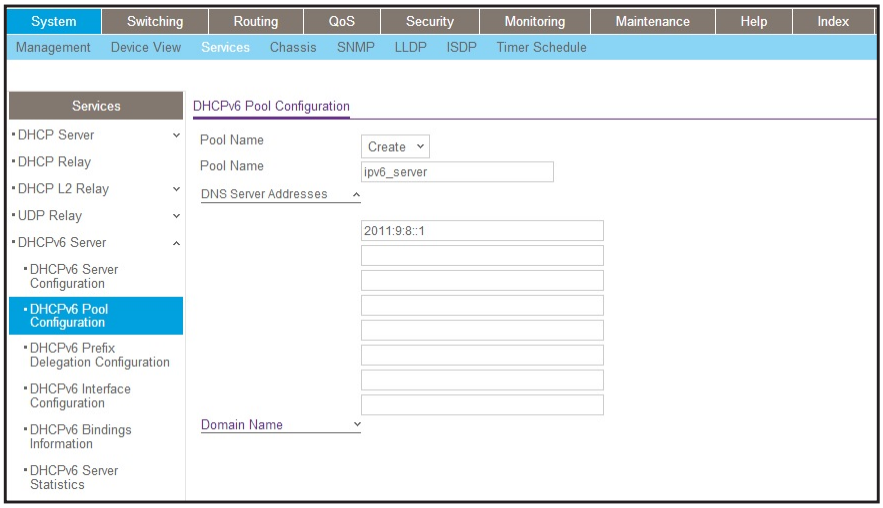
b. Select the Admin Mode **Enable** radio button.

c. Click the **Apply** button. Your settings are saved.

5. Create a DHCPv6 pool.

a. Select **System > Services > DHCPv6 Server > DHCPv6 Pool Configuration**.

A page similar to the following figure displays.



b. From the **Pool Name** menu, select **Create**.

c. In the **Pool Name** field, enter **ipv6_server**.

d. Click the **DNS Server Addresses** link, and enter **20011:9:18::1** in the first field.

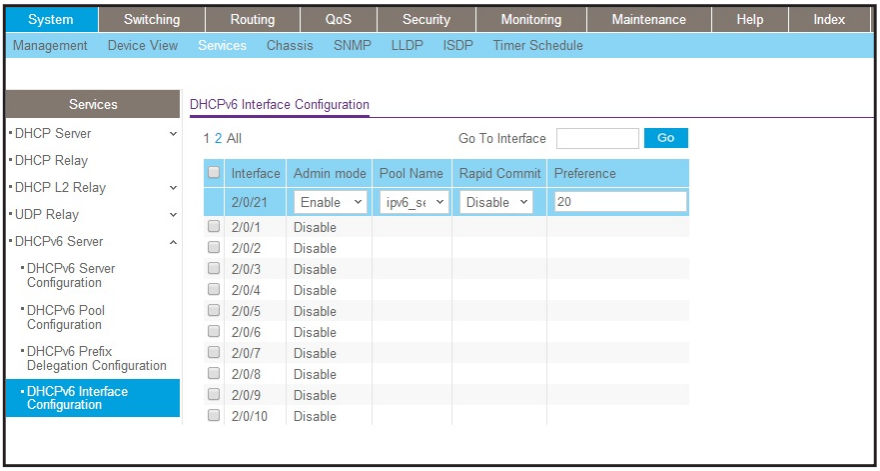
This is the IPv6 address of the DNS server.

e. Click the **Apply** button. Your settings are saved.

6. Enable DHCPv6 pool on interface 2/0/21.

a. Select **System > Services > DHCPv6 Server > DHCPv6 Interface Configuration**.

A page similar to the following figure displays.



b. Select the Interface **2/0/21** check box.

c. In the **Admin mode** menu, select **Enable**.

d. In the **Pool Name** menu, select **ipv6_server**.

e. Click the **Apply** button. Your settings are saved.

Configure a stateful DHCPv6 server

This example shows how you can use a DHCPv6 server to assign an IPv6 address directly to am IPv6 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.

The example is shown as CLI commands and as a main UI procedure.

CLI: Configure a stateful DHCPv6 server

To use the CLI to 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.

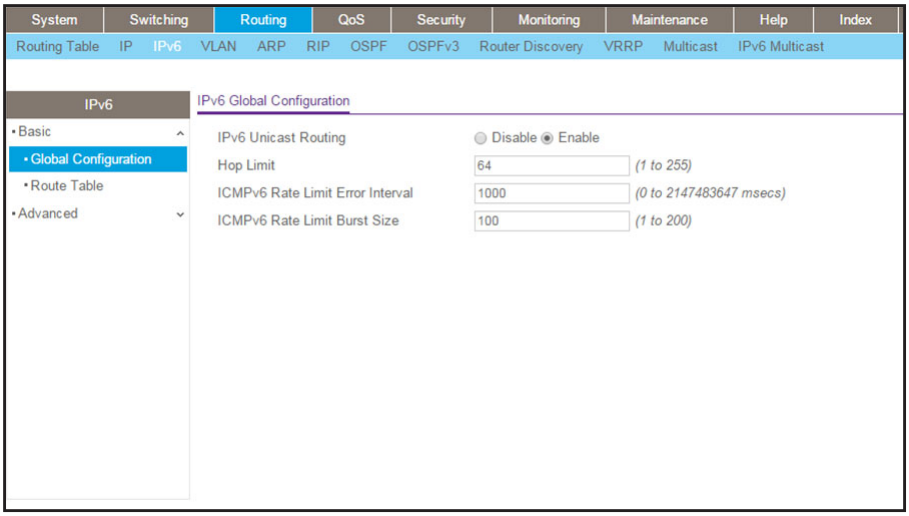
```
(Netgear Switch) (Config)#interface 1/0/1
(Netgear Switch) (Interface 1/0/1)#routing
(Netgear Switch) (Interface 1/0/1)#ipv6 address 2001:1:2::1/64
(Netgear Switch) (Interface 1/0/1)#ipv6 enable
(Netgear Switch) (Interface 1/0/1)#ipv6 dhcp server ipv6_server
(Netgear Switch) (Interface 1/0/1)#exit
```

Main UI: Configure a stateful DHCPv6 server

To use the main UI to configure a stateful DHCPv6 server:

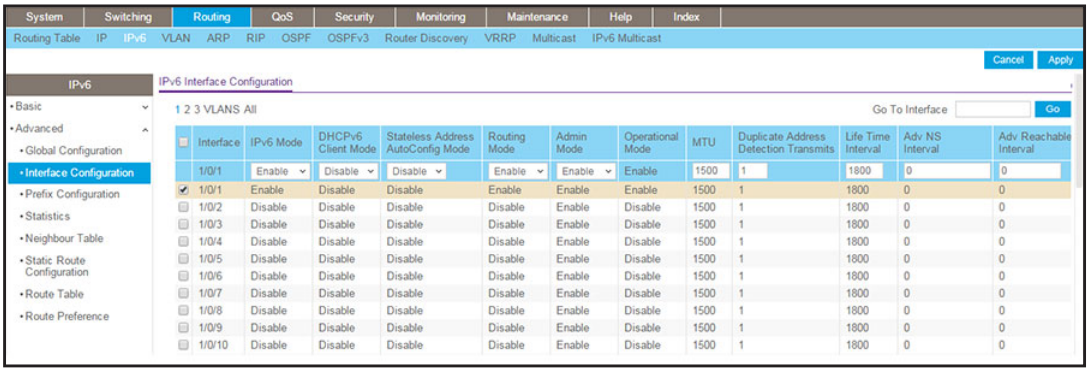
1. Enable IPv6 routing.
   a. Select **Routing > IPv6 > Basic > Global Configuration**.

      A page similar to the following figure displays.



   b. Select the IPv6 Unicast Routing **Enable** radio button.
   c. Click the **Apply** button. Your settings are saved.
2. Enable IPv6 routing on interface 1/0/1.
   a. Select **Routing > IPv6 > Advanced > Interface Configuration**.

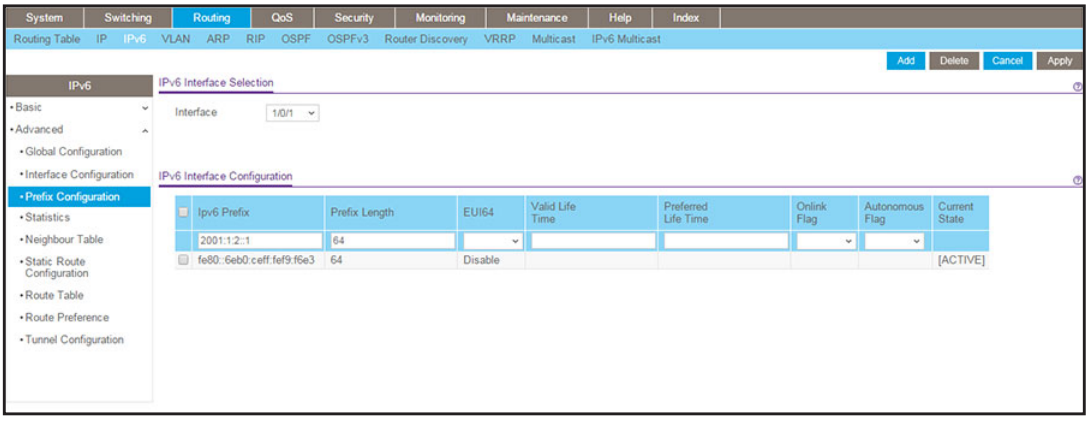
      A page similar to the following figure displays.



   b. Select the Interface **1/0/1** check box.
   c. In the **IPv6 Mode** menu, select **Enable**.
   d. In the **Routing Mode** menu, select **Enable**.
   e. Click the **Apply** button. Your settings are saved.

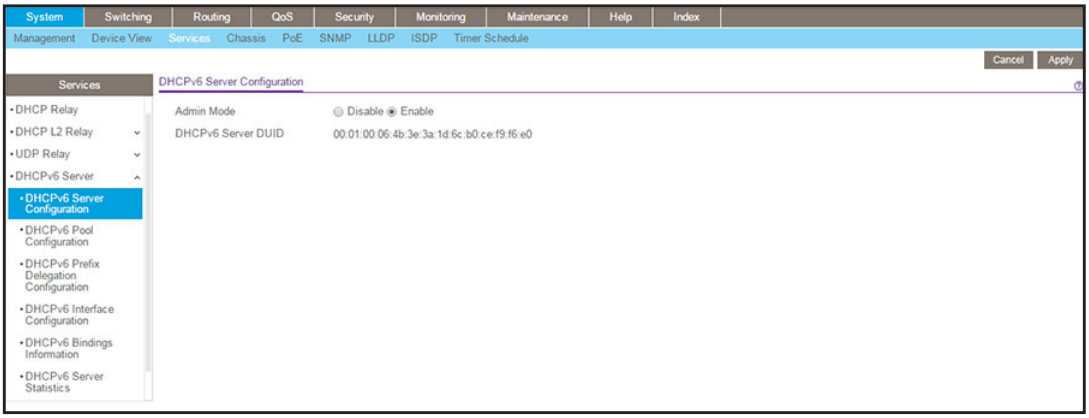
3. Configure the IPv6 address on interface 1/0/1.
   a. Select **Routing > IPv6 > Advanced > Prefix Configuration**.

      A page similar to the following figure displays.



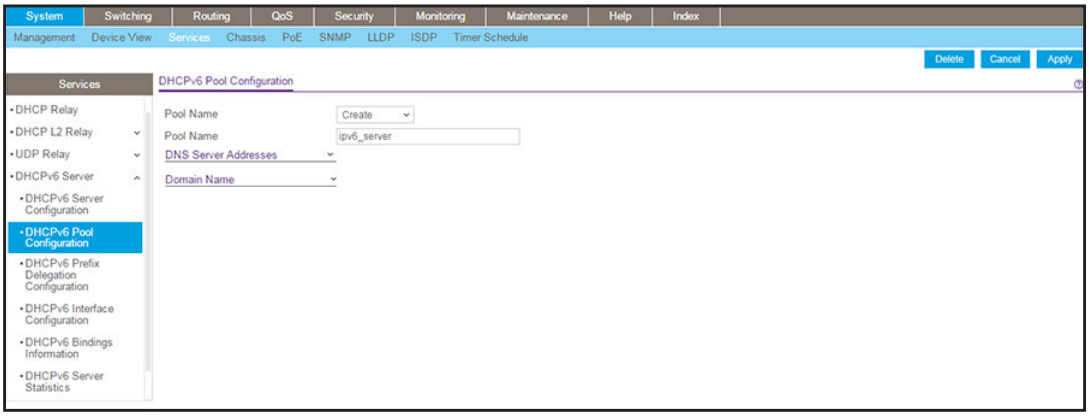
   b. In the **Interface** menu, select **1/0/1**.
   c. In the **IPv6 Prefix** field, enter **2001:1:2::1**.
   d. In the **Length** field, enter **64**.
   e. In the **EUI64** menu, select **Disable**.
   f. Click the **Add** button. Your settings are saved.
4. Enable the DHCPv6 service.
   a. Select **System > Services > DHCPv6 Server > DHCPv6 Server Configuration**.

      A page similar to the following figure displays.



   b. Select the Admin Mod **Enable** radio button.
   c. Click the **Apply** button. Your settings are saved.
5. Create the DHCPv6 pool.
   a. Select **System > Services > DHCPv6 Server > DHCPv6 Pool Configuration**.

A page similar to the following figure displays.



b. In the **Pool Name** menu, select **Create**.

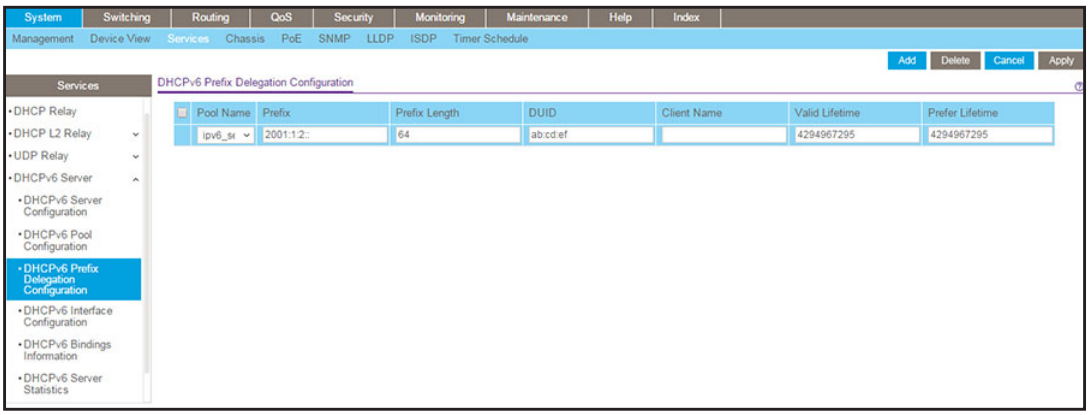
c. In the **Pool Name** field, enter **ipv6_server**.

d. Click the **Apply** button. Your settings are saved.

6. Configure the prefix for the DHCPv6 pool.

a. Select **System > Services > DHCPv6 Server > DHCPv6 Prefix Delegation Configuration**.

A page similar to the following figure displays.



b. In **Pool Name** menu, select **ipv6_server**.

c. In the **Prefix** field, enter **2001:1:2::**.

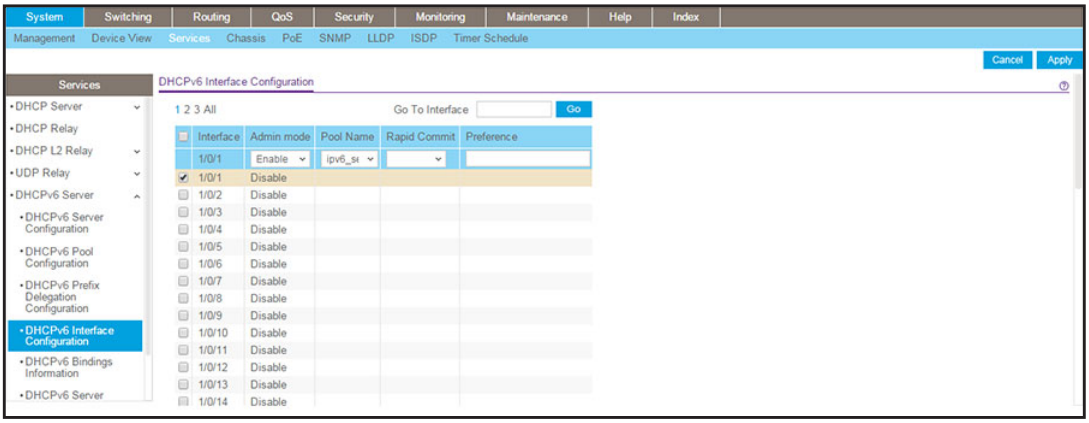
d. In the **Prefix Length** field, enter **64**.

e. Click the **Add** button. Your settings are saved.

7. Enable the DHCPv6 pool on interface 1/0/1.

a. **Select System > Services > DHCPv6 Server > DHCPv6 Interface Configuration**.

A page similar to the following figure displays.



b. Select the Interface **1/0/1** check box.

c. In the **Admin mode** menu, select **Enable**.

d. In the **Pool Name** menu, select **ipv6_server**.

e. Click the **Apply** button. Your settings are saved.

Set up a configuration with a DHCPv6 server and DHCPv6 relay

In the following figure, a switch functions as a DHCPv6 server and another switch functions as a DHCPv6 relay that is connected to a DHCPv6 client. Interface 1/0/6 on the DHCP server connect to interface 1/0/8 on the DHCPv6 relay. Interface 1/0/5 on the DHCPv6 relay connects to an interface on the DHCPv6 client.

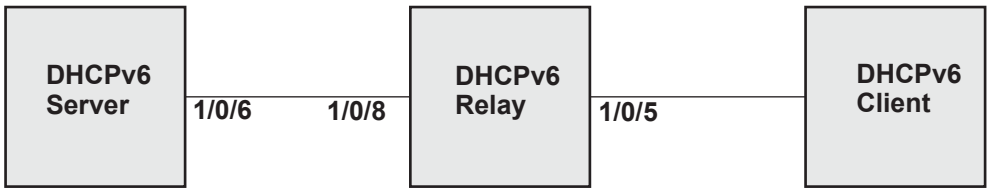


Figure 53. Configuration with a DHCPv6 server and DHCPv6 relay

The example is shown as CLI commands and as main UI procedures CLI and describes how to configure the DHCPv6 server and then how to configure the DHCPv6 relay.

CLI: Set up a configuration with a DHCPv6 server and DHCPv6 relay

The configuration is a two-step process:

- CLI: Configure the DHCPv6 server, add a static route, and display the IPv6 binding information
- CLI: Configure the DHCPv6 relay

CLI: Configure the DHCPv6 server, add a static route, and display the IPv6 binding information

To use the CLI to configure the DHCPv6 server, add a static route, and display the IPv6 binding information:

1. Enable IPv6 routing and DHCPv6 service on the DHCPv6 server.

```
(Netgear Switch) (Config)#ipv6 dhcp pool ipv6_server
(Netgear Switch) (Config)#ip routing
(Netgear Switch) (Config)#service dhcpv6
```

2. Create a DHCPv6 pool on the DHCPv6 server.

```
(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 on the DHCPv6 server.

```
(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
```

4. Configure interface 1/0/6 with PVID 1 on the DHCPv6 server.

   Interface 1/0/6 on the DHCPv6 server connects to the DHCPv6 relay.

```
(Netgear Switch) (Config)#interface 1/0/6
(Netgear Switch) (Interface 1/0/6)#vlan pvid 1
(Netgear Switch) (Interface 1/0/6)#vlan participation include 1
(Netgear Switch) (Interface 1/0/6)#exit
```

5. Configure a static route for 2001:2::/64 on the DHCPv6 server.

```
(Netgear Switch) (Config)#ipv6 route 2001:2::/64 2001:1::2
(Netgear Switch) (Config)#exit
```

6. Display the DHCPv6 binding information on the DHCPv6 server.

```
(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
```

CLI: Configure the DHCPv6 relay

To use the CLI to configure the DHCPv6 relay:

1. Enable IPv6 routing and DHCPv6 service on the DHCPv6 relay.

```
(Netgear Switch) (Config)#ip routing
(Netgear Switch) (Config)#ipv6 unicast-routing
(Netgear Switch) (Config)#service dhcpv6
```

2. Enable IPv6 mode on VLAN 1 on the DHCPv6 relay.

```
(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
```

3. Configure interface 1/0/8 with PVID 1 on the DHCPv6 relay.

Interface 1/0/8 on the DHCPv6 relay connects to the DHCPv6 server.

```
(Netgear Switch) (Config)#interface 1/0/8
(Netgear Switch) (Interface 1/0/8)#vlan pvid 1
(Netgear Switch) (Interface 1/0/8)#vlan participation include 1
(Netgear Switch) (Interface 1/0/8)#exit
```

4. Add routing VLAN 2 on the DHCPv6 relay.

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

5. Enable DHCPv6 relay service on VLAN 2 on the DHCPv6 relay.

```
(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
```

6. On the DHCPv6 relay, add PVID 2 to interface 1/0/5 for the connection to the DHCPv6 client.

   Interface 1/0/5 on the DHCPv6 relay connects to the DHCPv6 client.

```
(Netgear Switch) (Config)#interface 1/0/5
(Netgear Switch) (Interface 1/0/5)#vlan pvid 2
(Netgear Switch) (Interface 1/0/5)#vlan participation include 2
(Netgear Switch) (Interface 1/0/5)#ipv6 enable
(Netgear Switch) (Interface 1/0/5)#exit
```

Main UI: Set up a configuration with a DHCPv6 server and DHCPv6 relay

The configuration is a two-step process:

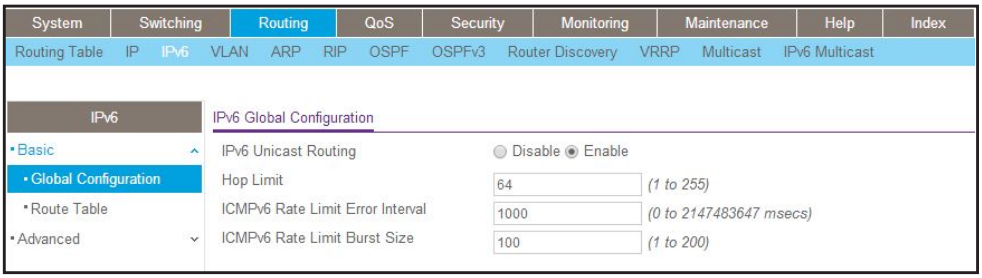
- Main UI: Configure the DHCPv6 server, add a static route, and display the IPv6 binding information
- Main UI: Configure the DHCPv6 relay

Main UI: Configure the DHCPv6 server, add a static route, and display the IPv6 binding information

To use the main UI to configure the DHCPv6 server, add a static route, and display the IPv6 binding information:

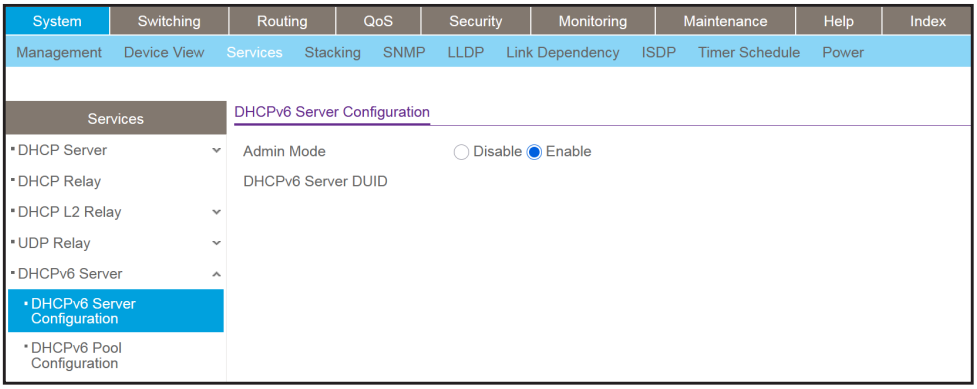
1. Enable IPv6 routing on the DHCPv6 server.
   a. Select **Routing > IPv6 > Basic > Global Configuration**.

      A page similar to the following figure displays.



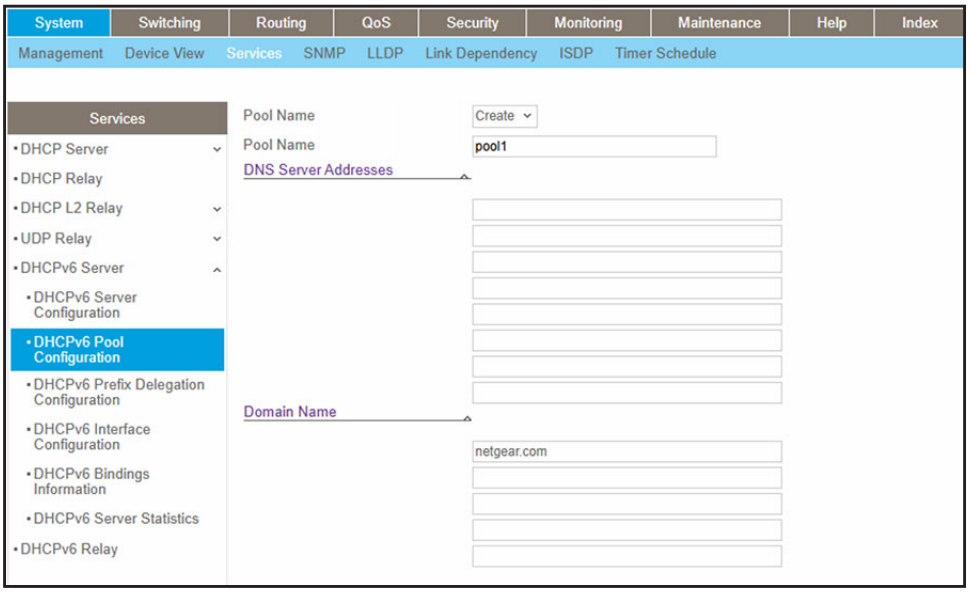
   b. Select the IPv6 Unicast Routing **Enable** radio button.
   c. Click the **Apply** button. Your settings are saved.
2. Enable DHCPv6 service on the DHCPv6 server.
   a. Select **System > Services > DHCPv6 Server > DHCPv6 Server Configuration**.

      A page similar to the following figure displays.



   b. Select the Admin Mode **Enable** radio button.
   c. Click the **Apply** button. Your settings are saved.
3. On the DHCPv6 server, create a DHCPv6 pool name and associated domain name.
   a. Select **System > Services > DHCPv6 Server > DHCPv6 Pool Configuration**.

A page similar to the following figure displays.



b. In the **Pool Name** menu, select **Create**.

c. In the **Pool Name** field, enter **pool1**.

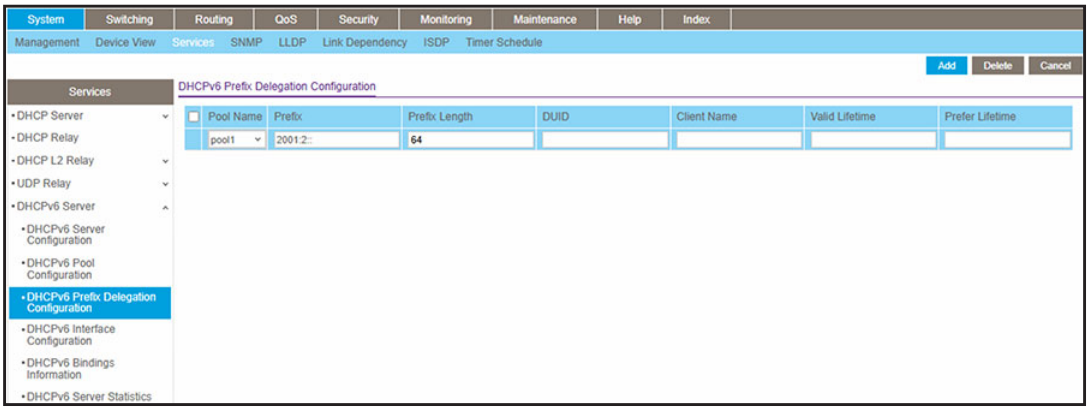
d. In the first **Domain Name** field, enter **netgear.com**.

e. Click the **Apply** button. Your settings are saved.

4. Create a prefix for DHCPv6 prefix delegation.

a. Select **System > Services > DHCPv6 Server > DHCPv6 Prefix Delegation Configuration**.

A page similar to the following figure displays.



b. In the **Pool Name** menu, select **pool1**.

c. In the **Prefix** field, enter **2001:2::**.

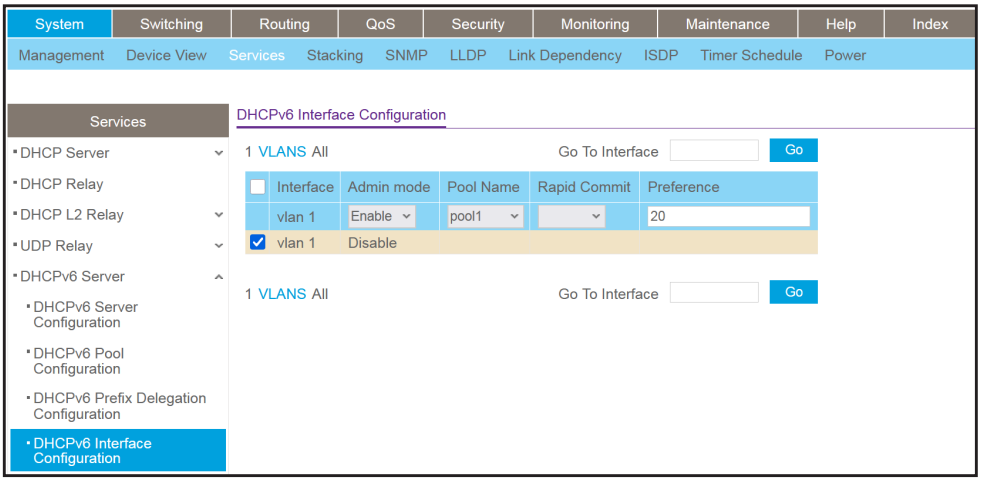
d. In the **Prefix Length** field, enter **64**.

e. Click the **Add** button. Your settings are saved.

5. Enable DHCPv6 service on VLAN 1 on the DHCPv6 server.

a. Select **System > Services > DHCPv6 Server > DHCPv6 Pool Interface**.

A page similar to the following figure displays.



b. Click **VLANS**. The VLAN interfaces displays.

c. Select the Interface **vlan 1** check box.

d. In the **Admin Mode** menu, select **Enable**.

e. In the **Pool Name** menu, select **pool1**.

f. In the **Preference** field, enter **20**.

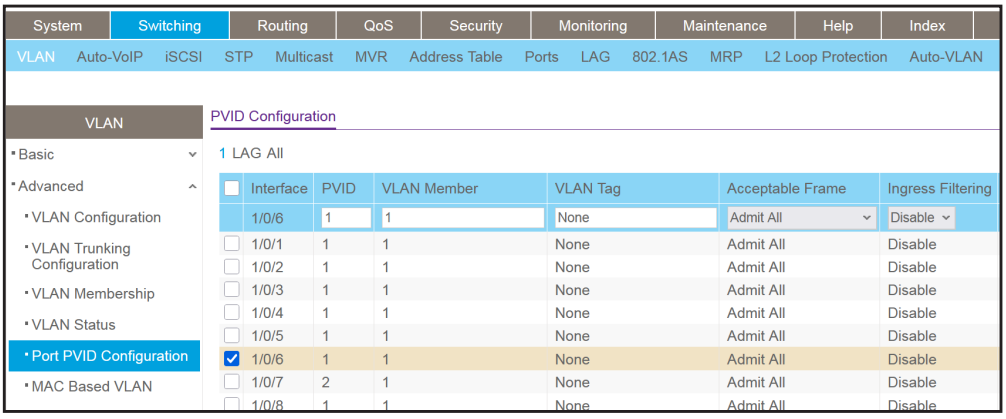
g. Click the **Apply** button. Your settings are saved.

6. Configure interface 1/0/6 with PVID 1 on the DHCPv6 server.

Interface 1/0/6 on the DHCPv6 server connects to the DHCPv6 relay.

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

A page similar to the following figure displays.



b. Select the Interface **1/0/6** check box.

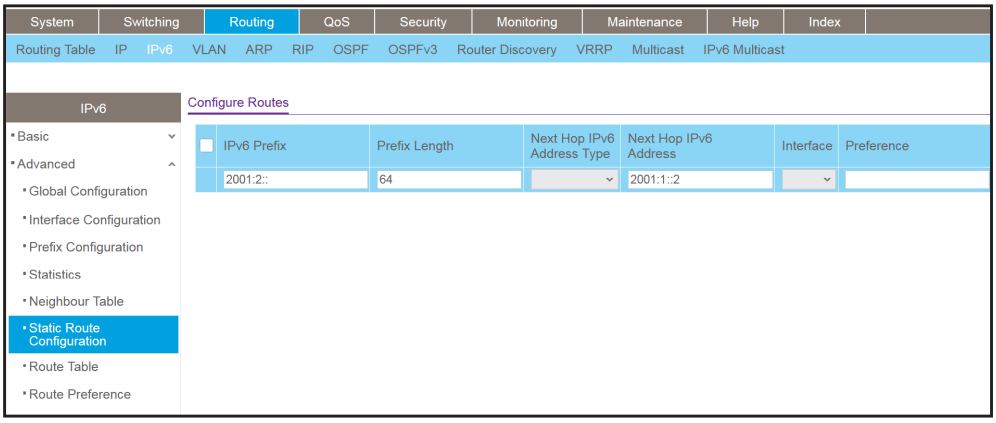
c. In the **PVID** field, enter **1**. (By default, the PVID for all interfaces is 1.)

d. Click the **Apply** button. Your settings are saved.

7. Configure a static route for 2001:2::/64 on the DHCPv6 server.

a. Select **Routing > IPv6 > Advanced > Static Route Configuration**.

A page similar to the following figure displays.



b. Configure the following settings:

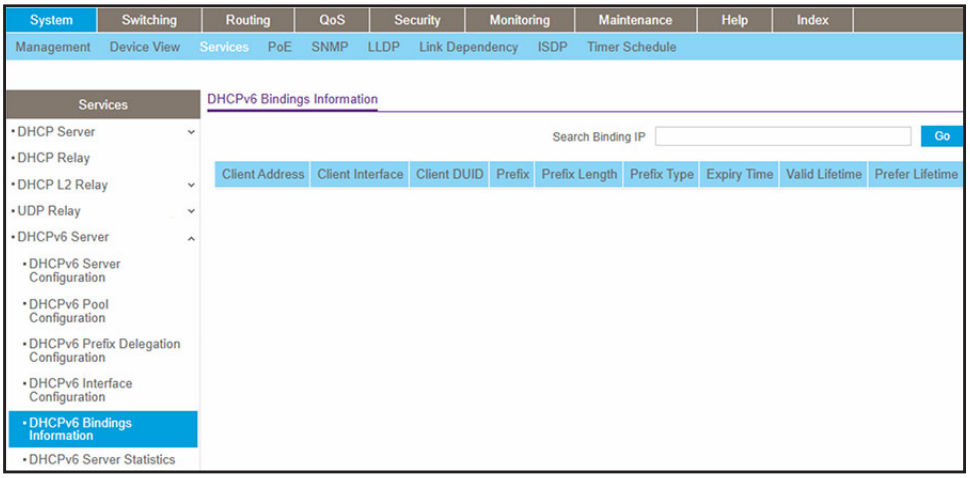
- In the **IPv6 Prefix** field, enter **2001:2::**.
- In the **Prefix Length** field, enter **64**.
- In the **Next Hop IPv6 Address** field, enter **2001:2::**.

c. Click the **Add** button. Your settings are saved.

8. Display the DHCPv6 binding information on the DHCPv6 server.

a. Select **System > Services > DHCPv6 Server > DHCPv6 Bindings Information**.

A page similar to the following figure displays.

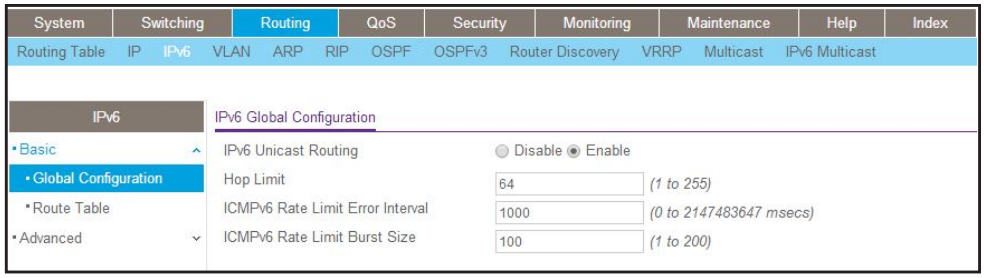


Main UI: Configure the DHCPv6 relay

To use the main UI to configure the DHCPv6 relay:

1. Enable IPv6 routing on the DHCPv6 relay.
   a. Select **Routing > IPv6 > Basic > Global Configuration**.

      A page similar to the following figure displays.

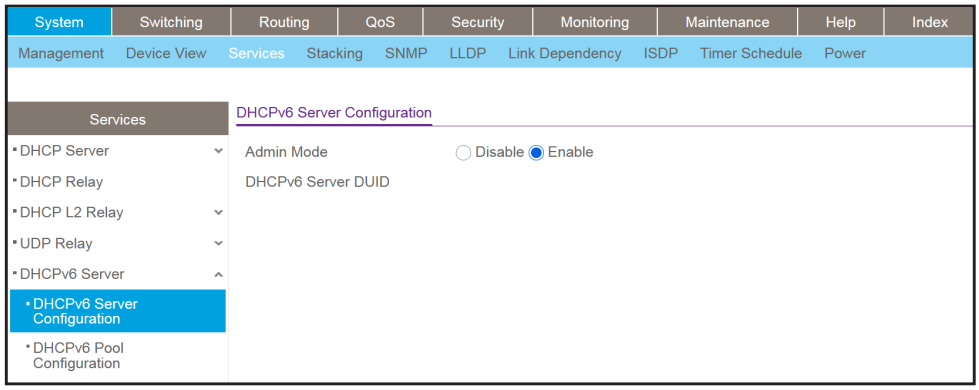


   b. Select the IPv6 Unicast Routing **Enable** radio button.
   c. Click the **Apply** button. Your settings are saved.
2. Enable DHCPv6 service on the DHCPv6 server.

   Note: DHCPv6 relay depends on the DHCPv6 server functionality so you must enable the DHCPv6 service globally.

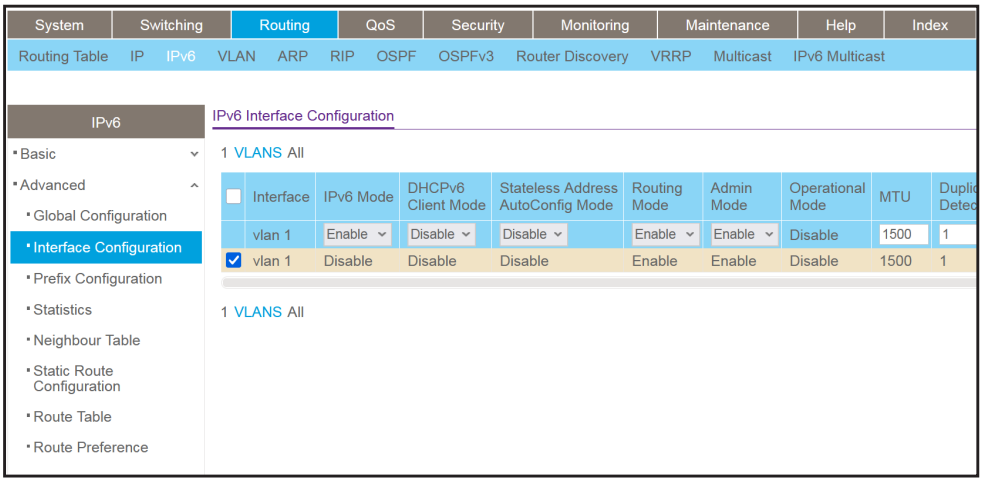
   a. Select **System > Services > DHCPv6 Server > DHCPv6 Server Configuration**.

      A page similar to the following figure displays.



   b. Select the Admin Mode **Enable** radio button.
   c. Click the **Apply** button. Your settings are saved.
3. Enable IPv6 mode on the VLAN 1 interface of the DHCPv6 relay.
   a. Select **Routing > IPv6 > Advanced > Interface Configuration**.

A page similar to the following figure displays.



b. Click **VLANS**. The VLAN interfaces displays.

c. Select the Interface **vlan 1** check box.

d. In the **IPv6 Mode** menu, select **Enable**.

e. In the **DHCPv6 Client Mode** menu, select **Disable**.

f. In the **Stateless Address AutoConfig Mode** menu, enter **Disable**.

g. In the **Routing Mode** menu, select **Enable**.

h. In the **Admin Mode** menu, select **Enable**.

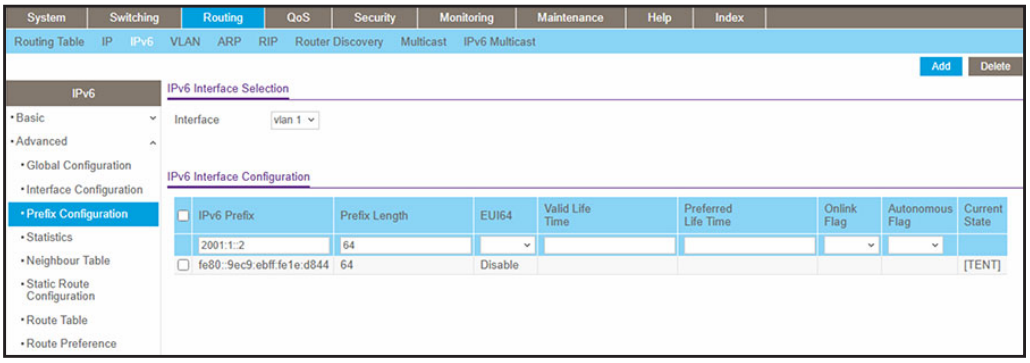
i. Click the **Apply** button. Your settings are saved.

4. Configure the VLAN 1 interface with IPv6 address 2001:1::2/64.

The VLAN 1 interface on the DHCPv6 relay connects to the DHCPv6 server.

a. Select **Routing > IPv6 > Advanced > Prefix Configuration**.

A page similar to the following figure displays.



b. In the Interface menu, select **vlan 1**.

c. In the **IPv6 Prefix** field, enter **2001:1::2**.

d. In the **Prefix Length** field, enter **64**.

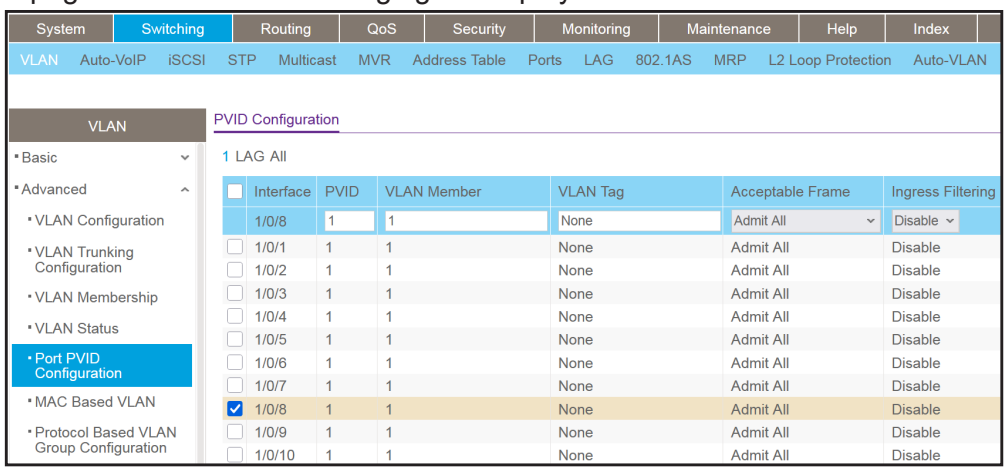
e. Click the **Add** button. Your settings are saved.

5. Configure interface 1/0/8 with PVID 1 (for VLAN 1) on the DHCPv6 relay.

   Interface 1/0/8, which is a member of VLAN 1, on the DHCPv6 relay connects to the DHCPv6 server.

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

      A page similar to the following figure displays.



   b. Select the Interface **1/0/8** check box.

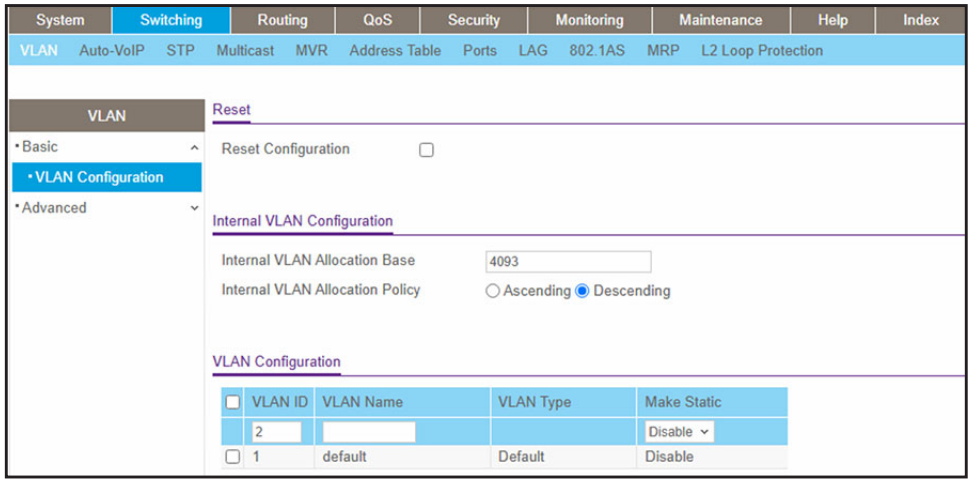
   c. In the **PVID** field, enter **1**. (By default, the PVID for all interfaces is 1.)

   d. Click the **Apply** button. Your settings are saved.

6. Add VLAN 2.

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

      A page similar to the following figure displays.



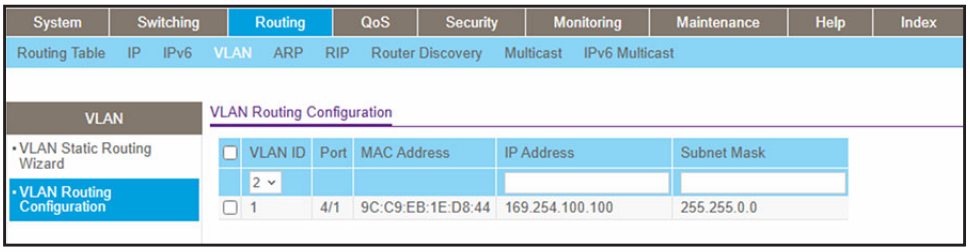
   b. In the **VLAN ID** field, enter **2**.

   c. Click the **Add** button. Your settings are saved.

7. Enable routing on VLAN 2, so that VLAN 2 becomes a routing interface.

   a. Select **Routing > VLAN > VLAN Routing Configuration**.

A page similar to the following figure displays.



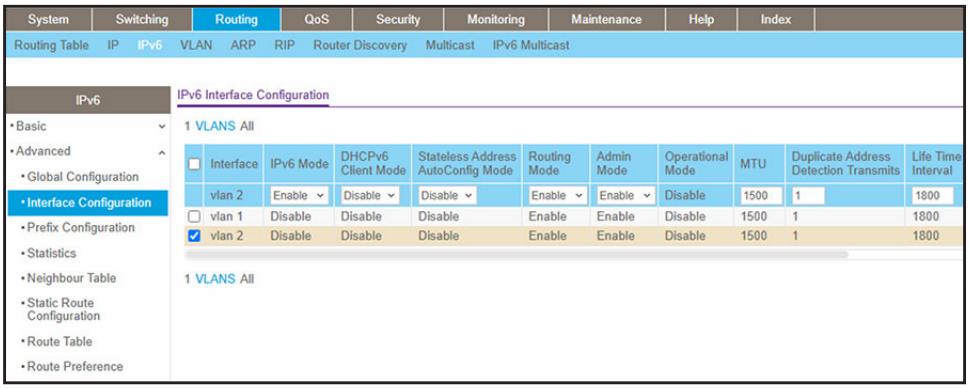
b. In the **VLAN ID** menu, select **2**.

c. Click the **Add** button. Your settings are saved.

8. Add the VLAN 2 routing interface on the DHCPv6 relay.

a. Select **Routing > IPv6 > Advanced > Interface Configuration**.

A page similar to the following figure displays.



b. Click **VLANS**. The VLAN interfaces displays.

c. Select the Interface **vlan 2** check box.

d. In the **IPv6 Mode** menu, select **Enable**.

e. In the **DHCPv6 Client Mode** menu, select **Disable**.

f. In the **Stateless Address AutoConfig Mode** menu, enter **Disable**.

g. In the **Routing Mode** menu, select **Enable**.

h. In the **Admin Mode** menu, select **Enable**.

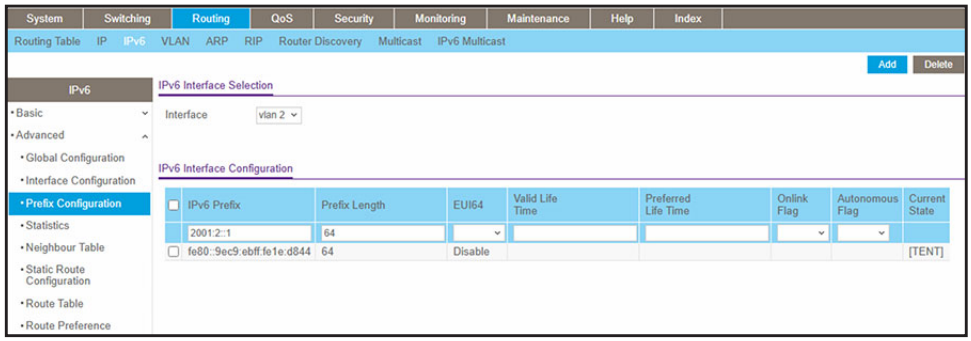
i. Click the **Apply** button. Your settings are saved.

9. Configure the VLAN 2 interface with IPv6 address 2001:2::1/64.

The VLAN 2 routing interface has interface 1/0/5 as a member. The 1/0/5 interface on the DHCPv6 relay connects to the DHCPv6 client.

a. Select **Routing > IPv6 > Advanced > Prefix Configuration**.

A page similar to the following figure displays.



b. In the Interface menu, select **vlan2**.

c. In the **IPv6 Prefix** field, enter **2001:2::1**.

d. In the **Prefix Length** field, enter **64**.

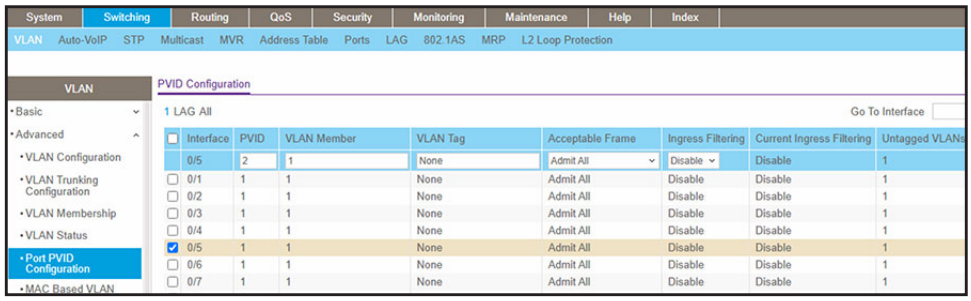
e. Click the **Add** button. Your settings are saved.

10. Configure interface 1/0/5 with PVID 2 (for VLAN 2) on the DHCPv6 relay.

Interface 1/0/5 on the DHCPv6 relay connects to the DHCPv6 client.

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

A page similar to the following figure displays.



b. Select the Interface **1/0/5** check box.

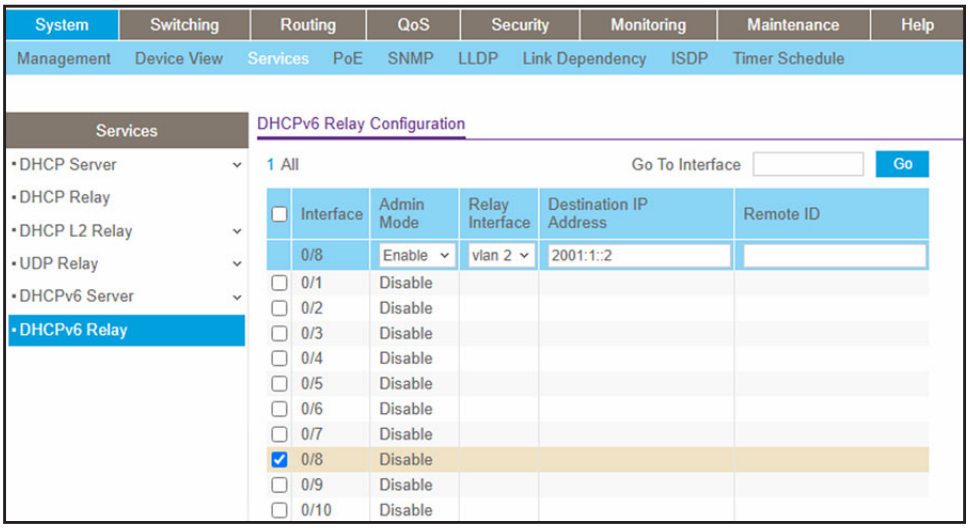
c. In the **PVID** field, enter **2**.

d. Click the **Apply** button. Your settings are saved.

11. Configure the DHCPv6 relay.

a. Select **System > Services > DHCPv6 Relay**.

A page similar to the following figure displays.



b. Select the Interface **1/0/8** check box.

c. In the **Admin Mode** menu, select **Enable**.

d. In the **Relay Interface** menu, select **vlan 2**.

e. In the **Destination IP Address** field, enter **2001:1::2**.

f. Click the **Apply** button. Your settings are saved.

27

DVLANs and Private VLANs

Double VLANS and private VLAN groups

This feature is supported on the M4250 series switches

This feature is supported on the M4300 series switches

This feature is supported on the M4350 series switches

This chapter includes the following sections:

- Double VLANs
- Private VLAN groups

Double VLANs

This section describes how to enable the double VLAN (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 that 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.

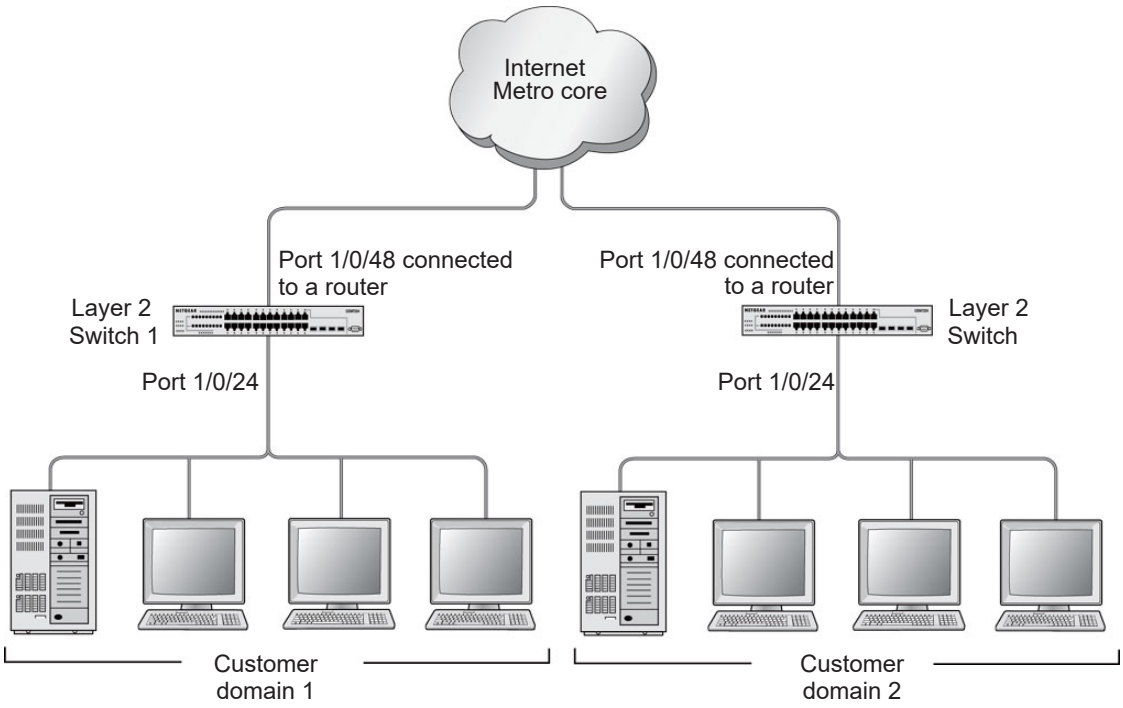


Figure 54. Double VLANS

This following example describes how to enable the double DVLAN feature. Double VLANs pass traffic from one customer domain (Customer domain 1) to another (Customer domain 2) 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 (and in the previous figure), the switches have the same configuration.

The example is shown as CLI commands and as a main UI procedure.

CLI: Create and enable a double VLAN

To use the CLI to create and enable a double VLAN, configure the following setting on each switch (Switch 1 and Switch 2):

1. Create VLAN 200.

```
(Netgear Switch) #vlan database
(Netgear Switch) (Vlan)#vlan 200
(Netgear Switch) (Vlan)#exit
```

2. Add interface 1/0/24 to VLAN 200 and add PVID 200 to interface 1/0/24.

```
(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
```

3. Add interface 1/0/48 to 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
```

4. Select interface 1/0/48 as the provider port for the double VLAN configuration.

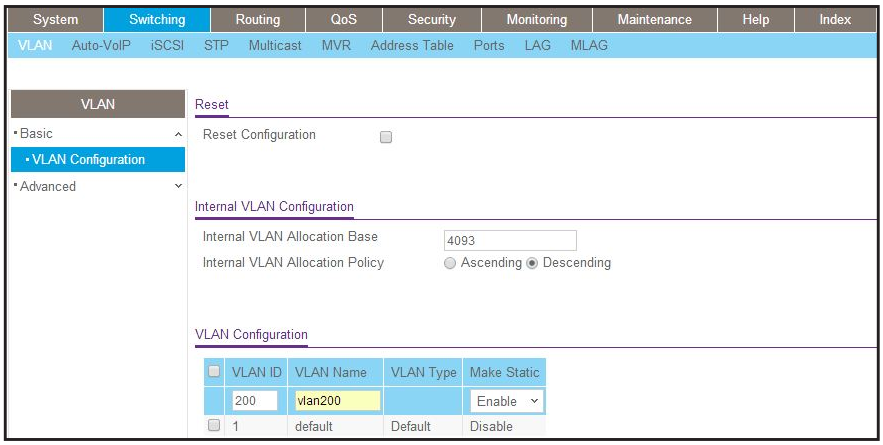
```
(Netgear Switch) (Config)#
(Netgear Switch) (Config)#interface 1/0/48
(Netgear Switch) (Interface 1/0/48)#mode dvlan-tunnel
(Netgear Switch) (Interface 1/0/48)#exit
```

Main UI: Create and enable a double VLAN

To use the main UI to create and enable a double VLAN, configure the following setting on each switch (Switch 1 and Switch 2):

1. Create VLAN 200:
   a. Select **Switching > VLAN > Basic > VLAN Configuration**.

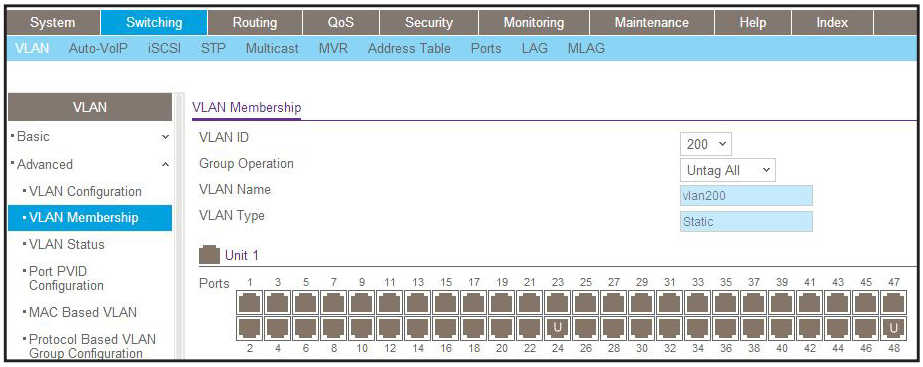
      A page similar to the following figure displays.



   b. Under VLAN Configuration, configure the following settings:
      - In the **VLAN ID** field, enter **200**.
      - In the **VLAN Name** field, enter **vlan200**.
      - In the **Make Static** menu, select **Enable**.

   c. Click the **Add** button. Your settings are saved.
2. Add ports 24 and 48 to VLAN 200.
   a. Select **Switching > VLAN > Advanced > VLAN Membership**.

      A page similar to the following figure displays.



   b. In the **VLAN ID** menu, select **200**.
   c. Click the gray boxes under ports **24** and **48** until U displays, which specifies that the egress packets are untagged for the ports.

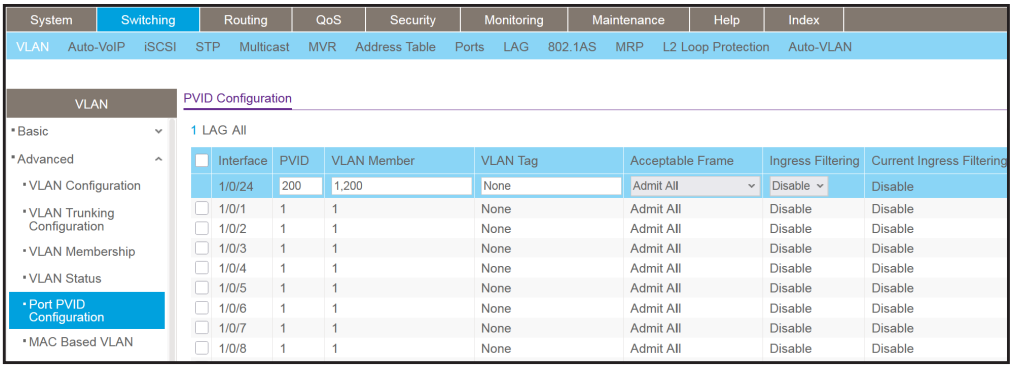
If your switch is a member of a stack, be sure that you select the ports in the correct unit.

d. Click the **Apply** button. Your settings are saved.

3. Change the port VLAN ID (PVID) of port 24 to 200:

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

A page similar to the following figure displays.



b. Select the Interface **1/0/24** check box.

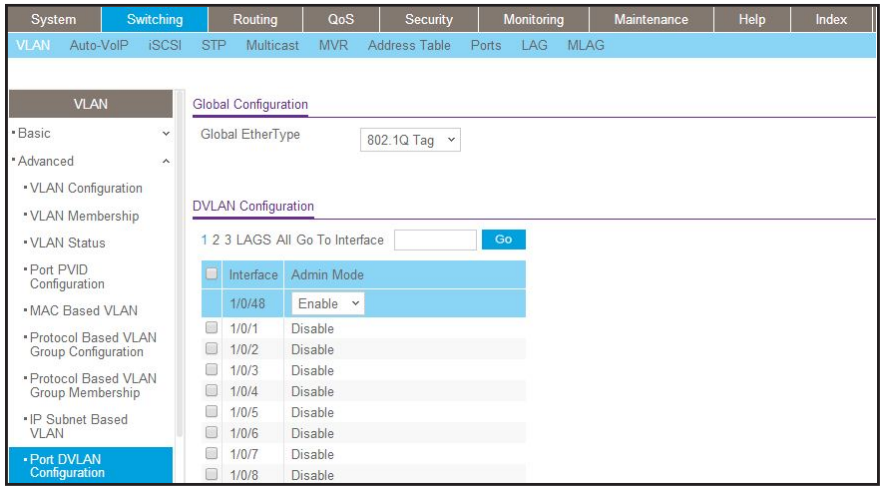
c. In the **PVID** field, enter **200**.

d. Click the **Apply** button. Your settings are saved.

4. Configure port 48 as the provider service port in the double VLAN configuration:

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

A page similar to the following figure displays.



b. Select the Interface **1/0/48** check box.

c. In the **Admin Mode** menu, select **Enable**.

d. Click the **Apply** button. Your settings are saved.

Private VLAN groups

A private VLAN group allows you to create groups of users within a VLAN. These users cannot communicate with members in different groups but only with members within the same group.

Two modes exist for a private group:

- **Isolated mode**: A member port in the group cannot forward its egress traffic to any other members in the same group.
- **Community mode**: A member port can forward traffic to other members in the same group, but not to members in other groups.

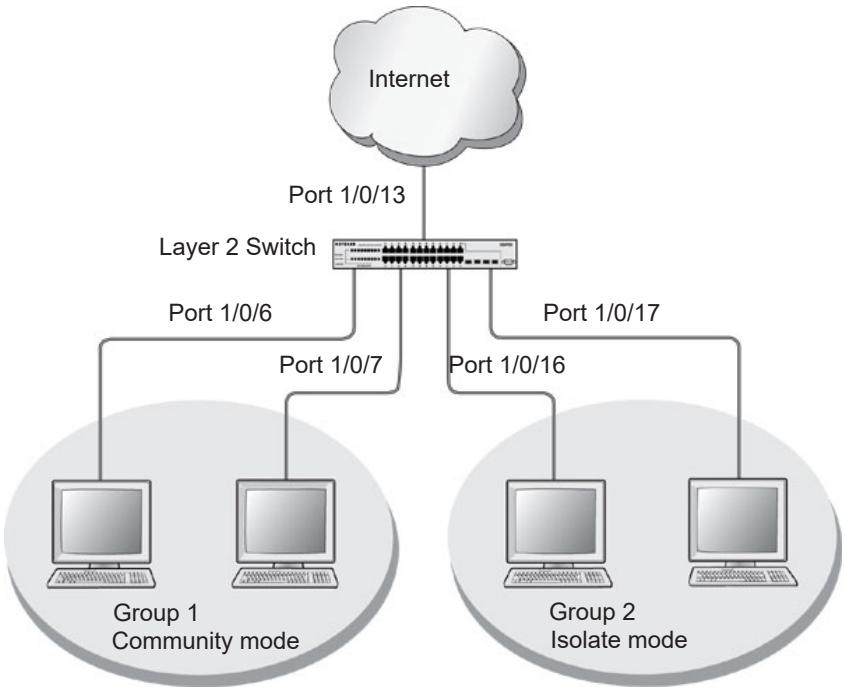


Figure 55. Private VLAN groups in community mode and isolated mode

The following example creates two groups. Group 1 is in community mode, and Group 2 is in isolated mode. The example is shown as CLI commands and as a main UI procedure.

CLI: Create private VLAN groups

To use the CLI to create two private groups and add member ports to each group:

1. Create a VLAN 200 and include ports 1/0/6, 1/0/7, 1/0/16, and 1/0/17.

```
(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 private group 1 in community mode.

```
(Netgear Switch) (Config)#
(Netgear Switch) (Config)#private-group name group1 1 mode community
```

3. Create a private group 2 in isolated mode.

```
(Netgear Switch) (Config)#private-group name group2 2 mode isolated
```

4. Add ports 1/0/16 and 1/0/7 to private group 1.

```
(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 ports 1/0/16 and 1/0/7 to private group 2.

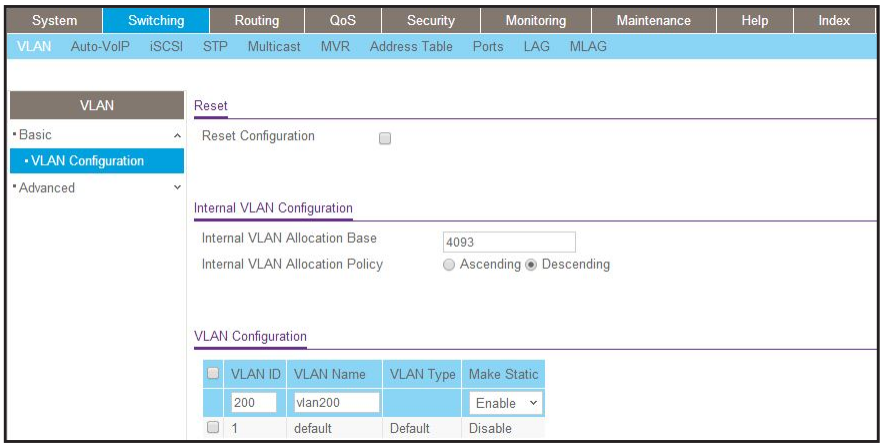
```
(Netgear Switch) (Config)#interface range 1/0/16-1/0/17
(Netgear Switch) (conf-if-range-1/0/16-1/0/17)#switchport private-group 2
(Netgear Switch) (conf-if-range-1/0/16-1/0/17)#exit
```

Main UI: Create private VLAN groups

To use the main UI to create two private groups and add member ports to each group:

1. Create VLAN 200.
   a. Select **Switching > VLAN > Basic > VLAN Configuration**.

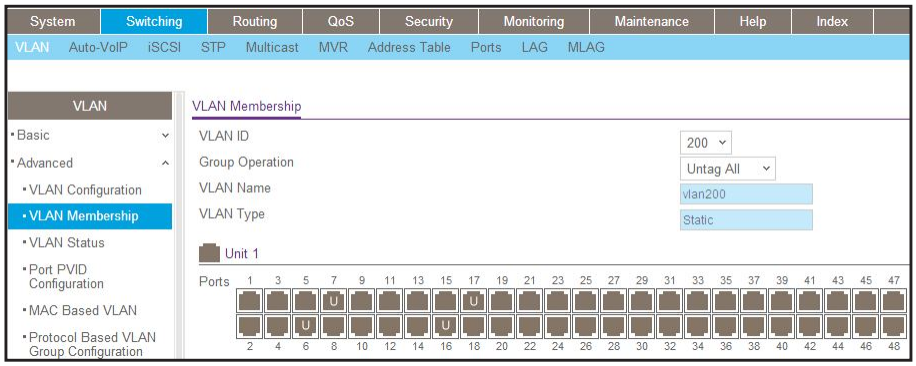
      A page similar to the following figure displays.



   b. Configure the following settings:
      - In the **VLAN ID** field, enter **200**.
      - In the **VLAN Name** field, enter **VLAN200**.
      - In the **Make Static** menu, select **Enable**.

   c. Click the **Add** button. Your settings are saved.
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 page similar to the following figure displays.



b. In the **VLAN ID** menu, select **200**.

c. Click the gray boxes under ports **6**, **7**, **16** and **17** until U displays, which specifies that the egress packets are untagged for the ports.

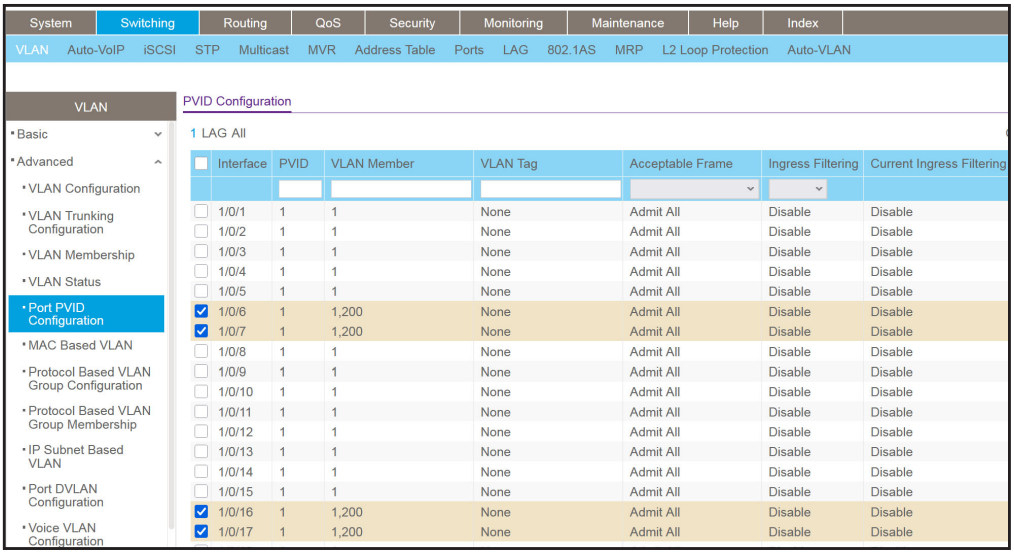
If your switch is a member of a stack, be sure that you select the ports in the correct unit.

d. Click the **Apply** button. Your settings are saved.

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 page similar to the following figure displays.



b. Select the Interface **1/0/6**,**1/0/7**,**1/0/16**, and **1/0/17** check boxes.

c. In the **PVID** field, enter **200**.

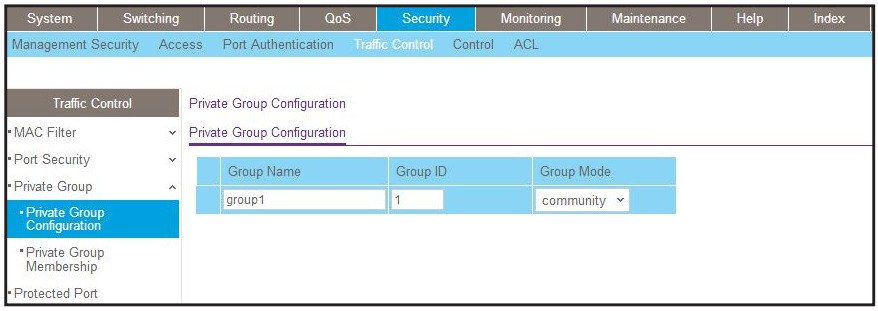
d. In the **Acceptable Frame** menu, select **Admit All**.

e. Click the **Apply** button. Your settings are saved.

4. Create a private VLAN group, group 1.

a. Select **Security > Traffic Control > Private Group > Private Group Configuration**.

A page similar to the following figure displays.



b. In the **Group Name** field, enter **group1**.

c. In the **Group ID** field, enter **1**.

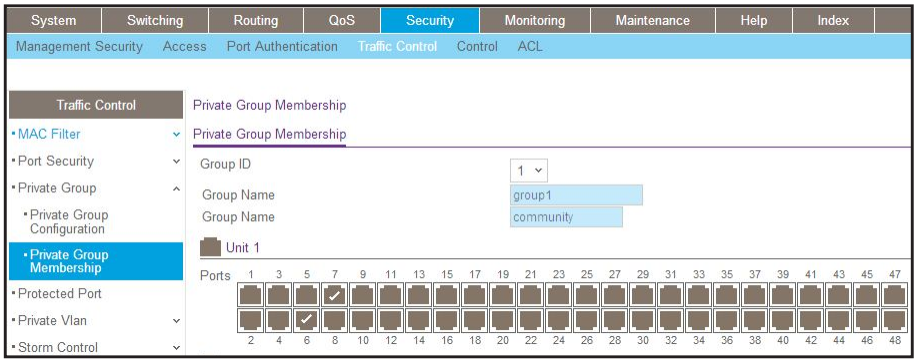
d. In the **Group Mode** menu, select **community**.

e. Click the **Add** button. Your settings are saved.

5. Add port 6 and 7 to group 1.

a. Select **Security > Traffic Control > Private Group > Private Group Membership**.

A page similar to the following figure displays.



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

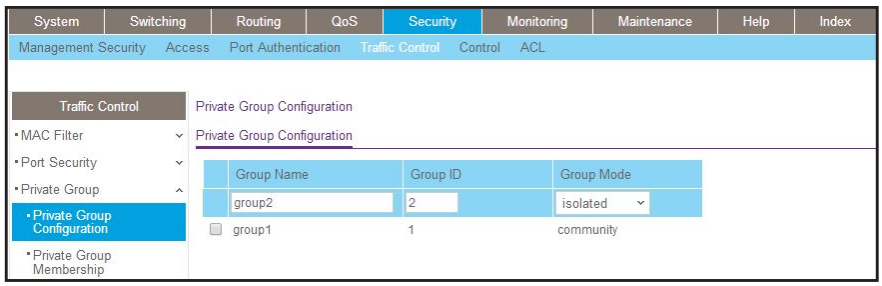
c. Click the gray boxes under ports **6** and **7**. A check mark displays in each box.

d. Click the **Apply** button. Your settings are saved.

6. Create a private group, group 2.

a. Select **Security > Traffic Control > Private Group > Private Group Configuration**.

A page similar to the following figure displays.



b. In the **Group Name** field, enter **group2**.

c. In the **Group ID** field, enter **2**.

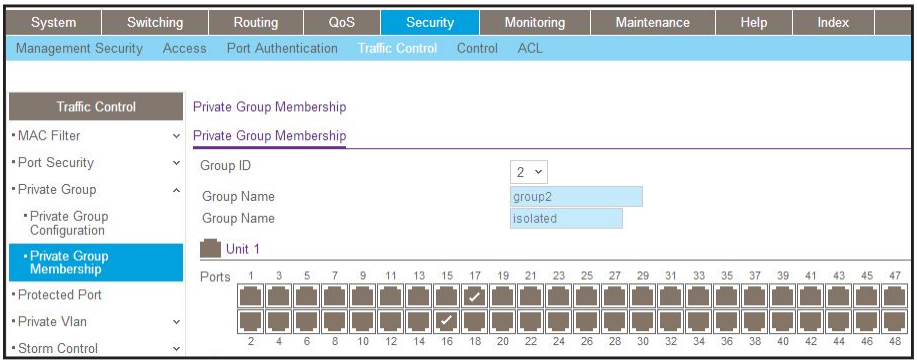
d. In the **Group Mode** menu, select **isolated**.

e. Click the **Add** button. Your settings are saved.

7. Add ports 16 and 17 to group 2.

a. Select **Security > Traffic Control > Private Group > Private Group Membership**.

A page similar to the following figure displays.



b. In the **Group ID** menu, select **2**.

c. Click the gray boxes under ports **16** and **17**. A check mark displays in each box.

d. Click the **Apply** button. Your settings are saved.

28

STP

Spanning Tree Protocol

This feature is supported on the M4250 series switches

This feature is supported on the M4300 series switches

This feature is supported on the M4350 series switches

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. Three STPs exist: 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 that RSTP 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 main UI procedure.

CLI: Configure Classic STP (802.1d)

To use the CLI to configure Classic STP:

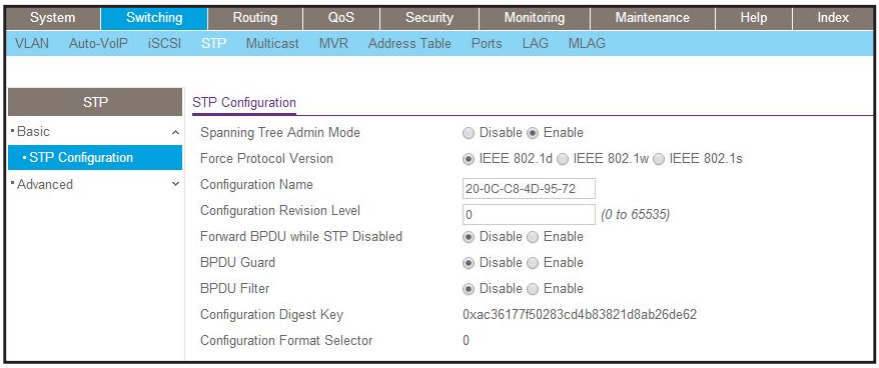
```
(Netgear Switch) (Config)# spanning-tree
(Netgear Switch) (Config)# spanning-tree mode stp
(Netgear switch) (Interface 1/0/3)# spanning-tree port mode
```

Main UI: Configure Classic STP (802.1d)

To use the main UI to configure Classic STP:

1. Enable 802.1d on the switch.
   a. Select **Switching > STP > STP Configuration**.

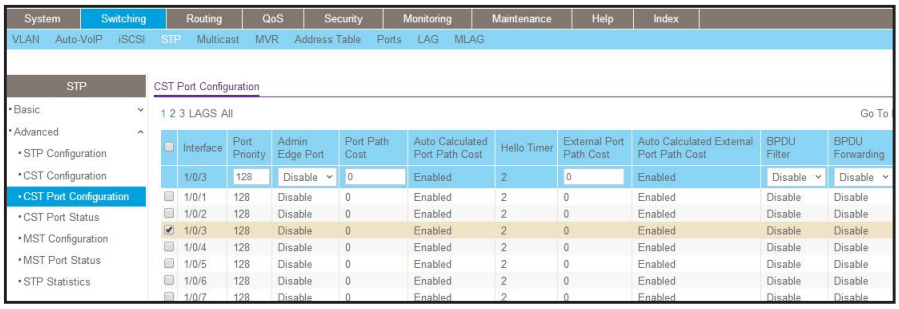
      A page similar to the following figure displays.



   b. Configure the following settings:
      - Select the Spanning Tree Admin Mode **Enable** radio button.
      - Select the Force Protocol Version **IEEE 802.1d** radio button.

   c. Click the **Apply** button. Your settings are saved.
2. Configure the CST port.
   a. Select **Switching > STP > Advanced > CST Port Configuration**.

      A page similar to the following figure displays.



   b. Select the Interface **1/0/3** check box.
   c. In the **Port Mode** menu (not shown in the previous figure), select **Enable**.
   d. Click the **Apply** button. Your settings are saved.

Configure Rapid STP (802.1w)

The example is shown as CLI commands and as a main UI procedure.

CLI: Configure Rapid STP (802.1w)

To use the CLI to configure Rapid STP:

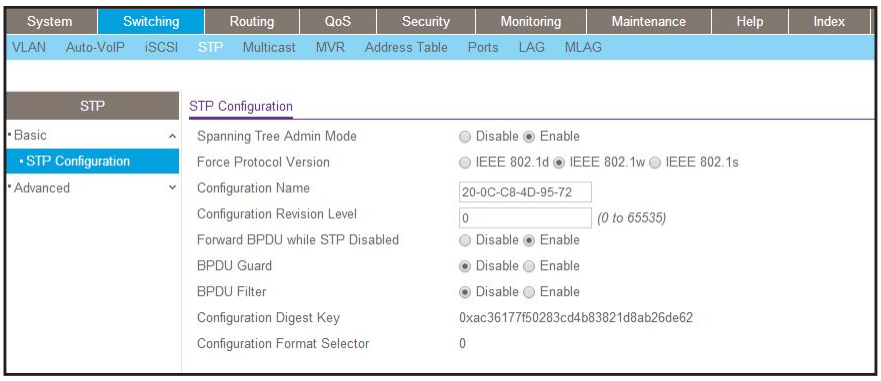
```
(Netgear switch) (Config)# spanning-tree
(Netgear switch) (Config)# spanning-tree mode rstp
(Netgear switch) (Interface 1/0/3)# spanning-tree port mode
```

Main UI: Configure Rapid STP (802.1w)

To use the main UI to configure Rapid STP:

1. Enable 802.1w on the switch:
   a. Select **Switching > STP > STP Configuration**.

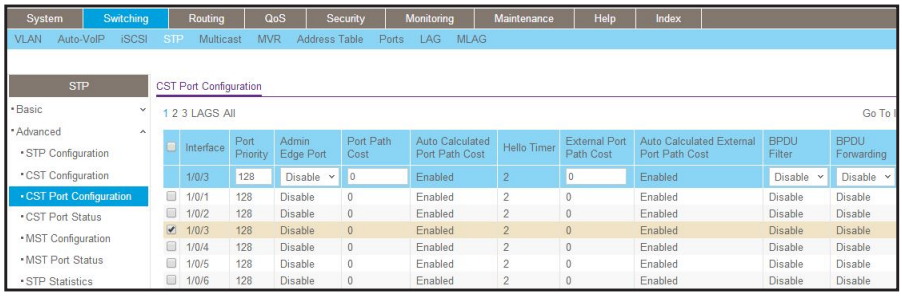
      A page similar to the following figure displays.



   b. Configure the following settings:
      - Select the Spanning Tree Admin Mode **Enable** radio button.
      - Select the Force Protocol Version **IEEE 802.1w** radio button.

   c. Click the **Apply** button. Your settings are saved.
2. Configure the CST port.
   a. Select **Switching > STP > CST Port Configuration**.

A page similar to the following figure displays.



b. Select the Interface **1/0/3** check box.

c. In the **Port Mode** menu (not shown in the previous figure), select **Enable**.

d. Click the **Apply** button. Your settings are saved.

Configure Multiple STP (802.1s)

The example is shown as CLI commands and as a main UI procedure.

CLI: Configure Multiple STP (802.1s)

To use the CLI to configure Multiple STP:

1. 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.

```
(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
```

2. Create MST instance 1:

```
(Netgear switch) (Config)# spanning-tree mst instance 1
```

3. Associate MST instance 1 with VLAN 2 and VLAN 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
```

4. Create MST instance 2:

```
(Netgear switch) (Config)# spanning-tree mst instance 2
```

5. Associate MST instance 2 with VLAN 11 and VLAN 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
```

6. For MST 1, configure the priority and cost on port 1/0/3:

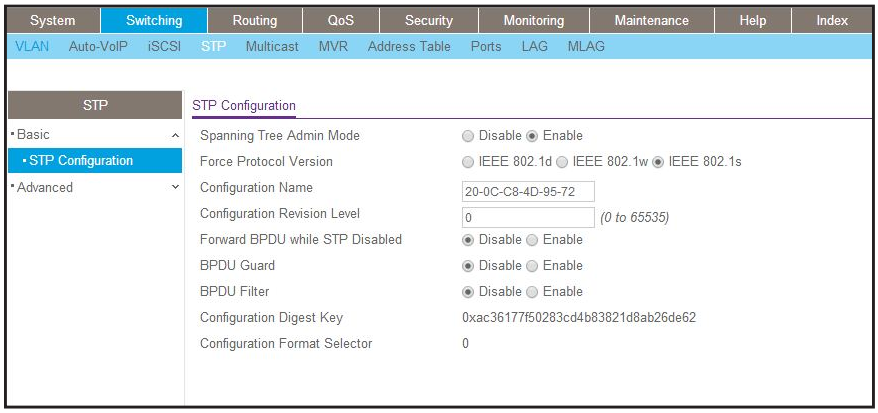
```
(Netgear switch) (Interface 1/0/3)# spanning-tree mst 1 port-priority 128
(Netgear switch) (Interface 1/0/3)# spanning-tree mst 1 cost 0
```

Main UI: Configure Multiple STP (802.1s)

To use the main UI to configure Multiple STP:

1. Enable 802.1s on the switch.
   a. Select **Switching > STP > STP Configuration**.

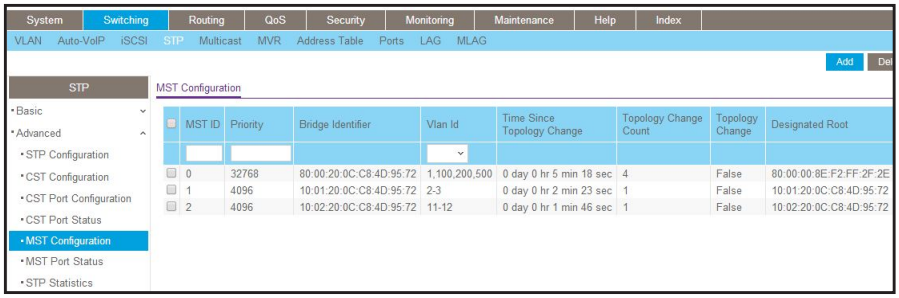
      A page similar to the following figure displays.



   b. Configure the following settings:
      - Select the Spanning Tree Admin Mode **Enable** radio button.
      - Select the Force Protocol Version **IEEE 802.1s** radio button.
      - In the **Configuration Name** field, enter **mstp_1**.
      - In the **Configuration Revision Level** field, enter **0**.

   c. Click the **Apply** button. Your settings are saved.
2. Configure MST instances 1 and 2.
   a. Select **Switching > STP > MST Configuration**.

A page similar to the following figure displays.



b. Configure MST ID 1.

- In the **MST ID** field, enter **1**.
- In the **Priority** field, enter **4096**.
- In the **VLAN ID** menu, select **2**.
- Click the **Add** button. Your settings are saved.
- In the **VLAN ID** menu, select **3**.
- Click the **Apply** button. Your settings are saved.

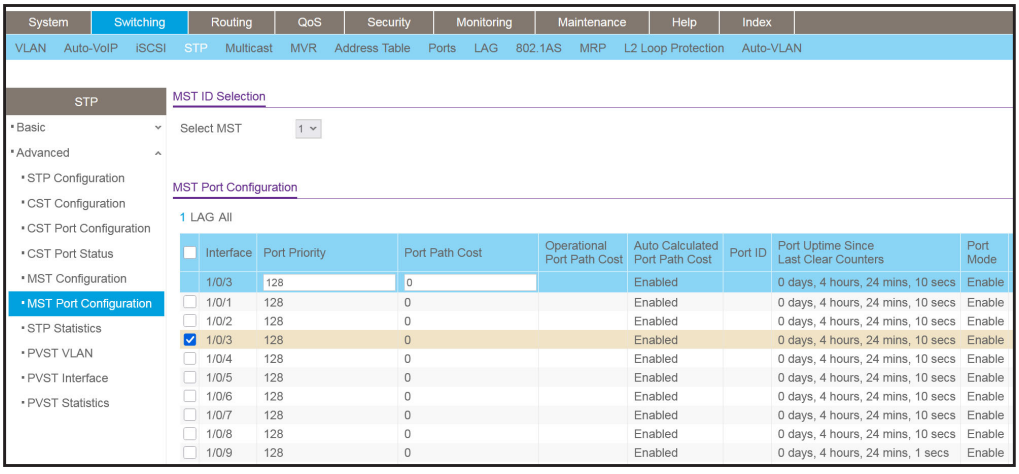
c. Configure MST ID 2.

- In the **MST ID** field, enter **2**.
- In the **Priority** field, enter **4096**.
- In the **VLAN ID** menu, select **11**.
- Click the **Add** button. Your settings are saved.
- In the **VLAN ID** menu, select **12**.
- Click the **Apply** button. Your settings are saved.

3. Configure the MST port.

a. Select **Switching > STP > Advanced > MST Port Configuration**.

A page similar to the following figure displays.



b. In the **Select MST** menu, select **1**.

c. Select the Interface **1/0/3** check box.
d. In the **Port Priority** field, enter **128**.
e. In the **Port Path Cost** field, enter **0**.

4. Click the **Apply** button. Your settings are saved.

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 convergence time after a link fails. 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 a 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.

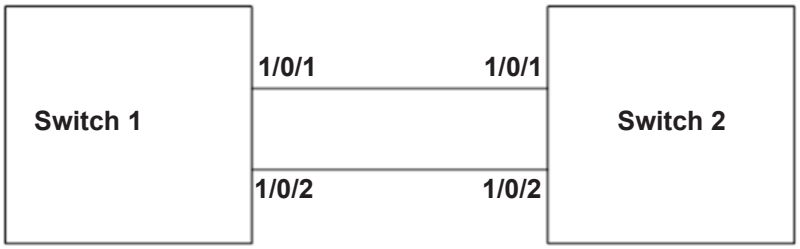


Figure 56. PVSTP configuration

The example is shown as CLI commands and as a main UI procedure.

CLI: Configure PVSTP

You must configure PVSTP on Switch 1 and Switch 2. This example assumes that all switches can support PVSTP. In this example, for both Switch 1 and Switch 2, 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.

Note: After you enable PVSTP (or PVRSTP) globally, PVSTP (or PVRSTP) is applied to VLANs automatically.

CLI: Configure PVSTP on Switch 1

To use the CLI to configure PVSTP on Switch 1:

1. Enable PVSTP.

```
(Netgear Switch) #config
(Netgear Switch) (Config)#spanning-tree mode pvst
```

2. 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
```

3. 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
```

4. To enable Switch 1 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

To use the CLI to configure PVSTP on Switch 1:

1. Enable PVSTP.

```
(Netgear Switch) #config
(Netgear Switch) (Config)#spanning-tree mode pvst
```

2. 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.
```

3. 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
```

Main UI: Configure PVSTP

You must configure PVSTP on Switch 1 and Switch 2. This example assumes that all switches can support PVSTP. In this example, for both Switch 1 and Switch 2, 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.

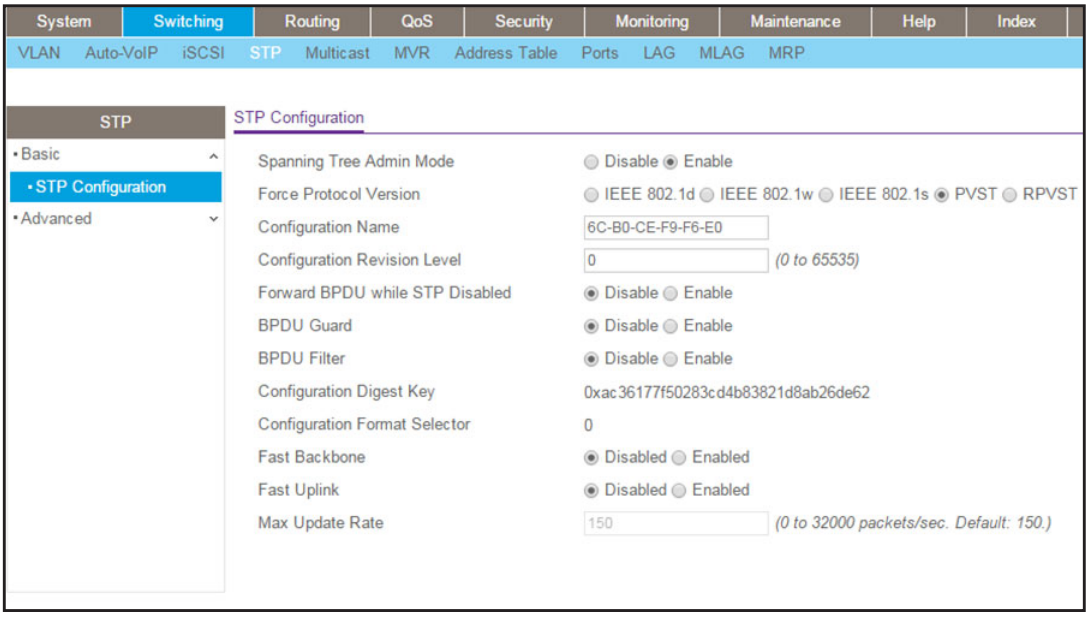
Note: After you enable PVSTP (or PVRSTP) globally, PVSTP (or PVRSTP) is applied to VLANs automatically.

Main UI: Configure PVSTP on Switch 1

To use the main UI to configure PVSTP on Switch 1:

1. Enable PVSTP.
   a. Select **Switching > STP > Basic > STP Configuration**.

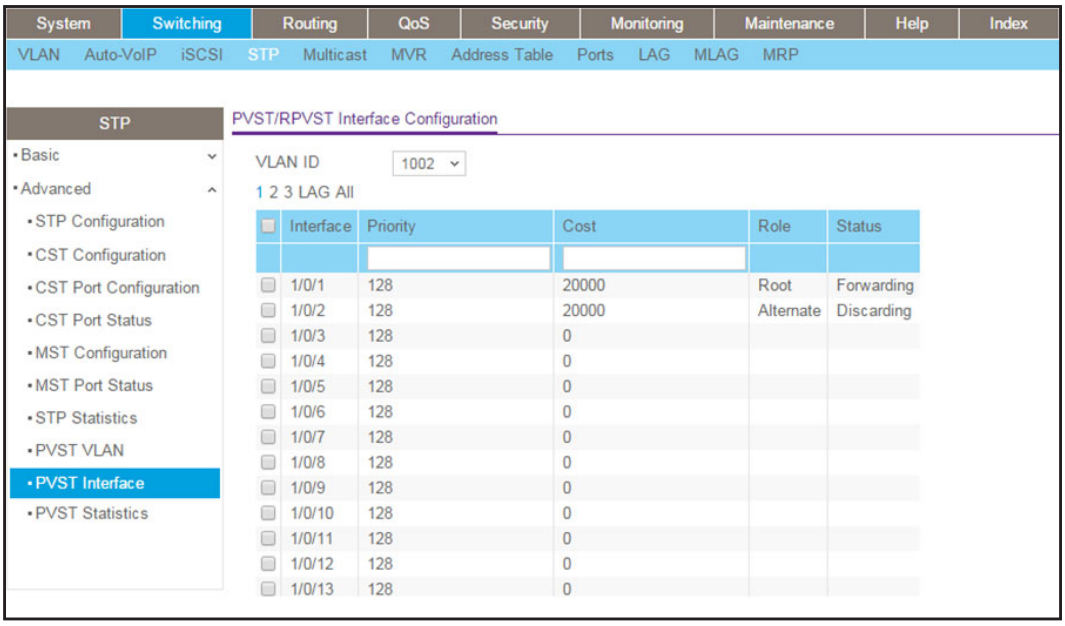
      A page similar to the following figure displays.



   b. Configure the following settings:
      - Select the Spanning Tree Admin Mode **Enable** radio button.
      - Select the Force Protocol Version **PVST** radio button.

   c. Click the **Apply** button. Your settings are saved.
2. Display the PVST status for port 1/0/1 and 1/0/2 in VLAN 1002.
   a. Select **Switching > STP > Advanced > PVST Interface**.

      A page similar to the following figure displays.



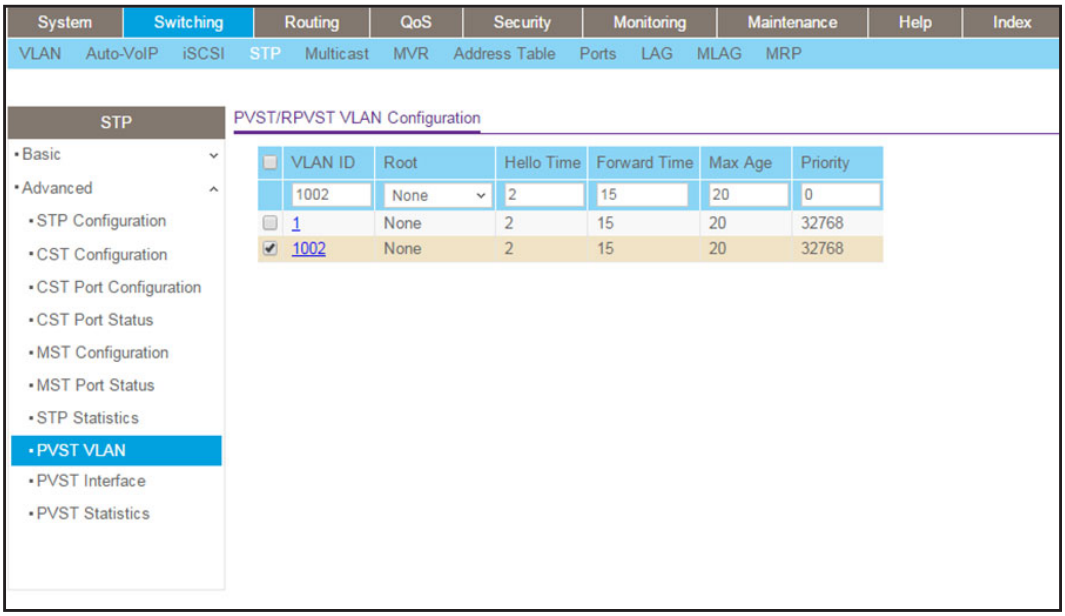
b. From the **VLAN ID** menu, select **1002**.

The roles of ports 1/0/1 and 1/0/2 display.

3. To enable the switch to be elected as the root, change the PVST priority to a lower value (for example, 0).

a. Select **Switching > STP > Advanced > PVST VLAN**.

A page similar to the following figure displays.



b. Select the VLAN ID **1002** check box.

c. In the **Priority** field, enter **0**.

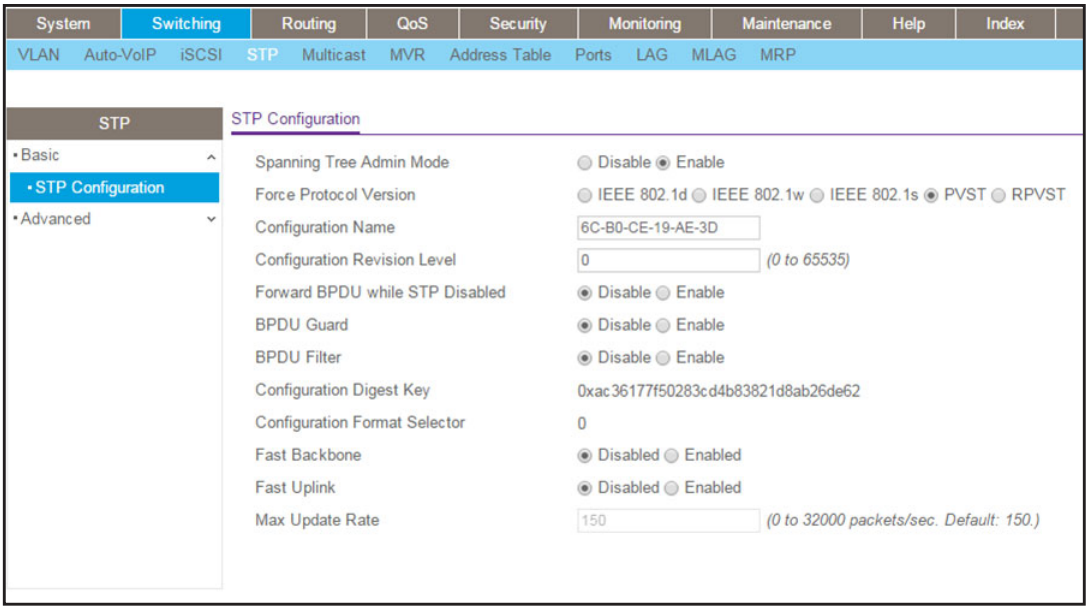
d. Click the **Apply** button. Your settings are saved.

Main UI: Configure PVSTP on Switch 2

To use the main UI to configure PVSTP on Switch 2:

1. Enable PVSTP.
   a. Select **Switching > STP > Basic > STP Configuration**.

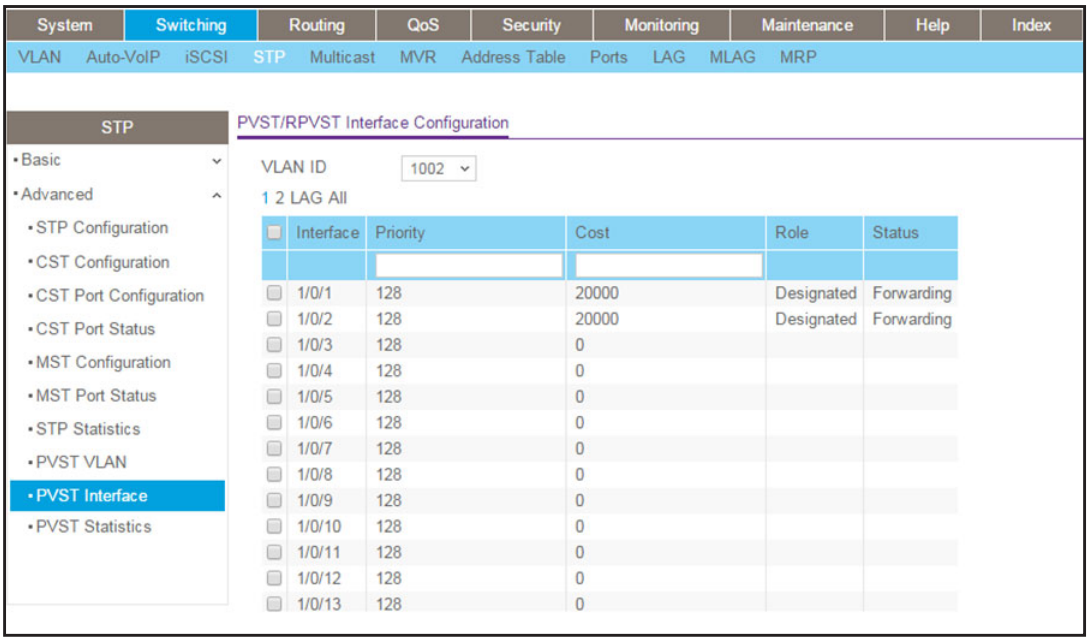
      A page similar to the following figure displays.



   b. Configure the following settings:
      - Select the Spanning Tree Admin Mode **Enable** radio button.
      - Select the Force Protocol Version **PVST** radio button.

   c. Click the **Apply** button. Your settings are saved.
2. Display the PVST status for ports 1/0/1 and 1/0/2 in VLAN 1002.
   a. Select **Switching > STP > Advanced > PVST Interface**.

      A page similar to the following figure displays.



b. From the **VLAN ID** menu, select **1002**.

The roles of ports 1/0/1 and 1/0/2 display.

29

IPv6 Interface Configuration

IPv6 routing and routing VLANs

This feature is supported on the M4250 series switches

This feature is supported on the M4300 series switches

This feature is supported on the M4350 series switches

This chapter includes the following sections:

- Create an IPv6 routing interface
- Create an IPv6 routing VLAN
- Configure DHCPv6 mode on a routing interface

Create an IPv6 routing interface

The example is shown as CLI commands and as a main UI procedure.

CLI: Create an IPv6 routing interface

To use the CLI to create an IPv6 routing interface, ping the interface, and display IPv6 information:

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
```

3. Ping the IPv6 address of interface 1/0/1.

```
(Netgear Switch) #ping ipv6 2000::2
Send count=3, Receive count=3 from 2000::2
Average round trip time = 1.00 ms
```

4. Display information about the IPv6 configuration.

```
(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
```

5. Display information about the IPv6 routing interface.

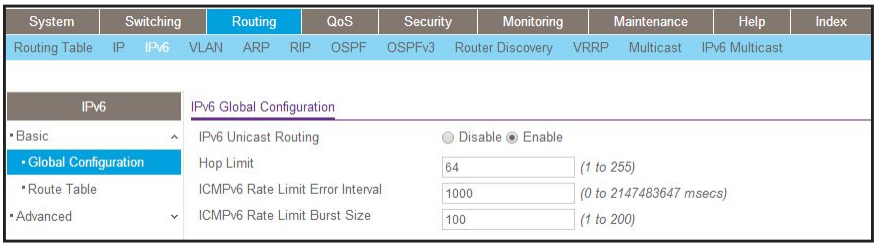
```
(Netgear Switch) #show ipv6 interface 1/0/1
IPv6 is enabled
IPv6 Prefix is ............................... FE80::21E:2AFF:FED9:249B/128
                                                        2000::2/64 [TENT]
Routing Mode.................................. Enabled
Administrative Mode........................... 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
```

Main UI: Create an IPv6 routing interface

To use the main UI to create an IPv6 routing interface and ping the interface:

1. Enable IPv6 forwarding and unicast routing on the switch.
   a. Select **Routing > IPv6 > Basic > Global Configuration**.

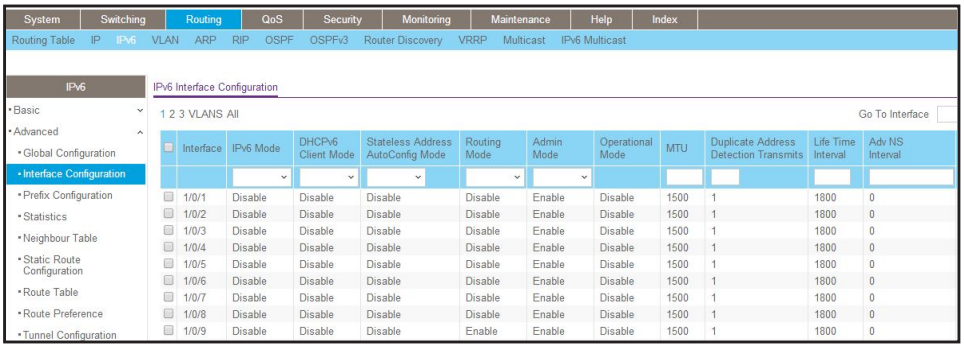
      A page similar to the following figure displays.



   b. Select the IPv6 Unicast Routing **Enable** radio button.
   c. Click the **Apply** button. Your settings are saved.

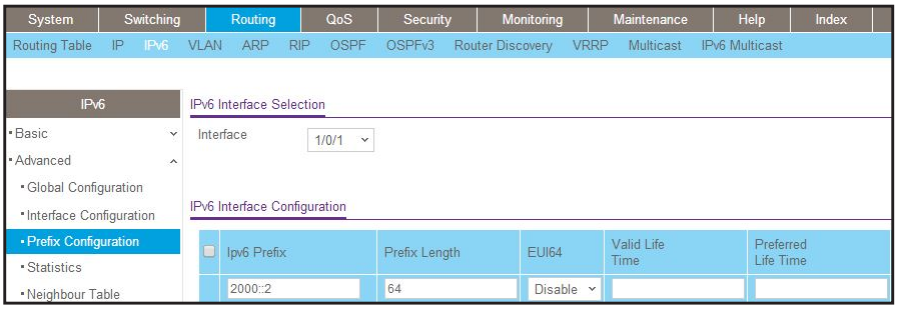
2. Enable IPv6 routing on interface 1/0/1.
   a. Select **Routing > IPv6 > Advanced > Interface Configuration**.

      A page similar to the following figure displays.



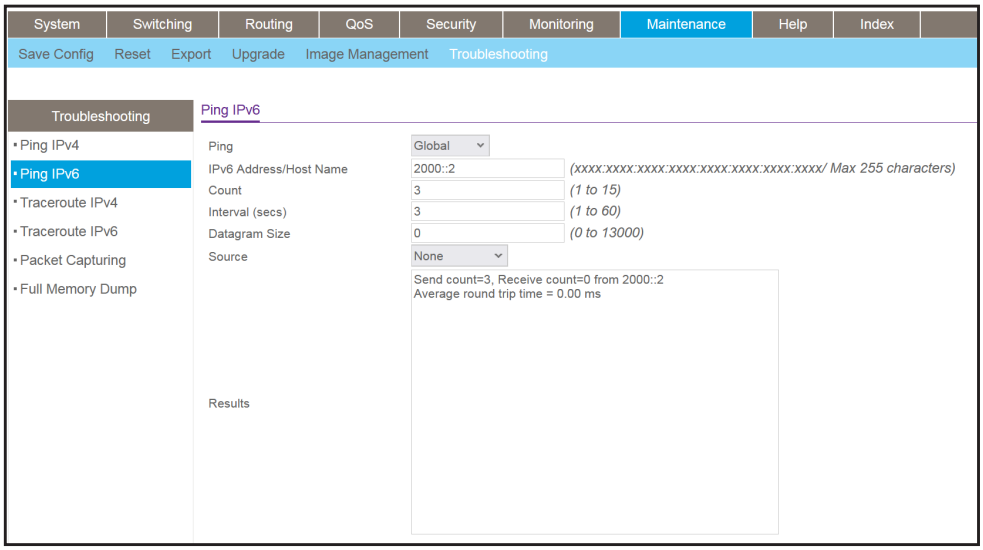
   b. Select the Interface **1/0/1** check box.
   c. In the **IPv6 Mode** menu, select **Enable**.
   d. Click the **Apply** button. Your settings are saved.
3. Assign an IPv6 address to the routing interface.
   a. Select **Routing > IPv6 > Advanced > Prefix Configuration**.

      A page similar to the following figure displays.



   b. In the **Interface** menu, select **1/0/1**.
   c. In the **IPv6 Prefix** field, enter **2000::2**.
   d. In the **Prefix Length** field, enter **64**.
   e. In the **EUI64** menu, select **Disable**.
   f. Click the **Add** button. Your settings are saved.
4. Select **Maintenance > Troubleshooting > Ping IPv6**.

A page similar to the following figure displays.



5. In the **IP Address/Host Name** field, enter **2000::2**.
6. Click the **Apply** button. The ping results display in the Results field.

Create an IPv6 routing VLAN

The example is shown as CLI commands and as a main UI procedure.

CLI: Create an IPv6 routing VLAN

To use the CLI to create a 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 500
(Netgear Switch) (Interface vlan 500)#routing
(Netgear Switch) (Interface vlan 500)#ipv6 enable
(Netgear Switch) (Interface vlan 500)#ipv6 address 2000::1/64
(Netgear Switch) (Interface vlan 500)#exit
```

4. Enable IPv6 forwarding and unicast routing on the switch.

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

5. Ping the IPv6 address of VLAN 500.

```
(Netgear Switch) #ping ipv6 2000::2
Send count=3, Receive count=3 from 2000::2
Average round trip time = 1.00 ms
```

6. Display information about the IPv6 configuration.

```
(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
```

7. Display information about the IPv6 routing interface.

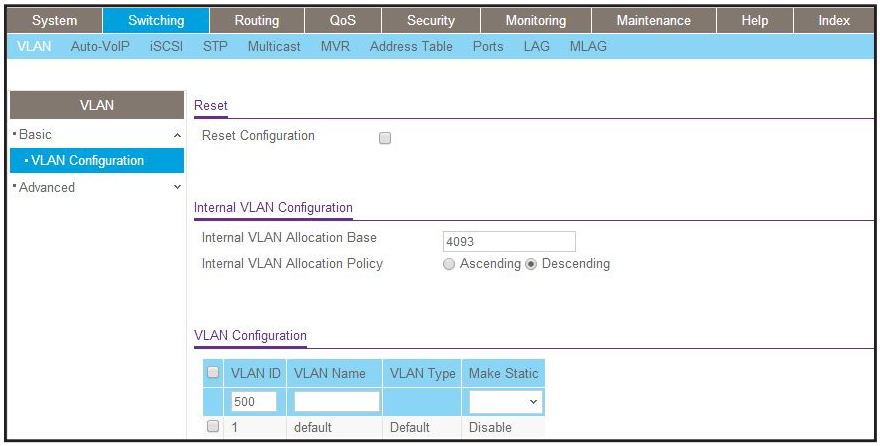
```
(Netgear Switch) #show ipv6 interface vlan 500
IPv6 is enabled
IPv6 Prefix is ............................... FE80::21E:2AFF:FED9:249B/128
                                                          2000::1/64
Routing Mode.................................. Enabled
Administrative Mode........................... 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
```

Main UI: Create an IPv6 VLAN routing Interface

To use the main UI to create a routing VLAN:

1. Create VLAN 500.
   a. Select **Switching > VLAN > Basic > VLAN Configuration**.

      A page similar to the following figure displays.



b. In the **VLAN ID** field, enter **500**.

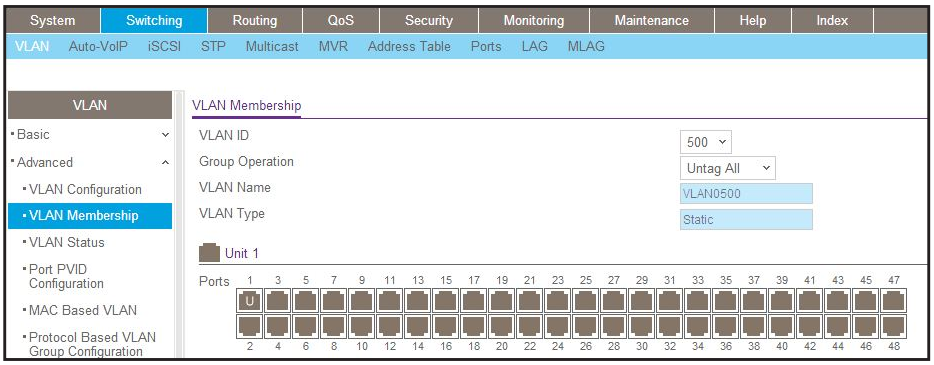
c. In the **Make Static** menu, select **Enable**.

d. Click the **Add** button. Your settings are saved.

2. Add port 1 to VLAN 500.

a. Select **Switching > VLAN > Advanced > VLAN Membership**.

A page similar to the following figure displays.



b. In the **VLAN ID** menu, select **500**.

c. Click the gray box under port **1** until U displays, which specifies that the egress packets are untagged for the port.

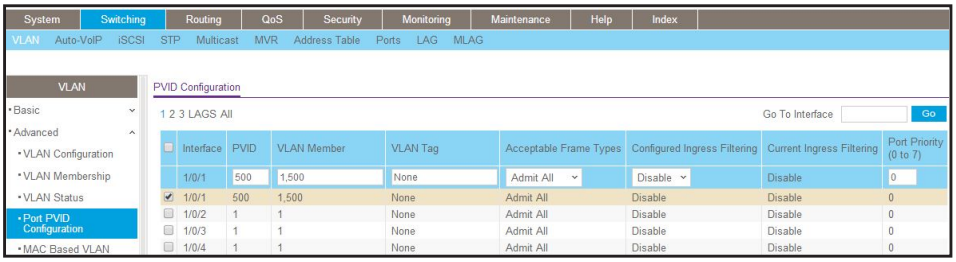
If your switch is a member of a stack, be sure that you select the port in the correct unit.

d. Click the **Apply** button. Your settings are saved.

3. Specify the PVID on port 1/0/1.

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

A page similar to the following figure displays.



b. Select the Interface **1/0/1** check box.

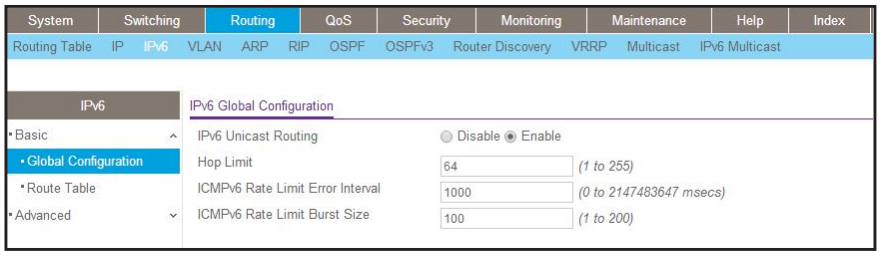
c. In the **PVID** field, enter **500**.

d. Click the **Apply** button. Your settings are saved.

4. Enable IPv6 forwarding and unicast routing on the switch.

a. Select **Routing > IPv6 > Basic > Global Configuration**.

A page similar to the following figure displays.



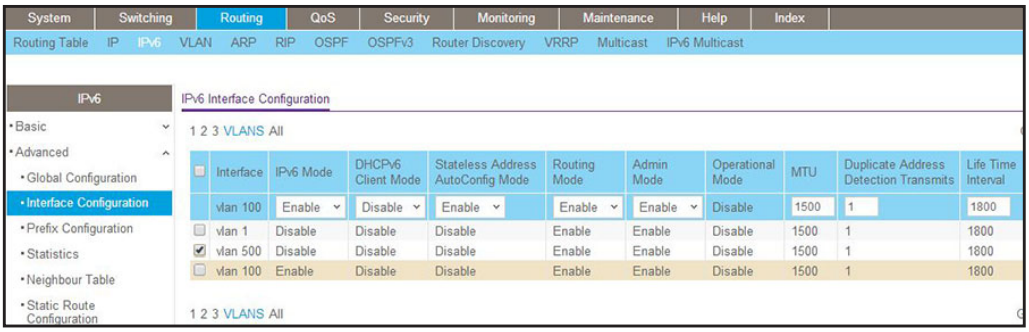
b. Select the IPv6 Unicast Routing **Enable** radio button.

c. Click the **Apply** button. Your settings are saved.

5. Enable IPv6 routing on the VLAN.

a. Select **Routing > IPv6 > Advanced > Interface Configuration**.

A page similar to the following figure displays.



b. Click **VLANS**. The VLAN interfaces displays.

c. Select the **vlan 500** check box.

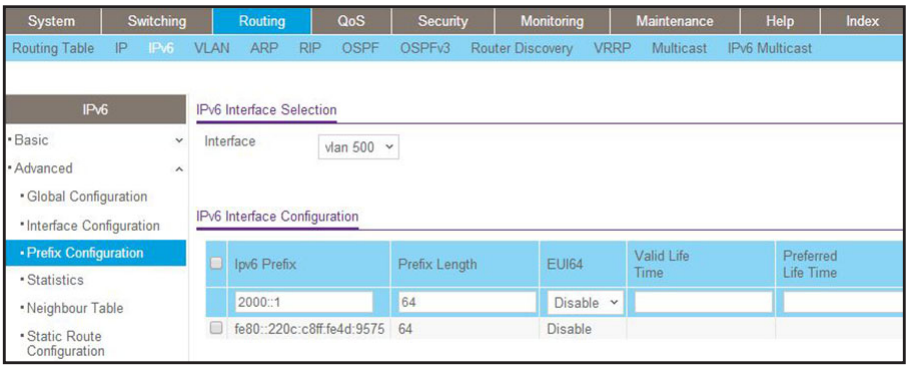
d. In the **IPv6 Mode** menu, select **Enable**.

e. Click the **Apply** button. Your settings are saved.

6. Assign an IPv6 address to the routing VLAN.

a. Select **Routing > IPv6 > Advanced > Prefix Configuration**.

A page similar to the following figure displays.



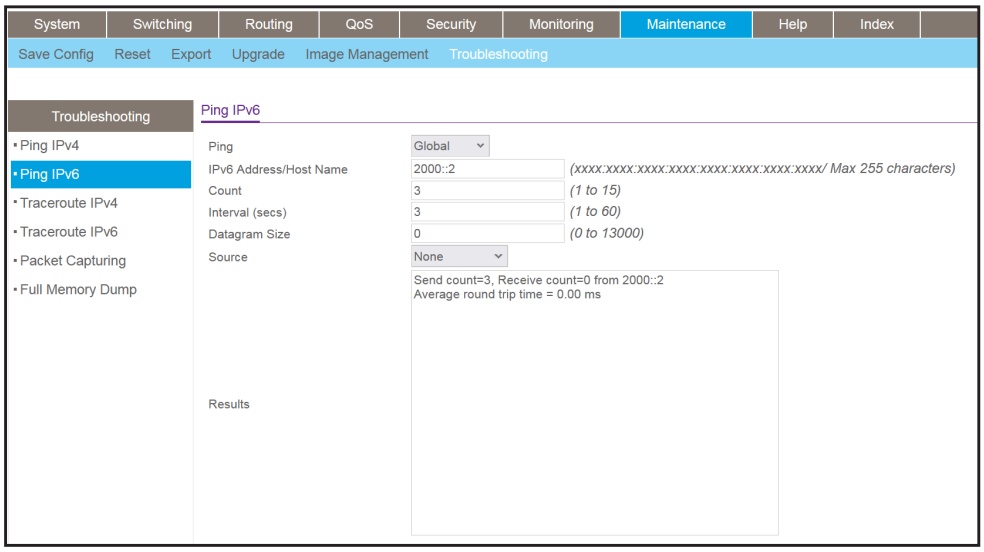
b. In the **Interface** field, select **vlan 500**.

c. In the **IPv6 Prefix** field, enter **2000::1**.

d. In the **Length** field, enter **64**.
e. In the **EUI64** menu, select **Disable**.
f. Click the **Add** button. Your settings are saved.

7. Select **Maintenance > Troubleshooting > Ping IPv6**.

   A page similar to the following figure displays.



8. In the **IP Address/Host Name** field, enter **2000::2**.
9. Click the **Apply** button. The ping results display in the Results field.

Configure DHCPv6 mode on a routing interface

A routing interface supports DHCPv6 mode, which allows a DHCPv6 server to allocate an IPv6 address.

Note: Before you enable DHCPv6 mode, you must disable IPv6 unicast mode globally.

The example is shown as CLI commands and as a main UI procedure.

CLI: Configure DHCPv6 mode on a routing interface

To use the CLI to assign configure DHCPv6 mode on a 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. Display the IPv6 address that is assigned from interface 1/0/23.

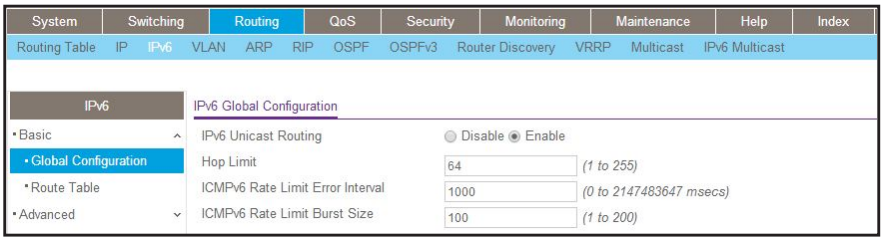
```
(Netgear Switch) #show ipv6 interface 1/0/23
IPv6 is enabled
IPv6 Prefix is ............................... FE80::E291:F5FF:FE06:2BF6/128
                                               2000::1D5C:7CFE:828F:8144/128 [DHCP]
Routing Mode.................................. Enabled
IPv6 Enable Mode.............................. 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
```

Main UI: Configure DHCPv6 mode on a routing Interface

To use the main UI to assign configure DHCPv6 mode on a routing interface:

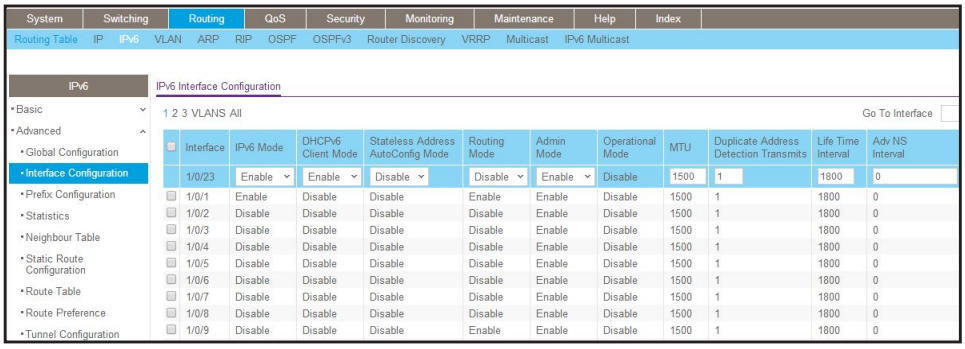
1. Enable IPv6 unicast globally.
   a. Select **Routing > IPv6 > Basic > Global Configuration**.

      A page similar to the following figure displays.



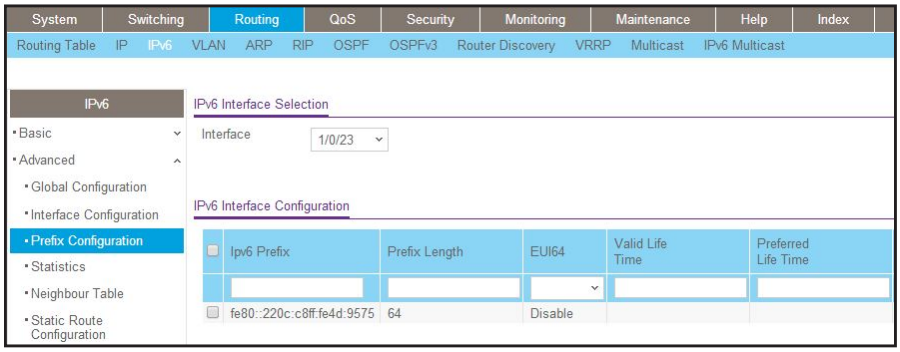
   b. Select the IPv6 Unicast Routing **Enable** radio button.
   c. Click **Apply** to apply the setting.
2. Enable DHCPv6 on interface 1/0/23.
   a. Select **Routing > IPv6 > Advanced > Interface Configuration**.

      A page similar to the following figure displays.



   b. Select the interface **1/0/23** check box.
   c. Configure the following settings:
      - In the **IPv6 Mode** menu, select **Enable**.
      - In the **Routing Mode** menu, select **Enable**.
      - In the **DHCPv6 Client Mode** menu, select **Enable**.
   d. Click **Apply** to apply the settings.
3. Display the IPv6 address that is assigned from interface 1/0/23.
   a. Select **Routing > IPv6 > Advanced > Prefix Configuration**.

A page similar to the following figure displays.



b. In the **Interface** menu, select **1/0/23**.

The IPv6 address assigned by the DHCPv6 server displays.

30

Tunnels for IPv6

6in4 tunnels and 6to4 tunnels

This feature is supported on the M4300 series switches

This chapter includes the following sections:

- IPv6 tunnel concepts
- Create a 6in4 tunnel
- Create a 6to4 tunnel

Note: Tunnels for IPv6 are supported on the M4300 series switches only. The M4250 series and M4350 series switches do not support tunnels for IPv6.

IPv6 tunnel concepts

Two methods exist for IPv6 sites to communicate with each other over the IPv4 network:

- **6in4 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.
- **6to4 tunnel**: 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, a 6in4 tunnel is created between Switch 1 and Switch 2. The tunnel carries IPv6 packets over IPv4 packets.

Figure 57. 6in4 tunnel configuration

The example is shown as CLI commands and as a main UI procedure.

CLI: Create a 6in4 tunnel

You must configure Switch 1 and Switch 2.

CLI: Create a 6in4 tunnel on Switch 1

To use the CLI to create a 6in4 tunnel on Switch 1:

1. Enable routing 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
```

2. Configure a tunnel interface on Switch 1:

```
(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
```

3. Display the tunnel interface on Switch 1 and ping the IPv6 address:

```
(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

To use the CLI to create a 6to4 tunnel on Switch 2:

1. Enable routing 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
```

2. Configure a tunnel interface on Switch 2:

```
(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
```

3. Display the tunnel interface on Switch 2:

```
(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
```

Main UI: Create a 6in4 tunnel

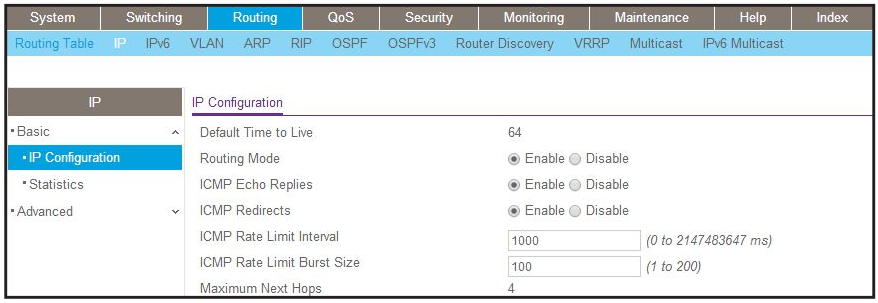
You must configure Switch 1 and Switch 2.

Main UI: Create a 6in4 tunnel on Switch 1

To use the main UI to create a 6in4 tunnel on Switch 1:

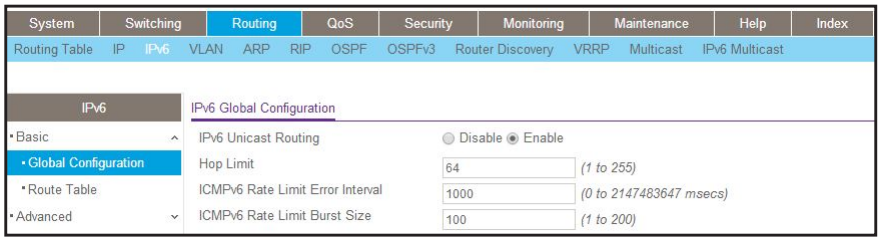
1. Enable IP routing on Switch 1.
   a. Select **Routing > IP > Basic > IP Configuration**.

      A page similar to the following figure displays.



   b. Select the Routing Mode **Enable** radio button.
   c. Click the **Apply** button. Your settings are saved.
2. Enable IPv6 forwarding and unicast routing on Switch 1.
   a. Select **Routing > IPv6 > Basic> Global Configuration**.

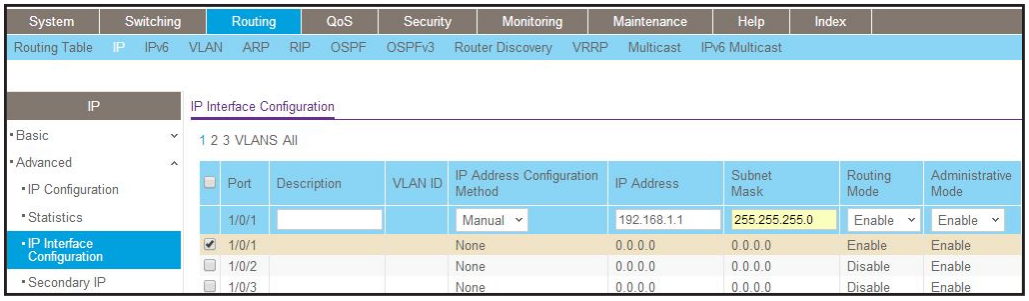
      A page similar to the following figure displays.



   b. Select the IPv6 Unicast Routing **Enable** radio button.
   c. Click the **Apply** button. Your settings are saved.

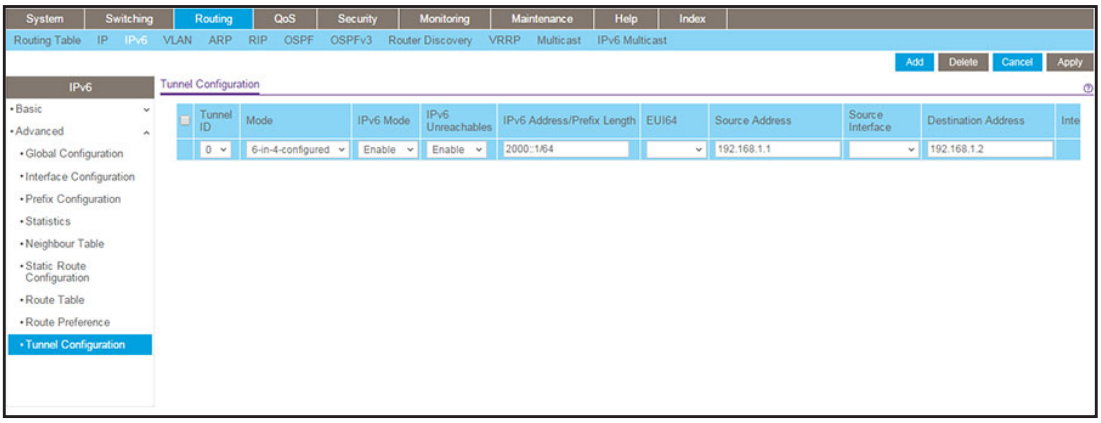
3. Create a routing interface on Switch 1 and assign an IP address to the interface.
   a. Select **Routing > IP > Advanced > IP Interface Configuration**.

      A page similar to the following figure displays.



   b. Select the Port **1/0/1** check box.
   c. Configure the following settings:
      - In the **IP Address** field, enter **192.168.1.1**.
      - In the **Subnet Mask** field, enter **255.255.255.0**.
      - In the **Routing Mode** menu, select **Enable**.
   d. Click the **Apply** button. Your settings are saved.
4. Create a 6-in-4 tunnel interface on Switch 1.
   a. Select **Routing > IPv6 > Advanced > Tunnel Configuration**.

      A page similar to the following figure displays.



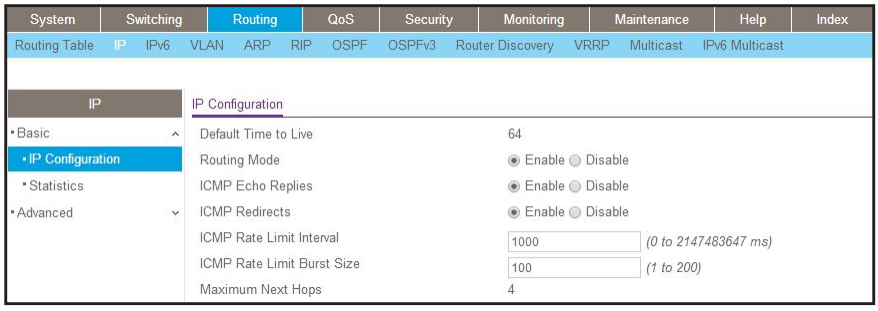
   b. Configure the following settings:
      - In the **Tunnel ID** menu, select **0**.
      - In the **Mode** menu, select **6-in-4-configured**.
      - In the **IPv6 Mode** menu, select **Enable**.
      - In the **IPv6 Address/Prefix Length** field, enter **2000::1/64**.
      - In the **Source Address** field, enter **192.168.1.1**.
      - In the **Destination Address** field, enter **192.168.1.2**.
   c. Click the **Apply** button. Your settings are saved.

Main UI: Create a 6in4 tunnel on Switch 2

To use the main UI to create a 6in4 tunnel on Switch 2:

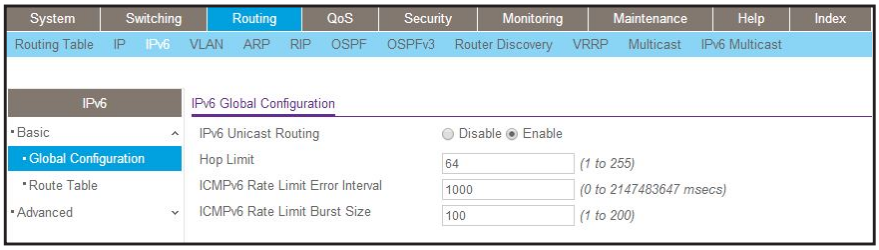
1. Enable IP routing on Switch 2.
   a. Select **Routing > IP > Basic > IP Configuration**.

      A page similar to the following figure displays.



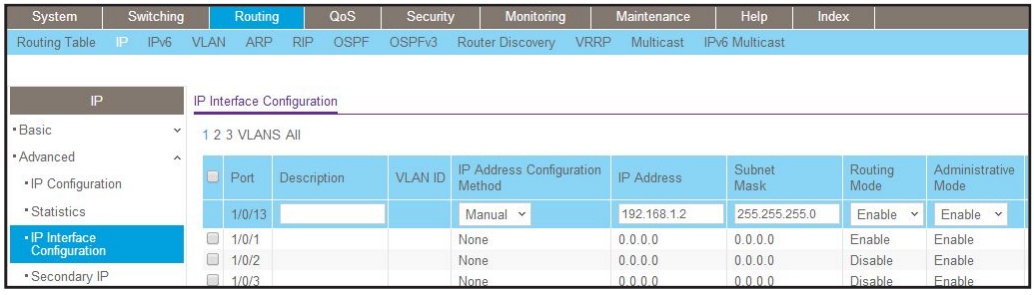
   b. Select the Routing Mode **Enable** radio button.
   c. Click the **Apply** button. Your settings are saved.
2. Enable IPv6 forwarding and unicast routing on Switch 2.
   a. Select **Routing > IPv6 > Basic > Global Configuration**.

      A page similar to the following figure displays.



   b. Select the IPv6 Unicast Routing **Enable** radio button.
   c. Click the **Apply** button. Your settings are saved.
3. Create a routing interface on Switch 2 and assign an IP address to the interface.
   a. Select **Routing > IP > Advanced > IP Interface Configuration**.

      A page similar to the following figure displays.



   b. Select the Port **1/0/13** check box.

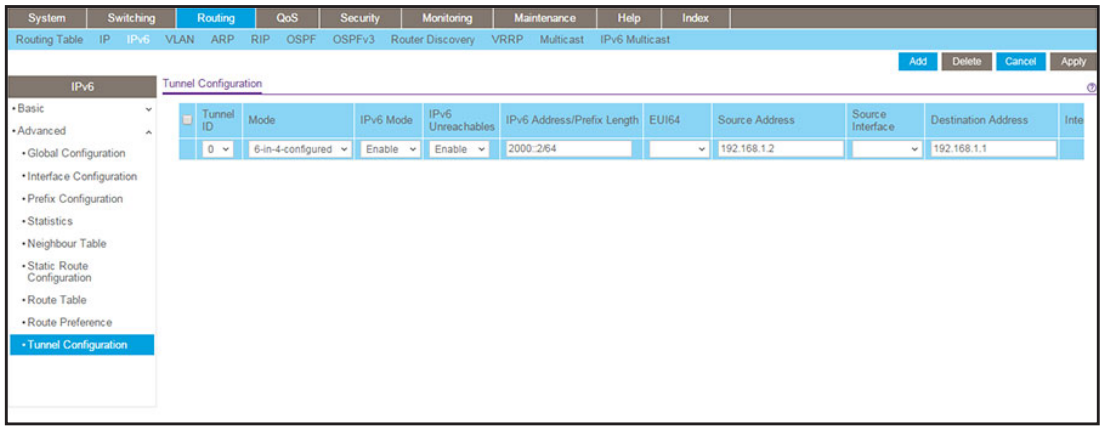
c. Configure the following settings:
   - In the **IP Address** field, enter **192.168.1.2**.
   - In the **Subnet Mask** field, enter **255.255.255.0**.
   - In the **Routing Mode** menu, select **Enable**.

d. Click the **Apply** button. Your settings are saved.

4. Create a 6-in-4 tunnel interface on Switch 2.

a. Select **Routing > IPv6 > Advanced > Tunnel Configuration**.

A page similar to the following figure displays.



b. In the **Tunnel ID** menu, select **0**.

c. In the **Mode** menu, 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 the **Apply** button. Your settings are saved.

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 the 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).

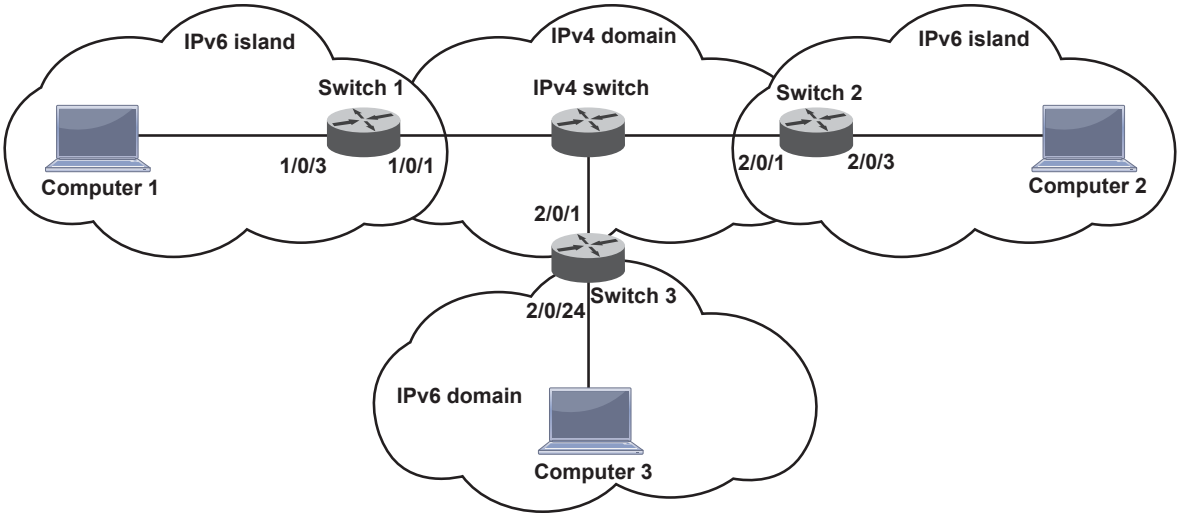


Figure 58. 6to4 tunnel configuration

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.

The example is shown as CLI commands and as a main UI procedure.

CLI: Create a 6to4 tunnel on Switch 1

To use the CLI to 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 an 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 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

To use the CLI to 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 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

To use the CLI to 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 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
```

Main UI: Create a 6to4 tunnel

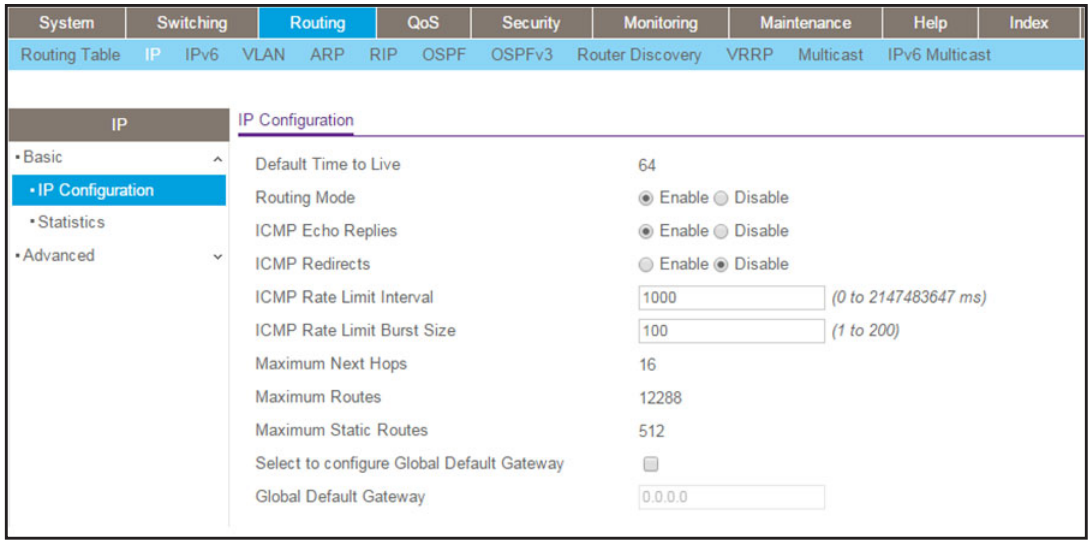
You must configure Switch1, Switch2, and Switch 3.

Main UI: Create a 6to4 tunnel on Switch 1

To use the main UI to create a 6to4 tunnel on Switch 1:

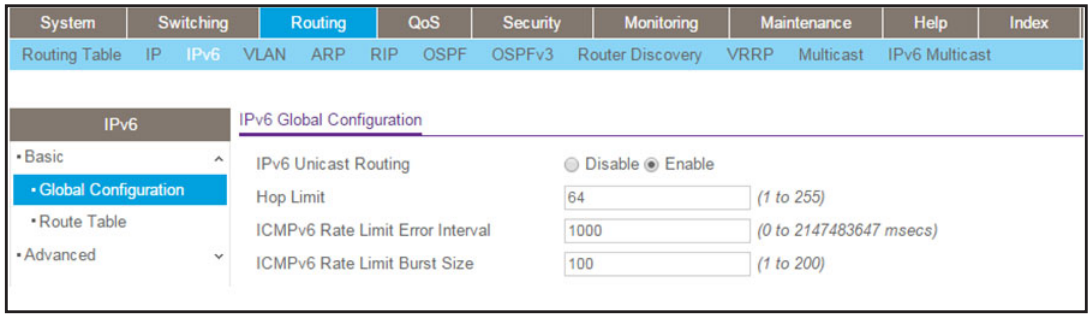
1. Enable IP routing on Switch 1.
   a. Select **Routing > IP > Basic > IP Configuration**.

      A page similar to the following figure displays.



   b. Select the Routing Mode **Enable** radio button.
   c. Click the **Apply** button. Your settings are saved.
2. Enable IPv6 forwarding and unicast routing on Switch 1.
   a. Select **Routing > IPv6 > Basic > Global Configuration**.

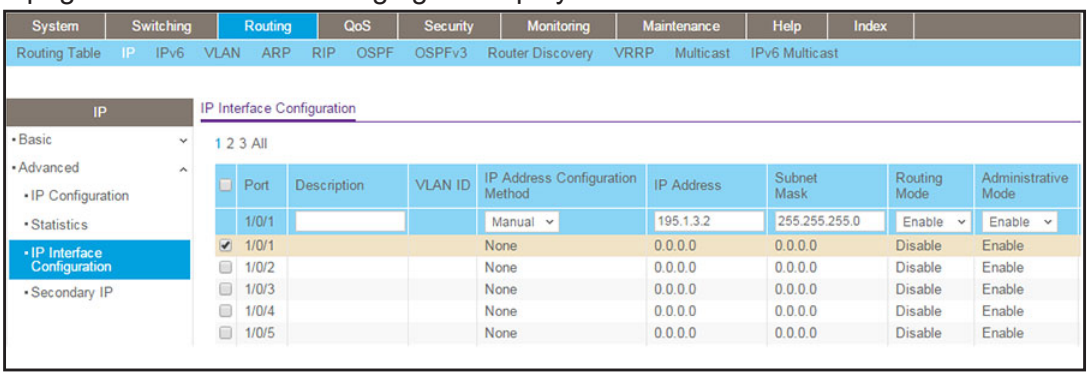
      A page similar to the following figure displays.



   b. Select the IPv6 Unicast Routing **Enable** radio button.
   c. Click the **Apply** button. Your settings are saved.

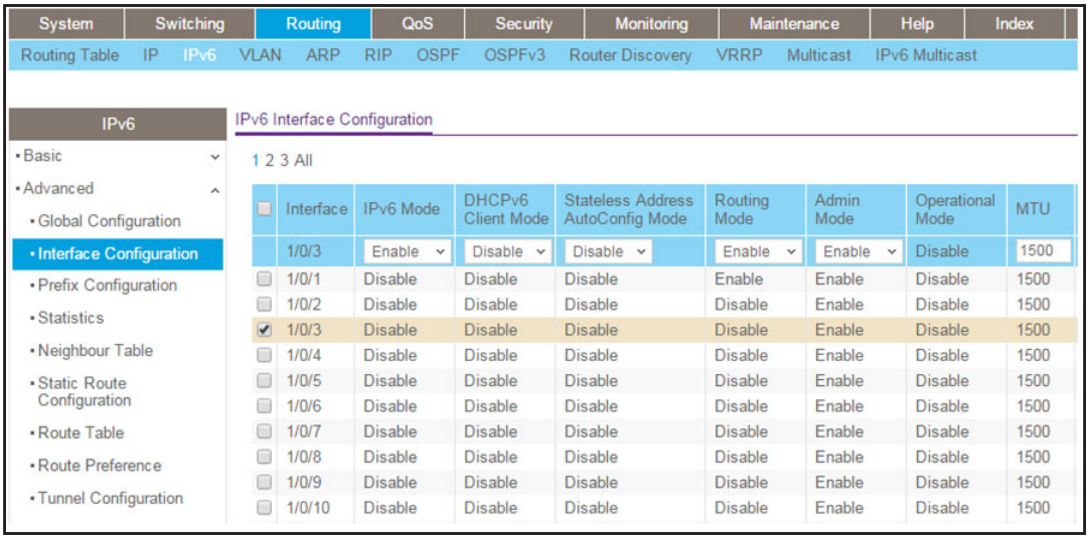
3. Create a routing interface on Switch 1 and assign an IP address to the interface.
   a. Select **Routing > IP > Advanced > IP Interface Configuration**.

      A page similar to the following figure displays.



   b. Select the Port **1/0/1** check box.
   c. Configure the following settings:
      - In the **IP Address Configuration Method** menu, 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** menu, select **Enable**.
   d. Click the **Apply** button. Your settings are saved.
4. Create an IPv6 routing interface on SwitcH 1.
   a. Select **Routing > IPv6 > Advanced > Interface Configuration**.

      A page similar to the following figure displays.



   b. Select the Interface **1/0/3** check.
   c. Configure the following settings:
      - In the **IPv6 Mode** menu, select **Enable**.

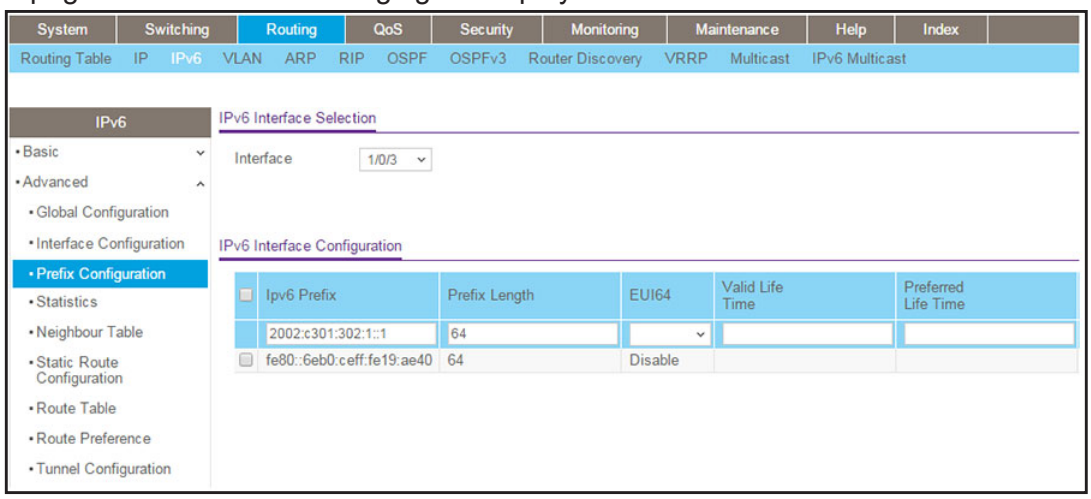
- In the **Routing Mode** menu, select **Enable**.

d. Click the **Apply** button. Your settings are saved.

5. Configure the IPv6 address for IPv6 routing interface 1/0/3 on Switch 1.

a. Select **Routing > IPv6 > Advanced > Prefix Configuration**.

A page similar to the following figure 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:

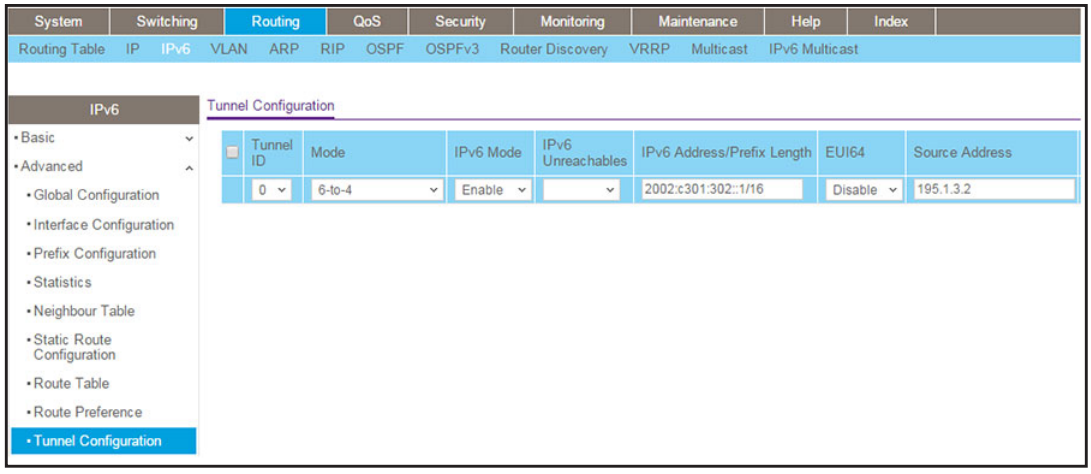
- In the **IPv6 Prefix** field, enter **2002:c301:302:1::1**.
- In the **Prefix Length** field, enter **64**.
- In the **EUI64** menu, select **Disable**.

d. Click the **Add** button. Your settings are saved.

6. Create a 6to4 tunnel interface on Switch 1.

a. Select **Routing > IPv6 > Advanced > Tunnel Configuration**.

A page similar to the following figure displays.



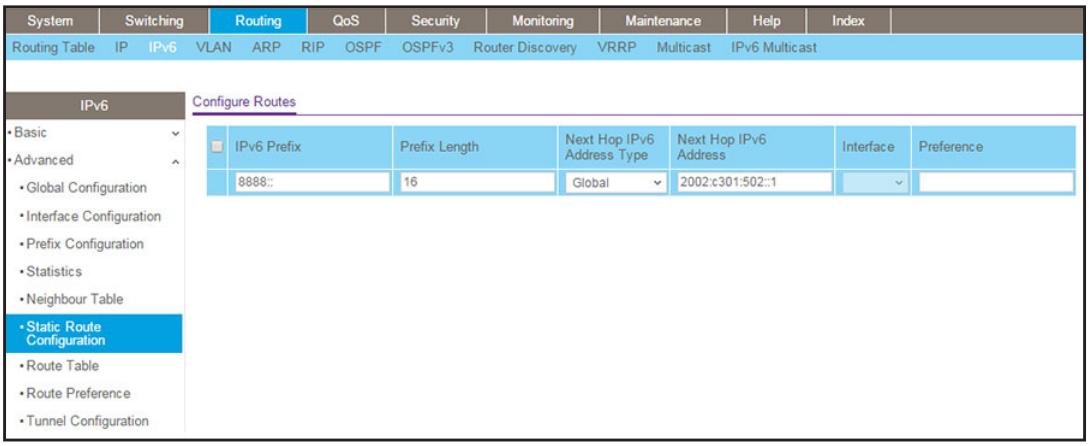
b. Configure the following tunnel settings:
   - In the **Tunnel ID** menu, select **0**.
   - In the **Mode** menu, select **6-to-4**.
   - In the **IPv6 Mode** menu, select **Enable**.
   - In the **IPv6 Address/Prefix Length** field, enter **2002:c301:302::1/16**.
   - In the **EUI64** menu, select **Disable**.
   - In the **Source Address** field, enter **195.1.3.2**.

c. Click the **Add** button. Your settings are saved.

7. Create a default route on Switch 1 for nonnative IPv6 addresses:

a. Select **Routing > IPv6 > Advanced > Static Route Configuration**.

A page similar to the following figure displays.



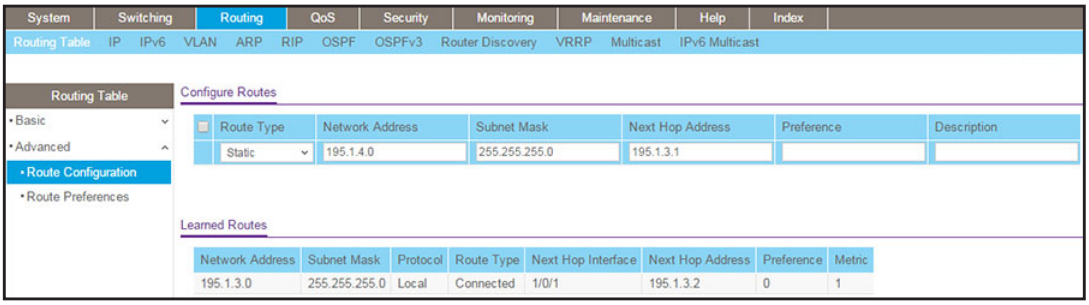
b. Configure the following route settings:
   - In the **IPv6 Prefix** field, enter **8888::**.
   - In the **Prefix Length** field, enter **16**.
   - In the **Next Hop IPv6 Address Type** menu, select **Global**.
   - In the **Next Hop IPv6 Address** field, enter **2002:c301:502::1**.

c. Click the **Add** button. Your settings are saved.

8. Create a static route on Switch 1 for subnet 195.1.4.0/24.

a. Select **Routing > Routing Table > Advanced > Route Configuration**.

A page similar to the following figure displays.



b. Configure the following route settings:

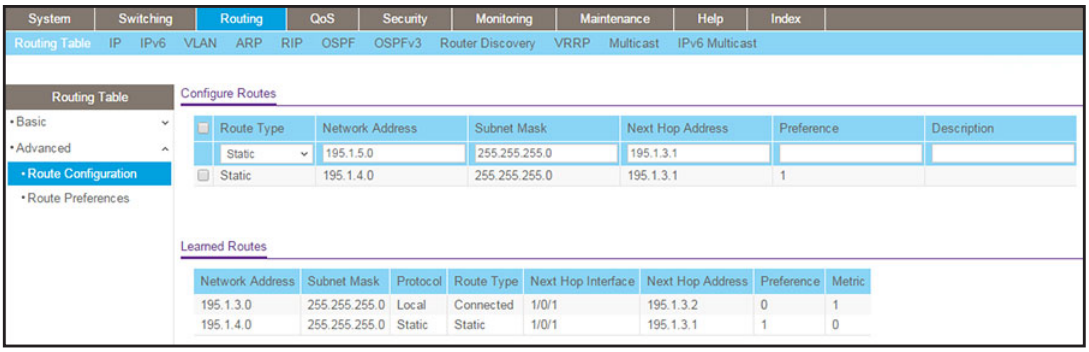
- In the **Route Type** menu, select **Static**.
- In the **Network Address** field, enter **195.1.4.0**.
- In the **Subnet Mask** field, enter **255.255.255.0**.
- In the **Next Hop Address** field, enter **195.1.3.1**.

c. Click the **Add** button. Your settings are saved.

9. Create a static route on Switch 1 for 195.1.5.0/24.

a. Select **Routing > Routing Table > Advanced > Route Configuration**.

A page similar to the following figure displays.



b. Configure the following route settings:

- In the **Route Type** menu, select **Static**.
- 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**.

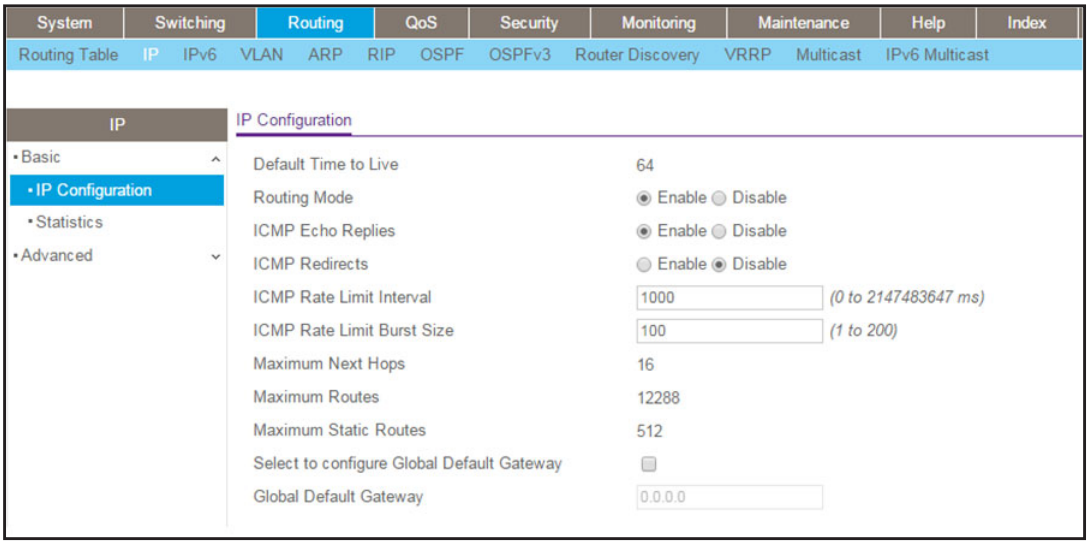
c. Click the **Add** button. Your settings are saved.

Main UI: Create a 6to4 tunnel on Switch 2

To use the main UI to create a 6to4 tunnel on Switch 2:

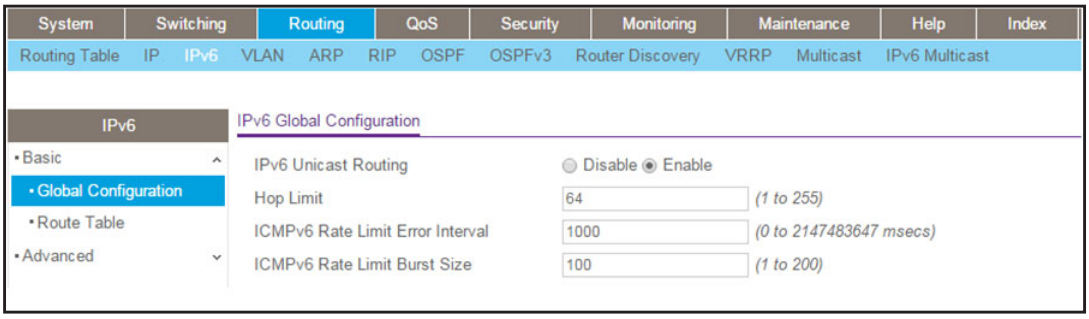
1. Enable IP routing on Switch 2.
   a. Select **Routing > IP > Basic > IP Configuration**.

      A page similar to the following figure displays.



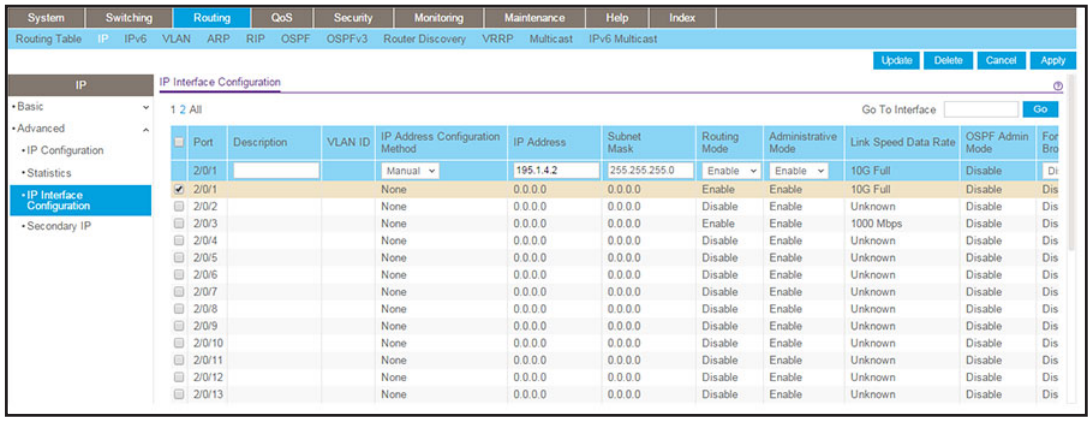
   b. Select the Routing Mode **Enable** radio button.
   c. Click the **Apply** button. Your settings are saved.
2. Enable IPv6 forwarding and unicast routing on Switch 2.
   a. Select **Routing > IPv6 > Basic> Global Configuration**.

      A page similar to the following figure displays.



   b. Select the IPv6 Unicast Routing **Enable** radio button.
   c. Click the **Apply** button. Your settings are saved.
3. Create a routing interface on Switch 2 and assign an IP address to the interface.
   a. Select **Routing > IP > Advanced > IP Interface Configuration**.

A page similar to the following figure displays.



b. Select the Port **2/0/1** check box.

c. Configure the following settings:

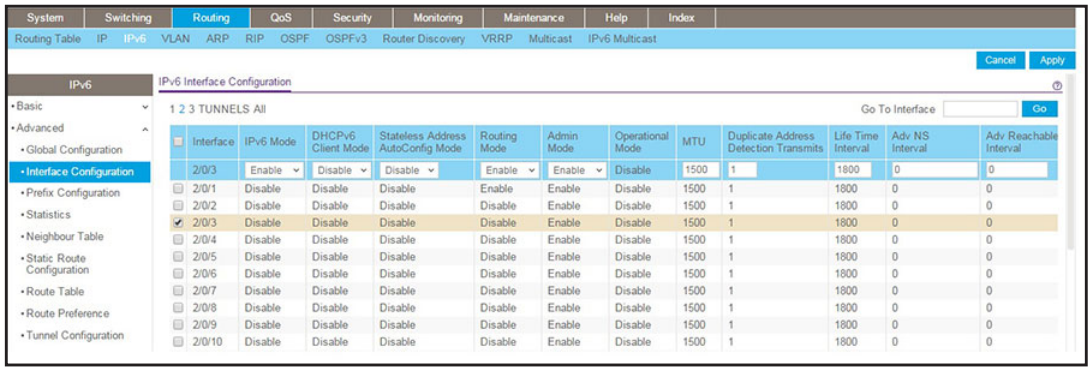
- In the **IP Address Configuration Method** menu, select **Manual**.
- In the **IP Address** field, enter **195.1.4.2**.
- In the **Subnet Mask** field, enter **255.255.255.0**.
- In the **Routing Mode** menu, select **Enable**.

d. Click the **Apply** button. Your settings are saved.

4. Create an IPv6 routing interface on Switch 2.

a. Select **Routing > IPv6 > Advanced > Interface Configuration**.

A page similar to the following figure displays.



b. Select the Interface **2/0/3** check box.

c. Configure the following settings:

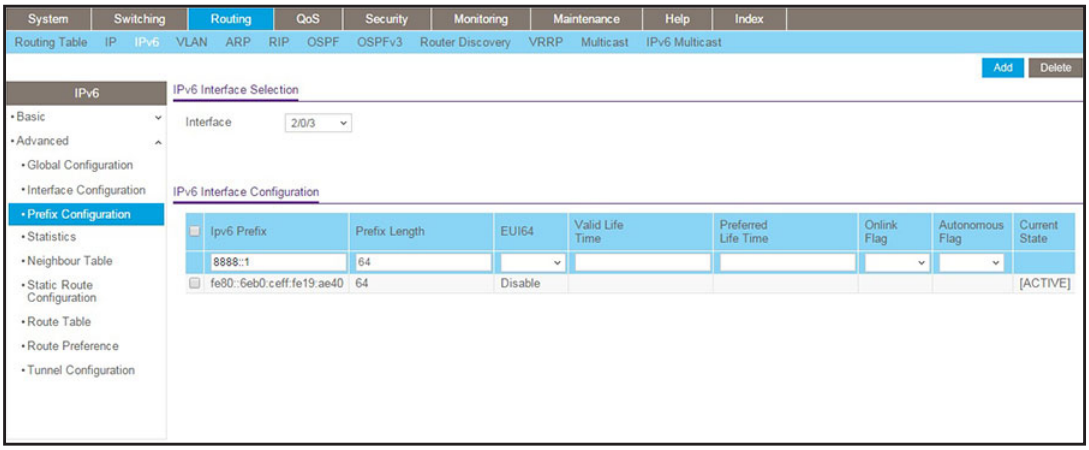
- In the **IPv6 Mode** menu, select **Enable**.
- In the **Routing Mode** menu, select **Enable**.

d. Click the **Apply** button. Your settings are saved.

5. Configure an IPv6 address for routing interface 2/0/3 on Switch 2.

a. Select **Routing > IPv6 > Advanced > Prefix Configuration**.

A page similar to the following figure 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:

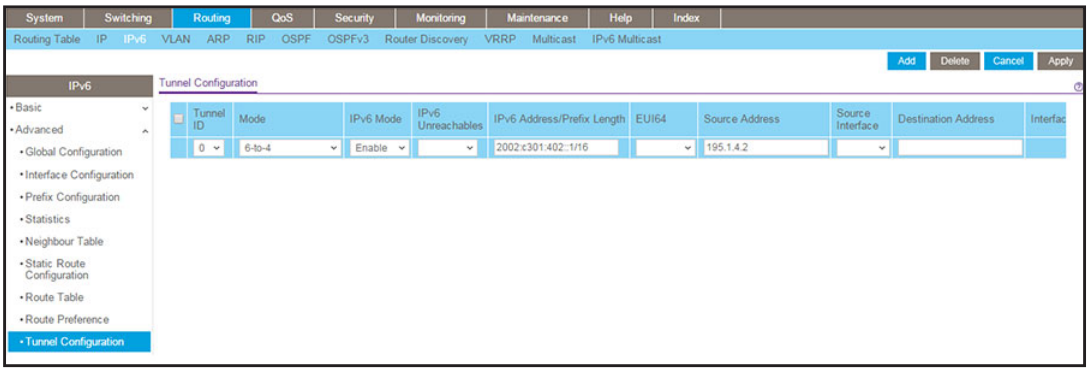
- In the **IPv6 Prefix** field, enter **2002:c301:402:1::1**.
- In the **Prefix Length** field, enter **64**.
- In the **EUI64** menu, select **Disable**.

d. Click the **Add** button. Your settings are saved.

6. Create a 6to4 tunnel interface on Switch 2.

a. Select **Routing > IPv6 > Advanced > Tunnel Configuration**.

A page similar to the following figure displays.



b. Configure the following tunnel settings:

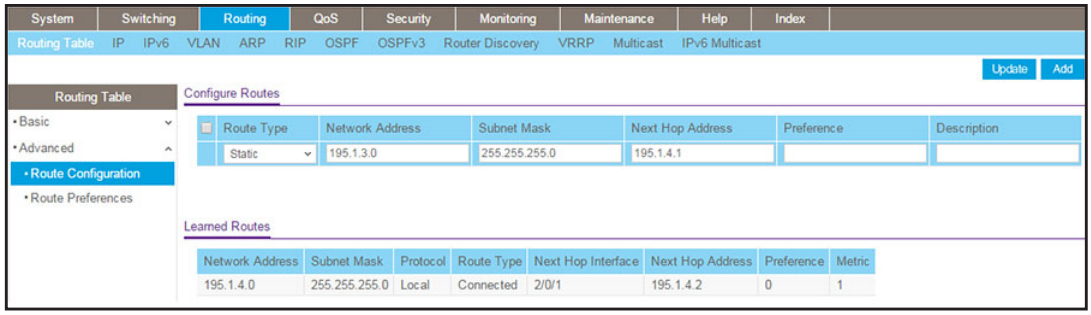
- In the **Tunnel ID** menu, select **0**.
- In the **Mode** menu, select **6-to-4**.
- In the **IPv6 Mode** menu, select **Enable**.
- In the **IPv6 Address/Prefix Length** field, enter **2002:c301:402::1/16**.
- In the **EUI64** menu, select **Disable**.
- In the **Source Address** field, enter **195.1.4.2**.

c. Click the **Add** button. Your settings are saved.

7. Create a static route on Switch 2 for subnet 195.1.3.0/24.

a. Select **Routing > Routing Table > Advanced > Route Configuration**.

A page similar to the following figure displays.



b. Configure the following route settings:

- In the **Route Type** menu, select **Static**.
- 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 the **Add** button. Your settings are saved.

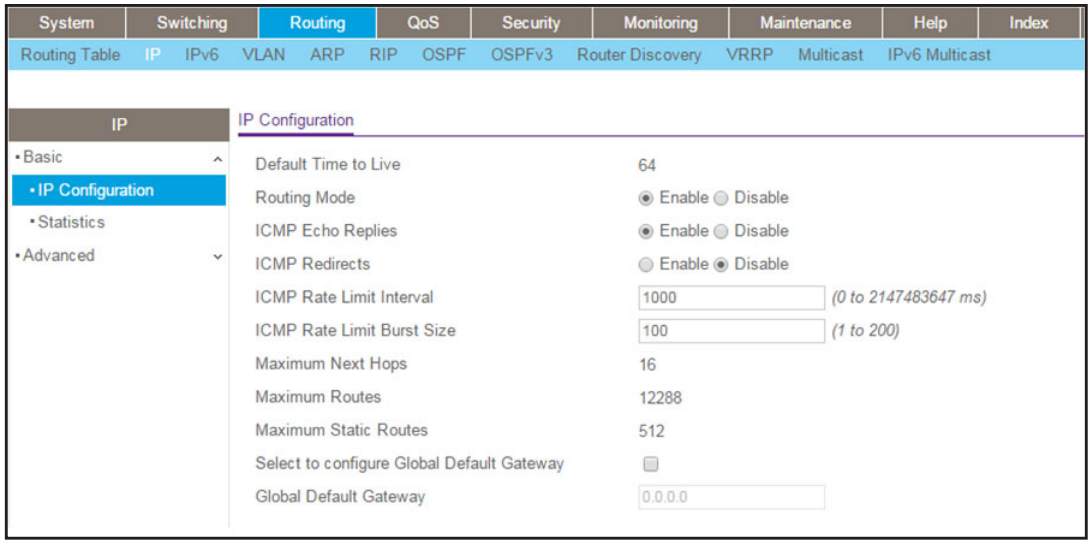
Main UI: Create a 6to4 tunnel on Switch 3

To use the main UI to create a 6to4 tunnel on Switch 3:

1. Enable IP routing on Switch 3.

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

A page similar to the following figure displays.



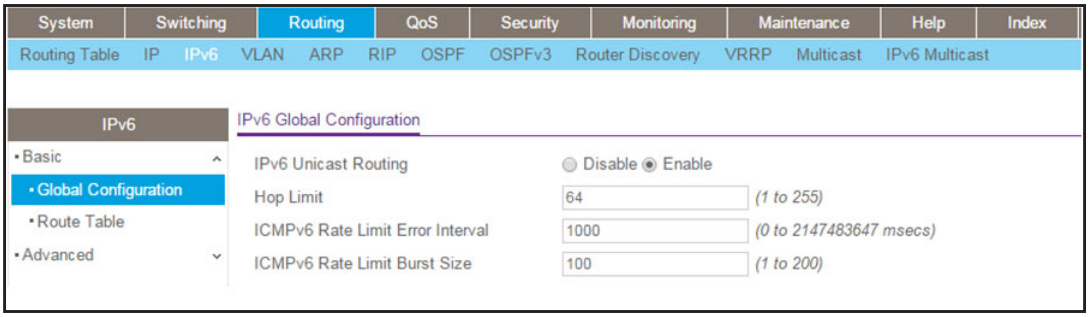
b. Select the Routing Mode **Enable** radio button.

c. Click the **Apply** button. Your settings are saved.

2. Enable IPv6 forwarding and unicast routing on Switch 3.

a. Select **Routing > IPv6 > Basic> Global Configuration**.

A page similar to the following figure displays.



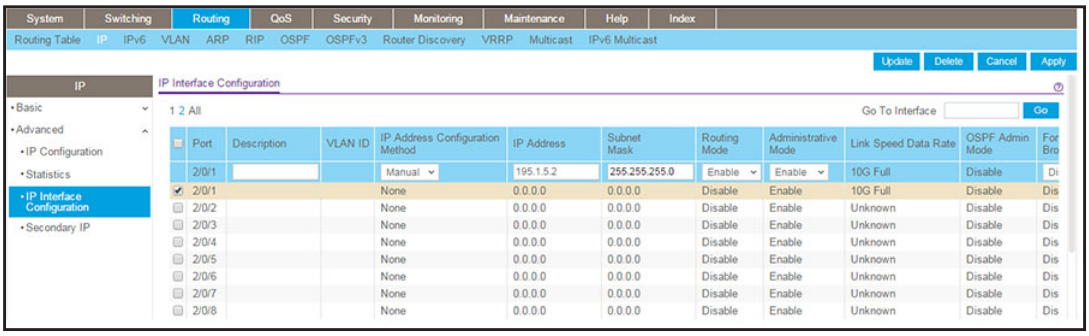
b. Select the IPv6 Unicast Routing **Enable** radio button.

c. Click the **Apply** button. Your settings are saved.

3. Create a routing interface on Switch 3 and assign an IP address to the interface.

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

A page similar to the following figure displays.



b. Select the Port **2/0/1** check box.

c. Configure the following settings:

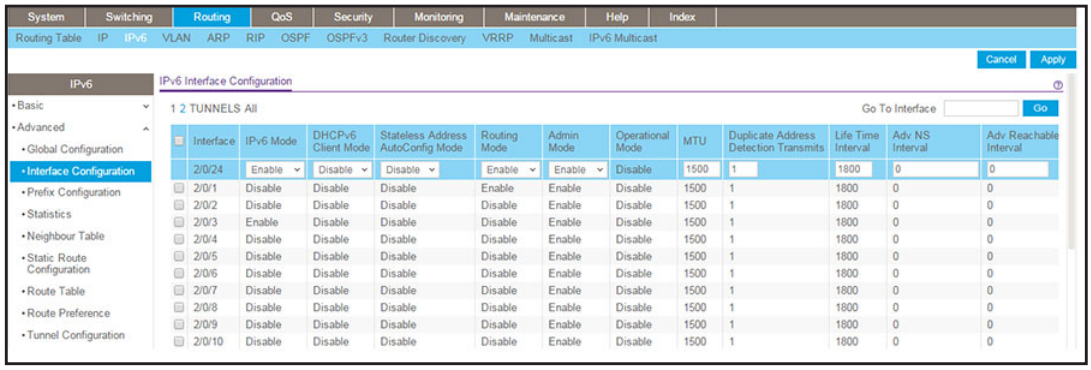
- In the **IP Address Configuration Method** menu, select **Manual**.
- In the **IP Address** field, enter **195.1.5.2**.
- In the **Subnet Mask** field, enter **255.255.255.0**.
- In the **Routing Mode** menu, select **Enable**.

d. Click the **Apply** button. Your settings are saved.

4. Create an IPv6 routing interface on Switch 3.

a. Select **Routing > IPv6 > Advanced > Interface Configuration**.

A page similar to the following figure displays.



b. Select the Interface **2/0/24** check box.

c. Configure the following settings:

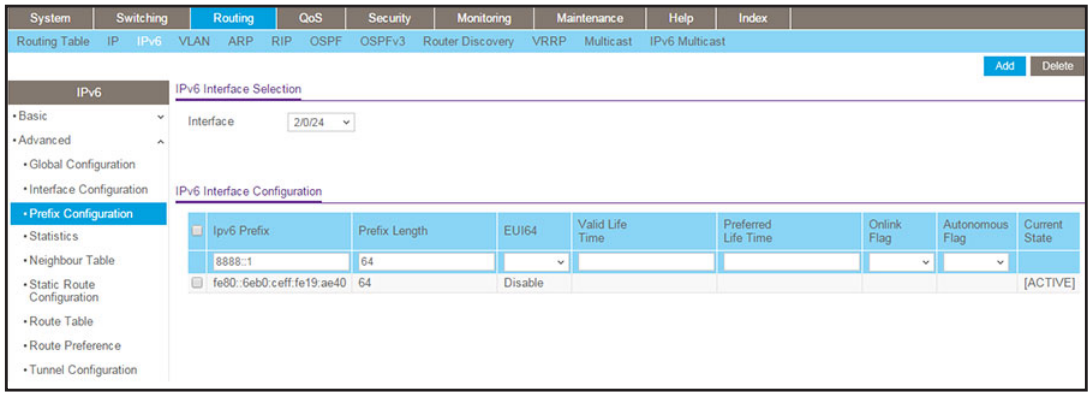
- In the **IPv6 Mode** menu, select **Enable**.
- In the **Routing Mode** menu, select **Enable**.

d. Click the **Apply** button. Your settings are saved.

5. Configure the IPv6 address on Switch 3 for the IPv6 routing interface 2/0/24.

a. Select **Routing > IPv6 > Advanced > Prefix Configuration**.

A page similar to the following figure 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:

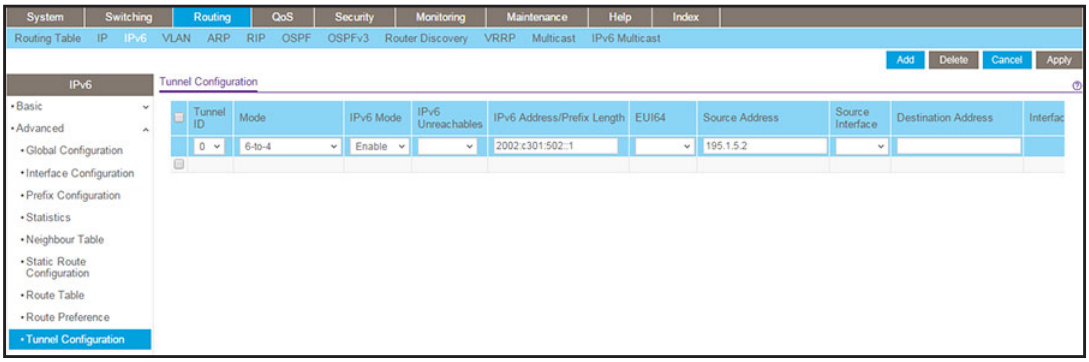
- In the **IPv6 Prefix** field, enter **8888::1**.
- In the **Prefix Length** field, enter **64**.
- In the **EUI64** menu, select **Disable**.

d. Click the **Add** button. Your settings are saved.

6. Create 6to4 tunnel interfaces on Switch 3.

a. Select **Routing > IPv6 > Advanced > Tunnel Configuration**.

A page similar to the following figure displays.



b. Configure the following tunnel settings:

- In the **Tunnel ID** menu, select **0**.
- In the **Mode** menu, select **6-to-4**.
- In the **IPv6 Mode** menu, select **Enable**.
- In the **IPv6 Address/Prefix Length** field, enter **2002:c301:402::1/16**.
- In the **EUI64** menu, select **Disable**.
- In the **Source Address** field, enter **195.1.4.2**.

c. Click the **Add** button. Your settings are saved.

d. Configure the following tunnel settings:

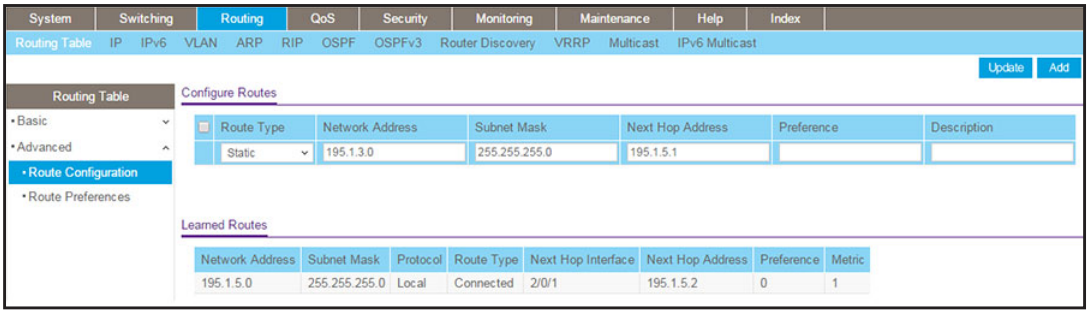
- In the **Tunnel ID** menu, select **0**.
- In the **Mode** menu, select **6-to-4**.
- In the **IPv6 Mode** menu, select **Enable**.
- In the **IPv6 Address/Prefix Length** field, enter **2002:c301:502::1/16**.
- In the **EUI64** menu, select **Disable**.
- In the **Source Address** field, enter **195.1.5.2**.

e. Click the **Add** button. Your settings are saved.

7. Create a static route on Switch 3 for subnet 195.1.3.0/24.

a. Select **Routing > Routing Table > Advanced > Route Configuration**.

A page similar to the following figure displays.



b. Configure the following route settings:

- In the **Route Type** menu, select **Static**.
- 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 the **Add** button. Your settings are saved.

31

PIM

Protocol Independent Multicast

This feature is supported on the M4250 series switches

This feature is supported on the M4300 series switches

This feature is supported on the M4350 series switches

This chapter includes the following sections:

- Protocol Independent Multicast concepts
- PIM-DM
- PIM-SM

Protocol Independent Multicast concepts

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. PIM is a widely used multicast routing protocol.

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.

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 IPv4 configuration only; IPv6 configuration is similar to IPv4 configuration.

Two types of PIM exist:

- 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

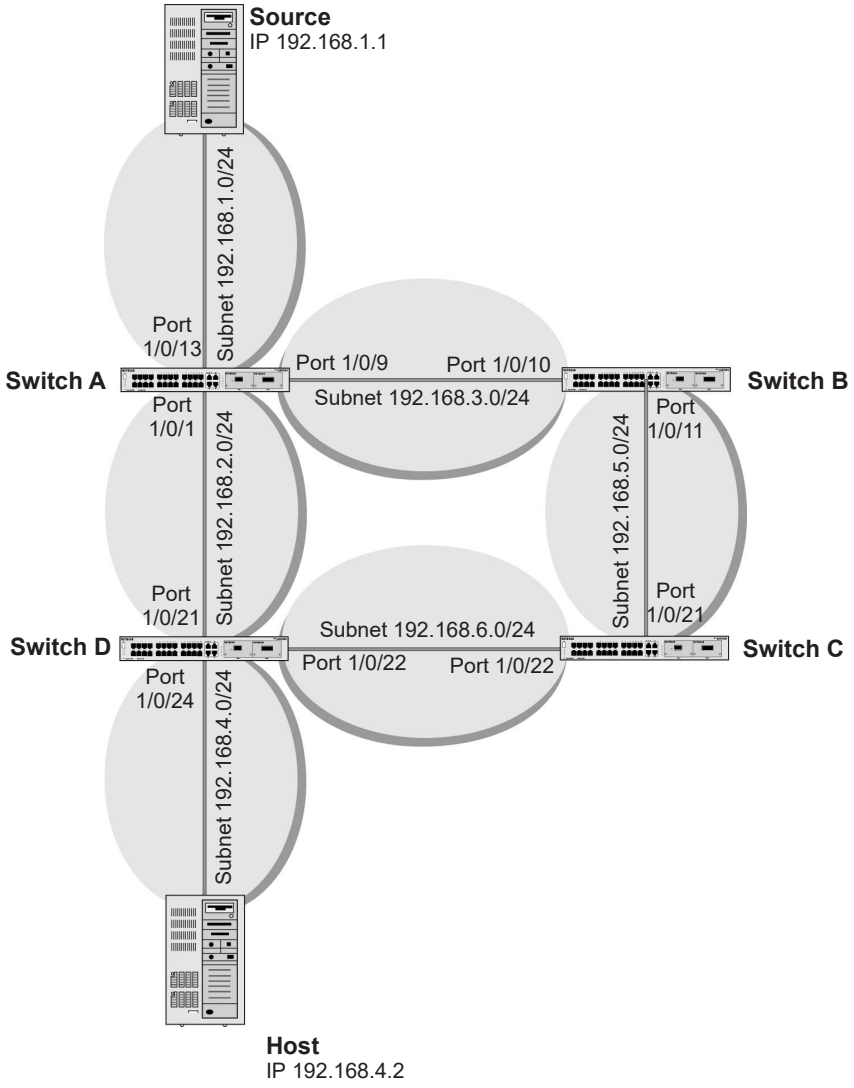


Figure 59. Configuring and Using PIM-DM

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 is built on the assumption 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 that are 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 that is directly attached to the source.

Two versions of PIM-DM exist:

- **Version 1**: This version uses IGMP messages, including query messages.
- **Version 2**: This version does not use IGMP messages; instead, it uses a message that is encapsulated in IP packets with protocol number 103. This means that version 2 replaces the query message of version 1 with the Hello message.

The example is shown as CLI commands and as a main UI procedure.

CLI: Configure PIM-DM

You must configure PIM-DM on Switch A, Switch B, Switch C, and Switch D.

CLI: Configure PIM-DM on Switch A

To use the CLI to configure PIM-DM on Switch A:

1. Enable IP routing, PIM-DM, and IP multicast forwarding on Switch A.

```
(Netgear Switch) #configure
(Netgear Switch) (Config)#ip routing
(Netgear Switch) (Config)#ip pim dense
(Netgear Switch) (Config)#ip multicast
```

2. Enable routing, RIP, and PIM on interface 1/0/1 of Switch A.

```
(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
```

3. Enable routing, RIP, and PIM on interface 1/0/9 of Switch A.

```
(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
```

4. Enable routing, RIP, and PIM on interface 1/0/13 of Switch A.

```
(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
```

CLI: Configure PIM on Switch B

To use the CLI to configure PIM on Switch B:

1. Enable IP routing, PIM-DM, and IP multicast forwarding on Switch B.

```
(Netgear Switch) #configure
(Netgear Switch) (Config)#ip routing
(Netgear Switch) (Config)#ip pim dense
(Netgear Switch) (Config)#ip multicast
```

2. Enable routing, RIP, and PIM on interface 1/0/10 of Switch B.

```
(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
```

3. Enable routing, RIP, and PIM on interface 1/0/11 of Switch B.

```
(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
```

CLI: Configure PIM-DM on Switch C

To use the CLI to configure PIM-DM on Switch C:

1. Enable IP routing, PIM-DM, and IP multicast forwarding on Switch C.

```
(Netgear Switch) #configure
(Netgear Switch) (Config)#ip routing
(Netgear Switch) (Config)#ip pim dense
(Netgear Switch) (Config)#ip multicast
```

2. Enable routing, RIP, and PIM on interface 1/0/21 of Switch C.

```
(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
```

3. Enable routing, RIP, and PIM on interface 1/0/22 of Switch C.

```
(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
```

CLI: Configure PIM-DM on Switch D

To use the CLI to configure PIM-DM on Switch D:

1. Enable IP routing, PIM-DM, and IP multicast forwarding on Switch D.

```
(Netgear Switch) #configure
(Netgear Switch) (Config)#ip routing
(Netgear Switch) (Config)#ip pim dense
(Netgear Switch) (Config)#ip igmp
(Netgear Switch) (Config)#ip multicast
```

2. Enable routing, RIP, and PIM on interface 1/0/21 of Switch D.

```
(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
```

3. Enable routing, RIP, and PIM on interface 1/0/22 of Switch D.

```
(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
```

4. Enable routing, IGMP, RIP, and PIM on interface 1/0/24 of Switch D.

```
(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 igmp
(Netgear Switch) (Interface 1/0/24)#ip rip
(Netgear Switch) (Interface 1/0/24)#ip pim
(Netgear Switch) (Interface 1/0/24)#exit
```

CLI: Display the multicast route table on Switches A, B, C, and D

To use the CLI to display the multicast route table on Switches A, B, C, and D:

```
(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


(Switch 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


(Switch 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


(Switch 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
```

Main UI: Configure PIM-DM

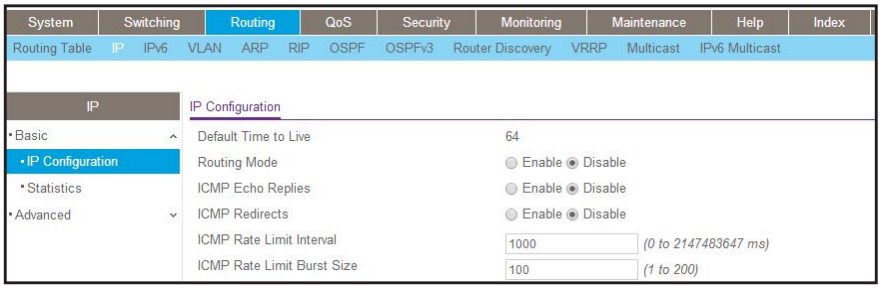
You must configure PIM-DM on Switch A, Switch B, Switch C, and Switch D.

Main UI: Configure PIM-DM on Switch A

To use the main UI to configure PIM-DM on Switch A:

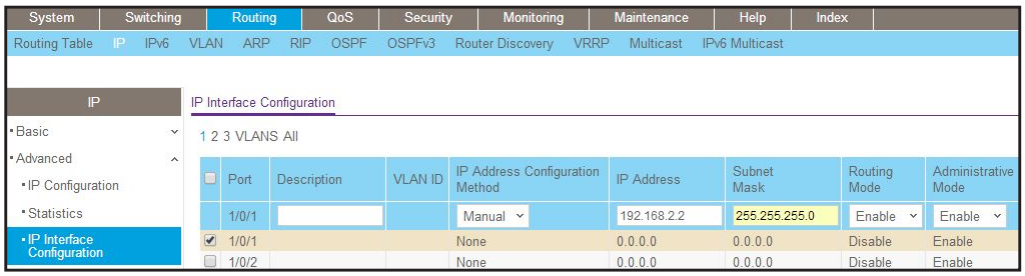
1. Enable IP routing on Switch A.
   a. Select **Routing > IP > Basic > IP Configuration**.

      A page similar to the following figure displays.



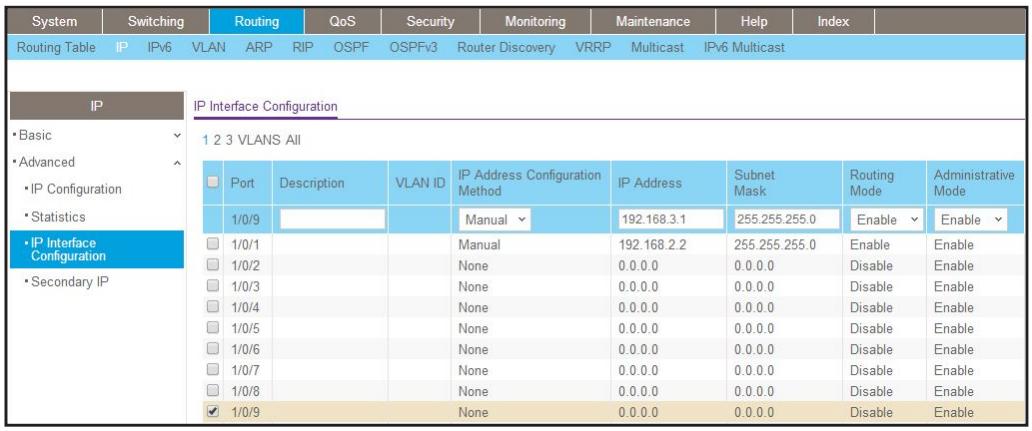
   b. Select the Routing Mode **Enable** radio button.
   c. Click the **Apply** button. Your settings are saved.
2. Configure routing on interface 1/0/1 and assign an IP address to the interface.
   a. Select **Routing > IP > Advanced > IP Interface Configuration**.

      A page similar to the following figure displays.

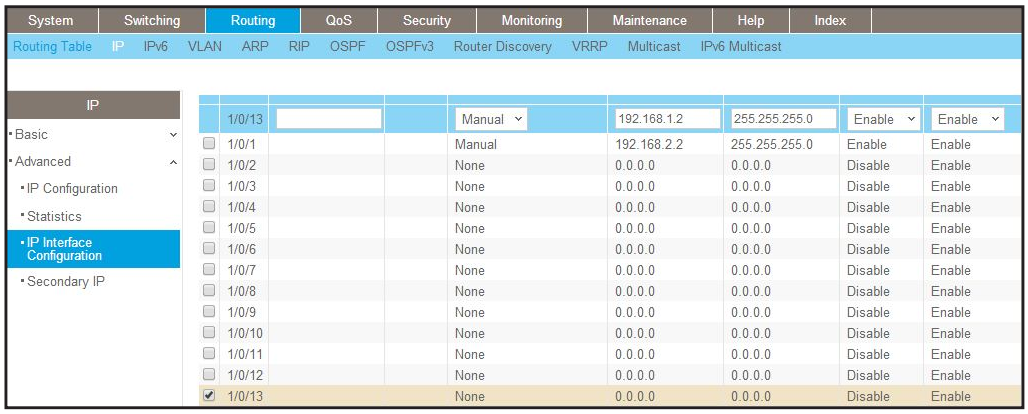


   b. Select the Port **1/0/1** check box.
   c. Configure the following settings:
      - In the **IP Address** field, enter **192.168.2.2**.
      - In the **Subnet Mask** field, enter **255.255.255.0**.
      - In the **Routing Mode** menu, select **Enable**.
   d. Click the **Apply** button. Your settings are saved.

3. Configure routing on interface 1/0/9 and assign an IP address to the interface.
   a. Remain on the same page.

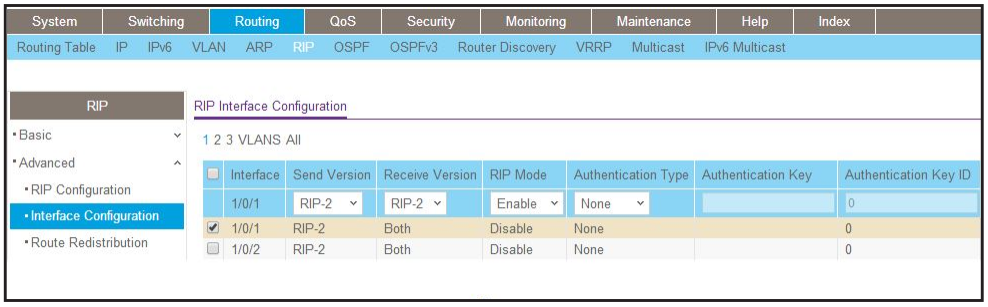


   b. Select the Port **1/0/9** check box.
   c. Configure the following settings:
      - In the **IP Address** field, enter **192.168.3.1**.
      - In the **Subnet Mask** field, enter **255.255.255.0**.
      - In the **Routing Mode** menu, select **Enable**.
   d. Click the **Apply** button. Your settings are saved.
4. Configure routing on interface 1/0/13 and assign an IP address to the interface.
   a. Remain on the same page.



   b. Select the Port **1/0/13** check box.
   c. Configure the following settings:
      - In the **IP Address** field, enter **192.168.1.2**.
      - In the **Subnet Mask** field, enter **255.255.255.0**.
      - In the **Routing Mode** menu, select **Enable**.
   d. Click the **Apply** button. Your settings are saved.
5. Enable RIP on the interface 1/0/1.
   a. Select **Routing > RIP > Advanced > Interface Configuration**.

A page similar to the following figure displays.



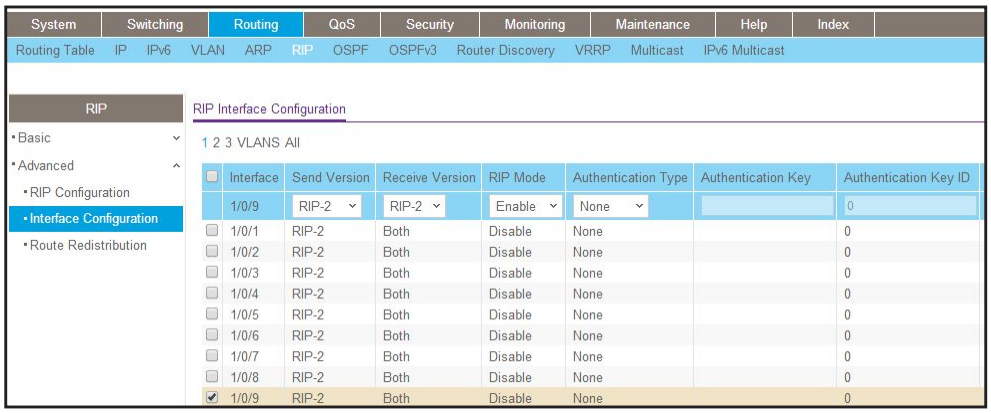
b. Select the Interface **1/0/1** check box.

c. In the **RIP Mode** menu, select **Enable**.

d. Click the **Apply** button. Your settings are saved.

6. Enable RIP on interface 1/0/9.

a. Remain on the same page.

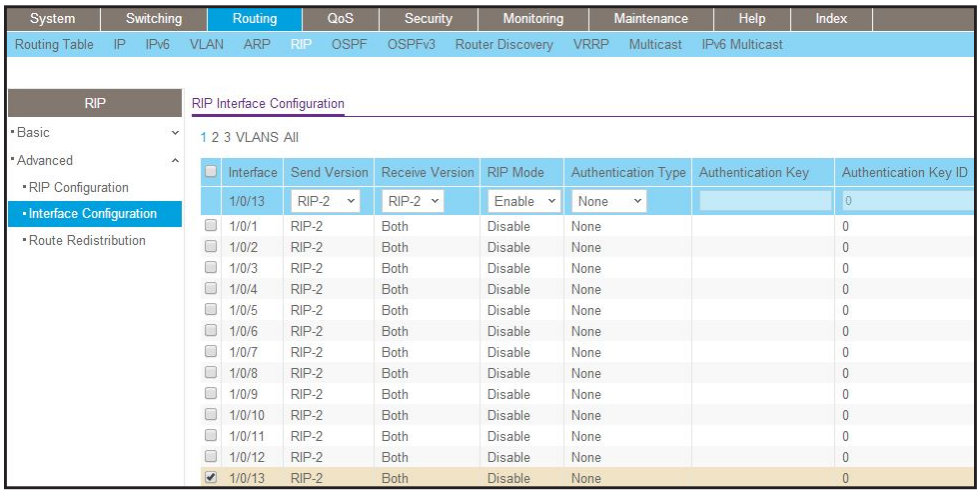


b. Select the Interface **1/0/9** check box.

c. In the **RIP Mode** menu, select **Enable**.

d. Click the **Apply** button. Your settings are saved.

7. Enable RIP on interface 1/0/13.
   a. Remain on the same page.

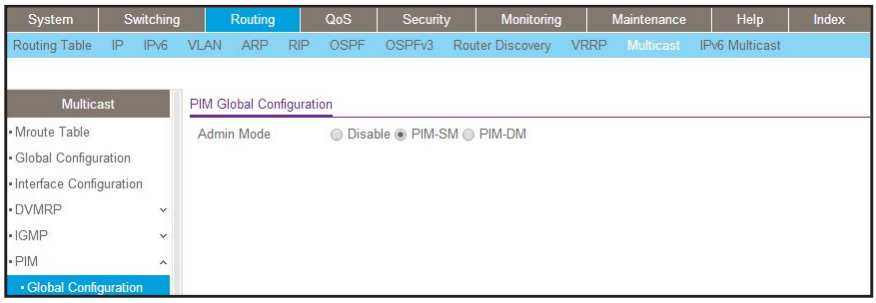


   b. Select the Interface **1/0/13** check box.
   c. In the **RIP Mode** menu, select **Enable**.
   d. Click the **Apply** button. Your settings are saved.
8. Enable multicast globally on Switch A.
   a. Select **Routing > Multicast > Global Configuration**.

      A page similar to the following figure displays.

   b. Select the Admin Mode **Enable** radio button.
   c. Click the **Apply** button. Your settings are saved.
9. Enable PIM-DM globally on Switch A.
   a. Select **Routing > Multicast > PIM > Global Configuration**.

      A page similar to the following figure displays.



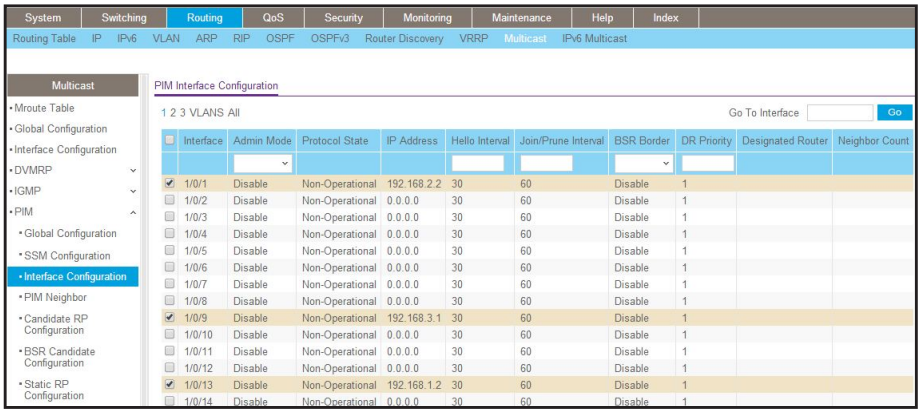
b. Select the **PIM-DM** radio button.

c. Click the **Apply** button. Your settings are saved.

10. Enable PIM on interfaces 1/0/1,1/0/9, and 1/0/13.

a. Select **Routing > Multicast > PIM > Interface Configuration**.

A page similar to the following figure displays.



b. Select the Interface **1/0/1**, **1/0/9**, and **1/0/13** check boxes.

c. In the **Admin Mode** menu, select **Enable**.

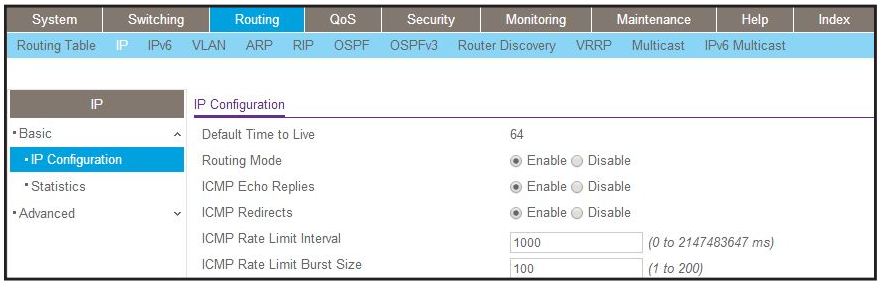
d. Click the **Apply** button. Your settings are saved.

Main UI: Configure PIM-DM on Switch B

To use the main UI to configure PIM-DM on Switch B:

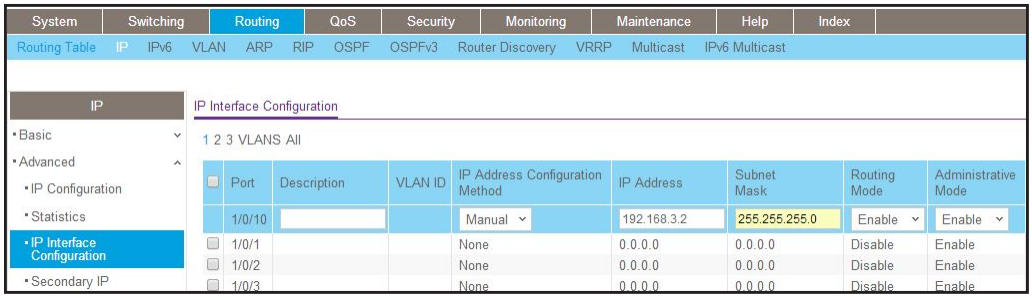
1. Enable IP routing on Switch B.
   a. Select **Routing > IP > Basic > IP Configuration**.

      A page similar to the following figure displays.



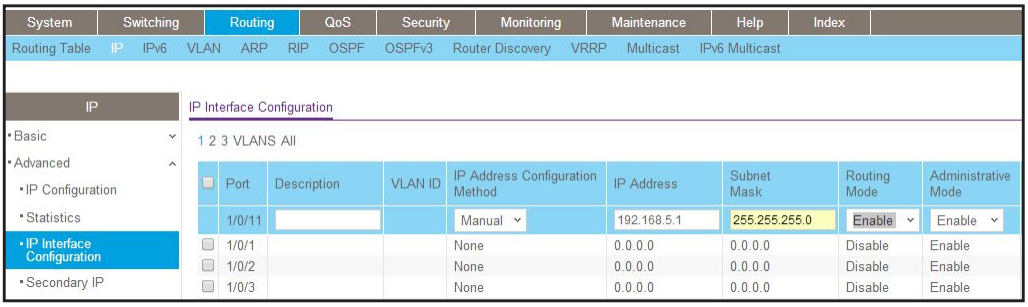
   b. Select the Routing Mode **Enable** radio button.
   c. Click the **Apply** button. Your settings are saved.
2. Configure routing on interface 1/0/10 and assign an IP address to the interface.
   a. Select **Routing > IP > Advanced > IP Interface Configuration**.

      A page similar to the following figure displays.



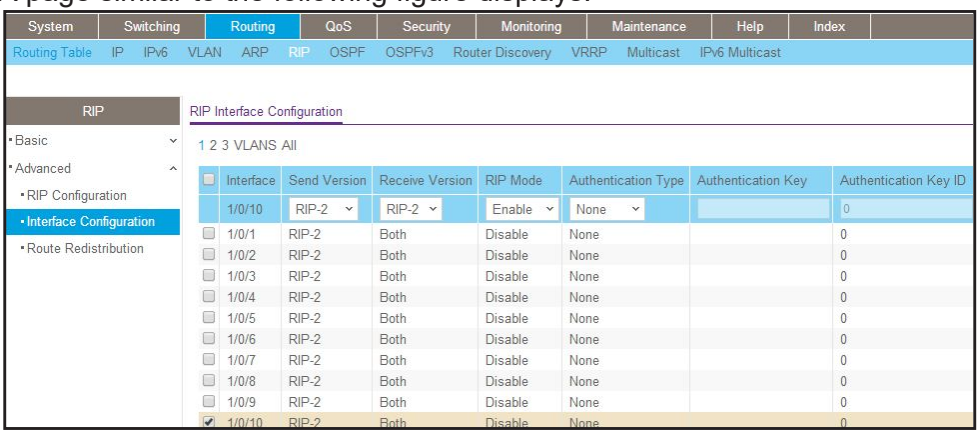
   b. Select the Port **1/0/10** check box.
   c. Configure the following settings:
      - In the **IP Address** field, enter **192.168.3.2**.
      - In the **Subnet Mask** field, enter **255.255.255.0**.
      - In the **Routing Mode** menu, select **Enable**.
   d. Click the **Apply** button. Your settings are saved.

3. Configure routing on interface 1/0/11 and assign an IP address to the interface.
   a. Remain on the same page.



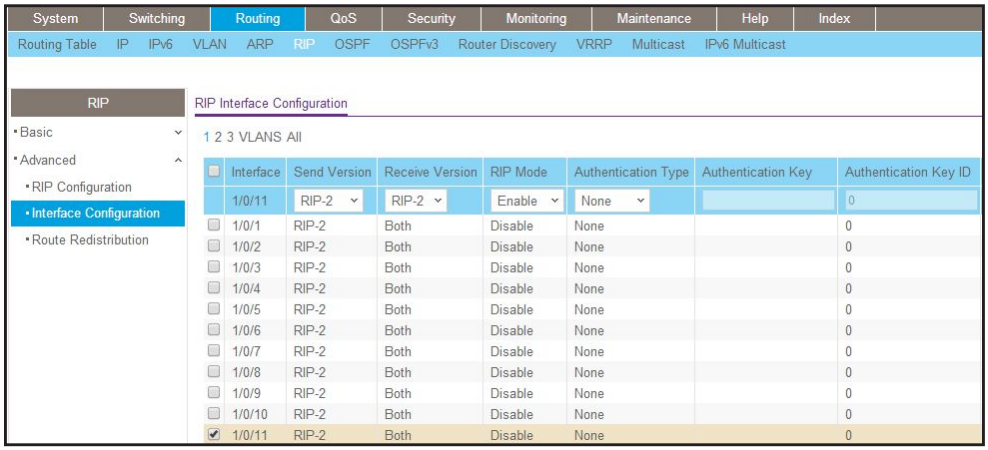
   b. Select the Port **1/0/11** check box.
   c. Configure the following settings:
      - In the **IP Address** field, enter **192.168.5.1**.
      - In the **Subnet Mask** field, enter **255.255.255.0**.
      - In the **Routing Mode** menu, select **Enable**.
   d. Click the **Apply** button. Your settings are saved.
4. Enable RIP on interface 1/0/10.
   a. Select **Routing > RIP > Advanced > Interface Configuration**.

      A page similar to the following figure displays.



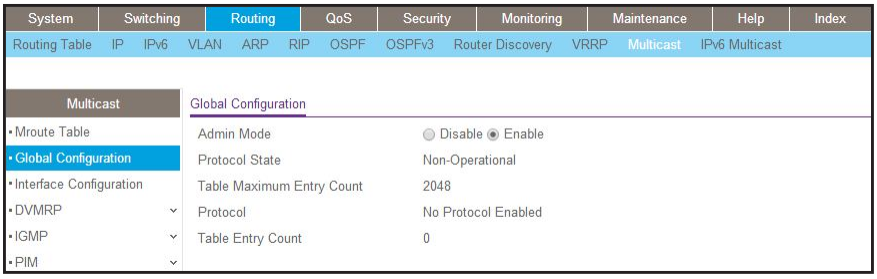
   b. Select the Interface **1/0/10** check box.
   c. In the **RIP Mode** menu, select the **Enable**.
   d. Click the **Apply** button. Your settings are saved.

5. Enable RIP on interface 1/0/11.
   a. Remain on the same page.



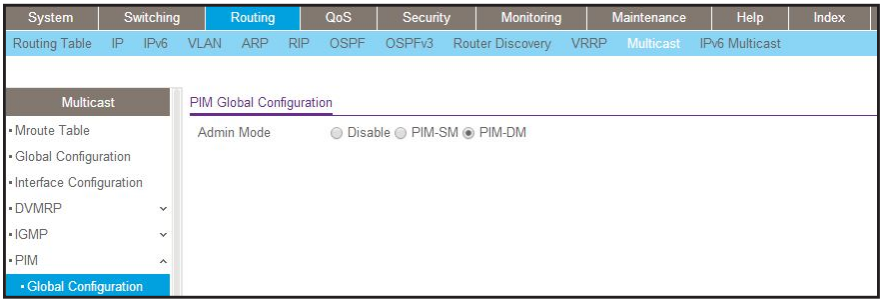
   b. Select the Interface **1/0/11** check box.
   c. In the **RIP Mode** menu, select the **Enable**.
   d. Click the **Apply** button. Your settings are saved.
6. Enable multicast globally on Switch B.
   a. Select **Routing > Multicast > Global Configuration**.

      A page similar to the following figure displays.



   b. Select the Admin Mode **Enable** radio button.
   c. Click the **Apply** button. Your settings are saved.
7. Enable PIM-DM globally on Switch B.
   a. Select **Routing > Multicast > PIM > Global Configuration**.

      A page similar to the following figure displays.



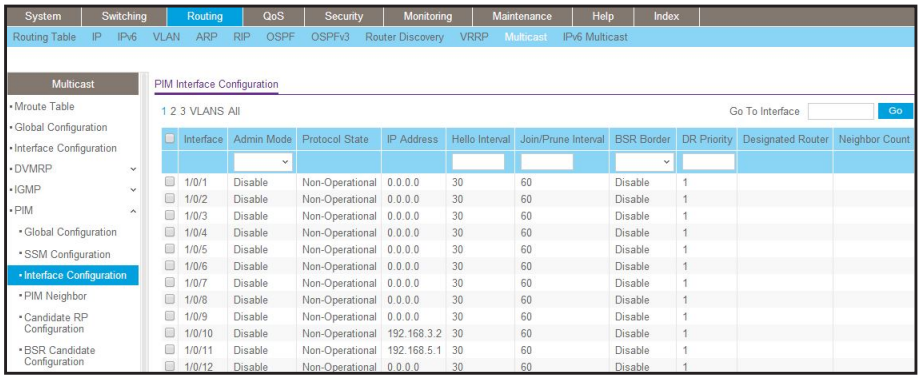
b. Select the Admin Mode **PIM-DM** radio button.

c. Click the **Apply** button. Your settings are saved.

8. Enable PIM on interfaces 1/0/10 and 1/0/11.

a. Select **Routing > Multicast > PIM > Interface Configuration**.

A page similar to the following figure displays.



b. Select the Interface **1/0/10** and **1/0/11** check boxes.

c. In the **Admin Mode** menu, select **Enable**.

d. Click the **Apply** button. Your settings are saved.

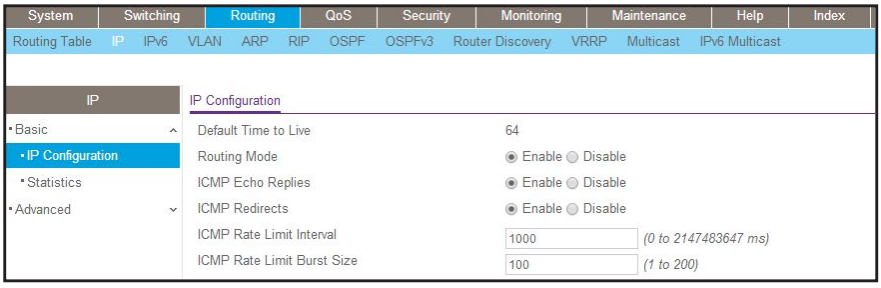
Main UI: Configure PIM-DM on Switch C

To use the main UI to configure PIM-DM on Switch C:

1. Enable IP routing on Switch C.

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

A page similar to the following figure displays.



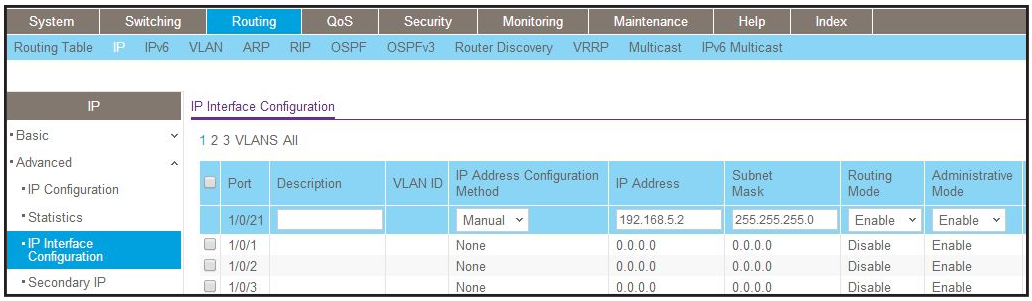
b. Select the Routing Mode **Enable** radio button.

c. Click the **Apply** button. Your settings are saved.

2. Configure routing on interface 1/0/21 and assign an IP address to the interface.

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

A page similar to the following figure displays.



b. Select the Port **1/0/21** check box.

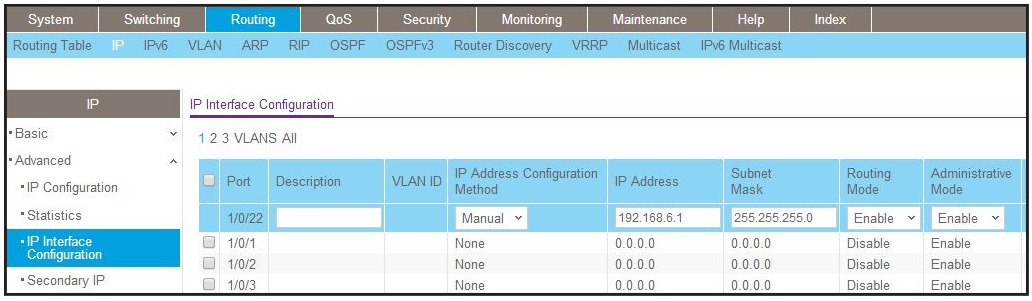
c. Configure the following settings:

- In the **IP Address** field, enter **192.168.5.2**.
- In the **Subnet Mask** field, enter **255.255.255.0**.
- In the **Routing Mode** menu, select **Enable**.

d. Click the **Apply** button. Your settings are saved.

3. Configure routing on interface 1/0/22 and assign an IP address to the interface.

a. Remain on the same page.



b. Select the Port **1/0/22** check box.

c. Configure the following settings:

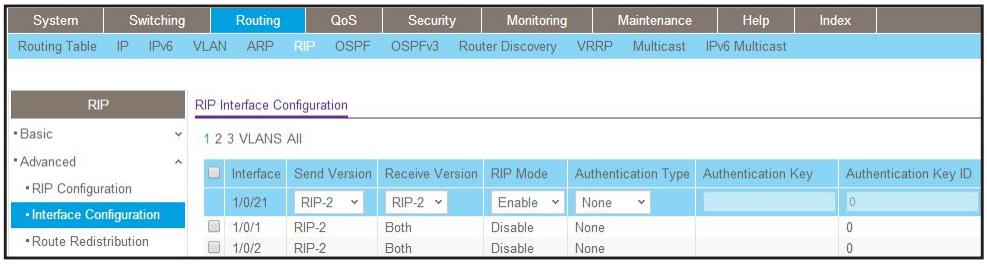
- In the **IP Address** field, enter **192.168.6.1**.
- In the **Subnet Mask** field, enter **255.255.255.0**.
- In the **Routing Mode** menu, select **Enable**.

d. Click the **Apply** button. Your settings are saved.

4. Enable RIP on interface 1/0/21.

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

A page similar to the following figure displays.



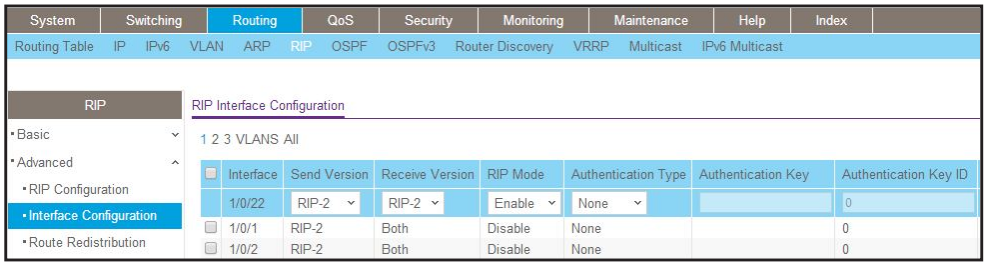
b. Select the Interface **1/0/21** check box.

c. In the **RIP Mode** menu, select **Enable**.

d. Click the **Apply** button. Your settings are saved.

5. Enable RIP on interface 1/0/22.

a. Remain on the same page.



b. Select the Interface **1/0/22** check box.

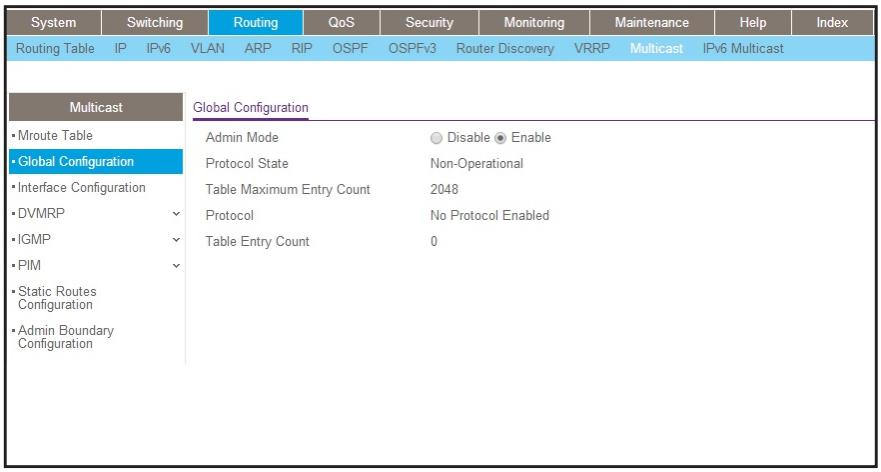
c. In the **RIP Mode** menu, select **Enable**.

d. Click the **Apply** button. Your settings are saved.

6. Enable mulicast globally on Switch C.

a. Select **Routing > Multicast > Global Configuration**.

A page similar to the following figure displays.

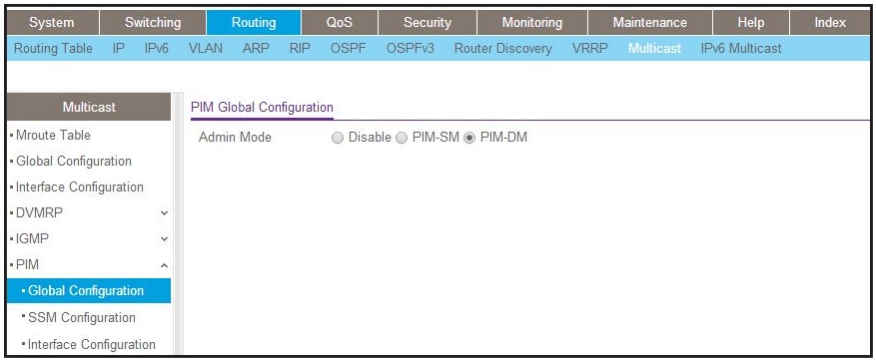


b. Select the Admin Mode **Enable** radio button.

c. Click the **Apply** button. Your settings are saved.

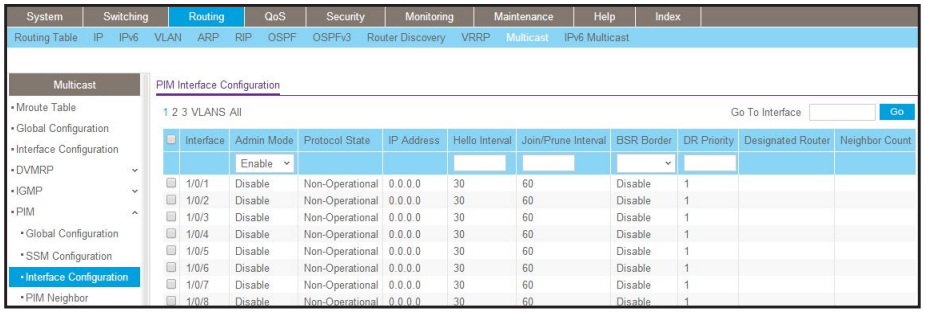
7. Enable PIM-DM globally on Switch C.
   a. Select **Routing > Multicast > PIM > Global Configuration**.

      A page similar to the following figure displays.



   b. Select the Admin Mode **PIM-DM** radio button.
   c. Click the **Apply** button. Your settings are saved.
8. Enable PIM on interfaces 1/0/21 and 1/0/22.
   a. Select **Routing > Multicast > PIM > Interface Configuration**.

      A page similar to the following figure displays.



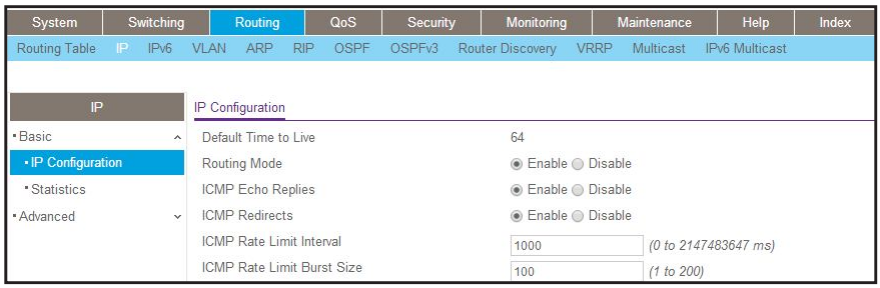
   b. Select the Interface **1/0/21** and **1/0/22** check boxes.
   c. In the **Admin Mode** menu, select **Enable**.
   d. Click the **Apply** button. Your settings are saved.

Main UI: Configure PIM-DM on Switch D

To use the main UI to configure PIM-DM on Switch D:

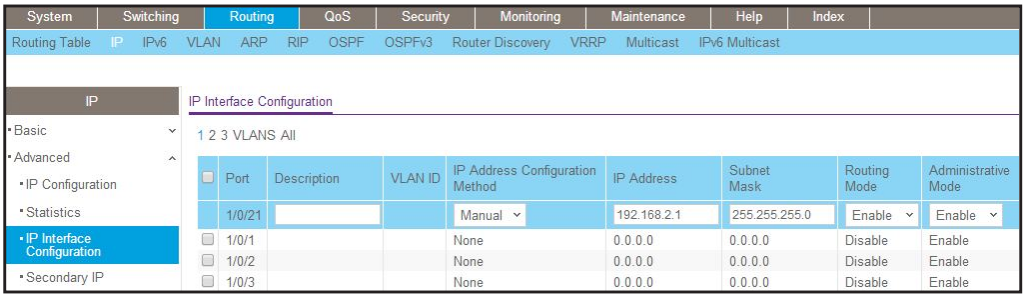
1. Enable IP routing on Switch D.
   a. Select **Routing > IP > Basic > IP Configuration**.

      A page similar to the following figure displays.



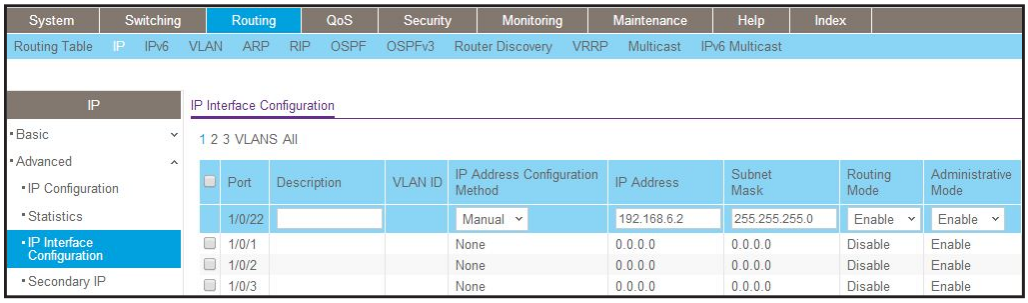
   b. Select the Routing Mode **Enable** radio button.
   c. Click the **Apply** button. Your settings are saved.
2. Configure routing on interface 1/0/21 and assign an IP address to the interface.
   a. Select **Routing > IP > Advanced > IP Interface Configuration**.

      A page similar to the following figure displays.

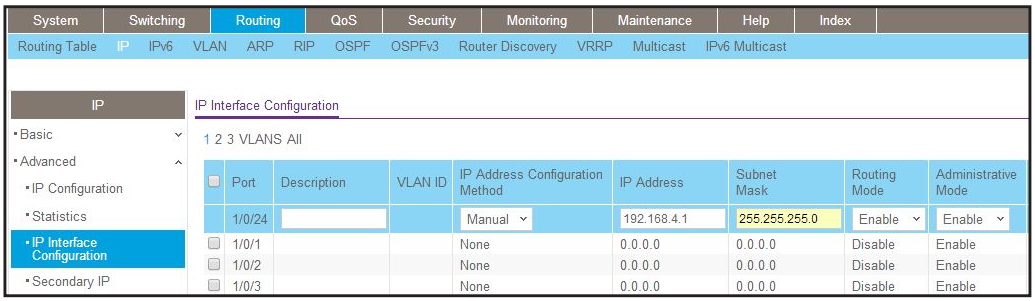


   b. Select the Port **1/0/21** check box.
   c. Enter the following information in the IP Interface Configuration.
      - In the **IP Address** field, enter **192.168.2.1**.
      - In the **Subnet Mask** field, enter **255.255.255.0**.
      - In the **Routing Mode** menu, select **Enable**.
   d. Click the **Apply** button. Your settings are saved.

3. Configure routing on interface 1/0/22 and assign an IP address to the interface.
   a. Remain on the same page.

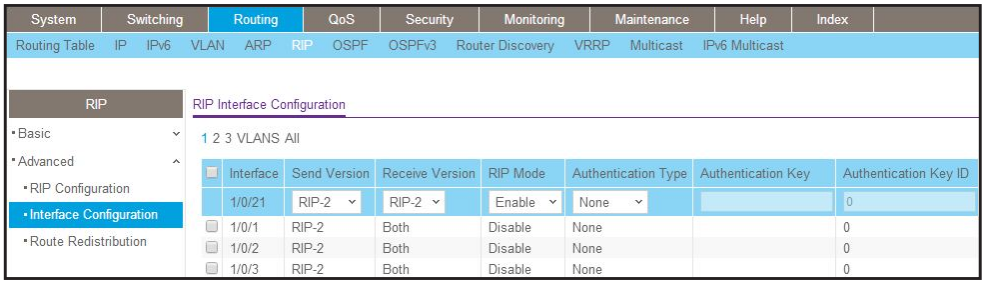


   b. Select the Port **1/0/22** check box.
   c. Configure the following settings:
      - In the **IP Address** field, enter **192.168.6.2**.
      - In the **Subnet Mask** field, enter **255.255.255.0**.
      - In the **Routing Mode** menu, select **Enable**.
   d. Click the **Apply** button. Your settings are saved.
4. Configure routing on interface 1/0/24 and assign an IP address to the interface.
   a. Remain on the same page.



   b. Select the Port **1/0/24** check box.
   c. Configure the following settings:
      - In the **IP Address** field, enter **192.168.4.1**.
      - In the **Subnet Mask** field, enter **255.255.255.0**.
      - In the **Routing Mode** menu, select **Enable**.
   d. Click the **Apply** button. Your settings are saved.
5. Enable RIP on interface 1/0/21.
   a. Select **Routing > RIP > Advanced > Interface Configuration**.

A page similar to the following figure displays.



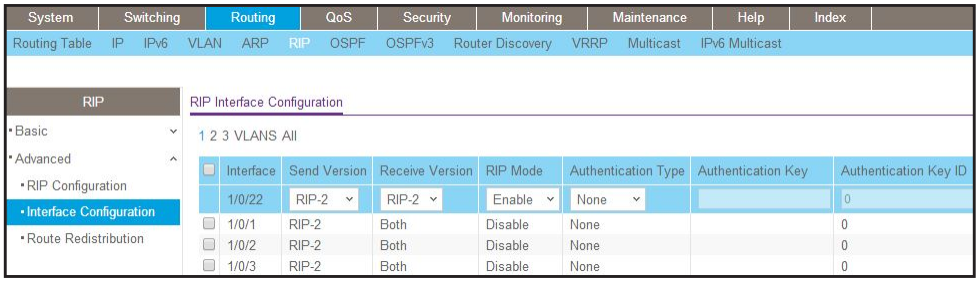
b. Select the Interface **1/0/21** check box.

c. In the **RIP Mode** menu, select **Enable**.

d. Click the **Apply** button. Your settings are saved.

6. Enable RIP on interface 1/0/22.

a. Remain on the same page.



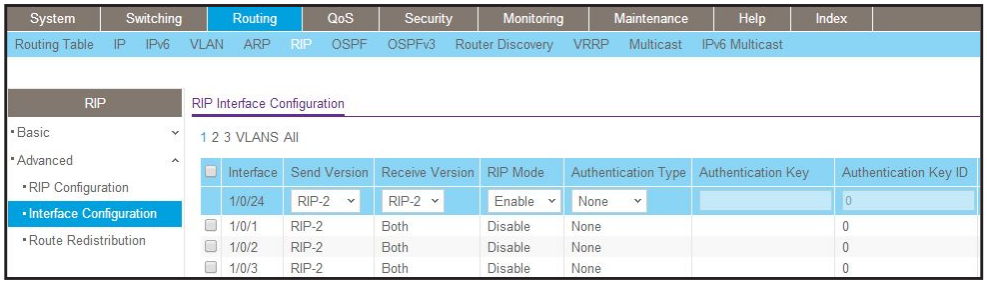
b. Select the Interface **1/0/22** check box.

c. In the **RIP Mode** menu, select **Enable**.

d. Click the **Apply** button. Your settings are saved.

7. Enable RIP on interface 1/0/24.

a. Remain on the same page.



b. Select the Interface **1/0/24** check box.

c. In the **RIP Mode** menu, select **Enable**.

d. Click the **Apply** button. Your settings are saved.

8. Enable multicast globally on Switch D.

a. Select **Routing > Multicast > Global Configuration**.

A page similar to the following figure displays.

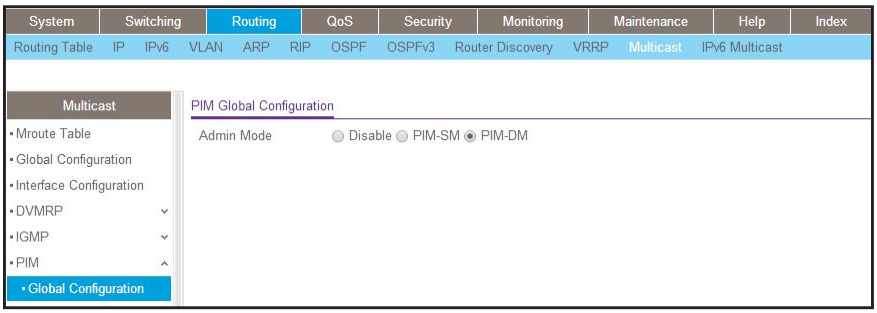
b. Select the Admin Mode **Enable** radio button.

c. Click the **Apply** button. Your settings are saved.

9. Enable PIM-DM globally on Switch D.

a. Select **Routing > Multicast > PIM > Global Configuration**.

A page similar to the following figure displays.



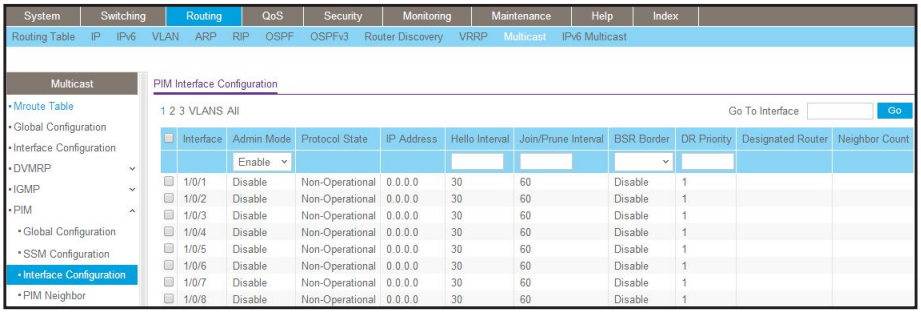
b. Select the Admin Mode **PIM-SM** radio button.

c. Click the **Apply** button. Your settings are saved.

10. Enable PIM on interfaces 1/0/21,1/0/22, and 1/0/24.

a. Select **Routing > Multicast > PIM > Interface Configuration**.

A page similar to the following figure displays.



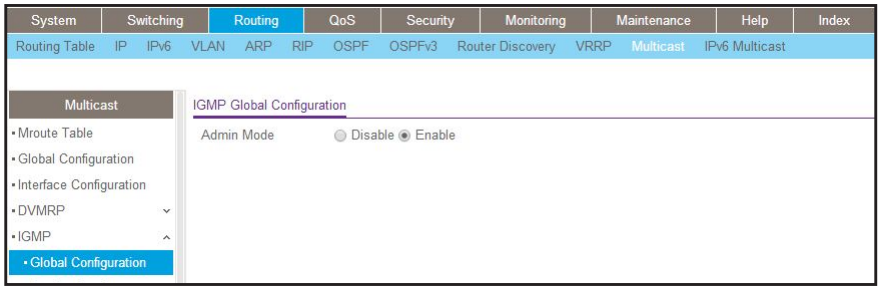
b. Select the Interface **1/0/21**, **1/0/22**, and **1/0/24** check boxes.

c. In the **Admin Mode** menu, select **Enable**.

d. Click the **Apply** button. Your settings are saved.

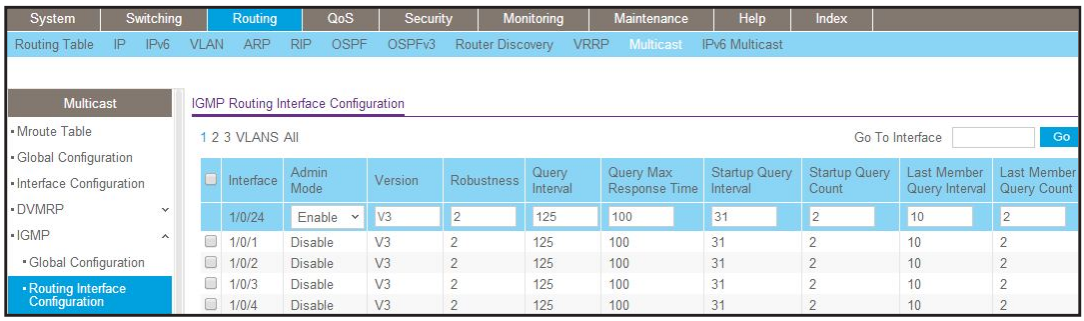
11. Enable IGMP globally on Switch D.
    a. Select **Routing > Multicast > IGMP > Global Configuration**.

       A page similar to the following figure displays.



    b. Select the Admin Mode **Enable** radio button.
    c. Click the **Apply** button. Your settings are saved.
12. Enable IGMP on interface 1/0/24.
    a. Select **Routing > Multicast > IGMP > Routing Interface Configuration**.

       A page similar to the following figure displays.



    b. Select the Interface **1/0/24** check box.
    c. In the **Admin Mode** menu, select **Enable**.
    d. Click the **Apply** button. Your settings are saved.

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.

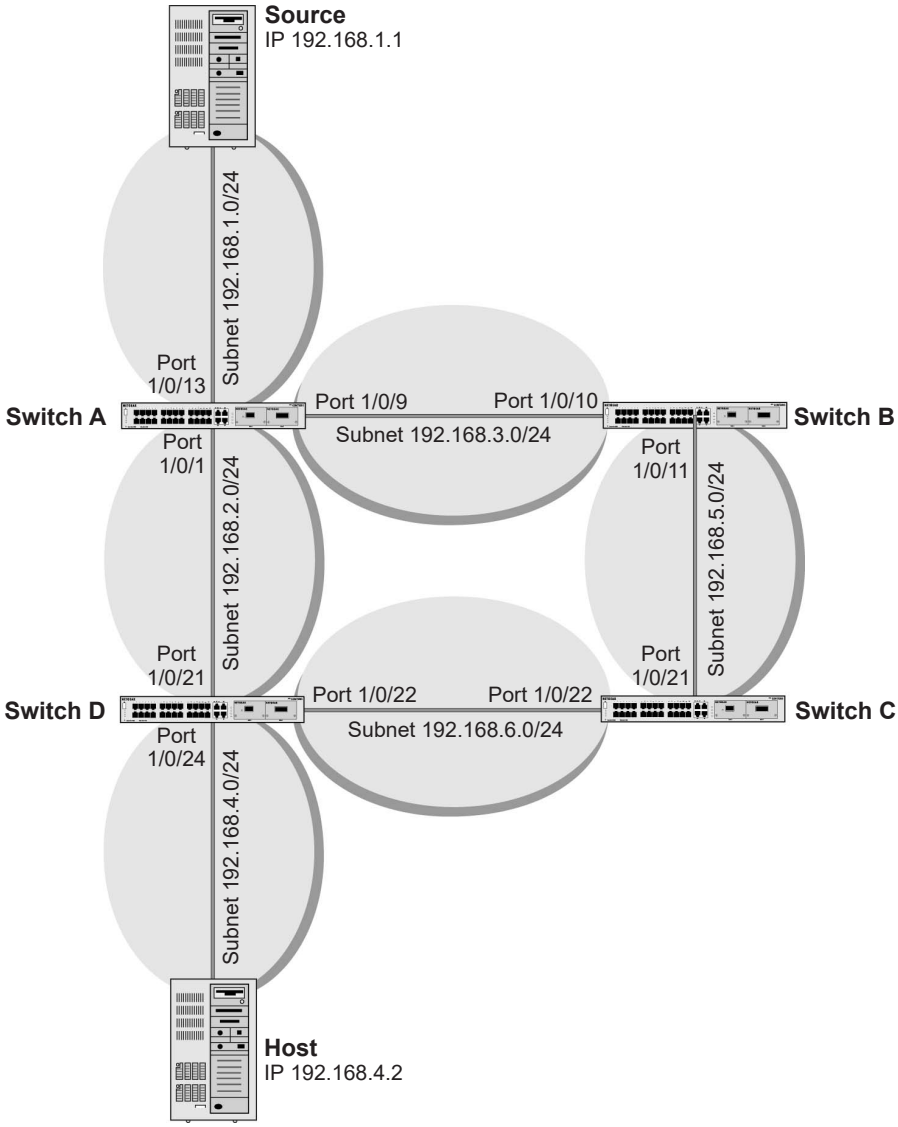


Figure 60. PIM-SM

PIM-SM uses shared trees by default and implements source-based trees for efficiency. PIM-SM is built on the assumption that no host wants 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 forward 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 network, a set of routers can be administratively enabled as candidate bootstrap routers. If it is not apparent which router must be the BSR, the candidates flood the domain with advertisements. The router with the highest priority is elected. If all the priorities are equal, 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 switches B, C, D as both RP-candidate and BSR-candidate. Switch B becomes the BSR because it has the highest priority. Switch D becomes the RP after RP election.

The example is shown as CLI commands and as a main UI procedure.

CLI: Configure PIM-SM

You must configure PIM-SM on Switch A, Switch B, Switch C, and Switch D.

CLI: Configure PIM-SM on Switch A

To use the CLI to configure PIM-SM on Switch A:

1. Enable IP routing on Switch A.

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

2. Enable PIM-SM on Switch A

```
(Netgear Switch) (Config)#ip pim sparse
```

3. Enable IP multicast forwarding on Switch A.

```
(Netgear Switch) (Config)#ip multicast
```

4. Enable routing, RIP, and PIM on interfaces 1/0/1, 1/0/9 and 1/0/13 to let Switch A 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
```

CLI: Configure PIM-SM and RP and BSR candidate configurations on Switch B

To use the CLI to configure PIM-SM and RP and BSR candidate configurations on Switch B:

1. Enable IP routing on Switch B.

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

2. Enable PIM-SM on Switch B.

```
(Netgear Switch) (Config)#ip pim sparse
```

3. Enable IP multicast forwarding on Switch B.

```
(Netgear Switch) (Config)#ip multicast
```

4. Enable routing, RIP, and PIM on interfaces 1/0/10 and 1/0/11 to let Switch B build a unicast IP routing table.

```
(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
```

5. Enable interface 1/0/11 on Switch B to advertise itself as a PIM candidate rendezvous point (RP) to a bootstrap router (BSR).

```
(Netgear Switch) (Config)#ip pim rp-candidate interface 1/0/11 225.1.1.1
255.255.255.0
```

6. Enable interface 1/0/10 on Switch B to announce its candidacy as a bootstrap router (BSR).

```
(Netgear Switch) (Config)#ip pim bsr-candidate interface 1/0/10 30 7
```

CLI: Configure PIM-SM and RP and BSR candidate configurations on Switch C

To use the CLI to configure PIM-SM and RP and BSR candidate configurations on Switch C:

1. Enable IP routing on Switch C.

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

2. Enable PIM-SM on Switch C.

```
(Netgear Switch) (Config)#ip pim sparse
```

3. Enable IP multicast forwarding on Switch C.

```
(Netgear Switch) (Config)#ip multicast
```

4. Enable routing, RIP, and PIM on interfaces 1/0/21 and 1/0/22 to let Switch C build a unicast IP routing table.

```
(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 92.168.6.1 255.255.255.0
(Netgear Switch) (Interface 1/0/22)#ip rip
(Netgear Switch) (Interface 1/0/22)#ip pim
(Netgear Switch) (Interface 1/0/22)#exit
```

5. Enable interface 1/0/22 on Switch C to advertise itself as a PIM candidate rendezvous point (RP) to a bootstrap router (BSR).

```
(Netgear Switch) (Config)#ip pim rp-candidate interface 1/0/22 225.1.1.1
255.255.255.0
```

6. Enable interface 1/0/21 on Switch C to announce its candidacy as a bootstrap router (BSR).

```
(Netgear Switch) (Config)#ip pim bsr-candidate interface 1/0/21 30 5
```

CLI: Configure PIM-SM, RP and BSR candidate configurations, and IGMP on Switch D

To use the CLI to configure PIM-SM, RP and BSR candidate configurations, and IGMP on Switch D:

1. Enable IP routing on Switch D.

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

2. Enable PIM-SM on Switch D.

```
(Netgear Switch) (Config)#ip pim sparse
```

3. Enable IP multicast forwarding on Switch D.

```
(Netgear Switch) (Config)#ip multicast
```

4. Enable routing, RIP, and PIM on interfaces 1/0/21, 1/0/22, and 1/0/24 to let Switch D build a unicast IP routing table.

```
(Netgear Switch) (Config)#interface 1/0/21
(Netgear Switch) (Interface 1/0/21)#routing
(Netgear Switch) (Interface 1/0/21)#ip address 92.168.2.1 255.255.255.0
(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
```

5. Enable interface 1/0/22 on Switch D to advertise itself as a PIM candidate rendezvous point (RP) to a bootstrap router (BSR).

```
(Netgear Switch) (Config)#ip pim rp-candidate interface 1/0/22 225.1.1.1
255.255.255.0
```

6. Enable interface 1/0/21 on Switch D to announce its candidacy as a bootstrap router (BSR).

```
(Netgear Switch) (Config)#ip pim bsr-candidate interface 1/0/221 30 3
```

7. Enable IGMP on Switch D.

```
(Netgear Switch) (Config)#ip igmp
```

CLI: Display the Multicast Route Table on Switches, A, B, C, and D

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.

To use the CLI to build the multicast route table on Switches A, B, C, and D:

```
(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    PIMSM         1/0/13        1/0/1

(Switch 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

(Switch 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

(Switch 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
```

Main UI: Configure PIM-SM

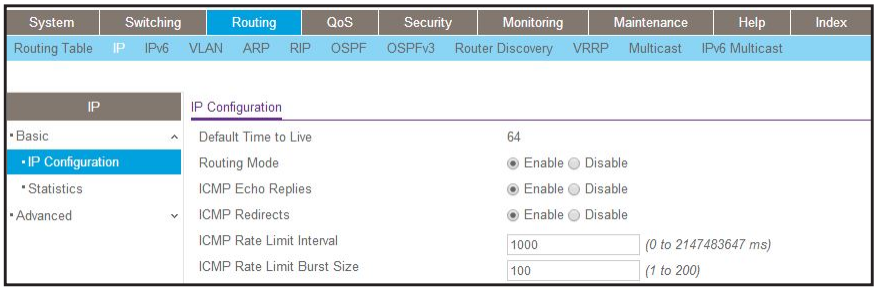
You must configure PIM-SM on Switch A, Switch B, Switch C, and Switch D.

Main UI: Configure PIM-SM on Switch A

To use the main UI to configure PIM-SM on Switch A:

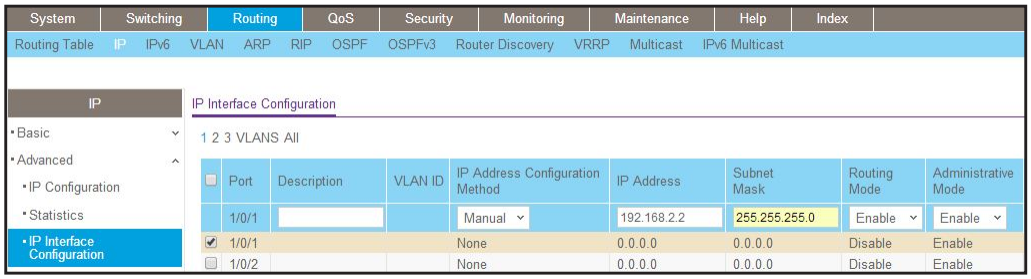
1. Enable IP routing on Switch A.
   a. Select **Routing > IP > Basic > IP Configuration**.

      A page similar to the following figure displays.



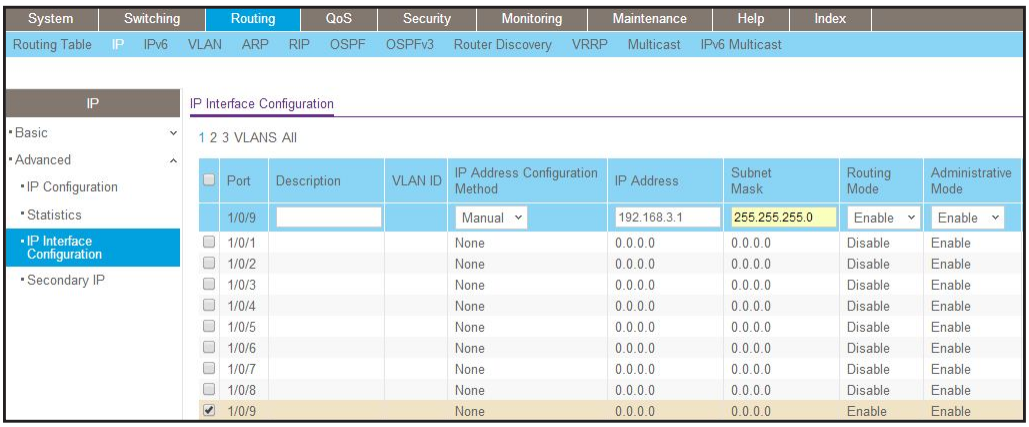
   b. Select the Routing Mode **Enable** radio button.
   c. Click the **Apply** button. Your settings are saved.
2. Configure routing on interface 1/0/1 and assign an IP address to the interface.
   a. Select **Routing > IP > Advanced > IP Interface Configuration**.

      A page similar to the following figure displays.

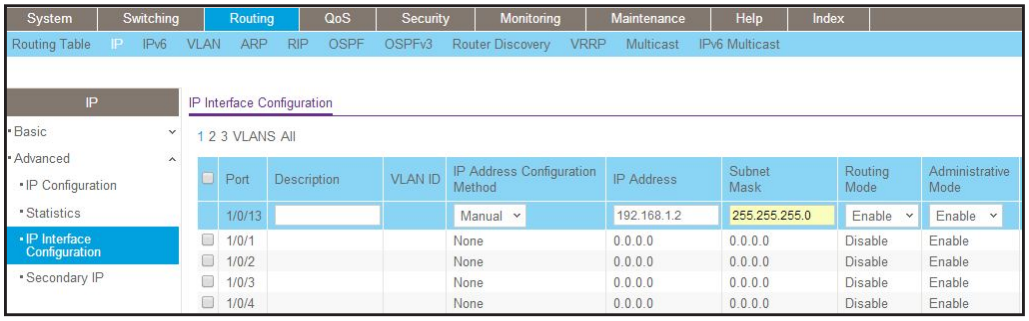


   b. Select the Port **1/0/1** check box.
   c. Configure the following settings:
      - In the **IP Address** field, enter **192.168.2.2**.
      - In the **Subnet Mask** field, enter **255.255.255.0**.
      - In the **Routing Mode** menu, select **Enable**.
   d. Click the **Apply** button. Your settings are saved.

3. Configure routing on interface 1/0/9 and assign an IP address to the interface.
   a. Remain on the same page.

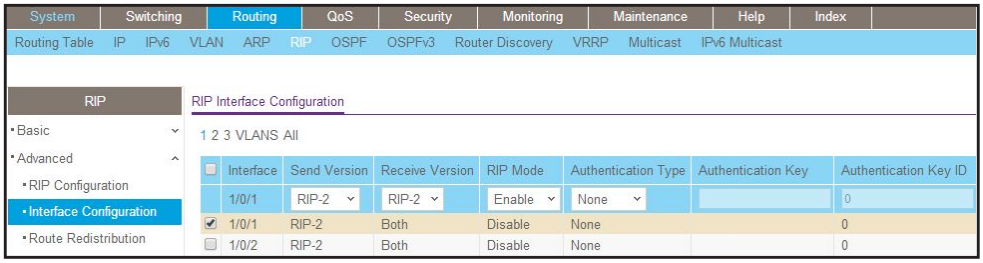


   b. Select the Port **1/0/9** check box.
   c. Configure the following settings:
      - In the **IP Address** field, enter **192.168.3.1**.
      - In the **Subnet Mask** field, enter **255.255.255.0**.
      - In the **Routing Mode** menu, select **Enable**.
   d. Click the **Apply** button. Your settings are saved.
4. Configure routing on interface 1/0/13 and assign an IP address to the interface.
   a. Remain on the same page.

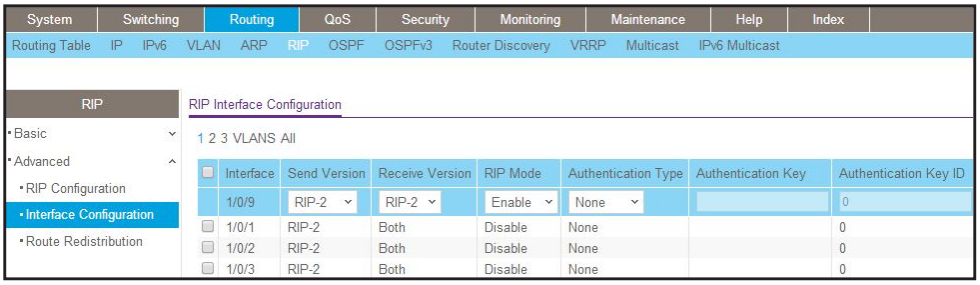


   b. Select the Port **1/0/13** check box.
   c. Configure the following settings:
      - In the **IP Address** field, enter **192.168.1.2**.
      - In the **Subnet Mask** field, enter **255.255.255.0**.
      - In the **Routing Mode** menu, select **Enable**.
   d. Click the **Apply** button. Your settings are saved.

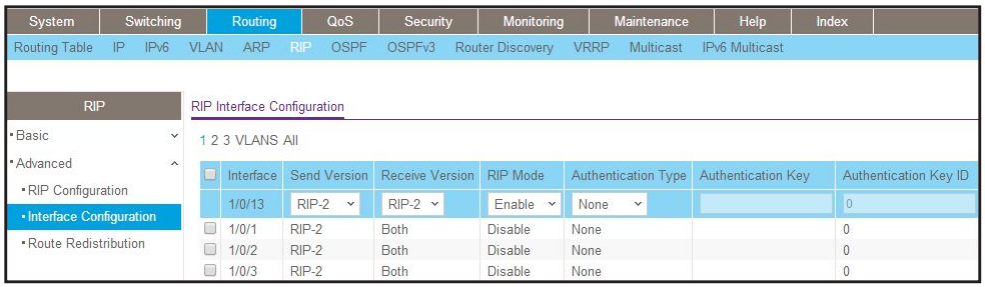
5. Enable RIP on interface 1/0/1.
   a. Remain on the same page.



   b. Select the Interface **1/0/1** check box.
   c. In the **RIP Mode** menu, select **Enable**.
   d. Click the **Apply** button. Your settings are saved.
6. Enable RIP on interface 1/0/9.
   a. Remain on the same page.

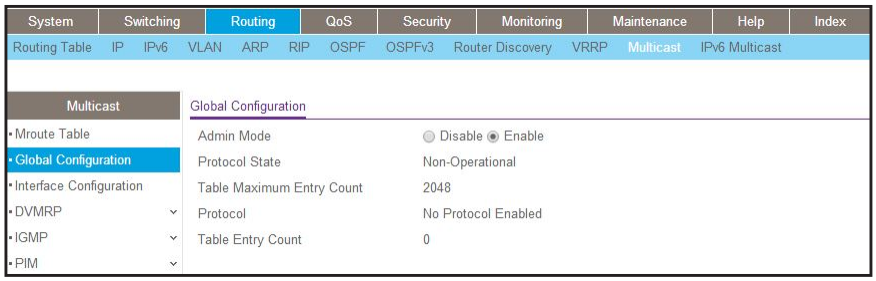


   b. Select the Interface **1/0/9** check box.
   c. In the **RIP Mode** menu, select **Enable**.
   d. Click the **Apply** button. Your settings are saved.
7. Enable RIP on interface 1/0/13.
   a. Remain on the same page.



   b. Select the Interface **1/0/13** check box.
   c. In the **RIP Mode** menu, select **Enable**.
   d. Click the **Apply** button. Your settings are saved.
8. Enable multicast globally on Switch A.
   a. Select **Routing > Multicast > Global Configuration**.

A page similar to the following figure displays.



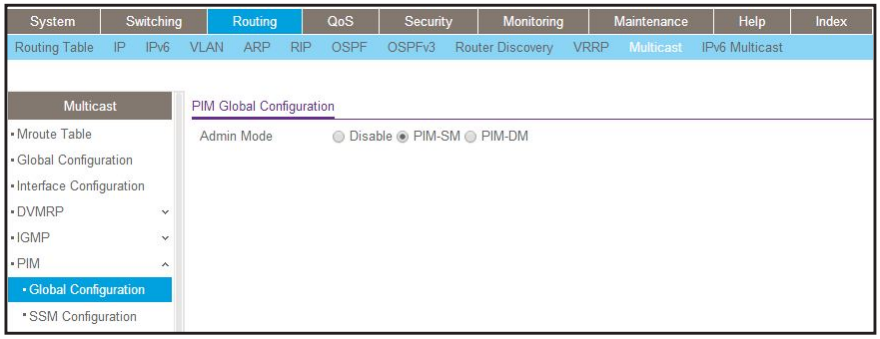
b. Select the Admin Mode **Enable** radio button.

c. Click the **Apply** button. Your settings are saved.

9. Enable PIM-SM globally on Switch A.

a. Select **Routing > Multicast > PIM > Global Configuration**.

A page similar to the following figure displays.



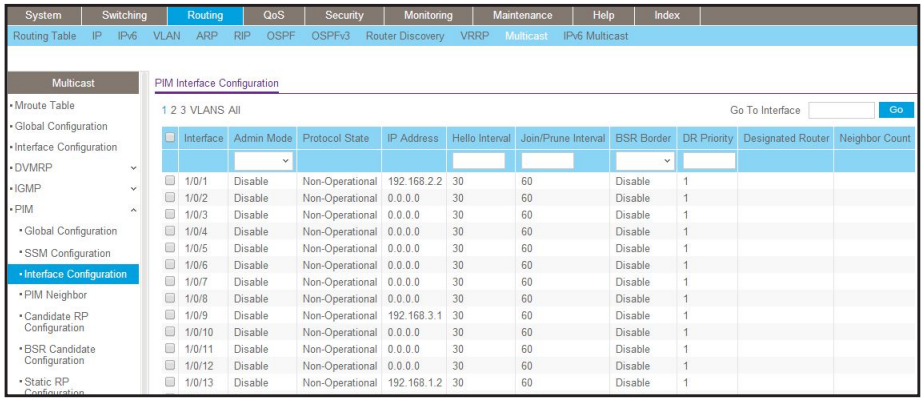
b. Select the Admin Mode **PIM-SM** radio button.

c. Click the **Apply** button. Your settings are saved.

10. Enable PIM-SM on interfaces 1/0/1,1/0/9, and 1/0/13.

a. Select **Routing > Multicast > PIM > Interface Configuration**.

A page similar to the following figure displays.



b. Select the Interface **1/0/1**, **1/0/9**, and **1/0/13** check boxes.

c. In the **Admin Mode** menu, select **Enable**.

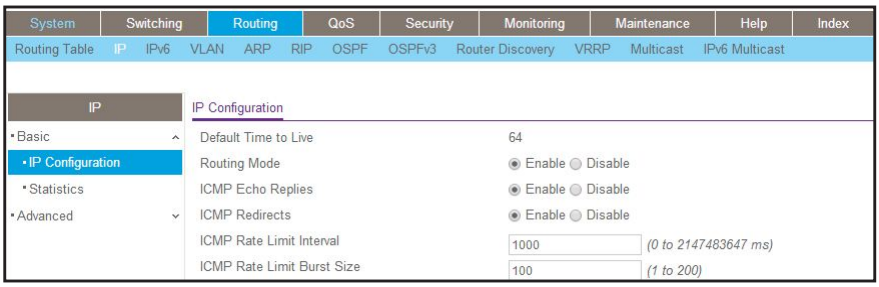
d. Click the **Apply** button. Your settings are saved.

Main UI: Configure PIM-SM and RP and BSR candidate configurations on Switch B

To use the main UI to configure PIM-SM and RP and BSR candidate configurations on Switch B:

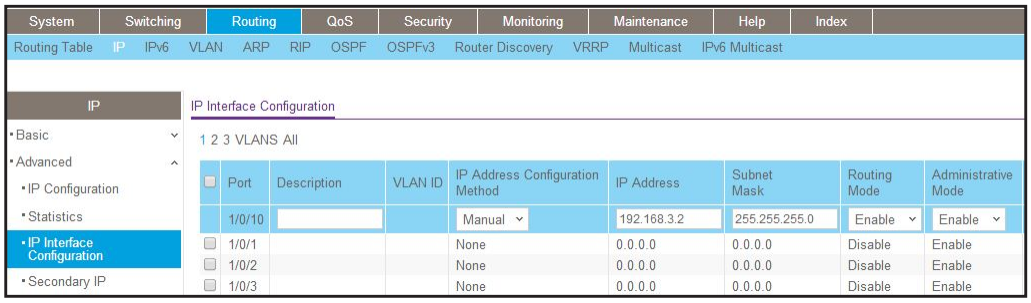
1. Enable IP routing on the switch.
   a. Select **Routing > IP > Basic > IP Configuration**.

      A page similar to the following figure displays.



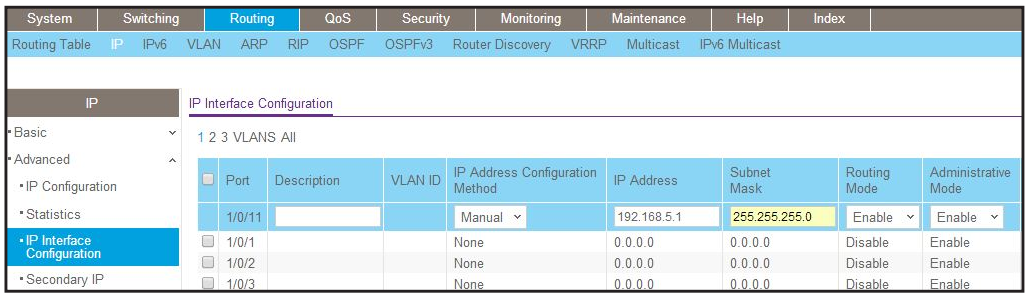
   b. Select the Routing Mode **Enable** radio button.
   c. Click the **Apply** button. Your settings are saved.
2. Configure routing on interface 1/0/10 and assign an IP address to the interface.
   a. Select **Routing > IP > Advanced > IP Interface Configuration**.

      A page similar to the following figure displays.



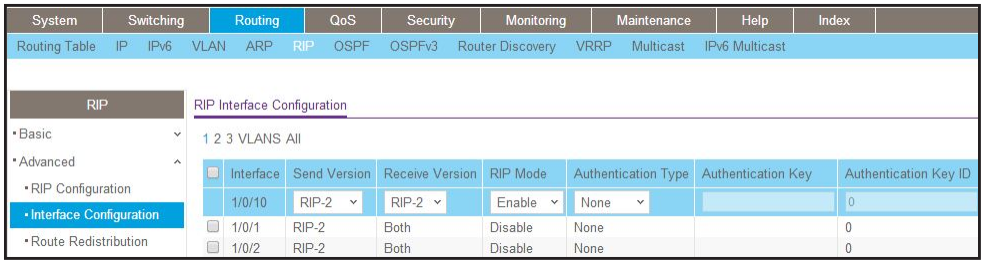
   b. Select the Port **1/0/10** check box.
   c. Configure the following settings:
      - In the **IP Address** field, enter **192.168.3.2**.
      - In the **Subnet Mask** field, enter **255.255.255.0**.
      - In the **Routing Mode** menu, select **Enable**.
   d. Click the **Apply** button. Your settings are saved.

3. Configure routing on interface 1/0/11 and assign an IP address to the interface.
   a. Remain on the same page.

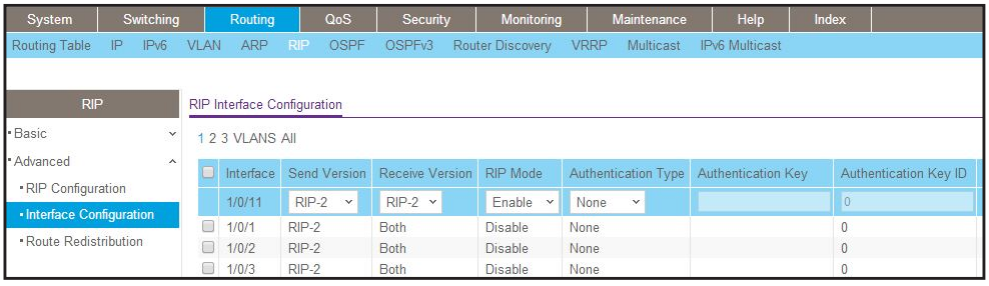


   b. Select the Port **1/0/11** check box.
   c. Configure the following settings:
      - In the **IP Address** field, enter **192.168.5.1**.
      - In the **Subnet Mask** field, enter **255.255.255.0**.
      - In the **Routing Mode** menu, select **Enable**.
   d. Click the **Apply** button. Your settings are saved.
4. Enable RIP on interface 1/0/10.
   a. Select **Routing > RIP > Advanced > Interface Configuration**.

      A page similar to the following figure displays.



   b. Select the Interface **1/0/10** check box.
   c. In the **RIP Mode** menu, select **Enable**.
   d. Click the **Apply** button. Your settings are saved.
5. Enable RIP on interface 1/0/11.
   a. Remain on the same page.



   b. Select the Interface **1/0/11** check box.
   c. In the **RIP Mode** menu, select **Enable**.

d. Click the **Apply** button. Your settings are saved.

6. Enable multicast globally on Switch B.

a. Select **Routing > Multicast > Global Configuration**.

A page similar to the following figure displays.

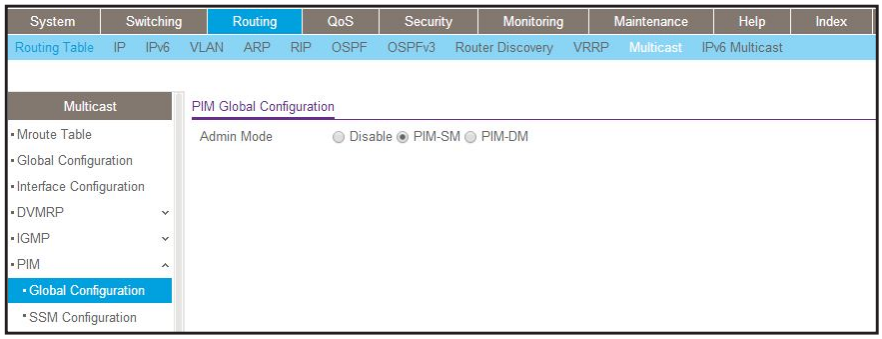
b. Select the Admin Mode **Enable** radio button.

c. Click the **Apply** button. Your settings are saved.

7. Enable PIM-SM globally on Switch B.

a. Select **Routing > Multicast > PIM > Global Configuration**.

A page similar to the following figure displays.



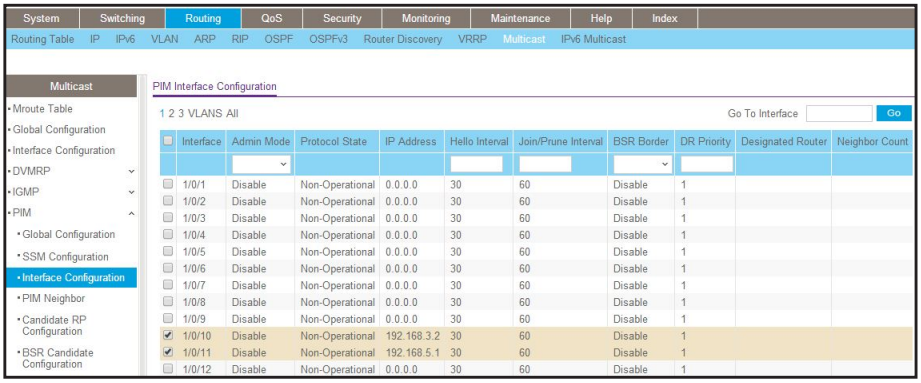
b. Select the **PIM-SM** radio button.

c. Click the **Apply** button. Your settings are saved.

8. Enable PIM on interfaces 1/0/10 and 1/0/11.

a. Select **Routing > Multicast > PIM > Interface Configuration**.

A page similar to the following figure displays.



b. Select the Interface **1/0/10** and **1/0/11** check boxes.

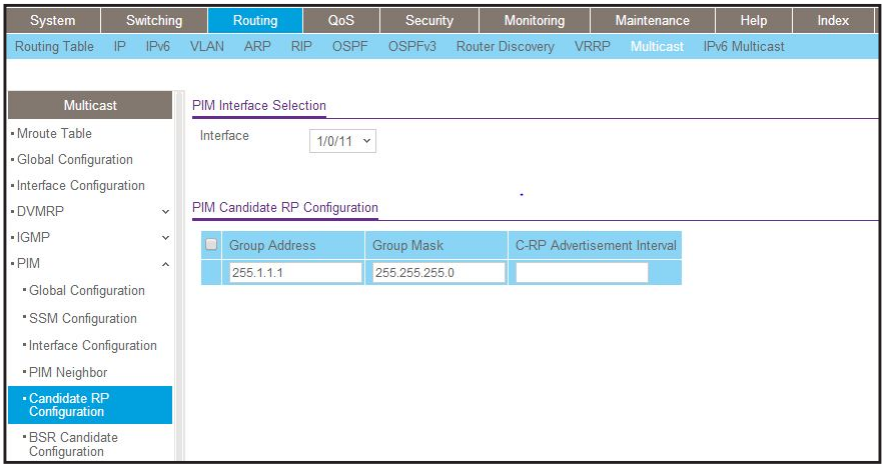
c. In the **Admin Mode** menu, select **Enable**.

d. Click the **Apply** button. Your settings are saved.

9. Set up the RP candidate configuration on Switch B.

a. Select **Routing > Multicast > PIM > Candidate RP Configuration**.

A page similar to the following figure displays.



b. In the **Interface** menu, select **1/0/11**.

c. In the **Group IP** field, enter **225.1.1.1**.

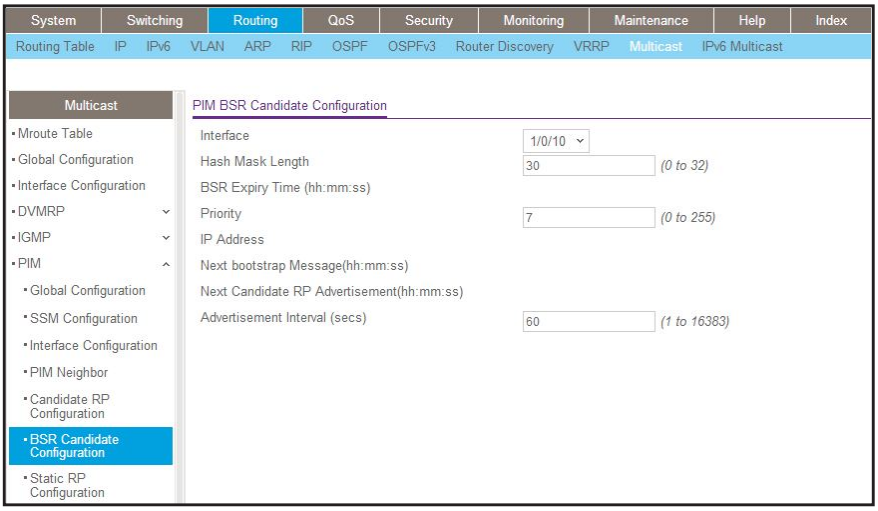
d. In the **Group Mask** field, enter **255.255.255.0**.

e. Click the **Add** button. Your settings are saved.

10. Set up the BSR candidate configuration on Switch B.

a. Select **Routing > Multicast > PIM > BSR Candidate Configuration**.

A page similar to the following figure displays.



b. In the **Interface** menu, select the **1/0/10**.

c. In the **Hash Mask Length** field, enter **30**.

d. In the **Priority** field, enter **7**.

e. Click the **Apply** button. Your settings are saved.

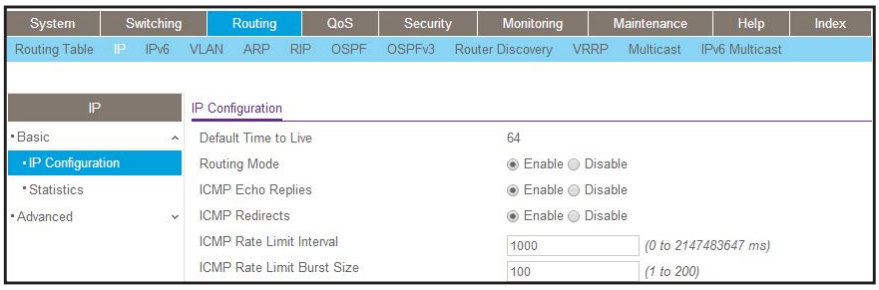
Main UI: Configure PIM-SM and RP and BSR candidate configurations on Switch C

To use the main UI to configure PIM-SM and RP and BSR candidate configurations on Switch C:

1. Enable IP routing on Switch C.

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

A page similar to the following figure displays.



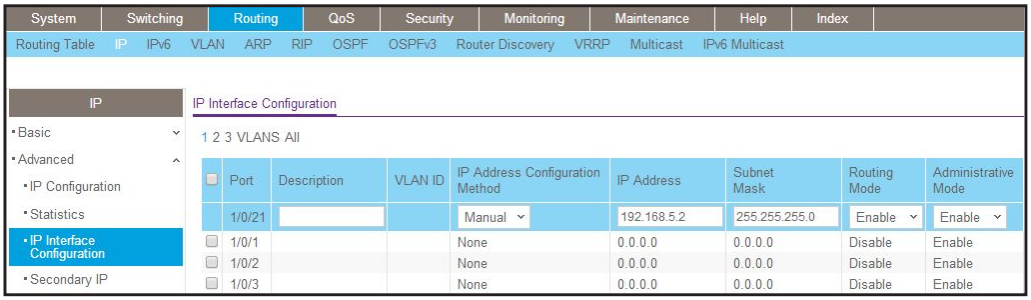
b. Select the Routing Mod **Enable** radio button.

c. Click the **Apply** button. Your settings are saved.

2. Configure routing on interface 1/0/21 and assign an IP address to the interface.

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

A page similar to the following figure displays.



b. Select the Port **1/0/21** check box.

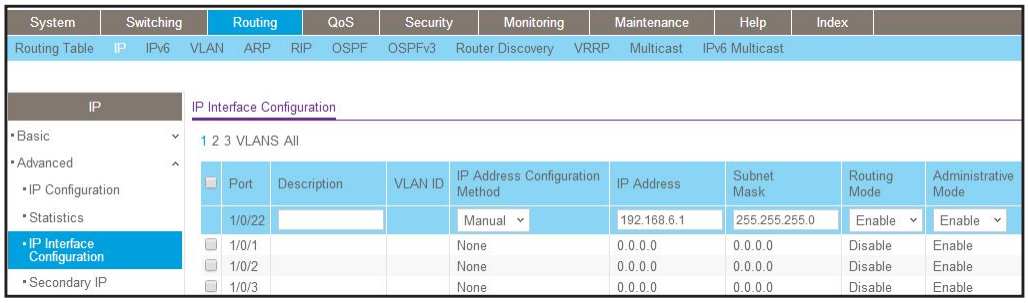
c. Configure the following settings:

- In the **IP address**, enter **192.168.5.2**.
- In the **Subnet Mask** field, enter **255.255.255.0**.
- In the **Routing Mode** menu, select **Enable**.

d. Click the **Apply** button. Your settings are saved.

3. Configure routing on interface 1/0/22 and assign an IP address to the interface.

a. Remain on the same page.



b. Select the Port **1/0/22** check box.

c. Configure the following settings:

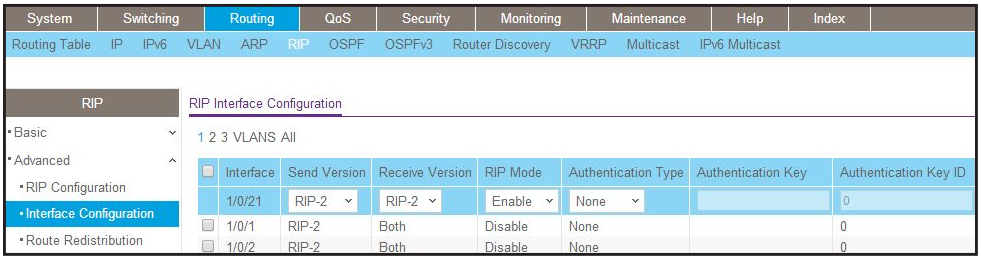
- In the **IP Address** field, enter **192.168.6.1**.
- In the **Subnet Mask** field, enter **255.255.255.0**.
- In the **Routing Mode** menu, select **Enable**.

d. Click the **Apply** button. Your settings are saved.

4. Enable RIP on the interface 1/0/21.

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

A page similar to the following figure displays.



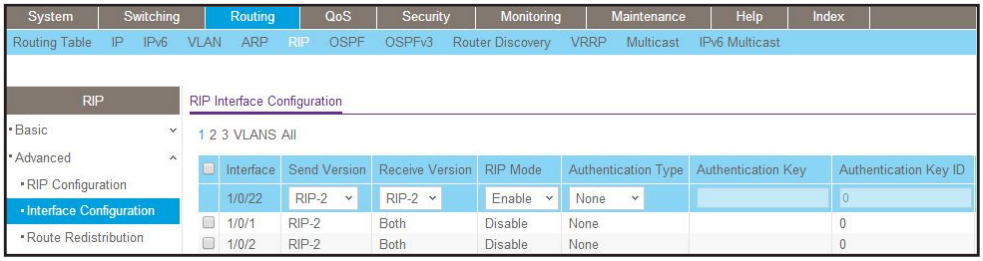
b. Select the Interface **1/0/21** check box.

c. In the **RIP Mode** menu, select **Enable**.

d. Click the **Apply** button. Your settings are saved.

5. Enable RIP on interface 1/0/22.

a. Remain on the same page.



b. Select the Interface **1/0/22** check box.

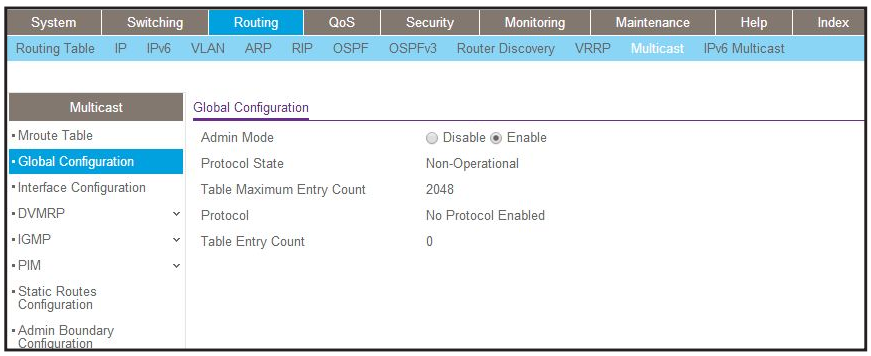
c. In the **RIP Mode** menu, select **Enable**.

d. Click the **Apply** button. Your settings are saved.

6. Enable multicast globally on Switch C.

a. Select **Routing > Multicast > Global Configuration**.

A page similar to the following figure displays.



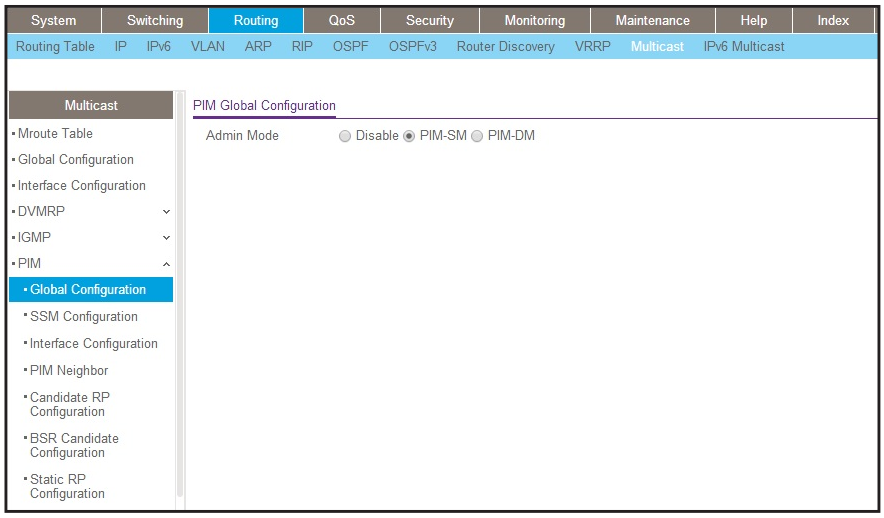
b. Select the Admin Mode **Enable** radio button.

c. Click the **Apply** button. Your settings are saved.

7. Enable PIM-SM globally on Switch C.

a. Select **Routing > Multicast > PIM > Global Configuration**.

A page similar to the following figure displays.



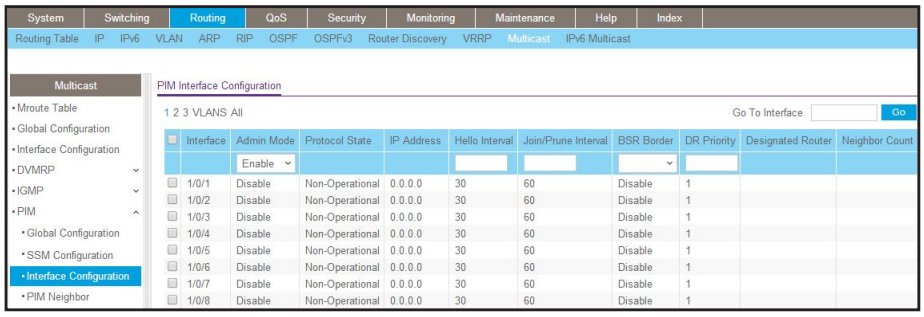
b. Select the Admin Mode **PIM-SM** radio button.

c. Click the **Apply** button. Your settings are saved.

8. Enable PIM on interfaces 1/0/21 and 1/0/22.

a. Select **Routing > Multicast > PIM > Interface Configuration**.

A page similar to the following figure displays.



b. Select the Interface **1/0/21** and **1/0/22** check boxes.

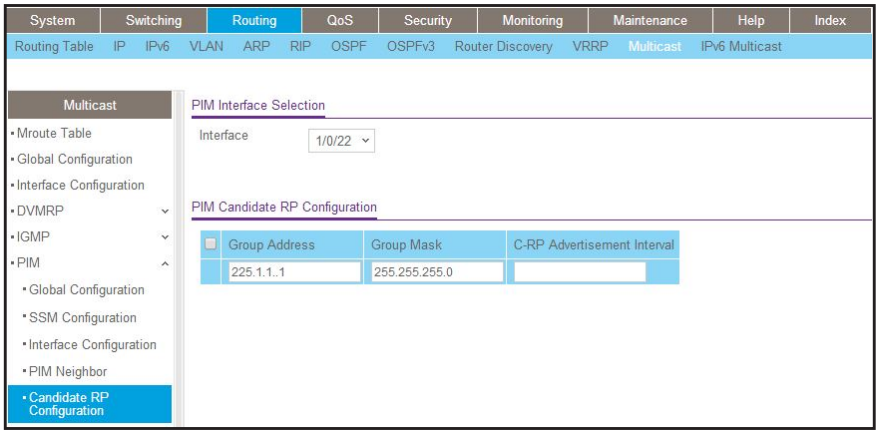
c. In the **Admin Mode** menu, select **Enable**.

d. Click the **Apply** button. Your settings are saved.

9. Set up the RP candidate configuration on Switch C.

a. Select **Routing > Multicast > PIM > Candidate RP Configuration**.

A page similar to the following figure displays.



b. In the **Interface** menu, select **1/0/22**.

c. In the **Group IP** field, enter **225.1.1.1**.

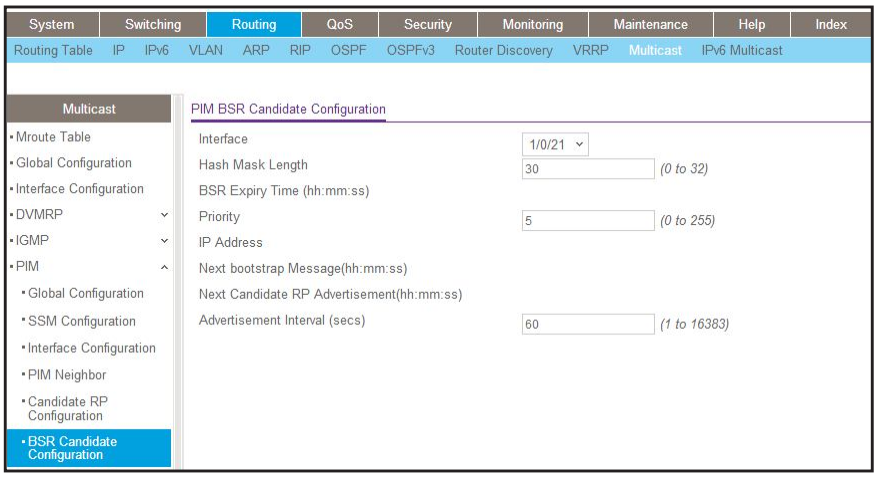
d. In the **Group Mask** field, enter **255.255.255.0**.

e. Click the **Add** button. Your settings are saved.

10. Set up the BSR candidate configuration on Switch C.

a. Select **Routing > Multicast > PIM > BSR Candidate Configuration**.

A page similar to the following figure displays.



b. In the **Interface** menu, select **1/0/21**.

c. In the **Hash Mask Length** field, enter **30**.

d. In the **Priority** field, enter **5**.

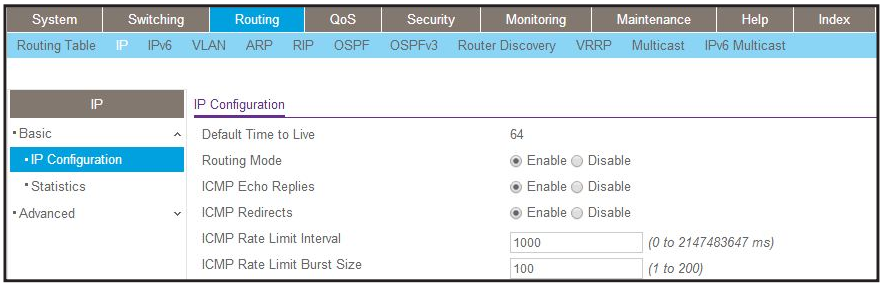
e. Click the **Apply** button. Your settings are saved.

Main UI: Configure PIM-SM, RP and BSR candidate configurations, and IGMP on Switch D

To use the main UI to configure PIM-SM, RP and BSR candidate configurations, and IGMP on Switch D:

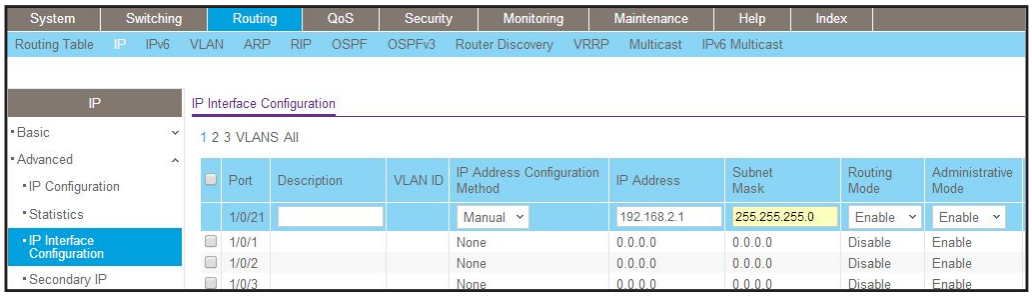
1. Enable IP routing on the switch.
   a. Select **Routing > IP > Basic > IP Configuration**.

      A page similar to the following figure displays.



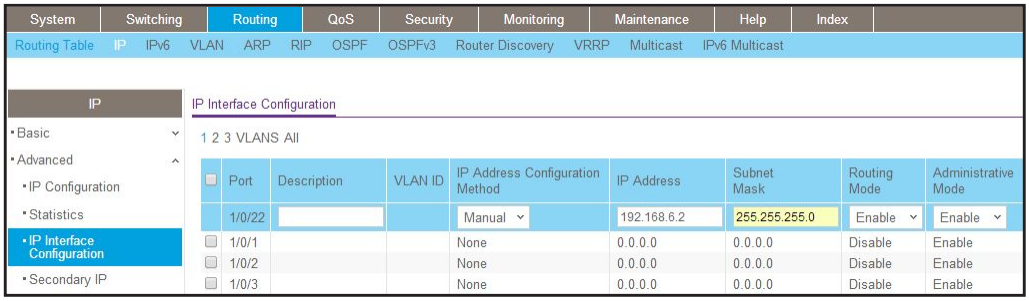
   b. Select the Routing Mode **Enable** radio button.
   c. Click the **Apply** button. Your settings are saved.
2. Configure routing on interface 1/0/21 and assign an IP address to the interface.
   a. Select **Routing > IP > Advanced > IP Interface Configuration**.

      A page similar to the following figure displays.

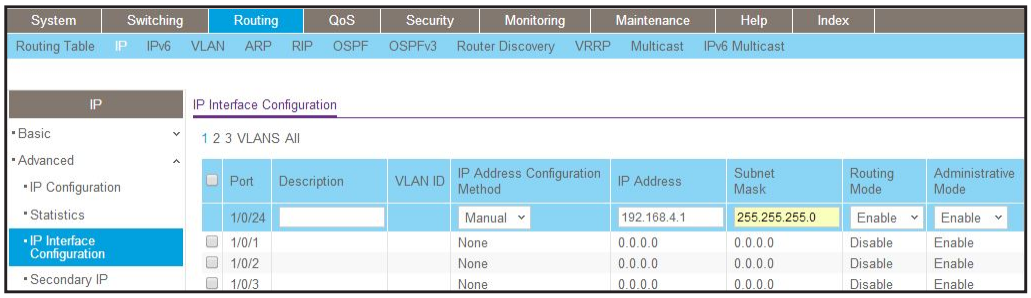


   b. Select the Port **1/0/21** check box.
   c. Configure the following settings:
      - In the **IP Address** field, enter **192.168.2.1**.
      - In the **Subnet Mask** field, enter **255.255.255.0**.
      - In the **Routing Mode** menu, select **Enable**.
   d. Click the **Apply** button. Your settings are saved.

3. Configure routing on interface 1/0/22 and assign an IP address to the interface.
   a. Remain on the same page.

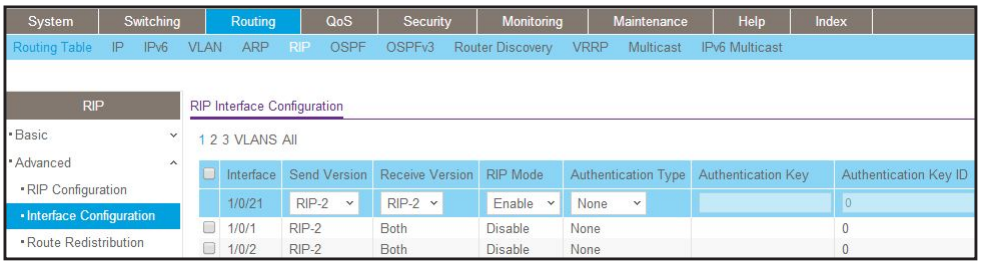


   b. Select the Port **1/0/22** check box.
   c. Configure the following settings:
      - In the **IP Address** field, enter **192.168.6.2**.
      - In the **Subnet Mask** field, enter **255.255.255.0**.
      - In the **Routing Mode** menu, select **Enable**.
   d. Click the **Apply** button. Your settings are saved.
4. Configure routing on interface 1/0/24 and assign an IP address to the interface.
   a. Remain on the same page.



   b. Select the Port **1/0/24** check box.
   c. Configure the following settings:
      - In the **IP Address** field, enter **192.168.4.1**.
      - In the **Subnet Mask** field, enter **255.255.255.0**.
      - In the **Routing Mode** menu, select **Enable**.
   d. Click the **Apply** button. Your settings are saved.
5. Enable RIP on interface 1/0/21.
   a. Select **Routing > RIP > Advanced > Interface Configuration**.

A page similar to the following figure displays.



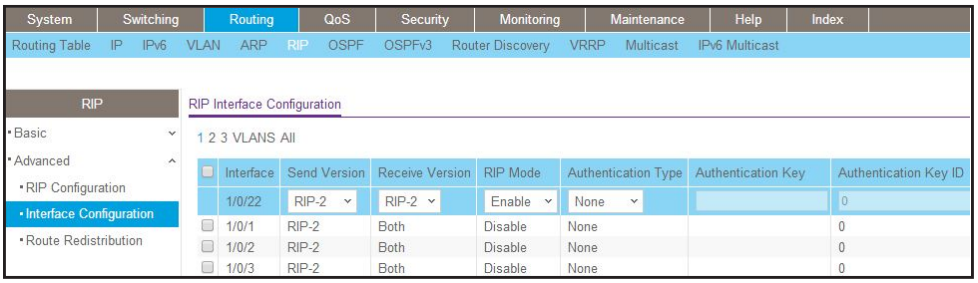
b. Select the Interface **1/0/21** check box.

c. In the **RIP Mode** menu, select **Enable**.

d. Click the **Apply** button. Your settings are saved.

6. Enable RIP on interface 1/0/22.

a. Remain on the same page.



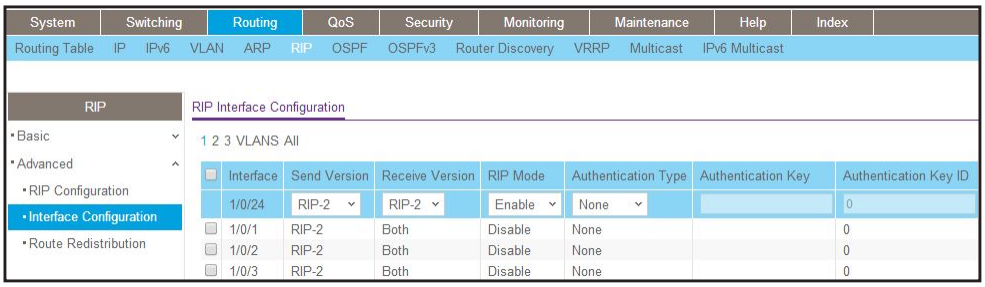
b. Select the Interface **1/0/22** check box.

c. In the **RIP Mode** menu, select **Enable**.

d. Click the **Apply** button. Your settings are saved.

7. Enable RIP on interface 1/0/24.

a. Remain on the same page.



b. Select the Interface **1/0/24** check box.

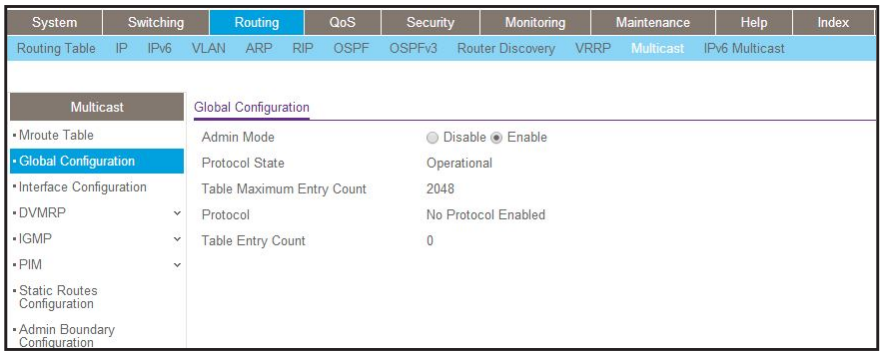
c. In the **RIP Mode** menu, select **Enable**.

d. Click the **Apply** button. Your settings are saved.

8. Enable multicast globally on Switch D.

a. Select **Routing > Multicast > Global Configuration**.

A page similar to the following figure displays.



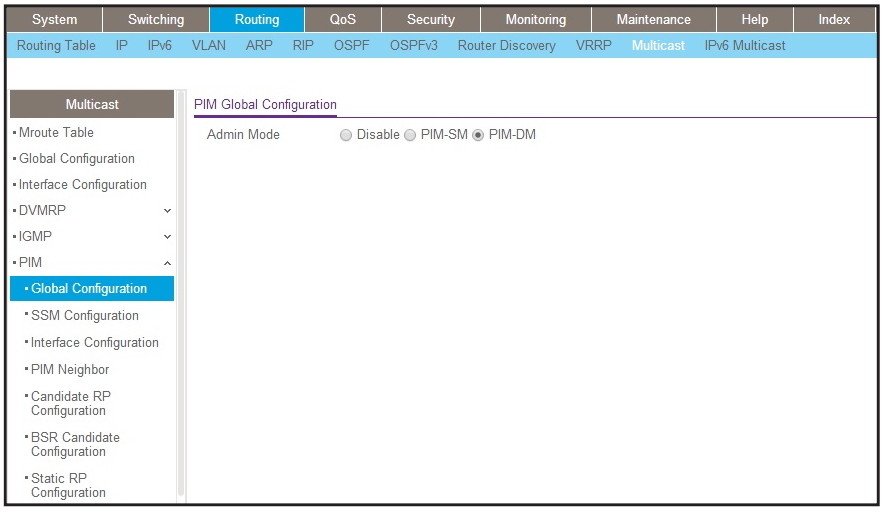
b. Select the Admin Mode **Enable** radio button.

c. Click the **Apply** button. Your settings are saved.

9. Enable PIM-SM globally on Switch D.

a. Select **Routing > Multicast > PIM > Global Configuration**.

A page similar to the following figure displays.



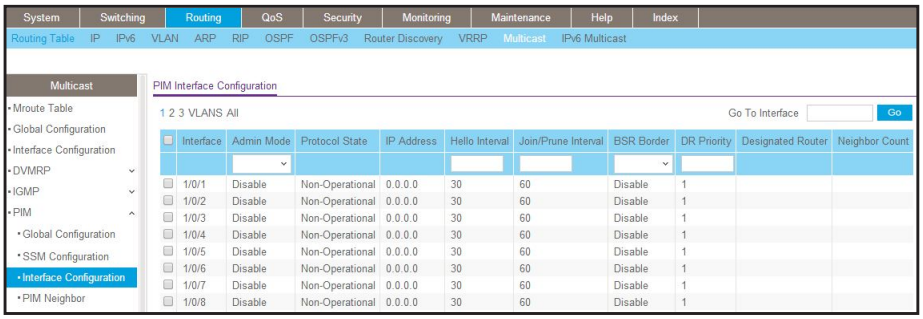
b. Select the Admin Mode **PIM-SM** radio button.

c. Click the **Apply** button. Your settings are saved.

10. Enable PIM on interfaces 1/0/21, 1/0/22, and 1/0/24.

a. Select **Routing > Multicast > PIM > Interface Configuration**.

A page similar to the following figure displays.



b. Select the Interface **1/0/21, 1/0/22**, and **1/0/24** check boxes.

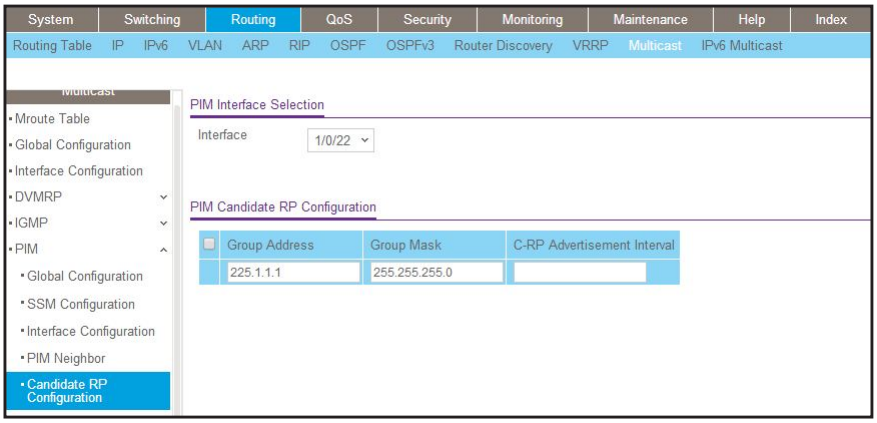
c. In the **Admin Mode** menu, select **Enable**.

d. Click the **Apply** button. Your settings are saved.

11. ‘Set up the RP candidate configuration on Switch D.

a. Select **Routing > Multicast > PIM > Candidate RP Configuration**.

A page similar to the following figure displays.



b. In the **Interface** menu, select **1/0/22**.

c. In the **Group IP** field, enter **225.1.1.1**.

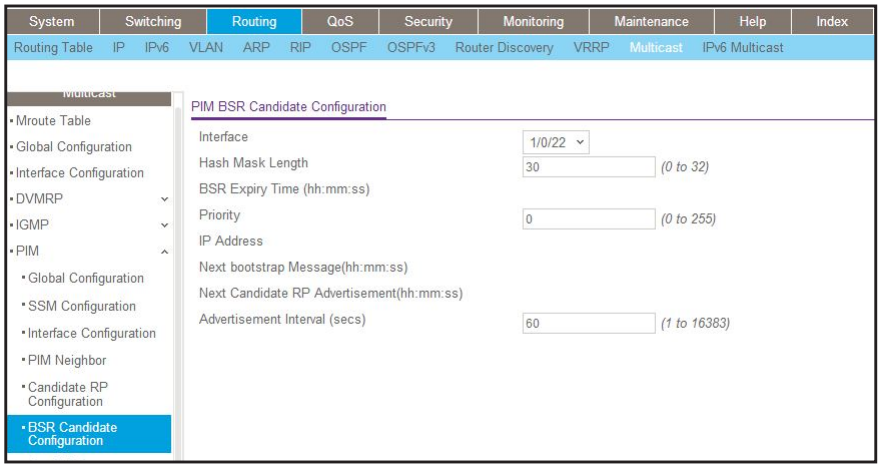
d. In the **Group Mask** field, enter **255.255.255.0**.

e. Click the **Add** button. Your settings are saved.

12. Set up the BSR candidate configuration on Switch D.

a. Select **Routing > Multicast > PIM > BSR Candidate Configuration**.

A page similar to the following figure displays.



b. In the **Interface** menu, select **1/0/22**.

c. In the **Hash Mask Length** field, enter **30**.

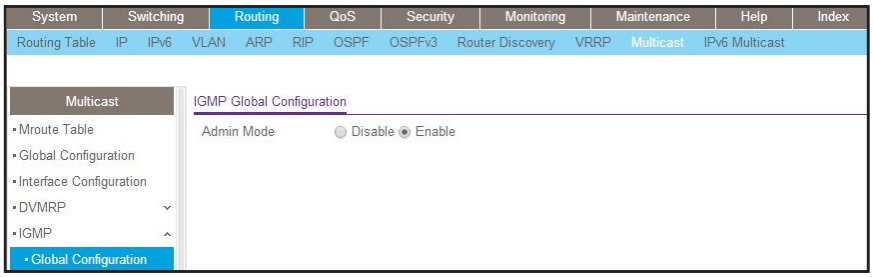
d. In the **Priority** field, enter **3**.

e. Click the **Apply** button. Your settings are saved.

13. Enable IGMP globally on Switch D.

a. Select **Routing > Multicast > IGMP > Global Configuration**.

A page similar to the following figure displays.



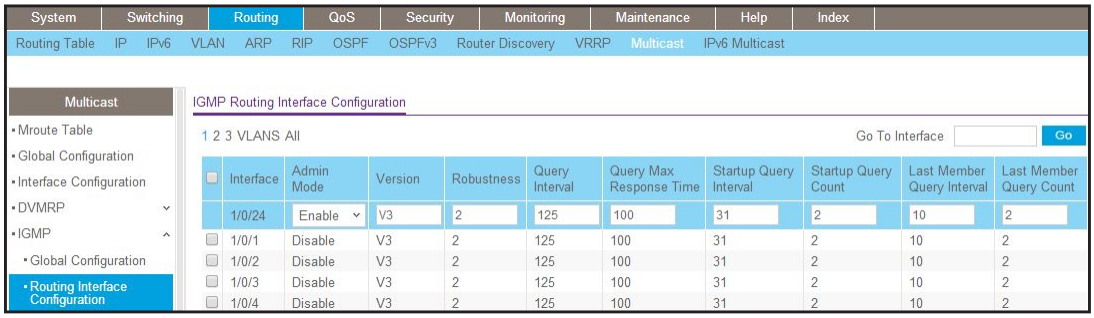
b. Select the Admin Mode **Enable** radio button.

c. Click the **Apply** button. Your settings are saved.

14. Enable IGMP on interface 1/0/24.

a. Select **Routing > Multicast > IGMP > Interface Configuration**.

A page similar to the following figure displays.



b. Select the Interface **1/0/24** check box.

c. In the **Admin Mode** menu, select **Enable**.

d. Click the **Apply** button. Your settings are saved.

32

DHCP L2 Relay and L3 Relay

Dynamic Host Configuration Protocol relays

This feature is supported on the M4250 series switches

This feature is supported on the M4300 series switches

This feature is supported on the M4350 series switches

This chapter includes the following sections:

- DHCP L2 relay
- DHCP L3 relay

DHCP L2 relay

DHCP relay agents eliminate the need for 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.

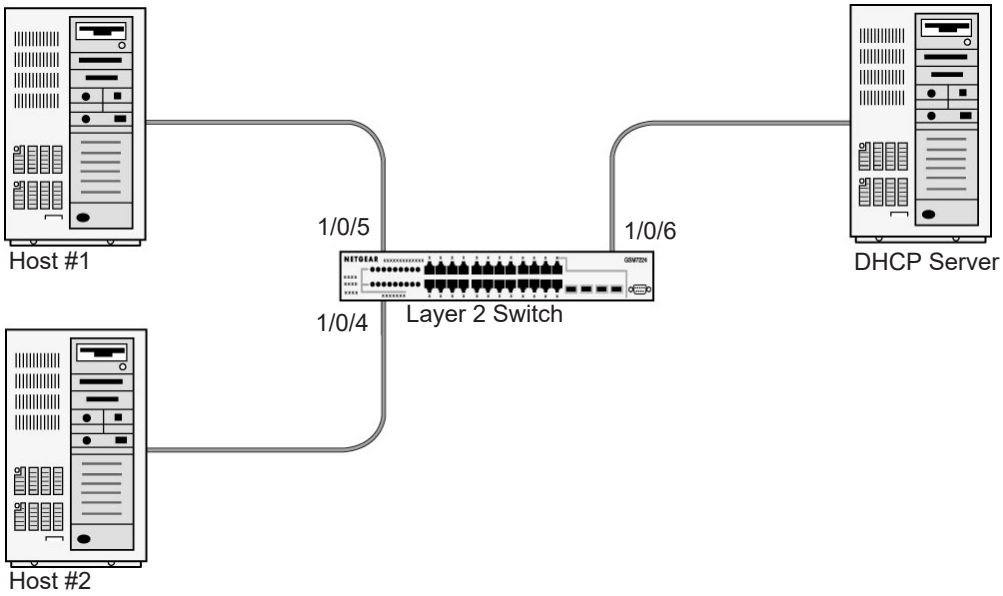


Figure 61. DHCP L2 relay

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.

The following example is shown as CLI commands and as a main UI procedure.

CLI: Configure DHCP L2 relay

To use the CLI to configure DHCP L2 relay:

1. Create VLAN 200:

```
(Netgear Switch)#vlan database
(Netgear Switch)(Vlan)#vlan 200
(Netgear Switch)(Vlan)#exit
```

2. Enable the DHCP L2 relay on VLAN 200.

```
(Netgear Switch) (Config)#dhcp l2relay
(Netgear Switch) (Config)#dhcp l2relay vlan 200
```

3. Enable Option 82 Circuit ID.

```
(Netgear Switch) (Config)#dhcp l2relay circuit-id vlan 200
```

4. Enable Option 82 Remote ID.

```
(Netgear Switch) (Config)#dhcp l2relay remote-id rem_id vlan 200
```

5. Enable DHCP L2 relay on port 1/0/4 and add the port to VLAN 200.

```
(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 and add the port to VLAN 200.

```
(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, trust packets with option 82 received on the port, and add the port to VLAN 200.

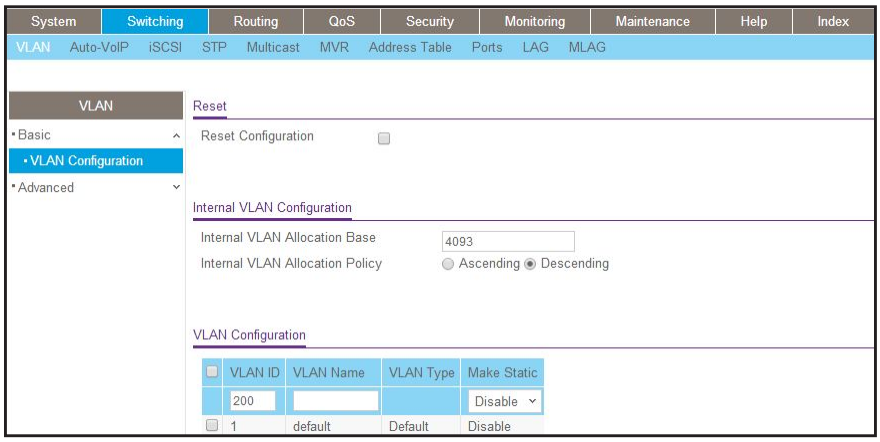
```
(Netgear Switch) (Config)#interface 1/0/6
(Netgear Switch) (Interface 1/0/6)# dhcp l2relay
(Netgear Switch) (Interface 1/0/6)# dhcp l2relay trust
(Netgear Switch) (Interface 1/0/6)# vlan pvid 200
(Netgear Switch) (Interface 1/0/6)# vlan participation include 200
(Netgear Switch) (Interface 1/0/6)# exit
```

Main UI: Configure DHCP L2 relay

To use the main UI to configure DHCP L2 relay:

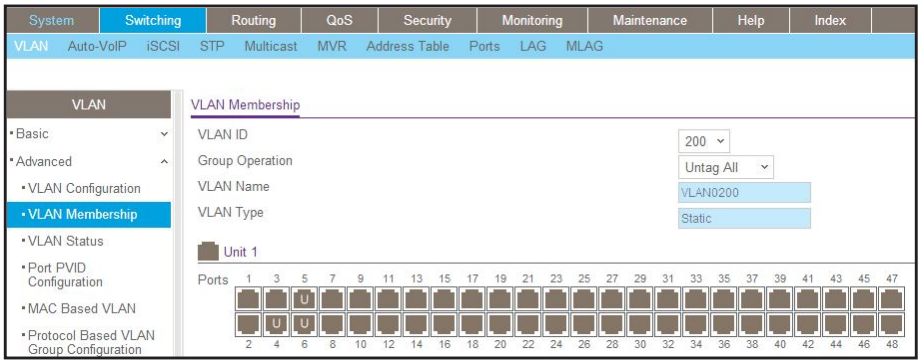
1. Create VLAN 200.
   a. Select **Switching > VLAN > Basic > VLAN Configuration**.

      A page similar to the following figure displays.



   b. In the **VLAN ID** field, enter **200**.
   c. In the **Make Static** menu, select **Static**.
   d. Click the **Add** button. Your settings are saved.
2. Add ports to VLAN 200.
   a. Select **Switching > VLAN > Advanced > VLAN Membership**.

A page similar to the following figure displays.



b. In the **VLAN ID** field, select **200**.

c. Click the gray boxes under ports **4**, **5**, and **6** until U displays, which specifies that the egress packets are untagged for the ports.

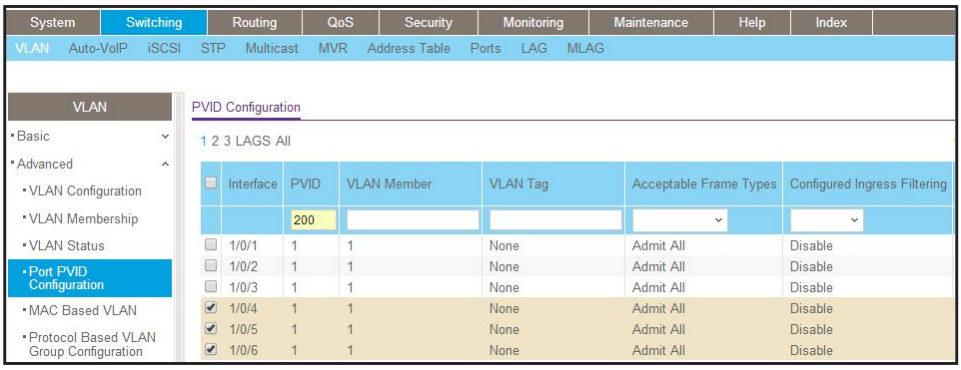
If your switch is a member of a stack, be sure that you select the ports in the correct unit.

d. Click the **Apply** button. Your settings are saved.

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 page similar to the following figure displays.



b. Select the Interface **1/0/4**, **1/0/5**, and **1/0/6** check boxes.

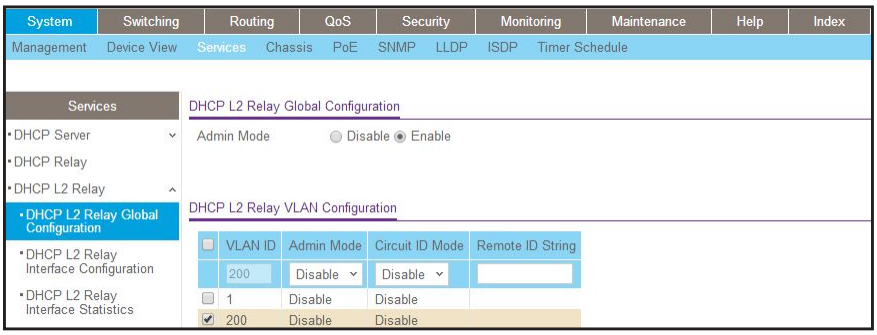
c. In the **PVID** field, enter **200**.

d. Click the **Apply** button. Your settings are saved.

4. Enable DHCP L2 relay on VLAN 200.

a. Select **System > Services > DHCP L2 Relay > DHCP L2 Relay Global Configuration**.

A page similar to the following figure displays.



b. Select the Admin Mode **Enable** radio button.

c. Select the VLAN ID **200** check box.

d. Configure the following settings:

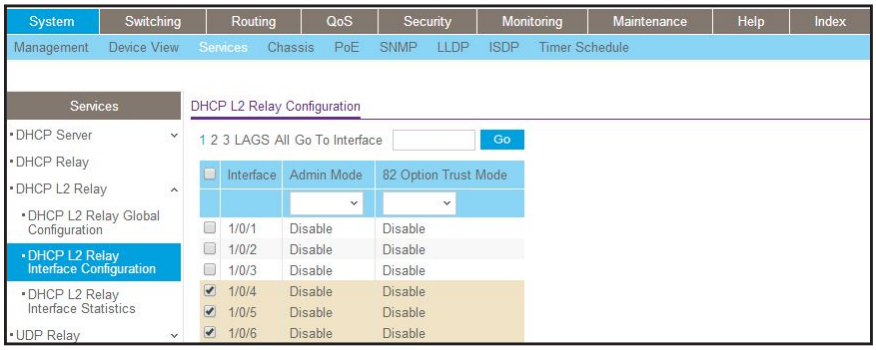
- In the **Admin Mode** menu, select **Enable**.
- In the **Circuit ID Mode** menu, select **Enable**.
- In the **Remote ID String** field, enter **rmt_id**.

e. Click the **Apply** button. Your settings are saved.

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 page similar to the following figure displays.



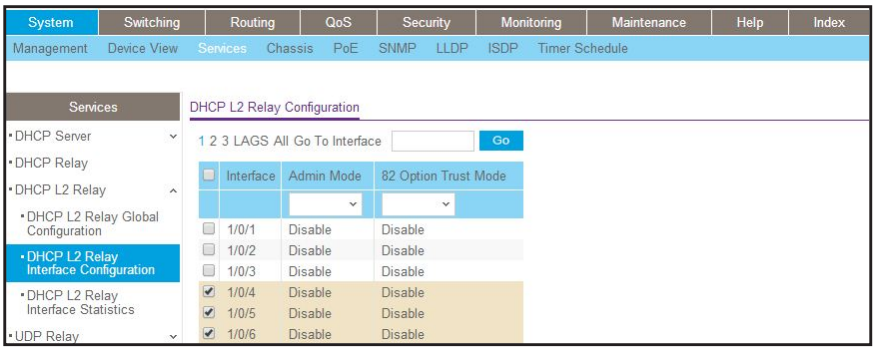
b. Select the Interface **1/0/4**, **1/0/5**, and **1/0/6** check boxes.

c. In the **Admin Mode** menu, select **Enable**.

d. Click the **Apply** button. Your settings are saved.

6. Enable DHCP L2 relay trust on interface 1/0/6.

   Remain on the same page.



   e. Select the Interface **1/0/6** check box.

   f. In the **82 Option Trust Mode** menu, select **Enable**.

   g. Click the **Apply** button. Your settings are saved.

DHCP L3 relay

You can configure DHCP L3 relay through which a DHCP client can receive an IP address from a DHCP server.

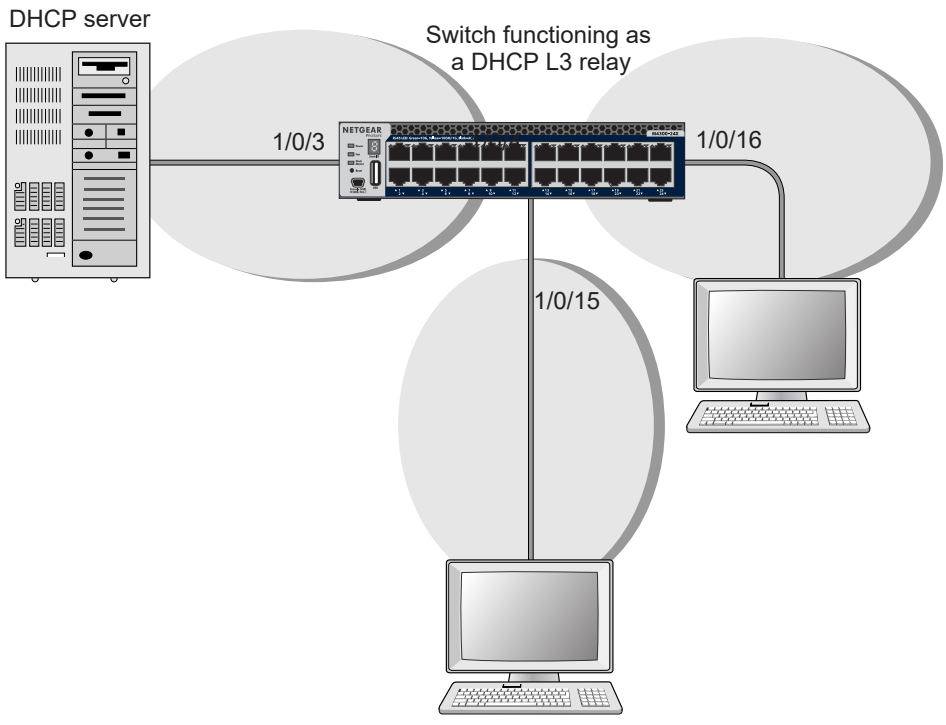


Figure 62. DHCP L3 relay

The example is shown as CLI commands and as a main UI procedure.

CLI: Configure DHCP L3 Relay

To use the CLI to configure DHCP L3 relay:

1. Enable routing on the switch.

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

2. Create routing interface 1/0/4 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 routing interfaces 1/0/15 and 1/0/16, which are connected to clients.

```
(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 DHCP L3 relay.

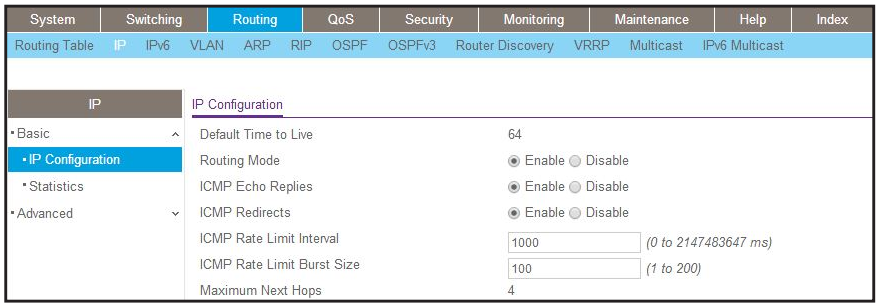
```
(Netgear Switch) (Config)#ip helper-address 10.100.1.1 dhcp
(Netgear Switch) (Config)#ip helper enable
```

Main UI: Configure DHCP L3 relay

To use the main UI to configure DHCP L3 relay:

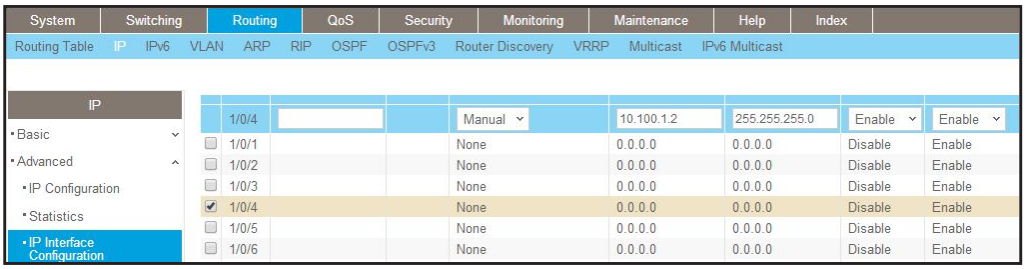
1. Enable routing mode on the switch.
   a. Select **Routing > IP > Basic > IP Configuration**.

      A page similar to the following figure displays.



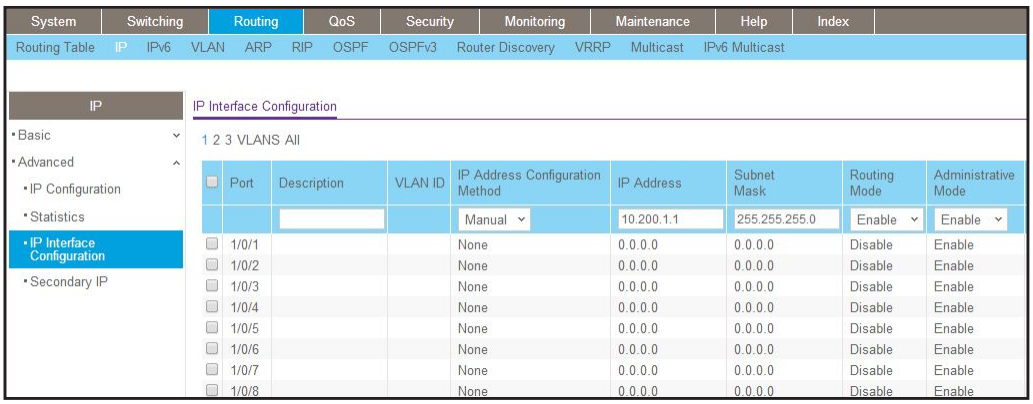
   b. Select the Routing Mode **Enable** radio button.
   c. Click the **Apply** button. Your settings are saved.
2. Create routing interface 1/0/4 and assign 10.100.1.2/24 to it.
   a. Select **Routing > IP > Advanced > IP Interface Configuration**.

      A page similar to the following figure displays.



   b. 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** menu, select **Enable**.
   f. Click the **Apply** button. Your settings are saved.
3. Create routing interface 1/0/15 and assign 10.200.1.1/24 to it.
   a. Select **Routing > IP > Advanced > IP Interface Configuration**.

A page similar to the following figure displays.



b. Select the Port **1/0/15** check box.

c. In the **IP Address Configuration Method** menu, enter **Manual**.

d. In the **IP Address** field, enter **10.200.1.1**.

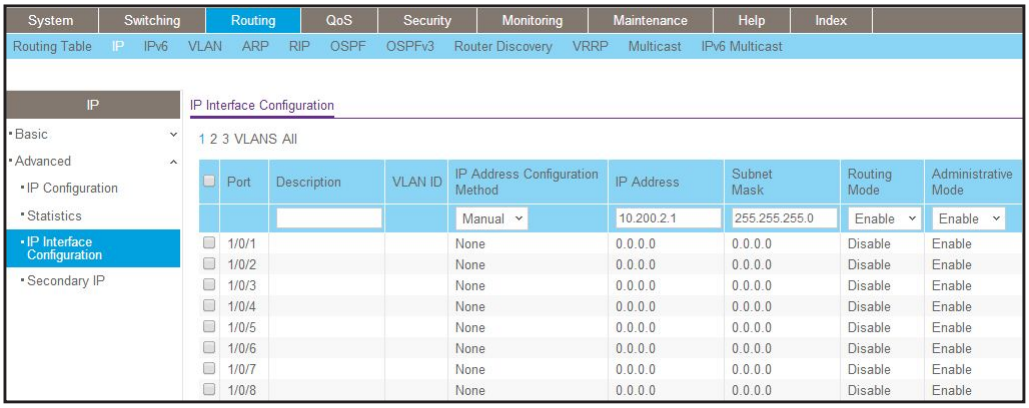
e. In the **Subnet Mask** field, enter **255.255.255.0**.

f. In the **Routing Mode** menu, select **Enable**.

g. Click the **Apply** button. Your settings are saved.

4. Create routing interface 1/0/16 and assign 10.200.2.1/24 to it.

a. Remain on the same page.



b. Select the Port **1/0/16** check box.

c. In the **IP Address Configuration Method** menu, select **Manual**.

d. In the **IP Address** field, enter **10.200.2.1**.

e. In the **Subnet Mask** field, enter **255.255.255.0**.

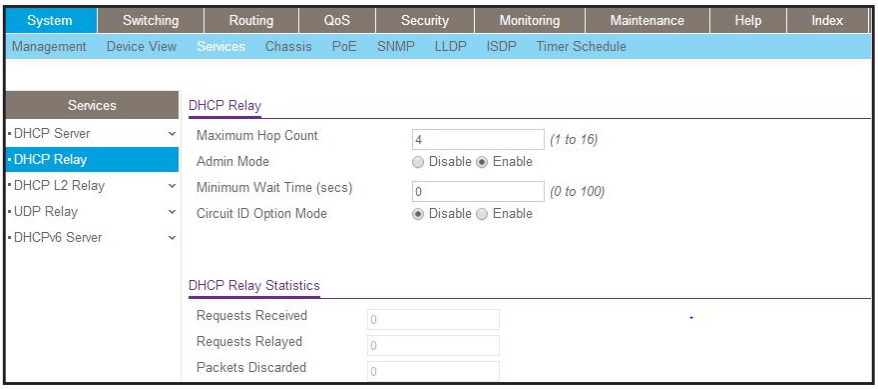
f. In the **Routing Mode** menu, select **Enable**.

g. Click the **Apply** button. Your settings are saved.

5. Enable DHCP L3 relay.

a. Select **System > Services > DHCP Relay**.

A page similar to the following figure displays.



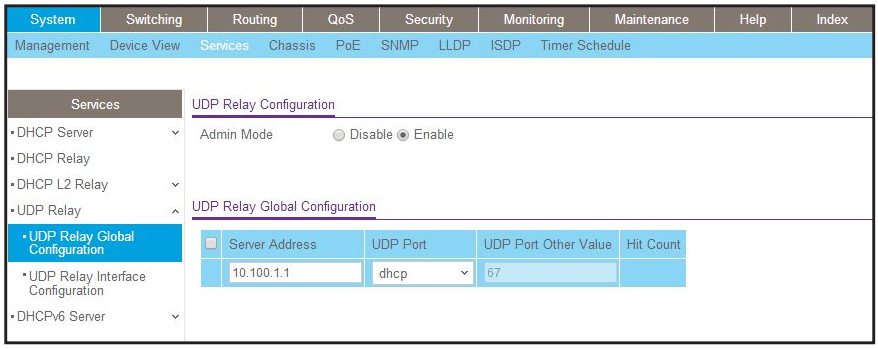
b. Select the Admin Mode **Enable** radio button.

c. Click the **Apply** button. Your settings are saved.

6. Configure the DHCP server IP address.

a. Select **System > Services > UDP Relay**.

A page similar to the following figure displays.



b. In the **Server Address** field, enter **10.100.1.1**.

c. In the **UDP Port** menu, select **dhcp**.

d. Click the **Add** button. Your settings are saved.

33

MLD

Multicast Listener Discovery

This feature is supported on the M4250 series switches

This feature is supported on the M4300 series switches

This feature is supported on the M4350 series switches

This chapter includes the following sections:

- Multicast Listener Discovery concepts
- Configure MLD
- Configure MLD snooping

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 example, 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.

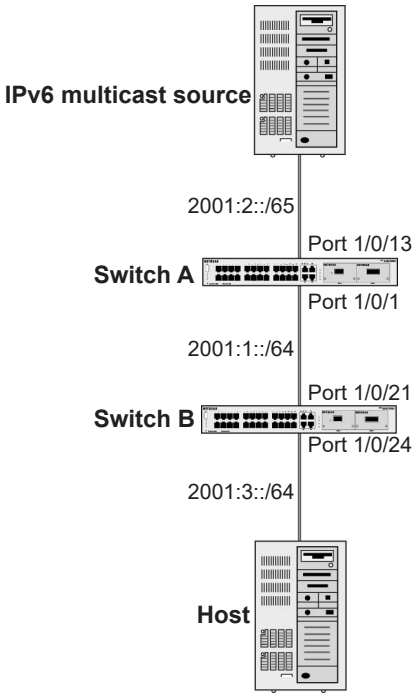


Figure 63. Configure MLD

The example is shown as CLI commands and as a main UI procedure.

CLI: Configure MLD

You must configure MLD and related features on Switch A and Switch B.

CLI: Configure MLD on Switch A

To use the CLI to configure MLD on Switch A:

1. Configure a static IPv6 route on VLAN 1 to build a unicast route table on Switch A.

```
(Netgear Switch) #configure
(Netgear Switch) (Config)#ipv6 route 2001:db8:1234::/48 interface vlan 1
(Netgear Switch) (Config)#exit
```

2. Enable IPv6 unicast routing on Switch A.

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

3. Enable IPv6 MLD on Switch A.

```
(Netgear Switch) (Config)#ipv6 mld router
```

4. Enable IPv6 PIM-DM on Switch A.

```
(Netgear Switch) (Config)#ipv6 pim dense
```

5. Enable IP multicast forwarding on Switch A.

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

6. Enable routing and PIM 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::1/64
(Netgear Switch) (Interface 1/0/1)#ipv6 enable
(Netgear Switch) (Interface 1/0/1)#ipv6 pim
(Netgear Switch) (Interface 1/0/1)#exit
```

7. Enable routing, PIM, and OSPF on interface 1/0/13.

```
(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
```

CLI: Configure MLD on Switch B

To use the CLI to configure MLD on Switch B:

1. Configure a static IPv6 route on VLAN 1 to build a unicast route table on Switch B.

```
(Netgear Switch) #configure
(Netgear Switch) (Config)#ipv6 route 2001:db8:1234::/48 interface vlan 1
(Netgear Switch) (Config)#exit
```

2. Enable IPv6 unicast routing on Switch B.

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

3. Enable IPv6 MLD on Switch B.

```
(Netgear Switch) (Config)#ipv6 mld router
```

4. Enable IPv6 PIM-DM on Switch B.

```
(Netgear Switch) (Config)#ipv6 pim dense
```

5. Enable IP multicast forwarding on Switch B.

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

6. Enable routing and PIM on interface 1/0/21.

```
(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)#exit
```

7. Enable routing, MLD, and PIM on interface 1/0/24.

```
(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
```

8. Display the MLD group information on Switch 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
```

Main UI: Configure MLD

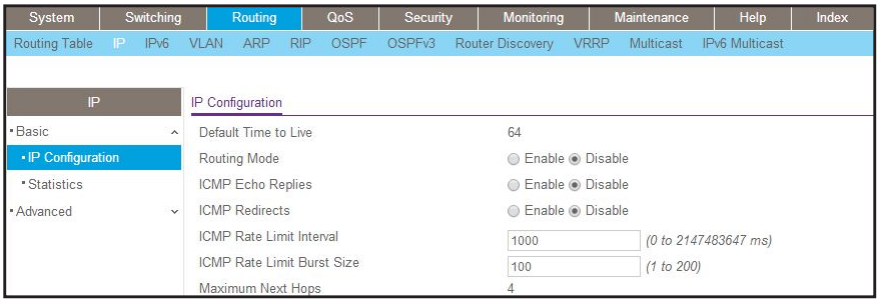
You must configure MLD and related features on Switch A and Switch B.

Main UI: Configure MLD on Switch A

To use the main UI to configure MLD on Switch A:

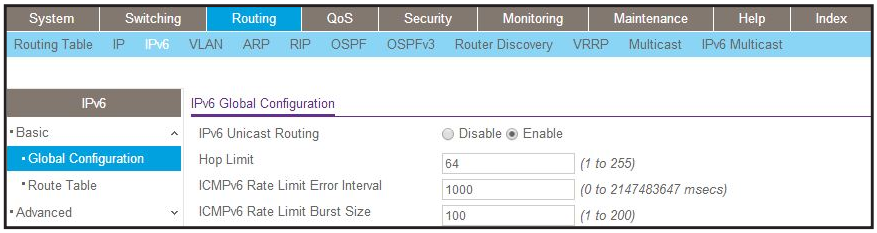
1. Enable IP routing on the switch.
   a. Select **Routing > IP > Basic > IP Configuration**.

      A page similar to the following figure displays.



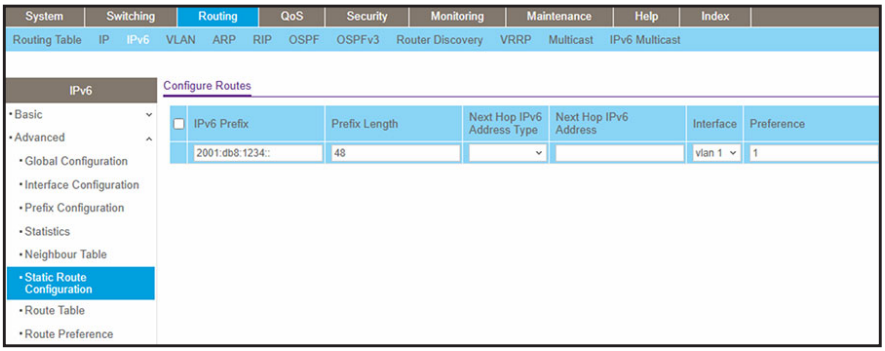
   b. Select the Routing Mode **Enable** radio button.
   c. Click the **Apply** button. Your settings are saved.
2. Enable IPv6 unicast routing on the switch.
   a. Select **Routing > IPv6 > Basic > Global Configuration**.

      A page similar to the following figure displays.



   b. Select the IPv6 Unicast Routing **Enable** radio button.
   c. Click the **Apply** button. Your settings are saved.
3. Configure a static IPv6 route on VLAN 1 to build a unicast route table on Switch A.
   a. Select **Routing > IPv6 > Advanced > Static Route Configuration**.

A page similar to the following figure displays.



b. Configure the following settings:

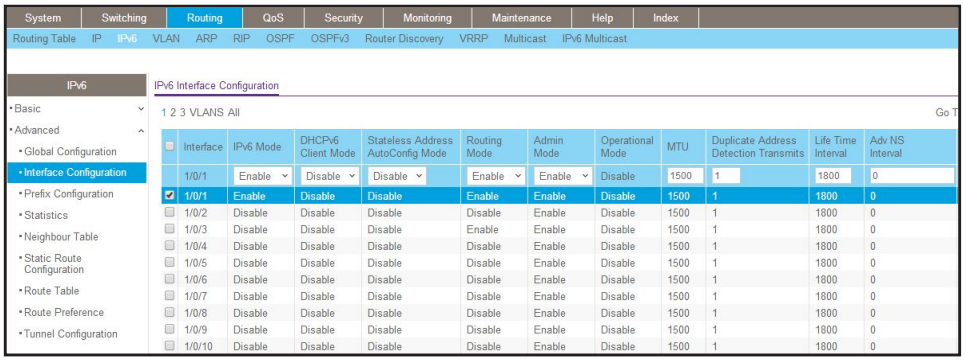
- In the **IPv6 Prefix** field, enter **2001:db8:1234::**.
- In the **Prefix Length** field, enter **48**.
- In the **Interface** menu, select **vlan 1**.
- In the **Preference** field, enter **1** (the default setting).

c. Click the **Apply** button. Your settings are saved.

4. Configure IPv6 routing on interfaces 1/0/1 and 1/0/13.

a. Select **Routing > IPv6 > Advanced > Interface Configuration**.

A page similar to the following figure displays.



b. Select the Interface **1/0/1** and **1/0/13** check boxes.

c. Configure the following settings:

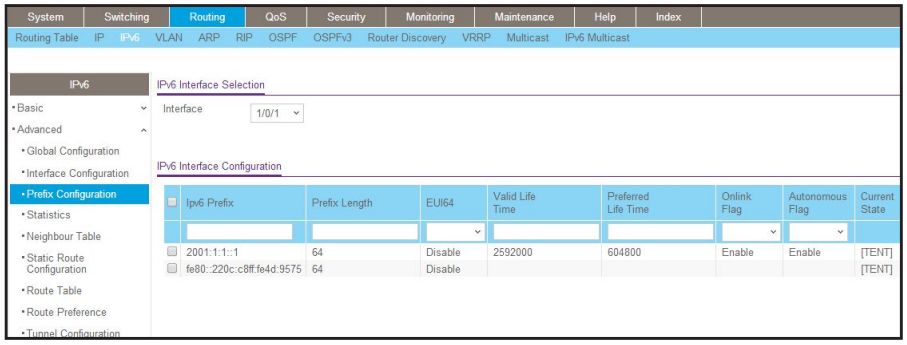
- In the **IPv6 Mode** menu, select **Enable**.
- In the **Routing Mode** menu, select **Enable**.
- In the **Admin Mode** menu, select **Enable**.

d. Click the **Apply** button. Your settings are saved.

5. Assign an IPv6 address to interface 1/0/1.

a. Select **Routing > IPv6 > Advanced > Prefix Configuration**.

A page similar to the following figure displays.



b. In the **Interface** menu, select **1/0/1**.

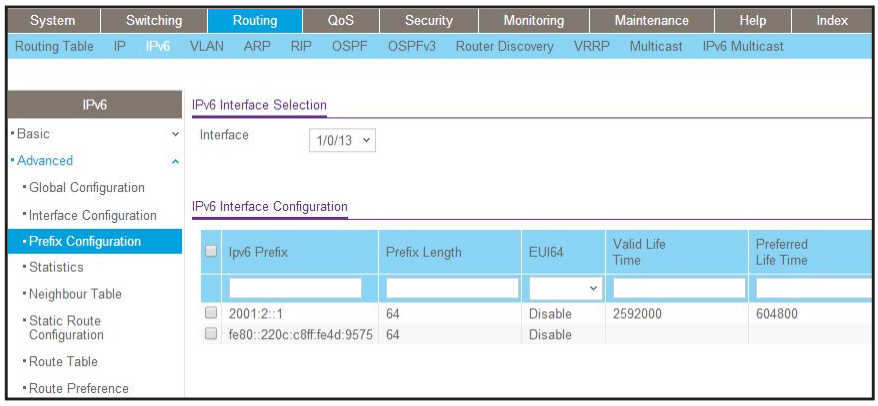
c. Configure the following settings:

- In the **IPv6 Prefix** field, enter **2001:1::1**.
- In the **Prefix Length** field, enter **64**.
- In the **EUI64** menu, select **Disable**.

d. Click the **Add** button. Your settings are saved.

6. Assign an IPv6 address to interface 1/0/13.

a. Remain on the same page.



b. In the **Interface** menu, select **1/0/13**.

c. Configure the following settings:

- In the **IPv6 Prefix** field, enter **2001:2::1**.
- In the **Prefix Length** field, enter **64**.
- In the **EUI64** menu, select **Disable**.

d. Click the **Add** button. Your settings are saved.

7. Enable multicast globally on Switch A.

a. Select **Routing > Multicast > Global Configuration**.

A page similar to the following figure displays.

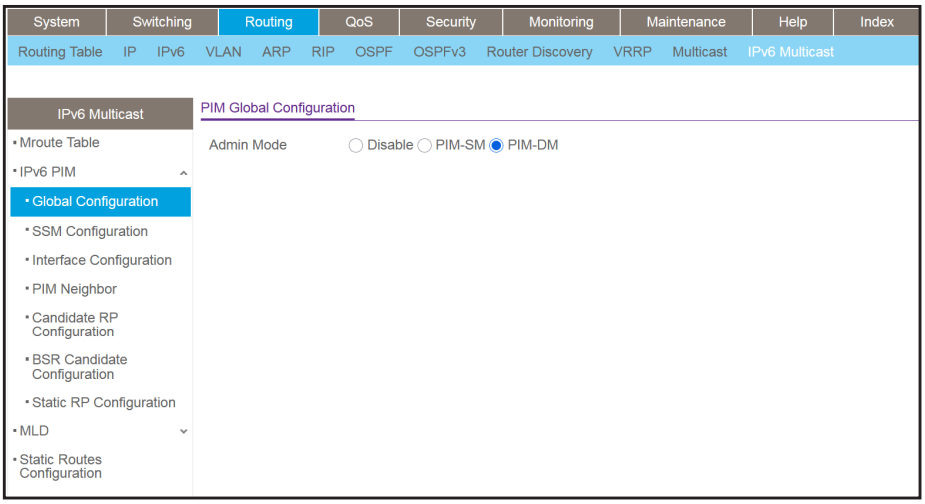
b. Select the Admin Mode **Enable** radio button.

c. Click the **Apply** button. Your settings are saved.

8. Enable PIM-DM globally on Switch A.

a. Select **Routing > IPv6 Multicast > IPv6 PIM > Global Configuration**.

A page similar to the following figure displays.



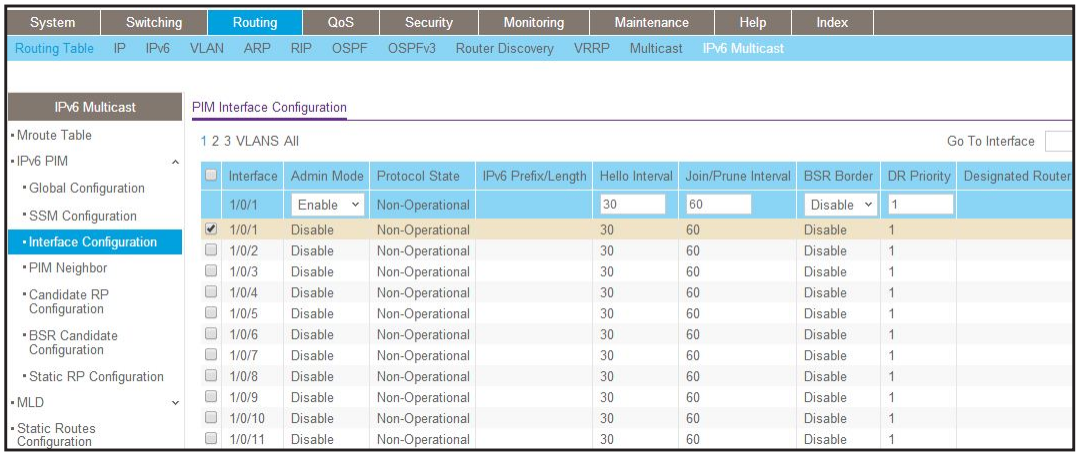
b. Select the Admin Mode **PIM-DM** radio button.

c. Click the **Apply** button. Your settings are saved.

9. Enable PIM on interfaces 1/0/1 and 1/0/13.

a. Select **Routing > IPv6 Multicast > IPv6 PIM > Interface Configuration**.

A page similar to the following figure displays.



b. Select the Interface **1/0/1** and **1/0/13** check boxes.

c. In the **Admin Mode** menu, select **Enable**.

d. Click the **Apply** button. Your settings are saved.

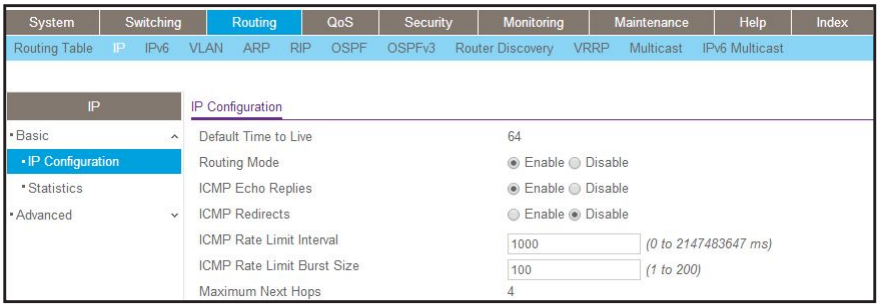
Main UI: Configure MLD on Switch B

To use the main UI to configure MLD on Switch B:

1. Enable IP routing on Switch B.

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

A page similar to the following figure displays.



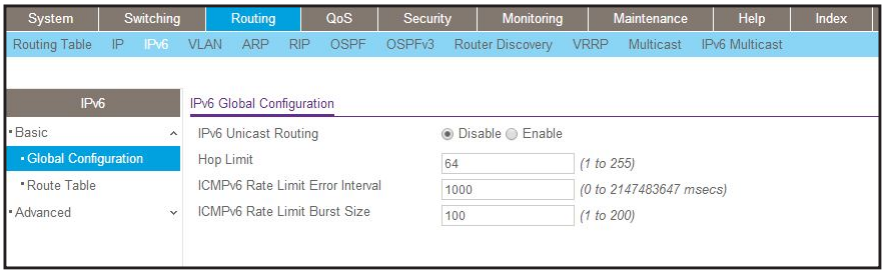
b. Select the Routing Mode **Enable** radio button.

c. Click the **Apply** button. Your settings are saved.

2. Enable IPv6 unicast routing on Switch B.

a. Select **Routing > IPv6 > Basic > Global Configuration**.

A page similar to the following figure displays.



b. Select the IPv6 Unicast Routing **Enable** radio button.

c. Click the **Apply** button. Your settings are saved.

3. Configure a static IPv6 route on VLAN 1 to build a unicast route table on Switch B.

a. Select **Routing > IPv6 > Advanced > Static Route Configuration**.

A page similar to the following figure displays.

b. Configure the following settings:

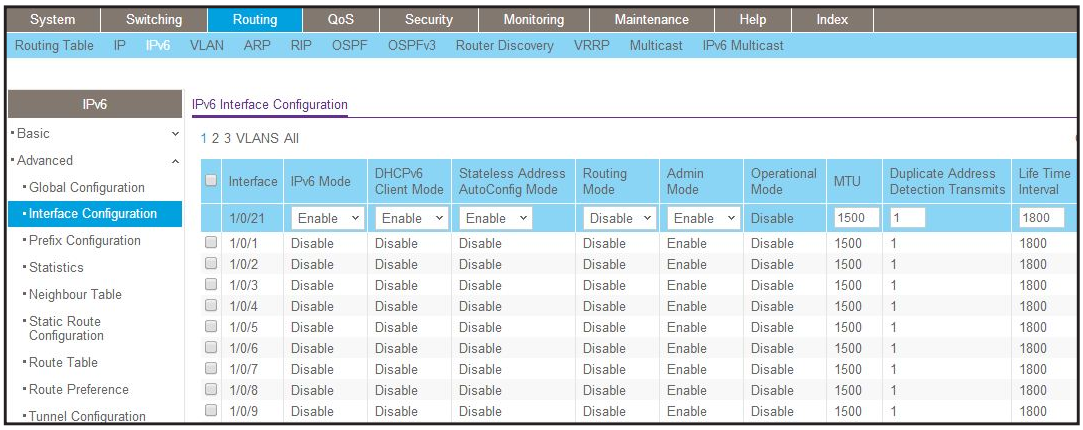
- In the **IPv6 Prefix** field, enter **2001:db8:1234::**.
- In the **Prefix Length** field, enter **48**.
- In the **Interface** menu, select **vlan 1**.
- In the **Preference** field, enter **1** (the default setting).

c. Click the **Apply** button. Your settings are saved.

4. Configure IPv6 routing on interfaces 1/0/21 and 1/0/24.

a. Select **Routing > IPv6 > Advanced > Interface Configuration**.

A page similar to the following figure displays.



b. Select the Interface **1/0/21** and **1/0/24** check boxes.

c. Configure the following settings:

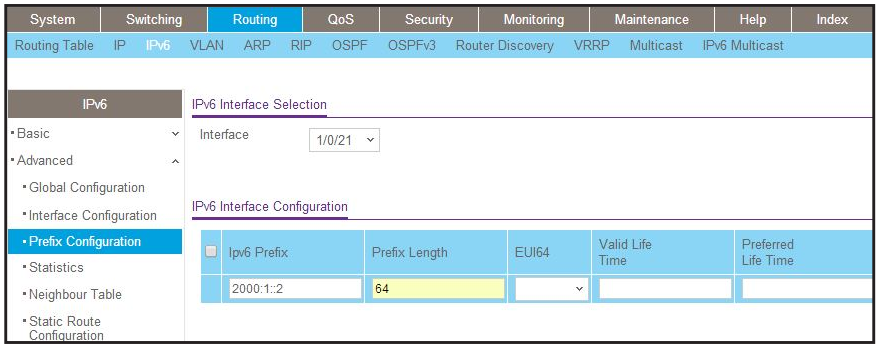
- In the **IPv6 Mode** menu, select **Enable**.
- In the **Routing Mode** menu, select **Enable**.
- In the **Admin Mode** menu, select **Enable**.

d. Click the **Apply** button. Your settings are saved.

5. Assign an IPv6 address to interface 1/0/21.

a. Select **Routing > IPv6 > Advanced > Prefix Configuration**.

A page similar to the following figure displays.



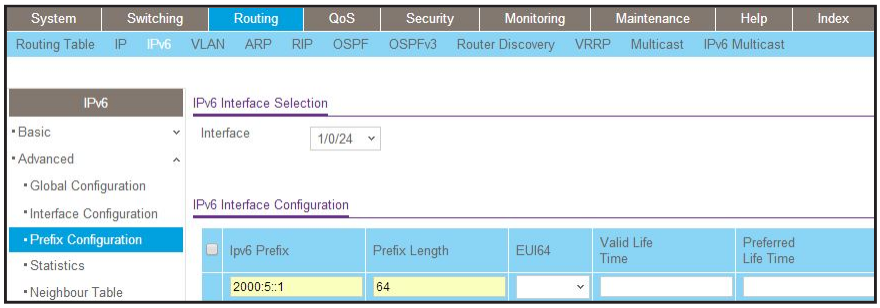
b. In the Interface field, select **1/0/21**.

c. Configure the following settings:

- In the **IPv6 Prefix** field, enter **2001:1::2**.
- In the **Prefix Length** field, enter **64**.
- In the **EUI64** menu, select **Disable**.

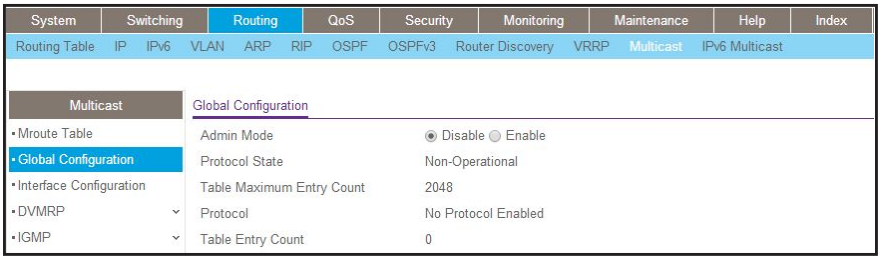
d. Click the **Add** button. Your settings are saved.

6. Assign an IPv6 address to interface 1/0/24.
   a. Remain on the same page.



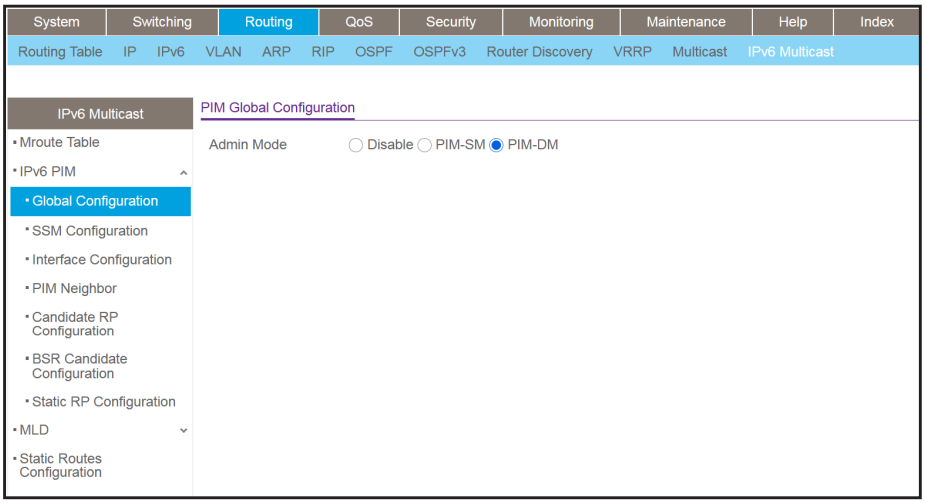
   b. In the **Interface** menu, select **1/0/24**.
   c. Configure the following settings:
      - In the **IPv6 Prefix** field, enter **2001:3::1**.
      - In the **Prefix Length** field, enter **64**.
      - In the **EUI64** menu, select **Disable**.
   d. Click the **Add** button. Your settings are saved.
7. Enable multicast globally on Switch B.
   a. Select **Routing > Multicast > Global Configuration**.

      A page similar to the following figure displays.



   b. Select the Admin Mode **Enable** radio button.
   c. Click the **Apply** button. Your settings are saved.
8. Enable PIM-DM globally on Switch B.
   a. Select **Routing > IPv6 Multicast > IPv6 PIM > Global Configuration**.

A page similar to the following figure displays.



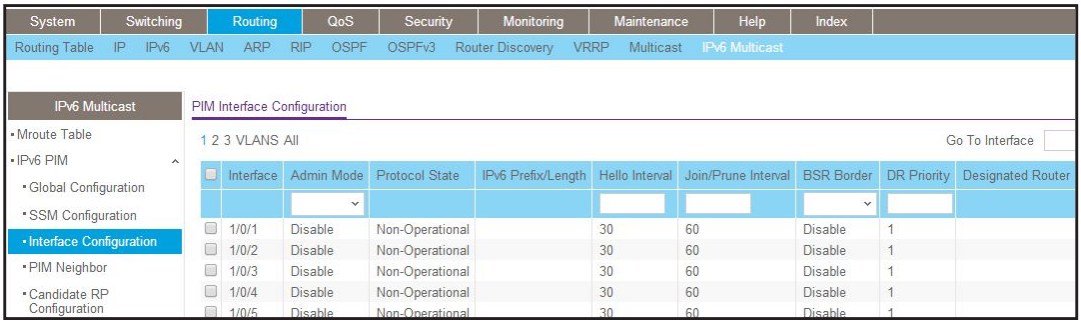
b. Select the Admin Mode **PIM-DM** radio button.

c. Click the **Apply** button. Your settings are saved.

9. Enable PIM on interfaces 1/0/21 and 1/0/24.

a. Select **Routing > IPv6 Multicast > IPv6 PIM > Interface Configuration**.

A page similar to the following figure displays.



b. Select the Interface **1/0/21** and **1/0/24** check boxes.

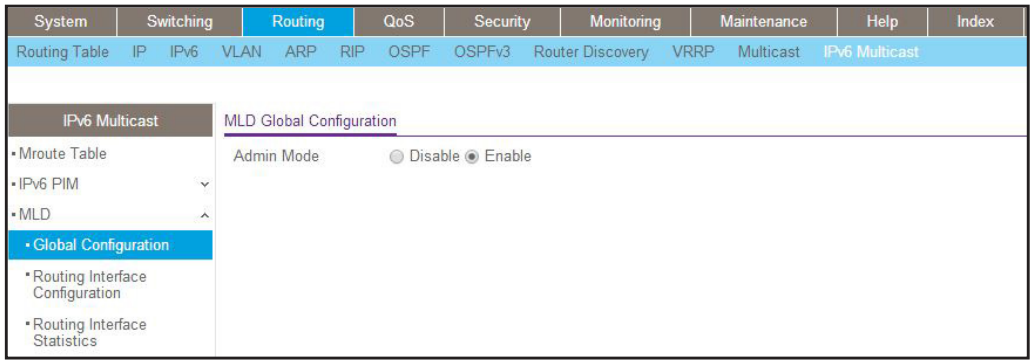
c. In the **Admin Mode** menu, select **Enable**.

d. Click the **Apply** button. Your settings are saved.

10. Enable MLD globally on Switch B.

a. Select **Routing > IPv6 Multicast > MLD > Global Configuration**.

A page similar to the following figure displays.



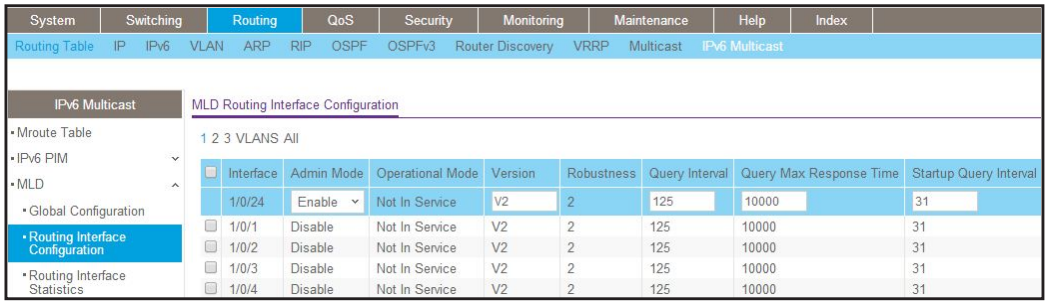
b. Select the Admin Mode **Enable** radio button.

c. Click the **Apply** button. Your settings are saved.

11. Enable MLD on interface 1/0/24.

a. Select **Routing > IPv6 Multicast > MLD > Routing Interface Configuration**.

A page similar to the following figure displays.



b. Select the Interface **1/0/24** check box.

c. In the **Admin Mode** menu, select **Enable**.

d. Click the **Apply** button. Your settings are saved.

Configure 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 request 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 that is 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. You can configure the switch to perform MLD snooping and IGMP snooping simultaneously.

CLI: Configure MLD snooping

To use the CLI to configure MLD snooping:

1. Create VLAN 300.

```
(Netgear Switch) #vlan
(Netgear Switch) (Vlan)#vlan 300
(Netgear Switch) (Vlan)#exit
```

2. Add interfaces 0/1 and 0/24 to VLAN 300.

```
(Netgear Switch) #config
(Netgear Switch) (Config)#interface 0/1
(Netgear Switch) (Interface 0/1)#vlan participation include 300
(Netgear Switch) (Interface 0/1)#vlan pvid 300
(Netgear Switch) (Interface 0/1)#exit
(Netgear Switch) (Config)#interface 1/0/4
(Netgear Switch) (Interface 0/4)#vlan participation include 300
(Netgear Switch) (Interface 0/4)#vlan pvid 300
(Netgear Switch) (Interface 0/4)#exit
(Netgear Switch) (Config)#exit
(Netgear Switch) (Config)#set mld
(Netgear Switch) (Config)#exit
```

3. Enable MLD snooping on VLAN 300.

```
(Netgear Switch) #vlan database
(Netgear Switch) (Vlan)#set mld 300
(Netgear Switch) (Vlan)#exit
```

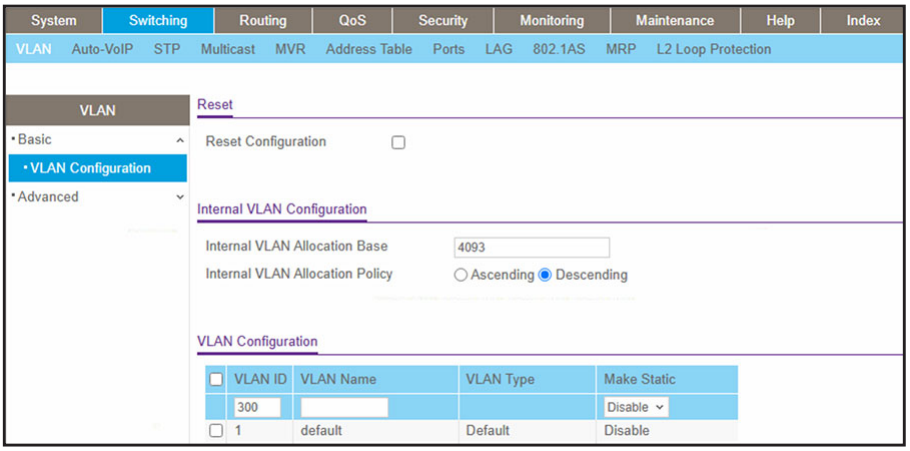
4. Display the MLD snooping configuration.

```
(Netgear Switch) #show mldsnooping
Admin Mode..................................... Enable
Multicast Control Frame Count.................. 0
Interfaces Enabled for MLD Snooping............ None
VLANs enabled for MLD snooping................. 300
```

Main UI: Configure MLD snooping

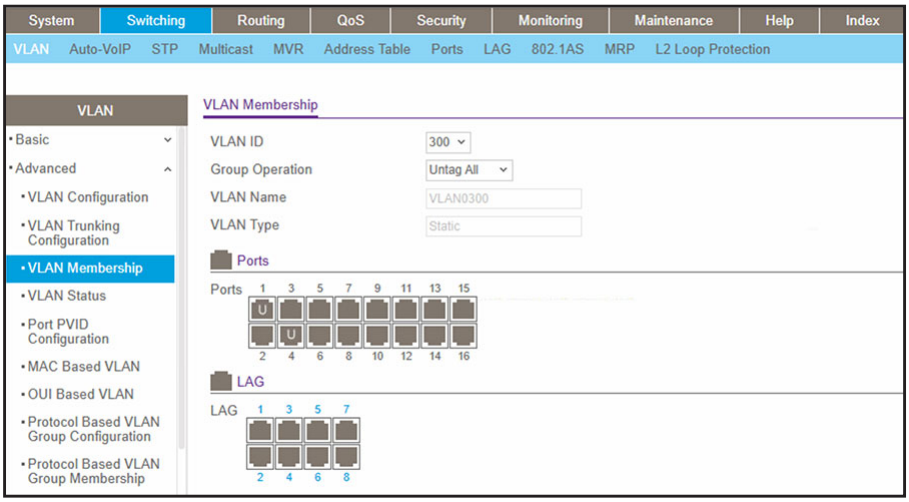
1. Create VLAN 300.
   a. Select **Switching > VLAN > Basic > VLAN Configuration**.

      A page similar to the following figure displays.



   b. In the **VLAN ID** field, enter **300**.
   c. Click the **Add** button. Your settings are saved.
2. Assign interfaces 0/1 and 0/4 to VLAN 300.
   a. Select **Switching > VLAN > Advanced > VLAN Membership**.

A page similar to the following figure displays.



b. In the **VLAN ID** menu, select **300**.

c. Click the gray boxes under ports **1** and **4** until U displays, which specifies that the egress packets are untagged for the ports.

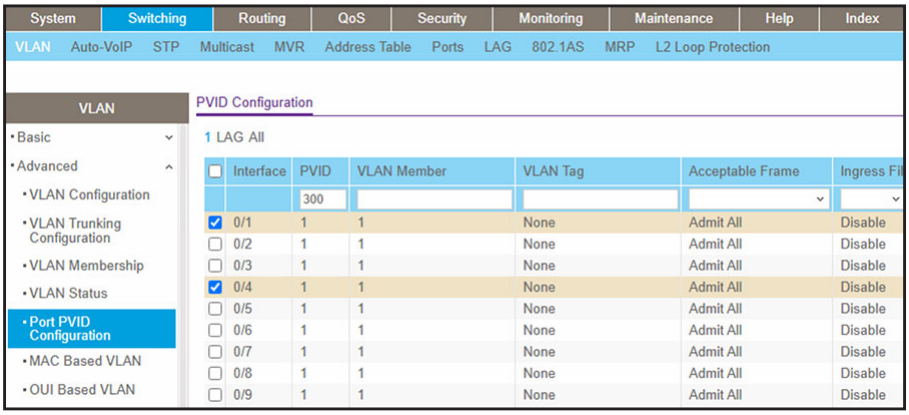
If your switch is a member of a stack, be sure that you select the ports in the correct unit.

d. Click the **Apply** button. Your settings are saved.

3. Assign a PVID to interfaces 0/1 and 0/4.

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

A page similar to the following figure displays.



b. Select the interface **0/1** and **0/4** check boxes.

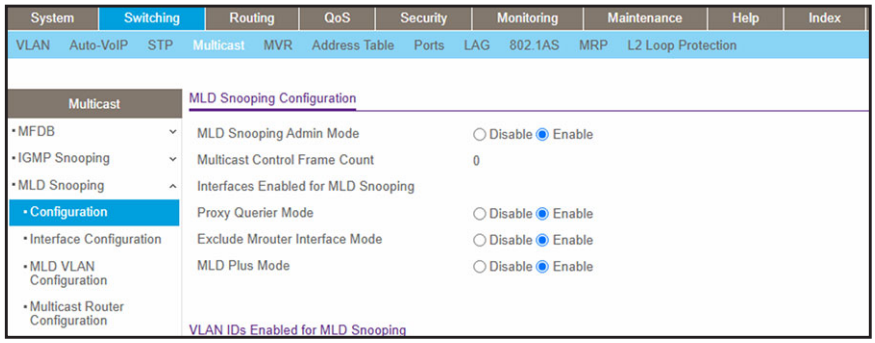
c. In the **PVID** field, enter **300**.

d. Click the **Apply** button. Your settings are saved.

4. Enable MLD snooping and MLD Plus Mode on the switch.

a. Select **Switching > Multicast > MLD Snooping > Configuration**.

A page similar to the following figure displays.



b. Select the MLD Snooping Admin Mode **Enable** radio button.

c. Select the MLD Plus Mode **Enable** radio button.

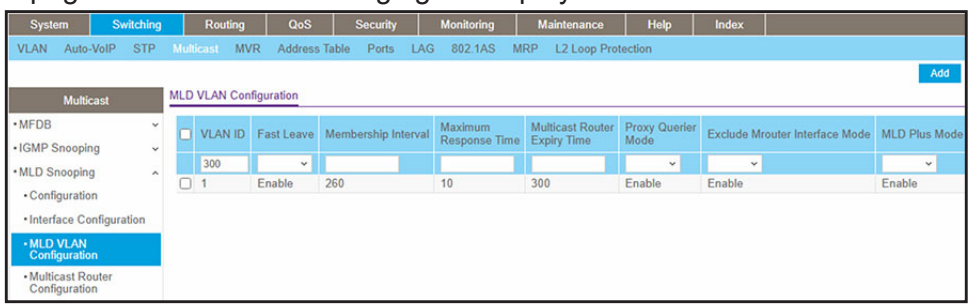
By default, MLD Plus Mode is enabled.

d. Click the **Apply** button. Your settings are saved.

5. Enable MLD snooping on VLAN 300.

a. Select **Switching > Multicast > MLD Snooping > MLD VLAN Configuration**.

A page similar to the following figure displays.



b. In the **VLAN ID** field, enter **300**.

c. Click the **Add** button. Your settings are saved.

34

DVMRP

Distance Vector Multicast Routing Protocol

This feature is supported on the M4300 series switches

This feature is supported on the M4350 series switches

This chapter includes the following sections:

- Distance Vector Multicast Routing Protocol concepts
- Configure DVMRP

Note: The Distance Vector Multicast Routing Protocol (DVMRP) feature is supported on the M4300 series and M4350 series switches only. The M4250 series switches do not support DVMRP.

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.

DVMRP operates as follows:

1. 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.
2. TTL restricts the area to be flooded by the message.
3. All the leaf routers that do not have members on directly attached subnetworks send back prune messages to the upstream router.
4. The branch that transmitted a prune message is deleted from the delivery tree.
5. The delivery tree, which is spanning to all the members in the multicast group, is constructed.

Configure DVMRP

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 that is built by DVMRP.

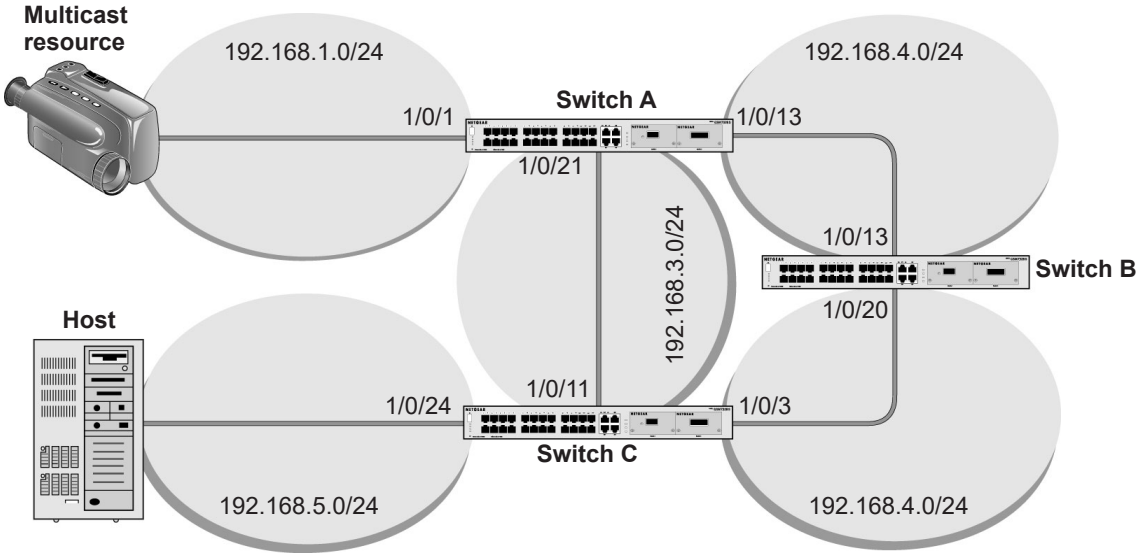


Figure 64. DVMRP

The example is shown as CLI commands and as a main UI procedure.

CLI: Configure DVMRP

You must configure DVMRP and related features on Switch A, Switch B, and Switch C.

CLI: Configure DVMRP on Switch A

To use the CLI to configure DVMRP 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 Switch A.

```
(Netgear Switch) (Config)#ip multicast
```

3. Enable DVMRP protocol on Switch A.

```
(Netgear Switch) (Config)#ip dvmrp
```

4. Enable DVMRP mode on 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
```

5. Display the DVMRP neighbors on Switch A.

```
(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
```

6. Display the multicast route summary on Switch A.

```
(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
```

CLI: Configure DVMRP on Switch B

To use the CLI to configure DVMRP 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 192.1.168.4.1 255.255.255.0
(Netgear Switch) (Interface 1/0/20)#exit
(Netgear Switch) (Config)#exit
```

2. Enable IP multicast forwarding on Switch B.

```
(Netgear Switch) (Config)#ip multicast
```

3. Enable DVMRP protocol on Switch B.

```
(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
```

5. Display the DVMRP neighbors on Switch B.

```
(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
```

6. Display the multicast route summary on Switch B.

```
(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
```

CLI: Configure DVMRP on Switch C

To use the CLI to configure DVMRP 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 Switch C.

```
(Netgear Switch) (Config)#ip multicast
```

3. Enable DVMRP protocol on Switch C.

```
(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 Switch C.

```
(Netgear Switch) (Config)# ip igmp
```

6. Enable IGMP mode on 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
```

7. Display the DVMRP neighbors on Switch C.

```
(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
```

8. Display the multicast route summary on Switch C.

```
(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
```

Main UI: Configure DVMRP

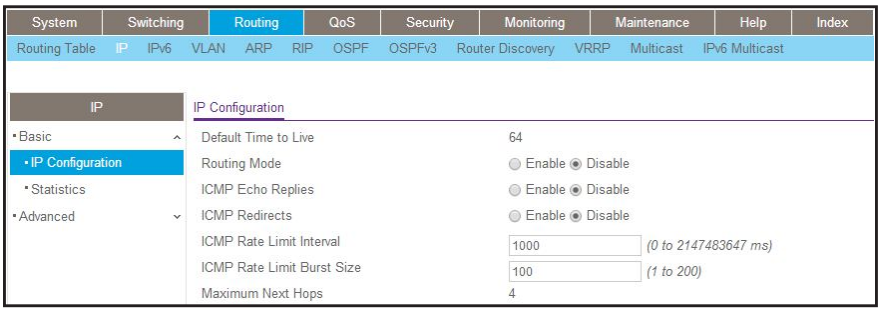
You must configure DVMRP and related features on Switch A, Switch B, and Switch C.

Main UI: Configure DVMRP on Switch A

To use the main UI to configure DVMRP on Switch A:

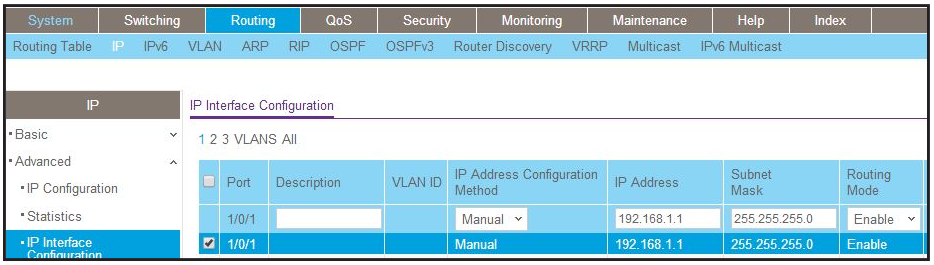
1. Enable IP routing on Switch A.
   a. Select **Routing > IP > Basic > IP Configuration**.

      A page similar to the following figure displays.



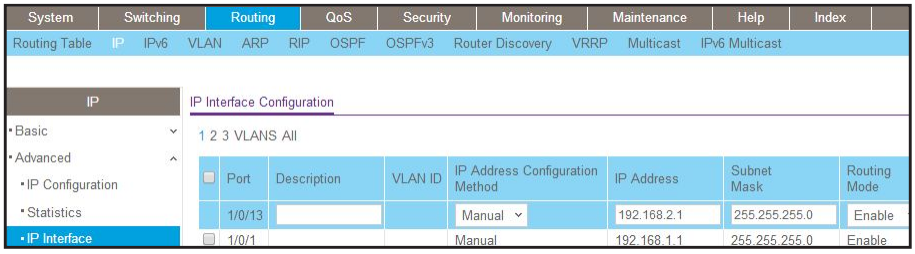
   b. Select the Routing Mode **Enable** radio button.
   c. Click the **Apply** button. Your settings are saved.
2. Configure routing on interface 1/0/1 and assign an IP address to the interface.
   a. Select **Routing > IP > Advanced > IP Interface Configuration**.

      A page similar to the following figure displays.

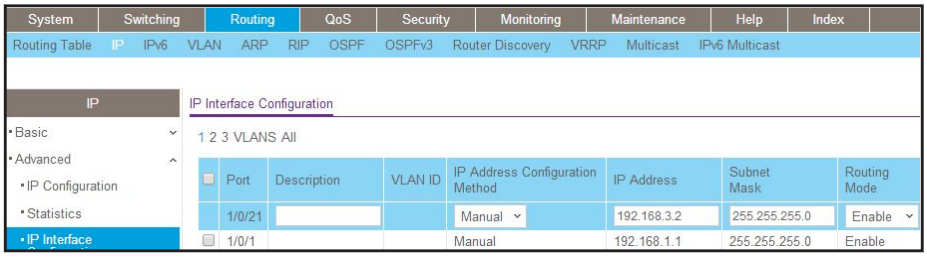


   b. Select the Port **1/0/1** check box.
   c. Configure the following settings:
      - In the **IP Address** field, enter **192.168.1.1**.
      - In the **Subnet Mask** field, enter **255.255.255.0**.
      - In the **Routing Mode** menu, select **Enable**.
   d. Click the **Apply** button. Your settings are saved.

3. Configure 1/0/13 as a routing port and assign an IP address to it.
   a. Remain on the same page.



   b. Select the Port **1/0/13** check box.
   c. Configure the following settings:
      - In the **IP Address** field, enter **192.168.2.1**.
      - In the **Subnet Mask** field, enter **255.255.255.0**.
      - In the **Routing Mode** menu, select **Enable**.
   d. Click the **Apply** button. Your settings are saved.
4. Configure routing on interface 1/0/21 and assign an IP address to the interface.
   a. Remain on the same page.



   b. Select the Port **1/0/21** check box.
   c. Configure the following settings:
      - In the **IP Address** field, enter **192.168.3.2**.
      - In the **Subnet Mask** field, enter **255.255.255.0**.
      - In the **Routing Mode** menu, select **Enable**.
   d. Click the **Apply** button. Your settings are saved.
5. Enable IP multicast on Switch A.
   a. Select **Routing > Multicast > Global Configuration**.

A page similar to the following figure displays.

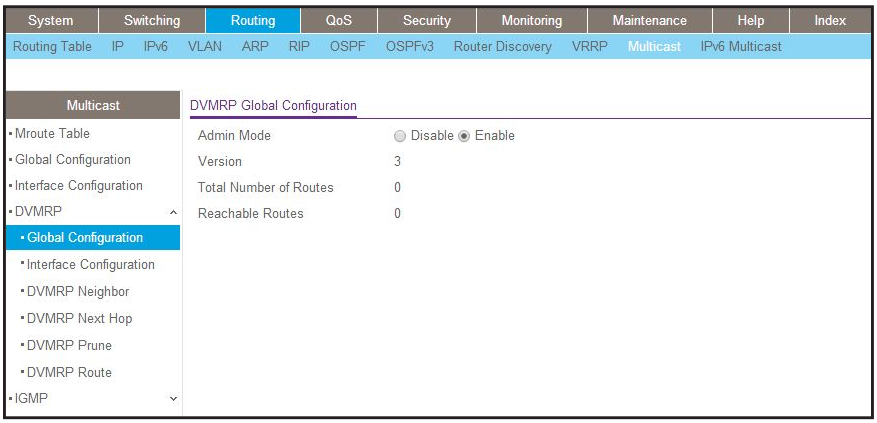
b. Select the Admin Mode **Enable** radio button.

c. Click the **Apply** button. Your settings are saved.

6. Enable DVMRP on Switch A.

a. Select **Routing > Multicast > DVMRP > Global Configuration**.

A page similar to the following figure displays.



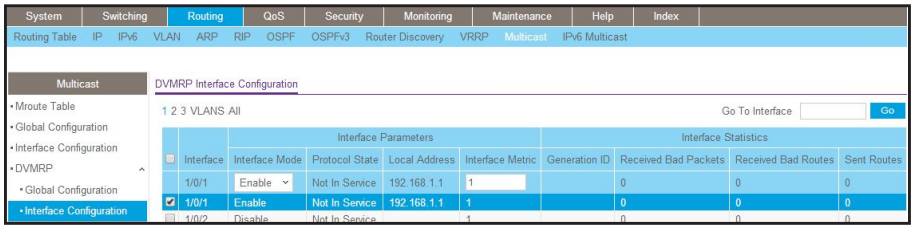
b. Select the Admin Mode **Enable** radio button.

c. Click the **Apply** button. Your settings are saved.

7. Enable DVMRP on interfaces 1/0/1, 1/0/13, and 1/0/21.

a. Select **Routing > Multicast > DVMRP > Interface Configuration**.

A page similar to the following figure displays.



b. Select the Interface **1/0/1**, **1/0/13**, and **1/0/21** check boxes.

c. In the **Interface Mode** menu, select **Enable**.

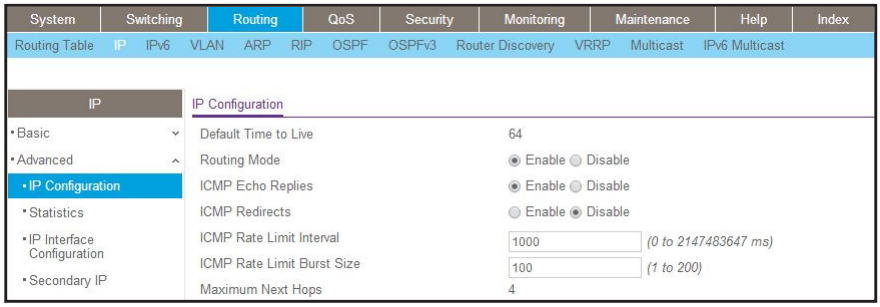
d. Click the **Apply** button. Your settings are saved.

Main UI: Configure DVMRP on Switch B

To use the main UI to configure DVMRP on Switch B:

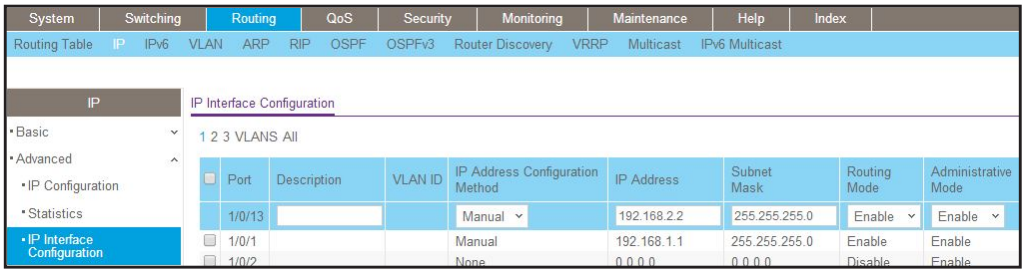
1. Enable IP routing on Switch B.
   a. Select **Routing > IP > Basic > IP Configuration**.

      A page similar to the following figure displays.



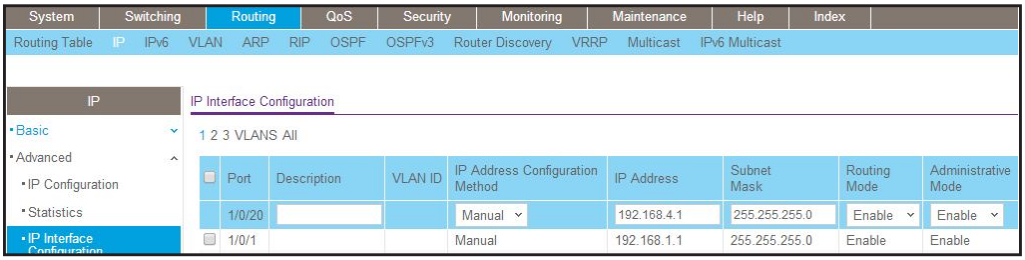
   b. Select the Routing **Enable** radio button.
   c. Click the **Apply** button. Your settings are saved.
2. Configure routing on interface 1/0/13 and assign and IP address to the interface.
   a. Select **Routing > IP > Advanced > IP Interface Configuration**.

      A page similar to the following figure displays.



   b. Select the Port **1/0/13** check box.
   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** menu, select **Enable**.
   d. Click the **Apply** button. Your settings are saved.

3. Configure routing on interface 1/0/20 and assign and IP address to the interface.
   a. Remain on the same page.

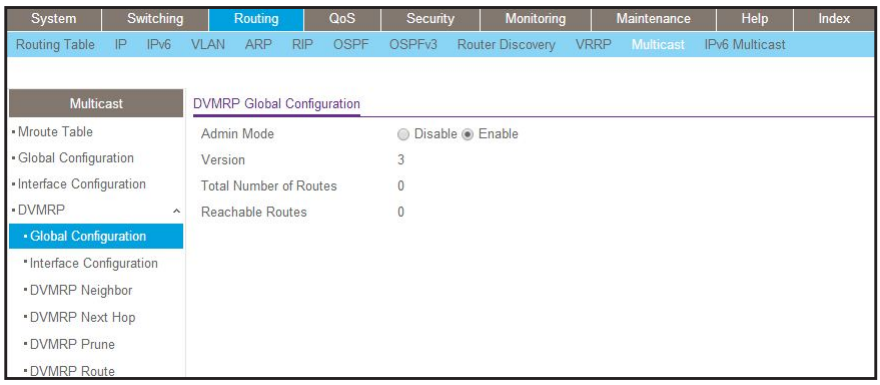


   b. Select the Port **1/0/20** check box.
   c. Configure the following settings:
      - In the **IP Address** field, enter **192.168.4.1**.
      - In the **Subnet Mask** field, enter **255.255.255.0**.
      - In the **Routing Mode** menu, select **Enable**.
   d. Click the **Apply** button. Your settings are saved.
4. Enable IP multicast on Switch B.
   a. Select **Routing > Multicast > Global Configuration**.

      A page similar to the following figure displays.

   b. Select the Admin Mode **Enable** radio button.
   c. Click the **Apply** button. Your settings are saved.
5. Enable DVMRP on Switch B.
   a. Select **Routing > Multicast > DVMRP> Global Configuration**.

A page similar to the following figure displays.



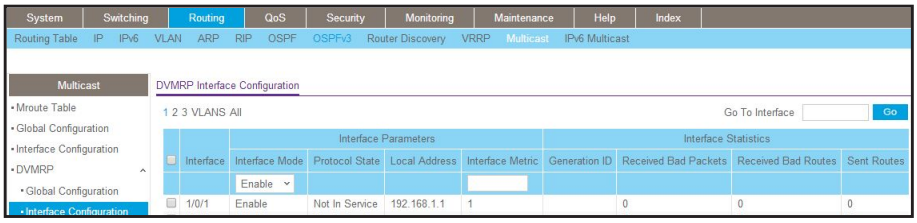
b. Select the Admin Mode **Enable** radio button.

c. Click the **Apply** button. Your settings are saved.

6. Enable DVMRP on interfaces 1/0/13 and 1/0/20.

a. Select **Routing > Multicast > DVMRP > Interface Configuration**.

A page similar to the following figure displays.



b. Select the Interface **1/0/13** and **1/0/20** check boxes.

c. In the **Interface Mode** field, select **Enable**.

d. Click the **Apply** button. Your settings are saved.

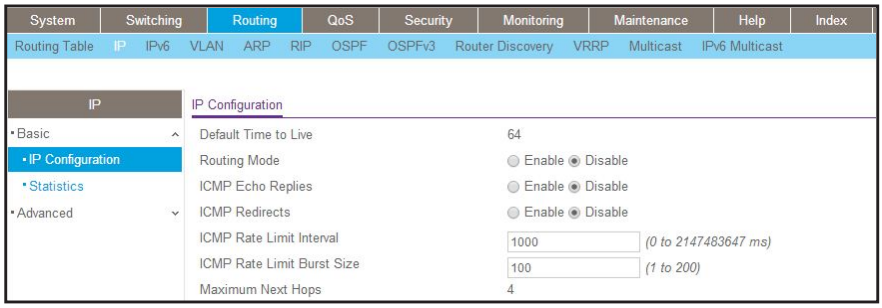
Main UI: Configure DVMRP on Switch C

To use the main UI to configure DVMRP on Switch C:

1. Enable IP routing on Switch C.

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

A page similar to the following figure displays.



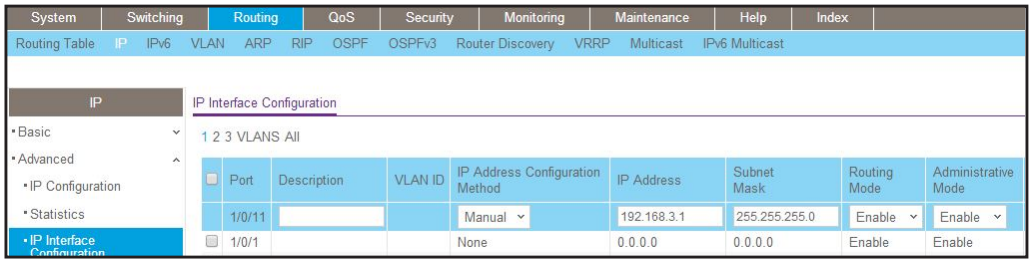
b. Select the Routing Mode **Enable** radio button.

c. Click the **Apply** button. Your settings are saved.

2. Configure routing on interface 1/0/11 and assign and IP address to the interface.

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

A page similar to the following figure displays.



b. Select the Port **1/0/11** check box.

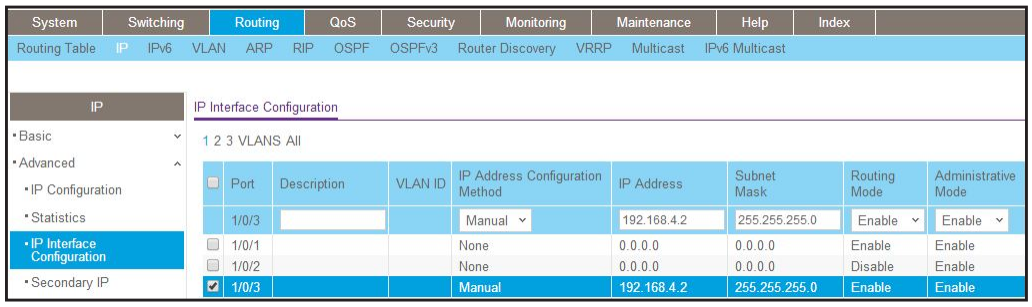
c. Configure the following settings:

- In the **IP Address** field, enter **192.168.3.1**.
- In the **Subnet Mask** field, enter **255.255.255.0**.
- In the **Routing Mode** menu, select **Enable**.

d. Click the **Apply** button. Your settings are saved.

3. Configure routing on interface 1/0/03 and assign and IP address to the interface.

a. Remain on the same page.



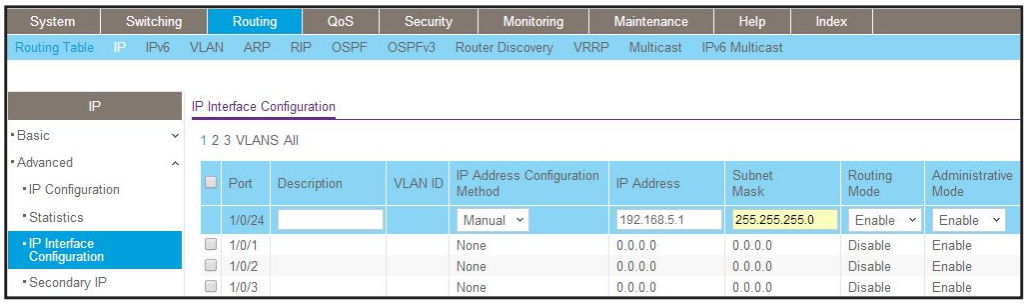
b. Select the Port **1/0/3** check box.

c. Configure the following settings:

- In the **IP Address** field, enter **192.168.4.2**.
- In the **Subnet Mask** field, enter **255.255.255.0**.
- In the **Routing Mode** menu, select **Enable**.

d. Click the **Apply** button. Your settings are saved.

4. Configure routing on interface 1/0/24 and assign and IP address to the interface.
   a. Remain on the same page.

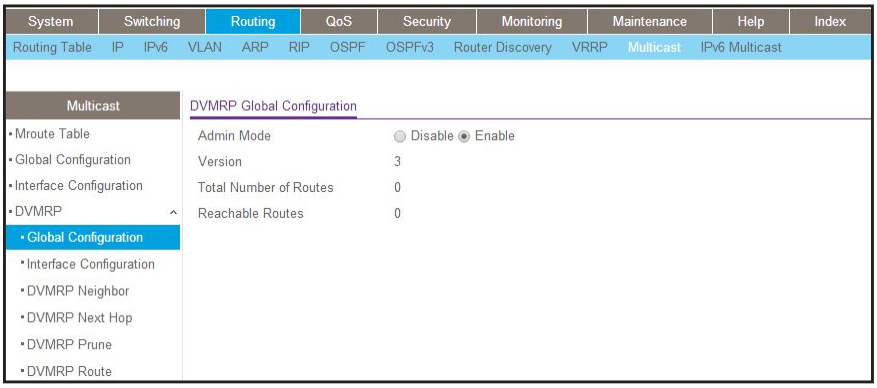


   b. Select the Port **1/0/24** check box.
   c. Configure the following settings:
      - In the **IP Address** field, enter **192.168.5.1**.
      - In the **Subnet Mask** field, enter **255.255.255.0**.
      - In the **Routing Mode** menu, select **Enable**.
   d. Click the **Apply** button. Your settings are saved.
5. Enable IP multicast on Switch C.
   a. Select **Routing > Multicast >Global Configuration**.

      A page similar to the following figure displays.

   b. Select Admin Mode the **Enable** radio button.
   c. Click the **Apply** button. Your settings are saved.
6. Enable DVMRP on Switch C.
   a. Select **Routing > Multicast > DVMRP > Global Configuration**.

A page similar to the following figure displays.



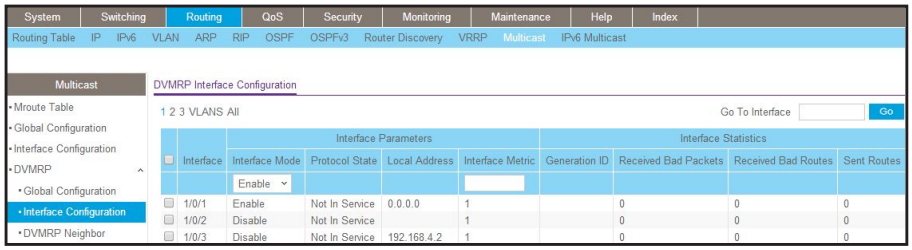
b. Select the Admin Mode **Enable** radio button.

c. Click the **Apply** button. Your settings are saved.

7. Enable DVMRP on interfaces 1/0/3, 1/0/11, and 1/0/24.

a. Select **Routing > Multicast > DVMRP > Interface Configuration**.

A page similar to the following figure displays.



b. Select the Interface **1/0/3**, **1/0/11**, and **1/0/24** check boxes.

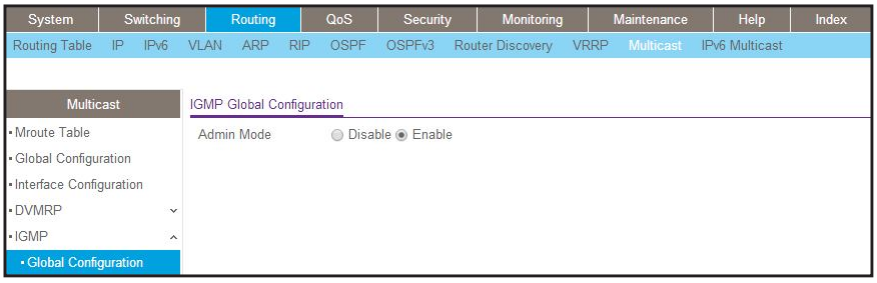
c. In the **Interface Mode** menu, select **Enable**.

d. Click the **Apply** button. Your settings are saved.

8. Enable IGMP on Switch C.

a. Select **Routing > Multicast > IGMP > Global Configuration**.

A page similar to the following figure displays.



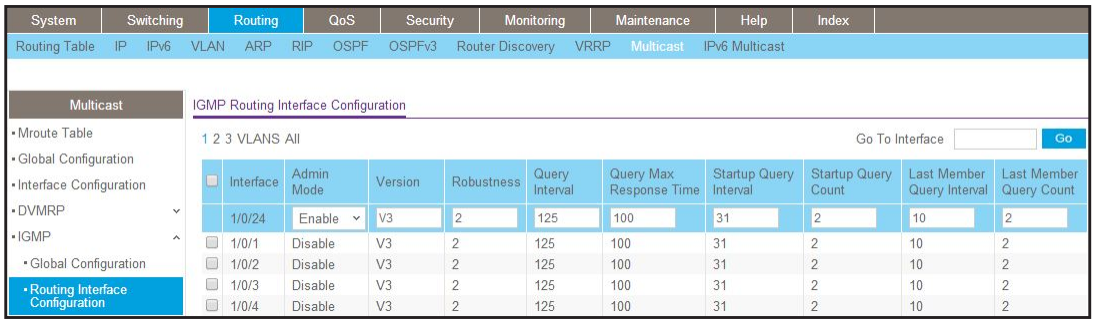
b. Select the Admin Mode **Enable** radio button.

c. Click the **Apply** button. Your settings are saved.

9. Enable IGMP on interface 1/0/24.

a. Select **Routing > Multicast > IGMP > Routing Interface Configuration**.

A page similar to the following figure displays.



b. Select the Interface **1/0/24** check box.

c. In the **Admin Mode** menu, select **Enable**.

d. Click the **Apply** button. Your settings are saved.

35

PTP End-to-End Transparent Clock

Manage Precision Time Protocol

This feature is supported on the M4250 series switches

This feature is supported on the M4300 series switches

This feature is supported on the M4350 series switches

This chapter includes the following sections:

- PTP concepts
- PTP time stamp operation
- PTP transparent clock concepts
- Manage the PTP end-to-end transparent clock

PTP concepts

Note: Precision Time Protocol (PTP)-transparent clocks (TC) and audio-video bridging (AVB) are mutually exclusive. You can either specify the settings for PTP-TC, as described in this chapter, or specify the settings for 802.1AS and MRP, both of which configure the switch for AVB and (see Chapter 36, Audio Video Bridging).

Precision Time Protocol (PTP, IEEE 1588) is a protocol that enables precise synchronization of clocks with a sub-microsecond accuracy across a packet-based network. PTP lets network devices of different precision and resolution synchronize to a grandmaster clock through an exchange of packets across the network. The switch supports PTP end-to-end transparent clock, which is enabled by default, both globally and at the port level.

Note: The switch itself is not affected by PTP.

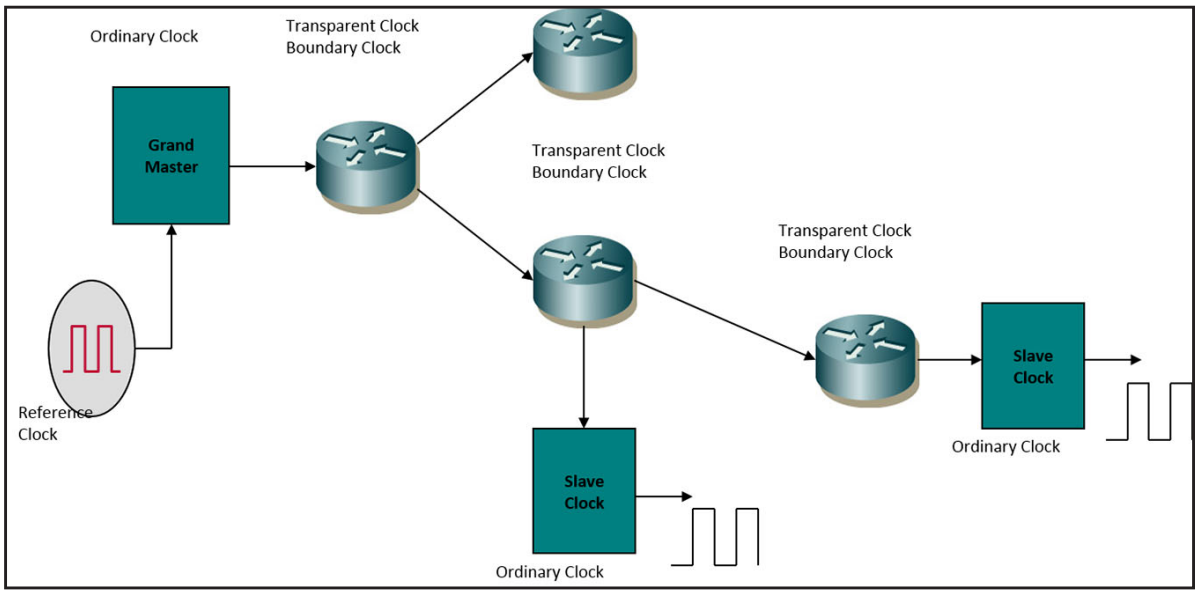


Figure 65. PTP topology

PTP time stamp operation

The IEEE 1588 protocol (PTP) requires protocol PTP packets to be time-stamped when they pass through the network.

Two types of time stamp operation exist:

- **Time stamp recording**. The switch records the time that a PTP event packet is received or transmitted. The record is available to the local CPU.
- **Time stamp correction**. The PTP packets are modified as they pass through a network device. The PTP packets include a correction field that can carry clock corrections for residence times of a transparent clock, path delay for peer-to-peer transparent clocks, and so on. The timestamp value is deducted from the correction field when the PTP packet comes in to the device and is added to the correction field when the packet leaves the device. The result is that the correction field is updated with the period that the packet spends in the device.

Two types of h*ardware* time stamp operation exist, one of which is supported by the switch:

- **1-step hardware time stamp**: The hardware supports corrections, allowing the PTP packets to be modified as they pass through the device. The switch supports 1-step hardware time stamps:

  The switch supports PTPv2 packets with a destination MAC address that is set to 01:1B:19:00:00:00. PTPv1 packets are forwarded, intact. The time stamp counter is 32 bits in length.

- **2-step hardware time stamp**: The hardware supports recording of time stamps of the PTP event packets. This time stamp is then retrieved by the local CPU on a device that supports the PTP firmware and is sent in a separate message. The following M4350 series switch models support 2-step hardware time stamps:
  - M4350-8M2V (SKU MSM4310)
  - M4350-16V4C (SKU VSM4320C)
  - M4350-24F4X (SKU MSM4328F)
  - M4350-24M4X4V (SKU MSM4332)
  - M4350-40F4C (SKU M4344FC)
  - M4350-40X4C (SKU XSM4344C)

PTP transparent clock concepts

A transparent clock (TC) is a PTP device that does not process PTP packets, but modifies them to account for the residence time correction. That is, the device measures the period that the PTP packets require to pass through the device, and then adds that time span to the PTP packets.

A transparent clock measures the variable delay as the PTP packets pass through a device. The measured delay is calculated by adding the residence time into the correction field of the PTP packet.

A transparent clock can be an end-to-end (E2E) clock or a peer-to-peer (P2P) clock. An E2E transparent clock updates the correction field of the PTP packet only with the residence time. A P2P clock can update the correction field with the residence time of packet and the path delay.

The following limitations apply to a PTP E2E transparent clock on a switch:

- You cannot configure a PTP E2E transparent clock at VLAN level. However, the feature functions well for VLAN-tagged packets.
- The PTP E2E transparent clock is intended for a standalone switch only.
- The PTP E2E transparent clock supports only the following three types of PTP event packets: Sync, Delay_Req, and Delay_Resp.

  Of these three PTP event type packets, the switch can update the PTP packet correction field only for Sync and Delay_Req. A Delay_Resp PTP packet passes through the switch without modification.
- The switch does not detect and modify other PTP event packets, such as Announce, pDelay_Req, pDelay_Resp, and FollowUp.
- The switch supports PTP version 2 (PTPv2) only. PTP version 1 (PTPv1) is not supported, but PTPv1 packets are forwarded, intact.

Manage the PTP end-to-end transparent clock

By default, the PTP E2E transparent clock is globally enabled on the switch, that is, on all physical ports. If you configure a LAG, the PTP E2E transparent clock is also enabled on the LAG because the feature is already enabled on all physical ports.

The examples are shown as CLI commands and as main UI procedures.

CLI: Manage the PTP end-to-end transparent clock

This section describes the management options for the PTP end-to-end transparent clock using the CLI.

CLI: Globally disable the PTP end-to-end transparent clock

To use the CLI to globally disable PTP end-to-end transparent clock:

```
(Netgear Switch) #configure
(Netgear Switch) (Config)#no ptp clock e2e-transparent
```

CLI: Disable the PTP end-to-end transparent clock for an interface

To use the CLI to disable PTP end-to-end transparent clock for interface 1/0/1:

```
(Netgear Switch) #configure
(Netgear Switch) (Config)#interface 1/0/1
(Netgear Switch) (Interface 1/0/1)#no ptp clock e2e-transparent
```

CLI: Globally reenable the PTP end-to-end transparent clock

To use the CLI to globally reenable PTP end-to-end transparent clock:

```
(Netgear Switch) #configure
(Netgear Switch) (Config)#ptp clock e2e-transparent
```

CLI: Reenable the PTP end-to-end transparent clock for an interface

To use the CLI to reenable PTP end-to-end transparent clock for interface 1/0/1:

```
(Netgear Switch) #configure
(Netgear Switch) (Config)#interface 1/0/1
(Netgear Switch) (Interface 1/0/1)#ptp clock e2e-transparent
```

CLI: Display the PTP end-to-end transparent clock status

To use the CLI to display the PTP end-to-end transparent clock status:

```
(Netgear Switch) #show ptp clock e2e-transparent

PTP TC mode..................................... Enabled

Interface   Configured Mode Operational Mode
---------   --------------- ----------------
1/1/1       Enabled         Disabled
1/1/2       Enabled         Disabled
1/1/3       Enabled         Disabled
1/1/4       Enabled         Disabled
1/1/5       Enabled         Disabled
1/1/6       Enabled         Disabled
1/1/7       Enabled         Disabled
1/1/8       Enabled         Disabled
1/2/1       Enabled         Disabled
1/2/2       Enabled         Disabled
1/2/3       Enabled         Disabled
1/2/4       Enabled         Disabled
1/2/5       Enabled         Disabled
1/2/6       Enabled         Disabled
1/2/7       Enabled         Disabled
1/2/8       Enabled         Disabled
```

Main UI: Manage the PTP end-to-end transparent clock

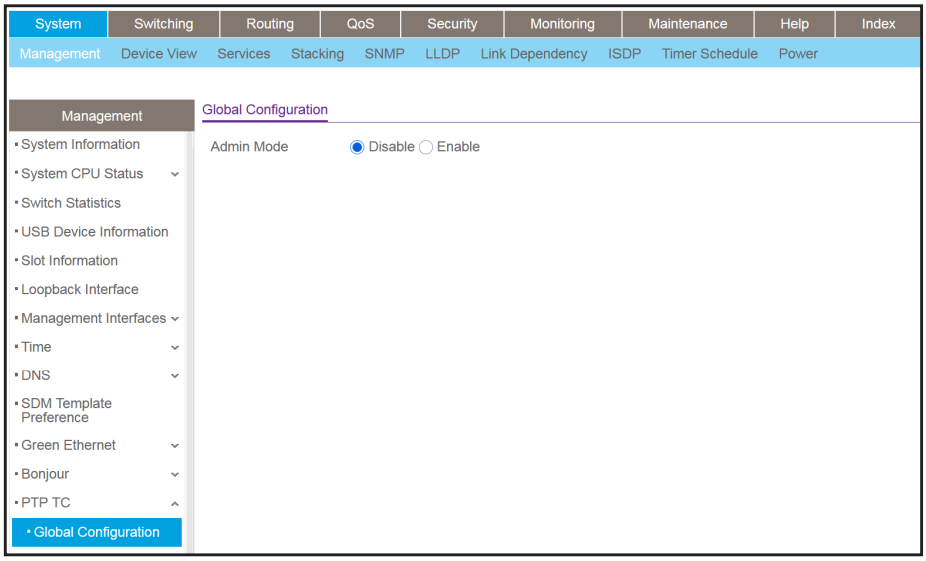
This section describes the management options for the PTP end-to-end transparent clock using the main UI.

Main UI: Globally disable the PTP end-to-end transparent clock

To use the main UI to globally disable PTP end-to-end transparent clock:

1. Select **System > Management > PTP TC > Global Configuration**.

   A page similar to the following figure displays.



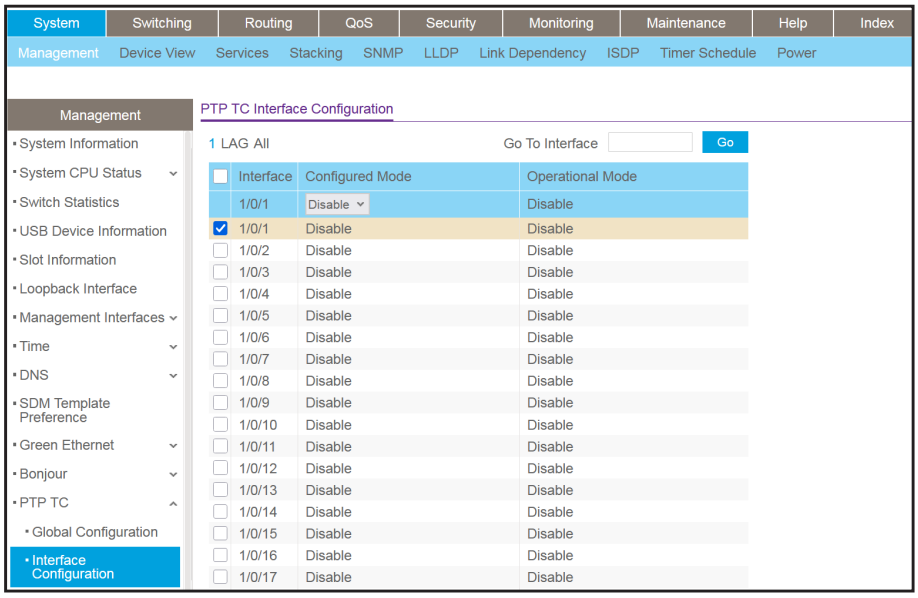
2. Select the Admin Mode **Disable** radio button.
3. Click the **Apply** button. Your settings are saved.

Main UI: Disable the PTP end-to-end transparent clock for an interface

To use the main UI to disable PTP end-to-end transparent clock for interface 1/0/1:

1. Select **System > Management > PTP TC > Interface Configuration**.

   A page similar to the following figure displays.



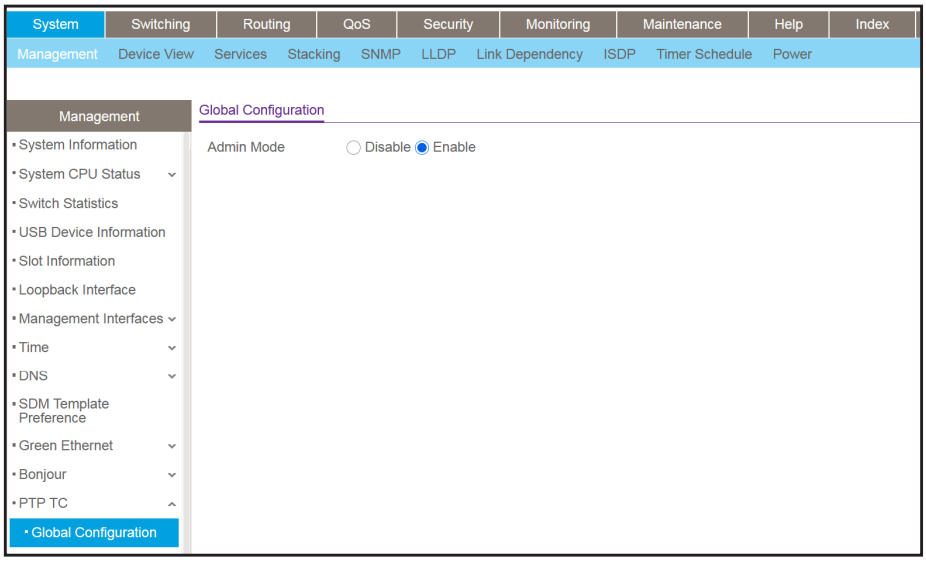
2. Select the Interface **1/0/1** check box.
3. In the Configured Mode menu, select **Disable**.
4. Click the **Apply** button. Your settings are saved.

Main UI: Globally reenable the PTP end-to-end transparent clock

To use the main UI to globally disable PTP end-to-end transparent clock:

1. Select **System > Management > PTP TC > Global Configuration**.

   A page similar to the following figure displays.



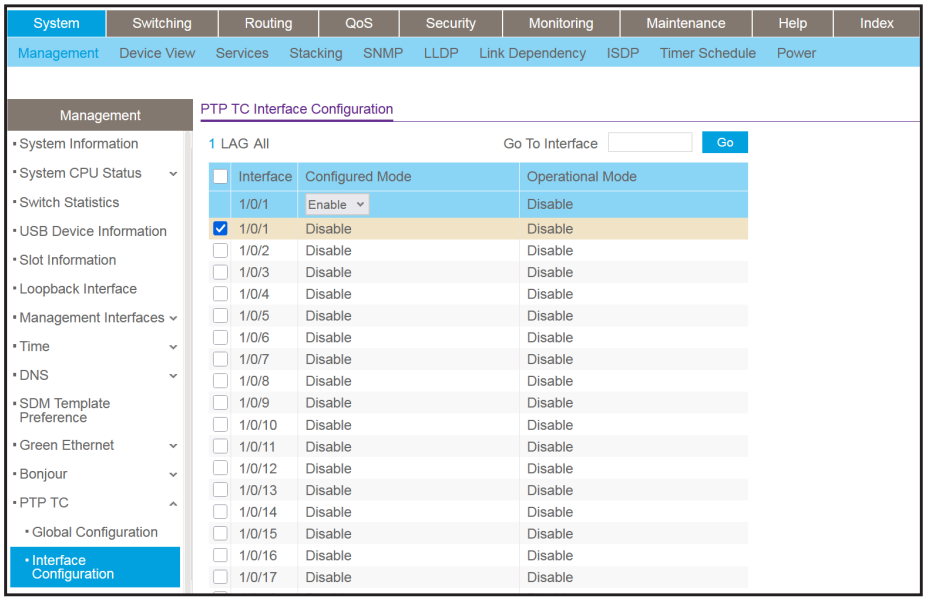
2. Select the Admin Mode **Enable** radio button.
3. Click the **Apply** button. Your settings are saved.

Main UI: Reenable the PTP end-to-end transparent clock for an interface and display the clock status

To use the main UI to enable PTP end-to-end transparent clock for interface 1/0/1 and display the clock status:

1. Select **System > Management > PTP TC > Interface Configuration**.

   A page similar to the following figure displays.



2. Select the Interface **1/0/1** check box.
3. In the Configured Mode menu, select **Enable**.
4. Click the **Apply** button. Your settings are saved.

   The Operational Mode field displays if PTP end-to-end transparent clock is enabled for an interface.

36

Audio Video Bridging

Manage Audio Video Bridging

This feature is supported on the M4250 series switches

This feature is supported on the M4300 series switches

This feature is supported on the M4350 series switches

This chapter includes the following sections:

- AVB concepts
- Enable AVB on the switch and configure AVB on interfaces

AVB concepts

Note: Audio-video bridging (AVB) and Precision Time Protocol (PTP)-transparent clocks (TC) are mutually exclusive. You can either specify the settings for 802.1AS and MRP, both of which configure the switch for AVB and are described in this chapter, or specify the settings for PTP-TC (see Chapter 35, PTP End-to-End Transparent Clock).

The AVB protocol suite includes the following protocols:

- **IEEE 802.1AS-2011**. IEEE 802.1AS-2011 Timing and Synchronization for Time-Sensitive Applications (generalized Precision Time Protocol [gPTP])
- **IEEE 802.1Qav-2009**. Forwarding and Queuing for Time-Sensitive Streams (FQTSS)
- **IEEE 802.1Qat-2010**. Stream Reservation Protocol (SRP)
- **IEEE 802.1BA-2011**. Audio Video Bridging (AVB) Systems
- **IEEE 1722-2011**. Layer 2 Transport Protocol for Time Sensitive Applications (AV Transport Protocol [AVTP])

The switch supports the following Multiple Registration Protocol (MRP) protocols:

- **MMRP**. Multiple MAC Registration Protocol (MMRP) registers MAC address information.
- **MVRP**. Multiple VLAN Registration Protocol (MVRP) registers VLAN membership.
- **MSRP**. Multiple Stream Reservation Protocol (MSRP) registers bandwidth requirement for an AV stream.

MRP lets devices register attributes to other devices in a network. MRP is the base registration protocol that is then used by MMRP and MSRP to propagate the registration.

MRP replaces Generic Attribute Registration Protocol (GARP), which is still supported on the switch. The following related protocols are also replaced:

- GARP Multicast Registration Protocol (GMRP) is replaced by MMRP but is still supported on the switch.
- GARP VLAN Registration Protocol (GVRP) is replaced by MVRP but is still supported on the switch.

MRP

MRP provides the same functionality as GARP, which it replaces.

MRP consist of an application and a declaration component. In addition, a distribution component is called the MRP Attribute Declaration (MAD), which transmits and processes incoming MRP Protocol Data Units (MRPPDUs). The application component keeps track of

attributes via registrations, and enforces any associated rules such as attribute restrictions. An AVB bridge such as a switch includes an MRP Attribute Propagation (MAP) component that propagates information among participating interfaces.

MMRP

MMRP propagates MAC address information in a network. MMRP replaces GMRP.

MMRP can register and deregister both individual MAC addresses and group MAC address memberships. This differs from GMRP, which supports only the propagation of group MAC address memberships.

MMRP lets end stations join or leave a multicast group or register an individual MAC address with a specific VLAN. If you enable MMRP, the switch can dynamically register and deregister MAC addresses.

MVRP

MVRP lets the switch automatically maintain dynamic VLAN registration entries and propagate the associated information over the network. This lets MVRP-aware devices to dynamically establish and update information about VLANs with active members, as well as information about the interfaces through which those members can be reached. MVRP replaces GVRP.

With MVRP, both end stations and switches can issue and revoke declarations related to VLAN membership, allowing MVRP participant to create or update a dynamic VLAN registration entry in the filtering database. Such an entry includes information about the VLAN and the interface on which it is received.

MVRP is also used by other protocols for dynamic VLAN creation over a network.

MSRP

MSRP reserves resources in a network so that time-sensitive traffic can flow from end to end. A typical network includes flows for multiple talkers (devices that transmit streams) and multiple listeners (devices that receive streams from one or more talkers). Each of these flows requires a specific bandwidth, frame rate, and time synchronization. MSRP can guarantee the resources through all intermediate devices between a talker and a listener.

For example, if a particular stream requires 1000 kbps, a frame rate of 128 kbps, and not more than a maximum delay of 120 micro seconds, the requirements must be guaranteed on each device between a talker and a listener. At each bridge, the delay component is increased with the delay that is associated with that particular link. (These streams use multicast MAC addresses as directory agents [DAs] so that source pruning can occur through MMRP. Time synchronization is handled by the 802.1AS protocol, which calculates the time delay between devices on a link and maintains an accurate network clock.) The end device that receives the stream determines if the accumulated delay is within its threshold and accepts or rejects the stream.

If all devices between a talker and a listener can provide the required bandwidth and honor the minimum delay, the end device can play the stream. If a device is unable to reserve resources or contributes to an unacceptable delay, a negative acknowledgement is sent to both the talker and the listener, enabling all devices to deallocate the resources that were allocated for the stream.

MSRP ensures that the path from a talker to a listener can provide guaranteed bandwidth and timing requirement to satisfy the rigorous demands of the Ethernet audio video transmissions.

802.1AS

802.1AS can ensure that QoS requirements are guaranteed for time-sensitive applications such as audio and video. Precision Time Protocol (PTP) forms the basis for 802.1AS. PTP can provide precise clock synchronization that relies on time-stamped packets. PTP is applicable to a distributed system that consist of one or more communicating nodes. The distribution of synchronous time information occurs hierarchically with a grandmaster clock. The grandmaster clock provides a common and precise time reference by exchanging timing information with one or more directly-attached devices. Such as attached device synchronizes its clocks with the grandmaster clock and, in turn, can function as master clock for a hierarchical layer of attached devices.

Time synchronization provides a common time base for sampling data streams at a source device and presenting those streams at a destination device with the same relative timing. End-to-end synchronization of clocks is critical for traffic that is highly time-sensitive with stringent latency and jitter requirements.

802.1AS supports the following:

- Network clock synchronization in the sub-microsecond range
- Synchronization of clocks with different precision, resolution and stability
- Fast convergence when topology changes occur

Enable AVB on the switch and configure AVB on interfaces

The example is shown as CLI commands and as a main UI procedure.

CLI: Enable AVB on the switch and configure AVB on interfaces

To use the CLI to enable AVB and related features on the switch and configure AVB on interfaces 0/1 and 0/2:

1. Enable AVB globally on the switch:

```
(Netgear Switch) #configure
(Netgear Switch) (Config)#dot1as
(Netgear Switch) (Config)#msrp
(Netgear Switch) (Config)#mvrp
(Netgear Switch) (Config)#exit
```

2. Configure AVB on interfaces 0/1 and 0/2:

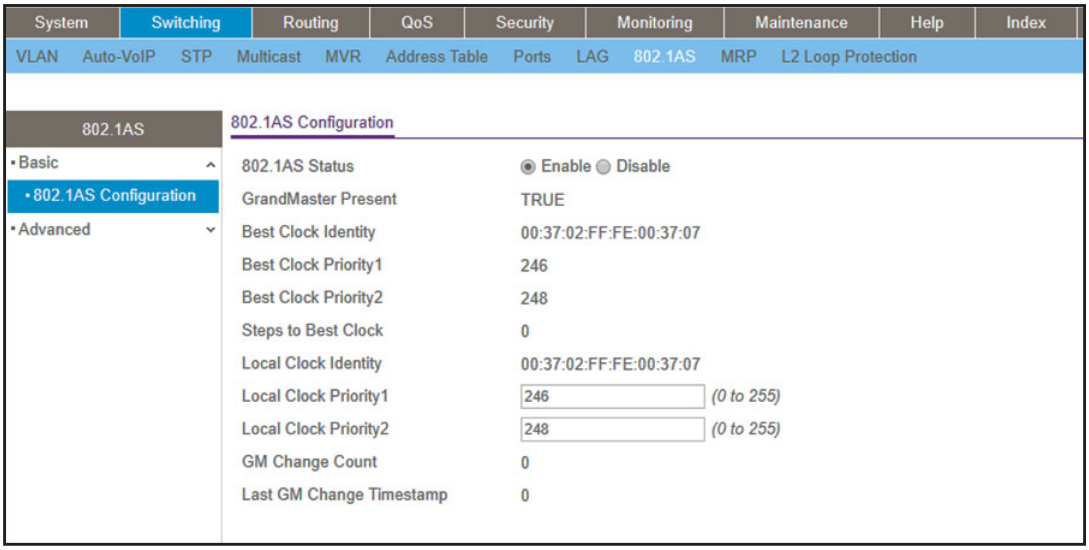
```
(Netgear Switch) #configure
(Netgear Switch) (Config)#interface 0/1
(Netgear Switch) (Interface 0/1)#dot1as
(Netgear Switch) (Interface 0/1)#mvrp
(Netgear Switch) (Interface 0/1)#msrp
(Netgear Switch) (Interface 0/1)#exit
(Netgear Switch) (Config)#interface 0/2
(Netgear Switch) (Interface 0/2)#dot1as
(Netgear Switch) (Interface 0/2)#mvrp
(Netgear Switch) (Interface 0/2)#msrp
(Netgear Switch) (Interface 0/2)#exit
```

Main UM: Enable AVB on the switch and configure AVB on interfaces

To use the main UI to enable AVB and related features on the switch and configure AVB on interfaces 0/1 and 0/2:

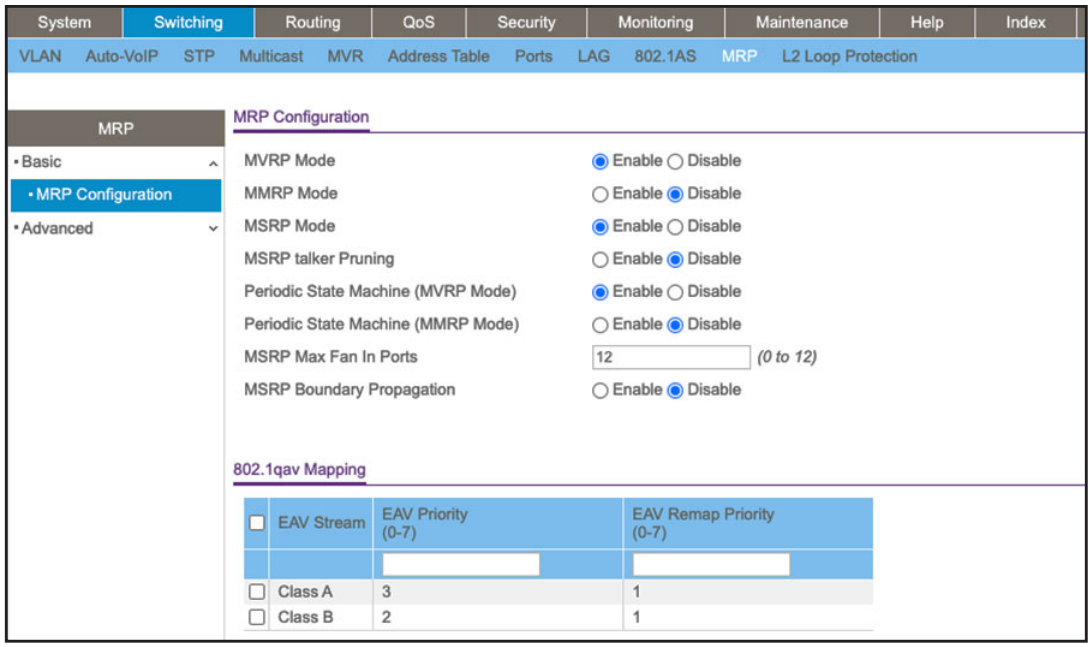
1. Enable 802.1AS on the switch.
   a. Select **Switching > 802.1AS > Basic > 802.1AS Configuration**.

      A page similar to the following figure displays.



   b. Select the 802.1AS Status **Enable** radio button.
   c. Click the **Apply** button. Your settings are saved.
2. Enable MVRP and MSRP on the switch.
   a. Select **Switching > MRP > Basic > MRP Configuration**.

      A page similar to the following figure displays.



b. Select the MVRP **Enable** radio button.

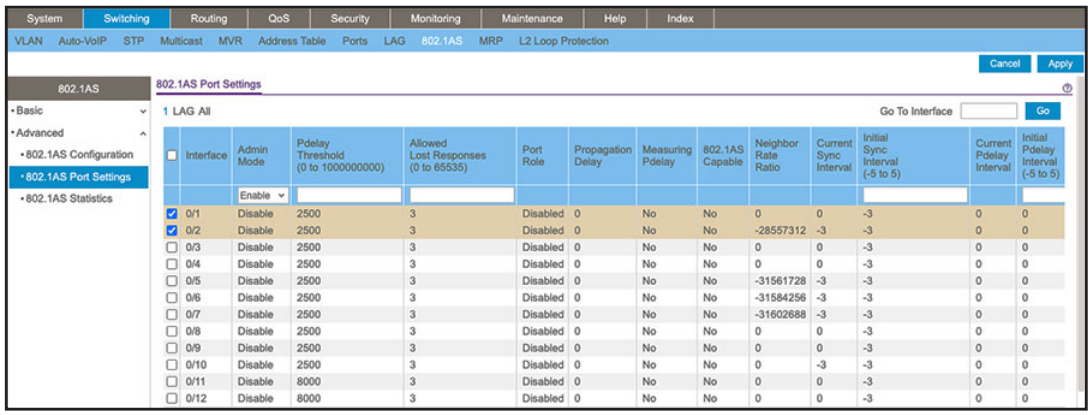
c. Select the MSRP **Enable** radio button.

d. Click the **Apply** button. Your settings are saved.

3. Enable 802.1AS on interfaces 0/1 and 0/2.

a. Select **Switching > 802.1AS > Advanced > 802.1AS Port Settings**.

A page similar to the following figure displays.



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

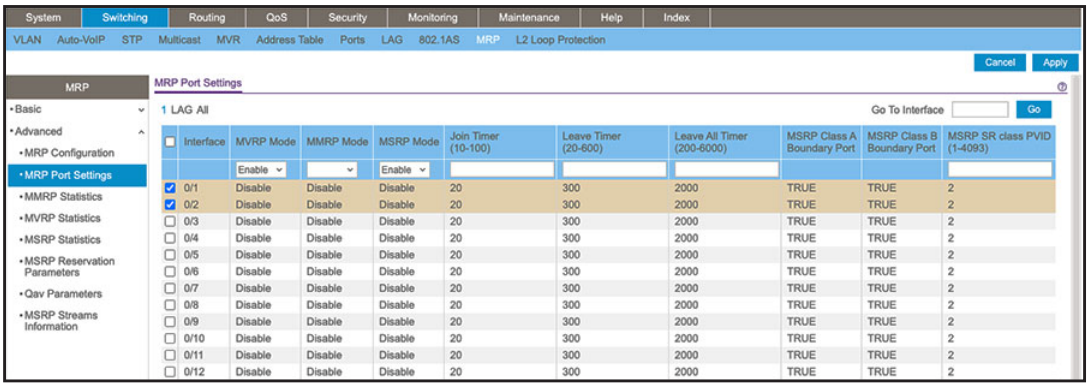
c. In the **Admin Mode** menu, select **Enable**.

d. Click the **Apply** button. Your settings are saved.

4. Enable MVRP and MSRP on interfaces 0/1 and 0/2.

a. Select **Switching > MRP > Advanced > MRP Port Settings**.

A page similar to the following figure displays.



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

c. In the **MVRP Mode** menu, select **Enable**.

d. In the **MSRP Mode** menu, select **Enable**.

e. Click the **Apply** button. Your settings are saved.

37

Link Dependency

Configure Link State Groups

This feature is supported on the M4250 series switches

This feature is supported on the M4300 series switches

This feature is supported on the M4350 series switches

This chapter includes the following sections:

- Link Dependency concepts
- 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.

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 menu, a downstream interface menu, 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.

Create a link state group

The example is shown as CLI commands and as a main UI procedure.

CLI: Create a link state group

To use the CLI to 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 interface 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 interface 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.

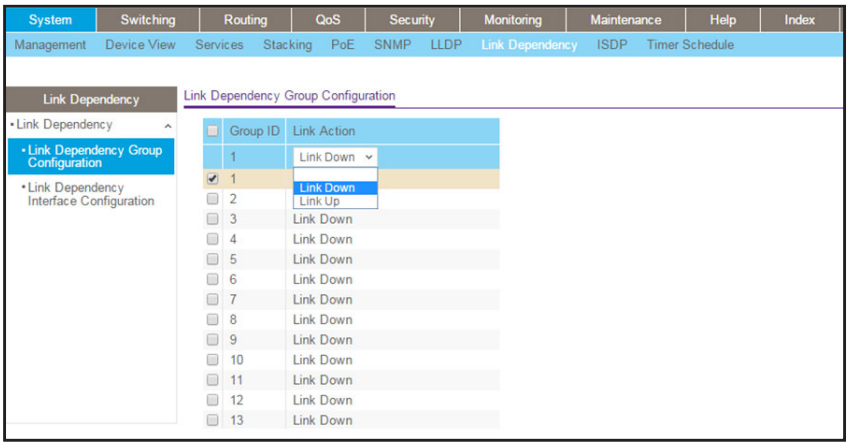
```
(Netgear Switch) #show link state group 1
GroupId  Downstream Interfaces   Upstream Interfaces   Link Action   Group State
-------  ----------------------  --------------------  ------------  -----------
1        1/0/5                   1/0/1                 Link Down     Up
```

Main UI: Create a link state group

To use the main UI to create a link state group:

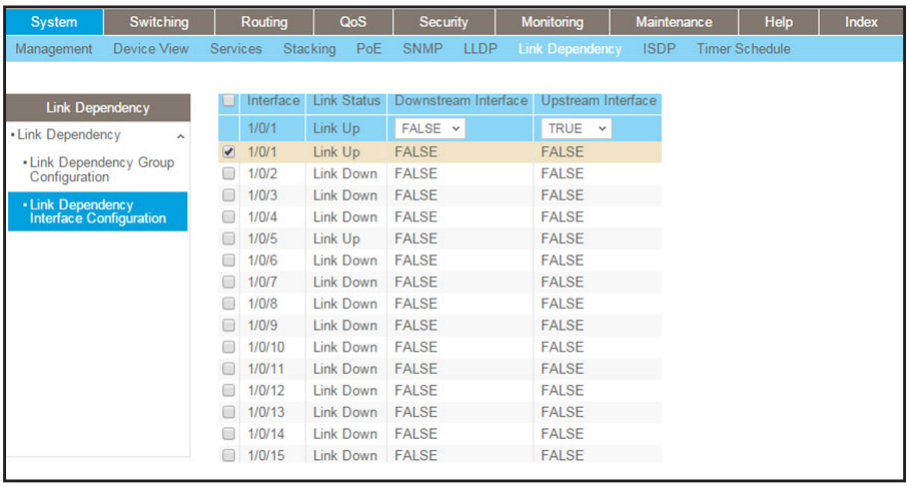
1. Configure the action for link state group with group number 1.
   a. Select **System > Link Dependency > Link Dependency Group Configuration**.

      A page similar to the following figure displays.



   b. Select the Group ID **1** check box.
   c. In the **Link Action** menu, select **Link Down**.
   d. Click the **Apply** button. Your settings are saved.
2. Configure interface 1/0/1 as an upstream link.
   a. Select **System > Link Dependency > Link Dependency Interface Configuration**.

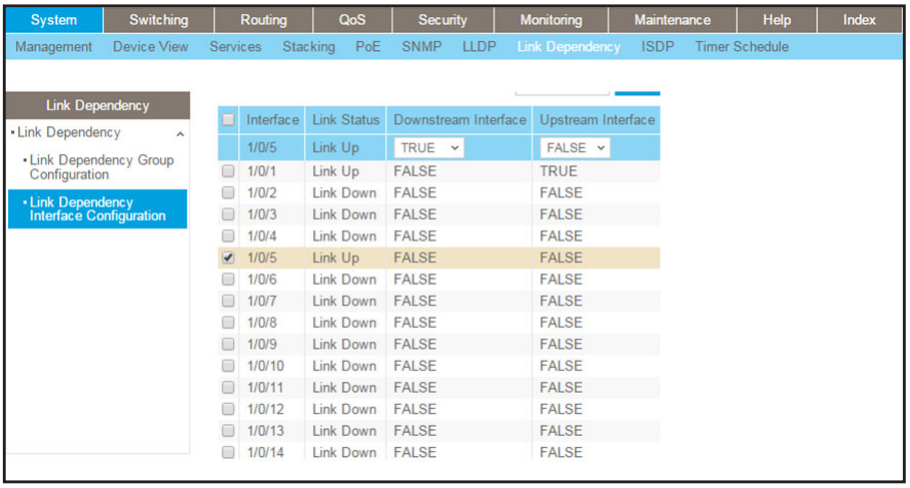
      A page similar to the following figure displays.



   b. Select the Interface **1/0/1** check box.
   c. In the **Upstream Interface** menu, select **True**.
   d. Click the **Apply** button. Your settings are saved.

3. Configure interface 1/0/5 as a downstream link
   a. Select **System > Link Dependency > Link Dependency Interface Configuration**.

      A page similar to the following figure displays.



   b. Select the Interface **1/0/5** check box.
   c. In the **Downstream Interface** menu, select **True**.
   d. Click the **Apply** button. Your settings are saved.

38

Captive Portals

Captive portals and client authentication

This feature is supported on the M4250 series switches

This feature is supported on the M4300 series switches

This feature is supported on the M4350 series switches

This chapter includes the following sections:

- Captive portal concepts
- Captive portal client concepts
- Enable a captive portal
- Block a captive portal instance
- Create users and groups for local authentication
- RADIUS user configuration
- SSL certificate concepts

Captive portal concepts

The captive portal feature blocks clients from accessing the network until user verification is 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 clients that are 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 so that all traffic coming to the port from unauthenticated clients is dropped, except for 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 HTTP or 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 HTTP or HTTPS traffic from unauthenticated clients to the authenticating server on the switch. A captive portal web page is sent back to the unauthenticated client, and the client can authenticate. If the client successfully authenticates, the client is given access to the port.

This is what you can do with the captive portal feature:

- Enable the feature on any of the physical ports on the switch.
  The feature is not supported for VLAN interfaces, loopback interfaces, or logical interfaces.
- Manage captive portals using the CLI, the main UI, and SNMP.
  One exception exists: To customize the captive portal web page, you must use the main UI.
- Control verification and authentication, assignment to interfaces, client sessions, and web page customization.
- Create multiple captive portal configuration instances. Each captive portal instance can control client access and provide specific 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.

Captive portal client concepts

The captive portal feature uses MAC-address based authentication rather than 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.

You can configure user verification to allow access for the following types of captive portal users:

- **Guest users**: Thee are users who do not have assigned user names and passwords.
- **Authenticated users**: These are users who must enter a user name and password, both of which must be validated against the local database or a RADIUS server. Network access is granted when user verification is confirmed.

Clients connecting to the captive portal interface can be placed in three states:

- **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.

Enable a captive portal

The example is shown as CLI commands and as a main UI procedure.

CLI: Enable a captive portal

To use the CLI to enable a captive portal:

1. Enable the 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 interface 1/0/1.

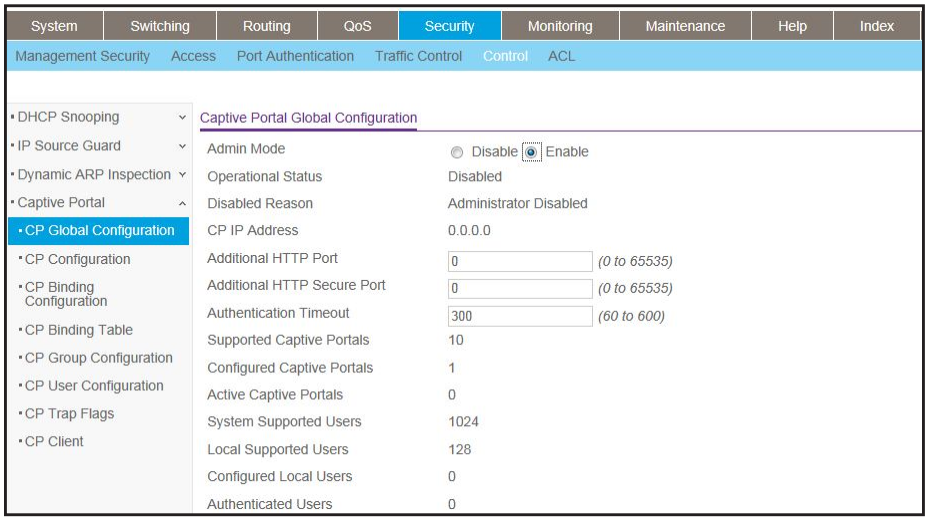
```
(Netgear Switch) (Config-CP 1)#interface 1/0/1
```

Main UI: Enable a captive portal

To use the main UI to enable a captive portal:

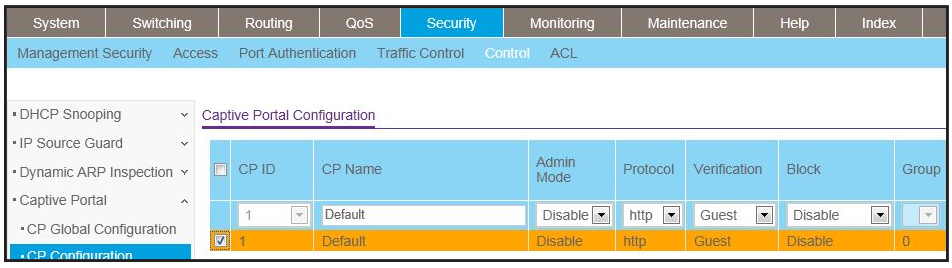
1. Enable captive portal on the switch.
   a. Select **Security > Control > Captive Portal > CP Global Configuration**.

      A page similar to the following figure displays.



   b. Select the Admin Mode **Enable** radio button.
   c. Click the **Apply** button. Your settings are saved.
2. Enable captive portal instance 1 on the switch.
   a. Select **Security > Control > Captive Portal > CP Configuration**.

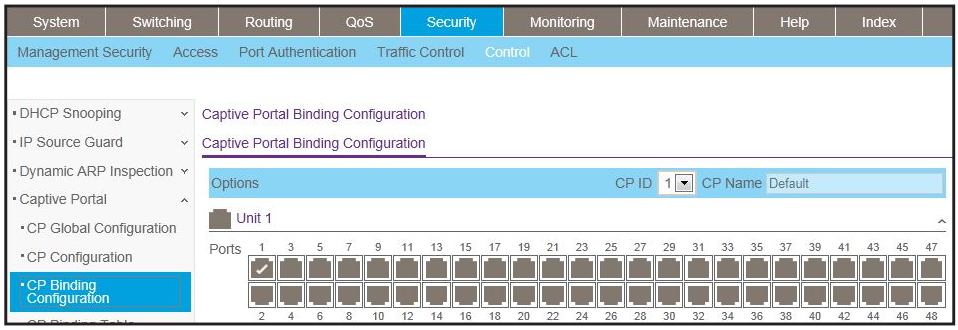
      A page similar to the following figure displays.



   b. Select the CP ID **1** check box.
   c. In the **Admin Mode** menu, select **Enable**.
   d. Click the **Apply** button. Your settings are saved.

3. Enable CP 1 on interface 1/0/1.
   a. Select **Security > Controls > Captive Portal > CP Binding Configuration**.

      A page similar to the following figure displays.



   b. In the **CP ID** menu, select **1**.
   c. Click the gray box under port **1**.
   d. Click the **Apply** button. Your settings are saved.

Block a captive portal instance

You 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 that is not saved in the configuration.

The example is shown as CLI commands and as a main UI procedure.

CLI: Block a captive portal instance

To use the CLI to block a captive portal instance:

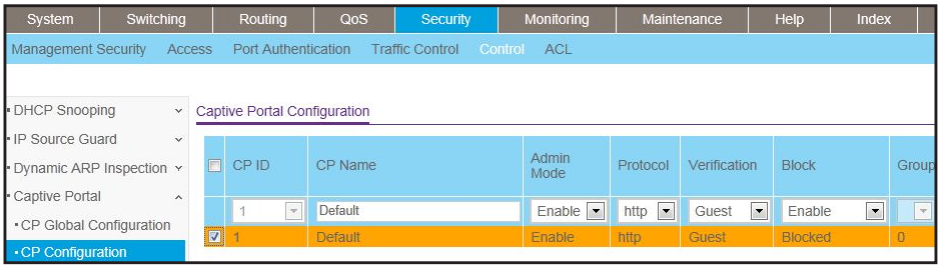
```
(Netgear Switch) #config
(Netgear Switch) (config)#captive-portal
(Netgear Switch) (Config-CP)#configuration 1
(Netgear Switch) (Config-CP 1)#block
```

Main UI: Block a captive portal instance

To use the main UI to block a captive portal instance:

1. Select **Security > Control > Captive Portal > CP Configuration**.

   A page similar to the following figure displays.



2. Select the CP ID **1** check box.
3. In the **Block** menu, select **Enable**.
4. Click the **Apply** button. Your settings are saved.

Create users and groups for local authentication

If you use local authentication, you must provide user identities for the 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. If more users are required, use a RADIUS server.

A local user can belong to one or more groups. One default group with the group name *Default* exists, and all new users are assigned to this group.

All new captive portal instances are also assigned to the Default group. You can create new groups and modify the user and 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.

The example is shown as CLI commands and as a main UI procedure.

CLI: Create a group and a user and add the user to the group

To use the CLI to create a group and a user and add the user to the group:

1. Create a group with group ID 2.

```
(Netgear Switch) #config
(Netgear Switch) (config)#captive-portal
(Netgear Switch) (Config-CP)# user group 2
```

2. Create a user with the name 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 with ID 2.

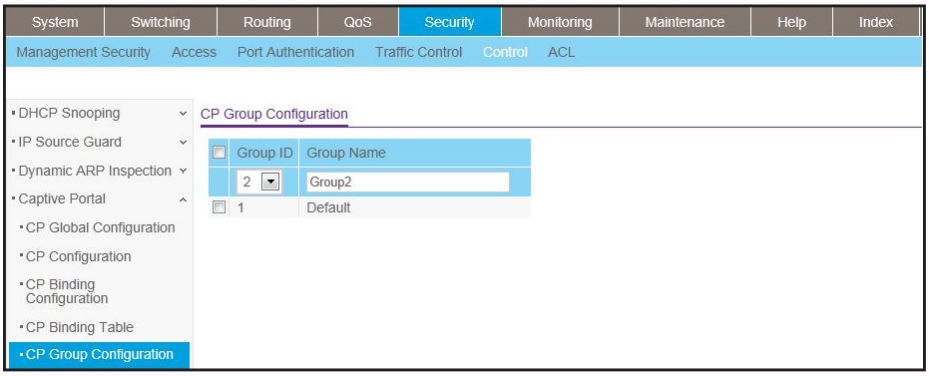
```
(Netgear Switch) (Config-CP)#user 2 group 2
```

Main UI: Create a group and a user and add the user to the group

To use the main UI to create a user and a group and add the user to the group:

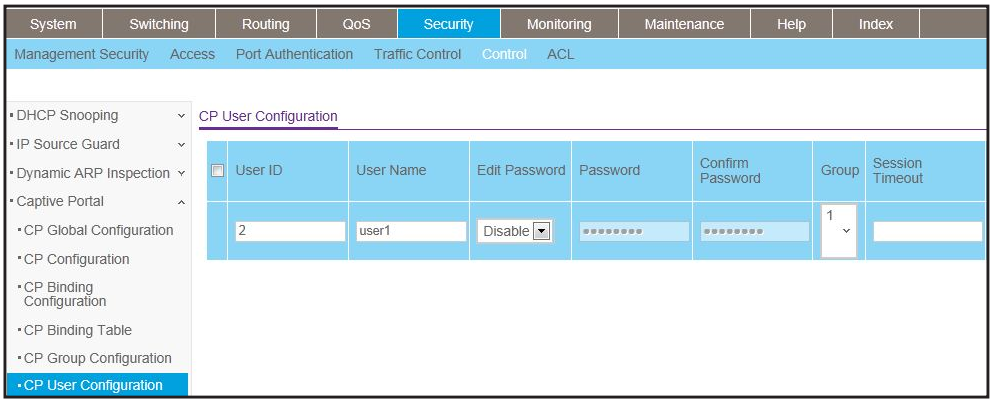
1. Create a group.
   a. Select **Security > Control > Captive Portal > CP Group Configuration**.

      A page similar to the following figure displays.



   b. In the **Group ID** field, select **2**.
   c. In the **Group Name** field, enter **Group2**.
   d. Click the **Add** button. Your settings are saved.
2. Create a user.
   a. Select **Security > Control > Captive Portal > CP User Configuration**.

      A page similar to the following figure displays.



   b. Configure the following settings:
      - 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 the **Add** button. Your settings are saved.

RADIUS user configuration

You can use a remote Remote Authentication Dial-In User Service (RADIUS) server for client authentication. The RADIUS authentication and accounting servers are configured separately from the captive portal configuration. To let the switch perform authentication and accounting using RADIUS, you must configure one or more RADIUS servers and then reference 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 indicates that the instance is disabled and lists a specific reason.

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 6. 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

The example is shown as CLI commands and as a main UI procedure.

CLI: Configure RADIUS as the verification mode for a captive portal

To use the CLI to configure RADIUS as the verification mode for a captive portal:

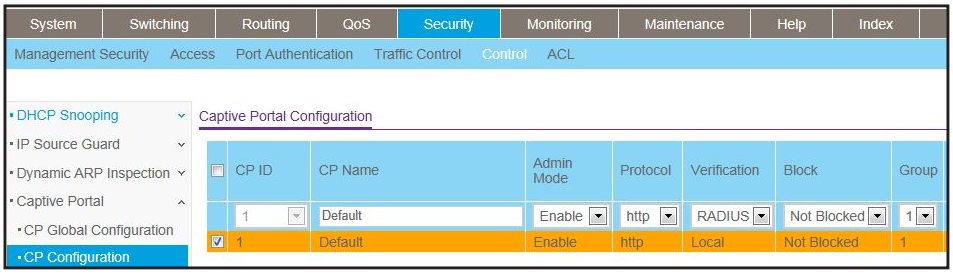
```
(Netgear Switch) #config
(Netgear Switch) (config)#captive-portal
(Netgear Switch) (Config-CP)#configuration 1
(Netgear Switch) (Config-CP 1)#radius-auth-server Default-RADIUS-Server
(Netgear Switch) (Config-CP 1)#verification radius
```

Main UI: Configure RADIUS as the verification mode for a captive portal

To use the main UI to configure RADIUS as the verification mode for a captive portal:

1. Select **Security > Control > Captive Portal > CP Configuration**.

   A page similar to the following figure displays.



2. Select the CP ID **1** check box.
3. In the **Verification** field, select **RADIUS**.
4. In the **Radius Auth Server** field, enter the RADIUS server name **Default-RADIUS-Server**.
5. Click the **Apply** button. Your settings are saved.

SSL certificate concepts

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.

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 no certificate is present on the switch, the captive portal instance is disabled and lists a specific reason.

39

iSCSI

Internal Small Computer System Interface

This feature is supported on the M4300 series switches

This feature is supported on the M4350 series switches

This chapter includes the following sections:

- iSCSI concepts
- Enable iSCSI awareness with a VLAN priority tag
- Enable iSCSI awareness with DSCP
- Set the iSCSI target port
- Display iSCSI sessions

Note: The Internal Small Computer System Interface (iSCSI) feature is supported on the M4300 series and M4350 series switches only. The M4250 series switches do not support iSCSI.

iSCSI concepts

The Internal Small Computer System Interface (iSCSI) feature is used in networks containing iSCSI initiators and targets for which you must 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 specific preference characteristics over other data passing through the switch. This feature can prevent session interruptions during times of congestion that would otherwise cause iSCSI packets to be dropped.

You can select a VLAN priority tag (VPT) or DSCP mapping for the QoS preferential treatment. iSCSI flows are assigned by default to the highest VPT/DSCP queue that is not used for switch management or voice VLAN. You must also configure the relevant Class of Service settings for the selected queue.

The following figure shows an example of iSCSI implementation.

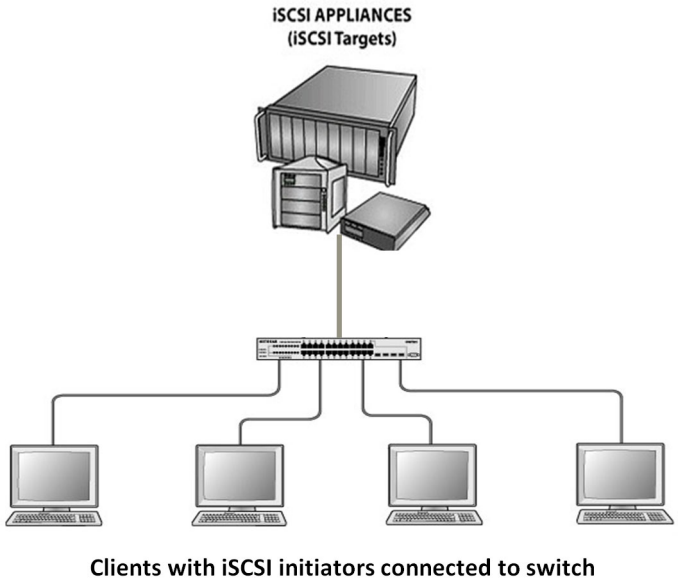


Figure 66. Sample iSCSI implementation

Enable iSCSI awareness with a VLAN priority tag

The example is shown as CLI commands and as a main UI procedure.

CLI: Enable iSCSI awareness with a VLAN priority tag

To use the CLI to enable iSCSI awareness, select a VPT, and set the aging time:

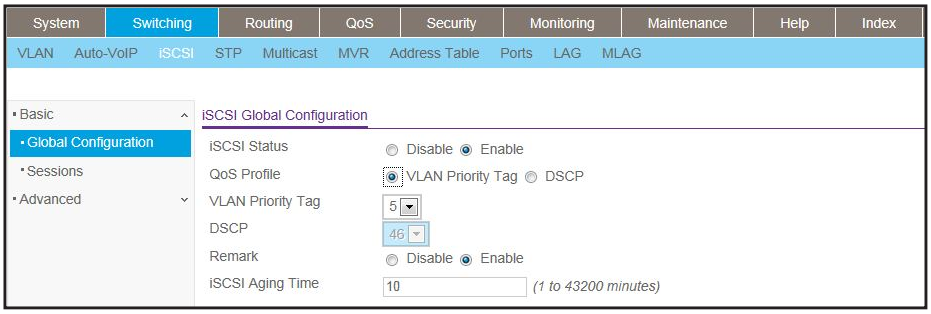
```
(Netgear Switch) #config
(Netgear Switch) (Config) #iscsi enable
(Netgear Switch) (Config) #iscsi cos vpt 5
(Netgear Switch) (Config) #iscsi aging time 10
(Netgear Switch) (Config) #exit
```

Main UI: Enable iSCSI awareness with a VLAN priority tag

To use the main UI to enable iSCSI awareness, select a VPT, and set the aging time:

1. Select **Switching > iSCSI > Basic > Global Configuration**.

   A page similar to the following figure displays.



2. Configure the following settings:
   - Select the iSCSI Status **Enable** radio button.
   - Select the QoS Profile **VLAN Priority Tag** radio button.
   - In the **VLAN Priority Tag** menu, select **5**.
   - Select the Remark **Enable** radio button.
   - In the **iSCSI Aging Time** field, enter **10**.
3. Click the **Apply** button. Your settings are saved.

Enable iSCSI awareness with DSCP

The example is shown as CLI commands and as a main UI procedure.

CLI: Enable iSCSI awareness with DSCP

To use the CLI to enable iSCSI awareness, set a DSCP queue, and set the aging time.

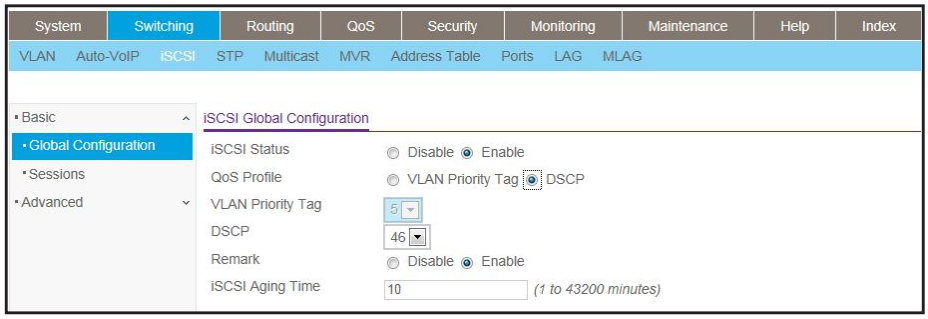
```
(Netgear Switch) #config
(Netgear Switch) (Config) #iscsi enable
(Netgear Switch) (Config) #iscsi cos dscp 46
(Netgear Switch) (Config) #iscsi aging time 10
(Netgear Switch) (Config) #exit
```

Main UI: Enable iSCSI awareness with DSCP

To use the main UI to enable iSCSI awareness, set a DSCP queue, and set the aging time.

1. Select **Switching > iSCSI > Basic > Global Configuration**.

   A page similar to the following figure displays.



2. Configure the following settings:
   - Select the iSCSI Status **Enable** radio button.
   - Select the QoS Profile **DSCP** radio button.
   - In the **DSCP** menu, select **46**.
   - Select the Remark **Enable** radio button.
   - In the **iSCSI Aging Time** field, enter **10**.
3. Click the **Apply** button. Your settings are saved.

Set the iSCSI target port

If iSCSI does not use the standard IANA-assigned iSCSI ports (3260 and 860), we recommend that you specify the target IP address. This enabled the switch to snoop 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 a main UI procedure.

CLI: Set the iSCSI target port

To use the CLI to set the iSCSI target port to 49154 at IP address 172.16.1.20:

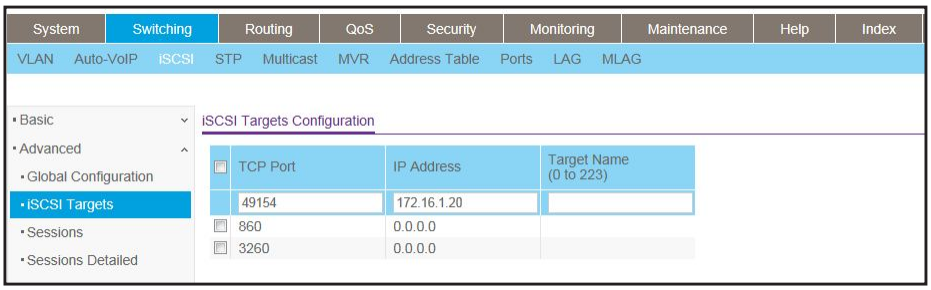
```
(Netgear Switch) #config
(Netgear Switch) (Config) #iscsi target port 49154 address 172.16.1.20
(Netgear Switch) (Config) #exit
```

Main UI: Set the iSCSI target port

To use the main UI to set the iSCSI target port to 49154 at IP address 172.16.1.20:

1. Select **Switching > iSCSI > Advanced > iSCSI Targets**.

   A page similar to the following figure displays.



2. In the **TCP Port** field, enter **49154**.
3. In the **IP Address** field, enter **172.16.1.20**.
4. Click the **Apply** button. Your settings are saved.

Display iSCSI sessions

The example is shown as CLI commands and as a main UI procedure

CLI: Display iSCSI sessions

To use the CLI to display information about iSCSI sessions:

```
(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) #
```

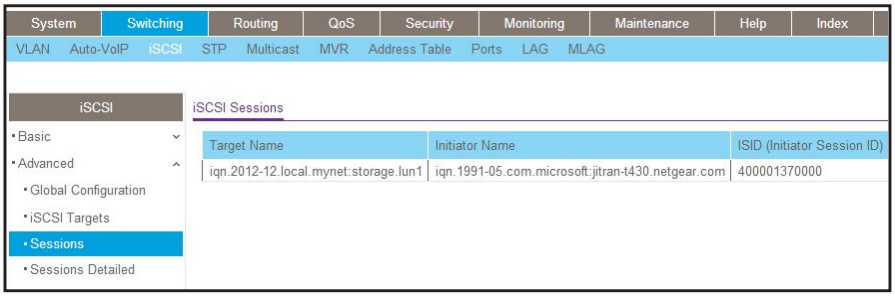
These commands show that there is an active iSCSI session. The initiator is at IP address 192.168.10.107 and the target is at IP address 192.168.10.116

Main UI: Display iSCSI sessions

To use the main UI to display information about iSCSI sessions:

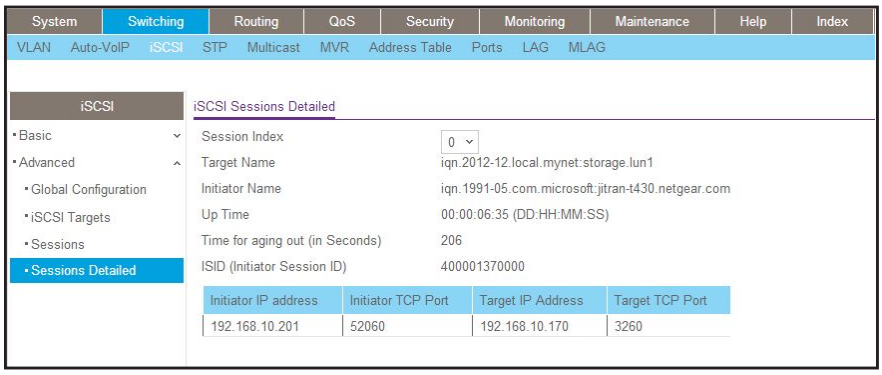
1. Select **Switching > iSCSI > Advanced > Sessions**.

   A page similar to the following figure displays.



2. Select **Switching > iSCSI > Advanced > Sessions Detailed**.

   A page similar to the following figure displays.



40

Override Factory Defaults

Use another factory default configuration file

This feature is supported on the M4250 series switches

This feature is supported on the M4300 series switches

This feature is supported on the M4350 series switches

This chapter includes one section:

- About overriding the factory default configuration file
- Install another factory default configuration file

About overriding 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.

Install another factory default configuration file

The example is shown as CLI commands only.

To 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..
```

5. Erase the old factory default configuration file from the switch.

```
(Netgear Switch) #erase factory-default
```

6. Reload the switch.

   The new factory default configuration file (that is, the factory_default.txt file) takes effect.

41

NETGEAR SFP

Small form-factor pluggables

This feature is supported on the M4250 series switches

This feature is supported on the M4300 series switches

This feature is supported on the M4350 series switches

This chapter includes one section:

- Connect a NETGEAR SFP transceiver module to a third-party switch.

Connect a NETGEAR SFP transceiver module to a third-party switch.

You can connect a NETGEAR SFP transceiver module that is inserted in a NETGEAR switch to a third-party switch.

For example, Cisco provides a way to support third-party small form-factor pluggables (SFPs). In the following procedure, the NETGEAR AGM731F is used as an example.

To let a NETGEAR AGM731F SFP function between a NETGEAR switch and a Cisco 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 autonegotiation mode can be configured on the NETGEAR switch and the Cisco switch.

NETGEAR switch with AGM731F	Cisco switch with AGM731F	Result
Autonegotiation mode	No speed nonegotiate mode	The link is up
No autonegotiation mode	Speed nonegotiate mode	The link is up

Index

Numerics

6in4 tunnels 577
6to4 tunnels 583
802.1AS 716
802.1d (classic STP) 549
802.1s (MSTP) 552
802.1w (RSTP) 551
802.1x (port security) 344

A

access ports 74
accounting for commands 393
ACL mirroring 216
ACL redirection 221
ACLs (access control lists) 180
active directory server, MAB 326
ARP (Address Resolution Protocol)
    dynamic inspection 361
    proxy feature 168
audio video bridging (AVB) 713
authentication manager 395
authorization, privileged EXEC commands 388
Auto VoIP 275
Auto-LAG 84
Automatic error recovery 444
Auto-Trunk 26
AVB (audio video bridging) 713

B

backup router, VRRP 175
banner, pre-login 426
bindings, static 375
bootstrap router (BSR) 628
border routers, OSPF 125
BSR (bootstrap router) 628

C

captive portals 727
change of authorization (CoA), RADIUS 398
class, DiffServ 251
classic STP 549
color conform policies, DiffServ 287
command accounting 393
compatibility, switch stack firmware 478
compatible mode, MVR 310
configuration files, switch stacks 478
configuration scripting 425
CoS (Class of Service) queuing 242

D

DAI (Dynamic ARP inspection) 361
default configuration file, overriding 745
default routes, port routing 93
dense mode, PIM 603
DHCP L2 relay 655
DHCP L3 relay 660
DHCP messages, maximum rate 376
DHCP reservation, configuring 504
DHCP servers
    configuring 500
    rogue, finding 371
DHCP snooping 368
DHCPv6 relay 523
DHCPv6 routing interface 572
DHCPv6 servers 508
Differentiated Services Code Point (DSCP)
    CoS queuing 242
    DiffServ 251
    iSCSI 738
DiffServ (Differentiated Services) 251
Distance Vector Multicast Routing Protocol (DVMRP) 685
DNS (domain name system) 495
double VLANs (DVLANs) 538
DSCP (Differentiated Services Code Point)
    CoS queuing 242
    DiffServ 251
    iSCSI 738
dual images 438
DVLANs (double VLANs) 538

DVMRP (Distance Vector Multicast Routing Protocol) 685
Dynamic ARP inspection (DAI) 361
dynamic mode
  DHCP server 500
  MVR 317
dynamic port locking 333

E

edge device, DiffServ 251
email alerting, syslog 460
end-to-end, PTP transparent clock 706
Error disablement 444
EXEC command authorization 388

F

factory defaults, overriding 745
firmware and firmware mismatch, switch stacks 472

G

GARP (Generic Attribute Registration Protocol) 58
groups
  captive portal 731
  link state 721
guest VLANs 349
GVRP (GARP VLAN Registration Protocol) 58

H

host name, DNS 497
hosts, logging 459

I

IGMP (Internet Group Management Protocol) snooping and querying 297
inter-area routers
  IPv4 119
  IPv6 511
interior node, DiffServ 251
IP ACLs 181
IP source guard 377
IPv6
  ACLs 233
  configuring interfaces 563
  DHCPv6 servers 508
  DiffServ 282
  inter-area routers 511
  tunnels 577
IPv6 stateless RA guard 400
iSCSI initiators and targets 738
isolated ports 64, 340
isolated VLANs 64, 202

L

LAG, Auto- 84
LAGs (link aggregation groups) 82
levels of severity, syslog 461
limits, dynamic and static MAC addresses 334
link dependency 721
locking ports 333
Loop protection 446

M

MAB (MAC Authentication Bypass) 325
MAC ACLs 180
MAC addresses, static 337
MAC Authentication Bypass (MAB) 325
MAC-based VLANs 36
management ACLs 231
managing, switch stacks 475
mapping
  CoS queues 242
  static 366
master router, VRRP 173
master switch and member switches, switch stacks 464
migrating configuration, switch stacks 474
mirroring
  ACLs 216
  ports 427
MLD (multicast listener discovery) 666
MMRP (Multiple MAC Registration Protocol) 715
monitoring, sFLow 488
moving, stack master 482
MRP (Multiple Registration Protocol) 714
MSRP (Multiple Stream Reservation Protocol) 715
MSTP (multiple STP) 552
multicast routers 301
multicast VLAN registration (MVR) 309
Multiple MAC Registration Protocol (MMRP) 715
Multiple Registration Protocol (MRP) 714
Multiple Stream Reservation Protocol (MSRP) 715
Multiple VLAN Registration Protocol (MVRP) 715
MVR (multicast VLAN registration) 309
MVRP (Multiple VLAN Registration Protocol) 715

N

network active directory server, MAB 326
network policy server, MAB 326
Nondisruptive configuration management 449
NSSA areas, OSPF 140

O

organizationally unique identifier (OUI) 276
OSPF (Open Shortest Path First) 119
OUI-based auto VoIP 276
outbound Telnet 441

P

Per VLAN (Rapid) Spanning Tree Protocol (PV(R)STP) 555
PIM (Protocol Independent Multicast) 603
policy based routing (PBR) 162
policy server, MAB 326
policy, DiffServ 251
port analyzer 428
port mirroring 427
port routing 88
port security 333
Precision Time Protocol (PTP) 704
preconfiguring, switch stack members 479
primary VLANs 64
priority values, switch stack members 467
private VLAN groups 542
private VLANs 64
promiscuous ports 65
protected ports 338
Protocol Independent Multicast (PIM) 603
protocol-based auto VoIP 275
protocol-based VLANs 39
PTP (Precision Time Protocol) 704
PV(R)STP (Per VLAN (Rapid) Spanning Tree Protocol) 555

Q

queriers, IGMP 303
queues, CoS 243

R

RADIUS
  accounting server 394
  assigning VLANs 356
  captive portal authorization 734
RADIUS change of authorization (CoA) 398
RADIUS server, MAB 326
redirection, ACLs 221
relay, DHCPv6 523
relays, DHCP L2 and DHCP L3 654
remote switched port analyzer (RSPAN) 428
renumbering, switch stack members 480
reverse path forwarding (RPF) 604
RIP (Routing Information Protocol) 105
rogue DHCP servers 371
route-map statement 162
routing interface, configuring for IPv6 564
routing, VLANs 98
RPF (reverse path forwarding) 604
RSPAN (remote switched port analyzer) 428
RSTP (rapid STP) 551
rules, ACLs 180

S

sampling, sFlow 492
SCCP (Skinny Call Control Protocol) 275
scheduler mode, strict priority 245
scripting, configuration 425
security, ports 333
service, DiffServ 251
Session Initiation Protocol (SIP) 275
session limit and time-out, Telnet 443
severity levels, syslog 461
sFlow monitoring 488
shaping traffic, CoS 248
Simple Network Time Protocol (SNTP) 407, 416
SIP (Session Initiation Protocol) 275
Skinny Call Control Protocol (SCCP) 275
small form-factor pluggable (SFP) 748
SNMP (Simple Network Management Protocol) 484
snooping
  DHCP 368
  IGMP 297
  MLD 679
SNTP (Simple Network Time Protocol) 407, 416
Spanning Tree Protocol (STP) 549
sparse mode, PIM 627
SSL certificates 735
stacking switches 463
stateful address assignment, IPv6 508
stateless DHCPv6 server 515, 519
stateless RA guard, IPv6 400

static bindings 375
static MAC addresses 337
static mapping 366
static port locking 333
static routes, port routing 94
STP (Spanning Tree Protocol) 549
strict priority schedule mode, CoS 245
stub areas, OSPF 131
subnet-based VLANs 44
switch port modes 74
switch stacks 463
system logging (syslog), logging, syslog 453

T

TACACS+ accounting server 393
target port, iSCSI 741
TCP flags, ACLs 187
Telnet, outbound 441
time zone, SNTP server 412
traceroute 424, 425
traffic shaping, CoS 248
transparent clock, PTP 705
traplogs, syslog 457
traps, SNMP 486
trunk ports 74
Trunk, Auto- 26
trust mode
    global, configuring 244
    interface, configuring for 247
trusted ports, CoS 242
tunnels, IPv6 577

U

untrusted ports, CoS 243
upgrading firmware, switch stacks 473
users, captive portal 731

V

Virtual Router Redundancy Protocol (VRRP)
    concepts and configuring 172
virtual VLANs 44
VLAN groups, private 542
VLAN priority tag (VPT) 738
VLAN routing
    concepts and configuring 98
    IPv6 567
    OSPF 151
    RIP 113
VLANs
    concepts and configuring 25
    double VLANs 538
    guest VLANs 349
    voice 47
voice VLANs 47
VoIP (voice over IP)
    auto 275
    DiffServ 267
VPTs (VLAN priority tag) 738
VRRP (Virtual Router Redundancy Protocol)
    concepts and configuring 172

W

WRED (weighted random early discard) 242
WRED explicit congestion notification 294